Manuale dell'utente di Cisco Router and Security Device Manager

2.4.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-RETI (6387)
Fax: 408 527-0883

Numero d'ordine cliente:
Numero parte del testo: OL-9959-04

LE SPECIFICHE E LE INFORMAZIONI RELATIVE AI PRODOTTI CONTENUTI NELLA PRESENTE GUIDA SONO SOGGETTI A MODIFICA SENZA PREAVVISO. TUTTE LE COMUNICAZIONI, LE INFORMAZIONI E LE RACCOMANDAZIONI SONO RITENUTE CORRETTE MA VENGONO PRESENTATE SENZA GARANZIA ALCUNA, ESPRESSA O IMPLICITA. GLI UTENTI DEVONO ASSUMERSI LA COMPLETA RESPONSABILITÀ PER L'UTILIZZO DI QUALSIASI PRODOTTO.

LA LICENZA PER IL SOFTWARE E LA GARANZIA LIMITATA PER IL PRODOTTO CORRELATO SONO ACCLUSE NEL PACCHETTO INFORMATIVO FORNITO CON IL PRODOTTO E SONO CITATE IN QUESTA GUIDA TRAMITE IL PRESENTE RIFERIMENTO. SE NON VIENE INDIVIDUATA LA LICENZA PER IL SOFTWARE O LA GARANZIA LIMITATA, RIVOLGERSI AL RAPPRESENTANTE CISCO PER OTTENERE UNA COPIA.

L'implementazione Cisco della compressione delle intestazioni è un adattamento del programma sviluppato dall'Università di Berkeley, California (UCB) come parte della versione di dominio pubblico del sistema operativo UNIX. Tutti i diritti riservati. Copyright © 1981, Regents of the University of California.

A PRESCINDERE DA QUALSIASI TIPO DI GARANZIA FORNITA, TUTTI I FILE DELLA DOCUMENTAZIONE E IL SOFTWARE DEI SUDDETTI FORNITORI VENGONO INCLUSI “COSÌ COME SONO” CON TUTTI I POSSIBILI DIFETTI. CISCO E I FORNITORI SOPRA INDICATI NON RILASCIANO ALCUNA GARANZIA, ESPLICITA O IMPLICITA, INCLUSE SENZA LIMITAZIONE LE GARANZIE DI COMMERCIABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO, DI NON VIOLAZIONE DEI DIRITTI ALTRUI O DERIVANTI DA CONSUETUDINE, USO O PRASSI COMMERCIALE.

IN NESSUN CASO CISCO O I SUOI FORNITORI SARANNO RESPONSABILI PER EVENTUALI DANNI INDIRETTI, SPECIALI, CONSEQUENZIALI O INCIDENTALI, INCLUSI SENZA LIMITAZIONE LA PERDITA DI PROFITTO O LA PERDITA O IL DANNEGGIAMENTO DEI DATI DERIVANTI DALL'UTILIZZO O DALL'INCAPACITÀ DI UTILIZZARE, ANCHE QUALORA CISCO O I SUOI FORNITORI SIANO STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI.

Tutti gli indirizzi IP (Internet Protocol) utilizzati in questo documento non si riferiscono ad indirizzi reali. Gli esempi, le rappresentazioni dei comandi e le figure presenti nel documento servono solo a scopo illustrativo. L'eventuale utilizzo di indirizzi IP reali nel contenuto illustrativo è da ritenersi non intenzionale e puramente casuale.

Manuale dell'utente di Cisco Router and Security Device Manager 2.4

SOMMARIO

CAPITOLO 1

Pagina principale

Nella pagina principale sono fornite le informazioni di base sull'hardware, sul software e sulla configurazione del router in uso. In questa pagina sono incluse le informazioni riportate di seguito.

Nome host

Nome configurato del router.

Informazioni sul router

Vengono visualizzate le informazioni di base sull'hardware e sul software del router in uso e, inoltre, sono inclusi i seguenti campi:

Hardware		Software	
Tipo di modello	Viene visualizzato il numero del modello di router.	**Versione IOS**	La versione del software Cisco IOS attualmente in esecuzione sul router.
Memoria totale/disponibile	RAM disponibile/RAM totale	**Versione Cisco SDM**	La versione del software Cisco Router and Security Device Manager (Cisco SDM) attualmente in esecuzione sul router.

Hardware		Software	
Capacità memoria flash totale	Memoria flash + webflash (se applicabile)		
Funzioni disponibili	Le funzioni disponibili nell'immagine Cisco IOS che il router sta utilizzando sono contrassegnate da un segno di spunta. Le funzioni che Cisco SDM verifica sono: IP, Firewall, VPN, IPS e NAC.		

Altro...

Altro... consente di visualizzare una finestra popup contenente dettagli aggiuntivi su hardware e software.

- Dettagli hardware: oltre alle informazioni presentate nella sezione Informazioni sul router, in questa scheda sono disponibili le informazioni riportate di seguito.
  - Avvio del router: memoria flash o file di configurazione.
  - Eventuali acceleratori del router, ad esempio gli acceleratori VPN.
  - Uno schema della configurazione hardware, comprendente anche la memoria flash e i dispositivi tipo flash USB e token USB installati.
- Dettagli software: oltre alle informazioni presentate nella sezione Informazioni sul router, in questa scheda sono disponibili le informazioni riportate di seguito.
  - Set di funzioni inclusi nell'immagine IOS.
  - Versione di Cisco SDM in esecuzione.

Panoramica della configurazione

In questa sezione della pagina principale vengono riepilogate le impostazioni di configurazione effettuate.

Nota Se questo argomento della Guida descritto nella pagina principale non contiene informazioni su una determinata funzione, significa che l'immagine Cisco IOS non supporta tale funzione. Ad esempio, se sul router è in esecuzione un'immagine Cisco IOS che non supporta le funzioni di protezione, nella pagina principale non vengono visualizzate le sezioni relative al criterio firewall, la rete VPN e Intrusion Prevention.

Visualizza configurazione corrente

Fare clic su questo pulsante per visualizzare la configurazione corrente del router.

Interfacce e connessioni	**Attivato (*n*)**: il numero delle connessioni LAN e WAN attivate.	**Disattivato (*n*)**: il numero delle connessioni LAN e WAN disattivate.	**Doppia freccia**: consente di mostrare/nascondere i dettagli.
Totale reti LAN supportate	Indica il numero totale delle interfacce LAN presenti nel router.	Totale reti WAN supportate	Indica il numero delle interfacce WAN supportate da Cisco SDM presenti nel router.
Interfaccia LAN configurata	Indica il numero delle interfacce LAN supportate da SDM attualmente presenti nel router.	Totale connessioni WAN	Indica il numero totale delle connessioni WAN supportate da Cisco SDM presenti nel router.
Server DHCP	Configurato/ Non configurato		
Pool DHCP (visualizzazione dettagli)	Se è configurato un solo pool, sono presenti gli indirizzi iniziali e finali del pool DHCP. Se sono configurati più pool, è presente un elenco dei nomi dei pool configurati.	**Numero di client DHCP (visualizzazione dettagli)**	Numero corrente dei client che acquisiscono indirizzi.
Interfaccia	**Tipo**	**IP/Maschera**	**Descrizione**
Nome dell'interfaccia configurata	Tipo interfaccia	Indirizzo IP e subnet mask	Indica la descrizione dell'interfaccia

Criteri firewall	**Attivo/Non attivo**	**Trusted (*n*)**	**Untrusted (*n*)**	**DMZ (*n*)**
	Attivo: firewall in funzione. Non attivo: firewall disattivato.	Numero delle interfacce (interne) trusted.	Numero delle interfacce (esterne) untrusted.	Numero delle interfacce DMZ.
Interfaccia	**Icona firewall**	**NAT**	**Inspection Rule**	**Regola di accesso**
Nome dell'interfaccia a cui è stato applicato un firewall	Eventuale scelta dell'interfaccia come interfaccia interna o esterna.	Nome o numero della regola NAT applicata all'interfaccia.	Nomi o numeri delle Inspection Rule in ingresso e in uscita.	Nomi o numeri delle regole di accesso in ingresso e in uscita.

VPN	**Attivato (*n*)**: indica il numero delle connessioni VPN attive.		
IPSec (Site-to-Site)	Indica il numero delle connessioni VPN site-to-site configurate.	**GRE su IPSec**	Indica il numero delle connessioni GRE su IPSec configurate.
Accesso Xauth richiesto	Indica il numero delle connessioni Easy VPN in attesa di un accesso Xauth. *Vedere nota*.	**Easy VPN Remote**	Indica il numero delle connessioni Easy VPN Remote configurate.
Nr. di client DMVPN	Se il router è configurato come hub DMVPN, indica il numero di client DMVPN.	**Numero di client VPN attivi**	Se il router sta funzionando come server Easy VPN, indica il numero di client Easy VPN con connessioni attive.
Interfaccia	**Tipo**	**Criterio IPSec**	**Descrizione**
Nome di un'interfaccia con una connessione VPN configurata.	Tipo di connessione VPN configurata sull'interfaccia.	Nome del criterio IPSec associato alla connessione VPN.	Descrizione della connessione.

Nota

- Alcuni server o concentratori VPN consentono l'autenticazione di client con Autenticazione estesa (XAuth), che indica il numero dei tunnel VPN in attesa di un accesso Xauth. Se un tunnel Easy VPN è in attesa di un accesso XAuth, in un altro riquadro messaggi viene visualizzato un pulsante Accesso. Facendo clic su **Accesso** è possibile immettere le credenziali per il tunnel.
- Se Xauth è stato configurato per un tunnel, comincerà a funzionare solo dopo aver fornito le informazioni per l'accesso e la password. Il tempo necessario per l'immissione di queste informazioni non è definito.

NAC Policy	**Attivo o Inattivo**
Colonna Interfaccia	**Colonna NAC Policy**
Il nome dell'interfaccia su cui si applicano le policy. Per esempio, FastEthernet 0 o Ethernet 0/0.	Il nome della Policy NAC

Routing		**Intrusion Prevention**	
Numero delle route statiche	Indica il numero delle route statiche configurate sul router.	**Firme attive**	Indica il numero delle firme attive utilizzate dal router. Possono essere firme incorporate o caricate da una posizione remota.
Protocolli routing dinamico	Elenca tutti i protocolli di routing dinamico configurati sul router.	**Numero delle interfacce con IPS attivato**	Indica il numero delle interfacce del router su cui è stato attivato IPS.

Routing		**Intrusion Prevention**	
		Versione SDF	La versione dei file SDF su questo router.
		Dashboard protezione	Un collegamento al dashboard protezione IPS in cui è possibile visualizzare e distribuire le prime dieci firme.

CAPITOLO 2

Procedura guidata LAN

La procedura guidata LAN di Cisco Router and Security Device Manager (Cisco SDM) mostra la configurazione di un'interfaccia LAN. Nella schermata sono elencate le interfacce LAN del router. È possibile selezionare qualsiasi interfaccia visualizzata nella finestra e fare clic su **Configura** per renderla un'interfaccia LAN e configurarla.

In questa finestra sono elencate le interfacce del router indicate come interfacce interne nella configurazione d'avvio, le interfacce Ethernet e le porte switch non configurate come interfacce WAN. Nell'elenco sono incluse le interfacce già configurate.

Quando si configura un'interfaccia come interfaccia LAN, Cisco SDM inserisce nel file di configurazione il testo di descrizione $ETH-LAN$ in modo tale che in seguito l'interfaccia verrà riconosciuta come interfaccia LAN.

Interfaccia

Nome dell'interfaccia

Configura

Scegliere questo pulsante per configurare l'interfaccia selezionata. Se l'interfaccia non è stata ancora configurata, Cisco SDM attiverà la procedura guidata LAN per facilitarne la configurazione. Se, invece, l'interfaccia è stata configurata mediante Cisco SDM, Cisco SDM visualizzerà una finestra Modifica che consente di cambiare le impostazioni della configurazione.

Se si seleziona un'interfaccia LAN con una configurazione non supportata da Cisco SDM, il pulsante Configura può essere disattivato. Per visualizzare l'elenco di queste configurazioni, vedere Motivi per i quali la configurazione di un'interfaccia Ethernet può essere di sola lettura.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurazione o modifica di un'interfaccia LAN o di una porta switch LAN.	Selezionare l'interfaccia LAN o la porta switch nell'elenco e fare clic su **Configura**. Se l'interfaccia non è stata ancora configurata o se si seleziona una porta switch, Cisco SDM attiverà la procedura guidata LAN per consentire all'utente di configurare l'interfaccia. Se l'interfaccia è già configurata e se non si tratta di una porta switch, facendo clic su **Configura** viene visualizzata una finestra Modifica in cui è possibile apportare delle modifiche alla configurazione LAN.
Riconfigurazione dell'indirizzo e della maschera IP o delle proprietà DHCP di un'interfaccia già configurata.	Selezionare un'interfaccia con un indirizzo IP e fare clic su **Configura**.
Configurazioni collegate alla rete LAN specifiche per elementi quali i server DHCP o le impostazioni MTU (maximum transmission unit).	Fare clic su **Interfacce e connessioni** della barra categoria Cisco SDM, quindi sulla scheda **Modifica interfacce e connessioni** ed eseguire tutte le modifiche di configurazione.
Reperimento di informazioni su come eseguire attività di configurazione correlate.	Visualizzare una delle seguenti procedure: • Come configurare una route statica? • Come visualizzare l'attività dell'interfaccia LAN? • Come attivare o disattivare un'interfaccia? • Come visualizzare i comandi IOS inviati al router? • Come avviare l'applicazione wireless da Cisco SDM?

Quando necessario, è possibile ritornare a questa schermata per configurare le interfacce LAN aggiuntive.

Configurazione Ethernet

La procedura guidata mostra la configurazione di un'interfaccia Ethernet in una rete LAN. Sono richieste le seguenti informazioni:

- Un indirizzo IP e una subnet mask per l'interfaccia Ethernet.
- Un pool d'indirizzi DHCP se si decide di utilizzare DHCP in questa interfaccia.
- Indirizzi dei server DNS e WINS nella rete WAN.
- Un nome di dominio.

Procedura guidata LAN - Selezionare un'interfaccia

Selezionare l'interfaccia in cui si desidera configurare una connessione LAN. In questa finestra sono elencate le interfacce che sono in grado di supportare le configurazioni Ethernet LAN.

Procedura guidata LAN - Indirizzo IP e subnet mask

Questa finestra consente di configurare un indirizzo IP e una subnet mask per l'interfaccia Ethernet scelta nella prima finestra.

Indirizzo IP

Immettere l'Indirizzo IP dell'interfaccia in formato decimale separato da punti. L'amministratore di rete deve determinare gli indirizzi IP delle interfacce LAN. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. Per ottenere questo valore, contattare l'amministratore di rete. La subnet mask consente al router di determinare quale parte dell'indirizzo IP viene utilizzato per definire l'indirizzo di rete e dell'host.

In alternativa, selezionare il numero di bit di rete. Questo valore è utilizzato per calcolare la subnet mask. È possibile richiedere il numero di bit di rete da immettere all'amministratore di rete.

Procedura guidata LAN - Attivare il server DHCP

Questa schermata consente di attivare un server DHCP sul router. Un server DHCP assegna automaticamente indirizzi IP riutilizzabili ai dispositivi nella rete LAN. Quando si attiva un dispositivo nella rete, il server DHCP concede un Indirizzo IP. Quando il dispositivo esce dalla rete, l'indirizzo IP ritorna al pool e può essere utilizzato da un altro dispositivo.

Per attivare un server DHCP sul router

Fare clic su **Sì**.

Procedura guidata LAN - Pool di indirizzi DHCP

Questa schermata consente di configurare il pool di indirizzi IP DHCP. Gli indirizzi IP assegnati dal server DHCP vengono ottenuti da un pool comune configurato mediante l'indicazione dell'indirizzo IP iniziale e dell'indirizzo finale nell'intervallo.

Per maggiori informazioni vedere Pool di indirizzi DHCP.

Nota Se sono presenti pool di indirizzi discontinui configurati sul router, i campi degli indirizzi IP iniziali e finali saranno di sola lettura.

IP iniziale

Immettere la parte iniziale dell'intervallo degli indirizzi IP per il server DHCP da utilizzare nell'assegnazione degli indirizzi ai dispositivi nella rete LAN. È l'indirizzo IP più piccolo dell'intervallo.

IP finale

Immettere l'Indirizzo IP con il numero più elevato nell'intervallo degli indirizzi IP.

Campi Server DNS e Server WINS

Se in questa finestra vengono visualizzati i campi Server DNS e Server WINS, è possibile fare clic su Opzioni DHCP per visualizzare informazioni relative agli stessi.

Opzioni DHCP

In questa finestra è possibile configurare le opzioni DHCP inviate agli host della rete LAN che richiedono gli indirizzi IP dal router. Non si tratta di opzioni che l'utente configura per il router, ma di parametri che saranno inviati agli host della rete LAN che ne fanno richiesta. Per impostare queste proprietà per il router, fare clic su **Attività aggiuntive** nella barra categoria Cisco SDM, quindi su **DHCP** e configurare le impostazioni nella finestra Pool DHCP.

Server DNS 1

Il server DNS consente di eseguire la mappatura di un dispositivo conosciuto mediante l'indirizzo IP. Se è stato configurato un server DNS per la rete, immettere l'indirizzo IP per quel dispositivo.

Server DNS 2

Se nella rete è disponibile un server DNS aggiuntivo, è possibile immettere l'indirizzo IP per quel server in questo campo.

Nome di dominio

Con il server DHCP che si sta configurando sul router verranno forniti servizi ad altri dispositivi interni al dominio. Immettere il nome del dominio.

Server WINS 1

Per alcuni client è necessario disporre di WINS (Windows Internet Naming Service) per connettersi ai dispositivi in Internet. Se nella rete è disponibile un server WINS, immettere l'indirizzo IP per il server in questo campo.

Server WINS 2

Se nella rete è disponibile un server WINS aggiuntivo, immettere l'indirizzo IP per il server in questo campo.

Procedura guidata LAN - Modalità VLAN

Questa schermata consente di determinare il tipo di informazioni VLAN che saranno riportate sulla porta switch. Le porte switch possono essere indicate in modalità di accesso e quindi potranno trasmettere solo i dati relativi alla rete VLAN a cui sono assegnate, oppure in modalità trunking e quindi potranno trasmettere i dati per tutte le reti VLAN inclusa quella a cui sono assegnate.

Se questa porta switch sarà collegata a un unico dispositivo, ad esempio a un unico PC o a un telefono IP, oppure se questo dispositivo sarà collegato a una porta di un dispositivo di rete, ad esempio un altro switch, ovvero una porta in modalità di accesso, selezionare **Dispositivo singolo**.

Se invece questa porta switch sarà collegata a un dispositivo di rete, ad esempio un altro switch, vale a dire una porta in modalità trunking, selezionare **Dispositivo di rete**.

Procedura guidata LAN - Porta switch

Questa schermata consente di assegnare un numero VLAN esistente a una porta switch o di creare una nuova interfaccia VLAN da assegnare alla porta switch LAN.

VLAN esistente

Per assegnare la porta switch a una rete VLAN già definita, ad esempio la rete VLAN predefinita (VLAN 1), immettere il numero ID VLAN nel campo Identificatore di rete (VLAN).

Nuova VLAN

Se si desidera creare una nuova interfaccia VLAN a cui verrà assegnata la porta switch, immettere il nuovo numero ID VLAN nel campo Nuova VLAN, quindi immettere l'indirizzo IP e la subnet mask della nuova interfaccia logica VLAN nei campi Indirizzo IP e Subnet mask.

Includere la rete VLAN in un bridge IRB che forma un bridging con la rete wireless. (Use Wireless Application to complete.)

Se si seleziona questa casella, la porta switch forma parte del bridging con la rete wireless. L'altra parte del bridging deve essere configurata utilizzando l'applicazione wireless. I campi Indirizzo IP e Subnet mask in Nuova VLAN sono disattivate se questa casella è selezionata.

Una volta completata la configurazione LAN, eseguire la procedura indicata di seguito per avviare l'applicazione wireless e completare la configurazione del bridging.

Passo 1 Selezionare **Applicazione wireless** dal menu Strumenti di Cisco SDM. L'applicazione viene visualizzata in un'altra finestra del browser.

Passo 2 In Applicazione wireless, fare clic su **Wireless Express Security** e selezionare **Bridging** per le informazioni utili al completamento della configurazione del bridging.

Bridge IRB

Se si sta configurando un'interfaccia VLAN come parte di un bridge IRB, il bridge deve essere un membro di un bridge group.

Per creare un nuovo bridge group di cui l'interfaccia faccia parte, fare clic su **Crea un nuovo Bridge Group** e immettere un valore compreso tra 1 e 255.

Affinché l'interfaccia VLAN diventi membro di un bridge group esistente, fare clic su **Unisci un Bridge Group esistente** e selezionare un bridge group.

Nota Una volta completata la configurazione del bridge nell'applicazione wireless, occorre utilizzare lo stesso numero di bridge group immesso in questa schermata.

Configurazione BVI

Assegnare un indirizzo IP e una subnet mask all'interfaccia BVI. Se nella schermata precedente è stato selezionato un bridge group esistente, l'indirizzo IP e la subnet mask verranno visualizzati in questa schermata. È possibile apportarvi modifiche o lasciare i valori invariati**.**

Indirizzo IP

Immettere l'Indirizzo IP dell'interfaccia in formato decimale separato da punti. L'amministratore di rete deve determinare gli indirizzi IP delle interfacce LAN. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Net Mask

Immettere la subnet mask. Per ottenere questo valore, contattare l'amministratore di rete. La subnet mask consente al router di determinare quale parte dell'indirizzo IP viene utilizzato per definire l'indirizzo di rete e dell'host.

Bit di rete

In alternativa, selezionare il numero di bit di rete. Questo valore è utilizzato per calcolare la subnet mask. È possibile richiedere il numero di bit di rete da immettere all'amministratore di rete.

Pool DHCP per BVI

Quando si configura il router come un server DHCP, è possibile creare un pool di indirizzi IP che i client della rete possono utilizzare. Quando un client si disconnette dalla rete, l'indirizzo che è stato utilizzato viene restituito al pool per essere utilizzato da un altro host.

Configurazione server DHCP

Selezionare questa casella se si desidera che il router funzioni come un server DHCP. Specificare gli indirizzi IP iniziale e finale del pool. Assicurarsi di indicare gli indirizzi IP nella stessa subnet dell'indirizzo IP dell'interfaccia. Ad esempio, se all'interfaccia è stata assegnata l'indirizzo IP 10.10.22.1, con una subnet mask 255.255.255.0, si dispone di oltre 250 indirizzi per il pool ed è possibile specificare un **Indirizzo IP iniziale** 10.10.22.2 e un **Indirizzo IP finale** 10.10.22.253.

IRB per Ethernet

Se nel router è presente un'interfaccia wireless, è possibile utilizzare IRB (Integrated Routing and Bridging) affinché l'interfaccia faccia parte di un bridging con la rete LAN wireless e il traffico destinato alla rete wireless venga instradato attraverso questa interfaccia. Fare clic su **Sì** se si desidera configurare l'interfaccia di livello 3 per IRB (Integrated Routing and Bridging).

Se non si desidera che questa interfaccia venga utilizzata nel bridging verso l'interfaccia wireless, fare clic su **No**. Si sarà comunque in grado di configurarla come un'interfaccia di routing.

Configurazione Ethernet Layer 3

Cisco SDM supporta la configurazione Ethernet Layer 3 sui router con moduli switch 3750 installati. È possibile configurare le VLAN e attivare la funzione di DHCP server sulle interfacce Ethernet

Configurazione 802.1Q

È possibile configurare una VLAN che non utilizza il protocollo d'incapsulamento 802.1Q usato per le connessioni in trunking. Indicare il numero ID VLAN e selezionare **VLAN nativa** se non si desidera che la rete VLAN utilizzi il tagging 802.1Q.

Se invece si desidera utilizzare il tagging 802.1Q, lasciare la casella di controllo VLAN nativa non selezionata.

Configurazione Trunking o Routing

È possibile configurare interfacce Ethernet Layer 3 in modalità trunking 802.1Q o in modalità routing di base. Se si configura l'interfaccia per il trunking 802.1Q, è possibile configurare le VLAN sull'interfaccia, ed è possibile configurare una VLAN nativa che non utilizza il protocollo d'incapsulamento 802.1Q. Se si configura l'interfaccia per il routing non è possibile configurare interfacce secondarie o VLAN aggiuntive sull'interfaccia.

Configurazione modulo switch dispositivo

Se si sta configurando un'interfaccia Gigabit Ethernet per il routing, i parametri del modulo switch possono essere immessi in questa finestra. L'immissione di queste informazioni non è obbligatoria.

È possibile fornire un indirizzo IP e una subnet mask per il modulo switch, e le credenziali di login richieste per l'accesso all'interfaccia del modulo switch.

Selezionare la casella nella parte inferiore della schermata se si desidera accedere al modulo switch dopo avere fornito i parametri in questa procedura guidata e dopo aver trasmesso la configurazione al router.

Configura interfaccia Gigabit Ethernet

Indicare in questa finestra l'indirizzo IP e la subnet mask per le interfacce Gigabit Ethernet. Per maggiori informazioni sugli indirizzi IP e sulle subnet mask, vedere Procedura guidata LAN - Indirizzo IP e subnet mask.

Indirizzo IP dell'interfaccia fisica

Immettere in questi campi l'indirizzo IP e la subnet mask per l'interfaccia fisica Gigabit Ethernet.

Indirizzo IP delle sottointerfacce virtuali delle VLAN

Immettere in questi campi l'indirizzo IP e la subnet mask per la sottointerfaccia virtuale VLAN che si desidera creare sull'interfaccia fisica. Questi campi vengono visualizzati se si sta configurando l'interfaccia per il routing. I campi non vengono visualizzati se si sta configurando l'interfaccia per l'IRB (Integrated Routing and Bridging).

Riepilogo

In questa finestra viene fornito un riepilogo delle modifiche di configurazione eseguite per l'interfaccia selezionata.

Per salvare questa configurazione nella configurazione del router in esecuzione e uscire da questa procedura guidata

Fare clic su **Fine**. In Cisco SDM le modifiche apportate alla configurazione vengono salvate nella configurazione del router in esecuzione. Tali modifiche hanno effetto immediatamente ma andranno perse se il router verrà disattivato.

Se è stata selezionata l'opzione **Eseguire l'anteprima dei comandi prima dell'inoltro al router** nella finestra Preferenze utente, viene visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi dell'interfaccia della riga di comando inviati al router.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come configurare una route statica?

Per configurare una route statica:

Passo 1 Dalla barra categoria, fare clic su **Routing**.

Passo 2 Nel gruppo Routing statico, fare clic su **Aggiungi...**.

Viene visualizzata la finestra di dialogo Aggiungi IP route statica.

Passo 3 Nel campo Prefisso immettere l'indirizzo IP della rete della route statica di destinazione.

Passo 4 Nel campo Maschera prefisso immettere la subnet mask della rete di destinazione.

Passo 5 Per impostare come predefinita questa route statica, selezionare la casella di controllo **Imposta come route predefinita**.

Passo 6 Nel gruppo Inoltro, scegliere se identificare un'interfaccia del router o l'indirizzo IP del router di destinazione come metodo per inoltrare i dati, quindi scegliere l'interfaccia del router di inoltro o immettere l'indirizzo IP del router di destinazione.

Passo 7 Immettere eventualmente il valore della distanza da registrare nella tabella di routing nel campo Unità di misura distanza.

Passo 8 Per configurare la route statica come route permanente, ovvero una route che non viene cancellata nemmeno quando l'interfaccia viene chiusa o se il router non è in grado di comunicare con un altro router, selezionare la casella di controllo **Route permanente**.

Passo 9 Fare clic su **OK**.

Come visualizzare l'attività dell'interfaccia LAN?

È possibile visualizzare l'attività dell'interfaccia LAN utilizzando la modalità Controllo in Cisco SDM. Con tale modalità è possibile visualizzare statistiche sull'interfaccia LAN, incluso il numero di pacchetti e byte che sono stati inviati o ricevuti dall'interfaccia e il numero di errori in trasmissione o in ricezione che si sono verificati. Per visualizzare le statistiche sull'interfaccia LAN, eseguire la procedura descritta di seguito.

Passo 1 Nella barra degli strumenti, fare clic su **Controlla**.

Passo 2 Nel frame a sinistra, fare clic su **Stato dell'interfaccia**.

Passo 3 Nel campo Selezionare un'interfaccia, selezionare l'interfaccia LAN che si desidera utilizzare per visualizzare le statistiche.

Passo 4 Scegliere i dati da visualizzare selezionando le relative caselle di controllo. È possibile visualizzare fino a quattro statistiche per volta.

Passo 5 Fare clic su **Avvia monitoraggio** per visualizzare le statistiche di tutti i dati selezionati.

Viene visualizzata la schermata Dettagli interfaccia che mostra le statistiche selezionate. Il router viene interrogato ogni 10 secondi, quindi i dati visualizzati sono in tempo reale. Se si tratta di un'interfaccia attiva con trasmissione di dati viene visualizzato un incremento nel numero di pacchetti e byte trasferiti.

Come attivare o disattivare un'interfaccia?

È possibile disattivare un'interfaccia senza rimuoverne la configurazione e riattivare un'interfaccia non attiva.

Passo 1 Fare clic su **Interfacce e connessioni** nella barra categoria.

Passo 2 Fare clic sulla scheda **Modifica interfacce e connessioni**.

Passo 3 Selezionare l'interfaccia che si intende attivare o disattivare.

Passo 4 Se l'interfaccia è attiva, verrà visualizzato il pulsante Disattiva sotto Elenco interfacce. Scegliere questo pulsante per attivare l'interfaccia. Se l'interfaccia non è attiva, nella stessa posizione verrà visualizzato il pulsante Attiva. Scegliere questo pulsante per attivare l'interfaccia.

Come visualizzare i comandi IOS inviati al router?

Se si sta completando una procedura guidata per configurare una funzionalità, è possibile visualizzare i comandi Cisco IOS inviati al router facendo clic su **Fine**.

Passo 1 Dal menu Modifica di Cisco SDM, selezionare **Preferenze**.

Passo 2 Selezionare **Eseguire l'anteprima dei comandi prima dell'inoltro al router.**

Passo 3 Fare clic su **OK**.

Al successivo utilizzo di una procedura guidata per configurare il router e facendo clic su **Fine** nella finestra Riepilogo, verrà visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi CLI inviati alla configurazione del router. Dopo aver visualizzato i comandi, fare clic su**Invia.**

Se si sta modificando una configurazione, facendo clic su **OK** nella finestra di dialogo viene visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi Cisco IOS inviati al router.

Come avviare l'applicazione wireless da Cisco SDM?

Per avviare l'applicazione wireless da Cisco SDM utilizzare la procedura descritta di seguito.

Passo 1 Andare al menu Strumenti di Cisco SDM e selezionare **Applicazione wireless. L'applicazione viene avviata in un'altra finestra del browser.**

Passo 2 Nel pannello di sinistra, fare clic sul titolo della schermata di configurazione in cui si desidera operare. Per informazioni relative a ciascuna schermata, fare clic sull'icona della Guida nell'angolo in alto a destra. L'icona appare come un libro aperto con un punto interrogativo.

CAPITOLO 3

Autenticazione 802.1x

L'autenticazione 802.1x consente a un router Cisco IOS remoto di connettere utenti VPN autenticati a una rete protetta, tramite un tunnel VPN sempre attivo. Il router Cisco IOS esegue l'autenticazione degli utenti tramite un server RADIUS sulla rete protetta.

L'autenticazione 802.1x viene applicata alle porte switch o alle porte Ethernet (instradate) ma non a entrambi i tipi di interfaccia. Se l'autenticazione 802.1x viene applicata a una porta Ethernet, gli utenti non autenticati possono essere instradati all'esterno del tunnel VPN per accedere a Internet.

L'autenticazione 802.1x viene configurata sulle interfacce utilizzando la procedura guidata LAN. Tuttavia, prima di poter attivare l'autenticazione 802.1x su un'interfaccia, è necessario attivare AAA sul router Cisco IOS. Se si tenta di utilizzare la procedura guidata LAN prima di aver attivato AAA, viene visualizzata una finestra in cui si richiede se si desidera attivare AAA. Se si sceglie di attivare AAA, vengono visualizzate le finestre di configurazione 802.1x come parte della procedura guidata LAN. Se si sceglie di *non* attivare AAA, le finestre di configurazione 802.1x *non* vengono visualizzate.

Procedura guidata LAN - autenticazione 802.1x (porte switch)

In questa finestra è possibile attivare l'autenticazione 802.1x sulla porta o sulle porte switch selezionate per la configurazione utilizzando la procedura guidata LAN.

Attiva autenticazione 802.1x

Selezionare **Attiva autenticazione 802.1x** per attivare l'autenticazione 802.1x sulla porta switch.

Modalità host

Scegliere **Singolo** o **Multiplo**. La modalità Singolo consente l'accesso di un solo cliente autenticato. La modalità Multiplo consente l'accesso di qualsiasi numero di client dopo che è stata effettuata l'autenticazione di un solo client.

Nota Le porte sui router Cisco 85x e Cisco 87x possono essere impostate solo sulla modalità host Multiplo. La modalità Singolo per questi router è disattivata.

VLAN guest

Selezionare **VLAN guest** per attivare una VLAN per i client mancanti del supporto 802.1x. Se questa opzione viene attivata, scegliere una VLAN dal relativo elenco a discesa.

VLAN Auth-Fail

Selezionare **VLAN Auth-Fail** per attivare una VLAN per i client che non ottengono l'autorizzazione 802.1x. Se questa opzione viene attivata, scegliere una VLAN dal relativo elenco a discesa.

Riautenticazione periodica

Selezionare **Riautenticazione periodica** per forzare la riautenticazione dei client 802.1x a intervalli regolari. Scegliere di configurare l'intervallo localmente o di consentire che il server RADIUS imposti l'intervallo. Se si sceglie di configurare l'intervallo di riautenticazione localmente, immettere un valore compreso tra 1 e 65535 secondi. L'impostazione predefinita è 3600 secondi.

Opzioni avanzate

Fare clic su **Opzioni avanzate** per aprire una finestra con ulteriori parametri di autenticazione 802.1x.

Opzioni avanzate

In questa finestra è possibile modificare i valori predefiniti per numerosi parametri di autenticazione 802.1x.

Timeout server RADIUS

Immettere il tempo di attesa in secondi da parte del router Cisco IOS prima del timeout della sua connessione al server RADIUS. I valori devono essere compresi tra 1 e 65535 secondi. L'impostazione predefinita è 30 secondi.

Timeout risposta richiedente

Immettere il tempo di attesa di risposta da un client 802.1x del router Cisco IOS, in secondi, prima del timeout della connessione a tale client. I valori devono essere compresi tra 1 e 65535 secondi. L'impostazione predefinita è 30 secondi.

Timeout tentativi richiedente

Immettere il periodo di tempo durante il quale il router Cisco IOS tenta di connettersi a un client 802.1x prima del timeout della connessione a tale client. I valori devono essere compresi tra 1 e 65535 secondi. L'impostazione predefinita è 30 secondi.

Quiet Period

Immettere il tempo di attesa da parte del router Cisco IOS, in secondi, tra la connessione iniziale a un client e l'invio della richiesta di accesso. I valori devono essere compresi tra 1 e 65535 secondi. L'impostazione predefinita è 60 secondi.

Periodo limite velocità

I valori devono essere compresi tra 1 e 65535 secondi. Tuttavia, l'impostazione predefinita è 0 secondi, che disattiva il **Periodo limite velocità**.

Numero massimo tentativi riautenticazione

Immettere il numero massimo di tentativi di riautenticazione su un client 802.1x da parte del router Cisco IOS. I valori devono essere compresi tra 1 e 10. L'impostazione predefinita è 2.

Numero massimo tentativi

Immettere il numero massimo di richieste di accesso che possono essere inviate al client. I valori devono essere compresi tra 1 e 10. L'impostazione predefinita è 2.

Ripristina configurazione predefinita

Fare clic su **Ripristina configurazione predefinita** per reimpostare tutte le opzioni avanzate ai valori predefiniti.

Procedura guidata LAN - Server RADIUS per autenticazione 802.1x

Le informazioni di autenticazione 802.1x sono configurate e conservate in un database di criteri che risiede sui server RADIUS che eseguono Cisco Secure ACS versione 3.3. Il router deve convalidare le credenziali dei client 802.1x comunicando con un server RADIUS. Usare questa finestra per fornire le informazioni necessarie perché il router possa contattare uno o più server RADIUS. Ciascun server RADIUS specificato deve disporre di Cisco Secure ACS software versione 3.3 installato e configurato.

Nota Tutte le interfacce del router Cisco IOS attivate con l'autorizzazione 802.1x utilizzeranno i server RADIUS impostati in questa finestra. Quando si configura una nuova interfaccia, verrà visualizzata di nuovo questa schermata. Tuttavia, non si devono apportare aggiunte o modifiche alle informazioni del server RADIUS.

Scegliere l'origine Client RADIUS

La configurazione dell'origine RADIUS consente di specificare l'indirizzo IP dell'origine da inviare in pacchetti RADIUS collegati per il server RADIUS. Per maggiori informazioni su un'interfaccia, scegliere l'interfaccia e fare clic sul pulsante **Dettagli**.

L'indirizzo IP di origine nei pacchetti RADIUS inviati dal router deve essere configurato come l'indirizzo IP NAD del Cisco ACS Versione 3.3 o successiva.

Se si seleziona l'opzione **Router sceglie l'origine**, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo d'interfaccia attraverso il quale i pacchetti RADIUS escono dal router.

Se si sceglie un'interfaccia, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo dell'interfaccia che si sceglie come origine del client RADIUS.

Nota Il software Cisco IOS consente la configurazione di una sola interfaccia origine RADIUS sul router. Se il router ha già un'origine RADIUS configurata e si sceglie un'origine diversa, l'indirizzo IP collocato nei pacchetti inviati al server RADIUS diventa l'indirizzo IP della nuova origine e pertanto può non corrispondere all'indirizzo IP NAD configurato sul Cisco ACS.

Dettagli

Se si desidera un'istantanea delle informazioni su un'interfaccia prima di sceglierla, fare clic sul pulsante **Dettagli**. Questa schermata mostra l'indirizzo IP e la subnet mask, le regole di accesso e le Inspection Rule applicate all'interfaccia, il criterio IPSec e il criterio QoS applicato, e se sull'interfaccia è presente una configurazione di Easy VPN.

Colonne IP Server, Timeout, e Parametri

Le colonne IP Server, Timeout, e Parametri contengono informazioni che il router utilizza per contattare un server RADIUS. Se non ci sono informazioni sul server RADIUS associate all'interfaccia scelta, queste colonne sono vuote.

Casella di controllo Usa per 802.1x

Selezionare questa casella di controllo se si vuole usare il server RADIUS elencato per 802.1x. Le informazioni di autorizzazione 802.1x richieste del server devono essere configurate se 802.1x viene utilizzato con esito positivo.

Aggiungi, Modifica ed Esegui ping

Per fornire informazioni su un server RADIUS, fare clic sul pulsante **Aggiungi** e immettere le informazioni nella schermata visualizzata. Scegliere una riga e fare clic su **Modifica** per modificare le informazioni sul server RADIUS. Scegliere una riga e fare clic su **Esegui ping** per testare la connessione tra il router e il server RADIUS.

Nota Quando si esegue una prova ping, immettere l'indirizzo IP dell'interfaccia origine RADIUS nel campo origine della finestra di dialogo del ping. Se è stata scelta l'opzione **Il router sceglie l'origine**, non è necessario indicare alcun valore nel campo origine della finestra di dialogo del ping.

I pulsanti **Modifica** ed **Esegui ping** sono disattivati quando non sono disponibili informazioni sul server RADIUS per l'interfaccia selezionata.

Modifica autenticazione 802.1x (porte switch)

In questa finestra è possibile attivare e configurare i parametri di autenticazione 802.1x.

Se viene visualizzato un messaggio che indica che l'802.1x non può essere configurato in modalità trunk, non è possibile attivare l'autenticazione 802.1x per lo switch.

Se i parametri di autenticazione 802.1x vengono visualizzati ma sono disattivati, si è verificata una delle seguenti condizioni:

- AAA non è stato attivato.

  Per attivare AAA, andare a **Configura > Attività aggiuntive > AAA**.

- AAA è stato attivato ma non è stato configurato un parametro di autenticazione 802.1x.

  Per configurare un criterio di autenticazione 802.1x andare a **Configura > Attività aggiuntive > AAA > Criteri di autenticazione > 802.1x**.

Attiva autenticazione 802.1x

Selezionare **Attiva autenticazione 802.1x** per attivare l'autenticazione 802.1x su questa porta switch.

Modalità host

Scegliere **Singolo** o **Multiplo**. La modalità Singolo consente l'accesso di un solo cliente autenticato. La modalità Multiplo consente l'accesso di qualsiasi numero di client dopo che è stata effettuata l'autenticazione di un solo client.

Nota Le porte sui router Cisco 87x possono essere impostate solo sulla modalità host Multiplo. La modalità Singolo per questi router è disattivata.

VLAN guest

Selezionare **VLAN guest** per attivare una VLAN per i client mancanti del supporto 802.1x. Se questa opzione viene attivata, scegliere una VLAN dal relativo elenco a discesa.

VLAN Auth-Fail

Selezionare **VLAN Auth-Fail** per attivare una VLAN per i client che non superano l'autorizzazione 802.1x. Se questa opzione viene attivata, scegliere una VLAN dal relativo elenco a discesa.

Riautenticazione periodica

Selezionare **Riautenticazione periodica** per forzare la riautenticazione dei client 802.1x a intervalli regolari. Scegliere di configurare l'intervallo localmente o di consentire che il server RADIUS imposti l'intervallo. Se si sceglie di configurare l'intervallo di riautenticazione localmente, immettere un valore compreso tra 1 e 65535 secondi. L'impostazione predefinita è 3600 secondi.

Opzioni avanzate

Fare clic su **Opzioni avanzate** per aprire una finestra con ulteriori parametri di autenticazione 802.1x.

Procedura guidata LAN - Autenticazione 802.1x (VLAN o Ethernet)

Questa procedura guidata consente di attivare l'autenticazione 802.1x sulla porta Ethernet scelta per la configurazione utilizzando la procedura guidata LAN. Per i router Cisco 87x, la finestra è disponibile per la configurazione di una VLAN con l'autenticazione 802.1x.

Nota Prima di configurare 802.1x su una VLAN, verificare che 802.1x *non* sia configurata su alcuna porta switch VLAN. Verificare anche che la VLAN sia configurata per DHCP.

Utilizza l'autenticazione 802.1x per separare il traffico attendibile da quello non attendibile sull'interfaccia.

Selezionare **Utilizza l'autenticazione 802.1x per separare il traffico attendibile da quello non attendibile sull'interfaccia** per attivare l'autenticazione 802.1x.

Pool di indirizzi IP DHCP per i client 802.1x non attendibili

Per attivare una connessione a Internet per i client che non superano l'autenticazione 802.1x, è necessario che ad ogni client non attendibile venga assegnato un indirizzo IP univoco. Questi indirizzi IP derivano da un pool di indirizzi IP nuovi o esistenti, ma i pool utilizzati non possono sovrapporsi a quelli delle interfacce esistenti del router Cisco IOS.

Nota Il pool di indirizzi IP può sovrapporsi all'indirizzi IP utilizzato per un'interfaccia loopback. Tuttavia, verrà richiesto di confermare tale sovrapposizione prima che venga consentita.

Scegliere **Crea un nuovo pool** per configurare un nuovo pool di indirizzi IP per emettere indirizzi IP ai client non attendibili. È possibile che i seguenti campi siano già stati compilati con informazioni immesse in precedenza, ma è possibile modificarle o inserirne:

Rete	Immettere l'indirizzo IP di rete da cui deriva il pool di indirizzi IP.
Subnet Mask	Immettere la subnet mask per definire la rete e le porzioni host dell'indirizzi IP immesso nel campo **Rete**.
Server DNS 1	Il server DNS consente di eseguire la mappatura di un dispositivo conosciuto mediante l'indirizzo IP. Se è stato configurato un server DNS per la rete, immettere l'indirizzo IP per tale server.
Server DNS 2	Se nella rete è disponibile un server DNS aggiuntivo, immettere l'indirizzo IP per tale server.

Server WINS 1	Per alcuni client è necessario disporre di WINS (Windows Internet Naming Service) per connettersi ai dispositivi in Internet. Se nella rete è disponibile un server WINS, immettere l'indirizzo IP per tale server.
Server WINS 2	Se nella rete è disponibile un server WINS aggiuntivo, immettere l'indirizzo IP per tale server.

Se vi è un pool di indirizzi IP esistenti che si desidera utilizzare per emettere indirizzi IP ai clienti non attendibili, scegliere **Seleziona da un pool esistente**. Scegliere il pool esistente dal menu a tendina. Per visualizzare altre informazioni su un pool esistente, scegliere **Dettagli**.

Elenchi eccezioni

Fare clic su **Elenchi eccezioni** per creare o modificare un elenco eccezioni. L'elenco eccezioni consente di esentare alcuni client dall'autenticazione 802.1x consentendo però loro di utilizzare il tunnel VPN.

Esenta telefoni IP Cisco dall'autenticazione 802.1x

Selezionare **Esenta telefoni IP Cisco dall'autenticazione 802.1x** per esentare i telefoni IP Cisco dall'autenticazione 802.1x consentendo però loro di utilizzare il tunnel VPN.

Elenco eccezioni 802.1x

L'elenco eccezioni consente di esentare alcuni client dall'autenticazione 802.1x consentendo però loro di utilizzare il tunnel VPN. I clienti esenti vengono identificati mediante il relativo indirizzo MAC.

Aggiungi

Scegliere **Aggiungi** per aprire una finestra nella quale è possibile aggiungere l'indirizzo MAC di un client. L'indirizzo MAC deve essere in un formato corrispondente a uno degli esempi seguenti:

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4

Cisco SDM respinge gli indirizzi MAC formattati in modo erroneo, tranne per gli indirizzi MAC più brevi di quelli riportati negli esempi. Gli indirizzi MAC più brevi vengono completati con uno zero per ogni cifra mancante.

Nota La funzionalità 802.1x di Cisco SDM non supporta l'opzione CLI che associa i criteri agli indirizzi MAC e non include nell'elenco eccezioni gli indirizzi MAC a cui è associato un criterio.

Elimina

Scegliere **Elimina** per rimuovere un client scelto dall'elenco eccezioni.

Autenticazione 802.1x sulle interfacce Layer 3

Questa finestra consente di configurare l'autenticazione 802.1x su una Interfaccia Layer 3. Elenca le porte Ethernet e le interfacce VLAN che hanno o possono essere configurate con l'autenticazione 802.1x, consentendo di scegliere un'interfaccia modello virtuale e di creare un elenco eccezioni per consentire ai client di ignorare l'autenticazione 802.1x.

Nota Se i criteri sono stati impostati utilizzando la riga di comando, vengono visualizzati come informazioni di sola lettura in questa finestra. In questo caso, in tale finestra è possibile solo attivare o disattivare 802.1x.

Attività preliminari

Se nella finestra viene visualizzata un'attività preliminare, è necessario completarla per poter configurare l'autenticazione 802.1x. Viene visualizzato un messaggio che illustra l'attività preliminare insieme al collegamento alla finestra nella quale è possibile effettuarla.

Attiva autenticazione 802.1x globale

Selezionare **Attiva autenticazione 802.1x globale** per attivare l'autenticazione 802.1x su tutte le porte Ethernet.

Tabella Interfacce

La tabella delle interfacce presenta le colonne seguenti:

Interfaccia: visualizza il nome dell'interfaccia Ethernet o VLAN.

Autenticazione 802.1x: indica se per la porta Ethernet è attivata l'autenticazione 802.1x.

Modifica

Scegliere **Modifica** per aprire una finestra di parametri di autenticazione 802.1x modificabili. I parametri sono le impostazioni di autenticazione 802.1x per l'interfaccia scelta nella tabella Interfacce.

Criterio utente non attendibile

Scegliere un'interfaccia modello virtuale dall'elenco a discesa. L'interfaccia modello virtuale scelta rappresenta il criterio applicato ai client che non superano l'autenticazione 802.1x.

Per visualizzare ulteriori informazioni sull'interfaccia modello virtuale scelta, fare clic sul pulsante **Dettagli**.

Elenco eccezioni

Per maggiori informazioni sull'elenco eccezioni, vedere Elenco eccezioni 802.1x.

Esenta telefoni IP Cisco dall'autenticazione 802.1x

Selezionare **Esenta telefoni IP Cisco dall'autenticazione 802.1x** per esentare i telefoni IP Cisco dall'autenticazione 802.1x consentendo però loro di utilizzare il tunnel VPN.

Applica modifiche

Fare clic su **Applica modifiche** perché le modifiche abbiano effetto.

Annulla modifiche

Fare clic su **Annulla modifiche** per annullare le modifiche.

Modifica autenticazione 802.1x

Questa finestra consente di attivare e modificare i valori predefiniti per numerosi parametri di autenticazione 802.1x.

Attiva autenticazione 802.1x

Selezionare **Attiva autenticazione 802.1x** per attivare l'autenticazione 802.1x sulla porta Ethernet.

Riautenticazione periodica

Selezionare **Riautenticazione periodica** per forzare la riautenticazione dei client 802.1x a intervalli regolari. Scegliere di configurare l'intervallo localmente o di consentire che il server RADIUS imposti l'intervallo. Se si sceglie di configurare l'intervallo di riautenticazione localmente, immettere un valore compreso tra 1 e 65535 secondi. L'impostazione predefinita è 3600 secondi.

Opzioni avanzate

Fare clic su Opzioni avanzate per la descrizione dei campi del riquadro Opzioni avanzate.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come configurare l'autenticazione 802.1x su più porte Ethernet?

Dopo aver configurato l'autenticazione 802.1x su un'interfaccia, la procedura guidata LAN non visualizza più le opzioni di 802.1x per Ethernet, poiché Cisco SDM utilizza la configurazione 802.1x in modo globale.

Nota Per la configurazione degli switches, la procedura guidata LAN continua a visualizzare le opzioni 802.1x.

Se si desidera modificare la configurazione di autenticazione 802.1x su una porta Ethernet, andare a **Configura > Attività aggiuntive > 802.1x**.

CAPITOLO 4

Procedura guidata di creazione di una connessione

La procedura di creazione di una connessione consente di configurare le connessioni LAN e WAN per tutte le interfacce supportate da Cisco SDM.

Crea connessione

In questa finestra è possibile creare nuove connessioni LAN e WAN.

Nota Non è possibile utilizzare Cisco SDM per creare connessioni WAN per i router della serie Cisco 7000.

Crea nuova connessione

Scegliere un tipo di connessione da configurare sulle interfacce fisiche disponibili sul proprio router. Sono disponibili solo le interfacce che non sono state ancora configurate. Quando si fa clic sul pulsante di selezione di un tipo di connessione viene visualizzato uno schema dello scenario di utilizzo che illustra il tipo di connessione scelto. Se tutte le interfacce sono state configurate, questa parte della finestra non viene visualizzata.

Se il router presenta interfacce ATM (Asynchronous Transfer Mode) o seriali, è possibile configurare più connessioni da una singola interfaccia. In Cisco Router and Security Device Manager (Cisco SDM), infatti, per ciascuna interfaccia di questo tipo possono essere configurate interfacce secondarie.

Se sono presenti interfacce fisiche o logiche non supportate o se a un'interfaccia supportata è stata associata una configurazione non supportata, viene visualizzato il pulsante di opzione Altro (non supportato da Cisco SDM). Quando si fa clic sul pulsante di selezione Altro (non supportato da Cisco SDM), il pulsante Crea nuova connessione viene disattivato.

Se il router dispone di interfacce radio ma non si vede un pulsante di selezione **Wireless**, non è stato effettuato l'accesso come Amministratore di Cisco SDM. Se è necessario utilizzare l'applicazione wireless, andare al menu Strumenti di Cisco SDM e scegliere **Applicazione wireless**.

Tabella riassuntiva funzioni

Funzione	Procedura
Come effettuare configurazioni non previste da questa procedura guidata.	Visualizzare una delle seguenti procedure: • Come visualizzare i comandi IOS inviati al router? • Come configurare un'interfaccia WAN non supportata? • Come attivare o disattivare un'interfaccia? • Come visualizzare l'attività dell'interfaccia WAN? • Come configurare il protocollo NAT in un'interfaccia WAN? • Come configurare una route statica? • Come configurare un protocollo di routing dinamico? • Come configurare il DDR (Dial-on-Demand Routing) per la connessione ISDN o l'interfaccia asincrona?
Come configurare un'interfaccia non supportata da Cisco SDM.	Consultare la guida di configurazione del router per usare la CLI (interfaccia a riga di comando) per configurare l'interfaccia

Finestra iniziale della procedura guidata di configurazione dell'interfaccia WAN

In questa finestra sono elencati i tipi di connessione che è possibile configurare per questa interfaccia utilizzando Cisco SDM. Per configurare un altro tipo di connessione utilizzare l'interfaccia della riga di comando.

Finestra iniziale della procedura guidata di configurazione dell'interfaccia ISDN

PPP è il solo tipo di codifica supportato da Cisco SDM su una ISDN BRI.

Finestra iniziale di configurazione di un'interfaccia per modem analogico

PPP è l'unico tipo di codifica supportata da Cisco SDM su una connessione con modem analogico.

Finestra iniziale della procedura guidata di backup aux

L'opzione per configurare la porta AUX come connessione dial-up viene visualizzata soltanto per i router Cisco 831e 837.

Il pulsante di selezione Aux dial-backup è disattivato in presenza di una delle seguenti condizioni:

- Presenza di più di una route predefinita (default route)
- Presenza di una route predefinita (default route) configurata con un'interfaccia diversa dall'interfaccia WAN primaria.

L'opzione Aux dial-backup non è visualizzata in presenza di una delle seguenti condizioni:

- Il router non sta utilizzando un'immagine Cisco IOS che supporta la funzione Aux dial-backup.
- Non è configurata un'interfaccia WAN primaria.
- L'interfaccia asincrona è già configurata.
- L'interfaccia asincrona non è configurabile con Cisco SDM a causa della presenza di comandi Cisco IOS non supportati nella configurazione esistente.

Seleziona interfaccia

Questa finestra viene visualizzata se c'è più di un'interfaccia dello stesso tipo selezionata nella finestra Crea connessione. Selezionare l'interfaccia che si desidera utilizzare per questa connessione.

Se si sta configurando un'interfaccia Ethernet, Cisco SDM inserisce nel file di configurazione il testo di descrizione $ETH-WAN$ in modo tale che in seguito l'interfaccia verrà riconosciuta come interfaccia WAN.

Incapsulamento: PPPoE

In questa finestra è possibile attivare l'incapsulamento del protocollo PPPoE (Point-to-Point-Protocol over Ethernet). Questa operazione è necessaria se il provider di servizi o l'amministratore di rete richiedono router remoti per la comunicazione mediante PPPoE.

PPPoE è un protocollo utilizzato da molti provider di servizi ADSL (Asymmetric Digital Subscriber Line). Contattare il provider di servizi per informarsi se sulla propria connessione viene utilizzato il protocollo PPPoE.

Se si seleziona l'incapsulamento PPPoE, nella finestra Riepilogo Cisco SDM aggiunge automaticamente un'interfaccia dialer alla configurazione.

Attiva incapsulamento PPPoE

Se il provider di servizi richiede l'utilizzo del PPPoE da parte del router, selezionare questa casella per attivare l'incapsulamento PPPoE. Deselezionare questa casella se il provider non utilizza PPPoE. Questa casella di controllo non sarà disponibile se nel router è in esecuzione una versione di Cisco IOS che non supporta l'incapsulamento PPPoE.

Indirizzo IP - ATM o Ethernet con PPPoE/PPPoA

Selezionare il metodo che verrà utilizzato dall'interfaccia WAN per ottenere un indirizzo IP.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti.

Dinamico (client DHCP)

Se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere il nome del server DHCP che assegnerà gli indirizzi.

IP senza numero

Selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia cui è assegnato l'indirizzo IP che si desidera condividere.

Easy IP (IP negoziato)

Selezionando l'opzione **Easy IP (IP negoziato)**, il router otterrà un indirizzo IP mediante negoziazione PPP/IPCP.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Indirizzo IP - ATM con routing RFC 1483

Selezionare il metodo che verrà utilizzato dall'interfaccia WAN per ottenere un indirizzo IP.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Dinamico (client DHCP)

Se si seleziona l'opzione Dinamico, al router verrà assegnato in lease un indirizzo IP da un server DHCP remoto. Immettere il nome del server DHCP che assegnerà gli indirizzi.

IP senza numero

Selezionare l'opzione **IP senza numero**, se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia cui è assegnato l'indirizzo IP che si desidera condividere.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Indirizzo IP - Ethernet senza PPPoE

Selezionare il metodo che verrà utilizzato dall'interfaccia WAN per ottenere un indirizzo IP.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Dinamico (client DHCP)

Se si seleziona l'opzione Dinamico, al router verrà assegnato in lease un indirizzo IP da un server DHCP remoto. Immettere il nome del server DHCP che assegnerà gli indirizzi.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Indirizzo IP - Seriale con protocollo point-to-point

Selezionare il metodo che verrà utilizzato dall'interfaccia point-to-point per ottenere un indirizzo IP.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

IP senza numero

Selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia cui è assegnato l'indirizzo IP che si desidera condividere.

Easy IP (IP negoziato)

Selezionando l'opzione **Easy IP (IP negoziato)**, il router otterrà un indirizzo IP mediante negoziazione PPP/IPCP.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Indirizzo IP - Seriale con HDLC o Frame Relay

Selezionare il metodo che verrà utilizzato dall'interfaccia WAN per ottenere un indirizzo IP. Se viene utilizzato l'incapsulamento Frame Relay, Cisco SDM crea un'interfaccia secondaria, e l'indirizzo IP viene assegnato all'interfaccia secondaria creata da Cisco SDM.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

IP senza numero

Selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia cui è assegnato l'indirizzo IP che si desidera condividere.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Indirizzo IP - ISDN BRI o modem analogico

Selezionare il metodo che verrà utilizzato dall'interfaccia ISDN BRI o per modem analogico per ottenere un indirizzo IP.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

IP senza numero

Selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia il cui indirizzo IP verrà utilizzato dall'interfaccia che si sta configurando.

Easy IP (IP negoziato)

Selezionare l'opzione **IP negoziato** se l'interfaccia ottiene un indirizzo IP dal provider di servizi Internet mediante negoziazione dell'indirizzo PPP/IPCP ogni volta in cui viene eseguita una connessione.

DNS dinamico

Scegliere DNS dinamico se si vuole aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia. Fare clic sul pulsante **DNS dinamico** per configurare il DNS dinamico.

Autenticazione

Questa pagina viene visualizzata se si è attivato o si sta configurando quanto segue:

- PPP per una connessione seriale
- PPPoE Incapsulamento PPPoA per una connessione ATM
- PPPoE o incapsulamento PPPoA per una connessione Ethernet
- Una connessione tramite ISDN BRI o modem analogico

Il provider di servizi o l'amministratore di rete utilizzano una password del protocollo Challenge Handshake Authentication Protocol (CHAP) o del protocollo Password Authentication Protocol (PAP) per proteggere la connessione tra i dispositivi. Questa password protegge l'accesso in ingresso e in uscita.

Tipo di autenticazione

Selezionare la casella associata al tipo di autenticazione utilizzata dal provider di servizi. Se non si possiede questa informazione, è possibile selezionare entrambe le caselle. Il router tenterà entrambi i tipi di autenticazione e uno dei tentativi avrà esito positivo.

L'autenticazione CHAP è più sicura dell'autenticazione PAP.

Nome utente

Il nome utente che viene assegnato dal provider di servizi internet o dall'amministratore della rete e che è utilizzato come nome utente per l'autenticazione CHAP o PAP.

Password

Immettere la password esattamente nel modo in cui è stata fornita dal provider di servizi. Per le password la distinzione tra maiuscole e minuscole è significativa. Ad esempio, la password cisco è diversa dalla password Cisco.

Conferma password

Immettere la stessa password digitata nella casella precedente.

Tipo di switch e SPID

Le connessioni ISDN BRI richiedono l'identificazione dello switch type ISDN e, in alcuni casi, l'identificazione dei canali B che utilizzano numeri di profilo ID (SPID). informazioni che verranno fornite dal provider di servizi.

Tipo di switch ISDN

Selezionare un tipo di switch ISDN. Contattare il provider del servizio ISDN per conoscere il tipo di switch della propria connessione.

Cisco SDM supporta i tipi di switch BRI elencati di seguito.

- Per l'America del Nord
  - basic-5ess: switch Lucent (AT&T) 5ESS a frequenza base
  - basic-dms100: switch Northern Telecom DMS-100 a frequenza base
  - basic-ni: switch ISDN nazionale
- Per Australia, Europa e Regno Unito
  - basic-1tr6: switch ISDN 1TR6 (Germania)
  - basic-net3: switch NET3 ISDN BRI per i tipi di switch NET3 (Norvegia, Australia e Nuova Zelanda); switch conformi alla specifica ETSI per il sistema di indicazione Euro-ISDN E-DSS1
  - vn3: switch ISDN BRI (Francia)
- Per il Giappone
  - ntt: switch NTT ISDN
- Per i sistemi voce o PBX:
  - basic-qsig: switch PINX (PBX) con indicazione QSIG per Q.931 ()

SPID disponibili

Selezionare questa casella di controllo se il provider di servizi utilizza gli identificativi SPID.

Alcuni provider di servizi utilizzano gli identificativi SPID per definire i servizi a cui un determinato dispositivo ISDN è registrato. Il provider assegna al dispositivo ISDN uno o più numeri SPID quando ci si registra per la prima volta al servizio. Se il proprio provider di servizi utilizza gli SPID, il dispositivo ISDN utilizzato non sarà in grado di effettuare o ricevere chiamate finché non trasmette al provider di servizi uno SPID valido quando accede allo switch per inizializzare la connessione.

Attualmente solo gli switch di tipo DMS-100 e NI richiedono l'utilizzo di SPID. Benché gli switch AT&T 5ESS possano supportare gli SPID, in questo caso è preferibile configurare i servizi ISDN in modo che non richiedano l'uso di tali identificativi. Inoltre, gli SPID sono rilevanti solo presso l'interfaccia di accesso ISDN locale. I router remoti, infatti, non ricevono mai gli SPID.

Uno SPID è costituito di solito da un numero di telefono a 7 cifre con alcuni numeri opzionali. Comunque, i provider di servizi possono utilizzare schemi di numerazione differenti. Per lo switch di tipo DMS-100 sono assegnati due SPID, uno per ciascun canale B.

SPID1

Immettere il numero SPID del primo canale B su connessione BRI fornito dall'ISP.

SPID2

Immettere il numero SPID del secondo canale B su connessione BRI fornito dall'ISP.

Stringa di connessione

Immettere il numero di telefono dell'estremità remota della connessione ISDN BRI o con modem analogico. Tale numero verrà composto dall'interfaccia ISDN BRI o per modem analogico ogni volta che verrà effettuata una connessione. La stringa di connessione è fornita dal provider di servizi.

Configurazione di backup

Le interfacce ISDN BRI e per modem analogico possono essere configurate perché fungano da interfacce di backup per altre interfacce primarie. In tal caso verrà effettuata una connessione ISDN o con modem analogico solo se l'interfaccia primaria non è attiva. Se si verifica un guasto nell'interfaccia primaria e nella connessione, l'interfaccia ISDN BRI o con modem analogico tenterà immediatamente di stabilire una nuova connessione in modo da evitare l'interruzione dei servizi di rete.

Scegliere se è necessario che la connessione ISDN BRI o con modem analogico funzioni come connessione di backup.

Considerare i seguenti prerequisiti:

- L'interfaccia primaria deve essere configurata per la VPN site-to-site.
- L'immagine IOS del router deve supportare la funzionalità SAA ICMP Echo Enhancement.

Configurazione di backup - Interfaccia primaria e indirizzi IP per hop successivo

Per funzionare come connessione di backup, la connessione ISDN BRI o con modem analogico deve essere associata a un'altra interfaccia sul router che funzionerà da connessione primaria. La connessione ISDN BRI o con modem analogico verrà effettuata solo se per qualche motivo si verifica un guasto nell'interfaccia selezionata.

Interfaccia primaria

Selezionare l'interfaccia del router che s'intende utilizzare per la connessione primaria.

Indirizzo IP per hop successivo primario

Questo campo è opzionale. Immettere l'indirizzo IP, conosciuto anche come *indirizzo IP per l'hop successivo*, a cui l'interfaccia primaria si connetterà quando è attiva.

Indirizzo IP per hop successivo di backup

Questo campo è opzionale. Immettere l'indirizzo IP, conosciuto anche come *indirizzo IP per l'hop successivo*, a cui l'interfaccia di backup si connetterà quando è attiva.

Configurazione di backup - Nome host o indirizzo IP da rilevare

In questa schermata è possibile individuare un host specifico verso il quale deve essere mantenuta la connettività. Il router tiene traccia della connettività verso tale host e se si rilevano interruzioni sull'interfaccia primaria verrà automaticamente effettuata una connessione di backup utilizzando l'interfaccia ISDN BRI o per modem analogico.

Indirizzo IP da rilevare

Immettere l'indirizzo IP o il nome host dell'host di destinazione verso cui si desidera rilevare la connettività. Si consiglia di indicare in questo campo una destinazione contattata raramente.

Opzioni avanzate

Sono disponibili due opzioni avanzate, in base alla configurazione del router: Route statica predefinita e PAT (Port Address Translation). Se l'opzione Route statica non è visibile, nel router è già stata configurata una route statica. Se l'opzione PAT (Port Address Translation) non è visibile, nell'interfaccia è già stata configurata la connessione in modalità PAT.

Route statica predefinita

Selezionare questa casella per configurare una route statica per l'interfaccia esterna verso la quale sarà instradato il traffico in uscita. Se su questo router è già stata configurata un'interfaccia esterna questa casella non viene visualizzata.

Indirizzo per hop successivo

Se il provider di servizi ha fornito un indirizzo IP per l'hop successivo, immetterlo in questo campo. Lasciando vuoto questo campo, Cisco SDM utilizzerà l'interfaccia WAN che si sta configurando come interfaccia per l'hop successivo.

PAT (Port Address Translation)

Se i dispositivi sulla LAN sono dotati di indirizzi privati, è possibile consentire che condividano un unico indirizzo IP pubblico. È possibile garantire che il traffico venga diretto verso la destinazione giusta utilizzando la modalità PAT, che rappresenta più host in una LAN con un unico indirizzo IP e utilizza diversi numeri di porta per distinguerli. Se nell'interfaccia è già stata configurata la modalità PAT, l'opzione PAT non sarà visibile.

Inside Interface to be Translated

Scegliere l'interfaccia interna connessa alla rete della quale si desidera convertire gli indirizzi IP host.

Incapsulamento

In questa finestra, scegliere il tipo di incapsulamento che verrà utilizzato dal collegamento WAN. Contattare il provider di servizi o l'amministratore di rete per avere informazioni sul tipo di incapsulamento utilizzato per questo collegamento. Dal tipo di interfaccia dipendono i tipi di incapsulamento disponibili.

Rilevamento automatico

Fare clic su **Rilevamento automatico** per attivare in Cisco SDM il rilevamento del tipo di incapsulamento. Se Cisco SDM riesce a effettuare il rilevamento, verranno automaticamente visualizzati il tipo di incapsulamento e gli altri parametri di configurazione rilevati.

Nota Cisco SDM supporta il rilevamento automatico sui router SB106, SB107, Cisco 836 e Cisco 837. Ma se si sta configurando un router Cisco 837 con IOS Cisco versione 12.3(8)T o 12.3(8.3)T, la funzione di rilevamento automatico non è supportata.

Incapsulamenti disponibili

Nella tabella riportata di seguito sono mostrati gli incapsulamenti disponibili in caso di interfaccia ADSL, G.SHDSL o ADSL su ISDN.

Incapsulamento	Descrizione
PPPoE	Indica l'incapsulamento Point-to-Point Protocol over Ethernet. Questa opzione è disponibile se è stata selezionata un'interfaccia Ethernet o ATM. Se si configura PPPoE in un'interfaccia ATM, verranno create un'interfaccia secondaria ATM e un'interfaccia dialer. Il pulsante di opzione PPPoE verrà disattivato se nel router è in esecuzione una versione di Cisco IOS che non supporta l'incapsulamento PPPoE.

Incapsulamento	Descrizione
PPPoA	Point-to-Point protocol over ATM. Questa opzione è disponibile se è stata selezionata un'interfaccia ATM. Se si configura PPPoA in un'interfaccia ATM, verranno create un'interfaccia secondaria ATM e un'interfaccia dialer. Il pulsante di opzione PPPoA verrà disattivato se nel router è in esecuzione una versione di Cisco IOS che non supporta l'incapsulamento PPPoA.
Routing RFC 1483 con AAL5-SNAP	Questa opzione è disponibile se è stata selezionata un'interfaccia ATM. Se si configura una connessione RFC 1483, sarà creata un'interfaccia secondaria ATM, che sarà visibile nella finestra Riepilogo.
Routing RFC 1483 con AAL5-MUX	Questa opzione è disponibile se è stata selezionata un'interfaccia ATM. Se si configura una connessione RFC 1483, sarà creata un'interfaccia secondaria ATM, che sarà visibile nella finestra Riepilogo.

Nella tabella riportata di seguito sono mostrati gli incapsulamenti disponibili in caso di interfaccia seriale.

Incapsulamento	Descrizione
Frame Relay	Indica un incapsulamento Frame Relay. Questa opzione è disponibile se è stata selezionata un'interfaccia seriale. Se si crea una connessione Frame Relay, verrà creata un'interfaccia secondaria seriale, che sarà visibile nella finestra Riepilogo. **Nota** Se a un'interfaccia è stata aggiunta una connessione seriale Frame Relay e nella stessa interfaccia vengono configurate connessioni seriali successive, in questa finestra verrà attivato solo un incapsulamento Frame Relay.

Incapsulamento	Descrizione
Protocollo point-to-point	Indica un incapsulamento PPP. Questa opzione è disponibile se è stata selezionata un'interfaccia seriale.
HDLC (High Level Data Link Control)	Indica un incapsulamento HDLC. Questa opzione è disponibile se è stata selezionata un'interfaccia seriale.

PVC

Il routing ATM utilizza uno schema gerarchico a due livelli, percorsi virtuali e canali virtuali, contrassegnati rispettivamente da un valore VPI (Virtual Path Identifier) e un valore VCI (Virtual Channel Identifier). Un determinato percorso virtuale può contenere diversi canali virtuali corrispondenti a singole connessioni. Quando viene eseguita un'operazione di switching sulla base del valore VPI, tutte le cellule su quel determinato percorso virtuale vengono commutate indipendentemente dal valore VCI. Uno switch ATM è in grado di instradare il traffico in base al VCI, al VPI oppure a entrambi.

VPI

Immettere il valore VPI fornito dal provider di servizi o dall'amministratore di sistema. L'identificatore VPI viene utilizzato nello switching e nel routing ATM per identificare il percorso utilizzato da un certo numero di connessioni. Immettere il valore VPI fornito dal provider di servizi.

VCI

Immettere il valore VCI fornito dal provider di servizi o dall'amministratore di sistema. L'identificatore VCI viene utilizzato nello switching e nel routing ATM per identificare una particolare connessione all'interno di un percorso potenzialmente condiviso con altre connessioni. Immettere il valore VCI fornito dal provider di servizi.

Valori predefiniti di Cisco IOS

Nella tabella riportata di seguito sono riportati i valori predefiniti di Cisco IOS. Cisco SDM non sovrascriverà tali valori se sono stati modificati durante una configurazione precedente, ma se il router non è stato configurato in precedenza, occorrerà utilizzare questi valori.

Tipo di connessione	Parametro	Valore
ADSL	• Modalità operativa	• Auto
G.SHDSL	• Modalità operativa	• Annex A (Stati Uniti)
	• Frequenza di linea	• Auto
	• Tipo di dispositivo	• CPE
ADSL su ISDN	• Modalità operativa	• Auto

Configurazione degli identificatori LMI e DLCI

Se si sta configurando una connessione con incapsulamento Frame Relay, occorre specificare il protocollo utilizzato per monitorare la connessione, chiamato LMI (Local Management Identifier). Occorre, inoltre, fornire un identificatore univoco per questa particolare connessione, denominato DLCI (Data Link Connection Identifier).

Tipo LMI

Contattare il provider di servizi per avere informazioni su quale tipo di LMI utilizzare tra quelli elencati di seguito.

Tipo LMI	Descrizione
ANSI	Allegato D definito dall'American National Standards Institute (ANSI) standard T1.617.
Cisco	Tipo di LMI stabilito da Cisco Systems e altre tre società.

Tipo LMI	Descrizione
ITU-T Q.933	ITU-T Q.933 Annex A
Rilevamento automatico	Valore predefinito. Questa impostazione consente al router di individuare, mediante scambio di informazioni con lo switch, e di impostare quale tipo di LMI è utilizzato. Se la funzione di **rilevamento automatico** ha esito negativo, il router utilizzerà il tipo di LMI Cisco.

DLCI

Immettere il valore DLCI in questo campo. Questo numero deve essere univoco tra tutti i valori DLCI utilizzati in questa interfaccia.

Utilizzare l'incapsulamento Frame Relay IETF

Incapsulamento IETF (Internet Engineering Task Force). Questa opzione viene utilizzata per la connessione a router non prodotti da Cisco. Selezionare questa casella se s'intende connettere l'interfaccia a un router non Cisco.

Configurazione delle impostazioni del clock

La finestra Impostazioni clock è disponibile quando si sta configurando una linea T1 o E1. In questa pagina vengono visualizzate le impostazioni predefinite del clock Frame Relay. È necessario non modificarle a meno che non si abbiano esigenze diverse.

Sorgente di clock

Internal indica che il clock è stato generato internamente. Line indica che la sorgente si trova in rete. Il clock consente di sincronizzare la trasmissione dei dati. Il valore predefinito è **line**.

Frame T1

Questo campo consente di configurare la linea T1 o E1 per le operazioni con D4 Super Frame (sf) o Extended Superframe (esf). Il valore predefinito è **esf**.

Codice linea

Questo campo configura il router per operazioni sulle linee T1 con codifica B8ZS (Binary 8-Zeroes Substitution) o AMI (Alternate Mark Inversion). L'impostazione B8ZS assicura la densità su una linea T1 o E1 sostituendo le violazioni bipolari intenzionali nei bit in posizione 4 e 7 con una sequenza di bit di otto zeri. Quando il router è configurato con l'impostazione AMI, è necessario usare l'impostazione invertita della codifica dati per garantire la densità sulla linea T1. Il valore predefinito è **b8zs**.

Codifica dati

Fare clic su **invertito** se si sa che i dati utente sono invertiti su questo collegamento o se il Codice linea è impostato su AMI. altrimenti lasciare il valore predefinito **normal**. L'inversione dei dati viene utilizzata con protocolli orientati al bit come HDLC, PPP e LAPB (Link Access Procedure, Balanced) per garantire densità su una linea T1 con codifica AMI. I protocolli bit-oriented eseguono “inserimenti di zero” dopo ogni gruppo di cinque bit “uno” nel flusso dei dati. In questo modo si garantisce almeno uno zero per ogni otto bit. Se il flusso dei dati viene quindi invertito, almeno un bit ogni otto sarà a uno.

Cisco SDM imposterà la codifica dei dati su inverted se il codice linea è AMI e non ci sono fasce orarie configurate a 56 kbit/s. Se non si desidera utilizzare la codifica dei dati invertita con il codice linea AMI, occorre utilizzare l'interfaccia della riga di comando per configurare tutte le fasce orarie a 56 kbit/s.

FDL (Facilities Data Link)

Questo campo consente di configurare il comportamento del router sul collegamento FDL (Facilities Data Link) dell'Extended Superframe. Se configurato con **att**, il router implementa AT&T TR 54016, se configurato con **ansi**, implementa ANSI T1.403, se invece si scelgono entrambi, il router implementa **att** e **ansi**. Nel caso in cui si sceglie none, il router ignora il collegamento FDL. Il valore predefinito è **none**. Se il frame T1 o E1 è impostato su sf, Cisco SDM imposterà l'FDL su **none** e questo campo sarà in sola lettura.

Linea in uscita (LBO)

Questo campo è utilizzato per configurare il valore LBO (Line Build Out) della linea T1. Il valore LBO riduce la potenza di trasmissione del segnale di -7,5 o -15 decibel. Non è probabile che ciò sia necessario sulle linee T1 o E1 recenti. Il valore predefinito è **none**.

Richieste di loopback remoto

Questo campo specifica se il router passa al modo loopback quando sulla linea si riceve un codice loopback. Se si sceglie **full**, il router accetterà i loopback totali, mentre scegliendo **payload-v54** sceglierà i loopback payload.

Attiva creazione/rilevamento avvisi remoti

Selezionare questa casella se si desidera che la linea T1 del router crei avvisi remoti, detti “yellow alarm” e rilevi avvisi remoti inviati dal peer all'altra estremità del collegamento.

L'avviso remoto viene trasmesso da un router quando viene individuata una condizione di avviso: un “red alarm” (perdita di segnale) o un “blue alarm” (1 senza frame). In questo modo l'unità CSU/DSU (Channel Service Unit/Data Service Unit) ricevente viene informata che c'è un errore sulla linea.

Utilizzare questa impostazione solo quando il frame T1 è impostato su **esf**.

Elimina connessione

È possibile eliminare una connessione WAN che viene visualizzata nella finestra Modifica interfaccia/connessione. Questa finestra viene visualizzata quando si sta eliminando la configurazione di un'interfaccia e la connessione che si desidera eliminare contiene associazioni, ad esempio regole di accesso, applicate a quest'interfaccia. In questa finestra è possibile salvare le associazioni da utilizzare con un'altra connessione.

Quando si elimina una connessione, l'elenco Crea nuova connessione viene aggiornato nel caso in cui l'eliminazione renda disponibile un tipo di connessione non presente precedentemente.

È possibile eliminare automaticamente tutte le associazioni di cui la connessione dispone o eliminarle in un secondo momento.

Per visualizzare le associazioni disponibili per la connessione

Fare clic su **Visualizza dettagli**.

Per eliminare la connessione e tutte le associazioni

Scegliere **Eliminare automaticamente tutte le associazioni**, quindi fare clic su **OK** per consentire a Cisco SDM di eliminare la connessione e le associazioni.

Per eliminare manualmente le associazioni:

Se si desidera eliminare manualmente le associazioni, fare clic su **Visualizza dettagli** per visualizzare l'elenco delle associazioni di cui la connessione dispone. Tenendo presente le associazioni da eliminare, scegliere **Eliminare le associazioni in seguito**, quindi fare clic su **OK**. È possibile eliminare manualmente le associazioni utilizzando le istruzioni nell'elenco seguente.

Le associazioni possibili e le istruzioni per la loro eliminazione sono:

- Route statica predefinita: l'interfaccia è configurata come l'interfaccia di inoltro per una route statica predefinita. Per eliminare la route statica a cui l'interfaccia è associata, fare clic su **Configura** e quindi su **Routing**. Scegliere la route statica nella tabella Routing statico e fare clic su **Elimina**.
- Port Address Translation: la modalità PAT è configurata mediante l'interfaccia in cui è stata creata la connessione. Per eliminare l'associazione PAT, fare clic su **Configura** e quindi su **NAT**. Scegliere la regola associata a questa connessione e fare clic su **Elimina**.
- NAT—L'interfaccia è designato come interfaccia NAT interna o NAT esterna. Per eliminare l'associazione NAT, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Fare clic sulla connessione nell'Elenco interfacce, quindi fare clic su **Modifica**. Fare clic sulla scheda **NAT** e scegliere **Nessuno** nel menu a tendina NAT.
- ACL: all'interfaccia in cui è stata creata la connessione è applicato una lista ACL (Access Control List). Per eliminare l'ACL, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Scegliere la connessione in Elenco interfacce, quindi fare clic su **Modifica**. Selezionare la scheda **Associazione**, quindi nel gruppo Regola di accesso fare clic sul pulsante **...** accanto ai campi In ingresso e In uscita e scegliere **Nessuno**.

- Verifica: all'interfaccia in cui è stata creata la connessione è applicata un'Inspection Rule. Per eliminare l'Inspection Rule, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Scegliere la connessione in Elenco interfacce, quindi fare clic su **Modifica**. Selezionare la scheda **Associazione**, quindi nei campi In ingresso e In uscita del gruppo Inspection Rule scegliere **Nessuno**.
- Crittografia: all'interfaccia in cui è stata creata la connessione è applicata una mappa crittografica. Per eliminare la mappa crittografica, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Fare clic sulla connessione nell'Elenco interfacce, quindi fare clic su **Modifica**. Selezionare la scheda **Associazione**, quindi nel campo Criterio IPSec del gruppo VPN fare clic su **Nessuno**.
- EZVPN: all'interfaccia in cui è stata creata la connessione è applicata un'associazione Easy VPN. Per eliminare Easy VPN, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Fare clic sulla connessione nell'Elenco interfacce, quindi fare clic su **Modifica**. Selezionare la scheda **Associazione**, quindi nel campo Easy VPN del gruppo VPN fare clic su **Nessuno**.
- VPDN: nella configurazione del router sono presenti comandi VPDN necessari per una configurazione PPPoE. Se nel router sono configurate altre connessioni PPPoE, è necessario non eliminare i comandi VPDN.
- ip tcp adjust mss: questo comando è applicato a un'interfaccia LAN per regolare la dimensione massima dei pacchetti TCP. Se nel router sono configurate altre connessioni PPPoE, è necessario non eliminare questo comando.
- Connessione di backup: quando per l'interfaccia primaria è configurata una connessione di backup. Per eliminare l'associazione di backup, fare clic su **Configura** e quindi su **Interfacce e connessioni**. Scegliere l'interfaccia di backup in Elenco interfacce, quindi fare clic su **Modifica**. Selezionare la scheda **Backup** e deselezionare la casella di controllo **Attiva backup**.
- Modalità PAT su connessione di backup: nell'interfaccia di backup è configurata la modalità PAT. Per eliminare l'associazione PAT, fare clic su **Configura** e quindi su **NAT**. Scegliere la regola associata a questa connessione e fare clic su **Elimina**.
- Route predefinita non permanente su connessione di backup: l'interfaccia di backup è configurata con una route statica predefinita non permanente. Per eliminare la route statica non permanente, fare clic su **Configura** e quindi su **Routing**. Scegliere la route statica non permanente nella tabella Routing statico e fare clic su **Elimina**.

Riepilogo

In questa schermata è riepilogato il collegamento WAN configurato. È possibile rivedere le informazioni e, se è necessaria qualche modifica, fare clic sul pulsante Indietro per tornare alla schermata in cui è necessario apportare tali modifiche.

Verificare la connettività dopo la configurazione

Selezionare questa casella per consentire a Cisco SDM di verificare la connessione configurata dopo l'invio dei comandi al router. Cisco SDM verificherà la connessione e riporterà i risultati in un'altra finestra.

Per salvare questa configurazione nella configurazione del router in esecuzione e uscire da questa procedura guidata

Fare clic su **Fine**. In Cisco SDM le modifiche apportate alla configurazione vengono salvate nella configurazione del router in esecuzione. Tali modifiche diventeranno immediatamente effettive, tuttavia andranno perse se il router verrà disattivato.

Se è stata selezionata l'opzione **Eseguire l'anteprima dei comandi prima dell'inoltro al router** nella finestra delle preferenze Cisco SDM viene visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi dell'interfaccia della riga di comando inviati al router.

Verifica e risoluzione dei problemi di connettività

In questa finestra è possibile verificare la connessione configurata eseguendo un ping di un host remoto. Se il ping ha esito negativo, Cisco SDM segnala la probabile causa e vengono consigliate le azioni da eseguire per la risoluzione del problema.

Tipi di connessione sui quali è possibile effettuare una verifica

Cisco SDM è in grado di risolvere problemi di connessione ADSL, G.SHDSL V1 e G.SHDSL V2, utilizzando incapsulamenti PPPoE, AAL5SNAP o AAL5MUX.

Cisco SDM è in grado di risolvere problemi di connessione Ethernet con incapsulamento PPPoE.

Cisco SDM non può diagnosticare la risoluzione dei problemi sulle connessioni Ethernet incapsulate, le Connessioni seriali T1 o E1, le connessioni Analogiche e le connessioni ISDN. Cisco SDM fornisce un controllo ping di base per questi tipi di connessione.

Procedura di una verifica di base mediante ping

Quando Cisco SDM effettua una verifica di base mediante ping, viene seguita la procedura descritta di seguito.

1. Viene verificato se l'interfaccia è attiva o disattiva.
2. Viene verificato se le impostazioni DNS sono opzioni predefinite di Cisco SDM o nomi host indicati dall'utente.
3. Vengono verificate le configurazioni DHCP e IPCP nell'interfaccia.
4. Viene conclusa la fase di verifica dell'interfaccia.
5. Viene eseguito il ping della destinazione.

Cisco SDM riporta i risultati di ciascuna di queste verifiche nelle colonne Attività e Stato. Se il ping ha esito positivo, la connessione sarà segnalata come attiva. In caso contrario, la connessione viene riportata come disattiva e la verifica non riuscita viene segnalata.

Modalità di risoluzione dei problemi da parte di Cisco SDM

Per risolvere un problema di connessione, Cisco SDM esegue una verifica più completa rispetto alla verifica di base mediante ping. Se la verifica effettuata dal router ha esito negativo, Cisco SDM esegue verifiche aggiuntive in modo da fornire le possibili cause dell'errore. Ad esempio, se lo stato relativo al livello 2 è disattivato, Cisco SDM determina e segnala le cause dell'errore e vengono consigliate le azioni da eseguire per la risoluzione del problema. Cisco SDM esegue le seguenti attività:

1. Viene verificato lo stato dell'interfaccia. Se il protocollo di livello 2 è attivo, Cisco SDM procede al passo 2.

   In caso contrario, Cisco SDM verifica lo stato del collegamento PVC (Permanent Virtual Circuit) dell'interfaccia ATM per le connessioni XDSL o lo stato del protocollo PPPoE per connessioni Ethernet incapsulate.

   - Se la verifica del collegamento PVC dell'interfaccia ATM ha esito negativo, Cisco SDM visualizza le possibili cause dell'errore e le azioni da eseguire per la risoluzione del problema.
   - Se la connessione PPPoE non è attiva, c'è un problema di collegamento dei cavi. Cisco SDM, quindi, visualizza le cause e le azioni appropriate da eseguire.

   Dopo aver effettuato questi controlli, la verifica è terminata e Cisco SDM visualizza i risultati e le azioni consigliate da eseguire.

2. Viene verificato se le impostazioni DNS sono opzioni predefinite di Cisco SDM o nomi host indicati dall'utente.

3. Viene verificata la configurazione e lo stato dei protocolli DHCP o IPCP. Se il router è dotato di un indirizzo IP assegnato mediante DHCP o IPCP, Cisco SDM procede al passo 4.

   Se il router è configurato per i protocolli DHCP o IPCP ma non ha ricevuto un indirizzo IP mediante uno di questi metodi, Cisco SDM esegue le verifiche riportate nel passo indicato sopra1. Terminata la verifica, Cisco SDM visualizza i risultati insieme alle azioni consigliate da eseguire.

4. Viene eseguito il ping della destinazione. In caso di esito positivo del ping, Cisco SDM segnala la riuscita.

In caso di esito negativo del ping su una connessione xDSL con incapsulamento PPPoE, Cisco SDM verifica i seguenti elementi:

- lo stato del collegamento PVC dell'interfaccia ATM;
- lo stato del tunnel PPPoE;
- lo stato dell'autenticazione PPP.

Dopo aver effettuato questi controlli, Cisco SDM segnala il motivo della non riuscita del ping.

In caso di esito negativo del ping su una connessione Ethernet con incapsulamento PPPoE, Cisco SDM verifica i seguenti elementi:

- lo stato del tunnel PPPoE;
- lo stato dell'autenticazione PPP.

Dopo aver effettuato questi controlli, Cisco SDM segnala il motivo della non riuscita del ping.

In caso di esito negativo del ping su una connessione xDSL con incapsulamento AAL5SNAP o AAL5MUX, Cisco SDM verifica lo stato del collegamento PVC dell'interfaccia ATM e segnala il motivo della non riuscita del ping.

Indirizzo IP/Nome host

Specificare il nome del server per eseguire il ping dell'interfaccia WAN.

Determinato automaticamente da SDM

Cisco SDM esegue il ping dell'host predefinito per verificare l'interfaccia WAN. Cisco SDM rileva i server DNS del router configurati in modo statico e i server DNS importati in modo dinamico. Cisco SDM esegue il ping di tali server e nel caso il ping riesca tramite l'interfaccia sottoposta a test, Cisco SDM segnala l'esito positivo. Se nessun ping è riuscito o non sono stati trovati ping riusciti per l'interfaccia sottoposta a verifica, Cisco SDM segnala l'errore.

Specificato da utente

Specificare l'indirizzo IP del nome host prescelto per la verifica dell'interfaccia WAN.

Riepilogo

Fare clic su questo pulsante per visualizzare un riepilogo delle informazioni relative alla risoluzione dei problemi.

Dettagli

Fare clic su questo pulsante per visualizzare i dettagli delle informazioni relative alla risoluzione dei problemi.

Attività

In questa colonna sono visualizzate le attività legate alla risoluzione dei problemi.

Stato

Consente di visualizzare lo stato di ciascuna attività di risoluzione dei problemi, contrassegnato dalle icone e dagli avvisi riportati di seguito:


La connessione è attiva.


La connessione non è attiva.


La verifica ha avuto esito positivo.


La verifica ha avuto esito negativo.

Motivi errore

In questa casella vengono fornite le possibili cause dell'errore di connessione dell'interfaccia WAN.

Azioni consigliate

In questa casella vengono fornite possibili azioni per risolvere il problema.

Tabella riassuntiva funzioni

Funzione	Procedura
Risoluzione di problemi di connessione dell'interfaccia WAN	Fare clic sul pulsante **Avvia**. Quando la verifica è in esecuzione, l'etichetta del pulsante **Avvia** diventerà **Arresta**. Si ha quindi la possibilità di interrompere la risoluzione dei problemi durante la fase di verifica.
Salvataggio del report di verifica	Fare clic sul pulsante **Salva report** per salvare il report della verifica in formato HTML. Il pulsante è attivo solo quando la verifica è in corso o è completa.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come visualizzare i comandi IOS inviati al router?

Vedere la sezione Come visualizzare i comandi IOS inviati al router?

Come configurare un'interfaccia WAN non supportata?

In Cisco SDM non è possibile configurare ogni interfaccia WAN supportata dal router in uso. Se nel router viene rilevata un'interfaccia non supportata da Cisco SDM o un'interfaccia supportata con una configurazione non supportata, Cisco SDM visualizza un pulsante di opzione denominato Altro (non supportato da Cisco SDM). L'interfaccia non supportata viene visualizzata nella finestra Interfacce e connessioni, ma non può essere configurata mediante Cisco SDM.

Per configurare un'interfaccia non supportata, è necessario utilizzare l'interfaccia della riga di comando (CLI) del router.

Come attivare o disattivare un'interfaccia?

È possibile disattivare un'interfaccia senza rimuoverne la configurazione e riattivare un'interfaccia non attiva.

Passo 1 Fare clic su **Configura** sulla barra degli strumenti di Cisco SDM.

Passo 2 Fare clic su **Interfacce e connessioni** nel frame a sinistra.

Passo 3 Scegliere l'interfaccia che si intende attivare o disattivare.

Passo 4 Se l'interfaccia è attiva, verrà visualizzato il pulsante Disattiva sotto Elenco interfacce. Fare clic su questo pulsante per disattivare l'interfaccia. Se l'interfaccia non è attiva, nella stessa posizione verrà visualizzato il pulsante Attiva. Scegliere questo pulsante per attivare l'interfaccia.

Come visualizzare l'attività dell'interfaccia WAN?

È possibile visualizzare l'attività dell'interfaccia WAN utilizzando la funzione di controllo di Cisco SDM. Con le schermate di controllo è possibile visualizzare statistiche sull'interfaccia WAN, incluso il numero di pacchetti e byte che sono stati inviati o ricevuti dall'interfaccia e il numero di errori di trasmissione o ricezione che si sono verificati. Per visualizzare le statistiche sull'interfaccia WAN, eseguire la procedura descritta di seguito.

Passo 1 Nella barra degli strumenti, fare clic su **Controlla**.

Passo 2 Nel frame a sinistra, fare clic su **Stato dell'interfaccia**.

Passo 3 Nel campo Selezionare un'interfaccia, scegliere l'interfaccia WAN di cui si desidera visualizzare le statistiche.

Passo 4 Scegliere i dati da visualizzare selezionando le relative caselle di controllo. È possibile visualizzare fino a quattro statistiche per volta.

Passo 5 Fare clic su **Visualizza dettagli** per visualizzare le statistiche per tutti i dati selezionati.

Viene visualizzata la schermata Dettagli interfaccia che mostra le statistiche selezionate. Il router viene interrogato ogni 10 secondi, quindi i dati visualizzati sono in tempo reale. Se si tratta di un'interfaccia attiva con trasmissione di dati viene visualizzato un incremento nel numero di pacchetti e byte trasferiti.

Come configurare il protocollo NAT in un'interfaccia WAN?

Passo 1 Fare clic su **Configura** nella barra degli strumenti di Cisco SDM.

Passo 2 Fare clic su **NAT** nel frame a sinistra.

Passo 3 Nella finestra NAT, scegliere **Indica interfacce NAT**.

Passo 4 Scegliere l'interfaccia nella quale si desidera configurare il protocollo NAT.

Passo 5 Selezionare l'opzione **inside(trusted)** accanto all'interfaccia per designarla come interfaccia interna o trusted. Viene di solito definita interna un'interfaccia che serve una LAN le cui risorse devono essere protette. Selezionare l'opzione **outside(untrusted)** per designare l'interfaccia come un'interfaccia esterna. Tali interfacce sono solitamente connesse a una rete untrusted. Fare clic su **OK**.

L'interfaccia viene aggiunta al pool di interfacce che utilizza il protocollo NAT.

Passo 6 Rivedere le regole NAT (Network Address Translation) nella finestra NAT. Per aggiungere, eliminare o modificare una regola, fare clic sul pulsante appropriato nella finestra NAT.

Per maggiori informazioni, fare clic sui seguenti collegamenti:

- Aggiungi o Modifica regola di conversione indirizzi statici - Da interna a esterna
- Aggiungi o Modifica regola di conversione indirizzi statici - Da esterna a interna
- Aggiungi o Modifica regola di conversione indirizzi dinamici - Da interna a esterna
- Aggiungi o Modifica regola di conversione indirizzi dinamici - Da esterna a interna

Come configurare il protocollo NAT in un'interfaccia non supportata?

Cisco SDM è in grado di configurare il protocollo NAT (Network Address Translation) in un'interfaccia non supportata da Cisco SDM. Prima di configurare il firewall, è necessario configurare l'interfaccia mediante l'interfaccia della riga di comando (CLI) del router. È necessario che tale interfaccia disponga di almeno un indirizzo IP e che sia funzionante. Per verificare il corretto funzionamento della connessione, assicurarsi che lo stato dell'interfaccia sia attivato.

Dopo aver configurato l'interfaccia non supportata mediante CLI, è possibile configurare il protocollo NAT mediante Cisco SDM. Nell'elenco delle interfacce del router, l'interfaccia non supportata verrà visualizzata come "Altro".

Come configurare un protocollo di routing dinamico?

Per configurare un protocollo di routing dinamico, eseguire la procedura riportata di seguito.

Passo 1 Nella barra degli strumenti, fare clic su **Configura**.

Passo 2 Nel frame a sinistra, fare clic su **Routing**.

Passo 3 Nel gruppo di routing dinamico, scegliere il protocollo di routing dinamico che si desidera configurare.

Passo 4 Fare clic su **Modifica**.

Verrà visualizzata la finestra di dialogo Routing dinamico, che mostra la scheda del protocollo di routing dinamico selezionato.

Passo 5 Utilizzando i campi presenti in questa finestra di dialogo, configurare il protocollo di routing dinamico. Per visualizzare la spiegazione relativa ai campi della finestra di dialogo, fare clic su**?**.

Passo 6 Terminata la configurazione del protocollo di routing dinamico, scegliere **OK**.

Come configurare il DDR (Dial-on-Demand Routing) per la connessione ISDN o l'interfaccia asincrona?

Le connessioni ISDN BRI e asincrone sono connessioni di tipo dialup. Ciò significa che per stabilire una connessione, il router deve comporre un numero di telefono preconfigurato. I costi di questo tipo di connessione sono di solito determinati dal tempo di connessione e, nel caso di una connessione asincrona, dal periodo di tempo in cui la linea telefonica è occupata. Per questo tipo di connessioni è quindi consigliabile configurare il DDR.

Per configurare il DDR in Cisco SDM è possibile effettuare le operazioni descritte di seguito.

- Associare una regola (o ACL) alla connessione. In questo modo il router stabilisce una connessione solo quando riconosce il traffico che nella regola associata è stato identificato come interessante.
- Impostare i valori di timeout idle, in modo che il router termini la connessione dopo un certo intervallo di tempo in cui non c'è attività nella connessione.
- Abilitare PPP multilink, in modo che la connessione ISDN BRI utilizzi solo uno dei due canali B, a meno che sul primo canale B non venga superata una determinata percentuale di larghezza di banda. Questa soluzione consente di diminuire i costi di connessione quando il traffico è ridotto e il secondo canale B non è necessario e allo stesso tempo di utilizzare l'intera larghezza di banda della connessione ISDN BRI, se necessario.

Per configurare il DDR su una connessione ISDN BRI o asincrona esistente, seguire la procedura riportata di seguito.

Passo 1 Fare clic su **Configura** sulla barra degli strumenti di Cisco SDM.

Passo 2 Fare clic su **Interfacce e connessioni** nel frame a sinistra.

Passo 3 Scegliere l'interfaccia ISDN o asincrona in cui si desidera configurare il routing DDR.

Passo 4 Fare clic su **Modifica**.

Viene visualizzata la scheda Connessione.

Passo 5 Scegliere **Opzioni**.

Viene visualizzata la finestra di dialogo Modifica opzione dialer.

Passo 6 Se si desidera che la connessione venga stabilita dal router solo quando viene riconosciuto uno specifico traffico IP, fare clic sul pulsante di opzione **Filtra il traffico in base all'ACL selezionato** e immettere un numero di regola (ACL) per identificare quale traffico IP consentirà l'attivazione del router oppure fare clic sul pulsante **...** per cercare l'elenco delle regole e scegliere la regola che si desidera utilizzare per identificare il traffico IP.

Passo 7 Se si desidera configurare il router in modo da terminare la connessione quando per un certo intervallo di tempo non è attiva, vale a dire non c'è passaggio di traffico, nel campo **Valore di timeout idle**, immettere il numero di secondi in cui la connessione può rimanere non attiva prima che venga interrotta dal router.

Passo 8 Se si sta modificando una connessione ISDN e si desidera utilizzare il secondo canale B solo quando il traffico sul primo canale B supera una certa soglia, selezionare la casella di controllo **Attiva MultiLink PPP**, quindi nel campo **Soglia di carico**, immettere un numero compreso tra 1 e 255, dove 255 corrisponde al 100% della larghezza di banda, che determinerà la soglia sul primo canale B. Quando il traffico sul canale supera quella soglia, il router verrà connesso al secondo canale B. Inoltre, nel campo **Direzione dati** è possibile stabilire se tale soglia sia applicata al traffico in ingresso o in uscita.

Passo 9 Fare clic su **OK**.

Come modificare la configurazione dell'interfaccia radio?

È necessario utilizzare Applicazione wireless per modificare la configurazione di un'interfaccia radio esistente.

Passo 1 Fare clic su **Configura** sulla barra degli strumenti di Cisco SDM.

Passo 2 Fare clic su **Interfacce e connessioni** nel frame a sinistra e selezionare la scheda Modifica interfaccia/connessione.

Passo 3 Scegliere l'interfaccia radio e fare clic su **Modifica**. Nella scheda Connections, è possibile modificare l'indirizzo IP o le informazioni di bridging. Se si desidera modificare altri parametri wireless, fare clic su **Avvia applicazione wireless**.

CAPITOLO 5

Modifica interfaccia/connessione

In questa finestra sono visualizzate le interfacce e le connessioni del router. È inoltre possibile aggiungere, modificare, eliminare, attivare e disattivare le connessioni.

Aggiungi

Quando si seleziona un'interfaccia fisica non configurata e si fa clic su **Aggiungi**, il menu consente di aggiungere una connessione su tale interfaccia. Fare clic su **Aggiungi** per creare una nuova interfaccia di tipo loopback o tunnel. Se l'immagine Cisco IOS nel router supporta le VTI (Virtual Template Interfaces, interfacce modello virtuale), il menu contestuale contiene l'opzione di aggiunta di una VTI. Se il router presenta porte switch, è possibile aggiungere una nuova VLAN.

Se si desidera riconfigurare un'interfaccia e sono disponibili solo le opzioni Loopback e Tunnel quando si fa clic su **Aggiungi**, selezionare l'interfaccia e fare clic su **Elimina**. Tutti i tipi di connessioni disponibili per quel tipo di interfaccia verranno visualizzati nel menu Aggiungi. Fare clic su **Configurazioni delle interfacce disponibili** per visualizzare quali configurazioni sono disponibili per le interfacce.

Modifica

Quando si seleziona un'interfaccia e si fa clic su **Modifica** viene visualizzata una finestra di dialogo. Se l'interfaccia è supportata e configurata e non è una porta switch, in tale finestra saranno presenti le seguenti schede:

- Connessione
- Associazione

- NAT
- Servizio applicazione
- Generale

Se invece l'interfaccia non è supportata, in tale finestra *non* sarà presente la scheda Connessione. Se infine si seleziona una porta switch, viene visualizzata la finestra di dialogo Modifica porta switch. Il pulsante Modifica sarà disattivato se l'interfaccia è supportata ma non è stata configurata.

Elimina

Se si seleziona una connessione e si fa clic su **Elimina** viene visualizzata una finestra di dialogo in cui sono elencate le associazioni della connessione e in cui si richiede se si desidera rimuovere la connessione insieme alle associazioni. È anche possibile eliminare solo la connessione.

Riepilogo

Se si fa clic sul pulsante Riepilogo è possibile nascondere i dettagli relativi alla connessione e visualizzare solo l'indirizzo IP, il tipo, lo slot, lo stato e la descrizione.

Dettagli

Se si fa clic su **Dettagli** è possibile visualizzare l'area Dettagli relativi all'interfaccia, descritta in seguito. I dettagli relativi all'interfaccia sono visualizzati per impostazione predefinita.

Attiva o Disattiva

Quando l'interfaccia o la connessione selezionata è inattiva, questo comando viene visualizzato come pulsante **Attiva**. Fare clic sul pulsante **Attiva** per attivare l'interfaccia o la connessione selezionata. Quando l'interfaccia o la connessione selezionata è attiva, questo comando viene visualizzato come pulsante **Disattiva**. Fare clic sul pulsante **Disattiva** per disattivare manualmente l'interfaccia o la connessione selezionata. Questo pulsante non può essere utilizzato con un'interfaccia la cui configurazione non sia stata trasmessa al router.

Verifica connessione

Per verificare la connessione selezionata, fare clic su questo pulsante. Viene visualizzata una finestra di dialogo che consente di specificare un host remoto verso cui eseguire un ping durante la connessione. Si viene quindi informati sull'esito della verifica. Se la verifica ha esito negativo, vengono fornite informazioni sulle probabili cause del problema e sulle procedure da eseguire per risolverlo.

Elenco interfacce

In questo elenco sono visualizzate le interfacce fisiche e le connessioni logiche verso cui sono state configurate.

Interfacce

In questa colonna vengono elencate per nome le interfacce fisiche e logiche. Se un'interfaccia logica viene configurata per un'interfaccia fisica, l'interfaccia logica viene mostrata al di sotto di quella fisica.

Se Cisco SDM è in esecuzione su un router della famiglia Cisco 7000, sarà possibile creare una connessione solo su interfacce Ethernet e Fast Ethernet.

Indirizzo IP

Questa colonna può contenere i seguenti tipi di indirizzo IP:

- Indirizzo IP configurato dell'interfaccia.
- Client DHCP: l'interfaccia riceve un indirizzo IP da un server DHCP (Dynamic Host Configuration Protocol).
- Indirizzo IP negoziato: l'interfaccia riceve un indirizzo IP tramite negoziazione con il dispositivo remoto.
- IP senza numero: il router userà un solo indirizzo di un pool di indirizzi IP fornito dal provider di servizi Internet per il router in uso e per i dispositivi sulla LAN.
- Non applicabile: al tipo di interfaccia non può essere assegnato un indirizzo IP.

Tipo

In questa colonna è visualizzato il tipo di interfaccia, ad esempio Ethernet, seriale o ATM.

Slot

In questa colonna è visualizzato il numero dello slot fisico del router in cui è stata installata l'interfaccia. Se Cisco SDM è in esecuzione su un router Cisco 1710, il campo slot sarà vuoto.

Stato

In questa colonna viene indicato se l'interfaccia è attiva o disattiva. L'icona verde con la freccia rivolta verso l'alto sta a indicare che l'interfaccia è attiva. L'icona rossa con la freccia rivolta verso il basso sta a indicare che l'interfaccia è inattiva.

Descrizione

In questa colonna sono contenute le descrizioni fornite per la connessione.

Dettagli relativi all'interfaccia

In quest'area della finestra sono visualizzati i dettagli delle associazioni e, se disponibili, delle connessioni relative all'interfaccia selezionata nell'elenco interfacce. Nei dettagli relativi alle associazioni sono riportate informazioni quali le regole NAT (Network Address Translation), le regole di accesso e le Inspection Rule, i criteri IPSec e le configurazioni Easy VPN. Nei dettagli relativi alle connessioni, invece, sono indicate informazioni quali gli indirizzi IP, il tipo di incapsulamento e le opzioni DHCP.

Nome elemento

In questa colonna è indicato il nome dell'elemento di configurazione, ad esempio una combinazione indirizzo IP/subnet mask oppure un criterio IPSec. Il contenuto effettivo della colonna dipende dal tipo di interfaccia selezionata.

Valore elemento

Se per l'elemento selezionato è stato configurato un valore, esso viene visualizzato in questa colonna.

Tabella riassuntiva funzioni

Per:	Procedura:
Aggiunta di una nuova connessione	Fare clic su **Aggiungi** e selezionare la connessione nel menu di scelta rapida.
Aggiunta di una nuova interfaccia logica.	Fare clic su **Aggiungi** e selezionare un'interfaccia logica nel menu di scelta rapida.
Aggiunta di una nuova interfaccia VLAN	Fare clic su **Aggiungi**, selezionare **Nuova interfaccia logica** nel menu di scelta rapida e quindi selezionare **VLAN** nel sottomenu.
Modifica di un'interfaccia esistente.	Selezionare l'interfaccia che si desidera modificare e quindi fare clic su **Modifica**. **Nota** Se si sta modificando un tunnel GRE, la scheda Connessione non verrà visualizzata se tale tunnel non è stato configurato per l'utilizzo della modalità **gre ip**.
Reimpostazione di un'interfaccia fisica su uno stato non configurato.	Selezionare l'interfaccia fisica e quindi fare clic su **Reimposta**.
Eliminazione di un'interfaccia logica.	Selezionare l'interfaccia che si desidera eliminare, quindi fare clic su **Elimina**.
Reperimento di informazioni su come eseguire attività di configurazione correlate.	Visualizzare una delle seguenti procedure: • Come configurare una route statica? • Come visualizzare l'attività dell'interfaccia LAN? • Come attivare o disattivare un'interfaccia? • Come visualizzare i comandi IOS inviati al router? • Come configurare un'interfaccia WAN non supportata? • Come visualizzare l'attività dell'interfaccia WAN? • Come configurare il protocollo NAT in un'interfaccia WAN? • Come configurare una route statica? • Come configurare un protocollo di routing dinamico?

Interfacce e connessioni di sola lettura

Vi sono molte condizioni che impediscono di modificare mediante Cisco SDM un'interfaccia principale o secondaria precedentemente configurata.

- Per ulteriori informazioni sui motivi per cui un'interfaccia principale o secondaria precedentemente configurata come seriale risulta essere di sola lettura nell'elenco delle interfacce, consultare l'argomento della Guida Motivi per i quali la configurazione di un'interfaccia seriale o di un'interfaccia secondaria può essere di sola lettura.
- Per ulteriori informazioni sui motivi per cui un'interfaccia principale o secondaria precedentemente configurata come ATM risulta essere di sola lettura nell'elenco delle interfacce, consultare l'argomento della Guida Motivi per i quali la configurazione di un'interfaccia ATM o di un'interfaccia secondaria può essere di sola lettura.
- Per ulteriori informazioni sui motivi per cui un'interfaccia precedentemente configurata come Ethernet LAN o WAN risulta essere di sola lettura nell'elenco delle interfacce, consultare l'argomento della Guida Motivi per i quali la configurazione di un'interfaccia Ethernet può essere di sola lettura.
- Per ulteriori informazioni sui motivi per cui un'interfaccia precedentemente configurata come ISDN BRI risulta essere di sola lettura nell'elenco delle interfacce, consultare l'argomento della Guida Motivi per i quali la configurazione di un'interfaccia ISDN BRI può essere di sola lettura.

Connessione - Ethernet per IRB

Se nell'elenco Configura si seleziona **Ethernet per IRB**, in questa finestra di dialogo verranno visualizzati i campi seguenti.

Current Bridge Group/Associated BVI (Bridge Group corrente/BVI associata)

Questi campi di sola lettura contengono il valore Bridge Group corrente e il nome corrente della BVI (Bridge-Group Virtual Interface).

Crea un nuovo Bridge Group/Unisci un Bridge Group esistente

Selezionare questa opzione se si desidera rendere l'interfaccia un membro di un nuovo Bridge Group o se si desidera unirla a un Bridge Group esistente. Per creare un nuovo Bridge Group, immettere un numero compreso tra 1 e 255. Se si desidera unire l'interfaccia a un Bridge Group esistente, selezionare l'interfaccia BVI che è già membro di quel gruppo.

Indirizzo IP

Immettere l'indirizzo IP e la subnet mask nei relativi campi.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Ethernet per il routing

Se nell'elenco Configura si seleziona **Ethernet per il routing**, in questa finestra di dialogo verranno visualizzati i campi seguenti.

Indirizzo IP

Immettere un indirizzo IP e la subnet mask nei campi Indirizzo IP. Questo indirizzo sarà l'indirizzo IP di origine del traffico che proviene da questa interfaccia e l'indirizzo IP di destinazione per il traffico destinato agli host connessi a tale interfaccia.

DHCP Relay

Fare clic per configurare il router come DHCP Relay. Un dispositivo utilizzato come agente di relay DHCP inoltra le richieste DHCP a un server DHCP. Quando un dispositivo richiede l'assegnazione dinamica dell'indirizzo IP, esso effettua il broadcast di una richiesta DHCP. Un server DHCP risponde quindi a questa richiesta comunicando un indirizzo IP. Nella stessa subnet è possibile configurare al massimo un solo agente di relay DHCP o un solo server DHCP.

Nota Se il router è stato configurato in precedenza come un agente di relay DHCP con più indirizzi IP di server DHCP remoti, questi campi verranno disattivati.

Indirizzo IP del server DHCP remoto.

Immettere l'indirizzo IP del server DHCP che fornirà gli indirizzi ai dispositivi sulla LAN.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Metodi DNS dinamici esistenti

Questa finestra consente di scegliere un metodo DNS dinamico da associare con un'interfaccia WAN.

Questo elenco di metodi DNS dinamici mostra il nome di ciascun metodo e i parametri associati. Scegliere un metodo dall'elenco e fare clic su **OK** per associarlo all'interfaccia WAN.

Per aggiungere, modificare o cancellare i metodi DNS dinamici passare a **Configura > Attività aggiuntive > Metodi DNS dinamici**.

Aggiungi metodo DNS dinamico

Questa finestra consente di aggiungere un metodo DNS dinamico. Scegliere il tipo di metodo tra HTTP e IETF, e configurarlo.

HTTP

HTTP è un metodo DNS dinamico che aggiorna un provider di servizi DNS con modifiche dell'indirizzo IP dell'interfaccia associato.

Server

Se si usa HTTP, scegliere l'indirizzo del dominio del provider di servizi DNS dal menu a tendina.

Nome utente

Se si usa l'HTTP, immettere un nome utente per l'accesso al provider di servizi DNS.

Password

Se si usa l'HTTP, immettere una password per l'accesso al provider di servizi DNS.

IETF

IETF è un metodo DNS dinamico che aggiorna un provider di servizi DNS con modifiche dell'indirizzo IP dell'interfaccia associato.

Server DNS

Se si utilizza il metodo IETF senza aver configurato un server DNS per il router in **Configura > Attività aggiuntive > DNS**, immettere l'indirizzo IP del proprio server DNS.

Nome host

Immettere un nome host se non ne è stato configurato nessuno in **Configura > Attività aggiuntive > Proprietà router > Modifica > Host** o se si desidera sostituire il nome host configurato. Quando si aggiorna l'indirizzo IP dell'interfaccia, il metodo DNS dinamico invia il nome host insieme al nuovo indirizzo IP dell'interfaccia.

Nome di dominio

Immettere un nome dominio se non ne è stato configurato nessuno in **Configura > Attività aggiuntive > Proprietà router > Modifica > Dominio** o se si desidera sostituire il nome dominio configurato. Quando si aggiorna l'indirizzo IP dell'interfaccia, il metodo DNS dinamico invia il nome dominio insieme al nuovo indirizzo IP dell'interfaccia.

Wireless

Se il router presenta un'interfaccia wireless, è possibile avviare l'applicazione wireless da questa scheda. Tale applicazione può essere avviata anche dal menu Strumenti se si seleziona **Strumenti > Applicazione wireless**.

Associazione

Utilizzare questa finestra per visualizzare, creare, modificare o eliminare le associazioni fra le interfacce e le regole o le connessioni VPN.

Interfaccia

In questo campo è indicato il nome dell'interfaccia che è stata selezionata nella finestra Interfacce e connessioni.

Zona

Se questa interfaccia fa parte di una zona di protezione, nel campo viene visualizzato il nome di tale zona. Se si desidera includere questa interfaccia in una zona di protezione, fare clic sul pulsante a destra del campo, scegliere **Seleziona zona** e specificare la zona nella finestra di dialogo visualizzata. Per creare una nuova zona, scegliere **Crea zona**, specificare il nome della zona nella finestra di dialogo visualizzata e fare clic su OK. Nel campo della zona viene visualizzato il nome della zona creata.

Regola di accesso

In questo campo sono riportati i nomi o i numeri delle regole di accesso associate all'interfaccia. Le regole di accesso sono utilizzate per consentire o bloccare il traffico il cui indirizzo IP e i cui criteri di servizio corrispondono a quelli specificati nella regola.

In ingresso

In questo campo è indicato il nome o il numero della regola di accesso applicata al traffico in ingresso sull'interfaccia. Per applicare una regola, fare clic sul pulsante **...** e selezionare una regola esistente o creare una nuova regola e quindi selezionarla.

Quando si applica una regola al traffico in ingresso su un'interfaccia, tale regola filtra il traffico prima che questo acceda al router. I pacchetti bloccati dalla regola vengono scartati e non saranno instradati verso un'altra interfaccia. Quando a un'interfaccia si applica una regola nella direzione in ingresso, si impedisce non solo che il traffico in ingresso acceda a una rete trusted connessa al router, ma anche che esso venga instradato altrove dal router locale.

In uscita

In questo campo è indicato il nome o il numero della regola di accesso applicata al traffico in uscita dall'interfaccia. Per applicare una regola, fare clic sul pulsante **...** e selezionare una regola esistente o creare una nuova regola e quindi selezionarla.

Quando si applica una regola al traffico in uscita da un'interfaccia, la regola filtra il traffico dopo il suo ingresso nel router e prima della sua uscita dall'interfaccia. I pacchetti bloccati dalla regola vengono scartati prima di uscire dall'interfaccia.

Inspect Rule

In questo campo sono riportati i nomi delle Inspection Rule associate all'interfaccia. Le Inspection Rule creano dei varchi temporanei nel firewall in modo che gli host all'interno del firewall che hanno iniziato sessioni di un certo tipo possano ricevere solo il traffico di ritorno coerente con la sessione iniziata.

In ingresso

In questo campo è indicato il nome o il numero dell'Inspection Rule applicata al traffico in ingresso sull'interfaccia. Per applicare una regola in ingresso, fare clic sul menu a tendina **In ingresso** e selezionare una regola.

In uscita

In questo campo è indicato il nome o il numero dell'Inspection Rule applicata al traffico in uscita dall'interfaccia. Per applicare una regola in uscita, fare clic sul menu a tendina **In uscita** e selezionare una regola.

VPN

Le reti VPN consentono di proteggere il traffico dati trasmesso su linee che possono non essere sotto il controllo dell'organizzazione. È possibile utilizzare l'interfaccia selezionata in una VPN associando ad essa un criterio IPSec.

Criterio IPSec

In questo campo è riportato il criterio IPSec associato all'interfaccia. Per associare un criterio IPSec all'interfaccia, selezionare il criterio desiderato da questo elenco.

Nota Un'interfaccia può essere associata a un solo criterio IPSec.

Nota Per creare un tunnel GRE su IPSec, è necessario innanzitutto associare il criterio all'interfaccia tunnel e quindi all'interfaccia di origine del tunnel stesso. Ad esempio, per associare un criterio a un tunnel di tipo Tunnel3, la cui interfaccia di origine è Serial0/0, è necessario innanzitutto selezionare Tunnel3 nella finestra Interfacce e connessioni, fare clic su **Modifica,** associare il criterio e fare clic su **OK**. Quindi, è necessario selezionare l'interfaccia Serial0/0 e associarvi lo stesso criterio.

EzVPN

Se l'interfaccia è utilizzata per una connessione Easy VPN, in questo campo è visualizzato il nome della connessione.

Nota Non è consentito utilizzare la stessa interfaccia per una connessione VPN (Virtual Private Network) e una connessione Easy VPN.

Modifica delle associazioni

Quando si cambiano le proprietà di associazione di un'interfaccia le modifiche si riflettono nella parte inferiore della schermata Modifica interfaccia/connessione. Ad esempio, se all'interfaccia si associa un criterio IPSec, il nome di tale criterio viene automaticamente riportato anche nella parte inferiore della finestra. Se si elimina un'associazione, il valore riportato nella colonna Valore elemento cambia automaticamente in <Nessuno>.

NAT

Se s'intende utilizzare l'interfaccia in una configurazione NAT, è necessario stabilire se essa è interna o esterna. Selezionare la direzione del traffico a cui si desidera applicare la configurazione NAT. Se l'interfaccia è connessa a una LAN servita dal router, selezionare **Interna**. Se invece è connessa a Internet oppure alla WAN aziendale, selezionare **Esterna**. Se l'interfaccia selezionata non è utilizzabile in una configurazione NAT, ad esempio nel caso di un'interfaccia logica, questo campo viene disattivato e contiene il valore Non supportata.

Modifica porta switch

In questa finestra è possibile modificare le informazioni VLAN relative alle porte switch Ethernet.

Gruppo Modalità

Selezionare il tipo di dati VLAN da inoltrare attraverso la porta switch Ethernet. Se si seleziona **Accesso**, solo i dati destinati al numero VLAN specifico saranno inoltrati attraverso la porta switch. Se invece si seleziona **Trunking**, attraverso la porta switch saranno inoltrati i dati di tutte le VLAN, compresi i dati della VLAN stessa. Selezionare **Trunking** per effettuare solo il "trunking" delle porte VLAN connesse ad altri dispositivi di rete (ad esempio un altro switch) da connettere a dispositivi appartenenti a più VLAN.

VLAN

Per assegnare la porta switch a una VLAN, immettere il numero della rete VLAN desiderata. Se alla porta switch non è ancora stata assegnata una VLAN, in questo campo sarà riportato il valore predefinito VLAN 1. Per creare una nuova interfaccia VLAN con il corrispondente ID VLAN, immettere l'identificativo in questo campo e selezionare la casella di controllo **Rendi VLAN visibile all'elenco interfacce**.

Casella di controllo Rendi VLAN visibile all'elenco interfacce

Selezionare questa casella se si desidera creare una nuova VLAN con l'ID VLAN specificato nel campo VLAN.

Sovrapposizione partner

Selezionare un modulo switch da utilizzare come partner di sovrapposizione. Quando un dispositivo presenta più moduli switch, questi devono essere sovrapposti prima di altri partner di sovrapposizione.

Numero del Bridge Group

Se si desidera che questa porta switch formi parte di un bridging a una rete wireless, immettere il numero di bridge group esistente.

Velocità

Selezionare la velocità corrispondente alla rete alla quale sarà connessa la porta switch. In alternativa, selezionare **auto** per consentire l'impostazione automatica della velocità al valore ottimale.

Duplex

Selezionare **full** (completo) o **half** (metà) oppure **auto** per consentire l'impostazione automatica del duplex in base alla rete alla quale verrà connessa la porta switch.

Se l'opzione **Velocità** è impostata su **auto**, **Duplex** è disattivato.

Power Inline

L'elenco a discesa **Power inline** viene visualizzato se la porta switch supporta l'alimentazione elettrica in linea. Scegliere una delle seguenti opzioni:

- **auto**: rileva e alimenta automaticamente i dispositivi in linea.
- **never** (mai): l'alimentazione in linea non viene mai applicata.

Servizio applicazione

Questa finestra consente all'utente di associare criteri QoS e di controllare l'applicazione e il protocollo tramite l'interfaccia selezionata.

QoS

Per associare un criterio QoS all'interfaccia per il traffico in ingresso, selezionare un criterio QoS dall'elenco a discesa **In ingresso**.

Per associare un criterio QoS all'interfaccia per il traffico in uscita, selezionare un criterio QoS dall'elenco a discesa **In uscita**.

È possibile monitorare le statistiche QoS per l'interfaccia da **Controllo > Stato traffico > QoS**.

NetFlow

Per associare il controllo delle statistiche NetFlow all'interfaccia per il traffico in ingresso, selezionare la casella di controllo **In ingresso**.

Per associare il controllo delle statistiche NetFlow all'interfaccia per il traffico in uscita, selezionare la casella di controllo **In uscita**.

È possibile controllare le statistiche NetFlow per l'interfaccia da **Controllo > Stato dell'interfaccia**. È possibile controllare i talker principale e i protocolli principali NetFlow da **Controllo > Stato traffico > N flussi traffico principali**.

NBAR

Per associare il riconoscimento dell'applicazione basato sulla rete (NBAR) all'interfaccia, selezionare la casella di controllo **Protocollo NBAR**.

È possibile monitorare le statistiche NBAR per l'interfaccia da **Controllo > Stato traffico > Traffico applicazione/protocollo**.

Generale

In questa finestra sono mostrate le impostazioni generali di protezione che è possibile attivare o disattivare selezionando o deselezionando le caselle di controllo accanto ai nomi e alle descrizioni di tali impostazioni. Se la funzione Security Audit è stata autorizzata a disattivare determinate proprietà e si desidera riattivarle, è possibile utilizzare questa finestra. Di seguito sono riportate le proprietà elencate in questa finestra.

Descrizione

In questo campo si può immettere una breve descrizione della configurazione dell'interfaccia. Tale descrizione sarà visibile nella finestra Modifica Interfacce e Connessioni. Una descrizione come “Contabilità” o “Test Net 5” può aiutare altri utenti di Cisco SDM a comprendere la finalità della configurazione.

Broadcast IP

Un broadcast IP è un datagramma trasmesso all'indirizzo broadcast di una subnet alla quale il mittente non è connesso in modo diretto. Tale tipo di broadcast è instradato attraverso la rete come flusso di pacchetti unicast finché non arriva alla subnet di destinazione, dove viene convertito in un broadcast a livello di collegamento. A causa della natura dell'architettura degli indirizzamenti IP, solo l'ultimo router della catena, ovvero quello connesso direttamente alla subnet di destinazione, può identificare in modo definitivo un broadcast diretto. I broadcast diretti sono talvolta utilizzati per fini leciti ma ciò si verifica raramente al di fuori del settore dei servizi finanziari.

I broadcast IP sono utilizzati negli attacchi DoS di tipo smurf assai noti e diffusi e possono anche essere impiegati per altri attacchi similari. Gli attacchi di tipo smurf si basano sull'invio di richieste echo ICMP da un indirizzo mittente falsificato verso un indirizzo a broadcast diretto. Tutti gli host appartenenti alla subnet di destinazione reagiscono a tali richieste inviando una risposta al mittente falsificato. Inviando un flusso continuo di simili richieste chi conduce l'attacco informatico può creare un flusso di risposta molto più grande, che a sua volta inonda l'host di cui si sta falsificando l'indirizzo.

La disattivazione di “IP directed Broadcast” impedisce ai pacchetti di tipo “directed broadcast” di attraversare i link geografici saturandoli.

IP proxy ARP

Il protocollo ARP è utilizzato nelle reti per convertire gli indirizzi IP in indirizzi MAC. Di norma il protocollo ARP funziona in un'unica LAN e un router può agire da proxy per le richieste ARP, rendendo tali richieste disponibili anche fra più segmenti di LAN. Poiché questa soluzione rappresenta una violazione dei meccanismi di protezione delle LAN, i proxy ARP devono essere utilizzati solo fra due LAN aventi un uguale livello di protezione e solo se necessario.

IP route-cache flow

Questa opzione consente di attivare la funzione Cisco IOS NetFlow che permette di determinare, oltre ai flussi di dati correnti presenti sul router, la distribuzione dei pacchetti e dei protocolli. Tali informazioni sono utili per alcune attività, come la ricerca della fonte di un attacco mediante spoofing di indirizzo IP.

Nota L'opzione IP Route Cache-Flow abilita NetFlow in entrambe le direzioni di traffico, in ingresso e in uscita. Per abilitare NetFlow sul traffico in ingresso *o* in uscita, utilizzare le opzioni NetFlow disponibili nella scheda **Servizio applicazione**.

IP Redirects

I messaggi di ICMP redirect istruiscono il nodo finale ad utilizzare un router specifico per il traffico diretto verso una determinata destinazione. In una rete IP funzionante in modo corretto un router invia gli ICMP redirect soltanto verso gli host connessi alle proprie reti locali, nessun nodo finale invierà mai un ICM redirect, e nessun ICMP redirect attraverserà mai più di un hop sulla rete. Invece chi conduce un attacco può violare tali regole. Disattivare i reindirizzamenti ICMP non ha effetti negativi sulla rete e può eliminare gli attacchi di reindirizzamento.

IP mask-reply

I messaggi di risposta maschera ICMP vengono inviati quando è necessario comunicare a un dispositivo di rete la subnet mask di una determinata subnet della rete. I messaggi sono inviati da dispositivi di rete che sono a conoscenza di tali informazioni. Di conseguenza, questi messaggi possono essere impropriamente utilizzati per ottenere illecitamente informazioni sulla mappatura della rete.

IP Unreachables

L'invio di messaggi di questo tipo avviene quando un router riceve un pacchetto di tipo nonbroadcast in cui si utilizza un protocollo sconosciuto oppure quando riceve un pacchetto che non è in grado di inoltrare poiché non conosce alcun percorso per raggiungere la destinazione finale. Di conseguenza, questi messaggi possono essere impropriamente utilizzati per ottenere illecitamente informazioni sulla mappatura della rete.

Selezionare il tipo di configurazione Ethernet

Questa finestra viene visualizzata quando si fa clic su un'interfaccia nella finestra Interfacce e Connessioni e contemporaneamente Cisco SDM non riesce a determinare se l'interfaccia è configurata come interfaccia LAN o come interfaccia WAN. Quando si configura un'interfaccia tramite Cisco SDM è possibile impostarla come interfaccia interna o esterna. In base a tale scelta, Cisco SDM aggiunge automaticamente un testo descrittivo nel file di configurazione. Se invece si configura l'interfaccia utilizzando l'interfaccia della riga di comando (CLI), il file di configurazione non conterrà tale testo e quindi Cisco SDM non disporrà delle informazioni in esso contenute.

Per specificare che l'interfaccia è di tipo LAN:

Fare clic su **LAN** e quindi su **OK**. Cisco SDM aggiunge la riga di commento $ETH-LAN$ alla configurazione dell'interfaccia e l'interfaccia viene visualizzata nella finestra della configurazione guidata LAN con la designazione Interna nella finestra Interfacce e Connessioni.

Per specificare che l'interfaccia è di tipo WAN:

Fare clic su **WAN** e quindi su **OK**. Cisco SDM aggiunge la riga di commento $ETH-WAN$ alla configurazione dell'interfaccia e l'interfaccia viene visualizzata nella finestra della configurazione guidata WAN con la designazione Esterna nella finestra Interfacce e Connessioni.

Connessione - VLAN

Questa finestra consente di configurare un'interfaccia VLAN.

ID VLAN

Immettere l'ID della nuova interfaccia VLAN. Se si sta modificando un'interfaccia VLAN non è possibile modificare il suo ID.

Casella di controllo VLAN nativa

Selezionare se questa VLAN è una VLAN non-trunking.

Campi indirizzo IP

Tipo di indirizzo IP

Scegliere se l'interfaccia VLAN deve disporre di un indirizzo IP statico o di nessun indirizzo IP. Questo campo viene visualizzato se nel campo Configura come è selezionata l'opzione **Solo VLAN**.

Indirizzo IP

Immettere l'indirizzo IP dell'interfaccia VLAN.

Subnet Mask

Immettere la subnet mask dell'interfaccia VLAN o indicare il numero di bit di subnet mediante il campo a scorrimento.

DHCP Relay

Per maggiori informazioni fare clic su DHCP Relay.

Elenco sottointerfacce

Questa finestra visualizza le sottointerfacce configurate sull'interfaccia fisica scelta, e consente di aggiungere, modificare e rimuovere sottointerfacce. Per ogni sottointerfaccia configurata, la finestra visualizza l'ID della sottointerfaccia, l'ID della VLAN, l'indirizzo IP e la maschera e, se presente, una descrizione. Se ad esempio il router dispone di un'interfaccia FastEthernet1 e le sottointerfacce FastEthernet1.3 e FastEthernet1.5 sono state configurate, il contenuto di questa finestra potrebbe essere il seguente:

```
5       56      56.8.1.1/255.255.255.0
3       67      Bridge No. 77
```

In questo esempio la sottointerfaccia FastEthernet1.5 è configurata per il routing e la FastEthernet1.3 per IRB.

Nota Per visualizzare questa finestra si deve scegliere l'interfaccia fisica su cui le sottointerfacce sono configurate. Nell'esempio descritto per visualizzare questa finestra si dovrebbe scegliere FastEthernet 1. Scegliendo FastEthernet1.3 o FastEthernet1.5 e facendo clic su modifica, verrebbe visualizzata la finestra di dialogo di modifica con le informazioni relative a tale sottointerfaccia

Aggiunta, modifica, e eliminazione di pulsanti

Usare questi pulsanti per configurare, modificare e rimuovere le sottointerfacce dall'interfaccia fisica scelta.

Aggiungere o modificare l'interfaccia BVI

Aggiungere o modificare l'interfaccia BVI (Bridge Group Virtual Interface) in questa finestra. Se nel router è presente un'interfaccia Dot11Radio, viene creata automaticamente un'interfaccia BVI quando si configura un nuovo bridge group. L'operazione serve per supportare il bridging IRB. In questa finestra è possibile modificare l'indirizzo IP e la subnet mask.

Indirizzo IP/Subnet Mask

Immettere l'indirizzo IP e la subnet mask che si desidera attribuire all'interfaccia BVI.

Aggiungere o modificare l'interfaccia loopback

In questa finestra è possibile aggiungere un'interfaccia loopback all'interfaccia selezionata.

Indirizzo IP

Scegliere se si desidera che l'interfaccia loopback non disponga di alcun indirizzo IP o che disponga di un indirizzo IP statico.

Indirizzo IP statico

Se è stata selezionata l'opzione **Indirizzo IP specifico**, immettere l'indirizzo IP in questo campo.

Subnet Mask

Immettere la subnet mask in questo campo oppure specificare il numero dei bit di subnet nel campo a destra. Mediante la subnet mask il router è in grado di stabilire quali bit dell'indirizzo IP definiscono l'indirizzo di rete e quali bit definiscono invece l'indirizzo host.

Connessione - Interfaccia modello virtuale

È possibile aggiungere o modificare una VTI nel quadro di una configurazione 802.1x o VPN. Quando si modifica una VTI, i campi modificabili vengono visualizzati in una scheda Connessione.

Tipo di interfaccia

Selezionare **predefinita** o **tunnel**. Se si seleziona il tipo tunnel, è necessario selezionare anche la modalità tunnel.

Indirizzo IP

Scegliere **Senza numero**. La VTI utilizza l'indirizzo IP dell'interfaccia fisica scelta nel campo Senza numero per.

Senza numero per

Questo campo viene visualizzato quando si seleziona **Senza numero** nel campo Indirizzo IP. Scegliere l'interfaccia il cui indirizzo IP verrà utilizzato da questa VTI.

Modalità tunnel

Scegliere **IPSec-IPv4**.

Connessione - Ethernet LAN

Utilizzare questa finestra per configurare l'Indirizzo IP e le proprietà DHCP di un'interfaccia Ethernet che si desidera utilizzare come interfaccia LAN.

Indirizzo IP

Immettere l'indirizzo IP dell'interfaccia. Per ottenere l'indirizzo IP, contattare il provider di servizi o l'amministratore di rete. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. Per ottenere questo valore, contattare l'amministratore di rete. La subnet mask consente al router di determinare quale parte dell'indirizzo IP viene utilizzato per definire l'indirizzo di rete e di subnet.

DHCP Relay

Fare clic per configurare il router come agente di relay DHCP. Un dispositivo utilizzato come agente di relay DHCP inoltra le richieste DHCP a un server DHCP. Quando un dispositivo richiede l'assegnazione dinamica dell'indirizzo IP, esso effettua il broadcast di una richiesta DHCP. Un server DHCP risponde quindi a questa richiesta comunicando un indirizzo IP. Nella stessa subnet è possibile configurare un solo agente di relay DHCP o un solo server DHCP al massimo.

Nota Se il router è stato configurato in precedenza come un agente di relay DHCP con più indirizzi IP di server DHCP remoti, questo pulsante verrà disattivato.

Indirizzo IP del server DHCP remoto.

Se è stata selezionata l'opzione **DHCP Relay**, immettere l'indirizzo IP del server DHCP che fornirà gli indirizzi ai dispositivi appartenenti alla LAN.

Connessione - Ethernet WAN

In questa finestra è possibile aggiungere una connessione WAN Ethernet.

Attiva incapsulamento PPPoE

Fare clic su questa opzione se la connessione deve usare l'incapsulamento PPPoE (Protocollo Point-to-Point over Ethernet). Contattare il proprio provider dei servizi per sapere se sulla propria connessione viene utilizzato il protocollo PPPoE. Quando si configura una connessione PPPoE viene automaticamente creata un'interfaccia dialer.

Indirizzo IP

Selezionare uno dei tipi di indirizzo IP riportati di seguito e immettere le informazioni nei campi visualizzati. Se nella connessione Ethernet non viene utilizzato il protocollo PPPoE, solo le opzioni Indirizzo IP statico e Dinamico saranno visualizzate.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Dinamico (client DHCP)

Se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere il nome del server DHCP che assegnerà gli indirizzi.

IP senza numero

Scegliere **IP senza numero** se si desidera che interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia con l'indirizzo IP che questa interfaccia dovrà condividere.

Easy IP (IP negoziato)

Selezionando l'opzione Easy IP (IP negoziato), il router otterrà un indirizzo IP mediante negoziazione PPP/IPCP (Point-to-Point Protocol/IP Control Protocol).

Autenticazione

Consente di immettere le informazioni relative alla password di autenticazione CHAP/PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato selezionare **Nessuno** nel menu a tendina.

Proprietà Ethernet

In questa finestra è possibile configurare le proprietà di un collegamento Ethernet WAN.

Attiva incapsulamento PPPoE

Fare clic su **Attiva incapsulamento PPPoE** se il provider di servizi ne richiede l'utilizzo. Se si seleziona l'opzione PPPoE verrà attivato l'incapsulamento del protocollo Point-to-Point Protocol su Ethernet.

Indirizzo IP

Indirizzo IP statico

Questa opzione è disponibile se si utilizza l'incapsulamento PPPoE o anche senza implementare alcun tipo di incapsulamento. Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi presenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Dinamico (client DHCP)

Questa opzione è disponibile se si utilizza l'incapsulamento PPPoE o anche senza implementare alcun tipo di incapsulamento. Se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere il nome del server DHCP che assegnerà gli indirizzi.

IP senza numero

Questa opzione è disponibile nell'incapsulamento PPPoE. Selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia con l'indirizzo IP che questa interfaccia dovrà condividere.

Easy IP (IP negoziato)

Questa opzione è disponibile nell'incapsulamento PPPoE. Selezionando l'opzione **Easy IP (IP negoziato)**, il router otterrà un indirizzo IP mediante negoziazione PPP/IPCP.

Autenticazione

Consente di immettere le informazioni relative alla password di autenticazione CHAP/PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Ethernet senza incapsulamento

Usare questa finestra per configurare una connessione Ethernet senza incapsulamento.

Indirizzo IP

Selezionare il modo in cui il router otterrà un Indirizzo IP per questo collegamento.

- Indirizzo IP statico: se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi corrispondenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.
- Indirizzo IP dinamico: se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere quindi il nome o l'indirizzo IP del server DHCP.

Nome host

Se nella risposta DHCP contenente l'indirizzo IP dinamico il provider dei servizi indica un nome host per il router, è possibile immettere tale nome in questo campo per scopi informativi.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - ADSL

In questa finestra è possibile specificare o modificare le proprietà di un collegamento PPPoE supportato in una connessione ADSL.

Incapsulamento

Selezionare il tipo di incapsulamento da utilizzare per il collegamento.

- Se si seleziona l'opzione PPPoE verrà attivato l'incapsulamento del protocollo PPPoE (Point-to-Point Protocol over Ethernet).
- PPPoA indica l'incapsulamento Point-to-Point Protocol over ATM.
- L'opzione Routing RFC 1483 (AAL5 SNAP) indica che ogni PVC potrà funzionare con più protocolli.
- L'opzione Routing RFC 1483 (AAL5 MUX) indica che ogni PVC potrà funzionare con un solo tipo di protocollo.

Quando si modifica una connessione, l'incapsulamento visualizzato non è modificabile. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

Per maggiori informazioni su questi tipi di incapsulamento, fare clic su Incapsulamento.

VPI (Virtual Path Identifier)

L'identificatore VPI viene utilizzato nello switching e nel routing ATM per identificare il percorso utilizzato da un certo numero di connessioni. Immettere il valore VPI fornito dal provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

VCI (Virtual Circuit Identifier)

L'identificatore circuito virtuale (VCI) è utilizzato nello switching e routing ATM per identificare una determinata connessione. Immettere il valore VCI fornito dal provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

Indirizzo IP

Selezionare il modo in cui il router otterrà un Indirizzo IP per questo collegamento.

- Indirizzo IP statico: se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi corrispondenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.
- Indirizzo IP dinamico: se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere quindi il nome o l'indirizzo IP del server DHCP.
- Indirizzo IP senza numero: selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia con l'indirizzo IP che questa interfaccia dovrà condividere.
- IP negoziato: questa interfaccia otterrà un indirizzo IP mediante negoziazione PPP/IPCP (IP Control Protocol).

Nome host

Se il provider di servizi ha fornito un nome host per l'opzione 12 di DHCP, immettere tale nome in questo campo.

Modalità operativa

Scegliere una delle seguenti opzioni:

- **auto** - Se si seleziona questa opzione la linea ADSL (Asymmetric Digital Subscriber Line) verrà automaticamente configurata dopo una negoziazione automatica con il dispositivo DSLAM (Digital Subscriber Access Line Multiplexer) situato nella centrale telefonica.
- a**nsi-dmt** - Se si seleziona questa opzione la linea ADSL stabilirà una connessione in modalità ANSI T1.413 Issue 2.
- **itu-dmt** - Se si seleziona questa opzione la linea ADSL stabilirà una connessione in modalità ITU G.992.1.
- **adsl2** - Se si seleziona questa opzione la linea ADSL stabilirà una connessione in modalità ITU G.992.3. Questa modalità è disponibile per i moduli rete HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, e HWIC-1ADSLI ADSL.
- **adsl2+** - Se si seleziona questa opzione la linea ADSL stabilirà una connessione in modalità ITU G.992.4. Questa modalità è disponibile per i moduli rete HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, e HWIC-1ADSLI ADSL.
- **splitterless** - Se si seleziona questa opzione la linea ADSL stabilirà una connessione in modalità G.Lite. Questa modalità è disponibile per i moduli rete ADSL più vecchi come il WIC-1ADSL.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Attiva PPP Multilink

Per utilizzare il protocollo MLP (Multilink Point-to-Point Protocol) con questa interfaccia, selezionare questa casella di controllo. MLP consente di migliorare le prestazioni di una rete con più connessioni WAN utilizzando le funzioni di bilanciamento del carico, frammentazione dei pacchetti, larghezza di banda on demand e altre ancora.

Connessione - ADSL su ISDN

In questa finestra è possibile aggiungere o modificare una connessione ADSL su ISDN.

Incapsulamento

Selezionare il tipo di incapsulamento da utilizzare per il collegamento.

- Se si seleziona l'opzione **PPPoE** verrà attivato l'incapsulamento del protocollo PPPoE (Point-to-Point Protocol over Ethernet).
- L'opzione **RFC 1483 Routing** (**AAL5 SNAP**) indica che ogni PVC potrà funzionare con più protocolli.
- L'opzione **RFC 1483 Routing** (**AAL5 MUX**) indica che ogni PVC potrà funzionare con un solo tipo di protocollo.

Quando si modifica una connessione, l'incapsulamento visualizzato non è modificabile. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

VPI (Virtual Path Identifier)

L'identificatore VPI viene utilizzato nello switching e nel routing ATM per identificare il percorso utilizzato da un certo numero di connessioni. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

VCI (Virtual Circuit Identifier)

L'identificatore circuito virtuale (VCI) è utilizzato nello switching e routing ATM per identificare una determinata connessione. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

Indirizzo IP

Selezionare il modo in cui il router otterrà un Indirizzo IP per questo collegamento.

- Indirizzo IP statico: se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo IP e la subnet mask oppure i bit di rete nei campi corrispondenti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.
- Indirizzo IP dinamico: se si seleziona l'opzione **Dinamico**, il router acquisirà un indirizzo IP da un server DHCP remoto. Immettere quindi il nome o l'indirizzo IP del server DHCP.
- Indirizzo IP senza numero: selezionare l'opzione **IP senza numero** se si desidera che l'interfaccia condivida un indirizzo IP già assegnato a un'altra interfaccia. Quindi scegliere l'interfaccia con l'indirizzo IP che questa interfaccia dovrà condividere.
- IP negoziato: questa interfaccia otterrà un indirizzo IP mediante negoziazione PPP/IPCP (IP Control Protocol).

Modalità operativa

Selezionare la modalità di funzionamento della linea ADSL quando si tenta di stabilire una connessione.

Nota Se la versione di Cisco IOS in esecuzione sul router non supporta tutte e cinque le modalità di funzionamento, verranno visualizzate solo le modalità supportate.

- **annexb** - Modalità Allegato B standard di ITU-T G.992.1.
- **annexb-ur2** - Modalità Allegato B di ITU-T G.992.1.
- **auto** - Consente di configurare la linea ADSL (Asymmetric Digital Subscriber Line) dopo una negoziazione automatica con il dispositivo DSLAM (Digital Subscriber Access Line Multiplexer) situato nella centrale telefonica.
- **etsi** - Modalità ETSI (European Telecommunications Standards Institute).
- **multimode** - Modalità scelta dal firmware per ottimizzare le condizioni operative sui collegamenti (DSL) (Digital Line Subscriber). La modalità finale, a seconda delle impostazioni correnti del dispositivo DSLAM, può essere ETSI o standard Annex- B.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Attiva PPP Multilink

Per utilizzare il protocollo MLP (Multilink Point-to-Point Protocol) con questa interfaccia, selezionare questa casella di controllo. MLP consente di migliorare le prestazioni di una rete con più connessioni WAN utilizzando le funzioni di bilanciamento del carico, frammentazione dei pacchetti, larghezza di banda on demand e altre ancora.

Connessione - G.SHDSL

In questa finestra è possibile creare o modificare una connessione G.SHDSL.

Nota Se la connessione che si sta configurando utilizza un controller DSL, il Tipo di dispositivo e la Modalità operativa non sono visualizzati nella finestra di dialogo.

Incapsulamento

Selezionare il tipo di incapsulamento da utilizzare per il collegamento.

- Se si seleziona l'opzione **PPPoE** verrà attivato l'incapsulamento del protocollo PPPoE (Point-to-Point Protocol over Ethernet).
- **PPPoA** specifica l'incapsulamento Point-to-Point Protocol over ATM.
- L'opzione **RFC 1483 Routing** (**AAL5 SNAP**) indica che ogni PVC potrà funzionare con più protocolli.
- L'opzione **RFC 1483 Routing** (**AAL5 MUX**) indica che ogni PVC potrà funzionare con un solo tipo di protocollo.

Quando si modifica una connessione, l'incapsulamento visualizzato non è modificabile. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

Per maggiori informazioni su questi tipi di incapsulamento, fare clic su Incapsulamento.

VPI (Virtual Path Identifier)

L'identificatore VPI viene utilizzato nello switching e nel routing ATM per identificare il percorso utilizzato da un certo numero di connessioni. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

VCI (Virtual Circuit Identifier)

L'identificatore circuito virtuale (VCI) è utilizzato nello switching e routing ATM per identificare una determinata connessione. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

Indirizzo IP

Selezionare il modo in cui il router otterrà un indirizzo IP per questo collegamento. I campi visualizzati in quest'area possono cambiare in base al tipo di incapsulamento scelto. Per conoscere il metodo corretto che il router deve utilizzare per ottenere gli indirizzi IP, contattare il provider di servizi o l'amministratore di rete.

Indirizzo IP statico

Se si seleziona l'opzione **Indirizzo IP statico**, immettere l'indirizzo utilizzato dall'interfaccia e la subnet mask oppure i bit di rete. Per ottenere queste informazioni, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Indirizzo IP dinamico

Se si sceglie l'Indirizzo IP dinamico, l'interfaccia acquisirà un indirizzo IP da un server DHCP presente in rete. Se tale server utilizza l'opzione 12 di DHCP, questo trasmetterà un nome host e un indirizzo IP da utilizzare sul router. Per determinare il nome host trasmesso, contattare il provider di servizi o l'amministratore di rete.

IP senza numero

Selezionare questa opzione se si desidera che l'interfaccia condivida l'indirizzo IP con un'interfaccia Ethernet presente sul router. Se si seleziona questa opzione, è necessario specificare nell'elenco a discesa l'interfaccia Ethernet di cui si desidera utilizzare l'indirizzo.

Indirizzo IP per connessione remota in sede centrale

Immettere l'Indirizzo IP del sistema gateway utilizzato per questo collegamento. Per ottenere l'indirizzo IP, contattare il provider di servizi o l'amministratore di rete. Per gateway s'intende il sistema al quale il router deve connettersi per accedere a Internet o alla WAN aziendale.

Tipo di dispositivo

Selezionare uno dei seguenti valori:

CPE

Acronimo di Customer Premises Equipment. Se il tipo di incapsulamento è PPPoE, viene automaticamente selezionata l'opzione CPE e il campo viene disattivato.

CO

Acronimo di Central Office (sede centrale).

Modalità operativa

Selezionare uno dei seguenti valori:

Allegato A (indicazione per gli Stati Uniti)

Utilizzare questa opzione per impostare i parametri operativi regionali dell'America del Nord.

Allegato B (indicazione per i Paesi europei)

Utilizzare questa opzione per impostare i parametri operativi regionali europei.

Attiva PPP Multilink

Per utilizzare il protocollo MLP (Multilink Point-to-Point Protocol) con questa interfaccia, selezionare questa casella di controllo. MLP consente di migliorare le prestazioni di una rete con più connessioni WAN utilizzando le funzioni di bilanciamento del carico, frammentazione dei pacchetti, larghezza di banda on demand e altre ancora.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Configura controller DSL

Cisco SDM supporta la configurazione di Cisco WIC-1SHDSL-V2. In questo WIC è presente il supporto per T1, E1 o per una connessione G.SHDSL su un'interfaccia ATM. In Cisco SDM sono supportate solo le connessioni G.SHDSL che utilizzano l'interfaccia ATM. In questa finestra è possibile attivare una connessione G.SHDSL impostando su ATM la modalità del controller del WIC. Inoltre, è possibile creare o modificare le informazioni del controller DSL relative a questa connessione.

Modalità controller

In Cisco SDM per questo controller è supportata solo la modalità ATM, che consente di implementare una connessione G.SHDSL. Questo campo sarà automaticamente impostato su ATM quando si fa clic su OK.

Tipo di dispositivo

Specificare se la connessione riguarda la sede centrale (CO) o il CPE (Customer Premises Equipment).

Modalità operativa

Specificare se per la connessione DSL è necessario utilizzare la segnalazione Annex-A (per le connessioni DSL negli Stati Uniti) o la segnalazione Annex-B (per le connessioni DSL in Europa).

Modalità linea

Specificare se la connessione G.SHDSL è a 2 o a 4 cavi.

Numero linea

Selezionare il numero dell'interfaccia che s'intende utilizzare per la connessione.

Frequenza di linea

Selezionare la frequenza di linea DSL della porta G.SHDSL. Se è stata specificata una connessione a 2 cavi è possibile selezionare l'opzione **auto**. In questo modo l'interfaccia negozierà automaticamente la frequenza di linea fra la porta G.SHDSL e il dispositivo DSLAM. In alternativa, è possibile selezionare la frequenza della linea DSL effettiva. Le frequenze di linea supportate sono 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056 e 2312.

Se invece è stata definita una connessione a 4 cavi, è necessario selezionare una frequenza di linea fissa. Le frequenze di linea supportate in questo caso sono 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480 e 4608.

Nota Se agli estremi opposti dell'uplink DSL sono state configurate frequenze di linea differenti, la frequenza di linea effettiva corrisponde a quella inferiore.

Attiva margine rapporto suono/rumore

Il margine sul rapporto segnale/rumore rappresenta la soglia utilizzata dal modem DSL per determinare se occorre ridurre o aumentare la potenza del segnale in uscita in funzione dell'intensità del rumore presente sulla connessione. Se la frequenza di linea è stata impostata su “auto”, è possibile attivare questa funzione in modo da ottimizzare la qualità della connessione DSL. Si noti che non è consentito utilizzare questa funzione se la frequenza di linea è fissa. Per attivare il margine del rapporto segnale/rumore, selezionare questa casella e impostare i margini del rapporto nei campi Corrente e Snext. Per disattivare questa funzione, deselezionare la casella.

Corrente

Selezionare il margine del rapporto segnale/rumore in decibel (dB) per la connessione corrente. Quanto più basso è il rapporto selezionato, tanto maggiore sarà l'intensità di rumore tollerata nella connessione. Con l'impostazione di un valore in dB basso, il modem DSL consentirà una maggiore intensità di rumore sulla linea, determinando una connessione di qualità potenzialmente inferiore ma con una velocità di trasmissione più elevata. Se invece si imposta un valore elevato, il modem avrà una tolleranza al rumore ridotta, determinando una connessione di qualità più elevata ma con una velocità di trasmissione ridotta.

Snext

Selezionare il margine del rapporto segnale/rumore Snext (Self near end cross talk) in decibel.

Connessioni DSL

In questo campo sono visualizzate tutte le connessioni G.SHDSL correntemente configurate sul controller. Per configurare una nuova connessione G.SHDSL, fare clic su **Aggiungi**. Consente la visualizzazione della pagina Aggiungi connessione G.SHDSL, in cui è possibile configurare una nuova connessione. Per modificare una connessione G.SHDSL, selezionare la connessione in questo campo e fare clic su **Modifica**. Anche in questo caso viene visualizzata la pagina Aggiungi connessione G.SHDSL in cui è possibile modificare la configurazione della connessione. Per eliminare una connessione, selezionare la connessione in questo campo e fare clic su **Elimina**.

Aggiungi connessione G.SHDSL

In questa finestra è possibile creare o modificare una connessione G.SHDSL.

Incapsulamento

Selezionare il tipo di incapsulamento da utilizzare per il collegamento.

- Se si seleziona l'opzione **PPPoE** verrà attivato l'incapsulamento del protocollo PPPoE (Point-to-Point Protocol over Ethernet).
- **PPPoA** specifica l'incapsulamento Point-to-Point Protocol over ATM.
- L'opzione **RFC 1483 Routing** (**AAL5 SNAP**) indica che ogni PVC potrà funzionare con più protocolli.
- L'opzione **RFC 1483 Routing** (**AAL5 MUX**) indica che ogni PVC potrà funzionare con un solo tipo di protocollo.

Quando si modifica una connessione, l'incapsulamento visualizzato non è modificabile. Per modificare il tipo di incapsulamento occorre eliminare prima la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

VPI (Virtual Path Identifier)

L'identificatore VPI viene utilizzato nello switching e nel routing ATM per identificare il percorso utilizzato da un certo numero di connessioni. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare prima la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

VCI (Virtual Circuit Identifier)

L'identificatore VCI viene utilizzato nello switching e nel routing ATM per identificare una particolare connessione all'interno di un percorso potenzialmente condiviso con altre connessioni. Per ottenere questo valore, contattare il provider di servizi.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare questo valore, eliminare prima la connessione e quindi crearla nuovamente utilizzando il valore desiderato.

Indirizzo IP

Selezionare il modo in cui il router otterrà un indirizzo IP per questo collegamento. I campi visualizzati in quest'area possono cambiare in base al tipo di incapsulamento scelto. Per conoscere il metodo corretto che il router deve utilizzare per ottenere gli indirizzi IP, contattare il provider di servizi o l'amministratore di rete.

Indirizzo IP statico

Se si seleziona l'opzione Indirizzo IP statico, immettere l'indirizzo e la subnet mask o i bit di rete da utilizzare per l'interfaccia. Per ottenere queste informazioni, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Indirizzo IP dinamico

Se si seleziona questa opzione, l'interfaccia acquisirà un indirizzo IP da un server DHCP presente in rete. Se tale server utilizza l'opzione 12 di DHCP, questo trasmetterà un nome host e un indirizzo IP da utilizzare per il router. Per ottenere il nome host trasmesso, contattare il provider di servizi o l'amministratore di rete.

IP senza numero

Selezionare questa opzione se si desidera che l'interfaccia condivida l'indirizzo IP con un'interfaccia Ethernet presente sul router. Se si seleziona questa opzione, è necessario specificare l'interfaccia Ethernet nell'elenco a discesa.

Descrizione

Immettere una descrizione di questa connessione, per semplificarne l'individuazione e la gestione.

Attiva PPP Multilink

Per utilizzare il protocollo MLP (Multilink Point-to-Point Protocol) con questa interfaccia, selezionare questa casella di controllo. MLP consente di migliorare le prestazioni di una rete con più connessioni WAN utilizzando le funzioni di bilanciamento del carico, frammentazione dei pacchetti, larghezza di banda on demand e altre ancora.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si desidera aggiornare automaticamente i propri server DNS ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione appare soltanto se supportata dalla versione IOS del server Cisco utilizzato.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo **Metodo DNS dinamico** esattamente come viene visualizzato nell'elenco in Configura > Attività aggiuntive > Metodi DNS dinamici

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e selezionare un metodo esistente. Verrà visualizzata una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Interfaccia seriale, incapsulamento Frame Relay

Riempire questi campi se si desidera configurare un'interfaccia seriale secondaria per l'incapsulamento Frame Relay. Se si sta modificando o creando una connessione nella finestra Modifica interfacce e connessioni, non sarà consentita la modifica dell'incapsulamento visualizzato. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

Incapsulamento

Frame Relay chosen.

Indirizzo IP

Selezionare **Indirizzo IP statico** o **IP senza numero**.

Indirizzo IP

Se è stata selezionata l'opzione **Indirizzo IP statico**, immettere l'Indirizzo IP dell'interfaccia. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Se è stata selezionata l'opzione **Indirizzo IP statico**, immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di subnet. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

Per specificare la parte di indirizzo IP in cui è indicato l'indirizzo di rete è anche possibile immettere i bit di rete.

IP senza numero

Se si è scelto IP unnumbered l'interfaccia condividerà un indirizzo IP già assegnato a un'altra interfaccia. Scegliere l'interfaccia il cui indirizzo IP verrà condiviso dall'interfaccia che si sta configurando.

DLCI

Immettere in questo campo l'identificatore DLCI (Data Link Connection Identifier). Questo numero deve essere univoco tra tutti i valori DLCI utilizzati in questa interfaccia. Il valore DLCI fornisce un identificatore di Frame Relay univoco per la connessione.

Se si sta modificando una connessione esistente, questo campo risulterà essere disattivato. Per modificare l'identificatore DLCI, eliminare la connessione e quindi crearla nuovamente.

Tipo LMI

Contattare il proprio fornitore di servizi per sapere quale tipo di LMI (Local Management Interface) tra quelli di seguito elencati deve essere utilizzato. Il tipo di LMI specifica il protocollo utilizzato per monitorare la connessione:

ANSI

Allegato D definito dall'American National Standards Institute (ANSI) standard T1.617.

Cisco

Tipo di LMI definito da Cisco insieme ad altre tre società.

ITU-T Q.933

ITU-T Q.933 Annex A

Rilevamento automatico

Impostazione predefinita. Questa impostazione consente al router di individuare quale tipo di LMI è utilizzato. Se la funzione di rilevamento automatico ha esito negativo, il router utilizzerà il tipo di LMI Cisco.

Utilizzare l'incapsulamento Frame Relay IETF

Selezionare questa casella di controllo per utilizzare l'incapsulamento IETF (Internet Engineering Task Force). Questa opzione è utilizzata con i router non prodotti da Cisco. Selezionare questa casella se s'intende connettere l'interfaccia a un router non Cisco.

Impostazioni clock

Nella maggior parte dei casi è preferibile non modificare le impostazioni predefinite del clock. Se le esigenze dell'utente sono diverse da quelle predefinite, selezionare questa opzione e regolare le impostazioni del clock nella finestra visualizzata.

Il pulsante Impostazioni clock è disponibile solo quando si configura una connessione seriale T1 o E1.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Interfaccia seriale, incapsulamento PPP

Riempire questi campi se s'intende configurare un'interfaccia seriale per l'incapsulamento PPP (Point-to-Point Protocol). Se si sta modificando o creando una connessione nella finestra Modifica interfacce e connessioni, non sarà consentita la modifica dell'incapsulamento visualizzato. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

Incapsulamento

Il PPP scelto.

Indirizzo IP

Selezionare **Indirizzo IP statico**, **IP senza numero** o **IP negoziato**. Se si seleziona l'opzione **IP senza numero**, scegliere l'interfaccia con l'indirizzo IP da condividere. Se si seleziona **IP negoziato**, il router ottiene un indirizzo IP dal provider di servizi internet per questa interfaccia. Se si seleziona l'opzione **Specificare un indirizzo IP**, riempire i campi seguenti.

Indirizzo IP

Immettere l'Indirizzo IP da utilizzare per l'interfaccia secondaria point-to-point. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di rete. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

Per specificare la parte di indirizzo IP in cui è indicato l'indirizzo di rete è anche possibile immettere i bit di rete.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

Impostazioni clock

Nella maggior parte dei casi è preferibile non modificare le impostazioni predefinite del clock. Se le esigenze dell'utente sono diverse da quelle predefinite, selezionare questa opzione e regolare le impostazioni del clock nella finestra visualizzata.

Il pulsante Impostazioni clock è disponibile solo quando si configura una connessione seriale T1 o E1.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Interfaccia seriale, incapsulamento HDLC

Riempire questi campi se si desidera configurare un'interfaccia seriale per l'incapsulamento HDLC. Se si sta modificando o creando una connessione nella finestra Modifica interfacce e connessioni, non sarà consentita la modifica dell'incapsulamento visualizzato. Per modificare il tipo di incapsulamento è necessario eliminare la connessione e quindi crearla nuovamente utilizzando il tipo di incapsulamento desiderato.

Incapsulamento

HDLC selezionato.

Indirizzo IP

Selezionare **Indirizzo IP statico** o **IP senza numero**. Se si seleziona l'opzione **IP senza numero**, scegliere l'interfaccia con l'indirizzo IP da condividere. Se si seleziona l'opzione **Indirizzo IP statico**, riempire i campi seguenti.

Indirizzo IP

Immettere l'Indirizzo IP dell'interfaccia. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di rete. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

In alternativa, selezionare il numero di bit che specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete.

Impostazioni clock

Nella maggior parte dei casi è preferibile non modificare le impostazioni predefinite del clock. Se le esigenze dell'utente sono diverse da quelle predefinite, selezionare questa opzione e regolare le impostazioni del clock nella finestra visualizzata.

Il pulsante Impostazioni clock è disponibile solo quando si configura una connessione seriale T1 o E1.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Aggiungi/Modifica tunnel GRE

In questa finestra è possibile aggiungere un tunnel GRE a un'interfaccia o modificare un'interfaccia esistente. Se il tunnel GRE non è stato configurato con la modalità **gre ip**, questa finestra non verrà visualizzata.

Numero tunnel

Immettere il numero del tunnel.

Origine tunnel

Selezionare l'interfaccia che si desidera utilizzare per il tunnel. Questa interfaccia deve essere raggiungibile dall'altra estremità del tunnel, pertanto deve disporre di un Indirizzo IP pubblico e instradabile.

Destinazione tunnel

Si tratta dell'interfaccia sul router all'altra estremità del tunnel. Selezionare se si desidera specificare un indirizzo IP o un nome host e quindi immettere le informazioni richieste. Nel primo caso, immettere l'indirizzo IP e la subnet mask in formato decimale separato da punti (ad esempio 192.168.20.1 e 255.255.255.0).

Per evitare che il tunnel venga creato in modo non corretto, assicurarsi che l'indirizzo o il nome host immesso sia raggiungibile mediante il comando **ping**.

Tunnel IP Address

Immettere l'indirizzo IP del tunnel in formato decimale separato da punti (ad esempio 192.168.20.1). Per ulteriori informazioni, consultare la sezione Indirizzi IP e subnet mask.

Casella di controllo GRE Keepalive

Selezionare questa casella se si desidera che il router trasmetta dei GRE Keepalive. Specificare l'intervallo di tempo (in secondi) in cui effettuare l'invio di keepalive e il tempo di attesa (in secondi) fra i tentativi di trasmissione.

MTU

Immettere le dimensioni massime dell'unità di trasmissione (MTU). Se si desidera ridurre tali dimensioni in modo da evitare la frammentazione dei pacchetti, fare clic su **Regolare MTU per evitare la frammentazione**.

Larghezza di banda

Fare clic per specificare la larghezza di banda del tunnel in kilobyte.

Connessione - ISDN BRI

Riempire questi campi se si intende configurare una connessione ISDN BRI. Poiché in Cisco SDM per le connessioni ISDN BRI è supportato solo l'incapsulamento PPP, non è consentito modificare l'incapsulamento visualizzato.

Incapsulamento

Il PPP scelto.

Tipo di switch ISDN

Selezionare un tipo di switch ISDN. Contattare il provider del servizio ISDN per conoscere il tipo di switch della propria connessione.

Cisco SDM supporta i tipi di switch BRI elencati di seguito.

- Per l'America del Nord
  - basic-5ess - Switch Lucent (AT&T) 5ESS a frequenza base
  - basic-dms100 - Switch Northern Telecom DMS-100 a frequenza base
  - basic-ni - Switch ISDN nazionale
- Per Australia, Europa e Regno Unito
  - basic-1tr6 - Switch ISDN 1TR6 (Germania)
  - basic-net3 - Switch NET3 ISDN BRI per i tipi di switch NET3 (Norvegia, Australia e Nuova Zelanda); switch conformi alla specifica ETSI per il sistema di indicazione Euro-ISDN E-DSS1
  - vn3 - Switch ISDN BRI (Francia)
- Per il Giappone
  - ntt - Switch NTT ISDN
- Per i sistemi Voce/PBX
  - basic-qsig - Switch PINX (PBX) con indicazione QSIG per Q.931 ()

SPID

Selezionare questa opzione per immettere informazioni sull'identificativo SPID (Service Provider ID).

Alcuni provider di servizi utilizzano gli identificativi SPID per definire i servizi a cui un determinato dispositivo ISDN è registrato. Il provider assegna al dispositivo ISDN uno o più numeri SPID quando ci si registra per la prima volta al servizio. Se il proprio provider di servizi utilizza gli SPID, il dispositivo ISDN utilizzato non sarà in grado di effettuare o ricevere chiamate finché non trasmette al provider di servizi uno SPID valido quando accede allo switch per inizializzare la connessione.

Solo gli switch di tipo DMS-100 e NI richiedono l'utilizzo di SPID. Benché gli switch Lucent (AT&T) 5ESS possano supportare gli SPID, è preferibile configurare i servizi ISDN in modo che non richiedano l'uso di tali identificativi. Inoltre, gli SPID sono rilevanti solo presso l'interfaccia di accesso ISDN locale. I router remoti, infatti, non ricevono mai gli SPID.

Uno SPID è in genere costituito da un numero di telefono a 7 cifre con alcuni numeri opzionali. Comunque, i provider di servizi possono utilizzare schemi di numerazione differenti. Per lo switch di tipo DMS-100 sono assegnati due SPID, uno per ciascun canale B.

Numero di telefono remoto

Immettere il numero di telefono dell'estremità di destinazione della connessione ISDN.

Opzioni

Fare clic su questo pulsante se si desidera associare liste ACL a un elenco di dialer per identificare il traffico interessante, immettere le impostazioni del timer o attivare/disattivare il protocollo PPP Multilink.

Se si seleziona l'opzione relativa all'identificazione del traffico interessante, il router stabilirà delle connessioni attive solo quando rileva un traffico interessante.

Se invece si seleziona l'opzione relativa alle impostazioni del timer, il router terminerà automaticamente le chiamate che risultino essere inattive per un determinato intervallo di tempo.

Infine, è possibile configurare il protocollo PPP Multilink per applicare il bilanciamento del carico fra i canali ISDN B.

Indirizzo IP

Selezionare **Indirizzo IP statico**, **IP senza numero** o **IP negoziato**. Se si seleziona l'opzione **Specificare un indirizzo IP**, riempire i campi seguenti.

Indirizzo IP

Immettere l'Indirizzo IP da utilizzare per l'interfaccia secondaria point-to-point. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di rete. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

Per specificare la parte di indirizzo IP in cui è indicato l'indirizzo di rete è anche possibile immettere i bit di rete.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - Modem analogico

Riempire questi campi se si intende configurare una connessione con modem analogico. Poiché in Cisco SDM per le connessioni con modem analogico è supportato solo l'incapsulamento PPP, non è consentito modificare l'incapsulamento visualizzato.

Incapsulamento

Il PPP scelto.

Numero di telefono remoto

Immettere il numero di telefono dell'estremità di destinazione della connessione con modem analogico.

Opzioni

Selezionare questa opzione se si desidera associare liste ACL a un elenco di dialer per identificare il traffico interessante o immettere le impostazioni del timer.

Se si seleziona l'opzione relativa all'identificazione del traffico interessante, il router stabilirà delle connessioni attive solo quando rileva un traffico interessante.

Se invece si seleziona l'opzione relativa alle impostazioni del timer, il router terminerà automaticamente le chiamate che risultino essere inattive per un determinato intervallo di tempo.

Disconnetti linea

Consente di disconnettersi dalla linea. Si consiglia di effettuare questa operazione dopo aver creato una connessione asincrona. In questo modo, infatti, la connessione viene automaticamente attivata dal traffico interessante.

Indirizzo IP

Selezionare **Indirizzo IP statico**, **IP senza numero** o **IP negoziato**. Se si seleziona l'opzione **Specificare un indirizzo IP**, riempire i campi seguenti.

Indirizzo IP

Immettere l'Indirizzo IP da utilizzare per l'interfaccia secondaria point-to-point. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di rete. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

Per specificare la parte di indirizzo IP in cui è indicato l'indirizzo di rete è anche possibile immettere i bit di rete.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Connessione - (AUX Backup)

Riempire questi campi se si desidera configurare una connessione asincrona di tipo dialup che utilizza la porta della console in modo che quest'ultima funzioni anche da porta AUX su un Cisco 831 o 837. Dopo aver immesso le informazioni in questa finestra, fare clic su **Dettagli di backup** e immettere le informazioni di backup di connessione necessarie per questo tipo di connessione. Si noti che poiché in Cisco SDM per le connessioni con modem analogico è supportato solo l'incapsulamento PPP, non è consentito modificare l'incapsulamento visualizzato.

L'opzione di configurazione della porta aux come connessione di tipo dialup verrà visualizzata solo per i router Cisco 831 e 837. Questa opzione non sarà disponibile per questi tipi di router se si verifica una delle seguenti condizioni:

- Il router non sta utilizzando una versione Cisco IOS Zutswang.
- Non è configurata un'interfaccia WAN primaria.
- L'interfaccia asincrona è già configurata.
- L'interfaccia asincrona non è configurabile con Cisco SDM a causa della presenza di comandi Cisco IOS non supportati nella configurazione esistente.

Incapsulamento

Il PPP scelto.

Numero di telefono remoto

Immettere il numero di telefono dell'estremità di destinazione della connessione con modem analogico.

Opzioni

Selezionare questa opzione se si desidera associare liste ACL a un elenco di dialer per identificare il traffico interessante o immettere le impostazioni del timer.

Se si seleziona l'opzione relativa all'identificazione del traffico interessante, il router stabilirà delle connessioni attive solo quando rileva un traffico interessante.

Se invece si seleziona l'opzione relativa alle impostazioni del timer, il router terminerà automaticamente le chiamate che risultino essere inattive per un determinato intervallo di tempo.

Disconnetti linea

Consente di disconnettersi dalla linea. Si consiglia di effettuare questa operazione dopo aver creato una connessione asincrona. In questo modo, infatti, la connessione viene automaticamente attivata dal traffico interessante.

Indirizzo IP

Selezionare **Indirizzo IP statico**, **IP senza numero** o **IP negoziato**. Se si seleziona l'opzione **Specificare un indirizzo IP**, riempire i campi seguenti.

Indirizzo IP

Immettere l'Indirizzo IP da utilizzare per l'interfaccia secondaria point-to-point. Per ottenere questo indirizzo, rivolgersi all'amministratore di rete o al provider di servizi. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask. La subnet mask specifica la parte di indirizzo IP in cui è indicato l'indirizzo di rete. Questo valore è sincronizzato con i bit di rete. Per ottenere il valore della subnet mask o dei bit di rete, contattare l'amministratore di rete o il provider di servizi Internet.

Bit di subnet

Per specificare la parte di indirizzo IP in cui è indicato l'indirizzo di rete è anche possibile immettere i bit di rete.

Dettagli di backup

Consente di visualizzare la finestra Configurazione di backup, da cui è possibile configurare le informazioni di backup della connessione. Tali informazioni sono obbligatorie per questo tipo di connessione e se si tenta di configurare le impostazioni di connessione senza prima immettere le informazioni riguardanti la configurazione della connessione di backup, verrà visualizzato un messaggio di errore.

Autenticazione

Consente di immettere le informazioni relative all'autenticazione CHAP o PAP.

DNS dinamico

Attivare il DNS dinamico se si vogliono aggiornare i propri server DNS automaticamente ogni volta che l'indirizzo IP dell'interfaccia WAN cambia.

Nota Questa funzione viene visualizzata solo se supportata dalla versione Cisco IOS sul router.

Per scegliere il metodo di DNS dinamico da utilizzare fare una delle seguenti azioni:

- Immettere il nome di un metodo DNS dinamico esistente.

  Immettere il nome nel campo Metodo DNS dinamico esattamente come viene visualizzato nell'elenco in **Configura > Attività aggiuntive > Metodi DNS dinamici**.

- Scegliere un metodo DNS dinamico esistente nell'elenco.

  Fare clic sul menu a tendina e scegliere un metodo esistente. Si apre una finestra con l'elenco dei metodi DNS dinamici esistenti. Questa opzione di menu è disponibile soltanto se ci sono metodi DNS dinamici esistenti.

- Creare un nuovo metodo per il DNS dinamico.

  Fare clic sul menu a tendina e scegliere di creare un nuovo metodo DNS dinamico.

Per eliminare dall'interfaccia un metodo DNS dinamico associato scegliere **Nessuno** dal menu a tendina.

Autenticazione

Questa pagina viene visualizzata se si è attivato il protocollo PPP per una connessione seriale o l'incapsulamento PPPoE per una connessione ATM o Ethernet, oppure se si sta configurando una connessione ISDN BRI o con modem analogico. Il provider di servizi o l'amministratore di rete utilizzano una password del protocollo Challenge Handshake Authentication Protocol (CHAP) o del protocollo Password Authentication Protocol (PAP) per proteggere la connessione tra i dispositivi. Questa password protegge l'accesso in ingresso e in uscita.

CHAP/PAP

Selezionare la casella associata al tipo di autenticazione utilizzata dal provider di servizi. Se non si possiede questa informazione, è possibile selezionare entrambe le caselle. Il router tenterà entrambi i tipi di autenticazione e uno dei tentativi avrà esito positivo.

L'autenticazione CHAP è più sicura dell'autenticazione PAP.

Nome di accesso

Il nome di accesso è fornito dal provider di servizi ed è utilizzato come nome utente per l'autenticazione CHAP o PAP.

Password

Immettere la password esattamente nel modo in cui è stata fornita dal provider di servizi. Per le password la distinzione tra maiuscole e minuscole è significativa. Ad esempio, la password *test* è diversa dalla password *TEST*.

Reimmettere password

Immettere la stessa password digitata nella casella precedente.

Dettagli SPID

Alcuni provider di servizi utilizzano i numeri SPID (Service Provider ID) per definire i servizi a cui un determinato dispositivo ISDN è registrato. Il provider assegna al dispositivo ISDN uno o più numeri SPID quando ci si registra per la prima volta al servizio. Se il proprio provider di servizi utilizza gli SPID, il dispositivo ISDN utilizzato non sarà in grado di effettuare o ricevere chiamate finché non trasmette al provider di servizi uno SPID valido quando accede allo switch per inizializzare la connessione.

Solo gli switch di tipo DMS-100 e NI richiedono l'utilizzo di SPID. Gli switch AT&T 5ESS possono supportare gli SPID ma è preferibile configurare i servizi ISDN in modo che non richiedano l'uso di tali identificativi. Inoltre, gli SPID sono rilevanti solo presso l'interfaccia di accesso ISDN locale. I router remoti, infatti, non ricevono mai gli SPID.

Uno SPID è in genere costituito da un numero di telefono a 7 cifre con alcuni numeri opzionali. Comunque, i provider di servizi possono utilizzare schemi di numerazione differenti. Per lo switch di tipo DMS-100 sono assegnati due SPID, uno per ciascun canale B.

SPID1

Immettere lo SPID del primo canale B su connessione BRI fornito dall'ISP.

SPID2

Immettere lo SPID del secondo canale B su connessione BRI fornito dall'ISP.

Opzioni dialer

Le interfacce ISDN BRI e quelle con modem analogico possono essere configurate per il DDR (dial-on-demand routing) che attiva la chiamata telefonica soltanto in circostanze determinate, risparmiando sul tempo e quindi sui costi di connessione. Questa finestra consente di configurare le opzioni che specificano quando le connessioni ISDN BRI o con modem analogico devono essere iniziate e terminate.

Associazione elenco dialer

Mediante gli elenchi di dialer è possibile associare a una lista ACL una connessione ISDN BRI o con modem analogico al fine di identificare il *traffico interessante*. Se si attiva l'opzione relativa all'identificazione del traffico interessante, l'interfaccia stabilirà una connessione solo quando il router rileva un traffico dati che corrisponde a un elemento dell'ACL.

Consenti tutto il traffico IP

Selezionare questa opzione se si desidera che l'interfaccia stabilisca una connessione ogni volta che attraverso l'interfaccia viene trasmesso un qualsiasi tipo di traffico IP.

Filtra il traffico in base all'ACL selezionato

Selezionare questa opzione per associare all'interfaccia una ACL. Questa lista deve essere stata creata mediante l'interfaccia Regole. Solo il tipo di traffico corrispondente a quello identificato nell'ACL comporterà un tentativo di connessione da parte dell'interfaccia.

È possibile immettere il numero ACL che si desidera associare all'interfaccia dialer per identificare il traffico interessante, oppure fare clic sul pulsante a fianco del campo per sfogliare l'elenco di ACL o creare una nuova ACL e quindi selezionarla.

Impostazioni timer

Mediante queste impostazioni è possibile configurare un limite massimo di tempo entro il quale una connessione priva di traffico resterà attiva. In questo modo le connessioni termineranno automaticamente, consentendo di ottenere riduzioni sui tempi e sui costi di connessione.

Valore di timeout idle

Immettere il numero di secondi che devono trascorrere prima che una connessione inattiva (ovvero priva di traffico) venga automaticamente terminata.

Valore di timeout idle veloce

Il Timeout idle veloce viene utilizzato quando la connessione è attiva mentre una connessione concorrente è in attesa di essere effettuata. Il tempo di timeout veloce determina il numero di secondi senza traffico interessato che deve trascorrere prima che la connessione attiva venga terminata per potere effettuare la connessione concorrente in attesa.

Ciò si verifica quando su un'interfaccia avente una connessione attiva all'indirizzo IP di un determinato hop successivo si riceve un'altra connessione contenente dati interessanti diretti verso un hop successivo diverso. Poiché la connessione dialer è point-to-point, i pacchetti concorrenti non possono essere trasmessi finché la connessione corrente è attiva. Questo parametro indica l'intervallo di tempo di inattività della prima connessione che deve trascorrere prima che questa venga terminata per consentire al sistema di effettuare la connessione concorrente.

Attiva PPP Multilink

Questo protocollo consente di effettuare il bilanciamento del carico su più canali ISDN BRI B e interfacce asincrone. Abilitando il protocollo PPP Multilink quando si stabilisce una connessione ISDN si utilizza inizialmente un solo canale B. Se il carico del traffico sulla connessione supera la soglia specificata (immessa come percentuale della larghezza di banda complessiva), viene effettuata una connessione sul secondo canale B e il traffico viene instradato su entrambe le connessioni. Questa soluzione consente di diminuire i tempi e costi di connessione quando il traffico è ridotto e di utilizzare l'intera larghezza di banda ISDN BRI, se necessario.

Selezionare o deselezionare questa casella di controllo se si desidera attivare o disattivare Altrimenti deselezionare.

Soglia di carico

Utilizzare questo campo per configurare la percentuale di larghezza di banda occupata su un solo canale ISDN BRI superata la quale viene automaticamente effettuata un'altra connessione su un canale dello stesso tipo per bilanciare il carico del traffico. Immettere un numero compreso fra 1 e 255, dove 255 corrisponde al 100% della larghezza di banda della prima connessione.

Direzione dati

In Cisco SDM il protocollo PPP Multilink è supportato solo per il traffico di rete in uscita.

Configurazione di backup

Le interfacce ISDN BRI e per modem analogico possono essere configurate perché fungano da interfacce di backup per altre interfacce primarie. In tal caso verrà effettuata una connessione ISDN o con modem analogico solo se l'interfaccia primaria non è attiva. Se si verifica un guasto nell'interfaccia primaria e nella connessione, l'interfaccia ISDN BRI o con modem analogico tenterà immediatamente di stabilire una nuova connessione in modo da evitare l'interruzione dei servizi di rete.

Attiva backup

Selezionare questa opzione se si desidera che l'interfaccia ISDN BRI o con modem analogico funzioni come connessione di backup. Deselezionare questa casella di controllo se non si desidera che l'interfaccia ISDN BRI o l'interfaccia del modem analogico sia l'interfaccia di backup.

Interfaccia primaria

Selezionare l'interfaccia sul router che s'intende utilizzare per la connessione primaria. La connessione ISDN BRI o con modem analogico verrà effettuata solo se per qualche motivo si verifica un guasto nell'interfaccia selezionata.

Dettagli di traccia

In questa sezione è possibile individuare un host specifico verso il quale deve essere mantenuta la connettività. Il router tiene traccia della connettività verso tale host e in caso di perdita di connessione da parte dell'interfaccia primaria, verrà automaticamente effettuata una connessione di backup utilizzando l'interfaccia ISDN BRI o con modem analogico.

Nome host o indirizzo IP da rilevare

Immettere il nome o l'indirizzo IP dell'host di destinazione verso cui si desidera rilevare la connettività. Specificare una destinazione raramente contattata come sito su cui verificare la connettività.

Numero oggetto traccia

Si tratta di un campo di sola lettura in cui è visualizzato un numero di oggetto interno generato e utilizzato in Cisco SDM per rilevare la connettività verso l'host remoto.

Inoltro a hop successivi

Questi campi sono opzionali. È possibile immettere l'indirizzo IP a cui l'interfaccia primaria e le interfacce di backup si connetteranno quando sono attive. Questo indirizzo è noto come indirizzo IP per l'hop successivo. Se non si immette alcun indirizzo IP di questo tipo, Cisco SDM provvederà automaticamente a configurare delle route statiche utilizzando il nome dell'interfaccia. Si noti che in caso di backup a una connessione di tipo WAN Multipoint, come ad esempio una connessione Ethernet, è necessario immettere gli indirizzi IP per l'hop successivo affinché il routing venga eseguito correttamente. Se invece il backup riguarda una connessione point-to-point, questa informazione non é necessaria.

Indirizzo IP per hop successivo primario

Immettere l'indirizzo IP per hop successivo dell'interfaccia primaria.

Indirizzo IP per hop successivo di backup

Immettere l'indirizzo IP per hop successivo dell'interfaccia di backup ISDN BRI o con modem analogico.

CAPITOLO 6

Creazione firewall

Un firewall è un insieme di regole finalizzato alla protezione delle risorse della LAN mediante il filtraggio dei pacchetti ricevuti dal router. I pacchetti che non soddisfano i criteri specificati nell'insieme di regole vengono scartati. I pacchetti che soddisfano tali criteri, invece, possono attraversare l'interfaccia a cui è applicato l'insieme di regole. Questa procedura guidata consente di creare un firewall per la LAN attraverso i prompt visualizzati in una sequenza di schermate.

In questa finestra, selezionare il tipo di firewall che si desidera creare.

Nota

- Per configurare un firewall sul router mediante Cisco Router and Security Device Manager (Cisco SDM), tale router deve disporre di un'immagine Cisco IOS che supporti il set di funzioni Firewall.
- Prima di poter configurare un firewall, è necessario che le configurazioni LAN e WAN siano complete.

Firewall di base

Fare clic su questo pulsante se si desidera utilizzare Cisco SDM per creare un firewall utilizzando le regole predefinite. Nello scenario del caso di utilizzo viene mostrata una tipica configurazione di rete in cui si utilizza questo tipo di firewall.

Firewall avanzato

Fare clic su questo pulsante se si desidera effettuare mediante Cisco SDM la procedura guidata di configurazione del firewall. Tale procedura consente di creare una rete DMZ e di specificare una Inspection Rule. Nello scenario del caso di utilizzo visualizzato quando si seleziona questa opzione viene mostrata una tipica configurazione di un firewall per Internet.

Tabella riassuntiva funzioni

Funzione	Procedura
Creazione di un firewall mediante Cisco SDM. Questa opzione può essere utile se non si desidera configurare una rete DMZ o se è presente un'unica interfaccia esterna.	Fare clic su **Firewall di base**. Quindi fare clic su **Avvia attività selezionata**. Cisco SDM richiede di identificare le interfacce presenti sul router, quindi utilizza le regole di accesso e le Inspection Rule predefinite di Cisco SDM.
Creazione di un firewall avanzato mediante la procedura guidata di Cisco SDM. Questa opzione può essere utile se il router presenta più interfacce interne ed esterne e si desidera configurare una DMZ.	Selezionare **Firewall avanzato**. Quindi fare clic su **Avvia attività selezionata**. Cisco SDM visualizza l'Inspection Rule predefinita e consente di utilizzarla nel firewall. In alternativa, è possibile creare un'Inspection Rule personalizzata. Infine, Cisco SDM per il firewall utilizzerà una regola di accesso predefinita.

Funzione	Procedura
Ulteriori informazioni sulle attività non contemplate nella procedura guidata.	Selezionare un argomento dall'elenco seguente: • Come visualizzare l'attività del firewall? • Come configurare un firewall in un'interfaccia non supportata? • Come configurare un firewall dopo aver configurato una connessione VPN? • Come consentire il traffico specifico mediante un'interfaccia DMZ? • Come modificare un firewall esistente per consentire il traffico da una nuova rete o un nuovo host? • Come configurare il protocollo NAT in un'interfaccia non supportata? • Come configurare un pass-through NAT per un firewall? • Come consentire il passaggio del traffico verso il concentratore Easy VPN attraverso il firewall? • Come associare una regola a un'interfaccia? • Come annullare l'associazione di una regola di accesso a un'interfaccia? • Come eliminare una regola associata a un'interfaccia? • Come creare una regola di accesso per un elenco Java? • Come visualizzare i comandi IOS inviati al router? • Come consentire il traffico specifico verso la rete se non è disponibile una rete DMZ?

Procedura di configurazione Firewall di base

Questa opzione consente di proteggere la LAN con un firewall predefinito configurato automaticamente mediante Cisco SDM. A tale fine nella schermata successiva di Cisco SDM è necessario specificare le interfacce interne ed esterne. Fare clic su **Avanti** per iniziare la configurazione.

Configurazione dell'interfaccia Firewall di base

Identificare le interfacce presenti sul router in modo che il firewall venga applicato all'interfaccia corretta.

Interfacce esterne (untrusted)

Selezionare l'interfaccia del router connessa a Internet o alla WAN aziendale.

Nota Non impostare come interfaccia esterna (untrusted) l'interfaccia utilizzata per connettersi a Cisco SDM, altrimenti tale connessione verrà interrotta in Cisco SDM. Poiché dopo aver concluso la procedura guidata l'interfaccia esterna (untrusted) sarà protetta da un firewall, non sarà più possibile utilizzarla per avviare Cisco SDM.

Casella di controllo Consenti l'accesso protetto di Cisco SDM dalle interfacce esterne

Attivare questa casella se si desidera che gli utenti al di fuori del firewall possano accedere alla configurazione del router utilizzando Cisco SDM. La configurazione guidata visualizzerà una schermata che consente di specificare un indirizzo IP per l'host o per la rete che deve gestire il router dall'esterno. Il firewall verrà modificato in modo da consentire l'accesso all'indirizzo specificato. Se si specifica un indirizzo di rete, tutti gli host di tale rete saranno ammessi dal firewall.

Interfacce interne (trusted)

Selezionare le interfacce fisiche e logiche connesse alla LAN. È possibile selezionare più interfacce.

Configurazione del Firewall per l'Accesso remoto

La configurazione del un firewall può bloccare l'accesso al router da parte degli amministratori. È possibile specificare le interfacce del router da utilizzare per l'accesso di gestione remota e gli host da cui gli amministratori possono accedere a Cisco SDM per gestire il router. Il firewall verrà modificato in modo da consentire l'accesso remoto all'host specificato o alla rete specificata.

Selezionare l'interfaccia esterna

Se si sta usando la configurazione guidata avanzata del firewall, selezionare l'interfaccia mediante la quale gli utenti devono avviare Cisco SDM. Questo campo non è presente nella Configurazione guidata di base del Firewall.

Host/rete di origine

Se si desidera consentire l'accesso attraverso il firewall ad un solo host, selezionare **Indirizzo Host** e immettere l'indirizzo IP di un host. Scegliere **Indirizzo di rete** e immettere l'indirizzo di una rete e una subnet mask per consentire agli host della rete l'accesso attraverso il firewall. L'host o la rete deve essere accessibile dall'interfaccia specificata. Scegliere **Any** per consentire a qualsiasi host connesso alle interfacce specificate un accesso protetto alla rete.

Procedura di configurazione Firewall avanzata

Tale procedura guidata consente di creare un firewall per Internet mediante Cisco SDM fornendo informazioni sulle interfacce presenti sul router, specificando se si desidera configurare una rete DMZ e indicando le regole da utilizzare per il firewall.

Fare clic su **Avanti** per iniziare la configurazione.

Configurazione avanzata dell'interfaccia Firewall

Identificare le interfacce interne ed esterne del router e l'interfaccia di connessione con la rete DMZ.

Selezionare **esterna** o **interna** per indicare il tipo di interfaccia (esterna o interna). Le interfacce esterne sono connesse alla WAN aziendale o a Internet. Le interfacce interne, invece, sono connesse alla LAN.

Casella di controllo Consenti l'accesso protetto di Cisco SDM dalle interfacce esterne

Attivare questa casella se si desidera che gli utenti al di fuori del firewall possano accedere alla configurazione del router utilizzando Cisco SDM. La configurazione guidata visualizzerà una schermata che consente di specificare un indirizzo IP per l'host o per la rete che deve gestire il router dall'esterno. Il firewall verrà modificato in modo da consentire l'accesso all'indirizzo specificato. Se si specifica un indirizzo di rete, tutti gli host di tale rete saranno ammessi dal firewall.

Interfaccia DMZ

Selezionare l'interfaccia di router connessa a una rete DMZ, se presente. Una rete DMZ è un'area cuscinetto utilizzata per isolare il traffico proveniente da una rete untrusted. Se si dispone di una rete DMZ, selezionare l'interfaccia a esso collegata.

Configurazione avanzata del servizio DMZ per il firewall

In questa finestra è possibile visualizzare le voci di regola che consentono di specificare quali servizi della rete DMZ si desidera rendere disponibili attraverso le interfacce esterne del router. Il traffico dati relativo ai tipi di servizio specificati verrà fatto passare nella rete DMZ attraverso le interfacce esterne.

Configurazione servizio DMZ

In quest'area sono visualizzate le voci relative ai servizi DMZ configurati sul router.

Indirizzo IP iniziale

Si tratta del primo indirizzo IP dell'intervallo contenente gli indirizzi degli host della rete DMZ.

Indirizzo IP finale

Si tratta dell'ultimo indirizzo IP dell'intervallo contenente gli indirizzi degli host della rete DMZ. Se in questa colonna non è elencato alcun valore, si presume che la rete DMZ contenga un unico host, avente l'indirizzo IP specificato nella colonna Indirizzo IP iniziale. Nell'intervallo è possibile specificare un massimo di 254 host.

Tipo di servizio

Tale voce specifica il tipo di servizio, TCP (Transmission Control Protocol) o UDP (User Datagram Protocol).

Servizio

Tale voce specifica il nome del servizio, come ad esempio Telnet o FTP, o un numero di protocollo.

Per configurare una voce di servizio DMZ

Fare clic su **Aggiungi** e quindi creare la voce nella finestra Configurazione servizio DMZ.

Per modificare una voce di servizio DMZ

Selezionare la voce di servizio e fare clic su **Modifica**. Quindi, modificare la voce nella finestra Configurazione servizio DMZ.

Configurazione servizio DMZ

In questa finestra è possibile creare o modificare una voce di servizio DMZ.

Indirizzo IP host

Immettere l'intervallo contenente gli indirizzi degli host della rete DMZ a cui tale voce si riferisce. Il firewall consentirà al traffico dati relativo al servizio TCP o UDP specificato di raggiungere gli host indicati nell'intervallo.

Indirizzo IP iniziale

Immettere il primo indirizzo IP dell'intervallo (ad esempio, 172.20.1.1). Se il protocollo NAT (Network Address Translation) è attivo, è necessario immettere l'indirizzo tradotto secondo tale protocollo, detto *indirizzo globale interno*.

Indirizzo IP finale

Immettere l'ultimo indirizzo IP dell'intervallo (ad esempio, 172.20.1.254). Se il protocollo NAT è attivo, è necessario immettere l'indirizzo tradotto secondo tale protocollo.

Servizio

TCP

Fare clic su questa opzione se si desidera consentire il traffico dati di un servizio TCP.

UDP

Fare clic su questa opzione se si desidera consentire il traffico dati di un servizio UDP.

Servizio

Immettere il nome o il numero del servizio. Se non si conosce il nome o il numero, fare clic sul pulsante e selezionare il servizio desiderato nell'elenco visualizzato.

Configurazione della protezione applicazioni

Cisco SDM fornisce criteri di protezione delle applicazioni preconfigurati utilizzabili per proteggere la rete. Usare la barra del cursore per selezionare il livello di protezione che si desidera e per vedere una descrizione della protezione corrispondente. La schermata di riepilogo della procedura guidata visualizza il nome del criterio, SDM_HIGH, SDM_MEDIUM o SDM_LOW, e le impostazioni di configurazione della policy. È anche possibile visualizzare i dettagli della policy facendo clic sulla scheda Protezione applicazioni e la scelta del nome della policy

Pulsante anteprima comandi

Fare clic per visualizzare i comandi IOS che costituiscono questo policy.

Pulsante Criteri personalizzati per la Protezione applicazioni

Questo pulsante e il campo Nome criterio sono visibili se si sta utilizzando la Configurazione avanzata del Firewall. Scegliere questa opzione se si desidera creare un proprio criterio di protezione delle applicazioni. Se il criterio è già presente, immetterne il nome nel campo o fare clic sul pulsante a destra, scegliere **Seleziona un criterio esistente** e selezionare il criterio. Per creare un criterio fare clic sul pulsante, scegliere **Crea un nuovo criterio** e creare il criterio nella finestra di dialogo visualizzata.

Configurazione server dei nomi di dominio

Perché la protezione applicazioni possa funzionare nel router deve essere configurato l'indirizzo IP di almeno un server DNS. Fare clic su **Attivare il nome host basato su DNS alla conversione degli indirizzi** e fornire l'indirizzo IP del server DNS primario. Se è disponibile un server DNS secondario, immettere il suo indirizzo IP nel campo **Server DNS secondario**.

Gli indirizzi IP che si immettono saranno visibili nella finestra Proprietà finestra sotto Attività aggiuntive.

Configurazione server URL Filtering

I server di URL Filtering sono in grado di memorizzare e mantenere maggiori quantità di informazioni di filtraggio URL rispetto a un file di configurazione router. Se la rete presenta server URL Filtering, è possibile configurare il router in modo che li utilizzi. È possibile configurare ulteriori parametri dei server URL Filtering andando a **Configura > Attività aggiuntive > Filtri URL.** Per maggiori informazioni vedere la sezione URL Filtering.

Filtra richiesta HTTP tramite Server URL Filtering

Selezionare la casella **Filtra richiesta HTTP tramite Server URL Filtering** per consentire il filtraggio URL da parte di server URL Filtering.

Tipo server URL Filtering

Cisco SDM supporta i server URL Filtering Secure Computing e Websense. Scegliere **Secure Computing** o **Websense** per specificare il tipo di server URL Filtering in rete.

Indirizzo IP/Nome host

Immettere l'indirizzo IP o il nome host del server URL Filtering.

Seleziona zona interfaccia

Questa finestra viene visualizzata se un'interfaccia di router diversa da quella che si sta configurando fa parte di una zona di protezione con firewall con criteri basato sulle zone. Per ulteriori informazioni su questo argomento, vedere Firewall con criteri basati su zone.

Seleziona zona

Selezionare la zona di protezione di cui si desidera che l'interfaccia entri a far parte. Se si sceglie di non assegnare l'interfaccia a una zona, è molto probabile che il traffico non passi attraverso l'interfaccia.

Zone interne ZPF

Le zone che includono interfacce utilizzate nei tunnel GRE (Generic Routing Encapsulation) devono essere designate come zone interne (trusted) per consentire al traffico GRE di passare attraverso il firewall.

In questa finestra sono elencate le zone configurate e le interfacce che ne fanno parte. Per designare una zona come interne, selezionare la colonna **interna (trusted)** della riga corrispondente a tale zona.

Riepilogo

In questa schermata sono riepilogate le informazioni relative al firewall. È possibile rivedere le informazioni presentate in questa schermata e fare clic sul pulsante Indietro per tornare alle schermate precedenti della procedura guidata nel caso in cui si desideri apportare delle modifiche.

La schermata di riepilogo presenta una descrizione discorsiva della configurazione. Per vedere i comandi CLI trasmessi da Cisco SDM al router scegliere Modifica > Preferenze e fare clic su **Eseguire l'anteprima dei comandi prima dell'inoltro al router**.

Interfacce interne (trusted)

Cisco SDM elenca le interfacce logiche e fisiche del router designate come interfacce interne in questa sessione della configurazione guidata, insieme ai loro indirizzi IP. In basso sono fornite descrizioni di ciascuna definizione di configurazione applicata alle interfacce interne. Ad esempio:

```
Interfacce interne (trusted):
FastEthernet0/0 (10.28.54.205)
Applica la regola di accesso in ingresso per impedire il traffico di
spoofing.
Applica la regola di accesso in ingresso per impedire il traffico
originato da un indirizzo di loopback locale e broadcast.
Applica la regola di accesso in ingresso per consentire ogni altro
tipo di traffico.
Applica il criterio di protezione applicazioni SDM_HIGH ai dati in
ingresso.
```

Questo esempio mostra il criterio di Protezione applicazioni SDM_HIGH di Cisco SDM al traffico in ingresso su questa interfaccia.

Interfacce esterne (untrusted)

Cisco SDM elenca, con i relativi indirizzi IP, le interfacce logiche e fisiche del router scelte come interfacce esterne nel corso della procedura guidata. In basso sono fornite descrizioni di ciascuna definizione di configurazione applicata alle interfacce esterne. Ad esempio:

```
FastEthernet0/1 (142.120.12.1)
Attiva il controllo diunicast reverse path forwarding per le
interfacce non tunnel.
Applica la regola di accesso in ingresso per consentire il traffico
del tunnel IPSec, se necessario.
Applica la regola di accesso in ingresso per consentire il traffico
del tunnel GRE per le interfacce se necessario.
Applica la regola di accesso in ingresso per consentire il traffico
ICMP.
Applica la regola di accesso in ingresso per consentire il traffico
NTP, se necessario.
Applica la regola di accesso in ingresso per impedire il traffico di
spoofing.
Applica la regola di accesso in ingresso per impedire il traffico
originato da un indirizzo di loopback locale, privato e broadcast.
Applica la regola di accesso in ingresso per consentire il traffico di
servizio destinato all'interfaccia DMZ.
Servizio ftp da 10.10.10.1 a 10.10.10.20
```

```
Applica la regola di accesso in ingresso per consentire l'accesso di
SDM protetto dall'host/la rete da 140.44.3.0 255.255.255.0
Applica la regola di accesso in ingresso per impedire ogni altro tipo
di traffico.
```

Si noti che questa configurazione attiva l'inoltro del percorso inverso, una funzione che consente al router di scartare i pacchetti privi di un indirizzo IP sorgente verificabile, e consente il traffico ftp degli indirizzi DMZ da 10.10.10.1 a 10.10.10.20.

Interfaccia DMZ

Se si è configurato un firewall avanzato, in quest'area è visualizzata l'interfaccia DMZ scelta insieme al relativo indirizzo IP. Ancora sotto, Cisco SDM riporta la descrizione delle regole di accesso e delle Inspection Rule associate a tale interfaccia. Ad esempio:

```
FastEthernet (10.10.10.1)
Applica l'Inspection Rule CBAC in uscita.
Applica la regola di accesso in ingresso per impedire ogni altro tipo
di traffico.
```

Per salvare questa configurazione nella configurazione del router in esecuzione e uscire da questa procedura guidata

Fare clic su **Fine**. In Cisco SDM le modifiche apportate alla configurazione vengono salvate nella configurazione del router in esecuzione. Tali modifiche diventeranno immediatamente effettive, tuttavia andranno perse se il router verrà disattivato.

Se è stata selezionata l'opzione **Eseguire l'anteprima dei comandi prima dell'inoltro al router** nella finestra Preferenze utente, viene visualizzata la finestra Invia configurazione al router. In questa finestra è possibile visualizzare i comandi CLI inviati al router.

Avviso SDM - Accesso SDM

Questa finestra viene visualizzata quando è stato indicato che Cisco SDM deve poter accedere al router dalle interfacce esterne. Informa che è necessario verificare che SSH e HTTPS siano configurati e che almeno una delle interfacce designate come esterne siano configurate con un indirizzo IP statico. Per farlo, è necessario verificare vi sia un'interfaccia esterna configurata con un indirizzo IP statico, per poi associare un criterio di gestione a tale interfaccia.

Come stabilire se un'interfaccia esterna è configurata con un indirizzo IP statico

Effettuare le seguenti operazioni per stabilire se un'interfaccia esterna è configurata con un indirizzo IP statico.

Passo 1 Fare clic su **Configura > Interfacce e Connessioni > Modifica Interfaccia/Connessione**.

Passo 2 Esaminare la colonna IP della tabella Interfaccia per stabilire se un'interfaccia esterna ha un indirizzo IP statico.

Passo 3 Se non vi è alcuna interfaccia esterna con un indirizzo IP statico, selezionarne una e fare clic su **Modifica** per visualizzare una finestra di dialogo che consente di riconfigurare le informazioni relative all'indirizzo IP per tale interfaccia.

Se vi è un'interfaccia esterna con un indirizzo IP statico, prenderne nota e completare la seguente procedura.

Configurazione di SSH e HTTPS

Completare le seguenti operazioni per configurare un criterio di gestione per SSH e HTTPS sul router.

Passo 1 Fare clic su **Configura > Attività aggiuntive > Accesso al router > Accesso gestione**.

Passo 2 Se non vi è un criterio di gestione, fare clic su **Aggiungi**. Se si desidera modificare un criterio di gestione esistente, selezionarlo e fare clic su **Modifica**.

Nota Se si modifica un criterio di gestione, è necessario che sia associato a un'interfaccia con un indirizzo IP statico.

Passo 3 Nella finestra di dialogo visualizzata, immettere le informazioni sull'indirizzo nel riquadro Host/rete di origine. Le informazioni sull'indirizzo IP immesse devono includere l'indirizzo IP del PC che verrà utilizzato per gestire il router.

Passo 4 Scegliere un'interfaccia esterna con indirizzo IP statico nel riquadro Interfaccia di gestione. L'interfaccia deve avere una route all'indirizzo IP specificato nel riquadro Host/rete di origine.

Passo 5 Nella casella Protocolli di gestione, selezionare **Consenti SDM**.

Passo 6 Selezionare **HTTPS** e **SSH** per consentire questi protocolli.

Passo 7 Fare clic su OK per chiudere la finestra di dialogo.

Passo 8 Fare clic su **Applica modifiche** nella finestra in cui sono visualizzati i criteri di accesso alla gestione.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come visualizzare l'attività del firewall?

Il monitoraggio dell'attività del firewall si effettua mediante la creazione di voci di registro. Se sul router è stata attivata la funzione di registrazione, ogni volta che si attiva una regola di accesso configurata in modo da generare voci di registro in determinati casi (ad esempio, se si rileva un tentativo di connessione proveniente da un indirizzo IP bloccato) verrà creata una voce di registro visualizzabile nella modalità Controllo.

Attivazione della registrazione

La prima fase della procedura di visualizzazione dell'attività del firewall consiste nell'attivazione della registrazione sul router. A tale fine:

Passo 1 Dal frame a sinistra, selezionare **Attività aggiuntive.**

Passo 2 Nella struttura Attività aggiuntive, fare clic su **Registrazione** e quindi sul pulsante **Modifica**.

Passo 3 Nella schermata Syslog, selezionare **Registrazione in buffer**.

Passo 4 Nel campo Dimensione buffer, immettere la quantità di memoria del router che si desidera utilizzare per il buffer di registrazione. Il valore predefinito è 4096 byte. Benché un buffer di grandi dimensioni possa contenere più voci di registro, occorre raggiungere un opportuno compromesso fra le dimensioni del buffer e il potenziale impatto negativo sulle prestazioni del router.

Passo 5 Fare clic su **OK**.

Configurazione delle regole di accesso per cui si desidera creare voci di registro

Oltre ad attivare la registrazione, è necessario specificare le regole di accesso per cui si desidera creare delle voci di registro. A tale fine:

Passo 1 Dal frame a sinistra, selezionare **Attività aggiuntive.**

Passo 2 Nella struttura Attività aggiuntive, fare clic su **Editor ACL** e quindi sul pulsante **Regole di accesso**.

Tutte le regole di accesso sono visualizzate nella tabella superiore sul lato destro della schermata. Nella tabella inferiore sono invece mostrati gli indirizzi IP di origine e di destinazione e i servizi consentiti o bloccati dalla regola.

Passo 3 Nella tabella superiore, fare clic sulla regola che si desidera modificare.

Passo 4 Fare clic su **Modifica**.

Viene visualizzata la finestra di dialogo Modifica regola.

Passo 5 Nel campo Voce regola sono visualizzate le combinazioni indirizzo IP di origine/indirizzo IP di destinazione/servizio consentite o bloccate dalla regola. Fare clic sulla voce di regola che si desidera configurare in modo da creare delle voci di registro.

Passo 6 Fare clic su **Modifica**.

Passo 7 Nella finestra di dialogo della voce di regola, selezionare la casella di controllo **Corrispondenze di registro per la voce**.

Passo 8 Per chiudere le finestre di dialogo visualizzate, fare clic su **OK**.

A seguito di tali modifiche verranno create delle voci di registro ogni volta che si tenta di effettuare una connessione utilizzando l'intervallo di indirizzi IP e richiedendo i servizi definiti nella voce di regola.

Passo 9 Ripetere la procedura dal passo 4 al passo 8 per ognuna delle voci di regola che si desidera configurare in modo da creare delle voci di registro.

Dopo aver completato la configurazione della registrazione, seguire la procedura di seguito riportata per visualizzare l'attività del firewall.

Passo 1 Nella barra degli strumenti, selezionare **Modalità di controllo**.

Passo 2 Nel frame a sinistra, selezionare **Stato del firewall**.

Nelle statistiche del firewall è possibile sia verificare l'avvenuta configurazione del firewall sia visualizzare il numero di tentativi di connessione bloccati.

Nella tabella sono visualizzate tutte le voci di registro relative al router create dal firewall, oltre all'ora e al motivo per cui ogni voce è stata generata.

Come configurare un firewall in un'interfaccia non supportata?

In Cisco SDM è possibile configurare un firewall in un'interfaccia non supportata da Cisco SDM. Prima di configurare il firewall, è necessario configurare l'interfaccia mediante l'interfaccia della riga di comando (CLI) del router. È necessario che tale interfaccia disponga di almeno un indirizzo IP e che sia funzionante. Per ulteriori informazioni sulla procedura di configurazione di un'interfaccia mediante CLI, consultare la guida di configurazione del software del router.

Per verificare il corretto funzionamento della connessione, nella finestra Interfacce e connessioni assicurarsi che lo stato dell'interfaccia sia attivo.

Di seguito è riportata la configurazione di un'interfaccia ISDN su un router Cisco 3620.

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
!This is the data BRI WIC
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 100.100.100.100 name junky 883531601
 dialer hold-queue 10
 isdn switch-type basic-5ess
 isdn tei-negotiation first-call
 isdn twait-disable
 isdn spid1 80568541630101 6854163
 isdn incoming-voice modem
```

Per ottenere informazioni sulle altre possibili configurazioni, consultare la guida di configurazione del software del router.

Dopo aver configurato mediante CLI l'interfaccia non supportata, è possibile utilizzare Cisco SDM per configurare il firewall. Nei campi dell'elenco delle interfacce del router l'interfaccia non supportata verrà visualizzata come “Altro”.

Come configurare un firewall dopo aver configurato una connessione VPN?

Se si configura un firewall in un'interfaccia utilizzata in una VPN, è necessario che il firewall consenta il traffico locale fra i peer VPN locali e remoti. Se si utilizza la procedura guidata Firewall di base o avanzata, il traffico fra i peer VPN viene automaticamente consentito da Cisco SDM.

Se si crea una regola di accesso nell'Editor ACL disponibile in Attività aggiuntive, la gestione delle istruzioni di tipo consenti o di tipo blocca della regola è del tutto manuale e di conseguenza è necessario garantire esplicitamente che il traffico sia consentito fra i peer VPN. Le istruzioni di seguito riportate sono esempi dei tipi di istruzioni da includere nella configurazione per consentire il traffico VPN:

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

Come consentire il traffico specifico mediante un'interfaccia DMZ?

Per configurare l'accesso a un server Web su una rete DMZ attraverso il firewall, seguire la procedura di seguito riportata:

Passo 1 Nel frame a sinistra, selezionare **Firewall e ACL.**

Passo 2 Selezionare **Firewall avanzato**.

Passo 3 Fare clic su **Avvia attività selezionata**.

Passo 4 Fare clic su **Avanti**.

Viene visualizzata la schermata Configurazione avanzata dell'interfaccia Firewall.

Passo 5 Nella tabella Interfaccia, selezionare quali interfacce sono connesse alle reti protette dal firewall e quali invece sono connesse alle reti esterne al firewall.

Passo 6 Nel campo Interfaccia DMZ, selezionare l'interfaccia connessa alla rete DMZ.

Passo 7 Fare clic su **Avanti>**.

Passo 8 Nel campo Indirizzo IP, immettere l'indirizzo IP o l'intervallo di indirizzi IP dei server Web.

Passo 9 Nel campo Servizio, selezionare TCP.

Passo 10 Nel campo Porta, immettere **80** oppure **www**.

Passo 11 Fare clic su **Avanti>**.

Passo 12 Fare clic su **Fine**.

Come modificare un firewall esistente per consentire il traffico da una nuova rete o un nuovo host?

Per modificare la configurazione del firewall in modo da consentire il traffico da una nuova rete o un nuovo host è possibile utilizzare la scheda Modifica criterio firewall.

Passo 1 Nel frame a sinistra, selezionare **Firewall e ACL**.

Passo 2 Fare clic sulla scheda **Modifica criterio firewall**.

Passo 3 Nel pannello di selezione del traffico, scegliere un'interfaccia di origine e una di destinazione per indicare il flusso di traffico al quale il firewall è stato applicato e quindi fare clic su **Vai**. Se al flusso di traffico è stato applicato un firewall, nella grafica del router verrà visualizzata un'icona di firewall. Se per il flusso di traffico selezionato non viene visualizzata la regola di accesso che si desidera modificare, selezionare un'altra interfaccia di origine o di destinazione.

Passo 4 Esaminare la regola di accesso nell'area Servizi. Per visualizzare la finestra di dialogo per l'aggiunta di una nuova voce di regola di accesso, utilizzare il pulsante **Aggiungi**.

Passo 5 Immettere un'istruzione di tipo consenti per la rete o l'host a cui si desidera consentire l'accesso alla rete. Fare clic su **OK** nella finestra di dialogo della voce di regola.

Passo 6 La nuova voce viene visualizzata nell'area Servizi.

Passo 7 Se necessario, utilizzare i pulsanti **Taglia** e **Incolla** per cambiare la posizione della voce nell'elenco.

Come configurare il protocollo NAT in un'interfaccia non supportata?

Cisco SDM è in grado di configurare il protocollo NAT (Network Address Translation) in un'interfaccia non supportata da Cisco SDM. Prima di configurare il firewall, è necessario configurare l'interfaccia mediante l'interfaccia della riga di comando (CLI) del router. È necessario che tale interfaccia disponga di almeno un indirizzo IP e che sia funzionante. Per verificare il corretto funzionamento della connessione, assicurarsi che lo stato dell'interfaccia sia attivato.

Dopo aver configurato mediante CLI l'interfaccia non supportata, è possibile configurare una connessione NAT. Nell'elenco delle interfacce del router, l'interfaccia non supportata verrà visualizzata come “Altro”.

Come configurare un pass-through NAT per un firewall?

Se è stata configurata una connessione NAT e si sta configurando il firewall, è necessario configurarlo in modo da consentire il traffico proveniente dal proprio indirizzo IP pubblico. A tale fine occorre configurare una ACL. Per configurare una ACL che consenta il traffico proveniente dal proprio indirizzo IP pubblico:

Passo 1 Nel frame a sinistra, selezionare **Attività aggiuntive**.

Passo 2 Nella struttura Regole, selezionare **Editor ACL** e quindi **Regole di accesso**.

Passo 3 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi regola.

Passo 4 Nel campo Nome/numero, immettere un nome o un numero univoco per la nuova regola.

Passo 5 Nel campo Tipo, selezionare **Regola standard**.

Passo 6 Nel campo Descrizione, immettere una breve descrizione della nuova regola, quale ad esempio “Consenti il pass-through NAT”.

Passo 7 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi voce di regola standard.

Passo 8 Nel campo Azione, scegliere **Consenti**.

Passo 9 Nel campo Tipo, selezionare **Host**.

Passo 10 Nel campo Indirizzo IP, immettere l’indirizzo IP pubblico.

Passo 11 Nel campo Descrizione, immettere una breve descrizione, quale ad esempio “Indirizzo IP pubblico”.

Passo 12 Fare clic su **OK**.

Passo 13 Fare clic su **OK**.

La nuova regola viene visualizzata nella tabella Regole di accesso.

Come consentire il passaggio del traffico verso il concentratore Easy VPN attraverso il firewall?

Per consentire il traffico verso un concentratore VPN attraverso il firewall è necessario creare o modificare una regola di accesso che consenta il traffico VPN. A tale fine:

Passo 1 Nel frame a sinistra, selezionare **Attività aggiuntive**.

Passo 2 Nella struttura Regole, selezionare **Editor ACL** e quindi **Regole di accesso**.

Passo 3 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi regola.

Passo 4 Nel campo Nome/numero, immettere un nome o un numero univoco per la regola.

Passo 5 Nel campo Descrizione, immettere una descrizione della nuova regola, quale ad esempio “Traffico concentratore VPN”.

Passo 6 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi voce di regola estesa.

Passo 7 Nel campo Tipo del gruppo Host/rete di origine, selezionare **Una rete**.

Passo 8 Nei campi Indirizzo IP e Maschera carattere jolly, immettere l'indirizzo IP e la maschera della rete del peer VPN di origine.

Passo 9 Nel campo Tipo del gruppo Host/rete di destinazione, selezionare **Una rete**.

Passo 10 Nei campi Indirizzo IP e Maschera carattere jolly, immettere l'indirizzo IP e la maschera della rete del peer VPN di destinazione.

Passo 11 Nel gruppo Protocollo e servizio, selezionare **TCP**.

Passo 12 Nei campi Porta di origine, selezionare = e immettere il numero di porta **1023**.

Passo 13 Nei campi Porta di destinazione, selezionare = e immettere il numero di porta **1723**.

Passo 14 Fare clic su **OK**.

La nuova regola viene visualizzata nell'Elenco voci di regola.

Passo 15 Ripetere la procedura dal passo 7 al passo 15 creando le voci di regola per i protocolli e, dove richiesto, per i numeri di porta di seguito elencati.

- Protocollo **IP**, Protocollo IP **GRE**
- Protocollo **UDP**, Porta di origine **500**, Porta di destinazione **500**
- Protocollo **IP**, Protocollo IP **ESP**
- Protocollo **UDP**, Porta di origine **10000**, Porta di destinazione **10000**

Passo 16 Fare clic su **OK**.

Come associare una regola a un'interfaccia?

Se si utilizza la procedura guidata Firewall di Cisco SDM, le regole di accesso e le Inspection Rule create vengono automaticamente associate all'interfaccia per cui si è creato il firewall. Se si sta creando una regola in Attività aggiuntive/Editor ACL, è possibile associarla a un'interfaccia della finestra Aggiungi o modifica regola. Se le regole non venissero associate a un'interfaccia in questa fase, è comunque possibile eseguire questa operazione in un secondo momento.

Passo 1 Fare clic su **Interfacce e connessioni** nel pannello a sinistra e quindi fare clic sulla scheda **Modifica interfacce e connessioni**.

Passo 2 Selezionare l'interfaccia a cui si desidera associare una regola e quindi fare clic su **Modifica**.

Passo 3 Nella scheda Associazione, immettere il nome o il numero della regola nei campi In ingresso o In uscita all'interno delle caselle Regola di accesso o Inspection Rule. Se si desidera che la regola effettui il filtraggio del traffico prima che questo arrivi all'interfaccia, utilizzare il campo In ingresso. Se invece si desidera che la regola effettui il filtraggio del traffico che ha già raggiunto il router ma che può uscirne attraverso l'interfaccia selezionata, utilizzare il campo In uscita.

Passo 4 Fare clic su **OK** nella scheda Associazione.

Passo 5 Nella finestra Regole di accesso o nella finestra Inspection Rules, esaminare la colonna Utilizzata da per verificare che la regola è stata associata all'interfaccia.

Come annullare l'associazione di una regola di accesso a un'interfaccia?

È possibile che sia necessario rimuovere l'associazione fra una regola di accesso e un'interfaccia. La rimozione dell'associazione non comporta l'eliminazione della regola di accesso. Se occorre, è possibile associare tale regola ad altre interfacce. Per rimuovere l'associazione fra una regola di accesso e un'interfaccia, eseguire la procedura di seguito riportata.

Passo 1 Fare clic su **Interfacce e connessioni** nel pannello a sinistra e quindi fare clic sulla scheda **Modifica interfacce e connessioni**.

Passo 2 Selezionare l'interfaccia per cui si desidera annullare l'associazione alla regola di accesso.

Passo 3 Fare clic su **Modifica**.

Passo 4 Nella scheda Associazione, trovare la regola di accesso nei campi In ingresso o In uscita all'interno della casella Regola di accesso. Tale regola potrebbe presentare un nome o un numero.

Passo 5 Fare clic nel campo In ingresso o In uscita e quindi fare clic sul pulsante a destra.

Passo 6 Fare clic su **Nessuno (cancella associazione regole)**.

Passo 7 Fare clic su **OK**.

Come eliminare una regola associata a un'interfaccia?

In Cisco SDM non è consentito eliminare una regola associata a un'interfaccia; occorre prima rimuovere l'associazione fra la regola e l'interfaccia e quindi eliminare la regola di accesso.

Passo 1 Fare clic su **Interfacce e connessioni** nel pannello a sinistra e quindi fare clic sulla scheda **Modifica interfacce e connessioni**.

Passo 2 Selezionare l'interfaccia per cui si desidera annullare l'associazione alla regola.

Passo 3 Fare clic su **Modifica**.

Passo 4 Nella scheda Associazione, trovare la regola nella casella Regola di accesso o nella casella Inspect Rule. Tale regola potrebbe presentare un nome o un numero.

Passo 5 Trovare la regola nella scheda Associazione. **Se si tratta di una regola di accesso,** fare clic su **Nessuno (cancella associazione regole). Se invece si tratta di una Inspection Rule, fare clic su Nessuno**.

Passo 6 Fare clic su **OK**.

Passo 7 Fare clic su **Regole** nel frame a sinistra. Utilizzare la struttura Regole per passare alla finestra Regola di accesso o Inspection Rule.

Passo 8 Selezionare la regola che si desidera rimuovere e quindi fare clic su **Elimina**.

Come creare una regola di accesso per un elenco Java?

Nelle Inspection Rule è possibile specificare degli elenchi Java. Gli elenchi Java si utilizzano per consentire il traffico associato ad applet Java proveniente da origini trusted. Queste origini sono definite in una regola di accesso a cui l'elenco Java fa riferimento. Per creare una regola di accesso di questo tipo e utilizzarla in un elenco Java, eseguire la procedura di seguito riportata:

Passo 1 Se è visualizzata la finestra Inspection Rules e si è fatto clic su **Elenco Java**, fare clic sul pulsante a destra del campo Numero e quindi fare clic su **Crea nuova regola (ACL) e seleziona.** Viene visualizzata la finestra Aggiungi regola.

Se invece è visualizzata la finestra Regole di accesso, per aprire la finestra Aggiungi regola fare clic su **Aggiungi**.

Passo 2 Nella finestra Aggiungi regola, creare una regola di accesso standard che consenta il traffico proveniente dagli indirizzi ritenuti trusted. Se ad esempio si desidera consentire il traffico associato ad applet Java proveniente dagli host 10.22.55.3 e 172.55.66.1 è possibile creare nella finestra Aggiungi regola le seguenti voci di regola di accesso:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

È possibile immettere una descrizione sia per le voci sia per la regola.

Non occorre associare la regola all'interfaccia alla quale si sta applicando l'Inspection Rule.

Passo 3 Fare clic su **OK** nella finestra Aggiungi regola.

Passo 4 Se la presente procedura è stata iniziata nella finestra Inspection Rules, fare clic su **OK** nella finestra Elenco Java. Non è necessario eseguire i passi 5 e 6.

Passo 5 Se la presente procedura è iniziata nella finestra Regole di accesso, passare alla finestra Inspection Rules, selezionare l'Inspection Rule per cui si desidera creare un elenco Java e quindi fare clic su **Modifica**.

Passo 6 Selezionare **http** nella colonna Protocolli e quindi fare clic su **Elenco Java**.

Passo 7 Nel campo Numero elenco Java, immettere il numero dell'elenco di accesso creato. Fare clic su **OK**.

Come consentire il traffico specifico verso la rete se non è disponibile una rete DMZ?

La procedura guidata Firewall consente di specificare il traffico dati che si desidera consentire sulla rete DMZ. Se non si dispone di una rete DMZ è comunque possibile, mediante la funzione Criterio firewall, consentire a determinati tipi di traffico esterno di accedere alla rete interna.

Passo 1 Configurare un firewall utilizzando la procedura guidata Firewall.

Passo 2 Fare clic su **Modifica ACL/Criterio firewall**.

Passo 3 Per visualizzare la regola di accesso che si desidera modificare, impostare come interfaccia di origine l'interfaccia esterna (untrusted) e come interfaccia di destinazione l'interfaccia interna (trusted). Viene visualizzata la regola di accesso applicata al traffico in ingresso sull'interfaccia untrusted.

Passo 4 Per consentire l'accesso in rete a un particolare tipo di traffico non ancora autorizzato, fare clic su **Aggiungi** nell'area Servizi.

Passo 5 Creare le voci che occorrono nella finestra di dialogo della voce di regola. È necessario fare clic su **Aggiungi** per ognuna delle voci che si desidera creare.

Passo 6 Le voci create saranno visualizzate nell'elenco delle voci dell'area Servizi.

CAPITOLO 7

Criterio firewall

La funzione del criterio firewall consente di visualizzare e modificare le configurazioni del firewall (regole di accesso e/o le Inspection Rule CBAC) nell'ambito delle interfacce di cui filtrano il traffico. Con una rappresentazione grafica del router e delle interfacce relative, è possibile scegliere diverse interfacce sul router e controllare se è stata applicata a quella interfaccia una regola di accesso o un'Inspection Rule. È possibile inoltre visualizzare i dettagli delle regole mostrate nella finestra Modifica ACL/Criterio firewall.

Modifica ACL/criterio firewall

Per visualizzare le regole di accesso e le Inspection Rule nell'ambito delle interfacce a cui sono associate le regole, utilizzare la finestra Modifica ACL/Criterio firewall. Questa stessa finestra è utile anche per modificare le regole di accesso e le Inspection Rule visualizzate.

Configurazione di un firewall prima di utilizzare la funzione Criterio firewall

Prima di utilizzare la finestra Modifica ACL/Criterio firewall, è necessario effettuare le seguenti attività:

1. **Configurare le interfacce LAN e WAN**. Prima di poter creare un firewall, è necessario configurare le interfacce LAN e WAN. Per configurare le connessioni del router è possibile utilizzare le procedure guidate LAN e WAN.

2. **Utilizzare la procedura guidata del firewall per configurare un firewall e un'interfaccia DMZ**. Questa procedura è il modo più semplice per applicare le regole di accesso e le Inspection Rule alle interfacce interne ed esterne da identificare, inoltre consente di configurare un'interfaccia DMZ e di specificare i servizi consentiti nella rete DMZ.
3. **Passare alla finestra Criterio firewall per modificare il criterio firewall creato**. Dopo aver configurato le interfacce LAN e WAN e dopo aver creato un firewall, è possibile aprire questa finestra e ottenere una rappresentazione grafica del criterio in un flusso di traffico. È possibile visualizzare le voci delle regole di accesso e delle Inspection Rule ed effettuare tutte le dovute modifiche.

Utilizzo della funzione per visualizzare il criterio firewall

Una volta creato il firewall, è possibile utilizzare la finestra Vista criteri firewall per ottenere una visualizzazione grafica del firewall relativamente alle interfacce del router e per effettuare eventuali modifiche.

Per ulteriori informazioni, fare clic sull'azione che si desidera effettuare.

- Selezione flusso traffico
- Analisi del diagramma del traffico e selezione di una direzione di traffico
- Modifiche alle regole d'accesso
- Modifica delle Inspection Rule

Per un esempio di caso di utilizzo, vedere la sezione Scenario del caso di utilizzo del criterio firewall.

Nota Se il router dispone di un'immagine Cisco IOS che non supporta il set di funzioni Firewall, verrà visualizzata solo l'area Servizi e si potranno solo creare le voci di controllo di accesso.

Pulsante Applica modifiche

Consente di inviare le modifiche effettuate in questa finestra al router. Se si lascia la finestra Modifica ACL/Criterio firewall senza fare clic su **Applica modifiche**, in Cisco SDM viene visualizzato un messaggio indicante che occorre applicare le modifiche o annullarle.

Pulsante Annulla modifiche

Consente di annullare le modifiche effettuate in questa finestra. Questo pulsante non consente di eliminare le modifiche inviate al router tramite il pulsante **Applica modifiche**.

Selezione flusso traffico

Per *flusso di traffico* si intende il traffico che entra nel router tramite un'interfaccia specificata (l'interfaccia *di provenienza*) ed esce dal router tramite un'interfaccia specificata (l'interfaccia *di destinazione*). I controlli di visualizzazione del flusso di traffico di Cisco SDM sono allineati nella parte superiore della finestra Modifica ACL/criterio firewall.

Nota Nel router sono necessarie almeno due interfacce configurate. Se ne è presente solo una, Cisco SDM visualizzerà un messaggio con la richiesta di configurazione di un'altra interfaccia.

Nella tabella che segue vengono descritti i controlli di visualizzazione del flusso di traffico di Cisco SDM.

Provenienza	Selezionare l'interfaccia da cui ha origine il flusso di traffico desiderato. La rete connessa all'interfaccia di provenienza verrà protetta dal firewall. Nell'elenco **Provenienza** sono incluse tutte le interfacce con indirizzi IP configurati.
Destinazione	Selezionare l'interfaccia esterna che consente al traffico di lasciare il router. Nell'elenco **Destinazione** sono incluse tutte le interfacce con indirizzi IP configurati.
	Il pulsante Dettagli consente di visualizzare informazioni sull'interfaccia. Vengono forniti, ad esempio, dettagli sull'indirizzo IP, sul tipo di incapsulamento, sul criterio IPSec associato e sul tipo di autenticazione.

Pulsante Vai	Fare clic per aggiornare il del flusso di traffico con le informazioni sulle interfacce selezionate. Il diagramma non viene aggiornato finché non si fa clic su **Vai**. Questo pulsante viene disattivato se l'interfaccia di provenienza o di destinazione non è selezionata, oppure se le interfacce di provenienza e destinazione sono le stesse.
Visualizza opzione	Selezionare **Cambia interfaccia di provenienza e destinazione** per cambiare le interfacce selezionate in origine nelle caselle di riepilogo **Provenienza** e **Destinazione**. È possibile utilizzare l'opzione di scambio nel caso in cui si desidera creare un firewall per proteggere la rete connessa all'interfaccia di provenienza e all'interfaccia di destinazione. È possibile scegliere **Visualizza tutti le ACL nel flusso di traffico** nel momento in cui viene applicata una regola di accesso all'interfaccia di provenienza e un'altra regola all'interfaccia di destinazione per la direzione di traffico scelta. In un'altra finestra vengono visualizzate le voci di entrambe le regole di accesso.

Cisco SDM visualizza tutte le interfacce che dispongono di indirizzi IP in ordine alfabetico negli elenchi delle interfacce di **provenienza** e di **destinazione**. Per impostazione predefinita, Cisco SDM seleziona la prima interfaccia nell'elenco **Provenienza** e la seconda nell'elenco **Destinazione**. Utilizzare gli elenchi a discesa delle interfacce di **provenienza** e di **destinazione** per selezionare un altro flusso di traffico. Il flusso di traffico scelto viene visualizzato nel diagramma del traffico al di sotto dei controlli di visualizzazione del flusso di traffico.

Ad esempio, per visualizzare il flusso di traffico proveniente dalla rete connessa all'interfaccia router Ethernet 0 e uscente dal router tramite l'interfaccia seriale 0 disponibile, effettuare le seguenti operazioni:

Passo 1 Scegliere Ethernet 0 nell'elenco a discesa **Provenienza**.

Passo 2 Scegliere Seriale 0 nell'elenco a discesa **Destinazione**.

Passo 3 Fare clic su **Vai**.

Passo 4 Selezionare **Cambia interfaccia di provenienza e destinazione** nell'elenco a discesa Visualizza opzione per cambiare le interfacce selezionate in origine nelle caselle di riepilogo **Provenienza** e **Destinazione**.

Le regole di accesso applicate al traffico di origine e di ritorno possono essere diverse. Per ulteriori informazioni sul passaggio dal traffico di origine a quello di ritorno e viceversa nel diagramma di traffico, vedere Analisi del diagramma del traffico e selezione di una direzione di traffico.

Passo 5 Fare clic sul pulsante **Dettagli** accanto all'elenco a discesa **Provenienza** o **Destinazione** per aprire una finestra che mostra l'indirizzo IP, i criteri IPSec e altre informazioni su un'interfaccia.

Per lavorare con il diagramma del traffico, vedere Analisi del diagramma del traffico e selezione di una direzione di traffico. Per tornare alla descrizione della finestra Criterio firewall principale vedere Modifica ACL/criterio firewall.

Analisi del diagramma del traffico e selezione di una direzione di traffico

Nel diagramma del traffico viene visualizzato il router con le interfacce di provenienza e di destinazione scelte (per ulteriori informazioni, vedere Selezione flusso traffico). Vengono visualizzati anche i tipi di regole applicate per il flusso di traffico scelto, oltre alla direzione in cui sono state applicate.

Traffico di origine

Fare clic per evidenziare il flusso di traffico che entra nel router tramite l'interfaccia di provenienza ed esce dal router tramite l'interfaccia di destinazione. Una volta evidenziata quest'area, è possibile vedere i dettagli delle regole applicate nella direzione del flusso di traffico.

Traffico di ritorno

Fare clic per evidenziare il flusso di traffico che entra nel router tramite l'interfaccia di destinazione ed esce dal router tramite l'interfaccia di provenienza. Una volta evidenziata quest'area, è possibile vedere i dettagli delle regole applicate al traffico di ritorno.

Icone

Nel flusso di traffico le regole vengono rappresentate dalle icone:

	Il simbolo del filtro consente di indicare che è stata applicata una regola di accesso.
	La lente di ingrandimento segnala l'applicazione di un'Inspection Rule.
	Con l'icona del firewall nel router viene indicato che è stato applicato un firewall al flusso di traffico di origine. Cisco SDM consente di visualizzare un'icona di firewall se vengono soddisfatti i seguenti set di criteri: • Esiste un'Inspection Rule applicata al traffico di origine nella direzione in ingresso dell'interfaccia di provenienza e, inoltre, esiste una regola di accesso applicata alla direzione in ingresso dell'interfaccia di destinazione. • La regola di accesso nella direzione in ingresso dell'interfaccia di destinazione è una regola di accesso estesa e include almeno una voce di regola di accesso. Non viene visualizzata alcuna icona di firewall se è stato applicato un firewall al traffico di ritorno. Se la funzionalità del firewall è disponibile, ma al flusso di traffico non è stato applicato alcun firewall, al di sotto del diagramma del traffico verrà visualizzato **Firewall IOS: Inattivo**.
	Con una freccia destra vengono indicate le regole applicate al traffico di origine. Un'icona sulla linea del traffico dell'interfaccia di provenienza consente di indicare la presenza di una regola che filtra il traffico in ingresso al router. Un'icona sulla linea del traffico dell'interfaccia di destinazione consente di indicare la presenza di una regola che filtra il traffico in uscita dal router. Ponendo il mouse su questa icona, Cisco SDM visualizzerà i nomi delle regole applicate.
	Con una freccia sinistra vengono indicate le regole applicate al traffico di ritorno. Un'icona sulla linea del traffico dell'interfaccia di destinazione consente di indicare la presenza di una regola che filtra il traffico in ingresso al router. Un'icona sulla linea del traffico dell'interfaccia di provenienza consente di indicare la presenza di una regola che filtra il traffico in uscita dal router. Ponendo il cursore su questa icona, si visualizzano i nomi delle regole applicate.

Nota Anche se le icone vengono mostrate su una particolare interfaccia del diagramma, in un criterio firewall potrebbero essere incluse voci di controllo di accesso che influiscono sul traffico non rappresentato dal diagramma. Ad esempio, una voce che include l'icona del carattere jolly nella colonna Destinazione (vedere Modifiche alle regole d'accesso) potrebbe applicare al traffico in uscita delle interfacce diverse da quelle rappresentate dall'interfaccia di destinazione al momento selezionata. Il carattere jolly appare come un asterisco e rappresenta qualsiasi rete o host.

Per modificare una regola d'accesso, vedere Modifiche alle regole d'accesso. Per tornare alla descrizione della finestra Criterio firewall principale vedere Modifica ACL/criterio firewall.

Modifiche alle regole d'accesso

Nel pannello dei criteri vengono mostrati i dettagli delle regole applicate al flusso di traffico selezionato. Il pannello dei criteri viene aggiornato dopo aver selezionato le interfacce di provenienza e di destinazione e dopo che il diagramma del traffico è passato dall'attivazione/disattivazione del traffico di origine all'attivazione/disattivazione del traffico di ritorno

Il pannello dei criteri risulta vuoto quando si associa una regola di accesso senza alcuna voce a un'interfaccia. Ad esempio, se il nome di una regola è stato associato a un'interfaccia tramite l'interfaccia della riga di comando, senza tuttavia creare alcuna voce per la regola, questo pannello risulta vuoto. Se il pannello è vuoto, è possibile utilizzare il pulsante **Aggiungi** in modo da creare delle voci per la regola.

Campi intestazione area Servizi

Disponibilità funzioni firewall	Se l'immagine Cisco IOS utilizzata dal router supporta la funzione firewall, questo campo contiene il valore **Disponibile**.
Regola di accesso	Nome o numero della regola di accesso di cui vengono visualizzate le voci.
Inspection Rule	Nome o numero della Inspection Rule di cui vengono visualizzate le voci.
	Questa icona viene visualizzata quando si associa una regola di accesso a un'interfaccia senza tuttavia creare nessuna regola di accesso di quel nome o numero. Cisco SDM informa che il criterio non ha alcun effetto salvo la presenza di almeno una voce di regola di accesso.

Controlli area Servizi

Nella tabella sottostante vengono descritti i controlli presenti nell'area Servizi.

Pulsante Aggiungi	Consente di aggiungere una voce di regola di accesso. Specificare se si desidera aggiungere la voce prima o dopo la voce attualmente selezionata. Quindi creare la voce nella finestra Aggiungi una voce. Tenere presente che l'ordine delle voci è importante. Cisco SDM consente di visualizzare la finestra di dialogo Voci estese quando si aggiunge una voce dalla finestra Modifica ACL/Criterio firewall. Per aggiungere una regola standard, andare a **Attività aggiuntive > Editor ACL > Regole di accesso**.
Pulsante Modifica	Consente di modificare una voce di regola di accesso selezionata. Sebbene sia possibile solo aggiungere Rule entry di accesso estese nella finestra Modifica ACL/Criterio firewall, è consentito anche modificare la voce di regola standard precedentemente applicata all'interfaccia selezionata.

Pulsante Taglia	Consente di rimuovere una voce di regola di accesso selezionata. La voce si trova negli Appunti ed è possibile incollarla in un'altra posizione dell'elenco o in un'altra regola di accesso. Se si desidera riordinare una voce, è possibile tagliarla da un percorso, selezionarla prima o dopo il percorso per il quale si intende tagliarla, quindi fare clic su **Incolla**. Il menu di scelta rapida Incolla consente di posizionare la voce prima o dopo la voce selezionata.
Pulsante Copia	Selezionare una voce di rete, quindi fare clic su questo pulsante per collocare la voce negli Appunti.
Pulsante Incolla	Consente di incollare una voce degli Appunti alla regola selezionata. Verrà richiesto di specificare se si desidera incollare la voce prima o dopo la voce al momento selezionata. Nel caso in cui è presente una voce identica nella regola di accesso, Cisco SDM visualizza la finestra Aggiungi voce di regola estesa in modo da poter modificare quella voce. Cisco SDM non consente la presenza di voci duplicate all'interno della stessa regola.

Elenco a discesa Interfacce	Se il flusso di traffico selezionato (di origine o di ritorno) include una regola di accesso nell'interfaccia di provenienza o di destinazione, è possibile utilizzare questo elenco per passare da una regola all'altra.
	Se al flusso di traffico selezionato non è stato applicato un firewall, è possibile farlo selezionando Traffico di origine e facendo clic sul pulsante Applica firewall. Per impostazione predefinita, facendo clic su Applica firewall verrà associata un'Inspection Rule predefinita Cisco SDM alla direzione in ingresso dell'interfaccia di provenienza e, inoltre, verrà associata una regola di accesso alla direzione in ingresso dell'interfaccia di destinazione che impedisce il traffico. Se l'immagine Cisco IOS utilizzata dal router non supporta la funzione firewall, questo pulsante è disattivato. Ad esempio, se si desidera applicare un firewall di protezione alla rete connessa all'interfaccia **Ethernet 0** del traffico in ingresso nell'interfaccia Ethernet 1, selezionare Ethernet 0 dall'elenco a discesa **Provenienza** ed Ethernet 1 dall'elenco a discesa **Destinazione**. Quindi fare clic su **Applica firewall**. Se si desidera applicare un firewall di protezione alla rete connessa all'interfaccia Ethernet 1 del traffico in ingresso nell'interfaccia Ethernet 0, andare ad **Attività aggiuntive > Editor ACL > Regole di accesso**.

Se la regola è di sola lettura i pulsanti dell'area servizio sono disattivati. Una regola è di sola lettura se contiene sintassi che Cisco SDM non supporta. Le regole di sola lettura sono indicate dall'icona  .

In presenza di una regola standard che filtra il flusso di traffico di ritorno a cui si sta applicando il firewall, Cisco SDM informa che la regola di accesso standard verrà convertita in una regola estesa.

Campi voci area Servizi

Nella tabella sottostante vengono descritte le icone e gli altri dati delle voci relative all'area Servizi.

Campo	Descrizione	Icone	Significato
Azione	Traffico consentito o bloccato.		Consente il traffico di origine.
			Impedisce il traffico di origine.
Origine/ Destinazione	Indirizzo host o di rete o qualsiasi host o rete.		Indica l'indirizzo di una rete.
			Indica l'indirizzo di un host.
			Indica qualsiasi rete o host.
Servizio	Tipo di servizio filtrato.		Esempi: TCP, EIGRP, UDP, GRE. Vedere Servizi IP.
			Esempi: Telnet, HTTP, FTP. Vedere Servizi TCP.
			Esempi: SNMP, BOOTPC, RIP. Vedere Servizi UDP.
			Internet Group Management Protocol (IGMP).
			Esempi: echo-reply, host-unreachable. Vedere Tipi di messaggi ICMP.
Registro	Registrazione del traffico bloccato.		Registra traffico bloccato. Per la configurazione della registrazione del firewall vedere Registro firewall.
Opzioni	Opzioni configurate utilizzando l'interfaccia a riga di comando.	Nessuna icona.	
Descrizione	Qualsiasi descrizione fornita.	Nessuna icona.	

Per modificare una Inspection Rule, vedere Modifica delle Inspection Rule. Per tornare alla descrizione della finestra Criterio firewall principale vedere Modifica ACL/criterio firewall.

Modifica delle Inspection Rule

L'area Applicazioni viene visualizzata quando l'immagine Cisco IOS in esecuzione sul router supporta le Inspection Rule CBAC. Le voci delle Inspection Rule che filtrano il flusso di traffico vengono visualizzate nell'area Applicazioni; questa viene aggiornata quando viene scelto un nuovo flusso di traffico. Viene visualizzata l'Inspection Rule che influisce sulla direzione di traffico selezionata.

Nell'area Applicazioni verrà visualizzata una delle seguenti regole per il **traffico di origine**:

- l'Inspection Rule applicata in ingresso nell'interfaccia di provenienza, se presente;
- L'Inspection Rule applicata in uscita nell'interfaccia di destinazione, se la direzione in ingresso dell''interfaccia di provenienza non presenta alcuna Inspection Rule.

Cambia interfacce di provenienza e destinazione per trasferire altre regole nel menu Visualizza opzioni

Non sono visualizzate le Inspection Rule applicate al **traffico di ritorno**. È possibile visualizzare una delle Inspection Rule applicate al **traffico di ritorno** selezionando **Cambia interfaccia di provenienza e destinazione** nel menu Visualizza opzione. Nella finestra Protezione applicazioni delle attività Firewall e ACL è anche possibile vedere le Inspection Rule non visualizzate nella finestra Modifica ACL/Criterio firewall.

⚠	Questa icona viene visualizzata quando sono presenti due Inspection Rule nella direzione di traffico selezionata. Cisco SDM visualizza inoltre un messaggio di avviso, fornendo la possibilità di dissociare una delle Inspection Rule dall'interfaccia.

Controlli dell'area Applicazioni

Di seguito viene riportato l'elenco dei controlli dell'area Applicazioni.

Aggiungi: consente di aggiungere una Inspection Rule. Se non è presente alcuna Inspection Rule, è possibile aggiungere l'Inspection Rule predefinita Cisco SDM oppure crearne una personalizzata e aggiungerla. Se si aggiunge l'Inspection Rule predefinita Cisco SDM al flusso di traffico, questa verrà associata con il traffico in ingresso all'interfaccia di provenienza. È possibile aggiungere una voce per una specifica applicazione anche se è già presente un'Inspection Rule.

Modifica: Consente di modificare una voce selezionata.

Elimina: consente di eliminare la voce selezionata.

Impostazioni globali: consente di visualizzare una finestra di dialogo in cui è possibile impostare i timeout e le soglie globali.

Riepilogo: consente di visualizzare il nome e la descrizione dell'applicazione o del protocollo di ciascuna voce.

Dettagli: consente di visualizzare il nome, la descrizione dell'applicazione o del protocollo, lo stato avvisi, lo stato registrazione controllo e le impostazioni di timeout di ciascuna voce.

Campi voci area applicazioni

Nell'elenco seguente vengono descritti i campi delle voci relative all'area Applicazioni.

Protocollo applicazione: visualizza il nome dell'applicazione o protocollo. Ad esempio, **vdolive**.

Avviso: indica se un avviso è attivato (impostazione predefinita) o disattivato.

Registrazione controllo: indica se la registrazione controllo è attivata o disattivata (impostazione predefinita).

Timeout: visualizza il Tempo di attesa del router prima di bloccare il traffico di ritorno per questo protocollo o applicazione.

Descrizione: visualizza una breve descrizione. Ad esempio, **protocollo VDOLive**.

Per tornare alla descrizione della finestra Criterio firewall principale vedere Modifica ACL/criterio firewall.

Aggiungi applicazione *nome-applicazione*

Utilizzare questa finestra per aggiungere una voce di applicazione che si desidera controllare tramite il firewall Cisco IOS.

Azione avviso

Scegliere una opzioni seguenti:

- **default-on**: lasciare come predefinito. Il valore predefinito è **on**.
- **on**: attivare avviso.
- **off**: disattivare avviso.

Azione controllo

Scegliere una opzioni seguenti:

- **default-off**: lasciare come predefinito. Il valore predefinito è **off**.
- **on**: attivare registrazione controllo.
- **off**: disattivare registrazione controllo.

Timeout

Specificare per quanto tempo il router deve restare in attesa prima di bloccare il traffico di ritorno per questo protocollo o applicazione. Nel campo è specificato il valore predefinito per il protocollo o per l'applicazione

Aggiungi applicazione RPC

Aggiungere un numero di programma RPC in questa finestra e specificare le impostazioni dell'ora di avviso, di controllo, di timeout e di attesa.

Azione avviso

Scegliere una opzioni seguenti:

- **default-on**: lasciare come predefinito. Il valore predefinito è **on**.
- **on**: attivare avviso.
- **off**: disattivare avviso.

Azione controllo

Scegliere una opzioni seguenti:

- **default-off**: lasciare come predefinito. Il valore predefinito è **off**.
- **on**: attivare registrazione controllo.
- **off**: disattivare registrazione controllo.

Timeout

Specificare per quanto tempo il router deve restare in attesa prima di bloccare il traffico di ritorno per questo protocollo o applicazione. Nel campo è specificato il valore predefinito.

Numero del programma

Immettere un unico numero di programma in questo campo.

Tempo di attesa

È possibile specificare per quanti minuti consentire le connessioni RPC successive dalla stessa origine verso lo stesso indirizzo o porta di destinazione. Il tempo di attesa predefinito è di zero minuti.

Aggiungi applicazione frammento

In questa finestra è possibile aggiungere una voce di frammento a un'Inspection Rule in fase di configurazione nella finestra Modifica ACL/Criterio firewall. È inoltre possibile specificare le impostazioni di avviso, controllo e timeout. Tramite una voce di frammento si può impostare il numero massimo di pacchetti non riassemblati che il router deve accettare prima di eliminarli.

Azione avviso

Scegliere una opzioni seguenti:

- **default(on)**: lasciare come predefinito. Il valore predefinito è **on**.
- **on**: attivare avviso.
- **off**: disattivare avviso.

Azione controllo

Scegliere una opzioni seguenti:

- **default(off)**: lasciare come predefinito. Il valore predefinito è **off**.
- **on**: attivare registrazione controllo.
- **off**: disattivare registrazione controllo.

Timeout

Specificare per quanto tempo il router deve restare in attesa prima di bloccare il traffico di ritorno per questo protocollo o applicazione. Nel campo è specificato il valore predefinito.

Intervallo (opzionale)

Immettere il numero massimo di pacchetti non riassemblati che il router deve accettare prima di eliminarli. L'intervallo può essere compreso tra 50 e 10000.

Aggiungi o Modifica applicazione HTTP

Utilizzare questa finestra per aggiungere un'applicazione HTTP all'Inspection Rule.

Azione avviso

Scegliere una opzioni seguenti:

- **default-on**: lasciare come predefinito. Il valore predefinito è **on**.
- **on**: attivare avviso.
- **off**: disattivare avviso.

Azione controllo

Scegliere una opzioni seguenti:

- **default-off**: lasciare come predefinito. Il valore predefinito è **off**.
- **on**: attivare registrazione controllo.
- **off**: disattivare registrazione controllo.

Timeout

Specificare per quanto tempo il router deve restare in attesa prima di bloccare il traffico di ritorno per questo protocollo o applicazione. Nel campo è specificato il valore predefinito.

Host/rete per il download dell'applet Java

Si tratta di host e reti di origine di cui si deve verificare il traffico associato agli applet. È possibile specificare diversi host e reti.

Fare clic su **Aggiungi** per visualizzare la finestra Blocco applet Java nella quale è possibile specificare un host o una rete.

Fare clic su **Elimina** per rimuovere una voce dall'elenco.

Blocco applet Java

Utilizzare questa finestra per specificare se consentire o negare gli applet Java di un host o di una rete specifica.

Azione

Scegliere una opzioni seguenti:

- **Non bloccare (Consenti)**: consentire gli applet Java da questa rete o host.
- **Blocca (Nega)**: negare gli applet Java da questa rete o host.

Host/rete

Specificare la rete o l'host.

Tipo

Scegliere una opzioni seguenti:

- **Una rete**: mediante la selezione di questa opzione, viene fornito un indirizzo di rete nel campo dell'indirizzo IP. La maschera carattere jolly consente di immettere un numero di rete corrispondente a più subnet.
- **Un nome host o indirizzo IP**: mediante la selezione di questa opzione, viene fornito un indirizzo IP host o un nome host nel campo successivo.
- **Qualsiasi indirizzo IP**: selezionando questa opzione, l'azione specificata viene applicata a qualsiasi host o rete.

Indirizzo IP/Maschera carattere jolly

Immettere un indirizzo di rete, quindi la maschera carattere jolly per specificare la parte dell'indirizzo di rete che deve corrispondere esattamente.

Ad esempio, se sono stati immessi un indirizzo di rete di 10.25.29.0 e una maschera carattere jolly di 0.0.0.255, verrà filtrato qualsiasi applet Java con un indirizzo di origine contenente 10.25.29. Se la maschera carattere jolly fosse 0.0.255.255, verrebbe filtrato qualsiasi applet Java con un indirizzo di origine contenente 10.25.

IP/Nome host

Questo campo viene visualizzato se è stata selezionata l'opzione **Un nome host o indirizzo IP** come Tipo. Se si immette un nome host, è necessario un server DNS nella rete che possa risolvere il nome host in un indirizzo IP.

Avviso Cisco SDM: Inspection Rule

Questa finestra viene visualizzata quando tramite Cisco SDM vengono rilevate due Inspection Rule configurate per una direzione in un flusso di traffico. Ad esempio, è possibile applicare un'Inspection Rule al traffico in ingresso dall'interfaccia di provenienza e un'altra al traffico in uscita sull'interfaccia di destinazione. Due Inspection Rule non danneggiano il funzionamento del router, tuttavia possono risultare non necessarie. Cisco SDM consente di mantenere lo stato originale delle Inspection Rule e di eliminarle dall'interfaccia di provenienza o di destinazione.

- **Non effettuare modifiche**: Cisco SDM non consentirà l'eliminazione di alcuna Inspection Rule.
- **Mantenere il *nome* della Inspection Rule del** <nome-interfaccia> **in ingresso e dissociare il *nome* della Inspection Rule del**<nome-interfaccia> **in uscita**: Cisco SDM consentirà di mantenere una sola Inspection Rule e di dissociare la regola dall'altra interfaccia.
- **Mantenere il *nome* della Inspection Rule del** <nome-interfaccia> **in uscita e dissociare il *nome* della Inspection Rule del**<nome-interfaccia> **in ingresso**: Cisco SDM consentirà di mantenere una sola Inspection Rule e di dissociare la regola dall'altra interfaccia.

Prima di selezionare e fare clic su **OK**, è possibile fare clic su **Annulla** per stabilire se è necessario aggiungere delle voci all'Inspection Rule da conservare. Si possono aggiungere delle voci utilizzando il pulsante **Aggiungi** nella barra degli strumenti dell'area Applicazione nella finestra Modifica ACL/Criterio firewall.

Avviso Cisco SDM: Firewall

Facendo clic su **Applica firewall** nella finestra Modifica ACL/criterio firewall viene visualizzata la finestra. in cui è disponibile l'elenco delle interfacce alle quali si applica una regola e la descrizione della regola stessa.

Esempio:

```
SDM applica la configurazione del firewall alle interfacce seguenti:
Interfaccia interna (trusted) FastEthernet 0/0
* Applicare l'Inspection Rule predefinita SDM in ingresso
* Applicare ACL in ingresso. (Antispoofing, broadcast, local loopback
e così via).

Interfaccia esterna (untrusted) Serial 1/0
* Applicare l'elenco di accesso in ingresso per impedire il traffico
di ritorno.
```

Fare clic su **OK** per accettare le modifiche oppure su **Annulla** per interrompere l'applicazione del firewall.

Modifica criterio firewall

Nella finestra Modifica criterio firewall viene fornita la vista grafica dei criteri firewall presenti nel router; è possibile aggiungere ACL ai criteri senza chiuderla. Leggere le procedure nei paragrafi che seguono per informazioni su come visualizzare le informazioni di questa finestra e aggiungere regole.

Operazioni preliminari alla visualizzazione di informazioni in questa finestra

Se non è stata configurata alcuna zona, coppia di zone o Mappa criteri, tale finestra risulta vuota. Creare una configurazione di base contenente questi elementi andando a **Configura > firewall e ACL > Crea firewall** e completando la configurazione guidata avanzata del firewall. Dopo questa operazione, è possibile creare zone, coppie di zone e criteri in base alle proprie esigenze andando a **Configura > Attività aggiuntive > Zone** per configurare le zone e a **Attività aggiuntive > Coppie di zone** per configurare altre coppie di zone. Per creare le mappe criteri che dovranno essere utilizzate dalle coppie di zone, andare a **Configura > Attività aggiuntive > C3PL**. Fare clic sul ramo **Mappa criteri** per visualizzare i rami aggiuntivi che consentono di creare le mappe criteri e le mappe classi che definiscono il traffico delle mappe criteri.

Espansione e compressione della visualizzazione di un criterio

Quando la visualizzazione di un criterio viene compressa, restano visibili solo il nome del criterio e le zone di origine e destinazione. Per espandere la visualizzazione del criterio in modo da visualizzare le regole che compongono il criterio, fare clic sul pulsante **+** a sinistra del nome del criterio. La vista espansa di un criterio firewall potrebbe avere un aspetto simile al seguente.

		Classificazione traffico			**Azione**	**Opzioni regola**
	ID	**Origine**	**Destinazione**	**Servizio**		
	criterio client-server (da client a server)					
	1	any	any	tcp	Consenti firewall	
				udp		
				icmp		
	2	Traffico senza corrispondenza			Elimina	

Il criterio denominato criterio client-server contiene due ACL. La regola con ID 1 consente il traffico TCP, UDP e ICMP da qualunque origine a qualunque destinazione. La regola con ID 2 elimina qualsiasi traffico privo di corrispondenza.

Aggiunta di una nuova regola a un criterio.

Per aggiungere una nuova regola a un criterio, completare le seguenti operazioni:

Passo 1 Fare clic in un punto qualsiasi per tale criterio, quindi fare clic sul pulsante **+ Aggiungi**.

- Per inserire una regola per nuovo traffico nell'ordine desiderato, selezionare una regola esistente, fare clic sul pulsante **+ Aggiungi** e scegliere **Inserisci** o **Inserisci dopo**. Le opzioni Inserisci e Inserisci dopo sono disponibili anche da un menu di scelta rapida visualizzato facendo clic con il pulsante destro del mouse su una regola esistente.

- Scegliendo **Regola nuovo traffico** la nuova regola viene automaticamente posta all'inizio dell'elenco.
- Scegliendo **Regola traffico esistente** è possibile selezionare una mappa classi esistente e modificarla. La nuova regola viene automaticamente posta all'inizio dell'elenco.

Passo 2 Completare la finestra di dialogo visualizzata. Per maggiori informazioni fare clic su Aggiungi regola.

Riordinamento delle regole all'interno di un criterio

Se un criterio contiene più regole che consentono il traffico, è possibile riordinarle selezionando una regola e facendo clic sul pulsante **Sposta su** o sul pulsante **Sposta giù**. Se è stata selezionata una regola che è già all'inizio dell'elenco o se è stata selezionata la regola Traffico senza corrispondenza, il pulsante Sposta su è disattivato. Se è stata selezionata una regola che è già alla fine dell'elenco, il pulsante Sposta giù è disattivato.

Per riordinare le regole è anche possibile utilizzare i pulsanti Taglia e Incolla. Per rimuovere una regola dalla sua posizione corrente, selezionarla e fare clic su **Taglia**. Per inserire la regola in una nuova posizione, selezionare una regola esistente, fare clic su **Incolla**, quindi scegliere **Incolla** o **Incolla dopo**.

Le operazioni Sposta su, Sposta giù, Taglia, Incolla e Incolla dopo sono disponibili anche dal menu di scelta rapida visualizzato facendo clic su una regola con il pulsante destro del mouse.

Copiare e incollare una regola

Copiare e incollare una regola è molto utile se un criterio contiene una regola utilizzabile con modifiche limitate o senza alcuna modifica in un altro criterio.

Per copiare una regola, selezionarla e fare clic sul pulsante **Copia** oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Copia**. Per incollare la regola in una nuova posizione, fare clic su **Incolla**, quindi scegliere **Incolla** o **Incolla dopo**. I pulsanti Incolla e Incolla dopo sono disponibili anche nel menu di scelta rapida. Quando si incolla una regola in una nuova posizione, viene visualizzata la finestra di dialogo Aggiungi regola che consente di apportare modifiche alla regola, se necessario.

Visualizzazione del diagramma di flusso della regola

Fare clic in un punto qualsiasi di un criterio firewall, quindi fare clic su Diagramma di flusso regola per visualizzare il Diagramma di flusso regola per tale criterio. Il Diagramma di flusso regola visualizza la zona di origine a destra dell'icona del router, quella di destinazione a sinistra dell'icona.

Applicazione delle modifiche

Per inviare le modifiche al router, fare clic su **Applica modifiche** nella parte inferiore dello schermo.

Annullamento delle modifiche

Per annullare le modifiche apportate ma non inviate al router, fare clic su **Annulla modifiche** nella parte inferiore dello schermo.

Aggiungi regola

Nella finestra Aggiungi regola è possibile definire un flusso di traffico e specificare i protocolli da verificare. Per aggiungere una nuova regola, completare le seguenti operazioni:

Passo 1 Nel campo Origine e destinazione, specificare che il traffico scorre tra due reti selezionando **Rete** o che il traffico scorre tra entità che possono essere reti o singoli host, selezionando **Qualsiasi**.

Passo 2 Immettere il nome del flusso di traffico nel campo Nome traffico.

Passo 3 Fare clic su **Aggiungi** accanto alle colonne Rete di origine e Rete di destinazione, quindi aggiungere gli indirizzi della rete di origine e di destinazione. È possibile aggiungere più voci per le reti di origine e di destinazione, oltre che modificare una voce esistente selezionandola e facendo clic su **Modifica**.

Passo 4 Se necessario, è possibile riordinare una voce selezionandola e facendo clic su **Sposta su** o su **Sposta giù**. Se la voce selezionata è già all'inizio dell'elenco, il pulsante Sposta su è disattivato. Se la voce selezionata è già alla fine dell'elenco, il pulsante Sposta giù è disattivato.

Passo 5 Immettere un nome che descrive i protocolli o i servizi identificati per la verifica nel campo Nome servizio.

Passo 6 È possibile aggiungere un servizio facendo clic su un ramo della struttura della colonna di sinistra, scegliendo un servizio e facendo clic su **Aggiungi>>**. Fare clic sull'icona **+** accanto a un ramo per visualizzare i servizi disponibili di tale tipo. Per rimuovere un servizio dalla colonna di destra, selezionarlo e fare clic su **<<Rimuovi**.

Passo 7 Specificare la gestione del traffico desiderata scegliendo **Consenti firewall**, **Consenti ACL** o **Elimina** nel campo Azione. Se si sceglie **Consenti firewall**, è possibile fare clic su Avanzate e scegliere una voce di menu se si desidera definire ulteriormente l'azione, ad esempio ispezionando i protocolli scelti nella casella dei servizi. Per ulteriori informazioni, vedere gli argomenti della Guida riportati di seguito.

- Verifica di applicazione
- URL Filtering
- Qualità del servizio (QoS)
- Verifica parametro

Passo 8 Se si seleziona l'azione **Elimina**, è possibile fare clic su **Registra** per registrare l'evento.

Passo 9 Fare clic su OK per chiudere questa finestra di dialogo e inviare le modifiche al router.

Aggiungi traffico

Utilizzare la finestra di dialogo Aggiungi traffico per creare una voce di indirizzo di origine e di destinazione per una regola.

Azione

Utilizzare l'opzione Includi o Escludi per specificare se si desidera che la regola sia applicata al traffico scambiato tra gli indirizzi di origine e di destinazione.

Scegliere **Includi** per includere questo traffico nella regola.

Scegliere **Escludi** per escludere questo traffico dalla regola.

Host/rete di origine e di destinazione

Specificare l'origine e la destinazione del traffico in questi campi.

Tipo

Scegliere una delle seguenti opzioni:

- Qualsiasi indirizzo IP: scegliere se non si desidera limitare il traffico di origine o di destinazione a qualsiasi host o rete.
- Una rete: scegliere se si desidera specificare un indirizzo di rete come origine o destinazione e specificare l'indirizzo di rete nei campi Indirizzo IP e Maschera carattere jolly.
- Un nome host o indirizzo IP: scegliere se si desidera specificare il nome o l'indirizzo IP di un host. Specificare quindi l'host nel campo IP/Nome host.

Indirizzo IP

Immettere l'indirizzo di rete. Questo campo viene visualizzato quando nel campo Tipo è stato scelto **Una rete**.

Maschera carattere jolly

Immettere la maschera caratteri jolly che specifica i bit utilizzati per l'indirizzo di rete. Se, ad esempio, l'indirizzo di rete è 192.168.3.0, specificare la maschera 0.0.0.255. Questo campo viene visualizzato quando nel campo Tipo è stato scelto **Una rete**.

IP/Nome host

Immettere il nome o l'indirizzo IP di un host in questo campo. Se viene immesso un nome, il router deve essere in grado di contattare un server DNS al fine di risolvere il nome in un indirizzo IP. Questo campo viene visualizzato quando si seleziona Un nome host o Indirizzo IP nel campo Tipo.

Verifica di applicazione

È possibile configurare la verifica approfondita dei pacchetti per le applicazioni o i protocolli elencati in questa schermata selezionando la casella accanto all'applicazione o al protocollo, facendo clic sul pulsante a destra del campo e scegliendo **Crea** o **Seleziona** dal menu di scelta rapida. Scegliere **Crea** per configurare una nuova mappa criteri. Scegliere **Seleziona** per applicare al traffico una mappa criteri esistente. Al termine, nel campo viene visualizzato il nome della mappa criteri.

Ad esempio, per creare una nuova mappa criteri per Instant Messaging, selezionare la casella accanto a IM, fare clic sul pulsante accanto al campo IM e scegliere **Crea**. Creare quindi la mappa criteri nella finestra di dialogo Configura verifica approfondita pacchetti.

URL Filtering

È possibile aggiungere un filtro URL selezionandone uno esistente nell'elenco Nome URL Filtering oppure facendo clic su **Crea nuovo** e creando un nuovo filtro URL nelle finestre di dialogo visualizzate. Le impostazioni del filtro URL selezionato o creato vengono riepilogate in questa finestra di dialogo.

Qualità del servizio (QoS)

È possibile eliminare il traffico che supera una determinata velocità per secondo, la Police Rate, e quello che supera un Burst Value specificato. Il valore di Police Rate deve essere compreso tra 8.000 e 2.000.000.000 bps. Il burst rate deve essere compreso tra 1.000 e 512.000.000 byte.

Verifica parametro

È possibile specificare una mappa parametri esistente nella finestra Verifica parametro scegliendo una mappa parametri nell'elenco Verifica mappa parametri oppure fare clic su **Crea nuova** per creare una nuova mappa parametri da applicare alla regola per il criterio che si sta modificando. I dettagli della mappa parametri specificati sono visualizzati nel riquadro di anteprima.

Per ulteriori informazioni sulle mappe parametri, fare clic su Timeout e soglie per Verifica mappe parametri e CBAC.

Seleziona traffico

È possibile selezionare una mappa di classi che specifica il traffico da aggiungere al criterio. Per visualizzare ulteriori informazioni su una particolare mappa classi, selezionare la mappa classi e fare clic su **Visualizza dettagli**.

Quando si fa clic su **OK**, viene visualizzata la finestra di dialogo Aggiungi nuova regola, con le informazioni della mappa classi scelta. È possibile apportare ulteriori modifiche alla mappa classi o lasciarla invariata. Se si apportano modifiche, è possibile cambiare il nome della mappa classi se non si desidera che le modifiche si applichino ad altri criteri che utilizzano la mappa classi originale.

Elimina regola

Questa finestra di dialogo viene visualizzata quando si elimina una regola contenente una mappa classi o ACL che si potrebbe voler eliminare insieme alla regola o mantenere per usarla in altre regole.

Elimina automaticamente le mappe classi e le ACL utilizzate da questa regola

Fare clic su questa opzione per rimuovere le mappe classi e le ACL che fanno parte di questa regola. Saranno rimosse dalla configurazione del router e non saranno utilizzabili da altre regole.

Eliminerò le mappe classi e le ACL inutilizzate più tardi

Fare clic su questa opzione per rimuovere la regola mantenendo però le mappe classi e le ACL. Queste possono essere conservate per utilizzarle in altre parti della configurazione del firewall.

Visualizza dettagli

Fare clic sul pulsante **Visualizza dettagli** per visualizzare i nomi delle mappe classi e delle ACL associate alla regola che si sta eliminando. La finestra di dialogo si espande per mostrare i dettagli. Quando si fa clic su Visualizza dettagli, il nome del pulsante diventa Nascondi dettagli.

Nascondi dettagli

Fare clic su **Nascondi dettagli** per chiudere la parte della finestra di dialogo relativa ai dettagli. Quando si fa clic su Nascondi dettagli, il nome del pulsante diventa Visualizza dettagli.

Eliminazione manuale delle mappe classi

Per eliminare manualmente una mappa classi, effettuare le seguenti operazioni.

Passo 1 Andare a **Configura > Attività aggiuntive > C3PL > Mappa classi**.

Passo 2 Fare clic sul nodo relativo al tipo di mappa classi da eliminare.

Passo 3 Selezionare il nome della mappa classi visualizzata nella finestra Visualizza dettagli, quindi fare clic su **Elimina**.

Eliminazione manuale degli ACL

Per eliminare manualmente un ACL, effettuare le seguenti operazioni:

Passo 1 Andare a **Configura > Attività aggiuntive > Editor ACL**.

Passo 2 Fare clic sul nodo relativo all'ACL da eliminare.

Passo 3 Selezionare il nome o il numero dell'ACL visualizzato nella finestra Visualizza dettagli, quindi fare clic su **Elimina**.

CAPITOLO 8

Protezione applicazioni

La Protezione applicazioni consente di creare criteri di protezione che si applicano all'uso della rete e delle applicazioni web. Si possono applicare i criteri creati a interfacce specifiche, clonare criteri esistenti in modo da sfruttarne le impostazioni per nuovi criteri, e rimuovere criteri dal router.

In questo capitolo sono contenute le seguenti sezioni:

Le finestre di Protezione applicazioni

I comandi che si trovano nelle finestre Protezione applicazioni consentono di associare i criteri alle interfacce, definire impostazioni globali e aggiungere, cancellare e clonare criteri di protezione delle applicazioni. I cassetti della protezione applicazioni consentono di portarsi rapidamente nell'area di protezione applicazioni in cui si devono effettuare modifiche.

Elenco nomi criterio

Selezionare in questo elenco il criterio che si vuole modificare. Se non sono stati già configurati dei criteri, l'elenco risulta vuoto e nella finestra Protezione applicazioni viene visualizzato un messaggio che indica che sul router non sono disponibili criteri. Per creare un criterio, fare clic sul pulsante **Azione** e scegliere **Aggiungi**.

Pulsanti di Protezione applicazioni

- **Azione**: fare clic su questo pulsante per aggiungere un criterio oppure per eliminare o clonare il criterio prescelto. Se sul router non sono presenti criteri già configurati, è disponibile soltanto l'azione **Aggiungi**.
- **Associa**: fare clic su questo pulsante per visualizzare una finestra di dialogo che consente di associare il criterio a un'interfaccia. Mediante tale finestra di dialogo è possibile scegliere l'interfaccia e specificare la direzione del traffico a cui applicare il criterio.
- **Impostazioni globali**: fare clic su questo pulsante per impostare i valori di timeout e soglia da applicare a tutti i criteri. Fare clic su Impostazioni globali per maggiori informazioni.

Cassetto e-mail

Fare clic per apportare modifiche alle impostazioni di protezione delle applicazioni e-mail. Per maggiori informazioni fare clic su E-mail.

Cassetto Instant Messaging (IM)

Fare clic per apportare modifiche alle impostazioni di protezione per Yahoo Messenger, MSN Messenger e altre applicazioni di messaggistica istantanea. Per maggiori informazioni fare clic su Instant Messaging.

Cassetto peer-to-peer

Fare clic per apportare modifiche alle impostazioni di protezione per KaZa A, eDonkey e altre applicazioni peer-to-peer. Per maggiori informazioni fare clic su Applicazioni/Protocolli.

Cassetto URL Filtering

Fare clic per aggiungere un elenco di URL che si desidera venga filtrato da un criterio di protezione dell'applicazione. È inoltre possibile aggiungere server di filtri.

Cassetto HTTP

Fare clic per apportare modifiche alle impostazioni di protezione HTTP. Per maggiori informazioni fare clic su HTTP.

Cassetto applicazioni/protocolli

Fare clic per apportare modifiche alle impostazioni di protezione di altre applicazioni e protocolli. Per maggiori informazioni fare clic su Applicazioni/Protocolli.

Nessun criterio di Protezione applicazioni

Questa finestra viene visualizzata da Cisco SDM quando si seleziona la scheda **Protezione applicazioni** ma sul router non sono stati configurati criteri di protezione per le applicazioni. Da questa finestra è possibile creare un criterio e visualizzare le impostazioni globali che forniscono i valori predefiniti dei parametri impostabili quando si creano i criteri.

Nome criterio

Il campo è vuoto quando non sono stati configurati criteri sul router. Scegliendo Aggiungi dal menu contestuale Azione si può creare un nome criterio e cominciare ad designare le impostazioni del criterio.

Azione

Se sul router non sono stati configurati criteri, è possibile scegliere **Aggiungi** dal menu contestuale per creare un criterio. Una volta configurato un criterio, sono disponibili ulteriori azioni: **Modifica** ed **Elimina**.

Associa

Se non sono stati configurati criteri, il pulsante è disattivato. Quando viene creato un criterio, fare clic su questo pulsante per associare il criterio a un'interfaccia. Per maggiori informazioni vedere la sezione Associa criterio a un'interfaccia.

Impostazioni globali

Le Impostazioni globali forniscono i valori predefiniti di timeout, delle soglie e di altri parametri dei criteri. Per ciascun parametro in Cisco SDM sono previsti valori predefiniti che possono essere modificati in modo da definire nuovi valori predefiniti da applicare in mancanza di valori specifici per le singole applicazioni o i singoli protocolli. Quando si crea un criterio è possibile accettare il valore predefinito di un determinato parametro oppure scegliere un'altra impostazione. Poiché le finestre di configurazione della Protezione applicazioni non visualizzano i valori predefiniti, per poterli vedere nella finestra Timeout e soglie globali si deve fare clic su questo pulsante. Per maggiori informazioni vedere la sezione Timeout e soglie per Verifica mappe parametri e CBAC.

E-mail

Specificare in questa finestra le applicazioni e-mail che si vogliono controllare. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Pulsante Modifica

Fare clic per modificare le impostazioni per l'applicazione prescelta. Le impostazioni create dall'utente hanno la precedenza sulle impostazioni globali configurate sul router.

Colonna applicazioni

Il nome dell'applicazione e-mail, ad esempio *bliff*, *esmtp* e *smtp*. Per modificare le impostazioni di un'applicazione, selezionare la casella situata a sinistra del nome dell'applicazione, quindi fare clic su **Modifica**.

Colonne Avvisi, Controllo e Timeout

Queste colonne visualizzano i valori esplicitamente impostati per un'applicazione. Se un'impostazione non è stata modificata per un'applicazione, la colonna è vuota. Ad esempio, se si è attivata la verifica dell'applicazione bliff, ma non sono state apportate modifiche alle impostazioni degli avvisi o del timeout, il valore *on* viene visualizzato nella colonna **Controllo** mentre le colonne **Avviso** e **Timeout** restano vuote.

Colonna Opzioni

Questa colonna può contenere campi se per l'applicazione prescelta sono disponibili altre impostazioni.

Campo MAX dati

Specifica il numero massimo di byte (dati) che possono essere trasferiti in una sessione SMTP (Simple Mail Transport Protocol). Quando si supera il valore massimo, il firewall scrive un messaggio d'avviso nel registro e chiude la sessione. Valore di default: 20 MB.

Casella di controllo Accesso protetto

Fa sì che sulle locazioni non protette venga utilizzata la crittografia per l'autenticazione.

Reimposta

Ripristina lo stato iniziale della connessione TCP se il cliente immette un comando non di protocollo prima del completamento dell'autenticazione.

Traffico router

Abilita l'ispezione del traffico destinato a o originato da un router. Applicabile solo ai protocolli H.323, TCP, e UDP.

Instant Messaging

Usare questa finestra per controllare il traffico per le applicazioni di messaggistica istantanea (IM) come Yahoo Messenger e MSN Messenger. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Fare clic su Comandi Consenti, Blocca e Allarme per informazioni su come specificare l'azione che il router deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Il seguente esempio illustra un blocco del traffico di Yahoo Messenger con generazione di allarmi all'arrivo di traffico per tale applicazione:

```
Yahoo Messenger        Blocca          Invia allarme (selezionato)
```

Il profilo SDM_HIGH blocca le applicazioni IM. Se il router usa il profilo SDM_HIGH e non blocca le applicazioni IM, tali applicazioni possono essere collegate mediante un nuovo server non specificato nel profilo. Per attivare il blocco di queste applicazioni sul router, selezionare la casella di controllo **Invia allarme** accanto alle applicazioni IM per visualizzare i nomi dei server da cui si connettono le applicazioni. Quindi utilizzare CLI per bloccare il traffico su questi server. Il seguente esempio usa il nome del server newserver.yahoo.com:

```
Router(config)# appfw nome criterio SDM_HIGH
Router(cfg-appfw-policy)# applicazione in yahoo
Router(cfg-appfw-policy-ymsgr)# server impedisce nome
newserver.yahoo.com Router(cfg-appfw-policy-ymsgr)# uscita
Router(cfg-appfw-policy)# uscita
Router(config)#
```

Nota

- Le applicazioni IM sono in grado di comunicare sia su porte di protocolli non native, come l'HTTP, sia mediante le porte di protocolli TCP e UDP native. Cisco SDM configura le azioni Blocco e Consenti sulla base della porta nativa dell'applicazione, e blocca sempre le comunicazioni condotte su porte HTTP.
- Alcune applicazioni IM, come MSN Messenger 7.0, usano le porte HTTP per impostazione predefinita. Per consentire l'uso di queste applicazioni, configurare l'applicazione IM in modo da utilizzare la porta nativa.

Applicazioni peer-to-peer

Questa pagina consente di creare le impostazioni dei criteri per applicazioni peer-to-peer, quali Gnutella, eDonkey e BitTorrent. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Fare clic su Comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Il seguente esempio illustra un blocco del traffico di BitTorrent con generazione di allarmi all'arrivo di traffico per tale applicazione:

Esempio 8-1 Blocco del traffico BitTorrent

```
BitTorrent              Blocco
```

Nota

- Le applicazioni peer-to-peer sono in grado di comunicare sia su porte di protocollo non native, come l'HTTP, sia mediante le porte dei loro protocolli TCP e UDP native. Cisco SDM configura le azioni Blocco e Consenti sulla base della porta nativa dell'applicazione, e blocca sempre le comunicazioni condotte su porte HTTP.
- I criteri protezione delle applicazioni non bloccheranno i file se questi saranno forniti da servizi a pagamento come altnet.com. I file scaricati dalle reti peer-to-peer invece vengono bloccati.

Filtri URL

URL Filtering consente di controllare l'accesso utenti ai siti Internet mediante gli elenchi di URL, in cui è possibile specificare se consentire o negare l'accesso a un URL. Includere le funzionalità di URL Filtering nel criterio di Protezione applicazioni facendo clic su **Attiva URL Filtering** in questa finestra.

Sul router è possibile configurare un elenco di URL locale da utilizzare per tutti i criteri di Protezione applicazioni. Gli elenchi di URL possono essere memorizzati anche sui server di URL Filtering ai quali il router può collegarsi. Le informazioni per questi server vengono salvate in un elenco di server di URL Filtering. Sul router è possibile configurare un elenco di server di URL Filtering da utilizzare per tutti i criteri di Protezione applicazioni.

In questa finestra è possibile gestire l'elenco di URL locale mediante i pulsanti **Aggiungi URL**, **Modifica URL** e **Importa elenco URL**. Poiché il software Cisco IOS consente di gestire questi elenchi con o senza un criterio di Protezione applicazioni configurato, tali elenchi possono essere gestiti anche mediante la finestra Attività aggiuntive.

Per informazioni sulla gestione di un elenco di URL locale, fare clic su Elenco URL locali.

Per informazioni sulla gestione dell'elenco di server di URL Filtering, fare clic su Server di URL Filtering.

Per informazioni sull'utilizzo di un elenco di URL locale assieme a elenchi di URL salvati su server di URL Filtering, fare clic su Precedenza di URL Filtering.

Per informazioni generali su URL Filtering, fare clic su Finestra URL Filtering.

HTTP

Specificare in questa finestra le impostazioni generali della verifica del traffico HTTP. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni fare clic su Le finestre di Protezione applicazioni.

Fare clic su Comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Per informazioni dettagliate sulla modalità di verifica del router per il traffico HTTP, consultare *Motore di verifica HTTP* al seguente collegamento:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455acb.html

Casella di controllo Rileva traffico HTTP non conforme

Selezionare questa casella se si desidera che Cisco SDM esamini il traffico HTTP dei pacchetti non conformi al protocollo HTTP. Utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Nota Il blocco del traffico HTTP non conforme può determinare l'interruzione del traffico ricevuto dai siti Web più noti che potrebbero non essere bloccati sulla base dei contenuti, qualora questi siti non siano conformi al protocollo HTTP.

Casella di controllo Rileva applicazioni di tunneling

Selezionare questa casella se si desidera che Cisco SDM esamini il traffico HTTP dei pacchetti generati dalle applicazioni di tunneling. Fare clic sui comandi Consenti, Blocca e Allarme per specificare l'azione che Cisco SDM deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Casella di controllo Imposta lunghezza URI massima

Selezionare questa casella se si desidera definire una lunghezza massima per gli URI (Universal Resource Indicators). Specificare la lunghezza massima in byte, quindi utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva un URL più lungo rispetto al valore impostato.

Casella di controllo Attiva verifica HTTP

Selezionare questa casella se si desidera che il router ispezioni il traffico HTTP. Per bloccare il traffico proveniente da applicazioni Java, è possibile specificare un filtro di blocco Java facendo clic sul pulsante... e specificando un'ACL esistente oppure creando una nuova ACL per la verifica di Java.

Casella di controllo Attiva verifica HTTPS

Selezionare questa casella se si desidera che il router ispezioni il traffico HTTPS.

Casella di controllo Imposta valore di timeout

Selezionare questa casella se si desidera impostare un limite di tempo per le sessioni HTTP e immettere un numero di secondi nel campo Timeout. Le sessioni attive per un tempo superiore saranno interrotte.

Attiva registrazione controllo

È possibile designare delle impostazioni di registrazione controllo CBAC da utilizzare in luogo di quelle nella finestra Timeout e soglie globali. Se si sceglie l'opzione **Predefinito**, viene utilizzata l'impostazione globale corrente. Se si sceglie l'opzione **Attivo**, si attiva esplicitamente la registrazione controllo CBAC per il traffico HTTP e HTTPS se è attiva la verifica HTTPS, con precedenza sull'impostazione globale di registrazione del controllo. Se si sceglie l'opzione **Disattivo**, si disattiva esplicitamente la registrazione controllo CBAC per il traffico HTTP e HTTPS se è attiva la verifica HTTPS, con precedenza sull'impostazione globale di registrazione del controllo.

Opzioni intestazione

È possibile far sì che il router consenta o neghi il traffico sulla base della lunghezza dell'intestazione HTTP e del metodo di richiesta contenuto nell'intestazione. I metodi di richiesta sono i comandi inviati ai server HTTP per l'acquisizione di URL, pagine web e l'esecuzione di altre azioni. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Casella di controllo Imposta lunghezza massima intestazione

Selezionare questa casella di controllo se si desidera che il router consenta o neghi il traffico sulla base della lunghezza dell'intestazione HTTP e specifichi la lunghezza massima delle intestazioni per la richiesta e la risposta. Utilizzare i comandi **Consenti**, **Blocca** e **Allarme** per specificare l'azione che il router deve attivare quando la lunghezza dell'intestazione supera tale valore.

Casella di controllo Configura metodo richiesta estensione

Se si desidera che il router consenta o neghi il traffico HTTP sulla base di un metodo di richiesta di estensione, selezionare la casella accanto a tale metodo di richiesta. Utilizzare i comandi **Consenti**, **Blocca** e **Allarme** per specificare l'azione che il router deve attivare quando rileva traffico che utilizza tale metodo di richiesta.

Caselle di controllo Configura metodo richiesta RFC

Se si desidera che il router consenta o neghi il traffico HTTP sulla base di uno dei metodi di richiesta HTTP specificati nella RFC 2616, *Hypertext Transfer Protocol-HTTP/1.1*, selezionare la casella accanto a tale metodo di richiesta. Utilizzare i comandi **Consenti**, **Blocca** e **Allarme** per specificare l'azione che il router deve attivare quando rileva traffico che utilizza tale metodo di richiesta.

Opzioni contenuto

È possibile far sì che il router esamini il contenuto del traffico HTTP e consenta o neghi il traffico e generi allarmi sulla base di quanto si desidera che venga controllato dal router. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Fare clic su Comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva traffico con le caratteristiche specificate in questa finestra.

Casella di controllo Verifica tipo di contenuto

Selezionare questa casella di controllo se si desidera che il router verifichi il contenuto dei pacchetti facendo corrispondere le risposte con le richieste, abilitando un allarme per i tipi di contenuto sconosciuto o utilizzando entrambi questi metodi. Utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando non è possibile accoppiare le richieste con le risposte e quando esso incontra un tipo di contenuto sconosciuto.

Casella di controllo Imposta lunghezza contenuto

Selezionare questa casella per impostare i valori minimo e massimo per la lunghezza dei dati di un pacchetto HTTP, e immettere tali valori negli appositi campi. Utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando la quantità di dati è inferiore al minimo o superiore al massimo consentito.

Casella di controllo Configura codifica trasferimento

Selezionare questa casella di controllo per far sì che il router verifichi il metodo di codifica dei dati nel pacchetto, quindi utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione che il router deve attivare quando rileva le codifiche indicate.

Casella di controllo Porzione

Il formato di codifica specificato nella RFC 2616, Hypertext Transfer Protocol-HTTP/1. Il corpo del messaggio viene trasferito in una serie di porzioni, in cui ciascuna porzione contiene un indicatore della propria dimensione.

Casella di controllo Comprimi

Il formato di codifica prodotto dall'utilità “compress” di UNIX.

Casella Deflate

Il formato “ZLIB” definito nella RFC 1950 “ZLIB Compressed Data Format Specification version 3.3”, combinato con l'algoritmo di compressione “deflate” descritto in RFC 1951 “DEFLATE Compressed Data Format Specification” versione 1.3.

Casella di controllo gzip

Il formato di codifica prodotto dal programma GNU zip (“gzip”).

Casella di controllo Identità

Codifica predefinita, che indica che non è stata eseguita alcuna codifica.

Applicazioni/Protocolli

Questa finestra consente di creare impostazioni dei criteri per applicazioni e protocolli non presenti in altre finestre. Per maggiori informazioni sui pulsanti e cassetti disponibili nella scheda Protezione applicazioni, fare clic su Le finestre di Protezione applicazioni.

Struttura ad albero Applicazioni/Protocolli

La struttura ad albero Applicazione/Protocolli consente di filtrare la lista sulla destra secondo il tipo di applicazioni e protocolli che si vogliono vedere. Scegliere prima il ramo del tipo generale che si vuole visualizzare. Il frame sulla destra visualizza le voci disponibili per il tipo scelto. Se alla sinistra di un ramo compare il segno più (+) sono presenti sottocategorie utilizzabili per migliorare il filtro. Fare clic sul segno + per espandere il ramo e selezionare la sottocategoria che si vuole visualizzare. Se l'elenco sulla destra è vuoto non ci sono applicazioni o protocolli disponibili per il tipo scelto. Per scegliere un'applicazione è possibile selezionare la casella accanto ad essa nella struttura, oppure selezionare la casella accanto ad essa nell'elenco.

Esempio: Se si desidera visualizzare tutte le applicazioni Cisco, fare clic sulla cartella del ramo **Applicazioni** e sulla cartella **Cisco**. Verranno visualizzate applicazioni come *clp*, *cisco-net-mgmt* e *cisco-sys*.

Pulsante Modifica

Fare clic su questo pulsante per modificare le impostazioni per l'applicazione prescelta. Le impostazioni qui effettuate hanno la precedenza sulle impostazioni globali configurate sul router.

Colonna applicazioni

Il nome dell'applicazione o protocollo, ad esempio *tcp*, *smtp o ms-sna*. Per modificare le impostazioni relative a un elemento, selezionare la casella situata a sinistra del nome dell'elemento e fare clic su **Modifica**.

Colonne Avvisi, Controllo e Timeout

In queste colonne vengono visualizzati i valori esplicitamente impostati per un elemento. Se per un elemento non viene modificata alcuna impostazione, la colonna è vuota. Ad esempio, se si è attivata la verifica dell'applicazione ms-sna, ma non sono state effettuate modifiche alle impostazioni degli avvisi o del timeout, il valore *on* viene visualizzato nella colonna **Controllo** mentre le colonne **Avviso** e **Timeout** restano vuote.

Colonna Opzioni

Questa colonna può contenere campi se sono disponibili altre impostazioni per l'elemento prescelto.

MAX Dati

Specifica il numero massimo di byte (dati) che possono essere trasferiti in una sessione SMTP (Simple Mail Transport Protocol). Quando si supera il valore massimo, il firewall scrive un messaggio d'avviso nel registro e chiude la sessione. Valore di default: 20 MB.

Accesso protetto

Fa sì che sulle locazioni non protette venga utilizzata la crittografia per l'autenticazione.

Reimposta

Ripristina lo stato iniziale della connessione TCP se il cliente immette un comando non di protocollo prima del completamento dell'autenticazione.

Traffico router

Abilita l'ispezione del traffico destinato a o originato da un router. Applicabile solo ai protocolli H.323, TCP, e UDP.

Timeout e soglie per Verifica mappe parametri e CBAC

Utilizzare queste informazioni per la creazione o la modifica di una mappa parametri per fini di verifica o per impostare le soglie e i timeout globali CBAC (Context-Based Access Control). utilizzati per determinare la durata della gestione delle informazioni sullo stato di una sessione e per determinare quando eliminare le sessioni non completamente disponibili. Questi timeout e soglie vengono applicati a tutte le sessioni.

I valori del timer globali possono essere specificati in secondi, minuti oppure ore.

Valore di timeout connessione TCP

Tempo di attesa per una connessione TCP da stabilire. Il valore predefinito è 30 secondi.

Attesa valore di timeout TCP FIN

Il periodo di tempo durante il quale una sessione TCP sarà ancora gestita dopo che è stato rilevato uno scambio FIN dal firewall. Il valore predefinito è 5 secondi.

Valore di timeout idle TCP

Il periodo di tempo durante il quale una sessione TCP sarà ancora gestita dopo che è stata rilevata un'assenza di attività dal firewall. Il valore predefinito è 3600 secondi.

Valore di timeout idle UDP

Il periodo di tempo durante il quale una sessione UDP (User Datagram Protocol) sarà ancora gestita dopo aver rilevato un'assenza di attività. Il valore predefinito è 30 secondi.

Valore di timeout DNS

Il periodo di tempo durante il quale una sessione DNS (Domain Name System) di ricerca del nome sarà ancora gestita dopo aver rilevato un'assenza di attività. Il valore predefinito è 5 secondi.

Soglie di attacchi DoS SYN Flooding

Un numero insolitamente elevato di sessioni semiaperte può indicare che è in atto un attacco DoS (Denial of Service). Le soglie di attacco DoS consentono al router di avviare l'eliminazione delle sessioni semiaperte una volta che tutte hanno raggiunto una soglia massima. Definendo le soglie, è possibile specificare il momento in cui il router può iniziare l'eliminazione delle sessioni semiaperte e quando invece interromperla.

Soglie sessione di un minuto. Questi campi consentono di specificare i valori della soglia per nuovi tentativi di connessione.

Inferiore	Interruzione dell'eliminazione di nuove connessioni dal momento in cui il numero di nuove connessioni è inferiore a questo valore. Il valore predefinito è 400 sessioni.
Superiore	Avvio eliminazione di nuove connessioni nel momento in cui il numero di nuove connessioni supera questo valore. Il valore predefinito è 500 sessioni.

Soglie massime per sessioni incomplete. Questi campi consentono di specificare i valori della soglia per il numero totale delle sessioni semiaperte esistenti.

Inferiore	Interruzione dell'eliminazione di nuove connessioni dal momento in cui il numero di nuove connessioni è inferiore a questo valore. Il valore predefinito è di 400 sessioni per le release di Cisco IOS precedenti alla 12.4(11)T. Se non viene esplicitamente impostato un valore Inferiore, Cisco IOS interrompe l'eliminazione delle nuove sessioni quando il numero di sessioni scende a 400. Per Cisco IOS release 12.4(11)T e successive, il valore predefinito è illimitato. Se non viene esplicitamente impostato un valore Inferiore, Cisco IOS non interrompe l'eliminazione delle nuove connessioni.
Superiore	Avvio eliminazione di nuove connessioni nel momento in cui il numero di nuove connessioni supera questo valore. Il valore predefinito è di 500 sessioni per le release di Cisco IOS precedenti alla 12.4(11)T. Se non viene esplicitamente impostato un valore Superiore, Cisco IOS avvia l'eliminazione delle sessioni quando viene stabilito un numero di sessioni maggiore di 500. Per Cisco IOS release 12.4(11)T e successive, il valore predefinito è illimitato. Se non viene esplicitamente impostato un valore Superiore, Cisco IOS non avvia l'eliminazione delle nuove connessioni.

TCP massimo di sessioni incomplete per host:

Con il router viene avviata l'eliminazione delle sessioni semiaperte per lo stesso host quando il numero totale dell'host supera questo valore. Il valore predefinito è 50. Se si seleziona il campo **Ora di blocco** e si immette un valore, il router continuerà a bloccare le nuove connessioni per questo host per il numero di minuti specificati.

Attiva controllo globale

Selezionare questa casella per attivare i messaggi di registrazione controllo CBAC per tutti i tipi di traffico.

Attiva avviso globale

Selezionare questa casella per attivare i messaggi di avviso CBAC per tutti i tipi di traffico.

Associa criterio a un'interfaccia

In questa finestra, selezionare l'interfaccia su cui si vuole applicare il criterio selezionato. Specificare anche se il criterio è da applicare per il traffico in ingresso, per il traffico in uscita o per il traffico nelle due direzioni.

Ad esempio, se il router dispone di interfacce FastEthernet 0/0 e FastEthernet 0/1 e si desidera applicare il criterio all'interfaccia FastEthernet 0/1, sul traffico nelle due direzioni, selezionare la casella di controllo accanto a FastEthernet 0/1, quindi selezionare le caselle nelle colonne In ingresso e In uscita. Affinché venga controllato solo il traffico in ingresso, selezionare la sola casella di controllo nella colonna In ingresso.

Modifica Inspection Rule

Usare questa finestra per specificare le impostazioni della regola di controllo personalizzata per un'applicazione. Le impostazioni qui effettuate e applicate sulla configurazione del router hanno la precedenza sulle impostazioni globali.

Fare clic sul pulsante **Impostazioni globali** nella finestra Protezione applicazioni, per visualizzare le impostazioni globali per i parametri che si possono impostare in questa finestra. Per maggiori informazioni vedere la sezione Timeout e soglie per Verifica mappe parametri e CBAC.

Campo Avviso

Scegliere una delle seguenti opzioni:

- **predefinito**: utilizzare l'impostazione globale per gli avvisi.
- **attivo**: generare un avviso quando si incontra traffico di questo tipo.
- **disattivo**: non generare un avviso quando si incontra traffico di questo tipo.

Campo di auditing

Scegliere una delle seguenti opzioni:

- **predefinito**: utilizzare le impostazioni globali per la registrazione di controllo.
- **attivo**: generare una registrazione di controllo quando si incontra traffico di questo tipo.
- **disattivo**: non generare una registrazione di controllo quando si incontra traffico di questo tipo.

Campo Timeout

Immettere il numero di secondi durante il quale una sessione di questa applicazione dovrà continuare ad essere gestita dopo il rilevamento di assenza di attività. Il valore di timeout che si immette imposta il valore di Timeout Idle del TCP se questa è un'applicazione TCP, o un valore di Timeout Idle se questa è un'applicazione UDP.

Altre opzioni

Per certe applicazioni è possibile impostare opzioni aggiuntive. Secondo l'applicazione, le opzioni possono essere descritte di seguito.

Campo MAX dati

Specifica il numero massimo di byte (dati) che possono essere trasferiti in una sessione SMTP (Simple Mail Transport Protocol). Quando si supera il valore massimo, il firewall scrive un messaggio d'avviso nel registro e chiude la sessione. Valore di default: 20 MB.

Casella di controllo Accesso protetto

Fa sì che sulle locazioni non protette venga utilizzata la crittografia per l'autenticazione.

Casella Reimposta

Ripristina lo stato iniziale della connessione TCP se il cliente immette un comando non di protocollo prima del completamento dell'autenticazione.

Casella di controllo Traffico router

Abilita l'ispezione del traffico destinato a o originato da un router. Applicabile solo ai protocolli H.323, TCP, e UDP.

Comandi Consenti, Blocca e Allarme

Utilizzare i comandi Consenti, Blocca e Allarme per specificare l'azione del router quando rileva traffico con le caratteristiche specificate. Per effettuare un'impostazione del criterio per un'opzione, selezionare la casella di controllo accanto ad essi. Quindi nella colonna Azione scegliere **Consenti** per consentire il passaggio di traffico relativo a tale opzione oppure scegliere **Blocca** per negare il passaggio del traffico. Se si desidera che un allarme venga inviato al registro ogni volta che si incontra traffico di questo tipo, selezionare **Invia allarme**. Il comando Invia allarme non è disponibile in tutte le finestre.

Perché Protezione applicazioni possa inviare allarmi al registro la registrazione deve essere attivata. Per maggiori informazioni, consultare il collegamento: Registro di Protezione dell'applicazione.

CAPITOLO 9

VPN site-to-site

Gli argomenti della guida di questa sezione descrivono le schermate di configurazione VPN site-to-site e le schermate della Guida alla progettazione VPN.

Guida alla progettazione VPN

Per un amministratore che deve impostare una rete VPN, la Guida alla progettazione VPN rappresenta un aiuto per stabilire il tipo di VPN da configurare. È necessario specificare il tipo di utente, il tipo di dispositivo con il quale il router stabilisce le connessioni VPN, il tipo di traffico che verrà trasportato da VPN e altre funzioni che devono essere configurate. Dopo avere fornito queste informazioni, la Guida alla progettazione VPN consiglierà un tipo di VPN e permetterà di avviare la procedura guidata per configurare quel tipo di VPN.

Creazione di una rete VPN site-to-site

Una rete VPN (Virtual Private Network) consente di proteggere il traffico che viaggia lungo linee che possono non essere di proprietà o sotto il controllo dell'organizzazione. Le reti VPN possono crittografare il traffico inviato lungo queste linee e autenticare i peer prima dell'invio.

Facendo clic sull'icona VPN, è possibile effettuare una semplice configurazione VPN tramite Cisco Router and Security Device Manager (Cisco SDM). Quando si utilizza la procedura guidata nella scheda Crea VPN site-to-site, in Cisco SDM vengono forniti i valori predefiniti per alcuni parametri di configurazione al fine di semplificare il processo di configurazione.

Per maggiori informazioni sulla tecnologia VPN, fare clic sul collegamento Ulteriori informazioni sul protocollo VPN.

Crea VPN site-to-site

Con questa opzione è possibile creare una rete VPN che connette due router.

Crea tunnel GRE sicuro (GRE su IPSec)

Con questa opzione è possibile configurare un tunnel con protocollo GRE (Generic Routing Encapsulation) tra il router e un sistema peer.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurazione del router come parte di una rete VPN che connette due router. Quando si configura una rete VPN tra due router, è possibile controllare la modalità di autenticazione del router remoto, la modalità di crittografia del traffico e quale traffico crittografare.	Selezionare **Crea VPN site-to-site**. Quindi fare clic su **Avvia attività selezionata**.
Configurazione di un tunnel GRE tra il router in uso e un altro router. È possibile configurare un tunnel GRE se è necessario connettere reti che utilizzano protocolli LAN diversi o se è necessario inviare protocolli di routing lungo la connessione al sistema remoto.	Selezionare Crea tunnel GRE sicuro (GRE su IPSec). Quindi fare clic su **Avvia attività selezionata**.

Funzione	Procedura
Reperimento di informazioni su come eseguire altre attività relative alle reti VPN non previste da questa procedura guidata.	Selezionare un argomento dall'elenco seguente: • Come visualizzare i comandi IOS inviati al router? • Come creare una rete VPN verso più siti? • Dopo aver configurato una connessione VPN, come configurare tale connessione sul router peer? • Come modificare un tunnel VPN esistente? • Come verificare il funzionamento della VPN? • Come verificare il funzionamento della VPN? • Come configurare un peer di backup per la VPN? • Come sistemare più dispositivi con diversi livelli di supporto VPN? • Come configurare una connessione VPN in un'interfaccia non supportata? • Come configurare una connessione VPN dopo aver configurato un firewall? • Come configurare un pass-through NAT per una connessione VPN? • Come configurare manualmente una DMVPN?
Configurazione di un concentratore Easy VPN. Istruzioni per la configurazione di server e concentratori Easy VPN sono disponibili all'indirizzo www.cisco.com.	Il collegamento seguente fornisce indicazioni utili sulla configurazione di un concentratore serie Cisco VPN 3000 per un client Easy VPN Remote Phase II e altre informazioni utili: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html (in inglese). La documentazione sulla serie Cisco VPN 3000 è disponibile al seguente indirizzo: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html (in inglese).

Procedura guidata VPN site-to-site

È possibile utilizzare le impostazioni predefinite di Cisco SDM per la maggior parte dei valori di configurazione oppure seguire le indicazioni fornite da Cisco SDM per la configurazione di una rete VPN.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurazione rapida di una rete VPN site-to-site utilizzando le impostazioni predefinite di Cisco SDM.	Selezionare **Configurazione rapida**, quindi fare clic su **Avanti**. In Cisco SDM viene fornito automaticamente un criterio IKE predefinito per controllare l'autenticazione, un set di trasformazione predefinito per controllare la crittografia dei dati e una regola IPSec predefinita che consente di crittografare tutto il traffico tra il router e il dispositivo remoto. La configurazione rapida è una scelta ottimale quando sia il router locale che il sistema remoto sono router Cisco che utilizzano Cisco SDM. La configurazione rapida configurerà la crittografia 3DES se supportata dall'immagine IOS, altrimenti configurerà la crittografia DES. Se è necessaria la crittografia AES o SEAL, fare clic su **Procedura guidata**.
Visualizzazione delle impostazioni predefinite della IKE Policy, del set di trasformazione e della regola IPSec che verranno utilizzate per configurare direttamente una rete VPN.	Fare clic su **Visualizza impostazioni predefinite**.
Configurazione di una rete VPN site-to-site utilizzando i parametri specificati dall'utente.	Selezionare **Procedura guidata**, quindi fare clic su **Avanti**. È possibile creare una configurazione personalizzata per la rete VPN e utilizzare qualsiasi impostazione predefinita Cisco SDM che possa essere necessaria. La procedura guidata consente di specificare un tipo di crittografia più avanzata rispetto a quella prevista dalla configurazione rapida guidata.

Visualizza impostazioni predefinite

Con questa finestra è possibile visualizzare le impostazioni predefinite della IKE Policy (Internet Key Exchange), del set di trasformazione e della regola IPSec che verranno utilizzate da Cisco SDM per configurare rapidamente una rete VPN site-to-site. Se è necessaria una configurazione diversa da quella mostrata in questa finestra, selezionare **Procedura guidata** e definire i valori di configurazione.

Informazioni sulla connessione VPN

Utilizzare questa finestra per identificare l'Indirizzo IP o il nome host del sito remoto in cui terminerà il tunnel VPN che si desidera configurare, per specificare l'interfaccia del router da utilizzare e per immettere la chiave precondivisa che verrà utilizzata da entrambi i router per l'autenticazione reciproca.

Selezionare l'interfaccia per la connessione VPN

Selezionare l'interfaccia sul router che consente di effettuare la connessione al sito remoto. Il router che si sta configurando è rappresentato come router locale nel diagramma Scenario caso di utilizzo.

Identità peer

Immettere l'indirizzo IP del peer IPSec (IP Security) remoto in cui terminerà il tunnel VPN che si desidera configurare. Il peer IPSec remoto potrebbe essere un altro router, un concentratore VPN o qualsiasi altro dispositivo gateway che supporta IPSec.

Peer con indirizzo IP dinamico

Selezionare questa opzione se i peer a cui si connette il router utilizzano indirizzi IP assegnati dinamicamente.

Peer con indirizzo IP statico

Selezionare questa opzione se il peer a cui si connette il router utilizza un indirizzo IP prestabilito.

Immettere l'indirizzo IP del peer remoto

Questa opzione è attivata nel caso in cui è stato selezionato il peer con indirizzo IP statico. Immettere l'indirizzo IP del peer remoto.

Autenticazione

Fare clic su questo pulsante se i peer VPN utilizzano una chiave precondivisa per autenticare le connessioni reciprocamente. La chiave deve essere uguale su ogni lato della connessione VPN.

Immettere la chiave precondivisa e inserirla nuovamente per la conferma. Le chiavi precondivise devono essere scambiate con l'amministratore del sito remoto tramite un metodo sicuro e pratico, ad esempio un messaggio di posta elettronica crittografato. Nella chiave precondivisa non devono essere utilizzati punti interrogativi (?) e spazi. La chiave precondivisa può contenere 128 caratteri al massimo.

Nota

- I caratteri immessi per la chiave precondivisa non vengono visualizzati durante la relativa digitazione. Si consiglia di prendere nota della chiave prima di immetterla in modo da poterla comunicare all'amministratore del sistema remoto.
- Le chiavi precondivise devono essere scambiate tra ogni coppia di peer IPSec che necessitano di stabilire tunnel protetti. Questo metodo di autenticazione è appropriato per una rete stabile con un numero limitato di peer IPSec, ma può causare problemi di scalabilità in una rete con un numero grande o crescente di peer IPSec.

Certificato digitale

Fare clic su questo pulsante se i peer VPN utilizzeranno i certificati digitali per l'autenticazione.

Nota Per l'autenticazione, il router deve disporre di un certificato digitale emesso da una Certificate Authority. Se non è stato configurato un certificato digitale per il router, andare in Componenti VPN e utilizzare la procedura guidata Certificato digitale per la registrazione.

Traffico da crittografare

Se si desidera configurare una connessione VPN site-to-site mediante la configurazione rapida, è necessario specificare le subnet di origine e di destinazione in questa finestra.

Origine

Scegliere l'interfaccia del router che costituirà l'origine del traffico in questa connessione VPN. Verrà crittografato tutto il traffico proveniente da questa interfaccia il cui indirizzo IP di destinazione si trova nella subnet specificata nell'area Destinazione.

Dettagli

Fare clic su questo pulsante per ottenere dettagli sull'interfaccia selezionata. Nella finestra dei dettagli sarà possibile visualizzare tutte le regole di accesso, i criteri IPSec, le regole NAT (Network Address Translation) o le Inspection Rule associate all'interfaccia. Per esaminare in dettaglio una regola, andare in Attività aggiuntive/Editor ACL e visualizzarla nella finestra Regole.

Destinazione

Indirizzo IP/Subnet Mask. Immettere l'indirizzo IP e la subnet mask della destinazione per questo traffico. Per maggiori informazioni su come immettere i valori in questi campi, vedere Indirizzi IP e subnet mask.

La destinazione è rappresentata come il router remoto nel diagramma Scenario caso di utilizzo, nella finestra principale della procedura guidata VPN.

Proposte IKE

In questa finestra sono elencate tutte le policy IKE (Internet Key Exchange) configurate sul router. Se non è stato configurata nessuna policy definita dall'utente, verrà visualizzata la IKE Policy predefinita Cisco SDM. Le IKE Policy consentono di controllare il modo in cui i dispositivi presenti in una rete VPN eseguono l'autenticazione.

Il router locale utilizzerà le IKE Policy elencate in questa finestra per negoziare l'autenticazione con il router remoto.

Il router locale e il dispositivo peer devono utilizzare entrambi la stessa policy. Il router che avvia la connessione VPN offre come prima policy quella con il numero più basso di priorità. Se il sistema remoto rifiuta quella policy, il router locale offre la policy successiva nell'ordine e così via finché il sistema remoto non accetta una policy. È necessario coordinarsi con l'amministratore del sistema peer affinché sia possibile configurare policy identiche su entrambi i router.

Per le connessioni Easy VPN, le IKE Policy vengono configurate solo sul server Easy VPN. Il client Easy VPN invia le proposte e il server risponde in base alle IKE Policy configurate.

Priorità

L'ordine in cui la policy verrà offerta durante la negoziazione.

Crittografia

In Cisco SDM sono supportati diversi tipi di crittografia, elencati in ordine di protezione. Più un tipo di crittografia è sicuro, maggiore sarà il tempo di elaborazione richiesto.

Nota

- Non tutti i router supportano tutti i tipi di crittografia. I tipi non supportati non verranno visualizzati nella schermata.
- Non tutte le immagini IOS supportano tutti i tipi di crittografia previsti in Cisco SDM. I tipi non supportati dall'immagine IOS non verranno visualizzati nella schermata.
- Se è attivata la crittografia hardware, nella schermata verranno visualizzati solo i tipi supportati dalla crittografia hardware.

In Cisco SDM sono supportati i tipi di crittografia elencati di seguito.

- DES: Data Encryption Standard. Questo formato supporta la crittografia a 56 bit.
- 3DES: Triple DES. Si tratta di un tipo più avanzato rispetto al DES in quanto supporta la crittografia a 168 bit.
- AES-128: crittografia AES (Advanced Encryption Standard) con chiave a 128 bit. L'AES fornisce una maggiore protezione rispetto al formato DES ed è più efficiente dal punto di vista computazionale del 3DES.
- AES-192: crittografia AES con chiave a 192 bit.
- AES-256: crittografia AES con chiave a 256 bit.

Hash

L'algoritmo di autenticazione da utilizzare per la negoziazione. In Cisco SDM sono supportati gli algoritmi seguenti:

- SHA_1: Secure Hash Algorithm. Un algoritmo hash utilizzato per autenticare i dati dei pacchetti.
- MD5: Message Digest 5. Un algoritmo hash utilizzato per autenticare i dati dei pacchetti.

Gruppi D-H

Gruppi Diffie-Hellman: Diffie-Hellman è un protocollo di crittografia a chiave pubblica che consente a due router di stabilire un segreto condiviso su un canale di comunicazione non protetto. In Cisco SDM sono supportati i gruppi seguenti:

- gruppo 1: D-H Group 1. Gruppo a 768 bit.
- gruppo 2: D-H Group 2. Gruppo a 1024 bit. Questo gruppo fornisce maggiore protezione del gruppo 1 ma richiede un tempo di elaborazione più lungo.
- gruppo 5: D-H Group 5. Gruppo a 1536 bit. Questo gruppo fornisce maggiore protezione del gruppo 2 ma richiede un tempo di elaborazione più lungo.

Autenticazione

Il metodo di autenticazione da utilizzare. Sono supportati i valori elencati di seguito.

- PRE_SHARE: l'autenticazione verrà eseguita mediante chiavi precondivise.
- RSA_SIG: l'autenticazione verrà eseguita mediante certificati digitali.

Nota È necessario scegliere il tipo di autenticazione specificato al momento dell'identificazione delle interfacce che utilizza la connessione VPN.

Tipo

Impostazioni predefinite Cisco SDM o Definito dall'utente. Se sul router non è stato configurata nessuna IKE Policy definita dall'utente, verrà visualizzata la IKE Policy predefinita.

Per aggiungere o modificare una IKE Policy

Se si desidera aggiungere una IKE Policy non inclusa in questo elenco, fare clic su **Aggiungi** e creare la policy nella finestra visualizzata. Se si desidera modificare una policy esistente, selezionare la policy e fare clic su **Modifica**. I criteri predefiniti Cisco SDM sono di sola lettura e non possono essere modificati.

Per accettare l'elenco delle policy

Per accettare l'elenco delle IKE Policy e continuare, fare clic su **Avanti**.

Set di trasformazione

In questa finestra sono elencati tutti i set di trasformazione predefiniti Cisco SDM e quelli aggiuntivi configurati sul router. Questi set di trasformazione potranno essere utilizzati dalla connessione VPN o DMVPN. Un set di trasformazione rappresenta una determinata combinazione di protocolli e algoritmi di protezione. Durante la negoziazione dell'associazione della protezione IPSec, i peer concordano nell'utilizzare un particolare set di trasformazione per proteggere un determinato flusso di dati. Una trasformazione descrive un particolare protocollo di protezione e gli algoritmi corrispondenti.

In questa finestra è possibile selezionare solo un set di trasformazione ma è possibile associare set di trasformazione aggiuntivi alla connessione VPN o DMVPN utilizzando le schede Modifica VPN o DMVPN.

Seleziona set di trasformazione

Selezionare il set di trasformazione che si desidera utilizzare da questo elenco.

Dettagli del set di trasformazione selezionato

In quest'area sono riportati i dettagli del set di trasformazione selezionato. Poiché non è necessario configurare tutti i tipi di crittografia, autenticazione e compressione, alcune colonne potrebbero risultare vuote.

Per conoscere i valori che possono essere presenti in ciascuna colonna, fare clic su **Aggiungi o Modifica set di trasformazione**.

Nome
Il nome fornito al set di trasformazione.

Crittografia ESP
Il tipo di crittografia ESP (Encapsulating Security Protocol) utilizzato. Se la crittografia ESP non è configurata per questo set di trasformazione, questa colonna sarà vuota.

Autenticazione ESP
Il tipo di autenticazione ESP utilizzato. Se l'autenticazione ESP non è configurata per questo set di trasformazione, questa colonna sarà vuota.

Autenticazione AH
Il tipo di autenticazione AH (Authentication Header) utilizzato. Se l'autenticazione AH non è configurata per questo set di trasformazione, questa colonna sarà vuota.

Compressione IP
Se la compressione IP non è configurata per questo set di trasformazione, questa colonna conterrà il valore COMP-LZS.

Nota La compressione IP non è supportata su tutti i router.

Modalità
In questa colonna è riportato uno dei seguenti valori:

- Trasporto (crittografia solo dati). La modalità Trasporto è utilizzata quando entrambi gli endpoint supportano l'IPSec. Questa modalità inserisce l'intestazione di autenticazione o il payload di protezione incapsulato dopo l'intestazione IP originale, pertanto solo il payload IP viene crittografato. Questo metodo consente agli utenti di applicare servizi di rete quali i controlli Qualità del servizio (QoS) ai pacchetti crittografati.
- Tunnel (crittografia dati e intestazione IP). La modalità Tunnel fornisce una protezione maggiore rispetto alla modalità Trasporto. Poiché tutto il pacchetto IP è incapsulato all'interno di AH o ESP, viene aggiunta una nuova intestazione IP e tutto il datagramma può essere crittografato. La modalità Tunnel consente ai dispositivi di rete quali i router di agire come un proxy IPSec per più utenti VPN.

Tipo
Definito dall'utente o Impostazioni predefinite Cisco SDM.

Tabella riassuntiva funzioni

Funzione	Procedura
Selezione di un set di trasformazione da utilizzare per la VPN.	Selezionare un set di trasformazione, quindi fare clic su **Avanti**.
Aggiunta di un set di trasformazione alla configurazione del router.	Fare clic su **Aggiungi** e creare il set di trasformazione nella finestra Aggiungi set di trasformazione. Quindi fare clic su **Avanti** per continuare con la configurazione della VPN.
Modifica di un set di trasformazione esistente.	Selezionare un set di trasformazione, quindi fare clic su **Modifica**. Modificare il set di trasformazione nella finestra Modifica set di trasformazione. Dopo aver modificato il set di trasformazione, fare clic su **Avanti** per continuare con la configurazione della VPN. I set di trasformazione predefiniti Cisco SDM sono di sola lettura e non possono essere modificati.
Associazione di set di trasformazione aggiuntivi a questa VPN.	Selezionare un set di trasformazione in questa finestra, quindi completare la procedura guidata VPN. Associare altri set di trasformazione alla VPN nella scheda Modifica.

Traffico da proteggere

In questa finestra è possibile definire il traffico protetto da questa VPN. La VPN può proteggere il traffico tra subnet specificate o il traffico specificato in una regola IPSec selezionata dall'utente.

Proteggere tutto il traffico all'interno delle seguenti subnet

Utilizzare questa opzione per specificare una singola subnet di origine (una subnet sulla LAN), di cui si desidera crittografare il traffico in uscita, e una subnet di destinazione supportata dal peer specificato nella finestra della connessione VPN.

Tutto il traffico che passa tra altre coppie di origine e destinazione verrà inviato non crittografato.

Origine

Immettere l'indirizzo della subnet di cui si desidera proteggere il traffico in uscita e specificare la relativa subnet mask. Per maggiori informazioni vedere Configurazioni delle interfacce disponibili.

Verrà protetto tutto il traffico proveniente da questa subnet di origine il cui indirizzo IP di destinazione si trova nella subnet di destinazione.

Destinazione

Immettere l'indirizzo della subnet di destinazione e specificare la relativa subnet mask. È possibile selezionare una subnet mask dall'elenco o specificarne una personalizzata. Il numero della subnet e la subnet mask devono essere immessi nel formato decimale separato da punti, come mostrato negli esempi precedenti.

Verrà protetto tutto il traffico diretto agli host in questa subnet.

Creare/selezionare un comando access-list per il traffico IPSec

Utilizzare questa opzione se è necessario specificare più origini e destinazioni e/o specifici tipi di traffico da crittografare. Una regola IPSec può essere composta da più voci, ognuna delle quali può specificare tipi di traffico, origini e destinazioni diversi.

Fare clic sul pulsante accanto al campo e specificare una regola IPSec esistente che definisce il traffico da crittografare oppure creare una regola IPSec da utilizzare per questa VPN. Se si conosce il numero della regola IPSec, immetterlo nella casella a destra. In caso contrario, fare clic sul pulsante **...** e cercare la regola. Una volta selezionata la regola, il numero relativo verrà visualizzato nella casella.

Nota Le regole IPSec sono regole estese in quanto possono specificare il tipo di traffico, l'origine e la destinazione. Se si immette il numero o il nome di una regola standard, viene visualizzato un messaggio di avviso indicante che è stato immesso il nome o il numero di una regola standard.

Qualsiasi pacchetto che non soddisfa i criteri nella regola IPSec viene inviato senza crittografia.

Riepilogo della configurazione

In questa finestra viene visualizzata la configurazione VPN o DMVPN creata. È possibile rivedere la configurazione e utilizzare il pulsante Indietro per apportare qualsiasi modifica.

Configurazione spoke

Se è stato configurato un hub DMVPN, l'utente o altri amministratori possono utilizzare una procedura generata in Cisco SDM, utile per configurare spoke DMVPN in quanto spiega le opzioni da selezionare nella procedura guidata e le informazioni da immettere nelle finestre di configurazione degli spoke. È possibile salvare queste informazioni in un file di testo utilizzabile dall'utente o da altri amministratori.

Verificare la connettività dopo la configurazione

Fare clic su questa opzione per verificare la connessione VPN appena configurata. I risultati della verifica verranno visualizzati in un'altra finestra.

Per salvare questa configurazione nella configurazione del router in esecuzione e uscire da questa procedura guidata

Fare clic su **Fine.** In Cisco SDM le modifiche apportate alla configurazione vengono salvate nella configurazione del router in esecuzione. Tali modifiche diventeranno immediatamente effettive, tuttavia andranno perse se il router verrà disattivato.

Se è stata selezionata l'opzione **Eseguire l'anteprima dei comandi prima dell'inoltro al router** nella finestra delle preferenze Cisco SDM, verrà visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi CLI inviati al router.

Configurazione spoke

In questa finestra vengono visualizzate informazioni che possono essere utilizzate per assegnare una configurazione a un router spoke che sia compatibile con l'hub DMVPN configurato. È riportato l'elenco delle finestre che devono essere completate e i dati da immettere in modo che lo spoke possa comunicare con l'hub.

I dati da immettere nella configurazione dello spoke riportati in questa finestra sono i seguenti:

- L'indirizzo IP pubblico dell'hub. Si tratta dell'indirizzo IP dell'interfaccia hub che supporta il tunnel mGRE.
- L'indirizzo IP del tunnel mGRE dell'hub.
- La subnet mask che deve essere utilizzata da tutte le interfacce tunnel nella DMVPN.
- Le informazioni sulla configurazione avanzata del tunnel.
- Il protocollo di routing da utilizzare e tutte le informazioni associate al protocollo quali il numero di sistema autonomo per il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) e l'ID del processo OSPF (Open Shortest Path First).
- L'algoritmo hash, la crittografia, il gruppo D-H e il tipo di autenticazione delle IKE Policy utilizzati dall'hub in modo che sia possibile configurare IKE Policy compatibili sullo spoke.
- Le informazioni sulla crittografia ESP e sulla modalità dei set di trasformazione utilizzati dall'hub. Se sullo spoke non sono stati configurati set di trasformazione simili, è possibili configurarli utilizzando queste informazioni.

Tunnel GRE protetto (GRE su IPSec)

GRE (Generic Routing Encapsulation) è un protocollo di tunneling sviluppato da Cisco che può incapsulare un'ampia gamma di tipi di pacchetto di protocollo all'interno di tunnel IP, creando un collegamento point-to-point virtuale con i router Cisco presso punti remoti su una rete IP. Collegando subnet con più protocolli in un ambiente backbone a protocollo singolo, il tunneling IP che utilizza il protocollo GRE consente l'espansione di rete in un ambiente backbone a protocollo singolo.

Questa procedura guidata consente di creare un tunnel GRE con crittografia IPSec. Quando si crea la configurazione di un tunnel GRE, è possibile creare anche una regola IPSec che descriva gli endpoint del tunnel.

Informazioni sul tunnel GRE

In questa schermata vengono fornite informazioni generali sul tunnel GRE.

Origine tunnel

Selezionare il nome o l'indirizzo IP dell'interfaccia che verrà utilizzata dal tunnel. L'indirizzo IP dell'interfaccia deve essere raggiungibile dall'altra estremità del tunnel, pertanto deve essere un indirizzo IP pubblico e instradabile. Se si immette un indirizzo IP non associato a nessuna interfaccia configurata, verrà generato un errore.

Nota In Cisco SDM sono elencate le interfacce con gli indirizzi IP statici e le interfacce configurate come senza numero nell'elenco delle interfacce. Nell'elenco non sono incluse le interfacce loopback.

Dettagli

Consente di ottenere dettagli sull'interfaccia selezionata. La finestra dei dettagli visualizza tutte le regole di accesso, i criteri IPSec, le regole NAT o le Inspection Rule associate all'interfaccia. Se a questa interfaccia è stata applicata una regola NAT che causa l'impossibilità di instradare l'indirizzo, il tunnel non funzionerà correttamente. Per esaminare una regola in dettaglio, andare in Attività aggiuntive/Editor ACL e visualizzarla nella finestra Regole.

Destinazione tunnel

Immettere l'indirizzo IP dell'interfaccia del router remoto all'altra estremità del tunnel. Si tratta dell'interfaccia di origine se si considera l'altra estremità del tunnel.

Assicurarsi che questo indirizzo sia raggiungibile utilizzando il comando **ping**. Il comando **ping** è disponibile dal menu Strumenti. Se l'indirizzo di destinazione non può essere raggiunto, il tunnel non verrà creato correttamente.

Indirizzo IP del tunnel GRE

Immettere l'indirizzo IP del tunnel. Gli indirizzi IP di entrambe le estremità del tunnel devono trovarsi nella stessa subnet. Al tunnel viene assegnato un indirizzo IP separato in modo che possa essere un indirizzo privato se necessario.

Indirizzo IP

Immettere l'indirizzo IP del tunnel in formato decimale separato da punti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask per l'indirizzo del tunnel in formato decimale separato da punti.

Informazioni sull'autenticazione VPN

I peer VPN utilizzano una chiave precondivisa per autenticare le connessioni reciprocamente. La chiave deve essere uguale su ogni lato della connessione VPN.

Chiave precondivisa

Fare clic su questo pulsante se i peer VPN utilizzano una chiave precondivisa per l'autenticazione, quindi immettere la chiave precondivisa e inserirla nuovamente per la conferma. Le chiavi precondivise devono essere scambiate con l'amministratore del sito remoto tramite un metodo sicuro e pratico, ad esempio un messaggio di posta elettronica crittografato. Nella chiave precondivisa non devono essere utilizzati punti interrogativi (?) e spazi.

Nota

- I caratteri immessi per la chiave precondivisa non vengono visualizzati durante la relativa digitazione. Si consiglia di prendere nota della chiave prima di immetterla in modo da poterla comunicare all'amministratore del sistema remoto.
- Le chiavi precondivise devono essere scambiate tra ogni coppia di peer IPSec che necessitano di stabilire tunnel protetti. Questo metodo di autenticazione è appropriato per una rete stabile con un numero limitato di peer IPSec, ma può causare problemi di scalabilità in una rete con un numero grande o crescente di peer IPSec.

Certificato digitale

Fare clic su questo pulsante se i peer VPN utilizzeranno i certificati digitali per l'autenticazione.

Per l'autenticazione, il router deve disporre di un certificato digitale emesso da una Certificate Authority. Se non è stato configurato un certificato digitale per il router, andare in Componenti VPN e utilizzare la procedura guidata Certificato digitale per la registrazione.

Nota Se si esegue l'autenticazione mediante certificati digitali, il tunnel VPN potrebbe non essere creato se il server della Certificate Authority contattato durante la negoziazione IKE non è configurato per rispondere alle richieste relative all'elenco dei certificati revocati (CRL, Certificate Revocation List). Per risolvere questo problema, andare alla pagina Certificati digitali, selezionare il punto di attendibilità configurato, quindi selezionare Nessuno per la revoca.

Informazioni sul tunnel GRE di backup

È possibile configurare un tunnel GRE su IPSec di backup che può essere utilizzato dal router quando si verifica un errore nel tunnel primario. Questo tunnel utilizzerà la stessa interfaccia configurata per il tunnel primario ma deve essere configurato con il router VPN di backup come peer. Se per il tunnel GRE su IPSec primario è configurato il routing, per verificare se il tunnel è ancora attivo vengono utilizzati i pacchetti Keepalive inviati dal protocollo di routing. Se il router smette di ricevere i pacchetti Keepalive sul tunnel primario, il traffico viene inviato attraverso il tunnel di backup.

Creare un tunnel GRE sicuro di backup per la resilienza

Selezionare questa casella se si desidera creare un tunnel di backup.

Indirizzo IP della destinazione del tunnel GRE di backup

Immettere l'indirizzo IP dell'interfaccia del router remoto all'altra estremità del tunnel. Si tratta dell'interfaccia di origine se si considera l'altra estremità del tunnel.

Assicurarsi che questo indirizzo sia raggiungibile utilizzando il comando **ping**. Il comando **ping** è disponibile dal menu Strumenti. Se l'indirizzo di destinazione specificato nella finestra di dialogo Esegui ping non può essere raggiunto, il tunnel non verrà creato correttamente.

Indirizzo IP del tunnel

Immettere l'indirizzo IP del tunnel. Gli indirizzi IP di entrambe le estremità del tunnel devono trovarsi nella stessa subnet. Al tunnel viene assegnato un indirizzo IP separato in modo che possa essere un indirizzo privato se necessario.

Indirizzo IP

Immettere l'indirizzo IP del tunnel in formato decimale separato da punti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Subnet Mask

Immettere la subnet mask per l'indirizzo del tunnel in formato decimale separato da punti.

Informazioni sul routing

In questa finestra è possibile configurare il routing per il traffico incanalato nel tunnel. Le informazioni aggiunte in questa finestra vengono visualizzate nella finestra Routing. Le modifiche apportate nella finestra Routing possono influire sul routing del traffico VPN. La configurazione del routing consente di specificare le reti che parteciperanno alla VPN GRE su IPSec. Inoltre, se si configura un tunnel GRE su IPSec di backup, i pacchetti Keepalive inviati dai protocolli di routing consentono al router di stabilire se nel tunnel primario si sono verificati errori.

Selezionare un protocollo di routing dinamico se il router è utilizzato nell'implementazione di una VPN estesa con un grande numero di reti nella VPN GRE su IPSec. Selezionare un routing statico se poche reti partecipano alla VPN.

EIGRP

Selezionare questa casella per utilizzare il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) per instradare il traffico. Quindi fare clic su **Avanti** per specificare le reti che parteciperanno alla VPN GRE su IPSec nella finestra Informazioni di routing.

OSPF

Selezionare questa casella per utilizzare il protocollo OSPF (Open Shortest Path First) per instradare il traffico. Quindi fare clic su **Avanti** per specificare le reti che parteciperanno alla VPN GRE su IPSec nella finestra Informazioni di routing.

RIP

Selezionare questa casella per utilizzare il protocollo RIP (Routing Information Protocol) per instradare il traffico. Quindi fare clic su **Avanti** per specificare le reti che parteciperanno alla VPN GRE su IPSec nella finestra Informazioni di routing.

Nota Questa opzione non è disponibile quando si configura un tunnel GRE su IPSec di backup.

Routing statico

Il routing statico può essere utilizzato in implementazioni di VPN più piccole in cui solo alcune reti private partecipano alla VPN GRE su IPSec. È possibile configurare una route statica per ogni rete remota in modo che il traffico destinato alle reti remote passi per i tunnel appropriati.

Informazioni sul routing statico

È possibile configurare una route statica per ogni rete remota in modo che il traffico destinato alle reti remote passi per i tunnel appropriati. Configurare la prima route statica nella finestra Informazioni sul routing statico. Se è necessario configurare route statiche aggiuntive, utilizzare la finestra Routing.

Selezionare questa casella se si desidera specificare una route statica per il tunnel, quindi selezionare una delle opzioni elencate di seguito.

- **Tunneling di tutto il traffico**: tutto il traffico verrà instradato attraverso l'interfaccia del tunnel e crittografato. In Cisco SDM viene creata una voce di route statica predefinita con l'interfaccia del tunnel come hop successivo.

  Se una route predefinita esiste già, Cisco SDM la modifica in modo da utilizzare l'interfaccia del tunnel come hop successivo, sostituendo l'interfaccia presente in origine, quindi viene creata una nuova voce statica per la rete di destinazione del tunnel che specifica l'interfaccia nella route predefinita originale come hop successivo.

  Nell'esempio seguente si presuppone che la rete all'altra estremità del tunnel sia 200.1.0.0, come specificato nei campi della rete di destinazione:

  ```
  ! Original entry
  ip route 0.0.0.0  0.0.0.0 FE0
  ! Entry changed by SDM
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ! Entry added by SDM
  ip route 200.1.0.0  255.255.0.0 FE0
  ```

  Se non esiste nessuna route predefinita, Cisco SDM ne crea una utilizzando l'interfaccia del tunnel come hop successivo. Ad esempio:

  ```
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ```

- **Esegui suddivisione tunnel**: la suddivisione del tunnel consente di crittografare e instradare attraverso l'interfaccia del tunnel il traffico destinato alla rete specificata nei campi Indirizzo IP e Maschera di rete. Tutto l'altro traffico non verrà crittografato. Quando questa opzione è selezionata, Cisco SDM crea una route statica per la rete utilizzando l'indirizzo IP e la maschera di rete.

  Nell'esempio seguente si presuppone che sia stato immesso l'indirizzo di rete 10.2.0.0/255.255.0.0 nei campi dell'indirizzo di destinazione:

  Nell'esempio seguente si presuppone che sia stato immesso l'indirizzo di rete 10.2.0.0/255.255.0.0 nei campi dell'indirizzo di destinazione:

  ```
  ip route 10.2.0.0 255.255.0.0 Tunnel0
  ```

  Quando si seleziona lo 'split tunneling' vengono visualizzati i campi Indirizzo IP e Subnet Mask, ed è necessario immettere l'Indirizzo IP e la Subnet Mask del peer di destinazione. È necessario verificare che l'indirizzo IP di destinazione, immesso nel campo Destinazione tunnel della finestra Informazioni sul tunnel GRE, sia raggiungibile. Se non è raggiungibile, non verrà stabilito nessun tunnel.

Indirizzo IP

Questa opzione è attivata con la suddivisione del tunnel. Immettere l'indirizzo IP della rete all'altra estremità del tunnel. In Cisco SDM verrà creata una voce di route statica per i pacchetti con un indirizzo di destinazione in quella rete. Questo campo è disattivato quando è selezionata l'opzione **Tunneling di tutto il traffico**.

È necessario verificare che l'indirizzo IP immesso in questo campo sia raggiungibile prima di configurare questa opzione. Se non è raggiungibile, non verrà stabilito nessun tunnel.

Maschera di rete

Questa opzione è attivata con la suddivisione del tunnel. Immettere la maschera utilizzata sulla rete all'altra estremità del tunnel. Questo campo è disattivato quando è selezionata l'opzione **Tunneling di tutto il traffico**.

Seleziona protocollo di routing

Utilizzare questa finestra per specificare il modo in cui le altre reti sottostanti il router sono notificate agli altri router della rete. Selezionare una delle seguenti opzioni:

- EIGRP: Extended Interior Gateway Routing Protocol.
- OSPF: Open Shortest Path First.
- RIP: Routing Internet Protocol.
- Routing statico. Questa opzione è attivata quando si sta configurando un tunnel GRE su IPSec.

Nota Il protocollo RIP non è supportato per la topologia DMVPN hub and spoke; tuttavia è disponibile per la topologia DMVPN fully-meshed.

Riepilogo della configurazione

In questa schermata è riepilogata la configurazione GRE che è stata completata. È possibile rivedere le informazioni in questa schermata e fare clic sul pulsante Indietro per tornare a qualsiasi schermata in cui si desideri apportare modifiche. Se si desidera salvare la configurazione, fare clic su **Fine**.

La configurazione del tunnel GRE crea una regola IPSec che specifica tra quali host potrà passare il traffico GRE. Questa regola IPSec viene visualizzata nel riepilogo.

Per salvare questa configurazione nella configurazione del router in esecuzione e uscire da questa procedura guidata

Fare clic su **Fine**. In Cisco SDM le modifiche apportate alla configurazione vengono salvate nella configurazione del router in esecuzione. Tali modifiche diventeranno immediatamente effettive, tuttavia andranno perse se il router verrà disattivato.

Se è stata selezionata l'opzione **Eseguire l'anteprima dei comandi prima dell'inoltro al router** nella finestra delle preferenze Cisco SDM, verrà visualizzata la finestra Invia. In questa finestra è possibile visualizzare i comandi CLI inviati al router.

Modifica VPN site-to-site

Le reti VPN (Virtual Private Network) consentono di proteggere i dati tra il router e un sistema remoto crittografando il traffico in modo che non possa essere letto da altri che utilizzano la stessa rete pubblica. In pratica consentono di proteggere una rete privata su linee pubbliche che possono essere utilizzate da altre organizzazioni.

Utilizzare questa finestra per creare e gestire connessioni VPN ai sistemi remoti. È possibile creare, modificare ed eliminare connessioni VPN e reimpostare connessioni esistenti. È possibile utilizzare questa finestra anche per configurare il router come un client Easy VPN con connessioni a uno o più server o concentratori Easy VPN.

Fare clic sul collegamento relativo alla parte della finestra per la quale si desidera ottenere informazioni.

Connessioni VPN site-to-site

Le connessioni VPN, talvolta chiamate *tunnel*, vengono create e gestite dall'apposita casella. Una connessione VPN collega l'interfaccia di un router a uno o più peer specificati da una mappa crittografica definita in un criterio IPSec (IP Security). È possibile visualizzare, aggiungere, modificare ed eliminare le connessioni VPN in questo elenco.

Colonna Stato

Lo stato della connessione indicato dalle icone riportate di seguito:

 La connessione è attiva.

 La connessione non è attiva.

 La connessione sta per essere stabilita.

Interfaccia

L'interfaccia del router connessa ai peer remoti in questa connessione VPN. Un'interfaccia può essere associata solo a un criterio IPSec. La stessa interfaccia apparirà su più righe se è definita più di una mappa crittografica per il criterio IPSec utilizzato in questa connessione.

Descrizione

Una breve descrizione di questa connessione.

Criterio IPSec

Il nome del criterio IPSec utilizzato in questa connessione VPN. Il criterio IPSec specifica la modalità di crittografia dei dati, i dati da crittografare e dove verranno inviati. Per maggiori informazioni fare clic su Ulteriori informazioni sulle connessioni VPN e i criteri IPSec.

Numero sequenza

Il numero di sequenza per questa connessione. Poiché un criterio IPSec può essere utilizzato in più di una connessione, la combinazione del numero di sequenza e del nome del criterio IPSec identifica in modo univoco questa connessione VPN. Il numero di sequenza non assegna priorità alla connessione VPN; il router tenterà di stabilire tutte le connessioni VPN configurate indipendentemente dal numero di sequenza.

Peer

Gli indirizzi IP o i nomi host dei dispositivi all'altra estremità della connessione VPN. Quando una connessione contiene più peer, i rispettivi indirizzi IP o nomi host vengono separati da virgole. È possibile configurare più peer per fornire percorsi di routing alternativi per la connessione VPN.

Set di trasformazione

Viene visualizzato il nome del set di trasformazione utilizzato da questa connessione VPN. Più nomi di set di trasformazione vengono separati da virgole. Un set di trasformazione specifica gli algoritmi che verranno utilizzati per crittografare i dati, garantire l'integrità dei dati e fornire la compressione dei dati. Entrambi i peer devono utilizzare lo stesso set di trasformazione e per stabilire quale utilizzeranno devono negoziare. È possibile definire più set di trasformazione per assicurarsi che il router possa offrire un set di trasformazione che sia accettabile da parte del peer che sta negoziando. I set di trasformazione sono un componente del criterio IPSec.

Regola IPSec

La regola che stabilisce quale traffico deve essere crittografato su questa connessione. La regola IPSec è un componente del criterio IPSec.

Tipo

La scelta può essere effettuata tra una delle opzioni riportate di seguito.

- Statico: tunnel VPN site-to-site statico. Il tunnel VPN utilizza mappe crittografiche statiche.
- Dinamico: tunnel VPN site-to-site dinamico. Il tunnel VPN utilizza mappe crittografiche dinamiche.

Pulsante Aggiungi

Consente di aggiungere una connessione VPN.

Pulsante Elimina

Consente di eliminare la connessione VPN selezionata.

Pulsante Verifica tunnel...

Consente di verificare il tunnel VPN selezionato. I risultati della verifica verranno visualizzati in un'altra finestra.

Pulsante Cancella connessione

Consente di reimpostare una connessione stabilita con un peer remoto. Questo pulsante è disattivato se è stato selezionato un tunnel VPN site-to-site dinamico.

Pulsante Genera mirroring...

Consente di creare un file di testo in cui viene acquisita la configurazione VPN del router locale; in questo modo a un router remoto può essere assegnata una configurazione VPN che gli consente di stabilire una connessione con il router locale. Questo pulsante è disattivato se è stato selezionato un tunnel VPN site-to-site dinamico.

Nota Qualsiasi connessione VPN configurata in precedenza, che viene rilevata in Cisco SDM e non utilizza le mappe crittografiche ISAKMP, verrà visualizzata come voce di sola lettura nella tabella delle connessioni VPN e non potrà essere modificata.

Aggiungi nuova connessione

Utilizzare questa finestra per aggiungere una nuova connessione VPN tra il router locale e un sistema remoto, a cui si fa riferimento come *peer*. La connessione VPN viene creata associando un criterio IPSec a un'interfaccia.

Per creare una nuova connessione VPN

Passo 1 Selezionare l'interfaccia che si desidera utilizzare per la VPN dall'elenco Seleziona interfaccia. In questo elenco vengono riportate solo le interfacce che non sono utilizzate in altre connessioni VPN.

Passo 2 Selezionare un criterio dall'elenco Scegli criterio IPSec. Fare clic su **OK** per tornare alla finestra delle connessioni VPN.

Aggiungi mappa crittografica

Utilizzare questa finestra per aggiungere una nuova mappa crittografica a un criterio IPSec esistente. In questa finestra viene visualizzata l'interfaccia associata alla connessione VPN selezionata nella finestra delle connessioni VPN, il criterio IPSec ad essa associato e le mappe crittografiche già contenute nel criterio.

La mappa crittografica specifica un numero di sequenza, il dispositivo peer all'altra estremità della connessione, il set di trasformazione che crittografa il traffico e la regola IPSec che stabilisce quale traffico viene crittografato.

Nota L'aggiunta di una mappa crittografica a un criterio IPSec esistente è l'unico modo per aggiungere un tunnel VPN a un'interfaccia già utilizzata in una connessione VPN esistente.

Interfaccia

L'interfaccia utilizzata in questa connessione VPN.

Criterio IPSec

Il nome del criterio IPSec che controlla la connessione VPN. Le mappe crittografiche che compongono il criterio IPSec vengono riportate nell'elenco sotto questo campo. Per maggiori informazioni fare clic su Ulteriori informazioni sulle connessioni VPN e i criteri IPSec.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurazione automatica della mappa crittografica.	Fare clic su **Aggiungi nuova mappa crittografica** e utilizzare la finestra Aggiungi mappa crittografica per creare la nuova mappa crittografica. Al termine fare clic su **OK**. Quindi fare clic su **OK** in questa finestra.
Utilizzo delle procedure guidate di Cisco Router and Security Device Manager (Cisco SDM) per aggiungere una nuova mappa crittografica a questa connessione.	Selezionare la casella **Utilizza aggiunta guidata**, quindi fare clic su **OK**. In Cisco SDM si verrà guidati nella creazione di una nuova mappa crittografica che verrà associata al criterio IPSec.

Procedura guidata mappa crittografica - Pagina iniziale

Questa procedura guidata aiuta a creare una mappa crittografica. Una mappa crittografica specifica i dispositivi peer all'altra estremità della connessione VPN, definisce la modalità di crittografia del traffico e identifica il traffico che verrà crittografato.

Fare clic su **Avanti** per iniziare la creazione di una mappa crittografica.

Procedura guidata mappa crittografica - Riepilogo della configurazione

Nella pagina di riepilogo della procedura guidata della mappa crittografica sono visualizzati i dati immessi nelle finestre della procedura guidata. È possibile rivederli, fare clic su Indietro per tornare a una schermata e apportare modifiche, ritornare alla finestra di riepilogo e fare clic su **Fine** per inviare la configurazione della mappa crittografica al router.

Elimina connessione

Utilizzare questa finestra per eliminare un tunnel VPN o semplicemente per annullarne l'associazione da un'interfaccia ma conservandone la definizione per un uso futuro.

Eliminare la mappa crittografica con numero di sequenza *n* dal criterio IPSec *nome criterio*

Fare clic su questo pulsante, quindi su **OK** per rimuovere la definizione del tunnel VPN. Con questa operazione, le associazioni create tra l'interfaccia, il criterio IPSec e i dispositivi peer andranno perse. Se più di un'interfaccia è stata associata alla definizione di questo tunnel, verranno eliminate anche queste associazioni.

Eliminare la mappa crittografica dinamica con numero di sequenza *n* dal set di mappe crittografiche dinamiche *nome set*

Questo pulsante viene visualizzato se è stato selezionato un tunnel VPN site-to-site dinamico. Fare clic su questo pulsante, quindi su **OK** per rimuovere la definizione del tunnel VPN. Con questa operazione, le associazioni create tra l'interfaccia, il criterio IPSec e i dispositivi peer andranno perse. Se più di un'interfaccia è stata associata alla definizione di questo tunnel, verranno eliminate anche queste associazioni.

Dissociare il criterio IPSec *nome criterio* dall'interfaccia *nome interfaccia* e conservarlo per un eventuale riutilizzo.

Fare clic su questo pulsante, quindi su **OK** per conservare la definizione del tunnel ma rimuoverne l'associazione dall'interfaccia. Se lo si desidera, sarà possibile associare questa definizione a un'altra interfaccia del router.

Esegui ping

In questa finestra è possibile eseguire il ping di un dispositivo peer. È possibile selezionare sia l'origine che la destinazione dell'operazione di ping. È possibile eseguire il ping di un peer remoto dopo aver reimpostato un tunnel VPN.

Origine

Selezionare o immettere l'indirizzo IP da cui originare il ping. Se l'indirizzo che si desidera utilizzare non è riportato nell'elenco, è possibile immetterlo in questo campo. Il ping può avere origine da qualsiasi interfaccia sul router. Per impostazione predefinita, il comando **ping** ha origine dall'interfaccia esterna con la connessione al dispositivo remoto.

Destinazione

Selezionare l'indirizzo IP di cui eseguire il ping. Se l'indirizzo che si desidera utilizzare non è riportato nell'elenco, è possibile immetterlo in questo campo.

Per eseguire il ping di un peer remoto:

Specificare l'origine e la destinazione, quindi fare clic su **Esegui ping**. È possibile leggere l'output del comando **ping** per determinare se l'esecuzione del ping è riuscita.

Per cancellare l'output del comando ping:

Fare clic su **Cancella**.

Genera mirroring...

In questa finestra viene mostrato il criterio IPSec utilizzato per la connessione tramite il tunnel VPN al peer selezionato; è possibile anche salvare il criterio in un file di testo utilizzabile al momento della configurazione della connessione VPN sul dispositivo peer.

Dispositivo peer

Selezionare l'indirizzo IP o il nome host del dispositivo peer per vedere il criterio IPSec configurato per il tunnel di connessione a quel dispositivo. Il criterio viene visualizzato nella casella sotto l'indirizzo IP del peer.

Per creare un file di testo del criterio IPSec

Fare clic su **Salva**, quindi specificare un nome e un percorso per il file di testo. È possibile fornire questo file di testo all'amministratore del dispositivo peer in modo che possa creare un criterio speculare a quello creato sul router. Fare clic su **Dopo aver configurato una connessione VPN, come configurare tale connessione sul router peer?** per istruzioni su come utilizzare il file di testo per creare un criterio di mirroring.

Precauzione Il file di testo generato non deve essere copiato nel file di configurazione del sistema remoto ma deve essere utilizzato solo per mostrare i dati configurati sul router locale affinché il dispositivo remoto possa essere configurato in modo compatibile. Possono essere utilizzati nomi identici per i criteri IPSec, le IKE Policy e i set di trasformazione sul router remoto ma i criteri e i set di trasformazione possono essere diversi. Se il file di testo viene semplicemente copiato nel file di configurazione remoto, è probabile che si verifichino errori di configurazione.

Avviso Cisco SDM: Regole NAT con ACL

Questa finestra viene visualizzata quando si configura una VPN con interfacce a cui sono associate regole NAT che utilizzano le regole di accesso. Questo tipo di regola NAT può cambiare gli indirizzi IP nei pacchetti prima che questi escano o entrino nella LAN; se la regola NAT cambia gli indirizzi IP di origine rendendoli non più corrispondenti alla regola IPSec configurata per la VPN, le connessioni VPN non funzioneranno correttamente. Per impedire che ciò accada, in Cisco SDM queste regole possono essere convertite in regole NAT che utilizzano route map. Le route map specificano le subnet che non devono essere convertite.

In questa finestra sono mostrate le regole NAT che devono essere modificate per garantire il corretto funzionamento della connessione VPN.

Indirizzo originale

L'indirizzo IP che verrà convertito dalla regola NAT.

Indirizzo convertito

L'indirizzo IP che sostituirà l'indirizzo originale.

Tipo di regola

Il tipo di regola NAT; può essere statico o dinamico.

Affinché le regole NAT elencate utilizzino le route map

Fare clic su **OK**.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come creare una rete VPN verso più siti?

È possibile utilizzare Cisco SDM per creare più tunnel VPN su un'interfaccia del router. Ogni tunnel VPN connetterà l'interfaccia selezionata sul router a una subnet diversa sul router di destinazione. È possibile configurare più tunnel VPN in modo che si connettano alla stessa interfaccia ma a subnet diverse sul router di destinazione oppure è possibile configurare più tunnel VPN che si connettano a diverse interfacce sul router di destinazione.

Innanzitutto, è necessario creare il tunnel VPN iniziale. I passi riportati di seguito descrivono come creare il tunnel VPN iniziale. Se è già stato creato il primo tunnel VPN ed è necessario aggiungere un altro tunnel alla stessa interfaccia, ignorare la prima procedura ed eseguire i passi della procedura successiva in questo argomento della Guida.

Creazione del tunnel VPN iniziale

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Selezionare **Crea VPN site-to-site**.

Passo 3 Fare clic su **Avvia attività selezionata**.

Viene avviata la procedura guidata VPN.

Passo 4 Fare clic su **Configurazione rapida**.

Passo 5 Fare clic su **Avanti>**.

Passo 6 Nel campo Selezionare l'interfaccia per la connessione VPN, scegliere l'interfaccia sul router di origine in cui creare il tunnel VPN. Si tratta dell'interfaccia connessa a Internet sul sistema locale nel diagramma Scenario caso di utilizzo.

Passo 7 Nel campo Identità peer, immettere l'indirizzo IP dell'interfaccia del router di destinazione.

Passo 8 Nei campi Autenticazione, immettere la chiave precondivisa che verrà utilizzata dai due peer VPN, quindi inserirla nuovamente.

Passo 9 Nel campo Origine, selezionare l'interfaccia che connette alla subnet di cui si desidera proteggere il traffico IP. Si tratta del router locale nel diagramma Scenario caso di utilizzo e di solito è un'interfaccia connessa alla LAN.

Passo 10 Nei campi Destinazione, immettere l'indirizzo IP e la subnet mask del router di destinazione.

Passo 11 Fare clic su **Avanti>**.

Passo 12 Fare clic su **Fine**.

Creazione di un tunnel aggiuntivo dalla stessa interfaccia di origine

Dopo aver creato il tunnel VPN iniziale, eseguire i passi riportati di seguito per creare un altro tunnel dalla stessa interfaccia di origine a un'interfaccia o a una subnet di destinazione diversa.

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Selezionare **Crea VPN site-to-site**.

Passo 3 Fare clic su **Avvia attività selezionata**.

Viene avviata la procedura guidata VPN.

Passo 4 Fare clic su **Configurazione rapida**.

Passo 5 Fare clic su **Avanti>**.

Passo 6 Nel campo Selezionare l'interfaccia per la connessione VPN, scegliere la stessa interfaccia utilizzata per creare la connessione VPN iniziale.

Passo 7 Nel campo Identità peer, immettere l'indirizzo IP dell'interfaccia del router di destinazione. È possibile immettere lo stesso indirizzo IP immesso al momento di creare la connessione VPN iniziale. Ciò indica che la seconda connessione VPN deve utilizzare la stessa interfaccia sul router di destinazione della connessione VPN iniziale. Se non si desidera collegare entrambe le connessioni VPN alla stessa interfaccia di destinazione, immettere l'indirizzo IP di un'interfaccia diversa sul router di destinazione.

Passo 8 Nei campi Autenticazione, immettere la chiave precondivisa che verrà utilizzata dai due peer VPN, quindi inserirla nuovamente.

Passo 9 Nel campo Origine, selezionare la stessa interfaccia utilizzata per creare la connessione VPN iniziale.

Passo 10 I campi Destinazione presentano le opzioni seguenti:

- Se nel campo Identità peer si è immesso l'Indirizzo IP di un'interfaccia diversa sul router di destinazione e si desidera proteggere il traffico IP proveniente da una rete secondaria specifica, immettere l'indirizzo IP e la subnet mask di tale rete secondaria nei rispettivi campi.
- Se nel campo Identità peer si è immesso lo stesso indirizzo IP utilizzato per la connessione VPN iniziale per indicare che questo tunnel VPN deve utilizzare la stessa interfaccia del router del tunnel VPN iniziale, immettere nei rispettivi campi l'indirizzo IP e la subnet mask della nuova subnet che si desidera proteggere.

Passo 11 Fare clic su **Avanti>**.

Passo 12 Fare clic su **Fine**.

Dopo aver configurato una connessione VPN, come configurare tale connessione sul router peer?

Cisco SDM genera VPN le configurazioni sul router. Cisco SDM include una funzione che genera un file di testo della configurazione che può essere utilizzato come modello per creare una configurazione VPN per il router peer a cui si connette il tunnel VPN. Il file di testo può essere utilizzato solo come modello dei comandi che devono essere configurati. Non può essere utilizzato senza poi apportare modifiche in quanto contiene informazioni che sono corrette solo per il router locale configurato.

Per generare una configurazione modello per il router VPN peer

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Nella struttura VPN, selezionare **VPN site-to-site**, quindi fare clic sulla scheda Modifica.

Passo 3 Selezionare la connessione VPN che si desidera utilizzare come modello, quindi fare clic su **Genera mirroring**.

Cisco SDM visualizza la schermata Genera mirroring.

Passo 4 Nel campo Dispositivo peer, selezionare l'indirizzo IP del dispositivo peer per il quale si desidera generare una configurazione consigliata.

La configurazione consigliata per il dispositivo peer viene visualizzata nella schermata Genera mirroring.

Passo 5 Fare clic su **Salva** per visualizzare la finestra di dialogo di salvataggio di Windows, quindi salvare il file.

Precauzione Non applicare la configurazione di mirroring al dispositivo peer senza apportare modifiche. Questa configurazione è un modello che richiede modifiche manuali. Utilizzarla solo come punto di partenza per creare la configurazione per il peer VPN.

Passo 6 Dopo aver salvato il file, utilizzare un editor di testo per apportare tutte le modifiche necessarie alla configurazione modello. Alcuni comandi devono essere modificati:

- Comandi relativi all'indirizzo IP del peer.
- Comandi relativi ai criteri di trasformazione.
- Comandi relativi all'indirizzo IP della mappa crittografica.
- Comandi ACL.
- Comandi relativi all'indirizzo IP dell'interfaccia.

Passo 7 Dopo aver modificato il file di configurazione del peer, inviarlo al router peer utilizzando un server TFTP.

Come modificare un tunnel VPN esistente?

Per modificare un tunnel VPN esistente

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Nella struttura VPN, selezionare **VPN site-to-site**, quindi fare clic sulla scheda Modifica.

Passo 3 Fare clic sulla connessione che si desidera modificare.

Passo 4 Fare clic su **Aggiungi**.

Passo 5 Selezionare **Mappe crittografiche statiche in <nome criterio>**

Passo 6 Nella finestra Aggiungi mappe crittografiche, è possibile aggiungere più mappe crittografiche alla connessione VPN.

Passo 7 Se è necessario modificare un componente qualsiasi della connessione, ad esempio il criterio IPSec o la mappa crittografica esistente, prendere nota dei nomi dei componenti nella finestra VPN, quindi andare alle finestre appropriate sotto Componenti VPN per apportare le modifiche.

Come verificare il funzionamento della VPN?

È possibile verificare il funzionamento della connessione VPN utilizzando la modalità di controllo in Cisco SDM. Se la connessione VPN funziona, la modalità di controllo visualizza la connessione VPN identificando gli indirizzi IP del peer di origine e di destinazione. A seconda che la connessione VPN sia un tunnel IPSec o una SA (Security Association) IKE (Internet Key Exchange), la modalità di controllo visualizza il numero di pacchetti trasferiti tramite la connessione o lo stato corrente della connessione. Per visualizzare le informazioni correnti su una connessione VPN, effettuare le operazioni riportate di seguito.

Passo 1 Nella barra degli strumenti, selezionare **Modalità di controllo**.

Passo 2 Nel frame di sinistra, selezionare **Stato VPN**.

Passo 3 Nel campo Selezionare una categoria, scegliere se visualizzare informazioni per i tunnel IPSec o per le SA IKE.

Ogni connessione VPN configurata verrà visualizzata come una riga sulla schermata.

Se si stanno visualizzando informazioni sul tunnel IPSec, è possibile verificare le informazioni riportate di seguito per stabilire se la connessione VPN funziona.

- Gli indirizzi IP del peer locale e remoto sono corretti, a indicare che la connessione VPN è stabilita tra siti e interfacce del router corretti.
- Lo stato del tunnel è attivato. Se lo stato del tunnel è disattivato o disattivato dall'amministratore, la connessione VPN non è attiva.
- Il numero di pacchetti di incapsulamento e di estrazione non è zero, a indicare che i dati sono stati trasferiti lungo la connessione e che il numero di errori inviati e ricevuti non è eccessivo.

Se si stanno visualizzando informazioni sulla SA IKE, è possibile verificare il funzionamento della connessione VPN controllando se gli indirizzi IP di origine e di destinazione sono corretti e se lo stato è “QM_IDLE”, a indicare che la connessione è stata autenticata e il trasferimento dei dati può avere luogo.

Come configurare un peer di backup per la VPN?

Per configurare più peer VPN all'interno di una singola mappa crittografica, effettuare le operazioni riportate di seguito.

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Nella struttura VPN, selezionare **Componenti VPN**, quindi **Criteri IPSec**.

Passo 3 Nella tabella dei criteri IPSec, fare clic sul criterio al quale si desidera aggiungere un altro peer VPN.

Passo 4 Fare clic su **Modifica**.

Viene visualizzata la finestra di dialogo Modifica criterio IPSec.

Passo 5 Fare clic su **Aggiungi**.

Passo 6 Viene visualizzata la finestra di dialogo Aggiungi mappa crittografica, in cui è possibile impostare i valori per la nuova mappa crittografica. Impostare i valori per la nuova mappa crittografica utilizzando tutte e quattro le schede presenti nella finestra di dialogo. Nella scheda Informazioni peer è contenuto il campo Specifica peer, in cui è possibile immettere l'indirizzo IP del peer che si desidera aggiungere.

Passo 7 Al termine fare clic su **OK**.

La mappa crittografica con l'indirizzo IP del nuovo peer viene visualizzata nella tabella “Mappe crittografiche nel criterio IPSec”.

Passo 8 Per aggiungere altri peer, ripetere i passi da 4 a 8.

Come sistemare più dispositivi con diversi livelli di supporto VPN?

Per aggiungere più set di trasformazione a una singola mappa crittografica, effettuare le operazioni riportate di seguito.

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Nella struttura VPN, selezionare **Componenti VPN**, quindi **Criteri IPSec**.

Passo 3 Nella tabella dei criteri IPSec, fare clic sul criterio che contiene la mappa crittografica alla quale si desidera aggiungere un altro set di trasformazione.

Passo 4 Fare clic su **Modifica**.

Viene visualizzata la finestra di dialogo Modifica criterio IPSec.

Passo 5 Nella tabella "Mappe crittografiche nel criterio IPSec", fare clic sulla mappa crittografica alla quale si desidera aggiungere un altro set di trasformazione.

Passo 6 Fare clic su **Modifica**.

Viene visualizzata la finestra di dialogo Modifica mappa crittografica.

Passo 7 Fare clic sulla scheda **Set di trasformazione**.

Passo 8 Nel campo Set di trasformazione disponibili, fare clic sul set che si desidera aggiungere alla mappa crittografica.

Passo 9 Fare clic su **>>** per aggiungere il set di trasformazione selezionato alla mappa crittografica.

Passo 10 Se si desidera aggiungere altri set di trasformazione a questa mappa crittografica, ripetere il passo 9 e il passo 10 per ogni set da aggiungere.

Fare clic su **OK**.

Come configurare una connessione VPN in un'interfaccia non supportata?

In Cisco SDM è possibile configurare una VPN su un'interfaccia non supportata da Cisco SDM. Prima di poter configurare la connessione VPN, è necessario utilizzare la CLI del router per configurare l'interfaccia. È necessario che tale interfaccia disponga di almeno un indirizzo IP e che sia funzionante. Per verificare il corretto funzionamento della connessione, assicurarsi che lo stato dell'interfaccia sia attivato.

Dopo aver configurato l'interfaccia non supportata utilizzando la CLI, è possibile utilizzare Cisco SDM per configurare la connessione VPN. L'interfaccia non supportata verrà visualizzata nei campi che richiedono di scegliere un'interfaccia per la connessione VPN.

Come configurare una connessione VPN dopo aver configurato un firewall?

Affinché una VPN possa funzionare con un firewall, è necessario configurare il firewall in modo che permetta la trasmissione del traffico tra gli indirizzi IP del peer locale e remoto. Per impostazione predefinita, questa configurazione viene creata in Cisco SDM quando si configura una VPN dopo aver già configurato un firewall.

Come configurare un pass-through NAT per una connessione VPN?

Se si sta utilizzando NAT per convertire gli indirizzi dalle reti esterne alla propria e se ci si sta collegando a un sito specifico all'esterno della propria rete tramite una VPN, è necessario configurare un pass-through NAT per la connessione VPN in modo che la conversione dell'indirizzo di rete non avvenga sul traffico VPN. Se il protocollo NAT è già stato configurato sul router e si sta configurando una nuova connessione VPN con Cisco SDM, si riceverà un messaggio di avviso indicante che il NAT verrà configurato da Cisco SDM in modo da non convertire il traffico VPN. È necessario accettare il messaggio in modo che in Cisco SDM vengano creati gli ACL necessari a proteggere il traffico VPN dalla conversione.

Se si sta configurando il NAT con Cisco SDM ed è già stata configurata una connessione VPN, attenersi alla procedura seguente per creare le ACL.

Passo 1 Dal frame di sinistra, selezionare **Attività aggiuntive/Editor ACL**.

Passo 2 Nella struttura Regole, scegliere **Regole di accesso**.

Passo 3 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi regola.

Passo 4 Nel campo Nome/numero, immettere un nome o un numero univoco per la nuova regola.

Passo 5 Nel campo Tipo, scegliere **Regola estesa**.

Passo 6 Nel campo Descrizione, immettere una breve descrizione della nuova regola.

Passo 7 Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi Rule entry standard.

Passo 8 Nel campo Azione, scegliere **Consenti**.

Passo 9 Nel campo Tipo del gruppo Host/rete di origine, selezionare **Una rete**.

Passo 10 Nei campi Indirizzo IP e subnet Mask, immettere l'indirizzo e la subnet mask del peer di origine della VPN.

Passo 11 Nel campo Tipo del gruppo Host/rete di destinazione, selezionare **Una rete**.

Passo 12 Nei campi Indirizzo IP e Maschera carattere jolly, immettere l'indirizzo IP e la subnet mask del peer VPN di destinazione.

Passo 13 Nel campo Descrizione, immettere una breve descrizione della rete o dell'host.

Passo 14 Fare clic su **OK**.

La nuova regola viene visualizzata nella tabella Regole di accesso.

CAPITOLO 10

Easy VPN Remote

Creare Easy VPN Remote

Cisco SDM consente di configurare il router come un client a un server o concentratore Easy VPN. Il router deve disporre di un'immagine Cisco IOS che supporta Easy VPN Phase II.

Per completare la configurazione è necessario disporre delle informazioni riportate di seguito.

- Indirizzo IP o nome host del server Easy VPN
- Nome gruppo IPSec
- Chiave

Ottenere queste informazioni dall'amministratore del server Easy VPN.

Configurare un client remoto Easy VPN

Questa procedura guidata mostra la configurazione di un client Easy VPN Remote Phase II.

Nota Se sul router non è in esecuzione un'immagine Cisco IOS che supporti Easy VPN Remote Phase II o versione successiva, non sarà possibile configurare un client Easy VPN.

Informazioni server

Le informazioni immesse in questa finestra identificano il tunnel Easy VPN, il server o concentratore Easy VPN cui tale router si collegherà, e il modo in cui si vuole che il traffico venga indirizzato nella VPN.

Nome connessione

Immettere il nome che si desidera attribuire alla connessione Easy VPN. Il nome deve essere univoco tra i nomi di tunnel Easy VPN per il router e non deve contenere spazi o caratteri speciali, ad esempio punti interrogativi (?).

Server Easy VPN

È possibile immettere le informazioni relative a un server Easy VPN primario e a uno secondario.

Server Easy VPN 1

Immettere l'indirizzo IP o il nome host del server o del concentratore Easy VPN primario a cui verrà connesso il router. Se si immette un nome host, è necessario un server DNS (Domain Name System) nella rete in grado di risolvere il nome host nell'indirizzo IP corretto per il dispositivo peer.

Server Easy VPN 2

Il campo Server Easy VPN 2 viene visualizzato quando l'immagine Cisco IOS sul router supporta Easy VPN Remote Phase III; in caso contrario, non è visualizzato.

Immettere l'indirizzo IP o il nome host del server o del concentratore Easy VPN secondario a cui verrà connesso il router. Se si immette un nome host, è necessario un server DNS sulla rete in grado di risolvere il nome host nell'indirizzo IP corretto per il dispositivo peer.

Modalità operativa

Scegliere Estensione rete o Client.

Selezionare **Client** se si desidera che i PC e altri dispositivi nelle reti interne del router formino una rete privata con indirizzi IP privati. Saranno utilizzati i protocolli NAT (Network Address Translation) e PAT (Port Address Translation). I dispositivi all'esterno della LAN non potranno effettuare il ping ai dispositivi nella LAN o raggiungerli direttamente.

Selezionare **Estensione rete** se si desidera che i dispositivi connessi alle interfacce interne dispongano di indirizzi IP instradabili e raggiungibili dalla rete di destinazione. I dispositivi sui due estremi della connessione formeranno una rete logica. Il PAT viene disattivato automaticamente consentendo ai PC e agli host sui due estremi della connessione di avere un accesso diretto reciproco.

Prima di selezionare questa impostazione interpellare l'amministratore del server o concentratore di Easy VPN.

Se si sceglie Estensione rete si può attivare la gestione remota del router selezionando la casella per la richiesta di un indirizzo IP assegnato dal server per il proprio router. Questo indirizzo IP può essere utilizzato per collegarsi al proprio router per la gestione remota e la risoluzione degli errori (ping, Telnet e Secure Shell). Questa modalità è nota come **Network Extension Plus**.

Nota Se il router non dispone di un'immagine Cisco IOS che supporti Easy VPN Remote Phase IV o successiva, non sarà possibile selezionare Network Extension Plus.

Autenticazione

Usare questa finestra per specificare la protezione per il tunnel remoto Easy VPN.

Autenticazione dispositivo

Selezionare Certificati digitali o Chiave precondivisa.

Nota L'opzione Certificati digitali è disponibile soltanto se supportata dall'immagine Cisco IOS presente sul proprio router.

Per utilizzare una chiave precondivisa, immettere il nome gruppo IPSec. Il nome del gruppo deve corrispondere al nome del gruppo definito sul server o concentratore VPN. Ottenere queste informazioni dall'amministratore di rete.

Immettere la chiave di gruppo IPSec. Tale chiave deve corrispondere alla chiave del gruppo definito sul server o concentratore VPN. Ottenere queste informazioni dall'amministratore di rete. Inserire nuovamente la chiave per confermarne la correttezza.

Autenticazione utente (XAuth)

L'Autenticazione utente (XAuth) è disponibile in questa finestra se la versione Cisco IOS presente sul router supporta Easy VPN Remote Phase III. Se l'autenticazione utente non è disponibile, essa deve essere impostata tramite riga di comando del router.

Scegliere una di queste opzioni per l'immissione del nome utente e della password XAuth:

- Manualmente in una finestra del browser web.

  Nota L'opzione browser web è disponibile soltanto se supportata dall'immagine Cisco IOS presente sul proprio router.

- Manualmente tramite la riga di comando o Cisco SDM
- Automaticamente salvando il nome utente e la password sul router.

Il server Easy VPN può utilizzare l'autenticazione XAuth per autenticare il router. Se il server consente il salvataggio della password, con questa opzione è possibile eliminare la necessità di immettere il nome utente e la password ogni volta che si stabilisce il tunnel Easy VPN. Immettere il nome utente e la password forniti dall'amministratore del server Easy VPN, e reimmettere la password per confermarne la correttezza. Le informazioni vengono salvate nel file di configurazione del router e utilizzate ogni volta che il tunnel viene stabilito.

Precauzione L'archiviazione di questi dati nella memoria del router crea un rischio di protezione, dal momento che chiunque abbia accesso alla configurazione del router può ottenere tali informazioni. Se non si desidera memorizzare i dati nel router, non inserirli in questa casella. Il server Easy VPN verificherà semplicemente il nome utente e la password nel router ogni volta che viene stabilita la connessione. Inoltre, Cisco SDM non può determinare se il server Easy VPN consente l'opzione per salvare la password. È necessario stabilire se il server permette tale salvataggio; in caso contrario, non è opportuno creare rischi di protezione inserendo le informazioni nella casella.

Impostazioni Interfacce e connessioni

Specificare in questa finestra le interfacce che verranno utilizzate nella configurazione Easy VPN.

Interfacce

Scegliere le interfacce interne ed esterne in questa casella.

Interfacce interne

Selezionare le interfacce interne (LAN) che servono le reti locali da includere in questa configurazione Easy VPN. È possibile selezionare più interfacce interne, con le seguenti restrizioni:

- Se si sceglie un'interfaccia che è già utilizzata in un'altra configurazione Easy VPN, il sistema comunica che l'interfaccia non può fare parte di due configurazioni Easy VPN.

- Se si scelgono interfacce già utilizzate in una configurazione Easy VPN, il sistema comunica che la configurazione di Easy VPN che si sta creando non può coesistere con la configurazione di Easy VPN esistente. Sarà quindi necessario scegliere se rimuovere i tunnel VPN esistenti da quelle interfacce e applicare ad essi la configurazione di Easy VPN.
- Le interfacce esistenti non vengono visualizzate nell'elenco delle interfacce se non possono essere usate in una configurazione Easy VPN. Per esempio le interfacce di loopback configurate sul router non compaiono nell'elenco.
- Un'interfaccia non può essere scelta come interfaccia interna e come interfaccia esterna.

I router serie Cisco 800 e Cisco 1700 supportano fino a tre interfacce interne. È possibile rimuovere le interfacce da una configurazione Easy VPN nella finestra Modifica Easy VPN Remote.

Interfacce esterne

Nell'elenco Interfacce, scegliere l'interfaccia esterna che si collega al server o concentratore Easy VPN.

Nota I router Cisco 800 non supportano l'utilizzo dell'interfaccia E 0 come interfaccia esterna

Impostazioni di connessione

Scegliere tra le attivazioni del tunnel VPN automatica, manuale o basata sul traffico.

Con l'impostazione manuale, è necessario fare clic sul pulsante **Connetti** o **Disconnetti** nella finestra Modifica Easy VPN Remote per stabilire o rimuovere il tunnel; tuttavia si ha il pieno controllo manuale sul tunnel mediante la finestra Modifica Easy VPN Remote. Inoltre, se per il router è impostato il timeout SA (Security Association), sarà necessario ristabilire manualmente il tunnel VPN ogni volta che si verifica un timeout. È possibile modificare le impostazioni di timeout SA nella finestra Impostazioni globali VPN di Componenti VPN.

Con l'impostazione automatica il tunnel VPN viene automaticamente stabilito nel momento in cui la configurazione di Easy VPN viene trasmessa al file di configurazione del router. Tuttavia non è possibile controllare manualmente il tunnel nella finestra Connessioni VPN. Quando si sceglie la connessione Easy VPN il pulsante Connetti o Disconnetti viene disattivato.

Con l'impostazione basata sul traffico il tunnel VPN viene automaticamente stabilito ogni volta che viene rilevato traffico (lato LAN) locale in uscita.

Nota L'opzione dell'attivazione basata su traffico è disponibile soltanto se supportata dalla versione Cisco IOS presente sul proprio router.

Riepilogo della configurazione

In questa finestra è visualizzata la configurazione Easy VPN che è stata creata e ne è consentito il salvataggio. Viene visualizzato un riepilogo simile al seguente:

```
Nome Easy VPN tunnel:test1
Easy VPN Server: 222.28.54.7
Gruppo: miaAzienda
Chiave: 1234
Controllo: Auto
Modalità: Client
Interfaccia esterna: BVI222
Interfacce interne: Dialer0
```

È possibile rivedere la configurazione in questa finestra e fare clic sul pulsante **Indietro** per modificare qualsiasi voce.

Facendo clic sul pulsante **Fine** le informazioni vengono immesse nella configurazione in esecuzione del router e, se il tunnel è stato configurato per il funzionamento automatico, il router tenta di contattare il concentratore o il server VPN.

Se si desidera modificare la configurazione Easy VPN successivamente, è possibile apportare le modifiche nella finestra Modifica Easy VPN Remote.

Nota In molti casi, il proprio router stabilisce la comunicazione con il server o il concentratore Easy VPN dopo avere fatto clic su **Fine** o su **Connetti** nella finestra Modifica Easy VPN Remote o nelle finestre Connessioni VPN. Tuttavia, se il dispositivo è stato configurato per l'utilizzo di XAuth, esso controlla il nome utente e la password sul router. Quando ciò si verifica, è necessario fornire un ID di accesso SSH (Secure Shell) e una password per eseguire la registrazione sul router e indicare l'accesso e la password XAuth per il server o il concentratore Easy VPN. È necessario eseguire questo processo ogni volta che si fa clic su **Fine** e la configurazione viene distribuita sul router e quando si disconnette e poi riconnette il tunnel nella finestra Modifica Easy VPN Remote. Scoprire se è utilizzata l'autenticazione XAuth e determinare il nome utente e la password richiesti.

Prova della connettività VPN

Se si sceglie di provare la connessione VPN appena configurata, i risultati del test saranno mostrati in un'altra finestra.

Modifica Easy VPN Remote

Le connessioni Easy VPN sono gestite da questa finestra. Una connessione Easy VPN indica una connessione configurata tra un client Easy VPN e un server o concentratore Easy VPN per fornire comunicazioni protette con altre reti che il server o concentratore supporta.

Nell'elenco delle connessioni sono visualizzate le informazioni sulle connessioni Easy VPN Remote configurate.

Stato

Lo stato della connessione indicato dalle icone e dagli avvisi riportati di seguito.

La connessione è attiva. Quando una connessione Easy VPN è attiva, il pulsante Disconnetti ne consente la disattivazione se il controllo del tunnel utilizzato è manuale.

La connessione non è attiva. Quando una connessione Easy VPN è disattivata, il pulsante Connetti ne consente l'attivazione se il controllo del tunnel utilizzato è manuale.

La connessione sta per essere stabilita.

XAuth richiesta: il server o il concentratore Easy VPN richiede un accesso e una password XAuth. Utilizzare il pulsante Accesso per immettere ID e password di accesso e stabilire la connessione.

Configurazione cambiata: la configurazione per questa connessione è stata modificata e deve essere trasmessa al router. Se la connessione fa uso del controllo manuale del tunnel, usare il pulsante Connetti per stabilire la connessione.

Nome

Il nome fornito alla connessione Easy VPN.

Modalità

Selezionare **Client** o **Estensione rete**. Nella modalità client, il concentratore o server VPN assegna un indirizzo IP singolo a tutto il traffico proveniente dal router; i dispositivi esterni alla LAN non hanno accesso diretto ai dispositivi nella LAN. Nella modalità di estensione rete, il concentratore o server VPN non sostituisce gli indirizzi IP e presenta una rete completamente instradabile ai peer sull'altra estremità della connessione VPN.

Dettagli

Scegliere una connessione Easy VPN Remote dall'elenco per vedere i valori delle impostazioni seguenti di tale connessione.

Autenticazione

Scegliere certificati digitali o chiave precondivisa. L'opzione chiave precondivisa mostra il gruppo utenti che condivide la chiave.

Interfaccia esterna

Questa è l'interfaccia che si collega al server o concentratore Easy VPN.

Interfacce interne

Sono le interfacce interne incluse nella connessione Easy VPN. Tutti gli host connessi a queste interfacce sono parte di VPN.

Easy VPN Server

I nomi o indirizzi IP dei server o concentratori Easy VPN. Se l'immagine Cisco IOS nel router supporta Easy VPN Remote Phase III, è possibile identificare due server o concentratori Easy VPN durante la configurazione tramite Cisco SDM.

Supporto subnet multiplo

Gli indirizzi delle subnet che non sono direttamente connesse al router ma possono utilizzare il tunnel. Un'ACL definisce quali sono le reti secondarie che sono autorizzate a fare uso del tunnel.

Attivazione tunnel

Scegliere tra automatica, manuale o basata sul traffico.

Se la connessione viene configurata con l'impostazione Manuale, è necessario fare clic sul pulsante **Connetti** per stabilire il tunnel; tuttavia è possibile avviarlo o interromperlo in qualsiasi momento facendo clic sul pulsante **Connetti** o **Disconnetti**.

Se la connessione è configurata con l'impostazione automatica il tunnel VPN verrà automaticamente stabilito quando la configurazione di Easy VPN sarà distribuita al file di configurazione del router. In questo caso, il pulsante **Connetti** o **Disconnetti** non viene attivato per questa connessione.

Se la connessione è configurata con l'impostazione basata sul traffico il tunnel VPN si stabilisce automaticamente ogni volta che viene rilevato del traffico qualificato per il router verso l'esterno. In questo caso, il pulsante **Connetti** o **Disconnetti** non viene attivato per questa connessione.

Connessione di backup

Una connessione Easy VPN Remote di backup configurata. Le connessioni di backup vengono configurate con la funzione Interfacce e connessioni di Cisco SDM.

Metodo di risposta XAuth

Se XAuth è attivato, il valore mostra una delle seguenti impostazioni sul modo in cui le credenziali XAuth vengono inviate:

- Devono essere immesse tramite Cisco SDM o dalla console del router
- Devono essere immesse da un browser del PC quando questo è aperto
- Le credenziali vengono inviate automaticamente perché sono state salvate sul router

Pulsante Aggiungi

Aggiungere una nuova connessione Easy VPN Remote.

Pulsante Modifica

Modifica una specifica connessione Easy VPN Remote.

Pulsante Elimina

Eliminare la connessione Easy VPN Remote specificata.

Pulsante Reimposta connessione

Fare clic per eliminare e ristabilire un tunnel con un peer.

Pulsante Verifica tunnel

Fare clic per verificare un tunnel VPN specificato. Il risultato della verifica è visibile in un'altra finestra.

Pulsante Connetti o Disconnetti o Accesso

Questo pulsante presenta la dicitura Connetti se si verificano tutte le seguenti condizioni:

- La connessione è configurata per l'uso del comando manuale del tunnel
- Il tunnel non è attivo
- La risposta XAuth *non* è impostata in modo tale da essere attivata da una sessione da un browser di PC.

Questo pulsante presenta la dicitura Disconnetti se si verificano tutte le seguenti condizioni:

- La connessione è configurata per l'uso del comando manuale del tunnel
- Il tunnel è attivo
- La risposta XAuth *non* è impostata in modo tale da essere attivata da una sessione di un browser del PC.

Questo pulsante presenta la dicitura Accesso se si verificano tutte le seguenti condizioni:

- Il server o concentratore Easy VPN che viene connesso fa uso di XAuth
- La risposta XAuth è impostata in modo tale da essere richiesta da Cisco SDM o dalla console del router
- Il tunnel è in attesa delle credenziali XAuth (Ia connessione è stata iniziata)

Se sulla connessione è impostato il controllo automatico o basato sul traffico del tunnel questo pulsante è disattivato.

Tabella riassuntiva funzioni

Funzione	Procedura
Creazione di una nuova connessione Easy VPN.	Fare clic su **Aggiungi** nella finestra Modifica Easy VPN Remote. Configurare la connessione nella finestra Aggiungi Easy VPN Remote e fare clic su **OK**. In questa finestra scegliere **Connetti** per la connessione al server Easy VPN.
Modifica di una connessione Easy VPN esistente.	Nella finestra Modifica Easy VPN Remote, scegliere la connessione da modificare e fare clic su **Modifica**. Si può vedere anche la seguente procedura: • Come modificare una connessione Easy VPN esistente?
Eliminazione di una connessione Easy VPN.	Nella finestra Modifica Easy VPN Remote, selezionare la connessione da eliminare e fare clic su **Elimina**.
Reimpostazione di una connessione stabilita tra il router e un peer VPN remoto. La connessione viene cancellata e ristabilita.	Selezionare una connessione attiva e fare clic su **Reimposta**. La finestra di stato visualizzata notifica l'esito della reimpostazione.
Eseguire una connessione a un server Easy VPN per il quale il router dispone di una connessione configurata.	Se la connessione utilizza il controllo manuale del tunnel, scegliere la connessione e fare clic su **Connetti**. Le connessioni che utilizzano il comando del tunnel automatico o basato sul traffico non possono essere attivate manualmente usando Cisco SDM. **Nota** Se il server o il concentratore Easy VPN è configurato per l'utilizzo di XAuth, il pulsante Connetti assume la dicitura Accesso e per completare la connessione è necessario immettere ad ogni attivazione il nome utente e la password. Ottenere queste informazioni dall'amministratore di rete. Se il server o concentratore remoto di Easy VPN richiede questa autenticazione è necessario prima fornire un ID e una password di accesso SSH (Secure Shell) per eseguire l'accesso al router e poi indicare il login e la password XAuth per il server o concentratore Easy VPN.

Funzione	Procedura
Eseguire una disconnessione da un server Easy VPN per il quale il router dispone di una connessione configurata.	Se la connessione utilizza il controllo manuale del tunnel, scegliere la connessione e fare clic su **Disconnetti**. Le connessioni che utilizzano il comando del tunnel automatico o basato sul traffico non possono essere disattivate manualmente usando Cisco SDM.
Determinare se è stata stabilita una connessione Easy VPN.	Quando viene stabilita la connessione, l'icona corrispondente è visualizzata nella colonna di stato.
Configurazione di un concentratore Easy VPN. Istruzioni per la configurazione di server e concentratori Easy VPN sono disponibili all'indirizzo www.cisco.com.	Il seguente collegamento fornisce le linee guida per la configurazione di un concentratore Cisco VPN 3000 per il funzionamento con un client Easy VPN Remote Phase II insieme ad altre informazioni utili. http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html (in inglese). La documentazione sulla serie Cisco VPN 3000 è disponibile al seguente indirizzo: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html (in inglese).
Consentire il passaggio del traffico attraverso il firewall verso il mio concentratore Easy VPN.	Vedere la sezione Come consentire il passaggio del traffico verso il concentratore Easy VPN attraverso il firewall?

Aggiungi o Modifica Easy VPN Remote

Utilizzare questa finestra per configurare il router con un client Easy VPN. Il router deve disporre di una connessione a un server o concentratore Easy VPN nella rete.

Nota Questa finestra viene visualizzata se l'immagine Cisco IOS nel router supporta Easy VPN Client Phase II.

La funzionalità Easy VPN Remote di Cisco implementa il protocollo Unity Client di Cisco che consente di definire la maggior parte dei parametri VPN in un server di accesso remoto VPN. Questo server può essere un dispositivo VPN dedicato, ad esempio un concentratore VPN 3000 o un Cisco PIX Firewall, oppure un router Cisco IOS che supporta il protocollo Cisco Unity Client.

Nota

- Se il server o il concentratore Easy VPN è stato configurato per utilizzare l'autenticazione XAuth, verranno richiesti un nome utente e una password ogni volta che il router stabilisce la connessione, anche quando la configurazione viene trasmessa al router e quando si esegue la disconnessione e la riconnessione del tunnel. Verificare se XAuth è utilizzato e quali sono il nome utente e la password richiesti.
- Se il router utilizza SSH (Secure Shell) è necessario immettere le informazioni di accesso e la password SSH la prima volta che si stabilisce la connessione.

Nome

Immettere un nome per la configurazione remota Easy VPN.

Modalità

Client: selezionare questa modalità se si desidera che i PC e altri dispositivi nelle reti interne del router formino una rete privata con indirizzi IP privati. Saranno utilizzati i protocolli NAT (Network Address Translation) e PAT (Port Address Translation). I dispositivi all'esterno della LAN non potranno effettuare il ping ai dispositivi nella LAN o raggiungerli direttamente.

Estensione rete: selezionare questa modalità se si desidera che i dispositivi connessi alle interfacce interne abbiano indirizzi IP instradabili e raggiungibili dalla rete di destinazione. I dispositivi sui due estremi della connessione formeranno una rete logica. Il PAT viene disattivato automaticamente consentendo ai PC e agli host sui due estremi della connessione di avere un accesso diretto reciproco.

Prima di selezionare questa impostazione interpellare l'amministratore del server o concentratore di Easy VPN.

Controllo tunnel

Selezionare **Automatico** o **Manuale**.

Con l'impostazione Manuale, è necessario fare clic sul pulsante **Connetti** nella finestra Modifica Easy VPN Remote per stabilire il tunnel; tuttavia si ha il pieno controllo manuale del tunnel nella finestra Connessioni VPN. I pulsanti Connetti e Disconnetti vengono disattivati ogni volta che si seleziona una connessione VPN con il controllo manuale del tunnel.

Con l'impostazione Automatico, il tunnel VPN viene stabilito automaticamente quando la configurazione Easy VPN è trasmessa al file di configurazione del router. Tuttavia non è possibile controllare manualmente il tunnel nella finestra Connessioni VPN. Se è selezionata questa connessione Easy VPN, i pulsanti Connetti e Disconnetti sono disattivati.

Server o Concentratore di Easy VPN

Specificare il nome o l'indirizzo IP del concentratore VPN o del server cui questo router si connette. Selezionare **Indirizzo IP** se si intende fornire un indirizzo IP oppure **Nome host** se si vuole fornire un nome host del server o del concentratore. Specificare il valore appropriato nel campo sottostante. Se si specifica un nome host, nella rete deve essere presente un server DNS che possa risolvere il nome host nell'indirizzo IP corretto. Se si immette un indirizzo IP, utilizzare il formato decimale separato da punti, ad esempio 172.16.44.1.

Gruppo

Nome gruppo

Immettere il nome gruppo IPSec. Il nome del gruppo deve corrispondere al nome del gruppo definito sul server o concentratore VPN. Ottenere queste informazioni dall'amministratore di rete.

Chiave di gruppo

Immettere la password di gruppo IPSec. Tale password deve corrispondere alla password del gruppo definita sul server o sul concentratore VPN. Ottenere queste informazioni dall'amministratore di rete.

Conferma chiave

Inserire nuovamente la password di gruppo per la conferma.

Interfacce

Interfaccia esterna verso il server o concentratore

Selezionare l'interfaccia che dispone della connessione al server o al concentratore Easy VPN.

Nota I router Cisco 800 non supportano l'utilizzo dell'interfaccia E 0 come interfaccia esterna.

Interfacce interne

Specificare le interfacce interne da includere nella configurazione Easy VPN. Tutti gli host connessi a queste interfacce faranno parte di VPN. I router serie Cisco 800 e Cisco 1700 supportano fino a tre interfacce interne.

Nota Un'interfaccia non può essere scelta come interfaccia interna e come interfaccia esterna.

Aggiungi o Modifica Easy VPN Remote - Impostazioni Easy VPN

Utilizzare questa finestra per configurare il router con un client Easy VPN. Il router deve disporre di una connessione a un server o concentratore Easy VPN nella rete.

Nota Questa finestra viene visualizzata se l'immagine Cisco IOS nel router supporta Easy VPN Client Phase III.

La funzionalità Easy VPN Remote di Cisco implementa il protocollo Unity Client di Cisco che consente di definire la maggior parte dei parametri VPN in un server di accesso remoto VPN. Questo server può essere un dispositivo VPN dedicato, ad esempio un concentratore VPN 3000 o un Cisco PIX Firewall, oppure un router Cisco IOS che supporta il protocollo Cisco Unity Client.

Nome

Immettere un nome per la configurazione remota Easy VPN.

Modalità

Client: selezionare la modalità **Client** se si desidera che i PC e altri dispositivi nelle reti interne del router formino una rete privata con indirizzi IP privati. Saranno utilizzati i protocolli NAT (Network Address Translation) e PAT (Port Address Translation). I dispositivi all'esterno della LAN non potranno effettuare il ping ai dispositivi nella LAN o raggiungerli direttamente.

Estensione rete: selezionare **Estensione rete** se si desidera che i dispositivi connessi alle interfacce interne dispongano di indirizzi IP instradabili e raggiungibili dalla rete di destinazione. I dispositivi sui due estremi della connessione formeranno una rete logica. Il PAT viene disattivato automaticamente consentendo ai PC e agli host sui due estremi della connessione di avere un accesso diretto reciproco.

Prima di selezionare questa impostazione interpellare l'amministratore del server o concentratore di Easy VPN.

Controllo tunnel

Selezionare **Automatico** o **Manuale**.

Con l'impostazione Manuale, è necessario fare clic sul pulsante **Connetti** nella finestra Connessioni VPN per stabilire il tunnel; tuttavia si ha il pieno controllo manuale del tunnel nella finestra Connessioni VPN. I pulsanti Connetti e Disconnetti vengono disattivati ogni volta che si seleziona una connessione VPN con il controllo manuale del tunnel.

Con l'impostazione Automatico, il tunnel VPN viene stabilito automaticamente quando la configurazione Easy VPN è trasmessa al file di configurazione del router. Tuttavia non è possibile controllare manualmente il tunnel nella finestra Connessioni VPN. Se è selezionata questa connessione Easy VPN, i pulsanti Connetti e Disconnetti sono disattivati.

Server

Si possono specificare fino a dieci server Easy VPN indicandone gli indirizzi IP o i nomi host, ed è possibile disporre l'elenco in modo da specificare l'ordine dei tentativi di connessione verso i vari server o router.

Aggiungi

Consente di specificare il nome o l'indirizzo IP di un concentratore o server VPN a cui si connette il router; quindi immettere l'indirizzo o il nome host nella finestra visualizzata.

Elimina

Fare clic per cancellare l'indirizzo IP o nome host specificato.

Sposta su

Fare clic per spostare verso l'alto l'indirizzo IP o nome host del server specificato. Il router tenterà di stabilire il collegamento ai router indicati nell'ordine in cui essi compaiono nell'elenco.

Sposta giù

Consente di spostare un indirizzo IP o il nome host selezionato in basso nell'elenco.

Interfaccia esterna verso il server o concentratore

Selezionare l'interfaccia che dispone della connessione al server o al concentratore Easy VPN.

Nota I router Cisco 800 non supportano l'utilizzo dell'interfaccia E 0 come interfaccia esterna.

Interfacce interne

Specificare le interfacce interne da includere nella configurazione Easy VPN. Tutti gli host connessi a queste interfacce faranno parte di VPN. I router serie Cisco 800 e Cisco 1700 supportano fino a tre interfacce interne.

Nota Un'interfaccia non può essere scelta come interfaccia interna e come interfaccia esterna.

Aggiungi o Modifica Easy VPN Remote - Informazioni di autenticazione

Questa finestra viene visualizzata se l'immagine Cisco IOS nel router supporta Easy VPN Client Phase III. Se l'immagine supporta Easy VPN Client Phase II, appare una finestra differente.

Usare la finestra per immettere le informazioni richieste perché il router venga autenticato dal server o dal concentratore Easy VPN.

Autenticazione dispositivo

Nome gruppo

Immettere il nome gruppo IPSec. Il nome del gruppo deve corrispondere al nome del gruppo definito sul server o concentratore VPN. Ottenere queste informazioni dall'amministratore di rete.

Chiave corrente

In questo campo sono visualizzati degli asterischi (*) se esiste un valore della chiave corrente IKE. Il campo risulta vuoto qualora non fosse stata configurata alcuna chiave.

Nuova chiave

Immettere una nuova chiave IKE in questo campo.

Conferma chiave

Reimmettere la nuova chiave per la conferma. Se i valori nei campi Nuova chiave e Conferma chiave non corrispondono, Cisco SDM richiede di inserirli nuovamente.

Autenticazione utente (XAuth)

Se il server o il concentratore Easy VPN è stato configurato per utilizzare l'autenticazione XAuth, verranno richiesti un nome utente e una password ogni volta che il router stabilisce la connessione, anche quando la configurazione viene trasmessa al router e quando si esegue la disconnessione e la riconnessione del tunnel. Determinare se è utilizzata l'autenticazione XAuth e ottenere il nome utente e la password richiesti.

Se l'autenticazione utente non è disponibile, essa deve essere impostata tramite riga di comando del router.

Scegliere una di queste opzioni per l'immissione del nome utente e della password XAuth:

- Da un PC

  Immettere manualmente il nome utente e la password in una finestra del browser web. Se si sceglie questa opzione è possibile selezionare la casella di controllo per utilizzare l'autenticazione HTTP di base per compensare i browser web che non supportano l'HTML 4.0 o JavaScript.

  Nota L'opzione browser web è disponibile soltanto se supportata dall'immagine Cisco IOS presente sul proprio router.

- Dal proprio router

  Immettere manualmente il nome utente e la password dalla riga di comando o da Cisco SDM.

- Automaticamente salvando il nome utente e la password sul router.

  Il server Easy VPN può utilizzare l'autenticazione XAuth per autenticare il router. Se il server consente il salvataggio della password, con questa opzione è possibile eliminare la necessità di immettere il nome utente e la password ogni volta che si stabilisce il tunnel Easy VPN. Immettere il nome utente e la password forniti dall'amministratore del server Easy VPN, e reimmettere la password per confermarne la correttezza. Le informazioni vengono salvate nel file di configurazione del router e utilizzate ogni volta che il tunnel viene stabilito.

Precauzione L'archiviazione di questi dati nella memoria del router crea un rischio di protezione, dal momento che chiunque abbia accesso alla configurazione del router può ottenere tali informazioni. Se non si desidera memorizzare i dati nel router, non inserirli in questa casella. Il server Easy VPN verificherà semplicemente il nome utente e la password nel router ogni volta che viene stabilita la connessione. Inoltre con Cisco SDM non è possibile rilevare automaticamente se il server Easy VPN consente il salvataggio delle password. È necessario stabilire se il server permette tale salvataggio; In caso contrario, per sicurezza, è opportuno evitare l'inserimento delle informazioni nella casella.

Immettere credenziali SSH

Se il router utilizza SSH (Secure Shell) è necessario immettere le informazioni di accesso e la password SSH la prima volta che si stabilisce la connessione. Utilizzare questa finestra per immettere i dati di accesso SSH e Telnet.

Immettere un nome utente valido

Immettere il nome utente dell'account SSH o Telnet che verrà utilizzato per l'accesso al router.

Immettere una password

Immettere la password associata al nome utente dell'account SSH o Telnet che verrà utilizzata per l'accesso al router.

Finestra Accesso XAuth

Questa finestra viene visualizzata quando il server Easy VPN richiede l'autenticazione estesa. Rispondere alla verifica immettendo le informazioni richieste, quali il nome utente dell'account, la password o altre informazioni, per stabilire correttamente il tunnel Easy VPN. Se non si è certi delle informazioni da fornire, contattare l'amministratore VPN.

Aggiungi o Modifica Easy VPN Remote - Impostazioni generali

Utilizzare questa finestra per configurare il router come client Easy VPN. Il router deve disporre di una connessione a un server o concentratore Easy VPN nella rete.

Nota Questa finestra viene visualizzata se l'immagine Cisco IOS caricata sul router supporta Easy VPN Client Phase IV.

La funzionalità Easy VPN Remote di Cisco implementa il protocollo Unity Client di Cisco che consente di definire la maggior parte dei parametri VPN in un server di accesso remoto VPN. Questo server può essere un dispositivo VPN dedicato, ad esempio un concentratore VPN 3000 o un Cisco PIX Firewall, oppure un router Cisco IOS che supporta il protocollo Cisco Unity Client.

Nome

Immettere un nome per la configurazione remota Easy VPN.

Server

Si possono specificare fino a dieci server Easy VPN indicandone gli indirizzi IP o i nomi host, ed è possibile disporre l'elenco in modo da specificare l'ordine dei tentativi di connessione verso i vari server o router.

Fare clic sul pulsante **Aggiungi** per specificare il nome o l'indirizzo IP di un concentratore o server VPN a cui si connette il router; quindi immettere l'indirizzo o il nome host nella finestra visualizzata.

Fare clic sul pulsante **Elimina** per eliminare l'indirizzo IP o il nome host specificato.

Fare clic sul pulsante **Sposta su** per spostare verso l'alto l'indirizzo IP o il nome host del server specificato nell'elenco. Il router tenterà di stabilire il collegamento ai router indicati nell'ordine in cui essi compaiono nell'elenco.

Fare clic sul pulsante **Sposta giù** per spostare verso il basso l'indirizzo IP o il nome host del server specificato nell'elenco.

Modalità

Client: selezionare la modalità **Client** se si desidera che i PC e gli altri dispositivi nelle reti interne del router formino una rete privata con indirizzi IP privati. Saranno utilizzati i protocolli NAT (Network Address Translation) e PAT (Port Address Translation). I dispositivi all'esterno della LAN non potranno effettuare il ping ai dispositivi nella LAN o raggiungerli direttamente.

Estensione rete: selezionare **Estensione rete** se si desidera che i dispositivi connessi alle interfacce interne dispongano di indirizzi IP instradabili e raggiungibili dalla rete di destinazione. I dispositivi sui due estremi della connessione formeranno una rete logica. Il PAT viene disattivato automaticamente consentendo ai PC e agli host sui due estremi della connessione di avere un accesso diretto reciproco.

Prima di selezionare questa impostazione interpellare l'amministratore del server o concentratore di Easy VPN.

Scegliendo Estensione rete si sarà anche in grado di:

- Consentire l'uso del tunnel alle subnet non direttamente connesse al router.

  Per consentire l'utilizzo del tunnel alle subnet non direttamente connesse al router fare clic sul pulsante **Opzioni** e configurare le opzioni di estensione della rete.

- Attivare la gestione remota e la risoluzione degli errori del proprio router.

  È possibile attivare la gestione remota del router selezionando la casella per la richiesta di un indirizzo IP assegnato dal server per il proprio router. Questo indirizzo IP può essere utilizzato per collegarsi al proprio router per la gestione remota e la risoluzione degli errori (ping, Telnet e Secure Shell). Questa modalità è denominata **Network Extension Plus**.

Opzioni di Estensione rete

Per consentire l'uso del tunnel alle subnet non direttamente connesse al router compiere i seguenti passi:

Passo 1 Nella finestra Opzioni selezionare la casella per consentire subnet multiple.

Passo 2 Scegliere di immettere le subnet manualmente oppure selezionare una ACL (Access Control List) esistente.

Passo 3 Per immettere manualmente le subnet fare clic sul pulsante **Aggiungi** e immettere l'indirizzo e la maschera della subnet. Cisco SDM genererà una ACL automaticamente.

Nota Le subnet immesse *non* devono essere direttamente connesse al router.

Passo 4 Per aggiungere un'ACL esistente immettere il suo nome oppure sceglierla dall'elenco a tendina.

Aggiungi o Modifica Easy VPN Remote - Informazioni di autenticazione

Usare la finestra per immettere le informazioni richieste perché il router venga autenticato dal server o dal concentratore Easy VPN.

Autenticazione dispositivo

Selezionare Certificati digitali o Chiave precondivisa.

Se si utilizza una chiave precondivisa, richiedere all'amministratore di rete il nome del gruppo IPSec e il valore della chiave IKE. Il nome deve corrispondere al nome del gruppo definito sul server o concentratore VPN.

Immettere il nome del gruppo IPSec nel campo Nome gruppo e il nuovo valore chiave IKE nel campo Nuova chiave. Immettere ancora la nuova chiave per la conferma nel campo Conferma chiave. Se i valori nei campi Nuova chiave e Conferma chiave non corrispondono, Cisco SDM richiede di inserirli nuovamente.

Il campo Chiave corrente visualizza degli asterischi (*) per mascherare il valore chiave IKE corrente. Il campo risulta vuoto qualora non fosse stata configurata alcuna chiave.

Autenticazione utente

Se il server o il concentratore Easy VPN è stato configurato per utilizzare l'autenticazione XAuth, verranno richiesti un nome utente e una password ogni volta che il router stabilisce la connessione, anche quando la configurazione viene trasmessa al router e quando si esegue la disconnessione e la riconnessione del tunnel. Determinare se è utilizzata l'autenticazione XAuth e ottenere il nome utente e la password richiesti.

Se il server consente il salvataggio delle password, con questa opzione è possibile eliminare la necessità di immettere il nome utente e la password ogni volta che si stabilisce il tunnel Easy VPN. Le informazioni vengono salvate nel file di configurazione del router e utilizzate ogni volta che il tunnel viene stabilito.

Scegliere una di queste opzioni per l'immissione del nome utente e della password XAuth:

- Manualmente in una finestra del browser web.

Nota L'opzione browser web è disponibile soltanto se supportata dall'immagine Cisco IOS presente sul proprio router.

- Manualmente tramite la riga di comando o Cisco SDM
- Automaticamente salvando il nome utente e la password sul router.

  Il server Easy VPN può utilizzare l'autenticazione XAuth per autenticare il router. Se il server consente il salvataggio delle password, con questa opzione è possibile eliminare la necessità di immettere il nome utente e la password ogni volta che si stabilisce il tunnel Easy VPN. Immettere il nome utente e la password forniti dall'amministratore del server Easy VPN, e reimmettere la password per confermarne la correttezza.

Nota Il campo Chiave corrente visualizza degli asterischi (*) per mascherare il valore chiave IKE corrente. Se questo campo è vuoto non è stata configurata nessuna chiave.

Le informazioni vengono salvate nel file di configurazione del router e utilizzate ogni volta che il tunnel viene stabilito.

Precauzione L'archiviazione di questi dati nella memoria del router crea un rischio di protezione, dal momento che chiunque abbia accesso alla configurazione del router può ottenere tali informazioni. Se non si desidera memorizzare i dati nel router, non inserirli in questa casella. Il server Easy VPN verificherà semplicemente il nome utente e la password nel router ogni volta che viene stabilita la connessione. Inoltre con Cisco SDM non è possibile rilevare automaticamente se il server consente il salvataggio delle password. È necessario stabilire se il server permette tale salvataggio; In caso contrario, per sicurezza, è opportuno evitare l'inserimento delle informazioni nella casella.

Aggiungi o Modifica Easy VPN Remote - Interfacce e connessioni

In questa finestra è possibile impostare le interfacce interna ed esterna, e specificare in che modo il tunnel viene attivato.

Interfacce interne

Scegliere l'interfaccia interna (LAN) da associare a questa configurazione di Easy VPN. È possibile selezionare più interfacce interne, con le seguenti restrizioni:

- Se si scelgono interfacce già utilizzate in un'altra configurazione Easy VPN, il sistema comunica che l'interfaccia non può fare parte di due configurazioni Easy VPN.
- Se si scelgono interfacce già utilizzate in una configurazione Easy VPN standard, il sistema comunica che la configurazione di Easy VPN che si sta creando non può coesistere con la configurazione di Easy VPN esistente. Cisco SDM richiederà se si desidera rimuovere i tunnel VPN esistenti da tali interfacce e applicare a questi la configurazione Easy VPN.
- Le interfacce esistenti non vengono visualizzate nell'elenco delle interfacce se non possono essere usate in una configurazione Easy VPN. Per esempio le interfacce di loopback configurate sul router non compaiono nell'elenco.
- Un'interfaccia non può essere scelta come interfaccia interna e come interfaccia esterna.

I router serie Cisco 800 e Cisco 1700 supportano fino a tre interfacce interne. È possibile rimuovere le interfacce da una configurazione Easy VPN nella finestra Modifica Easy VPN Remote.

Interfaccia esterna

Scegliere l'interfaccia esterna che si collega al server o concentratore Easy VPN.

Nota I router Cisco 800 non supportano l'utilizzo dell'interfaccia E 0 come interfaccia esterna

Interfaccia tunnel virtuale

Selezionare questa opzione se si desidera utilizzare un'interfaccia tunnel virtuale (VTI) per questa connessione. Se le VTI di questo elenco vengono utilizzate da altre connessioni VPN, fare clic su **Aggiungi** per crearne una nuova.

Controllo di connessione

Scegliere tra le attivazioni del tunnel VPN automatica, manuale o traffico interessante.

Con l'impostazione manuale è necessario fare clic sul pulsante **Connetti** o **Disconnetti** nella finestra Modifica Easy VPN Remote per stabilire o rimuovere il tunnel; tuttavia si ha il pieno controllo manuale sul tunnel nella finestra Modifica Easy VPN Remote. Inoltre, se per il router è impostato il timeout SA (Security Association), sarà necessario ristabilire manualmente il tunnel VPN ogni volta che si verifica un timeout. È possibile modificare le impostazioni di timeout SA nella finestra Impostazioni globali VPN di Componenti VPN.

Con l'impostazione automatica il tunnel VPN viene automaticamente stabilito nel momento in cui la configurazione di Easy VPN viene trasmessa al file di configurazione del router. Tuttavia non è possibile controllare manualmente il tunnel nella finestra Connessioni VPN. Quando si imposta questo tipo di connessione Easy VPN il pulsante Connetti (o Disconnetti) viene disattivato.

Con l'attivazione basata sul traffico interessante, il tunnel VPN viene automaticamente stabilito ogni volta che viene rilevato traffico (lato LAN) locale in uscita. Quando si imposta questo tipo di connessione Easy VPN il pulsante Connetti (o Disconnetti) viene disattivato.

Nota L'opzione Traffico interessante è disponibile soltanto se supportata dall'immagine Cisco IOS presente sul proprio router.

Informazioni aggiuntive

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come modificare una connessione Easy VPN esistente?

Per modificare una connessione esistente di Easy VPN Remote, eseguire i seguenti passi:

Passo 1 Dal frame di sinistra, selezionare **VPN**.

Passo 2 Nella struttura VPN, selezionare **Easy VPN Remote**.

Passo 3 Fare clic sulla scheda **Modifica Easy VPN Remote** e selezionare la connessione da modificare.

Passo 4 Fare clic su **Modifica.**

Viene visualizzata la finestra Modifica Easy VPN Remote.

Passo 5 Nella finestra Modifica Easy VPN Remote, fare clic sulle schede per visualizzare i valori che si desidera modificare.

Passo 6 Una volta apportate le modifiche, fare clic su **OK**.

Come si configura il backup di una connessione Easy VPN?

Per poter configurare una connessione di backup per Easy VPN Remote, il router deve disporre di un'interfaccia modem ISDN, asincrono o analogico.

Se l'interfaccia modem ISDN, asincrona o analogica non è stata configurata eseguire i passi seguenti:

Passo 1 Dal frame di sinistra, fare clic su **Interfacce e connessioni**.

Passo 2 Fare clic sulla scheda **Crea connessione**.

Passo 3 Scegliere l'interfaccia modem ISDN, asincrona o analogica dall'elenco.

Passo 4 Fare clic sul pulsante **Crea nuova connessione** e utilizzare la procedura guidata per configurare la nuova interfaccia.

Passo 5 Nella finestra prevista dalla procedura guidata impostare la nuova interfaccia come backup per una connessione Easy VPN Remote.

Se l'interfaccia modem ISDN, asincrona o analogica è stata configurata eseguire i passi seguenti:

Passo 1 Dal frame di sinistra, fare clic su **Interfacce e connessioni**.

Passo 2 Fare clic sulla scheda **Modifica interfaccia/connessione**.

Passo 3 Scegliere l'interfaccia modem ISDN, asincrona o analogica dall'elenco delle interfacce configurate.

Passo 4 Fare clic sul pulsante **Modifica**.

Passo 5 Fare clic sulla scheda **Backup** e configurare il backup per una connessione Easy VPN Remote.

Passo 6 Al termine della configurazione del backup, fare clic su **OK**.

CAPITOLO 11

Easy VPN Server

Nella funzionalità Easy VPN Server viene presentato il supporto server per client software Cisco VPN Client Release 3.x e successiva e client hardware Cisco VPN. Grazie a questa funzionalità un utente finale remoto può comunicare mediante IPSec (Protezione IP) con qualsiasi altro gateway VPN di Cisco IOS. I criteri IPSec gestiti a livello centrale vengono “inviati” al client tramite il server, semplificando la configurazione da parte dell'utente finale.

Al seguente link vi sono informazioni generali sulla soluzione Easy VPN di Cisco e altri link per informazioni più specifiche.

http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html (in inglese)

Creazione di un server Easy VPN

In questa procedura guidata sono illustrate le fasi necessarie per configurare un server Easy VPN nel router.

Questa procedura guidata facilita l’esecuzione delle seguenti attività finalizzate alla corretta configurazione di un Server Easy VPN su questo router.

- Scelta dell'interfaccia sulla quale termineranno le connessioni client e del metodo di autenticazione utilizzato per i server e i client Easy VPN
- Configurazione di criteri IKE.
- Configurazione di un set di trasformazione IPSec.
- Configurazione del metodo di autorizzazione di gruppo e di ricerca dei criteri di gruppo

- Configurazione dell'autenticazione utente
- Configurazione dei server RADIUS esterni
- Configurazione dei criteri per gli utenti remoti che si connettono ai client Easy VPN

Creare un server Easy VPN

Consente di creare la configurazione di un server Easy VPN nel router.

Pulsante Avvia procedura guidata Server Easy VPN

Consente di avviare la procedura guidata.

Procedura guidata del server Easy VPN

In questa finestra sono riepilogate le attività che verranno eseguite quando si utilizza la procedura.

Interfaccia e Autenticazione

Questa finestra permette di scegliere l'interfaccia nella quale si desidera configurare il Server Easy VPN.

Se si sceglie un'interfaccia già configurata in precedenza con un criterio IPSec site-to-site, in Cisco SDM viene visualizzato un messaggio indicante che tale criterio esiste già nell'interfaccia. Il criterio IPSec esistente è utilizzato da Cisco SDM per configurare Easy VPN Server.

Se l'interfaccia selezionata fa parte di un Easy VPN Remote, GREoIPSec o dell'interfaccia DMVPN, Cisco SDM visualizza un messaggio per la selezione di un'altra interfaccia.

Dettagli

Fare clic su questo pulsante per ottenere informazioni dettagliate sull'interfaccia selezionata. La finestra dei dettagli visualizza tutte le regole di accesso, i criteri IPSec, le regole NAT o le Inspection Rule associate all'interfaccia.

Fare clic su questo pulsante per ottenere dettagli sull'interfaccia scelta.

Autenticazione

Scegliere chiavi precondivise, certificati digitali o ambedue.

Se si sceglie chiavi precondivise, quando si configura la finestra di impostazione generale Aggiungi policy di gruppo si deve immettere un valore della chiave.

Se si sceglie certificati digitali, i campi chiavi precondivise non vengono visualizzati nella finestra di impostazione generale Aggiungi policy di gruppo.

Se si scelgono ambedue le opzioni certificati digitali e chiavi precondivise, l'immissione di un valore chiave nella finestra di impostazione generale Aggiungi policy di gruppo è opzionale.

Autorizzazione gruppo e ricerca criterio gruppo

In questa finestra è possibile definire un nuovo elenco di metodi di rete di autorizzazione AAA per la ricerca dei criteri di gruppo o selezionare un elenco metodi di rete esistente.

Solo locale

Con questa opzione è possibile creare un elenco di metodi solo per il database locale.

Solo RADIUS

Con questa opzione è possibile aggiungere dettagli sull'autenticazione utente per il database RADIUS.

Solo RADIUS e locale

Con questa opzione è possibile aggiungere dettagli sull'autenticazione utente per il database RADIUS e quello locale.

Tabella riassuntiva funzioni

Funzione	Procedura
Definizione di un elenco di metodi AAA per RADIUS e per il database locale. Quando si definiscono gli elenchi dei metodi per un RADIUS e per il database locale, nel router viene esaminato prima il server RADIUS e successivamente il database locale per l'autenticazione di gruppo.	Selezionare **Solo RADIUS e locale**. Fare clic su **Avanti**.
Definire un elenco di metodi AAA solo per il database locale. Quando si definisce un elenco di metodi AAA per il database locale, nel router viene esaminato il database locale per l'autenticazione di gruppo.	Selezionare **Solo locale**. Fare clic su **Avanti**.
Selezionare uno degli elenchi di metodi esistenti per l'autenticazione di gruppo. Quando si desidera definire gli elenchi di metodi AAA, si può considerare di selezionare un elenco di metodi già esistente.	Selezionare **Choose an existing AAA method list** (Selezionare un elenco metodi AAA esistente). Fare clic su **Avanti**.

Autenticazione utente (XAuth)

È possibile configurare l'autenticazione utente in Easy VPN Server. I dettagli sull'autenticazione utente possono essere archiviati in un server esterno, ad esempio un server RADIUS o un database locale o in entrambi. L'elenco metodi di autenticazione dell'accesso AAA viene utilizzato per stabilire l'ordine in cui ricercare i dettagli sull'autenticazione utente.

Solo locale

Con questa opzione è possibile aggiungere dettagli sull'autenticazione utente per il database locale.

Solo RADIUS e locale

Con questa opzione è possibile aggiungere dettagli sull'autenticazione utente per RADIUS e per il database locale.

Choose an existing AAA Method List (Selezionare un elenco metodi AAA esistente)

Con questa opzione è possibile selezionare un elenco di metodi dall'elenco di tutti gli elenchi dei metodi configurati nel router.

L'elenco metodi selezionato è utilizzato per l'autenticazione estesa.

Pulsante Aggiungi credenziali utente

Consente di aggiungere un account utente.

Account utente per XAuth

Consente di aggiungere un account per un utente da autenticare dopo l'autenticazione del dispositivo da parte di IKE.

Account utente

Gli account utente autenticati mediante autenticazione XAuth sono elencati in questa casella. Sono visibili il nome di account e il livello di privilegio.

Pulsante Aggiungi o Modifica

Utilizzare questi pulsanti per aggiungere o modificare gli account utente Gli account utente possono essere eliminati nella finestra **Attività aggiuntive > Accesso al router > Vista/Account utente**.

Nota Gli account utente della vista CLI non possono essere modificati da questa finestra. Se è necessario modificare gli account utente, andare in **Attività aggiuntive > Accesso al router > Account utente/Vista CLI**.

Aggiungi server RADIUS

In questa finestra è possibile aggiungere un nuovo server RADIUS, o modificare o eseguire il ping a un server RADIUS esistente.

Aggiungi

Consente di aggiungere un nuovo server RADIUS.

Modifica

Consente di modificare una configurazione del server RADIUS già esistente.

Esegui ping

Consente di eseguire il ping a un server RADIUS già esistente o a un server RADIUS appena configurato.

Criteri autorizzazione di gruppo / utente

In questa finestra è possibile aggiungere, modificare, duplicare o eliminare i criteri di gruppo utente nel database locale.

In tale finestra sono elencati i criteri di gruppo già configurati.

Nome gruppo

Nome fornito al gruppo utente.

Pool

Nome del pool di indirizzi IP dal quale vengono assegnati gli indirizzi IP agli utenti che si connettono da questo gruppo.

DNS

Indirizzo del server DNS del gruppo.

Questo indirizzo DNS viene inviato (“pushed”) agli utenti che si connettono a tale gruppo.

WINS

Indirizzo WINS (Windows Internet Naming Service) del gruppo.

L' indirizzo WINS viene inviato (“pushed”) agli utenti che si connettono a tale gruppo.

Nome di dominio

Nome di dominio del gruppo.

Questo nome di dominio viene inviato (“pushed”) agli utenti che si connettono a tale gruppo.

Suddividi ACL

ACL (Access Control List) che rappresenta le reti secondarie protette per la gestione dello ‘split tunnel’.

Timer inattività

La disconnessione dei tunnel VPN inattivi può contribuire a rendere più efficiente il funzionamento del Server Easy VPN grazie al recupero delle risorse non utilizzate.

Fare clic sulla casella di controllo **Configura Timer d'inattività** e immettere un valore per il tempo massimo per il quale il tunnel VPN può rimanere inattivo senza essere disconnesso. Immettere le ore nel campo di sinistra, i minuti nel campo di centro e i secondi nel campo di destra. Il tempo minimo consentito è 1 minuto.

Informazioni generali del gruppo

In questa finestra è possibile configurare, modificare e duplicare i criteri di gruppo.

Immettere un nome per questo Gruppo

Immettere il nome di gruppo nel campo fornito. Se il criterio di gruppo viene modificato, il campo è disattivato. Se si duplica un criterio di gruppo, è necessario immettere un nuovo valore nel campo.

Chiave precondivisa

Immettere la chiave precondivisa nei campi forniti.

Il campo **Chiave corrente** non può essere modificato.

Nota Non è necessario immettere una chiave preshared se per l'autenticazione del gruppo si stanno usando certificati digitali. I certificati digitali vengono utilizzato anche per l'autenticazione degli utenti.

Informazioni pool

Specifica un pool locale di indirizzi IP che vengono utilizzati per assegnare gli indirizzi IP ai client.

Crea un nuovo pool

Immettere l'intervallo di indirizzi IP per il pool di indirizzi IP locale nel campo Intervallo indirizzi IP.

Seleziona da un pool esistente

Selezionare l'intervallo di indirizzi IP dal pool di indirizzi IP esistente.

Nota Questo campo non può essere modificato se non ci sono pool di indirizzi IP predefiniti.

Subnet Mask (opzionale)

Immettere una subnet mask da inviare insieme agli indirizzi IP assegnati ai client di questo gruppo.

Numero massimo di connessioni consentite

Specificare il numero massimo di connessioni di client al Server Easy VPN consentite da questo gruppo.

In Cisco SDM sono consentite un massimo di 5000 connessioni per gruppo.

Tabella riassuntiva funzioni

Funzione	Procedura
Autenticazione dei client associati al gruppo.	Immettere la chiave nel campo Chiave precondivisa.
Crea un pool locale di indirizzi IP da assegnare ai client.	Immettere l'intervallo di indirizzi IP nel campo Crea un nuovo pool nell'area Informazioni pool.
Scegliere un intervallo di indirizzi IP dal pool esistente da assegnare ai client.	Scegliere l'intervallo di indirizzi IP dal campo Seleziona da un pool esistente nell'area Informazioni pool.

Configurazione DNS e WINS

In questa finestra si possono specificare le informazioni relative ai server DNS (Domain Name Service), e i server WINS (Windows Internet Naming Service).

DNS

Immettere l'indirizzo IP del server DNS primario e secondario nei campi forniti. L'immissione dell'indirizzo del server DNS è facoltativa.

WINS

Immettere l'indirizzo IP del server WINS primario e secondario nei campi forniti. L'immissione dell'indirizzo del server WINS è facoltativa.

Nome di dominio

Specificare il nome di dominio da inviare al client Easy VPN.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurare un server DNS.	Selezionare l'opzione **DNS**. Quindi immettere l'indirizzo IP del server DNS primario e di quello secondario nei campi visualizzati.
Configurare un server WINS.	Selezionare l'opzione **WINS**. Immettere gli indirizzi IP dei server WINS primario e secondario nei campi visualizzati.
Specificazione di un nome da inviare al client Easy VPN.	Immettere il nome di dominio nel campo **Nome di dominio**.

Suddivisione tunnel

In questa finestra è possibile suddividere il tunnel per il gruppo utente che si aggiunge.

La suddivisione dei tunnel consente di disporre di un tunnel sicuro per il sito centrale e di tunnel simultanei di testo non codificato per Internet. Per esempio tutto il traffico originato dal client viene inviato alla rete secondaria di destinazione mediante il tunnel VPN.

Inoltre, è possibile specificare quali gruppi di ACL rappresentano le subnet protette per la suddivisione del tunnel.

Attiva suddivisione tunnel

In questa casella è possibile aggiungere subnet protette e ACL per la suddivisione del tunnel.

Immettere le subnet protette

Aggiungere o rimuovere le sottoreti per le quali i pacchetti vengono inviati mediante tunnel dai client VPN.

Selezionare l'ACL di suddivisione del tunnel

Selezionare l'ACL da utilizzare per la suddivisione del tunnel.

Split DNS

Immettere i nomi di dominio Internet che possono essere risolti dal server DNS della propria rete. Si applicano le seguenti restrizioni:

- Sono consentite soltanto 10 voci
- Le voci devono essere separate con una virgola.
- Non usare spazi in nessun punto dell'elenco delle voci.
- Le voci duplicate e quelle con formati non validi non sono ammesse.

Nota Questa funzione appare soltanto se supportata dalla versione IOS del proprio server Cisco.

Tabella riassuntiva funzioni

Funzione	Procedura
Attivazione della suddivisione del tunnel.	Selezionare l'opzione **Attiva suddivisione del tunnel**.
Aggiunta di una subnet protetta.	Selezionare **Immettere le subnet protette** e fare clic su **Aggiungi**.
Eliminazione di una subnet protetta.	Scegliere **Immettere le subnet protette** e fare clic su **Elimina**.
Selezione dell'ACL da utilizzare per la suddivisione del tunnel.	Scegliere **Selezionare l'ACL di suddivisione del tunnel** e scegliere l'ACL tra le opzioni disponibili.
Utilizzo del server DNS della rete per risolvere determinati nomi di dominio.	Selezionare l'opzione **Attiva suddivisione tunnel** e immettere i nomi di dominio nel campo fornito. Inoltre è necessario configurare le subnet o selezionare un'ACL.

Impostazioni del client

Da questa finestra è possibile configurare attributi aggiuntivi per i criteri di protezione, come l'aggiunta o la rimozione di un server di backup, un Firewall Are-U-There, e Include-Local-LAN.

Nota Alcune delle funzioni descritte sotto sono visualizzate soltanto se supportate dalla versione IOS del proprio server Cisco.

Server di backup

È possibile specificare fino a 10 server in base all'indirizzo IP o al nome host come backup per il server Easy VPN e ordinare l'elenco per controllare i server ai quali il router eseguirà il primo tentativo di connessione nel caso in cui non sia possibile effettuare la connessione primaria al server Easy VPN.

Aggiungi

Fare clic su questo pulsante per specificare il nome o l'indirizzo IP di un server Easy VPN a cui si connette il router quando la connessione primaria non riesce; quindi immettere l'indirizzo o il nome host nella finestra visualizzata.

Elimina

Fare clic per eliminare un indirizzo IP o nome host specificato.

Configurazione - Push

È possibile specificare un file di configurazione di Easy VPN client usando un URL e un numero di versione. Il client Easy VPN invia l'URL e il numero di versione ai client hardware di Easy VPN che richiedono tale informazione. Solo i client hardware Easy VPN che appartengono alle policy del gruppo che si sta configurando possono richiedere l'URL e il numero di versione che si immette in questa finestra.

Immettere l'URL del file di configurazione nel campo URL. L'URL deve cominciare con un protocollo appropriato, e può includere nomi utente e password. Gli esempi seguenti sono URL per il download di un file di aggiornamento chiamato sdm.exe:

- http://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- https://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- ftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- tftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- scp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- rcp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe
- cns:
- xmodem:
- ymodem:
- null:
- flash:sdm.exe
- nvram:sdm.exe
- usbtoken[0-9]:sdm.exe

  L'intervallo di numeri della porta USB token va da 0 a 9. Ad esempio, per un token USB applicato alla porta USB 0, l'URL è usbtoken0:sdm.exe.
- usbflash[0-9]:sdm.exe

  L'intervallo di numeri della porta USB flash va da 0 a 9. Ad esempio, per un flash USB applicato alla porta USB 0, l'URL è usbtoken0:sdm.exe.
- disk[0-1]:sdm.exe

  Il numero del disco è 0 o 1. Ad esempio, per un disco numero 0, l'URL è disk0:sdm.exe.
- archive:sdm.exe
- tar:sdm.exe
- system:sdm.exe

In questi esempi, *username* è il nome utente e *password* è la password del sito.

Immettere il numero di versione del file nel campo Versione. Il numero di versione deve essere compreso tra 1 e 32767.

Browser Proxy

È possibile specificare le impostazioni del browser proxy per i client software Easy VPN. Il client Easy VPN invia l'URL e il numero di versione ai client hardware di Easy VPN che richiedono tale informazione. Solo i client software Easy VPN che appartengono alle policy del gruppo che si sta configurando possono richiedere l'impostazione del browser proxy che si immette in questa finestra.

Immettere il nome col quale si salvano le impostazioni proxy del server, oppure scegliere una delle seguenti voci del menu a tendina:

- Scegliere un'impostazione esistente…

  Apre una finestra con un elenco delle impostazioni browser Proxy esistenti.

- Creare nuova impostazione e selezionare…

  Apre una finestra in cui si possono creare nuove impostazioni browser proxy.

- Nessuno

  Elimina eventuali impostazioni del browser proxy assegnate al gruppo.

Firewall di tipo Are-U-There

È possibile limitare le connessioni VPN ai client sui quali sono in esecuzione firewall personali quali Black Ice o Zone Alarm.

Includi LAN locale

È possibile consentire l'accesso da una connessione tunnel non suddivisa alla rete secondaria locale contemporaneamente al client.

Perfect Forward Secrecy (PFS)

Abilitare la PFS se è richiesta dalle associazioni di protezione(SA) IPSec che si stanno usando.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di un server di backup.	Fare clic su **Aggiungi** nell'area Server di backup. Aggiungere l'indirizzo IP o il nome host del server di backup nella finestra visualizzata.
Eliminazione di un server di backup.	Selezionare il server di backup da eliminare dall'area Server di backup e fare clic su **Elimina**.
Riordinare i server di backup.	Eliminare i server di backup e ricrearli nell'ordine voluto.
Attivare il Firewall di tipo Are-U-There.	Selezionare l'opzione **Firewall di tipo Are-U-There**.
Attivare Includi LAN locale.	Selezionare l'opzione **Includi LAN locale**.
Specificare il numero massimo di connessioni client consentite per il gruppo che si sta creando.	Immettere il numero nel campo **Connessioni massime consentite nel gruppo**.

Scegliere le Impostazioni del Browser Proxy

Dall'elenco a tendina, scegliere le impostazioni del proxy del browser che si desidera assegnare al gruppo.

Nota Per aggiungere nuove impostazioni, scegliere **Aggiungi impostazioni browser** dal menu a tendina delle impostazioni browser nella finestra Impostazioni client o selezionare **Componenti VPN > Server Easy VPN > Impostazioni Proxy Browser** e fare clic su **Aggiungi**. Per eliminare le impostazioni, selezionare **Componenti VPN > Server Easy VPN > Impostazioni Proxy Browser** e fare clic su **Elimina**.

Aggiungi o Modifica impostazioni Proxy del Browser

In questa finestra si possono aggiungere o modificare le impostazioni del browser proxy.

Nome delle impostazioni Proxy Browser

Se si stanno aggiungendo impostazioni del browser proxy, immettere un nome che verrà visualizzato nei menu a tendina che elencano le impostazioni proxy del server. Quando si modificano le impostazioni proxy del browser, il campo nome è di sola lettura.

Impostazioni Proxy

Scegliere una opzioni seguenti:

- Senza Proxy Server

  Non si desidera che i client di questo gruppo utilizzino un server proxy quando viene utilizzato il tunnel VPN.

- Rileva automaticamente le impostazioni

  Si vuole che i client di questo gruppo rilevino automaticamente un proxy server quando utilizzano il tunnel VPN.

- Configurazione Proxy manuale

  Per i client di questo gruppo si intende configurare manualmente un proxy server.

Se si sceglie Configurazione proxy manuale, eseguire i passi seguenti per configurare manualmente un proxy server:

Passo 1 Immettere l'indirizzo IP del proxy server nel campo Indirizzo IP server.

Passo 2 Immettere il numero di porta usato dal proxy server per la ricezione delle richieste proxy nel campo Porta.

Passo 3 Immettere un elenco di indirizzi IP per i quali *non* si desidera che i client utilizzino il server proxy.

Separare gli indirizzi con virgole e non immettere nessuno spazio.

Passo 4 Se si desidera impedire che i client utilizzino il server proxy per gli indirizzi locali (LAN), selezionare la casella di controllo **Bypass del server proxy per gli indirizzi locali**.

Passo 5 Fare clic su **OK** per salvare le impostazioni proxy del browser.

Autenticazione utente (XAuth)

Questo consente di configurare attributi aggiuntivi per l'identificazione degli utenti, come Blocco gruppo, e salva Attributi password.

Banner XAuth

Immettere il testo di un banner da mostrare agli utenti durante le richieste XAuth.

Nota Questa funzione appare soltanto se supportata dalla versione IOS del proprio server Cisco.

Numero massimo di accessi consentiti per utente:

Specificare il numero massimo di connessioni simultanee che un utente può stabilire. Cisco SDM supporta un massimo di dieci accessi per utente.

Blocco gruppo

È possibile stabilire che un client possa connettersi al Server Easy VPN soltanto da un determinato gruppo utenti di provenienza.

Salva password

È possibile salvare localmente il nome utente e la password di autenticazione estesa nel client Easy VPN.

Tabella riassuntiva funzioni

Funzione	Procedura
Limitazione della connessione utente dal gruppo utente specifico.	Selezionare l'opzione **Attiva blocco gruppo**.
Salvataggio del nome utente e della password.	Selezionare l'opzione **Attiva salvataggio password**.
Specifica del numero massimo di connessioni simultanee che un utente può stabilire verso il Server Easy VPN.	Immettere il numero nel campo **Numero massimo di accessi consentiti**.

Aggiornamento Client

Da questa finestra si possono impostare notifiche di aggiornamento del software o firmware del client, e visualizzare le voci aggiornamento client esistenti. È possibile selezionare le voci di aggiornamento del client per la modifica o l'eliminazione.

Le notifiche vengono inviate automaticamente ai client che si collegano al server dopo che è stata salvata una configurazione di aggiornamento nuova o modificata. I client già connessi dovranno essere informati manualmente. Per inviare una notifica IKE manuale sulla disponibilità di un aggiornamento, scegliere un criterio di gruppo nella finestra Criteri di gruppo e fare clic sul pulsante **Invia aggiornamento**. La notifica sarà inviata ai client di gruppo che soddisfano i criteri di aggiornamento client.

Nota La finestra aggiornamento client è disponibile soltanto se supportata dalla versione IOS del proprio server Cisco.

Colonna Tipo di client

Il tipo di client cui la revisione è destinata.

Colonna Revisioni

Mostra quali revisioni sono disponibili.

Colonna URL

Fornisce la posizione delle revisioni.

Pulsante Aggiungi

Fare clic per configurare una nuova voce di aggiornamento client.

Pulsante Modifica

Fare clic per modificare la voce di aggiornamento client specificata.

Pulsante Elimina

Fare clic per eliminare la voce di aggiornamento client specificata.

Aggiungi o Modifica voce aggiornamento client

In questa finestra è possibile configurare una nuova voce di aggiornamento client.

Tipo di client

Immettere un tipo di client o sceglierne uno dal menu a tendina. Nei nomi del tipo di client si fa differenza tra maiuscole e minuscole.

Per i client software, il tipo di client è solitamente il sistema operativo, ad esempio *Windows*. Per i client hardware, il tipo di client è solitamente un numero di modello, ad esempio *vpn3002*.

Se si sta modificando una voce di aggiornamento client il campo tipo di cliente è di sola lettura.

URL

Immettere l'URL dell'ultima revisione del software o del firmware. L'URL deve cominciare con un protocollo appropriato, e può includere nomi utente e password.

Gli esempi seguenti sono URL per il download di un file di aggiornamento chiamato vpnclient-4-6.exe:

- http://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- https://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe

- ftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- tftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- scp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- rcp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- cns:
- xmodem:
- ymodem:
- null:
- flash:vpnclient-4.6.exe
- nvram:vpnclient-4.6.exe
- usbtoken[0-9]:vpnclient-4.6.exe

  L'intervallo dei numeri della porta USB token va da 0 a 9. Ad esempio, per un token USB applicato alla porta USB 0, l'URL è usbtoken0:vpnclient-4.6.exe.
- usbflash[0-9]:vpnclient-4.6.exe

  L'intervallo dei numeri della porta USB flash va da 0 a 9. Ad esempio, per un flash USB applicato alla porta USB 0, l'URL è usbflash0:vpnclient-4.6.exe.
- disk[0-1]:vpnclient-4.6.exe

  Il numero del disco è 0 o 1. Ad esempio, per un disco numero 0, l'URL è disk0:vpnclient-4.6.exe.
- archive:vpnclient-4.6.exe
- tar:vpnclient-4.6.exe
- system:vpnclient-4.6.exe

In questi esempi, *username* è il nome utente e *password* è la password del sito.

Revisioni

Immettere il numero di revisione dell'ultimo aggiornamento. È possibile immettere più numeri di revisione separati da virgole, ad esempio *4.3,4.4,4.5*. Non immettere spazi.

Riepilogo

In questa finestra è visualizzata la configurazione di Easy VPN Server che è stata creata e ne è consentito il salvataggio. È possibile rivedere la configurazione in questa finestra e fare clic sul pulsante **Indietro** per modificare qualsiasi voce.

Facendo clic sul pulsante **Fine** viene avviata la scrittura delle informazioni nella configurazione corrente del router. Se il tunnel è stato configurato per il funzionamento in modalità Auto, il router cerca di contattare il concentratore o server VPN.

Se si desidera modificare la configurazione Easy VPN Server in un secondo momento, è possibile apportare le modifiche nel riquadro Aggiungi o Modifica Server Easy VPN.

Per salvare questa configurazione nella configurazione correntemente utilizzata del router e chiudere la procedura guidata, fare clic su **Fine**. Le modifiche avranno effetto immediato.

Verificare la connettività VPN dopo la configurazione

Fare clic per verificare la connessione VPN appena configurata. Il risultato della verifica è visibile in una finestra separata.

Impostazioni Proxy del Browser

In questa finestra sono elencate le impostazioni del browser proxy, e la loro configurazione. È possibile aggiungere, modificare o eliminare le impostazioni del browser proxy. Usare i criteri di configurazione di gruppo per associare le impostazioni proxy con i gruppi client.

Nome

Il nome delle impostazioni proxy del browser

Impostazioni

Visualizza una delle seguenti voci:

- Senza Proxy Server

  I client non possono utilizzare proxy server quando si connettono mediante il tunnel VPN.

- Rileva automaticamente le impostazioni

  I client cercano di rilevare automaticamente un server proxy.

- Configurazione Proxy manuale

  Le impostazioni vengono configurate manualmente.

Dati server

Visualizza l'indirizzo IP del proxy server e il numero di porta usato.

Bypass degli indirizzi locali

Se attivato impedisce l'uso degli indirizzi locali (LAN) ai client.

Lista eccezioni

Un elenco di indirizzi IP per i quali *non* si desidera che i client utilizzino il server proxy.

Pulsante Aggiungi

Configurare le nuove impostazioni del browser proxy.

Pulsante Modifica

Modificare le impostazioni del browser proxy specificato.

Pulsante Elimina

Eliminare le impostazioni del browser proxy specificato. Le impostazioni proxy del browser associate con uno o più criteri di gruppo *non* possono essere eliminate finché tali associazioni non siano state rimosse.

Aggiungi o Modifica Server Easy VPN

In questa finestra è possibile visualizzare e gestire le connessioni del server Easy VPN.

Aggiungi

Fare clic su **Aggiungi** per aggiungere un Easy VPN Server nuovo.

Modifica

Fare clic su **Modifica** per modificare una configurazione Easy VPN Server esistente.

Elimina

Fare clic su **Elimina** per eliminare la configurazione specificata.

Colonna Nome

Il nome del criterio IPSec associato alla connessione.

Colonna Interfaccia

Il nome dell'interfaccia utilizzata per la connessione.

Colonna Autorizzazione gruppo

Il nome dell'elenco metodi utilizzato per la ricerca dei criteri di gruppo.

Colonna Autenticazione utente

Il nome dell'elenco metodi utilizzato per la ricerca dell'autenticazione utente.

Configurazione modalità

Visualizza una delle seguenti voci:

- Inizia

  La procedura è configurata in modo da iniziare le connessioni con i client Cisco Easy VPN Remote.

- Rispondi

  Il router è configurato in modo da attendere le richiesta dai client Cisco Easy VPN Remote prima di stabilire le connessioni.

Pulsante Verifica server VPN Server

Fare clic per verificare il tunnel VPN selezionato. Il risultato della verifica è visibile in una finestra separata.

Pulsante Limita accesso

Fare clic su questo pulsante per restringere l'accesso al gruppo per la connessione al Server Easy VPN specificato.

Questo pulsante è attivo soltanto se se si verificano le due seguenti condizioni:

- Sono presenti più d'una connessione di Server Easy VPN che usano il database locale per l'autenticazione degli utenti.
- È presente almeno una policy configurata di gruppo locale.

Aggiungi o Modifica connessione Easy VPN Server

In questa finestra è possibile aggiungere o modificare una connessione del Server Easy VPN.

Scegliere un'interfaccia

Se si aggiunge una connessione, selezionare l'interfaccia da utilizzare da questo elenco. Se si modifica la connessione, l'elenco viene disattivato.

Scegli criterio IPSec

Se si aggiunge una connessione, selezionare il criterio IPSec da utilizzare da questo elenco. Se si modifica la connessione, l'elenco viene disattivato.

Elenco metodi per ricerca criteri di gruppo

Selezionare l'elenco metodi da utilizzare per la ricerca dei criteri di gruppo dall'elenco. Gli elenchi metodi sono configurati selezionando **Attività aggiuntive** nella barra delle applicazioni di Cisco SDM e facendo clic sul nodo AAA.

Attiva autenticazione utente

Selezionare questa casella di controllo se si desidera che gli utenti vengano autenticati.

Elenco metodi per autenticazione utente

Selezionare l'elenco dei metodi da utilizzare per l'autenticazione utente dall'elenco. Gli elenchi metodi sono configurati selezionando Attività aggiuntive nella barra delle applicazioni di Cisco SDM e facendo clic sul nodo AAA.

Configurazione modalità

Selezionare **Inizia** se si desidera avviare le connessioni del router con i client Easy VPN Remote.

Selezionare **Rispondi** se si desidera che il router attenda le richieste dai client Easy VPN Remote prima di stabilire le connessioni.

Limita accesso

In questa finestra è possibile specificare quali criteri di gruppo possono utilizzare la connessione Easy VPN.

Per consentire a un gruppo l'accesso alla connessione del Server Easy VPN selezionare questa casella. Per negare a un gruppo l'accesso alla connessione del Server Easy VPN deselezionare questa casella.

Tabella riassuntiva funzioni

Funzione	Procedura
Limitare un criterio di gruppo ad una specifica connessione del server Easy VPN, negando a tutti gli altri criteri di gruppo di utilizzare tale connessione.	Selezionare la connessione al server Easy VPN specifica e fare clic sul pulsante **Limita accesso**. Selezionare la casella di controllo del gruppo di destinazione e deselezionare le caselle di controllo di tutti gli altri gruppi. Negare l'accesso al gruppo di destinazione in tutte le altre connessioni del server Easy, deselezionando nella finestra Limita accesso le relative caselle di controllo di tutte le connessioni.

Configurazione dei criteri di gruppo

In questa finestra è possibile vedere, aggiungere, duplicare e scegliere i criteri di gruppo per la modifica o l'eliminazione. I criteri di gruppo sono utilizzati per identificare le risorse per i client Easy VPN Remote.

Pulsante Pool comune

Consente di designare un pool esistente come pool comune per tutti i criteri di gruppo da utilizzare. Se non è stato configurato alcun pool locale, il pulsante è disattivato. I pool possono essere configurati facendo clic su **Attività aggiuntive > Pool Locali** oppure durante la configurazione delle connessioni del server Easy VPN.

Pulsanti Aggiungi, Modifica, Duplica ed Elimina

Utilizzare questi pulsanti per gestire i criteri di gruppo nel router. Selezionando **Duplica** vengono visualizzate le schede di modifica Criteri di gruppo.

Pulsante Invia aggiornamento

Fare clic per inviare una notifica IKE di aggiornamenti software o firmware ai client attivi del gruppo scelto. Se questo pulsante è disattivato il gruppo scelto non ha un aggiornamento client configurato.

Per configurare le notifiche di aggiornamento client per il gruppo prescelto, fare clic sul pulsante **Modifica** e successivamente sulla scheda **Aggiornamento Client**.

Colonna Nome gruppo

Il nome dei criteri di gruppo.

Colonna Pool

Il pool di indirizzi IP utilizzato dai client nel gruppo.

Colonna DNS

I server DNS utilizzati dai client in questo gruppo.

Colonna WINS

I server WINS utilizzati dai client in questo gruppo.

Colonna Nome di dominio

Il nome di dominio utilizzato dai client nel gruppo.

Colonna ACL

Se per il gruppo è specificata la suddivisione del tunnel, in questa colonna può essere contenuto il nome di una ACL che definisce quale traffico deve essere crittografato.

Finestra Dettagli

La finestra dettagli è un elenco di impostazioni di funzioni e di altri valori delle policy di gruppo prescelto. Le impostazioni delle funzioni sono visualizzate soltanto se supportate dalla versione IOS del proprio router Cisco, e si applicano soltanto al gruppo prescelto. Le seguenti impostazioni di funzionalità possono essere visualizzate nell'elenco:

- Autenticazione

  Il valore di una preshared key, se è configurata, oppure un certificato digitale se non è stata configurata una chiave preshared.

- Numero massimo di connessioni consentite

  Mostra il numero massimo di connessioni simultanee consentite. Cisco SDM supporta un massimo di 5000 connessioni simultanee per gruppo.

- Limitazione d’accesso

  Indica l'interfaccia esterna cui il gruppo specificato è limitato.

- Server di backup

  Mostra l'indirizzo IP dei server di backup che sono stati configurati.

- Firewall di tipo Are-U-There

  Limita le connessioni ai dispositivi sui quali sono in esecuzione Black Ice o Zone Alarm.

- Includi LAN locale

  Consente ad una connessione che *non* utilizza la suddivisione del tunnel di accedere alla rete locale secondaria contemporaneamente al client.

- PFS (Perfect Forward Secrecy)

  il PFS è necessario per IPSec.

- Push configurazione, URL e Versione

  Il server invia al client un file di configurazione dall'URL specificato e con il numero di versione specificato.

- Blocco gruppo

  I client sono limitati al gruppo.

- Salva password

  Le credenziali Xauth possono essere salvate sul client.

- Numero massimo di connessioni

  Il numero massimo di connessioni simultanee che un utente può stabilire. Cisco SDM supporta un massimo di dieci accessi simultanei per utente.

- Banner XAuth

  Il messaggio di testo mostrato agli utenti durante le richieste XAuth.

IP Pools (Pool di IP)

In questa finestra sono elencati i pool di indirizzi IP disponibili per i criteri di gruppo e configurati sul router. A seconda dell'area di Cisco SDM in cui si lavora, possono essere disponibili i pulsanti **Aggiungi**, **Modifica** e **Elimina** e può variare il nome della finestra di Cisco SDM. Utilizzare tali comandi per gestire i pool di IP locali sul router.

Colonna Nome pool

Il nome del pool di indirizzi IP.

Colonna Intervallo indirizzi IP

L'intervallo degli indirizzi IP per il pool selezionato. Un intervallo da 2.2.2.0 a 2.2.2.254 consente 255 indirizzi.

Colonna Dimensione della cache

La dimensione della cache per il pool.

Colonna Nome gruppo

Se un pool locale è configurato con l'opzione del gruppo mediante CLI, il nome del gruppo viene visualizzato nella colonna corrispondente. Questa colonna non viene visualizzata in tutte le aree di Cisco SDM.

Nota Non è possibile configurare pool locali con l'opzione del gruppo utilizzando Cisco SDM.

Aggiungi o Modifica pool locale IP

In questa finestra si può creare o modificare un pool locale di indirizzi IP.

Nome pool

Se si crea un pool, immettere il nome pool. Se si modifica un pool, questo campo è disattivato.

Intervallo indirizzi IP

Immettere o modificare gli intervalli di indirizzi IP per il pool nell'area. Un pool può contenere più intervalli di indirizzi IP. Utilizzare i pulsanti Aggiungi, Modifica ed Elimina per creare intervalli aggiuntivi, modificare gli intervalli e per eliminare gli intervalli degli indirizzi IP.

Dimensione della cache

In questo campo immettere o modificare le dimensioni della cache per il pool.

Aggiungi intervallo indirizzi IP

In questa finestra si può aggiungere una gamma di indirizzi IP ad un pool esistente.

Indirizzo IP iniziale

Immettere l'indirizzo IP più piccolo dell'intervallo.

Indirizzo IP finale

Immettere l'indirizzo IP più alto dell'intervallo.

CAPITOLO 12

Enhanced Easy VPN

Nelle sezioni che seguono vengono descritte le schermate di configurazione di Cisco Router and Security Device Manager per Enhanced Easy VPN.

Interfaccia e Autenticazione

Specificare l'interfaccia del router rispetto alla quale l'interfaccia del modello virtuale deve essere senza numero e specificare il metodo da utilizzare per l'autenticazione in questa finestra.

Interfaccia

Un'interfaccia del modello virtuale deve essere senza numero rispetto a un'interfaccia di router per ottenere un indirizzo IP.

Cisco consiglia di rimuovere il numero dell'interfaccia di modello virtuale rispetto a un indirizzo di loopback per ottenere una maggiore flessibilità. Per farlo, scegliere **Senza numero per nuova interfaccia loopback** ed immettere indirizzo IP e subnet mask per l'interfaccia loopback. Un esempio di indirizzo IP e subnet mask di loopback è 127.0.0.1, 255.255.255.0.

Per rimuovere il numero dell'interfaccia del modello virtuale rispetto a un'altra interfaccia, scegliere **Senza numero per** e scegliere l'interfaccia. È necessario scegliere l'interfaccia di terminazione del tunnel sul router. Fare clic su **Dettagli** per visualizzare l'indirizzo IP, l'autenticazione, il criterio e le altre informazioni sull'interfaccia scelta.

Autenticazione

Selezionare il metodo che i client Easy VPN devono scegliere per autenticarsi sul server Easy VPN Server configurato sul router. Le chiavi precondivise devono essere comunicate agli amministratori dei client Easy VPN. I certificati digitali non lo richiedono, ma ogni client deve richiedere la registrazione e ricevere un certificato digitale.

Server RADIUS

Nella finestra Server RADIUS è possibile identificare i server RADIUS che il router utilizzerà per la ricerca autorizzazione e criteri di gruppo e i gruppi VPN configurati sui server RADIUS.

Origine client RADIUS

La configurazione dell'origine RADIUS consente di specificare l'indirizzo IP dell'origine da inviare in pacchetti collegati per il server RADIUS.
Per visualizzare l'indirizzo IP e per altre informazioni su un'interfaccia, scegliere l'interfaccia e fare clic sul pulsante **Dettagli**.

L'indirizzo IP di origine nei pacchetti RADIUS inviati dal router deve essere configurato come l'indirizzo IP NAD di Cisco ACS (Access Control Server) versione 3.3 o successiva.

Se si seleziona l'opzione **Router sceglie l'origine**, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo dell'interfaccia attraverso la quale i pacchetti RADIUS escono dal router.

Se si sceglie un'interfaccia del router specifica, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo di quell'interfaccia.

Nota Il software Cisco IOS consente la configurazione di una sola interfaccia origine RADIUS sul router. Se il router ha già un'origine RADIUS configurata e si sceglie un'origine diversa, l'indirizzo IP collocato nei pacchetti inviati al server RADIUS diventa l'indirizzo IP della nuova origine e pertanto può non corrispondere all'indirizzo IP NAD configurato sul Cisco ACS.

Colonne Indirizzo IP del server, Parametri e Seleziona

Queste colonne riportano le informazioni principali sui server RADIUS utilizzati dal router. Nella colonna Indirizzo IP del server vengono elencati gli indirizzi IP di ogni server configurato. Nella colonna Parametri sono elencate le porte di autorizzazione e accounting relative a ciascun server. Nella colonna Seleziona è presente una casella di controllo per ogni server configurato. Selezionare la casella accanto a ogni server che si desidera utilizzare. Nella tabella che segue vengono mostrati dei dati di esempio.

Indirizzo IP del server	Parametri	Seleziona
192.168.108.14	Porta di autorizzazione 1645; Porta di accounting 1646	Selezionata
192.168.108.15	Porta di autorizzazione 3005; Porta di accounting 3006	

In questa configurazione, il server RADIUS con indirizzo IP 192.168.108.14 utilizza le porte di autorizzazione ed accounting standard, rispettivamente 1645 e 1646. Il router utilizzerà questo server per l'autenticazione e l'autorizzazione. Il server con indirizzo IP 192.168.108.15 utilizzerà porte non standard di autenticazione e autorizzazione. Il router non contatterà questo server perché la casella Seleziona non è selezionata.

Fare clic su **Aggiungi** per creare una voce per un server RADIUS. Selezionare la voce del server e fare clic su **Modifica** per modificare le informazioni che il router possiede per tale server. Scegliere la voce del server e fare clic su **Esegui ping** per testare la connessione tra il router e il server RADIUS.

Gruppi VPN in server RADIUS

Immettere i gruppi VPN configurati sul server RADIUS che si desidera rendere accessibile con questa connessione. Usare la virgola per separare le voci. Di seguito viene riportato un esempio di gruppo di voci.

```
WGP-1, WGP-2, ACCTG, CSVC
```

I nomi devono corrispondere ai nomi di gruppi configurati nel server RADIUS. Per facilitare l'amministrazione, devono corrispondere anche ai nomi di gruppi configurati per i client Easy VPN.

Criteri Autorizzazione gruppo e Utente gruppo

È possibile creare gruppi di utenti ognuno con il proprio pool di indirizzi IP, la propria configurazione di aggiornamento client, la propria configurazione di suddivisione tunnel e le altre impostazioni personalizzate. Questi attributi di gruppo vengono scaricati al client di tale gruppo quando si connettono al server Easy VPN. Lo stesso gruppo di nome deve essere configurato sui client che sono membri del gruppo, per garantire che vengano scaricati gli attributi di gruppo corretti.

Se sono già stati configurati dei criteri di gruppo, essi vengono visualizzati nell'elenco di questa finestra ed è possibile selezionarli per questa connessione selezionando la casella Seleziona a sinistra del nome del gruppo.

Nell'elenco vengono mostrati il nome del gruppo, il nome del pool di indirizzi IP, i nomi dei server DNS e WINS e il nome di dominio di ogni gruppo configurato. Quando si fa clic su **Aggiungi** per configurare le impostazioni per un nuovo gruppo o su **Modifica** per modificare le impostazioni, le modifiche vengono visualizzate in questo elenco. Per utilizzare le impostazioni di un gruppo esistente come base per la configurazione di un nuovo gruppo, selezionare il gruppo esistente e fare clic su **Duplica**. I pulsanti Aggiungi, Modifica e Duplica consentono di visualizzare finestre di dialogo utili per configurare le impostazioni del gruppo.

Configura timer d'inattività

Selezionare **Configura timer d'inattività** per specificare la durata della connessione per i client inattivi nei campi Timer inattività. Immettere i valori di tempo nel formato HH:MM:SS. Ad esempio, per immettere 3 ore, 20 minuti e 32 secondi, immettere i seguenti valori nei campi:

```
03:20:32
```

Il valore di timeout si applicherà a tutti i gruppi configurati per questa connessione.

Aggiungi o Modifica Easy VPN Server: scheda Generale

Immettere in questa finestra di dialogo le informazioni generali della connessione Easy VPN Server.

Nome di questa connessione

Immettere un nome che identifichi la connessione; tale nome viene visualizzato nella finestra Modifica Easy VPN Server.

Indirizzo IP dell'interfaccia tunnel virtuale

Fare clic su Interfaccia e Autenticazione per una descrizione dei campi Indirizzo IP dell'interfaccia tunnel virtuale.

Modalità tunnel

Scegliere **IPSec-IPV4** nel campo Modalità tunnel. L'opzione IPSec-IPV4 consente di creare un tunnel IP IPSec versione 4.

Descrizione

È possibile immettere una descrizione che sarà utile per gli amministratori di rete nella modifica delle configurazioni o nella risoluzione dei problemi della rete.

Aggiungi o Modifica Easy VPN Server: scheda IKE

La scheda IKE della finestra di dialogo Aggiungi Easy VPN Server consente di creare un Profilo IKE per questa connessione.

Tipo di identità corrispondenza

Il profilo IKE include i criteri di corrispondenza che consentono al router di identificare le connessioni in entrata e in uscita a cui si devono applicare i parametri di connessione IKE. I criteri di corrispondenza possono al momento essere applicati ai gruppi VPN. Il gruppo viene scelto automaticamente nel campo Tipo di identità corrispondenza.

Fare clic su **Aggiungi** per generare un elenco dei gruppi da includere nei criteri di corrispondenza.

Scegliere **Aggiungi nome gruppo esterno** per aggiungere il nome di un gruppo che non è configurato nel router e immettere il nome nella finestra di dialogo.

Scegliere **Seleziona da gruppi locali** per aggiungere il nome di un gruppo che è configurato nel router. Nella finestra di dialogo visualizzata, selezionare la casella accanto al gruppo da aggiungere. Se in altri profili IKE vengono utilizzati tutti i gruppi locali, SDM informa che tutti i gruppi sono stati selezionati.

Configurazione modalità

Scegliere **Rispondi** nel campo Configurazione modalità se il server Easy VPN deve rispondere alle richieste di configurazione della modalità.

Scegliere **Inizia** se il server Easy VPN deve iniziare le richieste di configurazione della modalità.

Scegliere **Entrambi** se il server Easy VPN deve sia iniziare le richieste di configurazione della modalità sia rispondere ad esse.

Criterio autorizzazione ricerca criterio gruppo

È necessario specificare un criterio di autorizzazione che controlli l'accesso ai dati dei criteri di gruppo sul server AAA. Scegliere **predefinito** se si desidera concedere l'accesso alle informazioni di ricerca dei criteri di gruppo. Per specificare un criterio, sceglierne uno esistente nell'elenco oppure fare clic su **Aggiungi** per creare un criterio nella finestra di dialogo visualizzata.

Criterio autenticazione utente

È possibile specificare un criterio di autenticazione degli utenti da utilizzare per gli accessi XAuth. Scegliere **predefinito** per consentire gli accessi XAuth.
Per specificare un criterio di controllo degli accessi XAuth, scegliere un criterio esistente nell'elenco oppure fare clic su **Aggiungi**, creando così un criterio nella finestra di dialogo visualizzata.

DPD (Dead Peer Discovery)

Fare clic su **DPD (Dead Peer Discovery)** per consentire al router di inviare messaggi DPD ai client Easy VPN Remote. Se un client non risponde ai messaggi DPD, la connessione viene interrotta.

Specificare il numero di secondi tra messaggi DPD nel campo Intervallo Keepalive. L'intervallo valido è compreso tra 10 e 3600 secondi.

Specificare il numero di secondi tra tentativi in seguito ad esito negativo dei messaggi DPD nel campo Tentativi. L'intervallo valido è compreso tra 2 e 60 secondi.

Il metodo DPD aiuta a gestire le connessioni senza intervento dell'amministratore ma genera pacchetti aggiuntivi che i due peer devono elaborare per mantenere la connessione.

Aggiungi o Modifica Easy VPN Server: scheda IPSec

Immettere in questa finestra di dialogo le informazioni necessarie per creare un profilo IPSec. Il profilo IPSec specifica i set di trasformazione da utilizzare, la modalità di determinazione di lifetime della Security Association (SA) e altre informazioni.

Colonna Set di trasformazione

Utilizzare le due colonne nella parte superiore della finestra di dialogo per specificare i set di trasformazione da includere nel profilo. La colonna di sinistra contiene i set di trasformazione configurati nel router. Per aggiungere al profilo un set di trasformazione configurato, selezionarlo e fare clic sul pulsante **>>**. Se la colonna di sinistra non contiene set di trasformazione o se occorre un set di trasformazione che non è stato creato, fare clic su **Aggiungi** e crearlo nella finestra di dialogo visualizzata.

Durata SA (Security Association) IPSec basata sul tempo

Se si desidera stabilire una nuova SA dopo un determinato periodo di tempo, fare clic su **Durata SA (Security Association) IPSec basata sul tempo**. Immettere il periodo di tempo nei campi HH:MM:SS a destra. L'intervallo valido è compreso tra 0:2:0 (2 minuti) e 24:0:0 (24 ore).

Durata SA (Security Association) IPSec basata sul volume di traffico

Se si desidera stabilire una nuova SA dopo il passaggio di una quantità definita di traffico attraverso il tunnel IPSec, fare clic su **Durata SA (Security Association) IPSec basata sul volume di traffico**. Immettere il numero di kilobyte che devono passare attraverso il tunnel prima che una SA venga abbandonata a favore di una nuova SA. L'intervallo valido è compreso tra 2560 KB a e 536870912 KB.

Tempo di inattività SA (Security Association) IPSec

Se si desidera stabilire una nuova SA dopo che il peer è stato inattivo per un periodo definito di tempo, fare clic su Tempo di inattività SA (Security Association) IPSec. Immettere il periodo di tempo di inattività nei campi HH:MM:SS a destra. L'intervallo valido è compreso tra 0:1:0 (1 minuto) e 24:0:0 (24 ore).

PFS (Perfect Forward Secrecy)

Se IPSec dovrà richiedere la PFS (Perfect Forward Secrecy) quando richiede nuove SA per questa interfaccia di modello virtuale o se dovrà richiedere la PFS nelle richieste ricevute dal peer, fare clic su **PFS (Perfect Forward Secrecy)**. È possibile specificare i valori riportati di seguito.

- gruppo 1: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 768 bit.
- gruppo 2: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 1024 bit.
- gruppo 5: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 1536 bit.

Crea interfaccia tunnel virtuale

Immettere in questa finestra di dialogo le informazioni per un'interfaccia tunnel virtuale.

Tipo di interfaccia

Scegliere **predefinita** o **tunnel** come tipo di interfaccia. Nel caso di modifica di interfaccia tunnel virtuale, viene visualizzato il valore configurato e il campo è di sola lettura.

Configurare l'indirizzo IP dell'interfaccia

L'indirizzo IP dell'interfaccia tunnel virtuale può essere senza numero rispetto a un'altra interfaccia oppure può non avere l'indirizzo IP. Scegliere **IP senza numero**, quindi scegliere il nome di un'interfaccia nel campo Senza numero per, oppure scegliere **Nessun indirizzo IP**.

Modalità tunnel

Cisco SDM supporta la modalità tunnel IPSec-IPv4 e questa è selezionata.

Seleziona zona

Questo campo viene visualizzato quando il router esegue un'immagine Cisco IOS che supporta il firewall con criteri basati su zone (ZPF, Zone-Policy Based Firewall) e vi è una zona che è stata configurata nel router. Se si desidera che questa interfaccia tunnel virtuale sia membro della zona, fare clic sul pulsante a destra del campo. Fare clic su Click **Seleziona zona** e selezionare la zona a cui si desidera che l'interfaccia appartenga oppure fare clic su **Crea zona** per creare una nuova zona per questa interfaccia.

Nota Non è necessario che l'interfaccia tunnel virtuale sia membro della zona. Tuttavia, il router non inoltra il traffico tra interfacce della zona e non.

CAPITOLO 13

DMVPN

In questa sezione vengono fornite le informazioni sulle schermate di configurazione della funzione DMVPN (Dynamic Multipoint Virtual Private Network).

Dynamic Multipoint VPN

Seguire la procedura guidata per configurare il router come hub Dynamic Multipoint VPN (DMVPN) oppure come spoke DMVPN. Una connessione VPN tipica è un tunnel IPSec point-to-point che connette due router. DMVPN consente di creare una rete con un hub centrale che si connette ad altri router remoti denominati spoke utilizzando un tunnel GRE su IPSec. Il traffico IPSec viene instradato attraverso l'hub agli spoke della rete. Cisco SDM consente di configurare il router come hub DMVPN primario o secondario oppure come spoke in una rete DMVPN.

Il seguente collegamento contiene ulteriori informazioni su DMVPN (è necessario l'ID di accesso CCO):

VPN IPSec multipoint

Cisco SDM supporta la configurazione di una DMVPN hub and spoke che utilizza profili IPSec per definire la crittografia. È possibile configurare una DMVPN fully-meshed e utilizzare mappe crittografiche per definire la crittografia nella DMVPN tramite CLI. Le DMVPN fully-meshed e le DMVPN che utilizzano mappe crittografiche vengono gestite e modificate tramite CLI. Cisco SDM supporta la configurazione di una DMVPN a partire dalla versione IOS 12.2(13)T.

Cisco SDM supporta la configurazione di una DMVPN singola su un router.

In questa schermata, identificare il router utilizzato come hub oppure come spoke nella rete DMVPN.

Dal momento che per configurare gli spoke occorrono informazioni sull'hub, è necessario configurare dapprima quest'ultimo. Se si sta configurando un hub, è possibile utilizzare la funzione Configurazione spoke disponibile nella finestra di riepilogo per generare una procedura da inviare agli amministratori degli spoke in modo da configurarli con le informazioni relative all'hub corrette. Prima di iniziare a configurare uno spoke, è necessario ottenere le informazioni corrette relative all'hub.

Crea uno spoke (client) in una DMVPN

Selezionare se il router utilizzato è uno spoke della rete DMVPN. Gli spoke sono endpoint logici della rete. Prima di iniziare la configurazione, è necessario eseguire il ping dell'hub per accertarsi di disporre della connettività a questo e di tutte le informazioni necessarie. Tali informazioni sono elencate nella Procedura guidata spoke DMVPN (Dynamic Multipoint VPN).

Crea un hub (server o testa di rete) in una DMVP

Selezionare se il router utilizzato è un hub della rete DMVPN. L'hub è il punto centrale logico di una rete DMVPN ed è collegato a ogni spoke tramite una connessione IPSec point-to-point. L'hub può instradare il traffico IPSec tra gli spoke della rete.

Procedura guidata hub DMVPN (Dynamic Multipoint VPN)

Questa procedura guidata consente di configurare il router come hub DMVPN. È opportuno configurare l'hub prima degli spoke, in modo da essere in grado di fornire agli amministratori degli spoke le informazioni necessarie a configurarli.

Nella finestra dell'applicazione viene illustrata la configurazione in corso. Una volta terminata la configurazione, sarà necessario fornire agli amministratori degli spoke le seguenti informazioni relative all'hub:

- L'indirizzo IP dell'interfaccia fisica dell'hub.
- L'indirizzo IP dell'interfaccia tunnel mGRE dell'hub.
- Il protocollo di routing dinamico da utilizzare per inviare gli aggiornamenti routing alla DMVPN e il numero di sistema autonomo (per EIGRP) oppure l'ID processo (per OSPF) da utilizzare.

La funzione di configurazione degli spoke di Cisco SDM consente di creare un file di testo contenente le informazioni di configurazione dell'hub necessarie agli amministratori degli spoke. Tale funzione è disponibile nella finestra Riepilogo di questa procedura guidata.

È inoltre necessario comunicare agli amministratori degli spoke la subnet mask da utilizzare nonché assegnare a ogni spoke un indirizzo IP nella stessa subnet dell'hub, in modo da evitare conflitti di indirizzo.

Tipo di hub

Le reti DMVPN possono essere configurate con un singolo hub oppure con un hub primario e uno di backup. Identificare il tipo di hub che si sta configurando.

Hub primario

Selezionare se si tratta di un hub primario nella rete DMVPN.

Hub di backup

Selezionare questo pulsante se il router è un hub di backup in una rete DMVPN fully-meshed

Configurare la chiave precondivisa

I peer DMVPN possono utilizzare una chiave precondivisa oppure certificati digitali per autenticare le connessioni reciproche. Se si utilizzano chiavi precondivise, ciascun hub e spoke della rete dovrà utilizzare la stessa chiave precondivisa.

Le chiavi precondivise devono essere scambiate con l'amministratore del sito remoto tramite un metodo protetto e prestabilito, ad esempio un messaggio di posta elettronica crittografato. Nella chiave precondivisa non devono essere utilizzati punti interrogativi (?) e spazi. La chiave precondivisa può contenere 128 caratteri al massimo.

Chiave precondivisa

Immettere la chiave precondivisa utilizzata nella rete DMVPN. Nella chiave precondivisa non devono essere utilizzati punti interrogativi (?) né spazi. La chiave precondivisa può contenere 128 caratteri al massimo.

Certificati digitali

Fare clic su questo pulsante se il router utilizza certificati digitali per l'autenticazione. I certificati digitali vengono configurati in Componenti VPN>Infrastruttura a chiave pubblica.

Confermare la chiave precondivisa

Inserire nuovamente la chiave per la conferma. Se i valori di questo campo e del campo Chiave precondivisa non corrispondono, Cisco SDM richiederà di inserirli nuovamente.

Configurazione dell'interfaccia tunnel GRE dell'hub

Il protocollo mGRE (Multipoint Generic Routing Encapsulation) viene utilizzato in una rete DMVPN per consentire a una singola interfaccia GRE di un hub di supportare un tunnel IPSec per ogni spoke. In tal modo la configurazione DMVPN risulta semplificata. GRE consente l'invio di aggiornamenti routing su connessioni IPSec.

Selezionare l'interfaccia che fornisce la connessione a Internet

Selezionare l'interfaccia del router che fornisce la connessione a Internet. Tale interfaccia è l'origine del tunnel GRE.

Se si seleziona un'interfaccia che utilizza una connessione di tipo dialup, è possibile che la connessione resti sempre attiva. Per stabilire se si tratta di una connessione di tipo dialup, è possibile esaminare le interfacce supportate in Interfacce e connessioni. In genere, per una connessione di tipo dialup saranno configurate interfacce quali ISDN oppure seriale asincrona.

Indirizzo IP

Immettere l'Indirizzo IP dell'interfaccia mGRE. Dovrà trattarsi di un indirizzo privato appartenente alla stessa subnet delle interfacce GRE degli altri router della rete. Ad esempio, le interfacce GRE potrebbero condividere la subnet 10.10.6.0 e disporre di indirizzi IP nell'intervallo compreso tra 10.10.6.1 e 10.10.6.254.

Subnet Mask

Immettere la maschera della subnet in cui si trovano le interfacce GRE. Ad esempio, la maschera per la subnet 10.10.6.0 potrebbe essere 255.255.255.0. Per ulteriori informazioni, vedere Indirizzi IP e subnet mask.

Pulsante Avanzate

Cisco SDM fornisce valori predefiniti per le impostazioni avanzate del tunnel. Tuttavia, l'amministratore dell'hub dovrà definire le impostazioni del tunnel e fornirle al personale di amministrazione degli spoke in modo da consentirne l'utilizzo.

Configurazione avanzata per l'interfaccia tunnel

Utilizzare questa finestra per configurare i parametri del tunnel GRE. Sebbene Cisco SDM fornisca valori predefiniti, è necessario ottenere i valori corretti dall'amministratore dell'hub e inserirli in questa finestra.

I valori predefiniti sono forniti in questo argomento della Guida. Se vengono modificati ed occorre ripristinarli, consultare questo argomento.

Stringa di autenticazione NHRP

Immettere la stringa che gli hub e gli spoke DMVPN dovranno utilizzare per autenticarsi per le transazioni NHRP. La lunghezza massima della stringa può essere di 8 caratteri. I caratteri speciali, ad esempio gli spazi e i punti interrogativi (?), non sono consentiti. Tutti i dispositivi della DMVPN devono essere configurati con la stessa stringa di autenticazione.

Impostazioni predefinite Cisco SDM: DMVPN_NW

ID rete NHRP

Immettere l'ID rete NHRP. L'ID di rete è un identificativo di rete univoco globale, a 32 bit per una rete NBMA (Nonbroadcast, Multiaccess), di intervallo compreso tra 1 e 4294967295.

Impostazioni predefinite Cisco SDM: 100000

Intervallo di sospensione NHRP

Immettere il numero di secondi per il quale gli ID di rete NHRP devono essere notificati come validi.

Impostazioni predefinite Cisco SDM: 360

Chiave tunnel

Immettere la chiave da utilizzare per questo tunnel. Tale chiave dovrà essere la stessa per tutti i tunnel mGRE della rete.

Impostazioni predefinite Cisco SDM: 100000

Larghezza di banda

Immettere la larghezza di banda desiderata, in kilobyte al secondo (kbit/s). I valori di larghezza di banda predefiniti sono impostati durante l'avvio; per visualizzare tali valori, utilizzare il comando EXEC di visualizzazione delle interfacce. L'impostazione della larghezza di banda solita nelle configurazioni DMVPN è 1000.

Impostazioni predefinite Cisco SDM: 1000

MTU

Immettere la quantità massima di dati, in byte, consentita per un pacchetto che attraversa il tunnel.

Impostazioni predefinite Cisco SDM: 1400

Ritardo trasmissione tunnel

Impostare un valore di ritardo per un'interfaccia, in decimi di microsecondi.

Impostazioni predefinite Cisco SDM: 1000

Hub primario

Se il router che si sta configurando è l'hub di backup della rete DMVPN, sarà necessario identificare l'hub primario fornendone gli indirizzi IP pubblico e privato.

Indirizzo IP pubblico

Immettere l'indirizzo IP dell'interfaccia nell'hub primario utilizzato per questo tunnel. Questo dovrà essere un indirizzo IP statico. Ottenere queste informazioni dall'amministratore dell'hub.

Indirizzo IP dell'interfaccia tunnel mGRE dell'hub

Immettere l'indirizzo IP dell'interfaccia tunnel mGRE nell'hub primario. Ottenere queste informazioni dall'amministratore dell'hub.

Seleziona protocollo di routing

Utilizzare questa finestra per specificare il modo in cui le altre reti sottostanti il router sono notificate agli altri router della rete. Selezionare una delle seguenti opzioni:

- EIGRP: Extended Interior Gateway Routing Protocol.
- OSPF: Open Shortest Path First.
- RIP: Routing Internet Protocol.
- Routing statico. Questa opzione è attivata quando si sta configurando un tunnel GRE su IPSec.

Nota Il protocollo RIP non è supportato per la topologia DMVPN hub and spoke; tuttavia è disponibile per la topologia DMVPN fully-meshed.

Informazioni sul routing

Utilizzare questa finestra per aggiungere o modificare le informazioni sul routing relative alle reti sottostanti il router che si desidera notificare agli altri router della rete. I campi di questa finestra variano in base al protocollo di routing specificato.

Per maggiori informazioni sui parametri RIP, vedere Aggiungi o Modifica route RIP.

Per maggiori informazioni sui parametri EIGRP, vedere Add or Edit EIGRP Route.

Per maggiori informazioni sui parametri OSPF, vedere Add or Edit an OSPF Route.

Selezionare la versione RIP da attivare

Specificare RIP versione 1 o 2.

Selezionare un ID processo OSPF/un numero AS EIGRP esistente

È possibile selezionare un ID processo per OSPF o un numero AS EIGRP esistente se ne è stato configurato uno in precedenza. Vedere Suggerimenti per la configurazione dei protocolli di routing per la rete DMVPN.

Crea un nuovo ID processo OSPF/numero AS EIGRP

Se non esiste alcun ID processo o se si desidera utilizzarne uno diverso, in questo campo è possibile configurarlo.

ID area OSPF per la rete tunnel

Immettere un nuovo ID area OSPF per la rete. Si tratta dell'ID area della rete tunnel. Cisco SDM aggiunge automaticamente la rete tunnel a questo processo mediante tale ID area.

Reti private notificate mediante *<nome protocollo>*

In quest'area vengono mostrate le reti notificate mediante il protocollo di routing selezionato. Se è stato già configurato il protocollo di routing specificato in questa procedura guidata, le reti specificate per la notifica saranno visualizzate in questo elenco.

Aggiungere tutte le reti private che si desidera notificare ai peer DMVPN tramite questo processo di routing. La procedura guidata DMVPN aggiunge automaticamente la rete tunnel a questo processo.

Rete: un indirizzo di rete. È possibile immettere l'indirizzo di una rete specifica e utilizzare la maschera carattere jolly per rendere la notifica generale.

Maschera carattere jolly: (protocolli EIGRP e OSPF) una maschera bit che specifica la parte di indirizzo di rete che deve corrispondere all'indirizzo fornito nella colonna della rete. Tale maschera può essere utilizzata per fare in modo che il router notifichi le reti appartenenti a un particolare intervallo, in base a un dato indirizzo. Un bit pari a 0 specifica che il bit dell'indirizzo di rete deve corrispondere al rispettivo bit dell'indirizzo di rete dato.

Ad esempio, se l'indirizzo di rete fosse 172.55.10.3 e la maschera carattere jolly fosse 0.0.255.255, il router notificherebbe tutte le reti che cominciano con i numeri 172.55, non soltanto la rete 172.55.10.3.

Area: numero dell'area OSPF di quella rete che viene mostrato quando è selezionata l'opzione OSPF. Ogni router di una particolare area OSPF mantiene un database topologico per quell'area.

Aggiungi: fare clic per aggiungere una rete oppure un gruppo di reti da notificare.

Modifica: fare clic per modificare i dati relativi a una rete o a un gruppo di reti notificate. Questo pulsante è attivato per le voci create durante l'istanza corrente di questa procedura guidata.

Elimina: fare clic per eliminare i dati relativi alla rete o al gruppo di reti selezionate. Questo pulsante è attivato per le voci create durante l'istanza corrente di questa procedura guidata.

Procedura guidata spoke DMVPN (Dynamic Multipoint VPN)

Questa procedura guidata consente di configurare il router come spoke in una rete DMVPN. Prima di iniziare la configurazione, è necessario eseguire il ping dell'hub per accertarsi che il router sia in grado di inviargli il traffico e disporre di tutte le informazioni relative all'hub. Un amministratore di hub che utilizza Cisco SDM per configurare l'hub è in grado di generare un file di testo contenente le informazioni di configurazione dell'hub necessarie agli amministratori degli spoke.

Prima di iniziare, è necessario ottenere le seguenti informazioni:

- L'indirizzo IP dell'interfaccia fisica dell'hub.
- L'indirizzo IP dell'interfaccia tunnel mGRE dell'hub.
- L'indirizzo IP e la subnet mask da utilizzare per lo spoke e comunicati dall'amministratore dell'hub. L'amministratore dell'hub dovrà assegnare indirizzi a ogni spoke, in modo da garantire che tutti i router della DMVPN si trovino nella stessa subnet e che ciascuno utilizzi un indirizzo univoco.
- Il protocollo di routing da utilizzare e il numero di sistema autonomo (per EIGRP) oppure l'ID processo (per OSPF) da utilizzare per inviare gli aggiornamenti routing alla DMVPN.

Topologia di rete DMVPN

Selezionare il tipo di rete DMVPN alla quale appartiene il router.

Rete Hub and Spoke

Selezionare questa opzione se si sta configurando il router in una rete nella quale ogni spoke dispone di una connessione GRE su IPSec point-to-point all'hub DMVPN e invierà il traffico destinato ad altri spoke attraverso l'hub. Se si seleziona questa opzione, nell'immagine vengono visualizzati i collegamenti dagli spoke all'hub.

Rete fully-meshed

Selezionare questa opzione se si sta configurando il router come spoke in grado di stabilire un tunnel IPSec diretto ad altri spoke della rete. Per supportare questa funzionalità viene configurato un tunnel GRE sullo spoke. Se si seleziona questa opzione, nell'immagine vengono visualizzati i collegamenti dagli spoke all'hub e tra i diversi spoke.

Nella schermata della procedura guidata sono elencate le immagini IOS necessarie per supportare una rete DMVPN fully-meshed.

Specificare le informazioni sull'hub

Utilizzare questa finestra per fornire le informazioni necessarie relative all'hub della DMVPN.

Indirizzo IP dell'interfaccia fisica dell'hub

Immettere l'indirizzo IP dell'interfaccia dell'hub. Ottenere questo indirizzo dall'amministratore dell'hub. Questo indirizzo sarà utilizzato come destinazione tunnel.

Indirizzo IP dell'interfaccia tunnel mGRE dell'hub

Immettere l'indirizzo IP dell'interfaccia tunnel mGRE dell'hub. Gli indirizzi del tunnel mGRE per l'hub e gli spoke devono trovarsi nella stessa subnet.

Configurazione dell'interfaccia tunnel GRE dello spoke

Per questo spoke sarà creata una connessione point-to-point tramite le informazioni immesse in questa finestra.

Selezionare l'interfaccia che fornisce la connessione a Internet

Selezionare l'interfaccia del router che fornisce la connessione a Internet. Tale interfaccia è l'origine del tunnel GRE su IPSec.

Se si seleziona un'interfaccia che utilizza una connessione di tipo dialup, è possibile che la connessione resti sempre attiva. Per stabilire se per l'interfaccia fisica selezionata è stata configurata una connessione di tipo dialup, ad esempio una connessione ISDN oppure asincrona, è possibile esaminare le interfacce supportate in Interfacce e connessioni.

Ripetere la registrazione con l'hub quando viene modificato l'indirizzo IP di *nome interfaccia*: questa opzione è disponibile se l'interfaccia selezionata riceve un indirizzo IP dinamico tramite DHCP o IPCP. Se si specifica questa opzione sarà possibile ripetere la registrazione dello spoke con l'hub non appena viene ricevuto un nuovo indirizzo IP.

Indirizzo IP

Immettere l'indirizzo IP per l'interfaccia GRE a questo hub. Dovrà trattarsi di un indirizzo privato appartenente alla stessa subnet delle interfacce GRE degli altri router della rete. Ad esempio, le interfacce GRE potrebbero condividere la subnet 10.10.6.0 e disporre di indirizzi IP nell'intervallo compreso tra 10.10.6.1 e 10.10.6.254.

Se si sta configurando uno spoke, sarà necessario utilizzare l'indirizzo IP assegnato al router dall'amministratore dell'hub. In caso contrario, si potrebbero verificare conflitti di indirizzi.

Subnet Mask

Immettere la subnet mask della subnet in cui si trovano le interfacce GRE. Tale valore deve essere assegnato dall'amministratore dell'hub e deve essere lo stesso per tutti i router della DMVPN. Ad esempio, la mask per la subnet 10.10.6.0 potrebbe essere 255.255.255.0. Per ulteriori informazioni, vedere Indirizzi IP e subnet mask.

Pulsante Avanzate

Fare clic su questo pulsante per fornire i parametri NHRP e di tunnel per questa connessione.

Cisco SDM fornisce valori predefiniti per le impostazioni avanzate del tunnel. Tuttavia, l'amministratore dell'hub dovrà definire le impostazioni del tunnel e fornirle al personale di amministrazione degli spoke in modo da consentirne l'utilizzo. Se si sta configurando uno spoke, ottenere le impostazioni del tunnel dall'amministratore dell'hub, fare clic su questo pulsante e immetterle nella finestra di dialogo visualizzata.

Avviso Cisco SDM - Dipendenza DMVPN

Questa finestra viene visualizzata quando l'interfaccia scelta per l'origine del tunnel DMVPN presenta una configurazione che ne impedisce l'utilizzo da parte di DMVPN. Cisco SDM informa l'utente del conflitto e fornisce l'opzione per consentire a Cisco SDM la modifica della configurazione in modo da rimuovere il conflitto.

Firewall

Se è stato applicato un firewall all'interfaccia indicata come origine del tunnel, Cisco SDM potrà aggiungere voci delle regole di accesso alla configurazione e consentire, in tal modo, il traffico GRE, IPSec e ISAKMP attraverso il firewall.

Visualizza dettagli

Fare clic su questo pulsante per visualizzare le voci di controllo dell'accesso che Cisco SDM aggiungerà alla regola di accesso se si seleziona **Consenti il traffico GRE, IPSec e ISAKMP attraverso il firewall**.

Tali voci consentono il traffico ISAKMP, GRE, i protocolli ESP (Encapsulating Security Protocol) e AHP (Authentication Header Protocol).

Modifica DMVPN (Dynamic Multipoint VPN)

In questa finestra sono visualizzate le configurazioni tunnel DMVPN esistenti. DMVPN consente di creare una rete con un hub centrale che si connette ad altri router remoti denominati spoke. Cisco SDM supporta la topologia di rete hub-and-spoke in cui il traffico GRE su IPSec viene instradato attraverso l'hub. Cisco SDM consente di configurare il router come hub DMVPN primario o secondario oppure come spoke in una rete DMVPN.

Il seguente collegamento contiene ulteriori informazioni su DMVPN (è necessario l'ID di accesso CCO): VPN IPSec multipoint

Cisco SDM supporta la configurazione di una DMVPN hub and spoke che utilizza profili IPSec per definire la crittografia. È possibile configurare una DMVPN fully-meshed e utilizzare mappe crittografiche per definire la crittografia nella DMVPN tramite CLI. Le DMVPN fully-meshed e le DMVPN che utilizzano mappe crittografiche vengono gestite e modificate tramite CLI.

Cisco SDM supporta la configurazione di una DMVPN singola su un router.

È necessario configurare dapprima l'hub, per definire gli indirizzi IP dell'hub e i parametri di routing con i quali dovranno essere configurati gli *spoke*. Per altri suggerimenti su come configurare i router in una DMVPN, vedere Suggerimenti sulla configurazione di DMVPN.

Interfaccia

L'interfaccia fisica di origine del tunnel.

Profilo IPSec

Il profilo IPSec utilizzato dal tunnel. Il profilo IPSec definisce i set di trasformazione utilizzati per crittografare il traffico del tunnel. Cisco SDM supporta l'utilizzo di profili esclusivamente IPSec per definire la crittografia in una DMVPN. Se si desidera utilizzare mappe crittografiche, configurare la DMVPN tramite l'interfaccia della riga di comando.

Indirizzo IP

L'indirizzo IP del tunnel GRE. Il tunnel GRE viene utilizzato per inviare gli aggiornamenti routing alla DMVPN.

Descrizione

Una breve descrizione di questo tunnel.

Pannello Dettagli

Nel pannello Dettagli vengono visualizzati i valori di tutta la configurazione del tunnel DMVPN.

Perché alcune interfacce tunnel vengono visualizzate in sola lettura?

Un'interfaccia tunnel viene visualizzata in sola lettura se è stata già configurata con associazioni di mappa crittografica e parametri NHRP. Da questa finestra sarà possibile modificare i parametri NHRP e le informazioni di routing; tuttavia sarà necessario modificare l'indirizzo IP, l'origine del tunnel e la destinazione del tunnel dalla finestra Interfacce e connessioni.

Aggiungi

Fare clic per aggiungere una nuova configurazione del tunnel DMVPN.

Modifica

Fare clic per modificare la configurazione del tunnel DMVPN selezionata.

Elimina

Fare clic per eliminare una configurazione del tunnel DMVPN.

Pannello Generale

In questo pannello, aggiungere o modificare i parametri di configurazione generali del tunnel DMVPN.

Indirizzo IP

Immettere l'indirizzo IP del tunnel. Dovrà trattarsi di un indirizzo privato appartenente alla stessa subnet degli altri indirizzi tunnel della DMVPN. Se si sta configurando uno spoke, sarà necessario utilizzare l'indirizzo assegnato al router dall'amministratore dell'hub, in modo che non si verifichino conflitti.

Maschera

Immettere la subnet mask assegnata dall'amministratore dell'hub alla DMVPN. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Origine tunnel

Selezionare l'interfaccia che dovrà essere utilizzata dal tunnel oppure immetterne l'indirizzo IP. Prima di selezionare un'interfaccia configurata per una connessione di tipo dialup, vedere Utilizzo di interfacce con configurazioni di tipo dialup.

Destinazione tunnel

Fare clic su **Si tratta di un tunnel GRE multipoint** in caso di tunnel DMVPN in una rete fully-meshed. Fare clic su **Nome host/IP** e specificare l'indirizzo IP o nome host se si tratta di una rete hub and spoke.

Profilo IPSec

Selezionare un profilo IPSec configurato per questo tunnel. Il profilo IPSec definisce i set di trasformazione utilizzati per crittografare il traffico del tunnel.

MTU

Immettere la quantità massima di dati, in byte, consentita per un pacchetto che attraversa il tunnel.

Larghezza di banda

Immettere la larghezza di banda desiderata, in kilobyte al secondo (kbit/s). I valori di larghezza di banda predefiniti sono impostati durante l'avvio; per visualizzare tali valori, utilizzare il comando EXEC di visualizzazione delle interfacce. Il valore della larghezza di banda tipica nelle configurazioni DMVPN è 1000.

Ritardo

Impostare un valore di ritardo per un'interfaccia, in decimi di microsecondi. Il valore del ritardo tipo nelle configurazioni DMVPN è 1000.

Chiave tunnel

Immettere la chiave da utilizzare per questo tunnel. Tale chiave dovrà essere la stessa per tutti i tunnel mGRE della rete.

Si tratta di un tunnel GRE multipoint

Selezionare questa opzione se si desidera un'interfaccia tunnel mGRE, vale a dire un'interfaccia in grado di mantenere connessioni con più peer. Se questo router viene configurato come hub DMVPN, è necessario selezionare questa casella di controllo per consentire all'hub di stabilire connessioni con gli spoke. Se il router viene configurato come spoke, selezionare questa casella di controllo se si sta configurando una DMVPN fully-meshed. In tal modo, uno spoke è in grado di stabilire una connessione all'hub per inviare traffico e ricevere informazioni sull'hop successivo per la connessione diretta a tutti gli altri spoke della DMVPN.

Pannello NHRP

Utilizzare questo pannello per fornire i parametri di configurazione NHRP.

Stringa di autenticazione

Immettere la stringa che gli hub e gli spoke DMVPN dovranno utilizzare per autenticarsi per le transazioni NHRP. La lunghezza massima della stringa può essere di 8 caratteri. Tutti le workstation NHRP della DMVPN devono essere configurate con la stessa stringa di autenticazione.

Intervallo di sospensione

Immettere il numero di secondi per il quale gli ID di rete NHRP devono essere notificati come validi.

ID rete

Immettere l'ID rete NHRP. L'ID di rete è un identificativo di rete univoco globale, a 32 bit per una rete NBMA (Nonbroadcast, Multiaccess), L'intervallo è compreso tra 1 e 4294967295. L'ID di rete deve essere univoco per ogni workstation NHRP.

Server hop successivo

In quest'area vengono elencati gli indirizzi IP dei server hop successivi che questo router può contattare. Quest'area dovrà contenere l'indirizzo IP dell'hub primario e secondario se si tratta di uno spoke. Se, al contrario, si tratta di un hub, quest'area dovrà contenere l'indirizzo IP degli altri hub della DMVPN.

Fare clic su **Aggiungi** per immettere l'indirizzo IP di un server hop successivo. Selezionare un server e fare clic su **Elimina** per eliminarlo dall'elenco.

Mappa NHRP

In quest'area sono elencati le mappature di indirizzi da IP a NBMA. Fare clic su **Aggiungi** per creare una nuova mappa. Una volta creata la mappa, questa sarà aggiunta all'elenco. Fare clic su **Modifica** per modificare una mappa selezionata. Fare clic su **Elimina** per rimuovere una configurazione mappa selezionata.

Configurazione mappa NHRP

Utilizzare questa finestra per creare o modificare una mappatura tra gli indirizzi IP e quelli NBMA.

Configura statisticamente mapping degli indirizzi IP-NMBA delle destinazioni IP connesse a una rete NBMA

Fare clic su questo pulsante se si sta configurando uno spoke in una rete fully-meshed. Dal momento che Cisco SDM considera gli hub di backup come spoke per gli hub primari, fare clic su questo pulsante anche se si sta configurando un hub di backup. In questa parte della finestra vengono fornite le informazioni di indirizzo necessarie agli spoke o agli hub di backup per contattare l'hub primario.

Destinazione raggiungibile tramite rete NBMA: immettere l'indirizzo IP del tunnel mGRE configurato sull'hub primario. Gli spoke e gli hub di backup utilizzano queste informazioni relative ai tunnel per stabilire un contatto con l'hub e creare un tunnel mGRE verso di esso. Gli spoke utilizzano il tunnel per inviare i dati crittografati all'hub e per richiedere a questo informazioni sugli hop successivi verso gli altri spoke.

Indirizzo BMA direttamene raggiungibile: immettere l'indirizzo IP statico dell'interfaccia dell'hub primario che supporta il tunnel mGRE.

Configura gli indirizzi NBMA utilizzati come destinazioni per la trasmissione o pacchetti multicast da inviare attraverso una rete tunnel

Utilizzare quest'area della finestra per fornire le informazioni utilizzate dai protocolli di routing.

Aggiungi dinamicamente gli indirizzi IP degli spoke alla cache multicast dell'hub: configurare questa opzione se si sta configurando un hub primario o un hub di backup. Questa opzione è necessaria all'hub per inviare gli aggiornamenti routing a tutti gli spoke DMVPN connessi.

Indirizzo IP dell'indirizzo NBMA direttamente raggiungibile: se si sta configurando uno spoke in una DMVPN fully-meshed oppure un hub di backup, selezionare questa casella e fornire l'indirizzo IP statico dell'interfaccia dell'hub primario che supporta il tunnel mGRE.

Pannello Routing

Utilizzare questo pannello per configurare le informazioni di routing per il cloud DMVPN.

Protocollo di routing

Selezionare il protocollo di routing dinamico utilizzato dagli hub e dagli spoke di questa DMVPN. Si noti che tutti i router della DMVPN devono essere configurati per il protocollo di routing selezionato.

- RIP: Routing Internet Protocol
- OSPF: Open Shortest Path First
- EIGRP: Extended Interior Gateway Routing Protocol

Campi RIP

Se è stato selezionato RIP come protocollo di routing dinamico, scegliere **Versione 1**, **Versione 2**, o **Predefinito**. Se si seleziona **Versione 2**, il router includerà la subnet mask nell'aggiornamento routing. Se, invece, si seleziona **Predefinito**, il router invierà gli aggiornamenti della versione 2, ma sarà in grado di ricevere gli aggiornamenti di entrambe le versioni del protocollo RIP.

Disattiva split horizon: se il router configurato è un hub, selezionare questa casella di controllo per disattivare lo split horizon dell'interfaccia tunnel mGRE. In tal modo il router potrà annunciare le route conosciute tramite l'interfaccia tunnel della stessa interfaccia.

Campi OSPF

Se si seleziona il protocollo OSPF, riempire i campi elencati di seguito.

ID processo OSPF: immettere l'ID processo. Questo valore identifica il processo OSPF agli altri router. Vedere Suggerimenti per la configurazione dei protocolli di routing per la rete DMVPN.

Tipo di rete OSPF: selezionare point-to-multipoint o broadcast. Se si sceglie point-to-multipoint OSPF aggiunge delle route alla tabella di routing degli spoke. Per impedirlo, è possibile selezionare broadcast.

Priorità OSPF: la priorità OSPF consente di identificare il router come hub oppure spoke. Se si tratta di un hub, immettere un valore di priorità 2. Se, invece, si tratta di uno spoke, immettere un valore 0.

Campi EIGRP

Se è stato selezionato il protocollo EIGRP, riempire i campi elencati di seguito.

Numero di sistema autonomo: immettere il numero di sistema autonomo del gruppo di router che utilizza EIGRP. I router con lo stesso numero di sistema autonomo EIGRP mantengono un database topologico dei router dell'area identificati da quel numero. Vedere Suggerimenti per la configurazione dei protocolli di routing per la rete DMVPN.

Disattiva split horizon: se il router configurato è un hub, selezionare questa casella di controllo per attivare lo split horizon dell'interfaccia tunnel mGRE. Lasciare la casella vuota per disattivare split horizon. In tal modo il router potrà annunciare le route conosciute tramite l'interfaccia tunnel della stessa interfaccia.

Utilizza hop successivo originale: se si tratta di un router hub DMVPN, EIGRP annuncerà questo router come hop successivo. Selezionare questa casella di controllo per fare in modo che EIGRP utilizzi l'hop successivo dell'IP originale per annunciare le route agli spoke DMVPN.

Come configurare manualmente una DMVPN?

È possibile configurare il router come hub oppure spoke DMVPN tramite le finestre di Componenti VPN e la finestra Modifica DMVPN (Dynamic Multipoint VPN). A questo scopo, è necessario completare le seguenti attività:

- Configurare un profilo IPSec. Non è possibile configurare una connessione DMVPN se non è stato configurato almeno un profilo IPSec.
- Configurare la connessione DMVPN.
- Specificare le reti da notificare al cloud DMVPN.

Le procedure per queste attività sono fornite di seguito.

Per configurare un profilo IPSec

È necessario configurare un criterio IPSec e quindi un tunnel DMVPN.

Passo 1 Fare clic su **VPN** nel pannello a sinistra, quindi fare clic su **Componenti VPN.**

Passo 2 Fare clic sul ramo Profili IPSec, quindi fare clic su **Aggiungi** nella finestra Profili IPSec.

Passo 3 Denominare il profilo, quindi selezionare il set di trasformazione che dovrà contenere nella finestra Aggiungi profilo IPSec. Se si desidera, è possibile immettere una breve descrizione.

Passo 4 Fare clic su **OK**.

Per configurare una connessione DMVPN

Passo 1 Nella struttura VPN, fare clic sul ramo **Dynamic Multipoint VPN**.

Passo 2 Fare clic su **Modifica DMVPN** (**Dynamic Multipoint VPN**).

Passo 3 Fare clic su **Aggiungi**.

Passo 4 Nella finestra Configurazione tunnel DMVPN, completare le schede Generale, NHRP e Routing per creare un tunnel DMVPN. Per ulteriori informazioni su un campo particolare, consultare la Guida in linea.

Per specificare le reti da notificare alla DMVPN

Se esistono reti sottostanti il router utilizzato e si desidera notificarle alla DMVPN, è possibile eseguire questa operazione aggiungendo i numeri di rete nelle finestre Routing.

Passo 1 Dal pannello a sinistra, fare clic su **Routing**.

Passo 2 Nella finestra Routing, selezionare il protocollo di routing specificato nella configurazione DMVPN e fare clic su **Modifica**.

Passo 3 Aggiungere i numeri di rete che si desidera notificare.

CAPITOLO 14

Impostazioni globali VPN

Di seguito vengono descritte le finestre Impostazioni globali VPN.

Impostazioni globali VPN

In questa finestra sono visualizzate le impostazioni globali VPN del router.

Pulsante Modifica

Fare clic sul pulsante **Modifica** per aggiungere o modificare le impostazioni globali VPN.

Attiva IKE

Il valore è True se IKE è attivato e False se IKE è disattivato.

Nota Se IKE è disattivato, la configurazione VPN non funzionerà.

Attiva modalità Aggressive

Il valore è True se è attiva la modalità Aggressive, è False se tale modalità è disattivata. La funzione della modalità Aggressive consente di specificare gli attributi del tunnel RADIUS per un peer IPSec e di inizializzare la negoziazione della modalità Aggressive IKE con gli attributi del tunnel.

Timeout Xauth

Il numero di secondi che il router deve attendere prima che un sistema risponda a un'autenticazione XAuth.

IKE Identity

Il nome host del router o l'indirizzo IP che il router utilizza per identificarsi nelle negoziazioni IKE.

Rilevamento peer inattivo

Il DPD (Dead Peer Detection, rilevamento peer inattivo) consente al router di rilevare un peer inattivo e, se trovato, di eliminare le Security Association IPSec e IKE a tale peer.

IKE Keepalive (Sec)

Il valore è il numero di secondi che il router deve attendere tra un invio e l'altro di pacchetti IKE keepalive.

IKE Retry (Sec)

Il valore è il numero di secondi che il router deve attendere tra vari tentativi per stabilire una connessione con un peer remoto. Per impostazione predefinita, il valore visualizzato è “2” secondi.

Tipo di rilevamento peer inattivo

Selezionare **Su richiesta** oppure **Periodico**.

Se impostato su **Su richiesta**, i messaggi relativi al rilevamento del peer inattivo vengono inviati in base ai modelli di traffico. Ad esempio, se da un router deve essere inviato il traffico in uscita ed è incerto lo stato del peer, al router viene inviato un messaggio DPD per richiedere lo stato di tale peer. Se dal router non deve essere inviato alcun traffico, il messaggio DPD non verrà mai inoltrato.

Se impostato su **Periodico**, i messaggi DPD vengono inviati dal router in base all'intervallo specificato dal valore IKE Keepalive.

Lifetime della Security Association (SA) IPSec (sec)

La durata della Security Association prima che scada e venga rigenerata. Il valore predefinito è 3600 secondi (1 ora).

Lifetime della Security Association (SA) IPSec (kilobyte)

Il numero di kilobyte che il router può inviare su una connessione VPN prima che la Security Association IPSec scada. La Security Association sarà rinnovata allo scadere del periodo più breve.

Impostazioni globali VPN: IKE

La finestra consente di specificare le impostazioni globali per IKE e IPSEC.

Attiva IKE

Lasciare questa casella selezionata se si desidera utilizzare la rete VPN.

Precauzione Se IKE è disattivato, la configurazione VPN non funzionerà.

Attiva modalità Aggressive

La modalità Aggressive consente di specificare gli attributi del tunnel RADIUS per un peer IPSec e iniziare una negoziazione Aggressive IKE con gli attributi del tunnel.

Identità (del router)

Questo campo specifica il modo in cui si identificherà il router. Selezionare **Indirizzo IP** o **nome host**.

Timeout Xauth

Il numero di secondi che il router deve attendere prima di ricevere una risposta da un sistema che richiede un'autenticazione XAuth.

Attiva rilevamento peer inattivo

Il DPD (Dead Peer Detection, rilevamento peer inattivo) consente al router di rilevare un peer inattivo e, se trovato, di eliminare le Security Association IPSec e IKE a tale peer.

La casella di controllo Attiva rilevamento peer inattivo è disattivata se l'immagine Cisco IOS utilizzata dal router non supporta tale funzionalità.

Keepalive

Specificare il numero di secondi durante il quale il router deve mantenere una connessione anche se inutilizzata.

Retry

Specificare il numero di secondi che il router deve attendere tra i vari tentativi per stabilire una connessione con un peer remoto. Il valore predefinito è '2' secondi.

Tipo di rilevamento peer inattivo

Selezionare **Su richiesta** o **Periodico**.

Se impostato su **Su richiesta**, i messaggi relativi al rilevamento del peer inattivo vengono inviati in base ai modelli di traffico. Ad esempio, se da un router deve essere inviato il traffico in uscita ed è incerto lo stato del peer, al router viene inviato un messaggio DPD per richiedere lo stato di tale peer. Se dal router non deve essere inviato alcun traffico, il messaggio DPD non verrà mai inoltrato.

Se impostato su **Periodico**, i messaggi DPD vengono inviati dal router in base all'intervallo specificato dal valore IKE Keepalive.

Impostazioni globali VPN: IPSec

Modificare le impostazioni globali IPSec in questa finestra.

Autenticare e generare nuova chiave dopo ogni

Selezionare questa casella e specificare l'intervallo di tempo durante il quale il router deve autenticare e generare una nuova chiave. Se non viene specificato un valore, il router autentica e genera una nuova chiave ogni ora.

Generare nuova chiave quando la chiave corrente è stata utilizzata per generare la crittografia di un volume di

Selezionare questa casella e specificare il numero di kilobyte che devono essere crittografati dalla chiave corrente prima che il router autentichi e generi una nuova chiave. Se non si specifica un valore, il router autenticherà e genererà una nuova chiave non appena la chiave corrente supera la crittografia di 4.608.000 kilobyte.

Impostazioni della crittografia della chiave VPN

La finestra Impostazioni della crittografia della chiave VPN viene visualizzata se l'immagine Cisco IOS sul router supporta la crittografia di tipo 6, conosciuta anche come *crittografia della chiave VPN*. È possibile utilizzare questa finestra per specificare una chiave principale da usare per la crittografia delle chiavi VPN, quali le chiavi precondivise, le chiavi Easy VPN e le chiavi XAuth. Se crittografate, queste chiavi non saranno più leggibili da un utente che visualizza il file di configurazione del router.

Attiva crittografia delle chiavi VPN

Selezionare l'opzione per attivare la crittografia di queste chiavi.

Chiave principale corrente

Questo campo contiene un asterisco (*) quando la chiave principale è stata configurata.

Nuova chiave principale

Immettere una nuova chiave IKE in questo campo. Il numero di caratteri del nome deve essere compreso tra 8 e 128.

Conferma chiave principale

Per confermare, immettere nuovamente la chiave principale in questo campo. Se i valori di questo campo e del campo Nuova chiave principale non corrispondono, Cisco SDM richiede di immettere nuovamente la chiave.

CAPITOLO 15

Protezione IP

IPSec (IP Security, protezione IP) è uno schema di standard aperti che fornisce riservatezza, integrità e autenticazione ai dati tra i peer partecipanti. Questi servizi di protezione sono forniti a livello IP; IPSec utilizza IKE per gestire la negoziazione di protocolli e algoritmi basati sul criterio locale, e per generare le chiavi di crittografia e autenticazione che devono essere utilizzate.

Cisco SDM consente di configurare set di trasformazione, regole e criteri IPSec.

Utilizzare la struttura IPSec per passare alle finestre di configurazione corrispondenti che si desidera utilizzare.

Criteri IPSec

In questa finestra sono visualizzati i criteri IPSec configurati nel router e le mappe crittografiche associate a ciascun criterio. Tali criteri sono utilizzati per definire le connessioni VPN. Per informazioni sulle relazioni tra i criteri IPSec, le mappe crittografiche e le connessioni VPN, vedere la sezione Ulteriori informazioni sulle connessioni VPN e i criteri IPSec.

Icona

Se questa icona viene visualizzata accanto al criterio IPSec, il criterio è di sola lettura e non può essere modificato. Un criterio IPSec può essere di sola lettura se contiene comandi che Cisco SDM non supporta.

Nome

Il nome del criterio IPSec.

Tipo

La scelta può essere effettuata tra una delle opzioni riportate di seguito.

- ISAKMP:IKE è utilizzato per stabilire le associazioni di protezione IPSec per proteggere il traffico specificato dalla voce della mappa crittografica. Le mappe crittografiche supportate da Cisco SDM sono ISAKMP (Internet Security Association and Key Management Protocol).
- Manuale: IKE non verrà utilizzato per stabilire le Security Association IPSec per proteggere il traffico specificato dalla voce della mappa crittografica.

  La creazione di mappe crittografiche dinamiche non è supportata da Cisco SDM. Tutte le mappe crittografiche manuali che sono state create utilizzando l'interfaccia della riga di comando (CLI) sono considerate di sola lettura da Cisco SDM.
- Dinamica: indica che la voce della mappa crittografica è utilizzata per fare riferimento a una mappa crittografica dinamica preesistente. Le mappe crittografiche dinamiche sono modelli di criteri utilizzati nell'elaborazione delle richieste di negoziazione da un dispositivo peer IPSec.

  La creazione di mappe crittografiche dinamiche non è supportata da Cisco SDM. Cisco SDM considera di sola lettura tutte le mappe crittografiche dinamiche che sono state create tramite l'interfaccia CLI.

Mappe crittografiche nel criterio IPSec

Nome

Il nome del criterio IPSec del quale fa parte la mappa crittografica.

Numero di sequenza

Quando in una connessione VPN viene utilizzato un criterio IPSec, la combinazione del numero di sequenza e nome del criterio IPSec identifica in modo univoco la connessione.

Peer

In questa colonna sono elencati gli indirizzi IP o i nomi host dei dispositivi peer specificati nella mappa crittografica. Più peer vengono separati da virgole.

Set di trasformazione

In questa colonna sono elencati i set di trasformazione della mappa crittografica.

Set di mappe crittografiche dinamiche nel criterio IPSec

Nome set di mappe crittografiche dinamiche

Il nome del set di mappe crittografiche dinamiche che consente agli amministratori di comprendere l'utilizzo del set.

Numero sequenza

Il numero di sequenza per il set di mappe crittografiche dinamiche.

Tipo

Il tipo è sempre dinamico.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di un criterio IPSec alla configurazione del router.	Fare clic su **Aggiungi**.
Modifica di un criterio IPSec esistente.	Selezionare il criterio e fare clic su **Modifica**.
Rimozione di una voce di mappa crittografica da un criterio.	Selezionare il criterio e fare clic su **Modifica**. Nella finestra selezionare la mappa crittografica da rimuovere e fare clic su **Elimina**. Quindi, fare clic su **OK** per ritornare alla finestra.
Rimozione di un criterio IPSec.	Selezionare il criterio e fare clic su **Elimina**.

Aggiungi o Modifica criterio IPSec

Utilizzare questa finestra per aggiungere o modificare un criterio IPSec.

Nome

Il nome del criterio IPSec. Tale nome può essere un qualsiasi set di caratteri alfanumerici, e può essere utile per includere i nomi dei peer nel nome del criterio o per includere altre informazioni pertinenti.

Mappe crittografiche nel criterio IPSec

In questa casella sono elencate le mappe crittografiche nel criterio IPSec. Nell'elenco sono inclusi il nome, il numero di sequenza e il set di trasformazione che compongono la mappa crittografica. È possibile selezionare una mappa crittografica e modificarla o eliminarla dal criterio IPSec.

Se si desidera aggiungere una mappa crittografica, fare clic su Aggiungi. Se si desidera conoscere la procedura di Cisco SDM, selezionare **Utilizza aggiunta guidata** e fare clic su **Aggiungi**.

Icona

Se una mappa è di sola lettura, l'icona corrispondente viene visualizzata in questa colonna. Una mappa crittografica può essere di sola lettura se contiene comandi che Cisco SDM non supporta.

Set di mappe crittografiche dinamiche nel criterio IPSec

In questa casella sono elencate le mappe crittografiche dinamiche nel criterio IPSec. Utilizzare il pulsante **Aggiungi** per aggiungere un set di mappe crittografiche dinamiche al criterio. Utilizzare il pulsante **Elimina** per rimuovere tale set di mappe.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di una mappa crittografica al criterio.	Fare clic su **Aggiungi** e creare una mappa crittografica nei pannelli Aggiungi mappa crittografica. In alternativa, selezionare **Utilizza aggiunta guidata** e fare clic su **Aggiungi**. **Nota** La procedura guidata consente di aggiungere un unico set di trasformazione alla mappa crittografica. Se occorrono più set di trasformazione nella mappa crittografica, non utilizzare tale procedura.
Modifica di una mappa crittografica nel criterio.	Selezionare la mappa crittografica, fare clic su **Modifica** e modificare la mappa nei pannelli Modifica mappa crittografica.
Rimozione di una mappa crittografica dal criterio.	Selezionare la mappa crittografica e fare clic su **Elimina**.

Aggiungi o Modifica mappa crittografica - Generale

Modificare in questa finestra i parametri generali relativi alla mappa crittografica. La finestra contiene i campi riportati di seguito.

Nome criterio IPSec

Un campo di sola lettura che contiene il nome del criterio in cui la mappa crittografica è utilizzata. Questo campo non viene visualizzato se si utilizza la procedura guidata mappa crittografica.

Descrizione

Immettere o modificare la descrizione della mappa crittografica in questo campo. La descrizione viene visualizzata nell'elenco Connessioni VPN e serve a distinguere questa mappa dalle altre nello stesso criterio IPSec.

Numero di sequenza

Un numero che insieme al nome del criterio IPSec viene utilizzato per identificare una connessione. In Cisco SDM il numero di sequenza viene generato automaticamente. Se si preferisce, è possibile immettere un proprio numero di sequenza.

Lifetime della Security Association

Le Security Association (SA) IPSec utilizzano chiavi condivise. Queste chiavi e le rispettive Security Association scadono insieme. Esistono due tipi di lifetime: lifetime a tempo e lifetime in base al volume del traffico. La Security Association scade quando viene raggiunto il primo di questi limiti.

È possibile utilizzare questo campo per specificare un lifetime della Security Association per questa mappa crittografica diverso dal lifetime specificato a livello globale. Nel campo Kilobyte è possibile specificare il lifetime come numero di kilobyte inviati, fino a un massimo di 4.608.000. Nel campi HH:MM:SS è possibile specificare il lifetime come ore, minuti e secondi. È inoltre possibile specificare entrambi i tipi di lifetime, a tempo e in base al volume del traffico. Se vengono specificati entrambi i criteri, il lifetime scade quando viene soddisfatto il primo criterio.

Attiva PFS (Perfect Forwarding Secrecy)

Quando le chiavi di protezione derivano da chiavi generate in precedenza, esiste un problema di sicurezza poiché se una chiave è compromessa, possono esserlo anche le altre. PFS garantisce che ogni chiave abbia una derivazione indipendente, assicurando così che se una chiave è compromessa, non lo sarà nessun altra. Se si attiva PFS, è possibile specificare l'utilizzo del metodo del gruppo 1, gruppo 2 o gruppo 5 di Diffie-Hellman.

Nota Se il router non supporta il gruppo 5, non verrà visualizzato nell'elenco.

Attiva RRI (Reverse Route Injection)

RRI (Reverse Route Injection) è utilizzato per compilare la tabella di routing di un router interno in cui è in esecuzione il protocollo OSPF (Open Shortest Path First) o RIP (Routing Information Protocol) per le sessioni di client VPN remoti o da LAN a LAN.

RRI aggiunge in modo dinamico route statiche ai client connessi al server Easy VPN.

Aggiungi o Modifica mappa crittografica - Informazioni peer

Una mappa crittografica include i nomi host o gli indirizzi IP dei peer interessati dalla Security Association. In questa schermata è possibile aggiungere e rimuovere i peer associati a questa mappa crittografica. Più peer forniscono al router più route per i dati crittografati.

Funzione	Procedura
Aggiunta di un peer all'Elenco corrente.	Immettere l'indirizzo IP o il nome host del peer, quindi fare clic su **Aggiungi**
Rimozione di un peer dall'Elenco corrente.	Selezionare il peer e fare clic su **Rimuovi**.

Aggiungi o Modifica mappa crittografica - Set di trasformazione

Utilizzare questa finestra per aggiungere e modificare il set di trasformazione utilizzato nella mappa crittografica. Una mappa crittografica include i nomi host o gli indirizzi IP dei peer interessati dalla Security Association. Più peer forniscono al router più route per i dati crittografati. I dispositivi alle due estremità della connessione VPN devono tuttavia utilizzare lo stesso set di trasformazione.

Utilizzare la procedura guidata mappa crittografica se è sufficiente che il router fornisca una mappa crittografica con un set di trasformazione.

Se si desidera configurare manualmente una mappa crittografica con più set di trasformazione (fino a un massimo di sei) per garantire che il router possa offrirne uno accettabile per il peer che sta negoziando, utilizzare **Aggiungi nuova mappa crittografica...** deselezionando l'opzione **Utilizza aggiunta guidata**. Se ci si trova già all'interno della procedura guidata mappa crittografica, uscire dalla procedura guidata, deselezionare **Utilizza aggiunta guidata**, quindi fare clic su **Aggiungi nuova mappa crittografica...**.

Se si configura manualmente una mappa crittografica con più set di trasformazione, è anche possibile ordinare i set. Questo sarà l'ordine utilizzato dal router per la negoziazione del set di trasformazione da utilizzare.

Set di trasformazione disponibili

Set di trasformazione configurati disponibili all'utilizzo nella mappa crittografica. Nella procedura guidata mappa crittografica, i set di trasformazione disponibili sono visualizzati nell'elenco a discesa **Seleziona set di trasformazione**.

Se non è stato configurato alcun set di trasformazione nel router, vengono visualizzati solo i set di trasformazione predefiniti forniti con Cisco SDM.

Nota

- Non tutti i router supportano tutti i set di trasformazione (tipi di crittografia). Nella finestra non verranno visualizzati i set di trasformazione non supportati.
- Non tutte le immagini IOS supportano tutti i set di trasformazione supportati da Cisco SDM. Nella finestra non verranno visualizzati i set di trasformazione non supportati dall'immagine IOS.
- Se è attivata la crittografia hardware, nella finestra verranno visualizzati solo i set di trasformazione supportati sia dalla crittografia hardware, sia dall'immagine IOS.

Dettagli del set di trasformazione selezionato (solo procedura guidata mappa crittografica)

Consente di visualizzare il nome, la crittografia, le caratteristiche di autenticazione e altri parametri della mappa crittografica selezionata.

Se questa icona viene visualizzata accanto al set di trasformazione, il set è di sola lettura e non può essere modificato.

Set di trasformazione selezionati in ordine di preferenza (solo configurazione manuale di mappa crittografica)

I set di trasformazione selezionati per la mappa crittografica, nell'ordine in cui verranno utilizzati. Durante le negoziazioni con un peer, il router offrirà i set di trasformazione nell'ordine fornito nell'elenco. È possibile utilizzare le frecce rivolte verso l'alto e verso il basso per riordinare l'elenco.

Tabella riassuntiva funzioni (solo procedura guidata mappa crittografica)

Funzione	Procedura
Utilizzo del set di trasformazione selezionato per la mappa crittografica.	Fare clic su **Avanti**.
Utilizzo di un altro set di trasformazione esistente.	Selezionarlo nell'elenco Seleziona set di trasformazione, quindi fare clic su **Avanti**.
Utilizzo di un nuovo set di trasformazione.	Fare clic su **Aggiungi** e creare il set di trasformazione nella finestra Aggiungi set di trasformazione. Quindi, tornare a questa finestra e fare clic su **Avanti**.
Modifica del set di trasformazione selezionato.	Fare clic su **Modifica**, quindi modificare il set di trasformazione nella finestra Modifica set di trasformazione.
Aggiunta di più set di trasformazione a questa mappa crittografica. È possibile compiere questa operazione per garantire che il router possa offrire un set di trasformazione che il peer accetterà di utilizzare.	Uscire dalla procedura guidata della mappa crittografica, deselezionare **Utilizza aggiunta guidata** e fare clic su **Aggiungi mappa crittografica**. La scheda Set di trasformazione consente di aggiungere e ordinare set di trasformazione.

Tabella riassuntiva funzioni (solo configurazione manuale di mappa crittografica)

Funzione	Procedura
Aggiunta di un set di trasformazione alla casella Set di trasformazione selezionati.	Selezionare un set di trasformazione nella casella Set di trasformazione disponibili e fare clic sulla freccia a destra.
Rimozione di un set di trasformazione dalla casella Set di trasformazione selezionati.	Selezionare il set di trasformazione che si desidera rimuovere e fare clic sulla freccia a sinistra.
Modifica dell'ordine di preferenza dei set di trasformazione selezionati.	Selezionare un set di trasformazione e fare clic sulla freccia rivolta verso l'alto o rivolta verso il basso.
Aggiunta di un set di trasformazione all'elenco Set di trasformazione disponibili.	Fare clic su **Aggiungi** e configurare il set di trasformazione nella finestra Aggiungi set di trasformazione.
Modifica di un set di trasformazione nell'elenco Set di trasformazione disponibili.	Fare clic su **Modifica** e configurare il set di trasformazione nella finestra Modifica set di trasformazione.

Aggiungi o Modifica mappa crittografica - Protezione del traffico

È possibile configurare la mappa crittografica per la protezione di tutto il traffico (solo procedura guidata mappa crittografica) oppure scegliere una regola IPSec per la protezione di traffico specifico.

Proteggere tutto il traffico all'interno delle seguenti subnet (solo procedura guidata mappa crittografica)

Utilizzare questa opzione per specificare una singola subnet di origine (una subnet sulla LAN), di cui si desidera crittografare il traffico, e una subnet di destinazione supportata dal peer specificato nella finestra Peer. Tutto il traffico che passa tra altre subnet di origine e destinazione verrà inviato non crittografato.

Origine

Immettere l'indirizzo della subnet di cui si desidera proteggere il traffico in uscita e specificare la relativa subnet mask. È possibile selezionare una subnet mask dall'elenco o specificarne una personalizzata. Il numero della subnet e la subnet mask devono essere immessi in formato decimale separato da punti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Verrà crittografato tutto il traffico proveniente da questa subnet di origine il cui indirizzo IP di destinazione si trova nella subnet di destinazione.

Destinazione

Immettere l'indirizzo della subnet di destinazione e specificare la relativa subnet mask. È possibile selezionare una subnet mask dall'elenco o specificarne una personalizzata. Il numero della subnet e la subnet mask devono essere immessi in formato decimale separato da punti.

Verrà crittografato tutto il traffico diretto agli host in questa subnet.

Regola IPSec (Creare/selezionare un comando access-list per il traffico IPSec)

È possibile aggiungere o modificare la regola IPSec utilizzata nella mappa crittografica. Utilizzare questa opzione se è necessario specificare più origini e destinazioni e/o specifici tipi di traffico da crittografare. Una regola IPSec può essere composta da più voci, ognuna delle quali può specificare tipi di traffico, origini e destinazioni diversi. Qualsiasi pacchetto che non soddisfa i criteri nella regola IPSec viene inviato non crittografato.

Nota Se si aggiunge una regola IPSec per una connessione VPN che utilizza un'interfaccia tunnel, la regola deve specificare gli stessi dati di origine e di destinazione della configurazione tunnel.

Per aggiungere o modificare la regola IPSec per la mappa crittografica, fare clic sul pulsante **...** a destra del campo della regola IPSec e selezionare una delle opzioni seguenti:

- **Seleziona regola esistente (ACL)** - Se la regola che si desidera utilizzare è già stata creata, fare clic su **OK**.

- **Crea una nuova regola e seleziona** - Se la regola desiderata non è stata creata, crearla e quindi fare clic su **OK**.
- **Nessuno** - Se si desidera cancellare l'associazione delle regole. Il campo della regola IPSec indica il nome della regola IPSec utilizzata ma se si seleziona l'opzione **Nessuno**, il campo viene svuotato.

Un ulteriore modo per aggiungere o modificare la regola IPSec per una determinata mappa crittografica è di immettere il numero della regola IPSec direttamente nel campo corrispondente.

Nota Le regole IPSec devono essere regole estese, non regole standard. Se il numero o il nome immesso indica una regola standard, Cisco SDM visualizzerà un messaggio di avviso quando si fa clic su OK.

Set di mappe crittografiche dinamiche

In questa finestra sono elencati i set di mappe crittografiche dinamiche configurate nel router.

Pulsanti Aggiungi/Modifica/Elimina

Utilizzare questi pulsanti per gestire le mappe crittografiche nella finestra. Se si tenta di eliminare un set di mappe crittografiche associate a un criterio IPSec, l'operazione verrà impedita da Cisco SDM. È necessario dissociare la mappa crittografica dal criterio prima di eliminarla. L'operazione può essere eseguita nella finestra Criteri IPSec.

Nome

Il nome della mappa crittografica dinamica.

Tipo

È sempre dinamico.

Aggiungi o Modifica set di mappe crittografiche dinamiche

Aggiungere o modificare un set di mappe crittografiche dinamiche in questa finestra.

Nome

Se si aggiunge una mappa crittografica dinamica, immettere il nome nel campo. Se si modifica un set di mappe crittografiche, il campo viene disattivato e non è possibile cambiare il nome.

Mappe crittografiche nel criterio IPSec

In quest'area sono elencate le mappe crittografiche utilizzate nel set. Utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** per aggiungere, rimuovere o modificare le mappe crittografiche dell'elenco.

Associare mappa crittografica al criterio IPSec

Numero sequenza

Immettere il numero di sequenza per identificare il set di mappe crittografiche. Il numero non può essere utilizzato da un altro set.

Selezionare il set di mappe crittografiche dinamiche

Selezionare il set di mappe crittografiche dinamiche che si desidera aggiungere dall'elenco.

Mappe crittografiche nel set di mappe crittografiche dinamiche

In quest'area sono elencati i nomi, i numeri di sequenza e i peer nel set di mappe crittografiche dinamiche selezionato.

Profili IPSec

In questa finestra sono elencati i profili IPSec configurati nel router. I profili sono formati da uno o più set di trasformazione configurati e vengono applicati ai tunnel mGRE per definire la modalità di crittografia del traffico incanalato nel tunnel.

Nome

Il nome del profilo IPSec.

Set di trasformazione

I set di trasformazione utilizzati nel profilo.

Descrizione

Una descrizione del profilo IPSec.

Aggiungi

Consente di aggiungere un nuovo profilo IPSec.

Modifica

Per modificare la configurazione del profilo, selezionare un profilo esistente e fare clic su **Modifica**.

Elimina

Consente di eliminare un profilo IPSec selezionato. Se il profilo che si sta eliminando è correntemente utilizzato in un tunnel DMVPN, è necessario configurare tale tunnel per utilizzare un profilo IPSec differente.

Dettagli del profilo IPSec

In quest'area dello schermo viene visualizzata la configurazione del profilo IPSec selezionato. Per una descrizione delle informazioni visualizzate in questa area, fare clic su Aggiungi o Modifica criterio IPSec.

Aggiungi o Modifica criterio IPSec

Immettere le informazioni necessarie per creare un profilo IPSec in questa finestra di dialogo. Un profilo IPSec specifica i set di trasformazione da utilizzare, la modalità di determinazione della lifetime Security Association (SA) e altre informazioni.

Colonne dei set di trasformazione

Utilizzare le due colonne nella parte superiore della finestra di dialogo per specificare i set di trasformazione da includere nel profilo. La colonna sinistra contiene i set di trasformazione configurati nel router. Per aggiungere un set di trasformazione configurato al profilo, selezionarlo e fare clic sul pulsante **>>**. Se la colonna sinistra non contiene alcun set di trasformazione o si necessita di un set di trasformazione ancora da creare, fare clic su **Aggiungi** e crearlo nella finestra di dialogo visualizzata.

Associazione profilo IKE

Per associare un profilo IKE a questo profilo IPSec, selezionare un profilo esistente dall'elenco. Se un profilo IKE è già stato associato, questo campo è di sola lettura.

Durata SA (Security Association) IPSec basata sul tempo

Per stabilire una nuova SA dopo che è trascorso un determinato periodo di tempo, fare clic su **Durata SA (Security Association) IPSec basata sul tempo**. Immettere il periodo di tempo nei campi HH:MM:SS di destra.

Durata SA (Security Association) IPSec basata sul volume di traffico

Per stabilire una nuova SA dopo che una determinata quantità di traffico è passata attraverso il tunnel IPSec, fare clic su **Durata SA (Security Association) IPSec basata sul volume di traffico**. Immettere il numero di kilobyte che devono passare attraverso il tunnel prima che la SA esistente venga interrotta a favore di una nuova SA.

Tempo di inattività SA (Security Association) IPSec

Per stabilire una nuova SA dopo che il peer è stato inattivo per un determinato periodo di tempo, fare clic su Tempo di inattività SA (Security Association) IPSec. Immettere il periodo di tempo di inattività nei campi HH:MM:SS di destra.

Perfect Forward Secrecy

Fare clic su **Perfect Forwarding Secrecy** se IPSec deve chiedere la PFS quando richiede nuove SA per questa interfaccia di modello virtuale oppure deve richiedere la PFS nelle richieste ricevute dal peer. È possibile specificare i valori riportati di seguito.

- gruppo 1: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 768 bit.
- gruppo 2: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 1024 bit.
- gruppo 5: per crittografare la richiesta PFS viene utilizzato il gruppo di moduli primario Diffie-Hellman a 1536 bit.

Aggiungi o Modifica profilo IPSec e Aggiungi mappa crittografica dinamica

Utilizzare la finestra per aggiungere o modificare un profilo IPSec o per aggiungere una mappa crittografica dinamica.

Nome

Immettere un nome per il profilo.

Set di trasformazione disponibili

In questa colonna sono elencati i set di trasformazione configurati nel router. Per aggiungere un set di trasformazione dall'elenco alla colonna Set di trasformazione selezionati, scegliere un set di trasformazione e fare clic sulla freccia a destra (>>).

Se è necessario configurare un nuovo set di trasformazione, fare clic sul nodo **Set di trasformazione** nella struttura IPSec per passare alla finestra corrispondente. Nella finestra, fare clic su **Aggiungi** per creare un nuovo set di trasformazione.

Set di trasformazione selezionati

In questa colonna sono elencati i set di trasformazione in uso nel profilo. È possibile selezionare più set di trasformazione in modo che il router che si sta configurando e quello sull'altra estremità del tunnel possano negoziare quale set di trasformazione utilizzare.

Set di trasformazione

In questa schermata è possibile visualizzare i set di trasformazione, aggiungerne di nuovi e modificare o rimuovere quelli esistenti.. Un set di trasformazione rappresenta una particolare combinazione di protocolli e algoritmi di protezione. Durante la negoziazione dell'associazione della protezione IPSec, i peer concordano nell'utilizzare un particolare set di trasformazione per proteggere un determinato flusso di dati.

È possibile creare più set di trasformazione e quindi specificarne uno o più di uno in una voce della mappa di crittografia. Il set di trasformazione definito nella voce verrà utilizzato nella negoziazione della Security Association IPSec per proteggere i flussi di dati specificati dall'elenco accesso della voce della mappa crittografica.

Durante le negoziazioni dell'associazione della protezione IPSec con IKE, i peer cercano un set di trasformazione che risulta lo stesso su entrambi i peer. Una volta trovato il set, viene selezionato e applicato al traffico protetto come parte delle Security Association IPSec di entrambi i peer.

Nome

Nome fornito al set di trasformazione.

Crittografia ESP

Cisco SDM riconosce i tipi di crittografia ESP riportati di seguito.

- ESP_DES: ESP (Encapsulating Security Payload), DES (Data Encryption Standard). DES supporta una crittografia a 56 bit.
- ESP_3DES: ESP, Triple DES. Si tratta di un tipo più avanzato rispetto al DES in quanto supporta la crittografia a 168 bit.

- ESP_AES_128: ESP, Advanced Encryption Standard (AES). Crittografia con chiave a 128 bit. L'AES fornisce una maggiore protezione rispetto al formato DES ed è più efficiente dal punto di vista computazionale del 3DES.
- ESP_AES_192: ESP, crittografia AES con chiave a 192 bit.
- ESP_AES_256: ESP, crittografia AES con chiave a 256 bit.
- ESP_NULL: algoritmo di crittografia Null, ma trasformazione crittografica utilizzata.
- ESP_SEAL: ESP con chiave di crittografia a 160 bit, algoritmo di crittografia SEAL (Software Encryption Algorithm). SEAL (Software Encryption Algorithm) è un algoritmo alternativo agli standard software DES (Data Encryption Standard), 3DES (Triple DES) e AES (Advanced Encryption Standard). La crittografia SEAL utilizza una chiave di crittografia a 160 bit e ha un impatto inferiore sulla CPU se paragonata ad altri algoritmi software.

Integrità ESP

Indica l'algoritmo di integrità utilizzato. La colonna contiene un valore se il set di trasformazione è configurato per fornire l'integrità dei dati e la crittografia. Nella colonna è contenuto uno dei valori riportato di seguito.

- ESP-MD5-HMAC: Message Digest 5, HMAC (Hash-based Message Authentication Code).
- ESP-SHA-HMAC: Security Hash Algorithm, HMAC.

Integrità AH

Indica l'algoritmo di integrità utilizzato. La colonna contiene un valore se il set di trasformazione è configurato per fornire l'integrità dei dati ma non la crittografia. Nella colonna è contenuto uno dei valori riportato di seguito.

- AH-MD5-HMAC: Message Digest 5.
- AH-SHA-HMAC: Security Hash Algorithm.

compressione IP

Indica se la compressione dei dati IP è utilizzata.

Nota Se il router non supporta tale compressione, la casella non verrà visualizzata.

Modalità

La colonna contiene uno dei valori riportati di seguito.

- Tunnel: le intestazioni e i dati sono crittografati. La modalità è utilizzata nelle configurazioni VPN.
- Trasporto: solo i dati sono crittografati. La modalità viene utilizzata quando gli endpoint di crittografia e quelli di comunicazione sono gli stessi.

Tipo

Definito dall'utente o Impostazioni predefinite Cisco SDM.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di un nuovo un set di trasformazione alla configurazione del router.	Fare clic su Aggiungi e creare il set di trasformazione nella finestra Aggiungi set di trasformazione.
Modifica di un set di trasformazione esistente.	Selezionare il set di trasformazione e fare clic su **Modifica**. Quindi, modificare il set di trasformazione nella finestra Modifica set di trasformazione.  **Nota** I set di trasformazione predefiniti Cisco SDM sono di sola lettura e non possono essere modificati.
Eliminazione di un set di trasformazione esistente.	Selezionare il set di trasformazione e fare clic su **Elimina**.  **Nota** I set di trasformazione predefiniti Cisco SDM sono di sola lettura e non possono essere eliminati.

Aggiungi o Modifica set di trasformazione

Utilizzare questa finestra per aggiungere o modificare un set di trasformazione.

Per ottenere una descrizione delle combinazioni di trasformazioni consentite e delle descrizioni delle trasformazioni, fare clic su **Combinazioni di trasformazioni consentite**.

Nota

- Non tutti i router supportano tutti i set di trasformazione (tipi di crittografia). Nella schermata non verranno visualizzati quelli non supportati.
- Non tutte le immagini IOS supportano tutti i set di trasformazione supportati da Cisco SDM. Nella schermata non verranno visualizzati i set di trasformazione non supportati dall'immagine IOS.
- Se è attivata la crittografia hardware, nella schermata verranno visualizzati solo i set di trasformazione supportati dalla crittografia hardware e dall'immagine IOS.
- I server Easy VPN supportano solo la modalità tunnel; non supportano quella di trasporto.
- I server Easy VPN supportano solo set di trasformazione con crittografia ESP; non supportano l'algoritmo AH.
- I server Easy VPN non supportano la crittografia ESP-SEAL.

Nome del set di trasformazione

Può essere un nome qualsiasi. Il nome non deve corrispondere a quello nel set di trasformazione utilizzato dal peer, tuttavia può essere utile attribuire ai set di trasformazione corrispondenti lo stesso nome.

Integrità dati con crittografia (ESP)

Selezionare questa casella se si desidera fornire integrità e crittografia ai dati ESP (Encapsulating Security Payload).

Algoritmo di integrità

Selezionare una delle seguenti opzioni:

- ESP_MD5_HMAC. Message Digest 5.
- ESP_SHA_HMAC. Security Hash Algorithm.

Crittografia

Cisco SDM riconosce i tipi di crittografia ESP riportati di seguito.

- ESP_DES. ESP (Encapsulating Security Payload), DES (Data Encryption Standard). DES supporta una crittografia a 56 bit.
- ESP_3DES. ESP, Triple DES. Si tratta di un tipo più avanzato rispetto al DES in quanto supporta la crittografia a 168 bit.
- ESP_AES_128. ESP, Advanced Encryption Standard (AES). Crittografia con chiave a 128 bit. L'AES fornisce una maggiore protezione rispetto al formato DES ed è più efficiente dal punto di vista computazionale del 3DES.
- ESP_AES_192. ESP, crittografia AES con chiave a 192 bit.
- ESP_AES_256. ESP, crittografia AES con chiave a 256 bit.
- ESP_SEAL: ESP con chiave di crittografia a 160 bit, algoritmo di crittografia SEAL (Software Encryption Algorithm). SEAL (Software Encryption Algorithm) è un algoritmo alternativo agli standard software DES (Data Encryption Standard), 3DES (Triple DES) e AES (Advanced Encryption Standard). La crittografia SEAL utilizza una chiave di crittografia a 160 bit e ha un impatto inferiore sulla CPU se paragonata ad altri algoritmi software.
- ESP_NULL. Algoritmo di crittografia Null, ma trasformazione crittografica utilizzata.

Nota I tipi di crittografia ESP disponibile dipendono dal router. A seconda del tipo di router che si configura, uno o più tipi di crittografia potrebbero non essere disponibili.

Integrità dati e indirizzi senza crittografia (AH)

Questa casella di controllo e i campi riportati di seguito vengono visualizzati quando si fa clic su **Mostra avanzate**.

Selezionare questa casella se si desidera fornire al router integrità dati e indirizzi AH (Authentication Header). L'intestazione dell'autenticazione non verrà crittografata.

Algoritmo di integrità

Selezionare una delle seguenti opzioni:

- AH_MD5_HMAC: Message Digest 5.
- AH_SHA_HMAC: Security Hash Algorithm.

Modalità

Selezionare le parti del traffico da crittografare.

- Trasporto. Crittografia solo dati: la modalità Trasporto è utilizzata quando IPSec è supportato da entrambi gli endpoint. Con Trasporto, AH o ESP vengono inseriti dopo l'intestazione IP originale, pertanto solo il payload IP viene crittografato. Questo metodo consente agli utenti di applicare servizi di rete quali i controlli Qualità del servizio (QoS) ai pacchetti crittografati. La modalità deve essere utilizzata solo quando la destinazione dei dati è sempre il peer VPN remoto.
- Tunnel. Crittografia dati e intestazione IP: la modalità Tunnel fornisce una protezione maggiore rispetto alla modalità Trasporto. Poiché tutto il pacchetto IP è incapsulato all'interno di AH o ESP, viene aggiunta una nuova intestazione IP e tutto il datagramma può essere crittografato. La modalità Tunnel consente ai dispositivi di rete, ad esempio un router, di agire come un proxy IPSec per più utenti VPN e deve essere utilizzata in tali configurazioni.

Compressione IP (COMP-LZS)

Selezionare questa casella se si desidera utilizzare la compressione dati.

Nota La compressione IP non è supportata su tutti i router. Se il router non supporta tale compressione, la casella è disattivata.

Regole IPSec

In questa finestra sono visualizzate le regole IPSec configurate per il router. Tali regole definiscono il traffico che verrà crittografato tramite IPSec. Nella parte superiore della finestra sono elencate le regole di accesso definite. Nella parte inferiore sono invece visualizzate le Rule entry di accesso selezionate nell'elenco delle regole.

Nelle regole IPSec sono contenuti l'indirizzo IP e le informazioni sul tipo di servizio. I pacchetti che soddisfano i criteri specificati nella regola vengono crittografati. I pacchetti che non soddisfano i criteri vengono inviati non crittografati.

Nome/Numero

Il nome o il numero della regola.

Utilizzata da

Le mappe crittografiche in cui è utilizzata la regola.

Tipo

Le regole IPSec devono specificare l'origine e la destinazione e devono poter specificare il tipo di traffico contenuto nel pacchetto. Pertanto le regole IPSec sono regole estese.

Descrizione

Una descrizione testuale della regola, se disponibile.

Azione

Consenti o **Nega**. **Consenti** indica che i pacchetti che soddisfano i criteri della regola sono protetti da crittografia. **Nega** indica che i pacchetti corrispondenti sono inviati non crittografati. Per maggiori informazioni vedere la sezione Significato delle parole chiave Consenti e Nega.

Origine

Un indirizzo IP o una parola chiave che specifica l'origine del traffico. **Any** specifica che l'origine può essere un qualsiasi indirizzo IP. Un indirizzo IP in questa colonna potrebbe essere visualizzato da solo o seguito da una maschera carattere jolly. Se presente, la maschera carattere jolly specifica le parti dell'indirizzo IP a cui deve corrispondere l'indirizzo IP di origine. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Destinazione

Un indirizzo IP o una parola chiave che specifica la destinazione del traffico. **Any** specifica che la destinazione può essere un qualsiasi indirizzo IP. Un indirizzo IP in questa colonna potrebbe essere visualizzato da solo o seguito da una maschera carattere jolly. Se presente, la maschera carattere jolly specifica le parti dell'indirizzo IP a cui deve corrispondere l'indirizzo IP di destinazione.

Servizio

Il tipo di traffico che deve essere contenuto nel pacchetto.

Tabella riassuntiva funzioni

Funzione	Procedura
Visualizzazione delle Rule entry di accesso di una determinata regola.	Selezionare la regola nell'elenco delle regole. Le voci della regola verranno visualizzate nella casella inferiore.
Aggiunta di una regola IPSec.	Fare clic su **Aggiungi** e creare la regola nella finestra visualizzata.
Eliminazione di una regola IPSec.	Selezionare la regola nell'elenco delle regole e fare clic su **Elimina**.
Eliminazione di una determinata voce della regola.	Selezionare la regola nell'elenco delle regole e fare clic su **Modifica**. Eliminare la voce nella finestra delle regole visualizzata.
Applicazione di una regola IPSec a un'interfaccia.	Applicare la regola nella finestra di configurazione dell'interfaccia.

CAPITOLO 16

Internet Key Exchange

Gli argomenti della guida di questa sezione descrivono le schermate di configurazione IKE (Internet Key Exchange).

IKE (Internet Key Exchange)

IKE (Internet Key Exchange) è un metodo standard per disporre di comunicazioni protette e autenticate e, inoltre, consente di stabilire delle chiavi di sessione (e relativa configurazione crittografica e di rete) tra due host presenti nella rete.

Cisco SDM consente di creare una IKE policy che proteggono le identità dei peer durante l'autenticazione. Cisco SDM consente anche di creare chiavi precondivise che i peer possono scambiarsi.

Tabella riassuntiva funzioni

Funzione	Procedura
Maggiori informazioni su IKE.	Fare clic su **Ulteriori informazioni sul protocollo IKE**.
Attivazione IKE. Per utilizzare le negoziazioni IKE è necessario attivare IKE per le connessioni VPN.	Fare clic su **Impostazioni globali**, quindi su **Modifica** per attivare IKE ed eseguire altre impostazioni globali per IKE.

Funzione	Procedura
Creazione di una IKE Policy. Cisco SDM fornisce una IKE Policy predefinita, tuttavia non è garantito che il peer abbia la stessa policy. È necessario configurare altre IKE Policy affinché il router sia in grado di fornire una IKE Policy accettata dal peer.	Fare clic sul nodo **IKE Policy** della struttura VPN. Per maggiori informazioni vedere la sezione IKE Policy.
Creazione di una chiave precondivisa. Durante l'utilizzo di IKE, i peer di ogni estremità devono scambiarsi una chiave precondivisa per effettuare l'autenticazione contemporaneamente.	Fare clic sul nodo **Chiave precondivisa** della struttura VPN. Per maggiori informazioni vedere la sezione Chiavi IKE precondivise.
Creazione di profilo IKE.	Fare clic sul nodo **Profilo IKE** della struttura VPN. Per maggiori informazioni vedere la sezione Profili IKE.

IKE Policy

Le negoziazioni IKE devono essere protette, quindi ciascuna di esse viene avviata su tutti i peer che soddisfano una IKE Policy comune (condiviso). In questa policy vengono indicati i parametri di protezione utilizzati per proteggere le negoziazioni IKE successive. In questa finestra sono visualizzate le IKE Policy configurate sul router ed è consentito aggiungere, modificare o eliminare una IKE Policy dalla configurazione del router. Se non è stato configurata nessuna IKE Policy sul router, nella finestra viene visualizzata la IKE Policy predefinita.

Una volta stabilito la conformità tra i due peer e la policy, i parametri di protezione della policy vengono identificati da una Security Association stabilita per ciascun peer. Queste Security Association vengono applicate a tutto il traffico IKE successivo durante la negoziazione.

Le IKE Policy di questo elenco sono disponibili per tutte le connessioni VPN.

Priorità

Un valore intero che specifica la priorità di questa policy rispetto alle altre IKE Policy configurate. Assegnare i numeri più bassi alle IKE Policy che si intende far utilizzare al router. Questi valori verranno forniti dal router durante la negoziazione.

Crittografia

Il tipo di crittografia da utilizzare per comunicare questa IKE Policy.

Hash

L'algoritmo di autenticazione per la negoziazione. Esistono due valori possibili:

- SHA (Secure Hash Algorithm)
- MD5 (Message Digest 5)

Autenticazione

Il metodo di autenticazione da utilizzare.

- Pre-SHARE. L'autenticazione verrà eseguita utilizzando chiavi precondivise.
- RSA_SIG. L'autenticazione verrà eseguita utilizzando firme digitali.

Tipo

SDM_DEFAULT o Definito dall'utente. Le policy SDM_DEFAULT non possono essere modificate.

Tabella riassuntiva funzioni

Funzione	Procedura
Maggiori informazioni sulle IKE Policy.	Vedere **Ulteriori informazioni sulle IKE Policy**.
Aggiunta di una IKE Policy alla configurazione del router. Cisco SDM fornisce una IKE Policy predefinita, tuttavia non è garantito che il peer abbia la stessa policy. È necessario configurare altre IKE Policy affinché il router sia in grado di fornire una IKE Policy accettata dal peer.	Fare clic su **Aggiungi** e configurare una nuova IKE Policy nella finestra Aggiungi IKE Policy.

Funzione	Procedura
Modifica di una IKE Policy esistente.	Scegliere la IKE Policy che si desidera modificare e quindi fare clic su **Modifica**. Quindi, modificare la IKE Policy nella finestra Modifica IKE Policy. Le IKE Policy predefinite sono di sola lettura e non possono essere modificati.
Rimozione di una IKE Policy dalla configurazione del router.	Scegliere la IKE Policy che si desidera rimuovere e quindi fare clic su **Rimuovi**.

Aggiungi o Modifica criterio IKE

Aggiungere o modificare una IKE Policy in questa finestra.

Nota

- Non tutti i router supportano tutti i tipi di crittografia. I tipi non supportati non verranno visualizzati nella schermata.
- Non tutte le immagini IOS supportano tutti i tipi di crittografia previsti in Cisco SDM. I tipi non supportati dall'immagine IOS non verranno visualizzati nella schermata.
- Se è attivata la crittografia hardware, nella schermata verranno visualizzati solo i tipi supportati dalla crittografia hardware e dall'immagine IOS.

Priorità

Un valore intero che specifica la priorità di questa policy rispetto alle altre IKE Policy configurate. Assegnare i numeri più bassi alle IKE Policy che si intende far utilizzare al router. Questi valori verranno forniti dal router durante la negoziazione.

Crittografia

Il tipo di crittografia da utilizzare per comunicare questa IKE Policy. In Cisco SDM sono supportati diversi tipi di crittografia, elencati in ordine di protezione. Più un tipo di crittografia è sicuro, maggiore sarà il tempo di elaborazione richiesto.

Nota Se il router non supporta un tipo di crittografia, questo non verrà visualizzato nell'elenco.

In Cisco SDM sono supportati i tipi di crittografia elencati di seguito.

- DES (Data Encryption Standard): è il formato che supporta la crittografia a 56 bit.
- 3DES (Triple Data Encryption Standard): si tratta di un tipo più avanzato rispetto al DES in quanto supporta la crittografia a 168 bit.
- AES-128: crittografia AES (Advanced Encryption Standard) con chiave a 128 bit. Fornisce una maggiore protezione rispetto al formato DES ed è più efficiente dal punto di vista computazionale del DES triplo.
- AES-192: crittografia AES (Advanced Encryption Standard) con chiave a 192 bit.
- AES-256: crittografia AES (Advanced Encryption Standard) con chiave a 256 bit.

Hash

L'algoritmo di autenticazione da utilizzare per la negoziazione. Esistono due opzioni:

- SHA (Secure Hash Algorithm)
- MD5 (Message Digest 5)

Autenticazione

Il metodo di autenticazione da utilizzare.

- Pre-SHARE. L'autenticazione verrà eseguita utilizzando chiavi precondivise.
- RSA_SIG. L'autenticazione verrà eseguita utilizzando firme digitali.

gruppi D-H

Gruppo D-H (Diffie-Hellman). Diffie-Hellman è un protocollo di crittografia a chiave pubblica che consente a due router di stabilire un segreto condiviso su un canale di comunicazione non protetto. Di seguito sono elencate le opzioni disponibili.

- Gruppo 1: Gruppo D-H a 768 bit. Gruppo D-H 1.
- Gruppo 2: Gruppo D-H a 1024 bit. Gruppo D-H 2. Questo gruppo fornisce maggiore protezione del gruppo 1 ma richiede un tempo di elaborazione più lungo.
- Gruppo 5: Gruppo D-H a 1526 bit. Gruppo D-H 5. Questo gruppo fornisce maggiore protezione del gruppo 2 ma richiede un tempo di elaborazione più lungo.

Nota

- Se il router non supporta il gruppo 5, non verrà visualizzato nell'elenco.
- I server Easy VPN non supportano il gruppo D-H 1.

Durata

Indica la durata di questa Security Association in ore, minuti e secondi. Il valore predefinito è un giorno oppure 24:00:00.

Chiavi IKE precondivise

Questa finestra consente di visualizzare, aggiungere, modificare ed eliminare le chiavi IKE precondivise dalla configurazione del router. Una chiave precondivisa viene scambiata con un peer remoto durante la negoziazione IKE. Entrambi i peer devono essere configurati con la stessa chiave.

Icona

Se una chiave precondivisa è di sola lettura, l'icona corrispondente viene visualizzata in questa colonna. La chiave precondivisa sarà di sola lettura se viene configurata con l'opzione CLI **no-xauth**.

IP/nome peer

Un indirizzo o un nome IP di un peer con cui questa chiave è condivisa. Con un indirizzo IP è possibile specificare tutti i peer presenti in una rete o in una subnet, oppure soltanto un host singolo. Se si specifica il nome, la chiave è condivisa sola dal peer denominato.

Maschera di rete

La maschera di rete consente di specificare in che misura l'indirizzo IP viene utilizzato per l'indirizzo di rete e in che misura per l'indirizzo host. Una maschera di rete di 255.255.255.255 indica che l'indirizzo IP del peer è un indirizzo per un host specifico. Una maschera di rete con zeri nei byte meno significativi indica, invece, che l'indirizzo IP del peer è un indirizzo di una rete o di una subnet. Ad esempio una maschera di rete di 255.255.248.0 consente di specificare che i primi 22 bit dell'indirizzo sono utilizzati per l'indirizzo di rete, mentre gli ultimi 100 bit rappresentano il numero host dell'indirizzo.

Chiave precondivisa

Non è possibile leggere la chiave precondivisa nelle finestre Cisco SDM. Per esaminare la chiave precondivisa, è necessario andare in **Visualizza- >Configurazione in corso**. Verrà visualizzata la configurazione corrente. La chiave è contenuta nel comando **crypto isakmp key**.

Funzione	Procedura
Aggiunta di una chiave precondivisa alla configurazione del router.	Fare clic su **Aggiungi** e aggiungere la chiave precondivisa nella finestra Aggiungi nuova chiave precondivisa.
Modifica di una chiave precondivisa esistente.	Selezionare la chiave precondivisa e fare clic su **Modifica**. Quindi, modificare la chiave nella finestra Modifica chiave precondivisa.
Rimozione di una chiave precondivisa esistente.	Selezionare la chiave precondivisa e fare clic su **Rimuovi**.

Aggiungi o Modifica chiave precondivisa

Utilizzare questa finestra per aggiungere o modificare una chiave precondivisa.

Chiave

Si tratta di una stringa alfanumerica che verrà scambiata con il peer remoto. Occorre configurare la stessa chiave con il peer remoto. La chiave deve risultare difficile da indovinare. Nella chiave precondivisa non devono essere utilizzati punti interrogativi (?) e spazi.

Reimmettere la chiave

Per confermare, immettere la stessa stringa del campo Chiave.

Peer

Selezionare **Nome host** se si desidera applicare la chiave a un host specifico. Selezionare **Indirizzo IP** se si desidera specificare una rete o una subnet oppure immettere l'indirizzo IP di un host specifico poiché non esiste alcun server DNS che converta i nomi degli host in indirizzi IP.

Nome host

Questo campo viene visualizzato se si seleziona "**Nome host**" nel campo Peer. Immettere il nome host del peer. Assicurarsi che nella rete si trovi un server DNS in grado di risolvere il nome host in un indirizzo IP.

Indirizzo IP/Subnet Mask

Questi campi vengono visualizzati quando si seleziona "Indirizzo IP" nel campo Peer. Immettere l'indirizzo IP di una rete o di una subnet nel campo Indirizzo IP. La chiave precondivisa verrà applicata a tutti i peer di quella rete o subnet. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Immettere una subnet mask se l'indirizzo IP immesso è l'indirizzo di una subnet e non l'indirizzo di un host specifico.

Autenticazione utente[Xauth]

Selezionare questa casella se i peer VPN site-to-site utilizzano XAuth per l'autenticazione. Se l'autenticazione Xauth è attiva nelle Impostazioni globali VPN, è attiva anche per i peer site-to-site e per le connessioni Easy VPN.

Profili IKE

I profili IKE, anche definiti profili ISAKMP, consentono di definire una serie di parametri IKE che possono essere associati ad uno o più tunnel IPSec. Un profilo IKE applica dei parametri a una connessione IPSec in entrata identificata unicamente attraverso il suo concetto di criteri di identità di corrispondenza. Questi criteri sono basati sull'identità IKE che è presentata dalle connessioni IKE in entrata e include l'indirizzo IP, FQDN (Fully Qualified Domain Name) e il gruppo di client remoti VPN (Virtual Private Network).

Per ulteriori informazioni sui profili ISAKMP, e sulla loro modalità di configurazione utilizzando l'interfaccia CLI Cisco IOS, andare a Cisco.com e seguire il percorso:

Products and Services > Cisco IOS Software > Cisco IOS Security > Cisco IOS IPSec > Product Literature > White Papers > ISAKMP Profile Overview (in inglese).

Profili IKE

Nell'area Profili IKE della schermata vengono elencati i profili IKE configurati e include il nome profilo, il profilo IPSec utilizzato e la descrizione dell'eventuale profilo. Se nessun profilo IPSec utilizza il profilo IKE selezionato, nella colonna Utilizzato da viene visualizzato il valore <nessuno>.

Quando si crea un profilo IKE da questa finestra, il profilo viene visualizzato nell'elenco. Quando si utilizza SDM per creare una configurazione server Easy VPN, vengono creati automaticamente i profili IKE, denominati da SDM, e visualizzati in questo elenco.

Dettagli del profilo IKE

Nell''area dello schermo relativa ai dettagli vengono visualizzati i valori di configurazione per il profilo selezionato. È possibile utilizzarla per visualizzare i dettagli senza fare clic sul pulsante Modifica e visualizzare un'altra finestra di dialogo. Se è necessario apportare modifiche, fare clic su Modifica e apportare le modifiche nella finestra di dialogo visualizzata. Per ulteriori informazioni sul contenuto di questa area, fare clic su Aggiungi o Modifica profilo IKE.

Aggiungi o Modifica profilo IKE

In questa finestra di dialogo è possibile immettere informazioni ed impostare valori per creare un profilo IKE ed associarlo a un'interfaccia tunnel virtuale.

Nome profilo IKE

Immettere un nome per il profilo IKE. Quando si modifica un profilo, questo campo è attivato.

Interfaccia tunnel virtuale

Scegliere l'interfaccia tunnel virtuale a cui si desidera associare questo profilo IKE dall'elenco Interfaccia tunnel virtuale. Per creare un'interfaccia tunnel virtuale, scegliere **Aggiungi**, quindi crearla nella finestra di dialogo visualizzata.

Tipo di identità corrispondenza

Il profilo IKE include i criteri di corrispondenza che consentono al router di identificare le connessioni in entrata e in uscita a cui si devono applicare i parametri di connessione IKE. I criteri di corrispondenza possono al momento essere applicati ai gruppi VPN. Il gruppo viene scelto automaticamente nel campo Tipo di identità corrispondenza.

Fare clic su **Aggiungi** per generare un elenco dei gruppi da includere nei criteri di corrispondenza.

Scegliere **Aggiungi nome gruppo esterno** per aggiungere il nome di un gruppo che non è configurato nel router e immettere il nome nella finestra di dialogo.

Scegliere **Seleziona da gruppi locali** per aggiungere il nome di un gruppo che è configurato nel router. Nella finestra di dialogo visualizzata, selezionare la casella accanto al gruppo da aggiungere. Se in altri profili IKE vengono utilizzati tutti i gruppi locali, SDM informa che tutti i gruppi sono stati selezionati.

Configurazione modalità

Scegliere **Rispondi** nel campo Configurazione modalità se il router deve rispondere alle richieste di configurazione della modalità.

Scegliere **Inizia** se il router deve iniziare le richieste di configurazione della modalità.

Scegliere **Entrambi** se il router deve sia iniziare le richieste di configurazione della modalità sia rispondere ad esse.

Criterio autorizzazione ricerca criterio gruppo

È necessario specificare un criterio di autorizzazione che controlli l'accesso ai dati dei criteri di gruppo sul server AAA. Scegliere **predefinito** se si desidera concedere l'accesso alle informazioni di ricerca dei criteri di gruppo. Per specificare un criterio, sceglierne uno esistente nell'elenco oppure fare clic su **Aggiungi** per creare un criterio nella finestra di dialogo visualizzata.

Criterio autenticazione utente

È possibile specificare un criterio di autenticazione degli utenti da utilizzare per gli accessi XAuth. Scegliere **predefinito** per consentire gli accessi XAuth. Per specificare un criterio di controllo degli accessi XAuth, scegliere un criterio esistente nell'elenco oppure fare clic su **Aggiungi**, creando così un criterio nella finestra di dialogo visualizzata.

DPD (Dead Peer Discovery)

Fare clic su **DPD (Dead Peer Discovery)** per consentire al router di inviare messaggi DPD ai peer. Se un peer non risponde ai messaggi DPD, la connessione viene interrotta.

Specificare il numero di secondi tra messaggi DPD nel campo Intervallo Keepalive. L'intervallo valido è compreso tra 1 e 3600 secondi.

Specificare il numero di secondi tra tentativi in seguito ad esito negativo dei messaggi DPD nel campo Tentativi. L'intervallo valido è compreso tra 2 e 60 secondi.

Il metodo DPD aiuta a gestire le connessioni senza intervento dell'amministratore ma genera pacchetti che i due peer devono elaborare per mantenere la connessione.

Descrizione

È possibile aggiungere una descrizione del profilo IKE che si sta aggiungendo o modificando.

CAPITOLO 17

Infrastruttura a chiave pubblica

Le finestre dell'infrastruttura a chiave pubblica consentono di generare richieste di registrazione, chiavi RSA e di gestire chiavi e certificati. È possibile utilizzare il processo SCEP (Simple Certificate Enrollment Process) per creare una richiesta di registrazione e una coppia di chiavi RSA, ricevere certificati online, creare una richiesta di registrazione che può essere inviata a un server della Certificate Authority (CA) in modalità non in linea.

Se si desidera utilizzare SDP (Secure Device Provisioning) per registrare i certificati, vedere Secure Device Provisioning.

Procedure guidate Certificati

Questa finestra consente di selezionare il tipo di registrazione in esecuzione e fornire informazioni all'utente sulle attività di configurazione da eseguire prima di iniziare la registrazione o sulle attività consigliate da Cisco prima della registrazione. Tali attività consentono di eliminare eventuali problemi che possono presentarsi.

Selezionare il metodo di registrazione utilizzato da Cisco SDM per generare la richiesta di registrazione.

Attività preliminari

Se Cisco SDM rileva che è necessario eseguire attività di configurazione prima di iniziare il processo di registrazione, questa casella consente di informare l'utente sulle attività da effettuare. Accanto al testo di avviso viene visualizzato un collegamento che porta alla sezione di Cisco SDM in cui è possibile completare la configurazione. Se Cisco SDM non rileva alcuna configurazione mancante, la finestra non sarà visualizzata. Le possibili attività preliminari sono descritte in Attività preliminari per le configurazioni PKI.

Protocollo SCEP (Simple Certificate Enrollment Protocol)

Fare clic su questo pulsante se si desidera stabilire una connessione diretta tra il router e il server della Certificate Authority (CA). Per effettuare questa operazione, è necessario disporre dell'URL di registrazione del server. La procedura guidata consente di effettuare le seguenti operazioni:

- Raccolta di informazioni per configurare un punto di attendibilità e inviarlo al router.
- Avvio di una registrazione con il server CA specificato nel punto di attendibilità.
- Se il server CA è disponibile, visualizzazione dell'impronta digitale del server CA come prova di accettazione.
- Se si accetta l'impronta digitale del server CA, completamento della registrazione.

Taglia e incolla / Importa da computer

Fare clic su questo pulsante se il router non riesce a stabilire una connessione diretta con il server CA o se si desidera generare una richiesta di registrazione e inviarla alla Certificate Authority in un altro momento. Dopo la generazione, la richiesta di registrazione può essere inviata alla CA successivamente. Per generare una richiesta, con la registrazione di tipo Taglia e incolla è necessario avviare la procedura guidata Certificati digitali e in seguito richiamarla dopo aver ottenuto i certificati per il server CA e per il router.

Nota Cisco SDM supporta solo le registrazioni di tipo Taglia e incolla PKCS#10 codificato base 64. Cisco SDM non supporta l'importazione delle registrazioni di certificati del tipo PEM e PKCS#12.

Pulsante Avvia attività selezionata

Consente di avviare la procedura guidata relativa al tipo di registrazione selezionato. Se Cisco SDM rileva un'attività obbligatoria da eseguire prima della registrazione, il pulsante viene disattivato. Una volta completata l'attività, il pulsante viene attivato.

Procedura guidata SCEP

In questa schermata viene visualizzata la procedura guidata SCEP in uso. Se non si desidera utilizzare il processo SCEP, fare clic su **Annulla** per uscire dalla procedura guidata.

Dopo aver completato la procedura guidata e dopo aver inviato i comandi al router, Cisco SDM tenta di contattare il server CA. Una volta contattato il server CA, Cisco SDM visualizza un messaggio con il certificato digitale del server.

Informazioni sulla Certificate Authority (CA)

In questa finestra vengono fornite tutte le informazioni per identificare il server CA. Viene inoltre specificata una password di verifica che sarà inviata insieme alla richiesta.

Nota Le informazioni immesse in questa schermata sono utilizzate per generare un punto di attendibilità con un metodo di controllo revoca predefinito di CRL. Se si sta modificando un punto di attendibilità esistente mediante la procedura guidata SCEP e se in questo punto è presente un metodo di revoca diverso da CRL, ad esempio OCPS, Cisco SDM non consentirà tale modifica. Se occorre modificare il metodo di revoca, andare nella finestra Certificati router, selezionare il punto di attendibilità configurato e fare clic sul pulsante **Controlla revoca**.

Nome alternativo del server CA

Il nome alternativo del server CA è un identificatore del punto di attendibilità che si sta configurando. Immettere un nome che consente di identificare un punto di attendibilità rispetto ad un altro.

URL di registrazione

Se si sta completando una registrazione SCEP, immettere l'URL di registrazione per il server CA in questo campo. Ad esempio,

```
http://CAuthority/enrollment
```

L'URL deve iniziare con http://. Assicurarsi che la connettività tra il router e il server CA funzioni prima di iniziare il processo di registrazione.

Questo campo non viene visualizzato se si sta completando una registrazione di tipo Taglia e incolla.

Password di verifica e Conferma password di verifica

Una password di verifica può essere inviata al server CA per utilizzarla in caso di revoca del certificato. È consigliabile effettuare questa operazione, poiché alcuni server CA non emettono certificati se il campo della password di verifica è vuoto. Per utilizzare una password di verifica, immettere la password e inserirla nuovamente nel campo di conferma. La password di verifica verrà inviata insieme alla richiesta di registrazione. Per motivi di sicurezza, la password di verifica è crittografata nel file di configurazione del router, quindi è necessario registrare la password e salvarla in una posizione facile da ricordare.

Questa password viene anche definita password di verifica.

Pulsante Opzioni avanzate

Le opzioni avanzate consentono di fornire maggiori informazioni sull'attivazione del router per contattare il server CA.

Opzioni avanzate

Utilizzare questa finestra per maggiori informazioni sull'attivazione del router per contattare il server CA.

Richiesta di certificato d'origine da un'interfaccia specifica

Selezionare questa casella per specificare una determinata interfaccia come origine del certificato.

Proxy HTTP e Porta HTTP

Se la richiesta di registrazione sarà inviata mediante un server proxy, immettere l'indirizzo IP del server proxy e il numero della porta da utilizzare per le richieste proxy in questi campi.

Attributi del nome dell'oggetto del certificato

Specificare le informazioni facoltative da includere nel certificato. Tutte le informazioni che si desidera includere nella richiesta di certificato verranno inserite nel certificato e saranno visualizzabili da qualsiasi punto in cui il router invia il certificato.

Includere nel certificato il nome FQDN (Fully Qualified Domain Name) del router.

Si consiglia di includere nel certificato il nome di dominio completo del router. Selezionare questa casella affinché Cisco SDM includa il nome di dominio completo del router nella richiesta di certificato.

Nota Se l'immagine Cisco IOS in esecuzione sul router non supporta questa funzione firewall, questo casella è disattivata.

FQDN

Se si attiva questo campo, immettere il nome FQDN dei router, ad esempio

`sjrtr.nomesocietà.net`

Includere indirizzo IP del router

Selezionare questa casella per includere un indirizzo IP valido configurato sul router nella richiesta di certificato. Se si seleziona questa casella, è possibile immettere manualmente un indirizzo IP o selezionare l'interfaccia di cui si intende utilizzare l'indirizzo IP.

Indirizzo IP

Consente di immettere un indirizzo IP e un indirizzo IP configurato sul router nel campo visualizzato. Immettere un indirizzo IP configurato sul router o un indirizzo assegnato al router.

Interfaccia

Selezionare un'interfaccia del router di cui si desidera includere l'indirizzo IP nella richiesta di certificato.

Includere il numero di serie del router

Selezionare questa casella se si desidera includere il numero seriale del router nel certificato.

Altri attributi dell'oggetto

Le informazioni immesse in questa finestra saranno inserite nella richiesta di registrazione. I server CA utilizzano lo standard X.500 per archiviare e mantenere le informazioni dei certificati digitali. Tutti i campi sono opzionali, ma si consiglia di immettere il maggior numero di informazioni possibili.

Nome comune (nc)

Immettere il nome comune da inserire in questo certificato. Sarà il nome utilizzato per cercare il certificato nella directory X.500.

Unità aziendale (ua)

Immettere l'unità aziendale o il nome del reparto da utilizzare per questo certificato. Sviluppo o Ufficio tecnico, ad esempio, possono essere unità aziendali.

Azienda(a)

Immettere il nome dell'organizzazione o dell'azienda. Questo è il nome dell'organizzazione X.500.

Stato (st)

Immettere lo stato o la provincia in cui si trova il router o l'azienda.

Paese (p)

Immettere il paese in cui si trova il router o l'azienda.

Email (e)

Immettere l'indirizzo email da inserire nel certificato del router.

Nota Se l'immagine Cisco IOS in esecuzione sul router non supporta questo attributo, il campo è disattivato.

Chiavi RSA

Includere una chiave pubblica RSA nella richiesta di registrazione. Dopo la concessione del certificato, la chiave pubblica sarà inclusa nel certificato affinché i peer possano utilizzarla per crittografare i dati inviati al router. La chiave privata viene conservata nel router, utilizzata per decrittografare i dati inviati dai peer e per la firma digitale delle transazioni durante le negoziazioni con i peer.

Genera nuova coppia di chiavi

Fare clic su questo pulsante per generare una nuova chiave da utilizzare nel certificato. Quando si genera una coppia di chiavi, è necessario specificare il modulo per determinare la dimensione della chiave. La nuova chiave viene visualizzata nella finestra Chiavi RSA al termine della procedura guidata.

Modulo

Immettere il valore relativo al modulo della chiave. Per un valore compreso tra 512 e 1024 immettere un valore intero multiplo di 64, mentre per un valore superiore a 1024, è possibile immettere 1536 o 2048. Se si immette un valore superiore a 512, la generazione della chiave può richiedere almeno un minuto.

Il modulo determina la dimensione della chiave. Più è grande il modulo, maggiore sarà la sicurezza della chiave; tuttavia, occorre più tempo per generare le chiavi con un modulo grande e le operazioni di crittografia/decrittazione necessitano di un tempo maggiore se le chiavi sono più grandi.

Genera coppie di chiavi distinte per la crittografia e per la firma

Per impostazione predefinita, Cisco SDM crea una coppia di chiavi con funzionalità generali che viene utilizzata sia per la crittografia sia per la firma. Se si desidera che Cisco SDM generi coppie di chiavi separate per crittografare e per firmare i documenti, selezionare questa casella di controllo. Cisco SDM genererà tali chiavi per la crittografaria e per la firma.

Utilizza coppia di chiavi RSA esistenti

Fare clic su questo pulsante per utilizzare una coppia di chiavi esistenti e selezionare la chiave dall'elenco a discesa.

Salva su token USB.

Selezionare la casella di controllo **Salva chiavi e certificati su token USB protetto** se si vogliono salvare le chiavi e i certificati su un token USB connesso al proprio router. Questa casella di controllo compare soltanto se c'è un token USB collegato al router.

Scegliere il nome del token USB dal menu a tendina **Token USB**. Immettere il PIN necessario per accedere al token USB in **PIN**.

Dopo avere scelto un token USB e immesso il suo PIN, fare clic su **Accesso** per accedere al token USB.

Riepilogo

In questa finestra sono riepilogate le informazioni fornite dall'utente e utilizzate per configurare un punto di attendibilità nel router e per avviare il processo di registrazione. Se nella finestra di dialogo Preferenze è attivato **Eseguire anteprima dei comandi prima dell'inoltro al router**, sarà possibile visualizzare l'anteprima di CLI inviata al router.

Per una registrazione SCEP

Dopo aver inviato i comandi al router, Cisco SDM tenta di contattare il server CA. Una volta contattato il server CA, Cisco SDM visualizza un messaggio con il certificato digitale del server.

Per una registrazione di tipo Taglia e incolla

Dopo aver inviato i comandi al router, Cisco SDM genera una richiesta di registrazione e visualizzata in un'altra finestra. Salvare la richiesta di registrazione e presentarla all'amministratore del server CA per ottenere il certificato del server CA e il certificato per il router. La richiesta di registrazione è in formato PKCS#10 codificato Base64.

Dopo aver ottenuto i certificati dal server CA, riavviare la procedura guidata Taglia e incolla e selezionare **Riprendi registrazione non completata** per importare i certificati nel router.

Certificato del server CA

In Cisco SDM viene visualizzata l'impronta digitale del certificato del server CA. Per proseguire il processo di registrazione è necessario accettare questo certificato. Se non si accetta il certificato, la registrazione non avrà luogo.

L'impronta digitale del certificato del server CA è:

In Cisco SDM viene visualizzato il valore esadecimale del certificato del server CA in lettere maiuscole. Ad esempio:

E55725EC A389E81E 28C4BE48 12B905ACD

Per accettare il certificato del server CA e proseguire il processo di registrazione

Fare clic su **Sì, accetto il certificato**, quindi fare clic su **Avanti**.

Per rifiutare il certificato del server CA ed interrompere il processo di registrazione

Fare clic su No, non accetto il certificato e fare clic su **Avanti**.

Stato registrazione

In questa finestra sono disponibili tutte le informazioni sullo stato del processo di registrazione. Se si verificano degli errori durante il processo, Cisco SDM visualizza le informazioni relative all'errore.

Una volta rilevato lo stato, fare clic su **Fine**.

Procedura guidata Taglia e incolla

Questa procedura consente di generare una richiesta di registrazione e di salvarla sul computer per inviarla alla Certificate Authority in modalità non in linea. Dal momento che non è possibile terminare la registrazione in un'unica sessione, verrà completata durante la procedura guidata quando si generano il punto di attendibilità e la richiesta di registrazione e dopo averli salvati sul computer.

Dopo aver inviato la richiesta di registrazione al server CA manualmente e aver ricevuto il certificato del server CA e il certificato per il router, avviare nuovamente la procedura guidata Taglia e incolla per completare la registrazione e importare i certificati nel router.

Attività di registrazione

Specificare se si sta iniziando una nuova registrazione o se si sta riepilogando una registrazione con una richiesta di registrazione salvata sul computer.

Avvia nuova registrazione

Fare clic su **Avvia nuova registrazione** per generare un punto di attendibilità, una coppia di chiavi RSA e una richiesta di registrazione che si possono salvare sul computer e inviare al server CA. La procedura guidata viene completata dopo aver salvato la richiesta di registrazione. Per completare la registrazione dopo aver ricevuto il certificato del server CA e il certificato per il router, avviare nuovamente la procedura guidata Taglia e incolla e selezionare **Riprendi registrazione non completata**.

Riprendi registrazione non completata

Fare clic su questo pulsante per riepilogare il processo di registrazione. È possibile importare i certificati ricevuti dal server CA e, se necessario, generare una nuova richiesta di registrazione per un punto di attendibilità.

Richiesta di registrazione

In questa finestra viene visualizzata la richiesta di registrazione di tipo PKCS#10 codificato base 64 generata dal router. Salvare la richiesta di registrazione nel computer e successivamente inviarla al server CA per ottenere il certificato.

Salva:

Nel computer individuare la directory in cui salvare il file di testo della richiesta di registrazione, nominare il file e fare clic su **Salva**.

Riprendi registrazione non completata

Per portare a termine una registrazione non completata, è necessario selezionare il punto di attendibilità associato alla registrazione non completata e quindi specificare la parte del processo di registrazione da completare. Se si sta importando un certificato del server CA o un certificato del router, il certificato deve essere disponibile sul computer.

Selezionare il nome alternativo del server CA (punto di attendibilità)

Selezionare il punto di attendibilità associato alla registrazione che si sta completando.

Importa certificati CA e router

Scegliere questa opzione per importare sia il certificato del server CA sia quello del router nella stessa sessione. Entrambi i certificati devono essere disponibili nel computer.

Questa opzione è disattivata se il certificato CA è già stato importato.

Importa certificato CA

Scegliere questa opzione per importare un certificato del server CA salvato nel computer. Dopo aver importato il certificato, Cisco SDM visualizzerà l'impronta digitale del certificato. Si può quindi verificare il certificato e accettarlo o rifiutarlo.

Questa opzione è disattivata se il certificato CA è già stato importato.

Importa certificati router

Scegliere questa opzione per importare un certificato per il router salvato nel computer. Dopo aver importato il certificato del router, Cisco SDM rileverà lo stato del processo di registrazione.

Nota È necessario importare il certificato del server CA prima di importare il certificato del router.

Genera richiesta di registrazione

Scegliere questa opzione se si deve generare una richiesta di registrazione per il punto di attendibilità selezionato. Il router genererà una richiesta di registrazione che è possibile salvare nel computer e inviare al server CA.

Cisco SDM genera una richiesta di registrazione in formato PKCS#10 codificato base 64.

Importa certificato CA

Se sul disco rigido è presente il certificato del server CA, è possibile individuarlo e importarlo sul router mediante questa finestra. È inoltre possibile copiare e incollare il testo del certificato nell'area di testo di questa finestra.

Pulsante Sfoglia

Consente di individuare il file del certificato sul computer.

Importa certificati router

Se sul disco rigido sono presenti uno o più certificati per il router assegnati dal server CA, è possibile cercarli e importarli nel router.

Importa altri certificati

Se si generano coppie di chiavi RSA distinte per la crittografia e la firma, si riceveranno due certificati per il router. Utilizzare questo pulsante per importare più di un certificato per il router.

Rimuovi certificato

Fare clic sulla scheda del certificato da rimuovere e quindi su **Rimuovi** certificato.

Sfoglia

Consente di localizzare il certificato e importarlo nel router.

Certificati digitali

In questa finestra è possibile visualizzare le informazioni relative ai certificati digitali configurati nel router.

Punti di attendibilità

Quest'area consente di visualizzare un riepilogo delle informazioni relative ai punti di attendibilità configurati nel router e i relativi dettagli; consente inoltre di modificarli e di determinare se un punto di affidabilità è stato revocato.

Pulsante Dettagli

Nell'elenco Punti di attendibilità vengono visualizzati solo il nome, l'URL di registrazione e il tipo di registrazione di un punto di attendibilità. Scegliere questo pulsante per visualizzare tutte le informazioni relative al punto di attendibilità selezionato.

Pulsante Modifica

È possibile modificare un punto di attendibilità se si tratta di un punto SCEP e se l'importazione dei certificati del server CA e del router non è stata completata correttamente. Se non si tratta di un punto di attendibilità SCEP o se sono stati inviati i certificati del server CA e del router associati a un punto di attendibilità SCEP, il pulsante è disattivato.

Pulsante Elimina

Consente di eliminare il punto di attendibilità selezionato. Con l'eliminazione di un punto di attendibilità vengono cancellati tutti i certificati ricevuti dalla Certificate Authority associata.

Pulsante Controlla revoca

Fare clic per controllare se il certificato selezionato è stato revocato. Cisco SDM visualizza una finestra di dialogo nella quale selezionare il metodo da utilizzare per il controllo della revoca. Per maggiori informazioni, vedere Controllo revoca e Metodo di controllo revoca: CRL.

Nome	Nome del punto di attendibilità.
Server CA	Il nome o l'indirizzo IP del server CA.
Tipo di registrazione	La scelta può essere effettuata tra una delle opzioni riportate di seguito. • Protocollo SCEP (Simple Certificate Enrollment Protocol): iscrizione eseguita mediante la connessione diretta al server CA. • Taglia e incolla: richiesta di registrazione importata dal computer. • TFTP: richiesta di registrazione eseguita con un server TFTP.

Catena di certificati per il *nome* dei punti di attendibilità

In quest'area sono visualizzati i dettagli dei certificati associati al punto di attendibilità selezionato.

Pulsante Dettagli

Consente di visualizzare il certificato selezionato.

Pulsante Aggiorna

Consente di aggiornare l'area Catena di certificati per punti di attendibilità:quando si seleziona un punto di attendibilità diverso nell'elenco Punti di attendibilità.

Tipo	La scelta può essere effettuata tra una delle opzioni riportate di seguito. • Certificato RA KeyEncipher: certificato di crittografia Rivest Adelman. • Certificato firma RA: certificato della firma Rivest Adelman. • Certificato CA: certificato dell'organizzazione CA. • Certificato: certificato del router.
Utilizzo	La scelta può essere effettuata tra una delle opzioni riportate di seguito. • Finalità generale: certificato con finalità generale utilizzato dal router per l'autenticazione nei peer remoti. • Firma: i certificati CA sono certificati di firme.
Numero di serie	Il numero seriale del certificato.
Mittente	Il nome del server CA che ha emesso il certificato.
Stato	La scelta può essere effettuata tra una delle opzioni riportate di seguito. • Disponibile: certificato disponibile all'utilizzo. • In sospeso: certificato applicato ma non disponibile all'utilizzo.
Scadenza (giorni)	Il numero di giorni in cui è possibile utilizzare il certificato prima della scadenza.
Data di scadenza	La data in cui il certificato scade.

Informazioni sul punto di attendibilità

Nella finestra Certificati router l'elenco Punti di attendibilità consente di visualizzare le informazioni principali su ciascun punto di attendibilità del router. Sono inoltre visualizzate tutte le informazioni necessarie per creare il punto di attendibilità.

Dettagli certificato

In questa finestra sono visualizzati tutti i dettagli dei punti di attendibilità non presenti nella finestra Certificati.

Controllo revoca

Specificare in questa finestra la modalità in cui il router deve controllare se il certificato è stato revocato.

Controllo revoca

Configurare la modalità in cui il router deve controllare le revoche e classificarle in base all'ordine di preferenza. Diversi sono i metodi che il router può utilizzare.

Utilizza/Metodo/Sposta su/Sposta giù

Selezionare i metodi da utilizzare, quindi scegliere i pulsanti **Sposta su** e **Sposta giù** per ordinare i metodi in base all'ordine di utilizzo.

- OCSP: contattare un server OCSP (Online Certificate Status Protocol) per determinare lo stato del certificato.
- CRL: controllo dei certificati revocati eseguito con un elenco certificati revocati.
- Nessuno: nessun controllo revoca.

URL query CRL

Attivato quando si seleziona CRL. Immettere l'URL in cui si trova l'elenco certificati revocati. Immettere l'URL solo se il certificato supporta X.500 DN.

URL OCSP

Attivato quando si seleziona OCSP. Immettere l'URL del server OCSP che si desidera contattare.

Metodo di controllo revoca: CRL

Specificare in questa finestra la modalità in cui il router deve controllare se il certificato è stato revocato.

Verifica

La scelta può essere effettuata tra una delle opzioni riportate di seguito.

- Nessuno: controllo del punto di distribuzione CRL incorporato nel certificato.
- Massimo sforzo: download di CRL dal server corrispondente se disponibile; in caso contrario, il certificato sarà accettato.
- Opzionale: controllo di CRL solo se è già stato eseguito il download nella cache come risultato del caricamento manuale.

URL query CRL

Immettere l'URL in cui si trova l'elenco certificati revocati. Immettere l'URL solo se il certificato supporta X.500 DN.

Finestra chiavi RSA

Questa finestra fornisce un sistema di crittografia e di autenticazione elettronico che utilizza un algoritmo elaborato da Ron Rivest, Adi Shamir e Leonard Adleman. L'algoritmo RSA è il sistema più utilizzato per la crittografia e l'autenticazione ed è incluso in Cisco IOS. Per utilizzare tale sistema, tramite un host di rete viene generata una coppia di chiavi, di cui una chiave è definita *chiave pubblica* e l'altra *chiave privata*. La chiave pubblica viene distribuita a tutti gli utenti che intendono inviare all'host dati crittografati. La chiave privata non viene condivisa. Quando si inviano dati da un host remoto, questi dati vengono crittografati con la chiave pubblica condivisa dall'host locale. Mediante la chiave privata, l'host locale consente di decrittografare i dati inviati.

Chiavi RSA configurate nel router

Nome	Nome della chiave. I nomi delle chiavi vengono assegnati automaticamente da Cisco SDM. La chiave "HTTPS_SS_CERT_KEYPAIR" e "HTTPS_SS_CERT_KEYPAIR.server" verrà visualizzata in sola lettura. Allo stesso modo, qualsiasi chiave bloccata/crittografata del router verrà visualizzata con le icone che ne indicano lo stato.
Utilizzo	Finalità generale o utilizzo. Le chiavi con finalità generale vengono utilizzate per crittografare i dati e per firmare il certificato. Se per crittografare i dati e per firmare i certificati vengono configurate chiavi distinte, queste sono denominate chiavi utilizzate.
Esportabile	Se in questa colonna è presente un segno di spunta, è possibile esportare la chiave in un altro router se quest'ultimo deve assumere il ruolo di router locale.

Dati della chiave

Consente di visualizzare una chiave RSA selezionata.

Pulsante Salva chiave sul computer

Consente di salvare i dati della chiave selezionata sul computer.

Genera coppia di chiavi RSA

Utilizzare questa finestra per generare una nuova coppia di chiavi RSA.

Etichetta

Immettere l'etichetta della chiave in questo campo.

Modulo

Immettere il valore relativo al modulo della chiave. Per un valore compreso tra 512 e 1024 immettere un valore intero multiplo di 64, mentre per un valore superiore a 1024, è possibile immettere 1536 o 2048. Se si immette un valore superiore a 512, la generazione della chiave può richiedere almeno un minuto.

Maggiore è la dimensione del modulo, più sicura sarà la chiave. Tuttavia le chiavi con moduli più grandi richiedono un tempo maggiore per generare ed elaborare, in caso di scambio.

Tipo

Selezionare il tipo di chiave da generare: **Finalità generale** o **Utilizzo**. Le chiavi con finalità generale vengono utilizzate per crittografare e per firmare i certificati. Se si generano chiavi utilizzate, un insieme di chiavi verrà utilizzato per crittografare e un altro per la firma dei certificati.

Casella di controllo Chiave esportabile

Selezionare questa casella se si desidera una chiave esportabile. È possibile inviare una coppia di chiavi esportabile a un router remoto se quest'ultimo deve sostituire il router locale.

Salva su token USB.

Selezionare la casella di controllo **Salva chiavi su token USB protetto** se si vogliono salvare le chiavi RSA su un token USB connesso al proprio router. Questa casella di controllo compare soltanto se c'è un token USB collegato al router.

Scegliere il nome del token USB dal menu a tendina **Token USB**. Immettere il PIN necessario per accedere al token USB in **PIN**.

Dopo avere scelto un token USB e immesso il suo PIN, fare clic su **Accesso** per accedere al token USB.

Credenziali Token USB

Questa finestra viene visualizzata quando si aggiungono o eliminano credenziali, come le coppie di chiavi RSA o i certificati digitali, che sono stati salvati su token USB. Per effettuare l'eliminazione è necessario fornire il nome del token USB e il PIN.

Scegliere il nome del token USB dal menu a tendina **Token USB**. Immettere il PIN necessario per accedere al token USB in **PIN**.

Token USB

In questa finestra è possibile configurare gli accessi al token USB. Questa finestra visualizza anche una lista di accessi configurati per il token USB. Quando un token USB è connesso al router Cisco, Cisco SDM utilizza l'accesso corrispondente per accedere al token.

Aggiungi

Fare clic su **Aggiungi** per aggiungere un nuovo token USB.

Modifica

Fare clic su **Modifica** per modificare un token USB esistente. Specificare l'accesso da modificare scegliendolo dall'elenco.

Elimina

Fare clic su **Elimina** per eliminare un token USB esistente. Specificare l'accesso da eliminare scegliendolo dall'elenco.

Nome del Token

Visualizza il nome utilizzato per accedere al token USB.

PIN utente

Visualizza il PIN utilizzato per accedere al token USB.

Numero massimo di tentativi per il PIN

Visualizza il numero di tentativi massimo che Cisco SDM effettuerà per accedere al token USB con il PIN fornito. Se l'accesso non riesce dopo il numero di tentativi specificati, Cisco SDM smetterà di cercare di accedere al token USB.

Timeout di rimozione

Visualizza il numero massimo di secondi in cui Cisco SDM continuerà a utilizzare le credenziali IKE (Internet Key Exchange) ottenute dal token USB dopo che il token è stato rimosso dal router.

Se Timeout di rimozione è vuoto verrà utilizzato il timeout predefinito. Il timeout predefinito viene calcolato a partire dal momento in cui si effettua un nuovo tentativo di accesso alle credenziali IKE.

File Config secondario

Visualizza il file di configurazione secondario che Cisco SDM cerca di trovare sul token USB. Il file di configurazione può essere un file CCCD o .cfg.

CCCD indica un file di configurazione. Sui token USB, un file CCCD viene caricato usando il software TMS.

Aggiungi o Modifica token USB

In questa finestra è possibile aggiungere o modificare gli accessi al token USB.

Nome del Token

Se si sta aggiungendo un accesso a un token USB, immettere il nome del token USB. Il nome immesso deve corrispondere al nome del token al quale si vuole accedere.

Il nome del token è impostato dal suo produttore. Per esempio, i token USB prodotti dalla Aladdin Knowledge Systems sono chiamati eToken.

È anche possibile utilizzare il nome “usbtoken*x*”, dove *x* è il numero della porta USB alla quale il token USB è connesso. Per esempio un token USB connesso alla porta USB 0 si chiamerà usbtoken0.

Se si sta modificando un accesso a un token USB, il campo Nome token non può essere modificato.

PIN corrente

Se si sta aggiungendo un accesso a un token USB o si sta modificando un accesso a un token USB privo di PIN, il campo PIN corrente visualizza la dicitura <Nessuno>. Se si sta modificando un accesso a un token USB provvisto di PIN, il campo Nome token visualizza ******.

Immettere il nuovo PIN

Immettere un nuovo PIN del token USB. Il nuovo PIN deve contenere almeno 4 cifre e deve corrispondere al nome del token al quale si vuole accedere. Se si sta modificando un accesso a un token USB, il PIN corrente sarà sostituito dal nuovo PIN.

Reimmettere il nuovo PIN

Reimmettere il nuovo PIN per confermarlo.

Numero massimo di tentativi per il PIN

Scegliere il numero di tentativi massimo che Cisco SDM effettuerà per accedere al token USB con il PIN fornito. Se l'accesso non riesce dopo il numero di tentativi specificati, Cisco SDM smetterà di cercare di accedere al token USB.

Timeout di rimozione

Immettere il numero massimo di secondi in cui Cisco SDM continuerà a utilizzare le credenziali IKE (Internet Key Exchange) ottenute dal token USB dopo che il token è stato rimosso dal router. Il numero di secondi deve essere compreso tra 0 e 480.

Se non si immette un numero verrà utilizzato il timeout predefinito. Il timeout predefinito viene calcolato a partire dal momento in cui si effettua un nuovo tentativo di accesso alle credenziali IKE.

File Config secondario

Specificare un file di configurazione esistente sul token USB. Il file può essere un file di configurazione parziale o completo. L'estensione del file deve essere .cfg.

Se può accedere al token USB, Cisco SDM unisce il file di configurazione specificato con la configurazione correntemente in esecuzione sul router.

Apri firewall

La schermata viene visualizzata quando Cisco SDM rileva un firewall nelle interfacce che blocca il traffico di ritorno indirizzato al router. Ad esempio, potrebbe essere visualizzata quando un firewall blocca il traffico DNS o PKI e impedisce al router di ricevere tale traffico dai server. Cisco SDM è in grado di modificare questi firewall in modo che i server possano comunicare con il router.

Modifica firewall

In quest'area sono elencate le interfacce di uscita e i nomi ACL ed è inoltre possibile selezionare i firewall che Cisco SDM deve modificare. Selezionare i firewall che Cisco SDM deve modificare nella colonna Azione. Cisco SDM li modificherà in modo da consentire il traffico SCEP o DNS dal server al router.

Tenere presente le seguenti informazioni sul traffico SCEP:

- Il firewall per i server CRL/OCSP non verrà modificato da Cisco SDM se questi non sono stati esplicitamente configurati nel router. Per consentire la comunicazione con i server CRL/OCSP, chiedere all'amministratore del server CA le informazioni corrette e modificare il firewall utilizzando la finestra Modifica ACL/Criterio firewall.
- Cisco SDM presuppone che il traffico inviato dal server CA al router passerà nelle stesse interfacce attraverso cui è stato inviato dal router al server CA. Se il traffico di ritorno del server CA passerà nel router tramite un'interfaccia diversa da quelle presenti negli elenchi Cisco SDM, è necessario aprire il firewall utilizzando la finestra Modifica ACL/Criterio firewall. Una situazione simile potrebbe verificarsi se si utilizza un routing asimmetrico con cui il traffico dal router al server CA esce dal router mediante un'interfaccia e il traffico di ritorno entra nel router tramite un'altra interfaccia.
- Le interfacce di uscita del router vengono determinate da Cisco SDM nel momento in cui si aggiunge la voce dei controlli di accesso di pass-through. Se si utilizza il protocollo di un routing dinamico per instradare le route al server CA e se una route viene modificata (le interfacce di uscita vengono modificate per il traffico SCEP destinato al server CA), è necessario aggiungere esplicitamente una voce dei controlli di accesso di pass-through ACE per tali interfacce mediante la finestra Modifica ACL/Criterio firewall.
- Cisco SDM aggiunge le voci dei controlli di accesso di pass-through ACE per il traffico SCEP, ma non vengono aggiunte per il traffico di revoca, ad esempio il traffico CRL e il traffico OCSP. Aggiungere esplicitamente tali voci per questo traffico mediante la finestra Modifica ACL/Criterio firewall.

Pulsante Dettagli

Fare clic su questo pulsante per visualizzare la voce di controllo dell'accesso che Cisco SDM aggiungerà al firewall se si consente la modifica.

Apri dettagli firewall

Questa finestra visualizza l'ACE (Access Control Entry) che Cisco SDM aggiungerebbe ad un firewall per consentire a vari tipi di traffico di accedere al router. Questa voce non viene aggiunta se non si seleziona **Modifica** nella finestra Apri firewall e se non si completa la procedura guidata.

CAPITOLO 18

Server Autorità di certificazione (CA)

È possibile configurare il router come server Autorità di certificazione (CA). Questo tipo di server consente di gestire le richieste di registrazione dei certificati provenienti dai client e può emettere e revocare i certificati digitali.

Per creare, ripristinare, modificare un server CA o eseguirne il backup, andare a **Configura > VPN > Infrastruttura a chiave pubblica > Server Autorità di certificazione > Crea server CA**.

Per gestire i certificati su un server CA esistente, andare a **Configura > VPN > Infrastruttura a chiave pubblica > Server Autorità di certificazione > Gestisci server CA**.

Per monitorare un server CA, andare a **Controllo > Stato VPN > Server CA**.

Crea server CA

In questa finestra è possibile avviare la procedura guidata di creazione di un server Autorità di certificazione (CA) o una procedura guidata di ripristino di un server CA. Su un router Cisco IOS è possibile impostare un solo server CA.

Tale server deve essere utilizzato per l'emissione di certificati agli host della rete privata, in modo che possano utilizzare questi certificati per l'autenticazione presso gli altri server.

Attività preliminari

Se Cisco SDM rileva attività di configurazione da eseguire prima di iniziare la configurazione del server CA, viene visualizzato un avviso in questa finestra. Accanto al testo di avviso viene visualizzato un collegamento che porta alla sezione di Cisco SDM in cui è possibile completare la configurazione. Se Cisco SDM non rileva alcuna configurazione mancante, la finestra non sarà visualizzata. Le possibili attività preliminari sono descritte in Attività preliminari per le configurazioni PKI.

Crea server Autorità di certificazione (CA)

Fare clic su questo pulsante per creare un server CA sul router. Dato che è possibile configurare un solo server CA sul router, questo pulsante è disattivato se è già configurato un server CA.

Nota Il server CA configurato utilizzando SDM consente di concedere e revocare certificati. Sebbene il router archivi il numero di serie e le altre informazioni identificative dei certificati concessi, non archivia i certificati stessi. Il server CA deve essere configurato con un URL diretto a un server di Autorità di registrazione (RA) in grado di archiviare i certificati concessi dal server CA.

Ripristina server CA

Se un server CA è già operativo sul router, è possibile ripristinarne la configurazione e le relative informazioni. Questa opzione è disattivata se non ci sono server CA configurati sul router.

Attività preliminari per le configurazioni PKI

Prima di iniziare la registrazione di un certificato o la configurazione di un server CA, è possibile che sia necessario completare le attività di configurazione di supporto. Prima che all'utente sia consentito di iniziare, SDM esamina la configurazione esistente, segnala le configurazioni da completare e fornisce collegamenti alle zone di SDM che consentono di completare tali configurazioni.

SDM può generare avvisi relativi alle seguenti attività di configurazione:

- Credenziali SSH non verificate: Cisco SDM richiede di fornire le credenziali SSH prima di iniziare.
- NTP non configurato: per la registrazione dei certificati è necessario fornire un orario preciso del router. L'identificazione di un server NTP (Network Time Protocol), dal quale il router può ottenere un orario preciso, fornisce un'origine ora senza alcun effetto se il router deve essere riavviato. Se l'organizzazione non dispone di un server NTP, potrebbe essere necessario utilizzare un server pubblicamente disponibile, quale il server descritto al seguente URL:

  http://www.eecis.udel.edu/~mills/ntp/clock2a.html
- DNS non configurato: la specifica dei server DNS consente di garantire che il router sia in grado di contattare il server di certificazione. Per contattare il server CA o un qualsiasi altro server per la registrazione del certificato come i server OCPS o gli archivi CRL, è necessaria la configurazione DNS se i server sono immessi come nomi e non come indirizzi IP.
- Dominio e/o Nome host non configurati: è necessario configurare il dominio e il nome host prima di iniziare la registrazione.

Procedura guidata server CA: Pagina iniziale

La procedura guidata Server Autorità di certificazione (CA) facilita l'utente durante la configurazione di un server CA. Prima di iniziare, accertarsi di avere le seguenti informazioni:

- Informazioni generali sul server CA: il nome che si intende dare al server, il nome dell'ente di emissione del certificato da utilizzare, il nome utente e la password che i richiedenti la registrazione dovranno immettere quando inviano la richiesta al server.
- Informazioni più dettagliate sul server: se il server funzionerà in modalità Autorità di registrazione (RA) o Autorità di certificazione (CA), il livello di informazioni su ogni certificato che il server archivierà, se il server dovrà concedere i certificati automaticamente e la durata dei certificati concessi, oltre alle richieste di registrazione aperte.
- Informazioni di supporto: collegamenti al server RA che archivierà i certificati e al server del punto di distribuzione elenco certificati revocati (CDP, Certificate Revocation List).

Procedura guidata server CA: Informazioni sull'autorità di certificazione

In questa finestra è possibile immettere le informazioni di base sul server CA che si sta configurando.

Nome server CA

Fornire un nome per identificare il server nel campo Nome server CA. Potrebbe essere il nome host del router o qualunque altro nome immesso.

Concedi

Scegliere **Manuale** se si desidera concedere i certificati manualmente. Scegliere **Auto** se si desidera che il server conceda i certificati in modo automatico. L'impostazione Auto, utilizzata principalmente per fini di debug, non è consigliata, perché provoca l'emissione di certificati senza richiedere le informazioni di registrazione.

Avviso **Non impostare Concedi su Auto se il router è connesso a Internet. Impostare Concedi su Auto solo per fini interni, ad esempio per l'esecuzione di procedure di debug.**

URL CDP

Immettere l'URL di un server punto di distribuzione CRL (CDP) nel campo URL CDP. L'URL deve essere nel formato HTTP. Ad esempio:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

Il CRL (Certificate Revocation List) è l'elenco dei certificati revocati. I dispositivi che devono verificare la validità del certificato di un altro dispositivo acquisiranno il CRL dal server CA. Dato che è possibile che molti dispositivi tentino di acquisire il CRL, il suo trasferimento su un dispositivo remoto, preferibilmente un server HTTP, ridurrà le conseguenze in termini di prestazioni sul router Cisco IOS che ospita il server CA. Se il dispositivo di controllo non è in grado di connettersi al CDP, utilizzerà come backup SCEP per acquisire il CRL dal server CA.

Attributi nome ente emittente

Nome comune (nc)

Immettere il nome comune da utilizzare per il certificato. Potrebbe essere il nome del server CA, il nome host del router o qualunque altro nome scelto.

Unità aziendale (ua)

Immettere l'unità aziendale o il nome del reparto da utilizzare per questo certificato. Supporto IT o Ufficio tecnico, ad esempio, possono essere unità aziendali.

Azienda (a)

Immettere il nome dell'organizzazione o dell'azienda.

Stato (st)

Immettere lo stato o la provincia in cui si trova l'azienda.

Paese (p)

Immettere il paese in cui si trova l'azienda.

Email (e)

Immettere l'indirizzo email da inserire nel certificato del router.

Opzioni avanzate

Fare clic su questo pulsante per accedere alle opzioni avanzate relative al server CA.

Opzioni avanzate

La schermata Opzioni avanzate consente di modificare i valori predefiniti delle impostazioni del server e di specificare l'URL del database che deve contenere le informazioni sui certificati.

Database

In questa sezione della finestra di dialogo è possibile configurare il livello database, l'URL del database e il formato del database.

Livello database

Scegliere il tipo di dati che verranno archiviati nel database di registrazione certificati:

- **minimal**: viene archiviata una quantità di informazioni sufficiente per continuare ad emettere nuovi certificati senza conflitti. Si tratta dell'impostazione predefinita.
- **names**: oltre alle informazioni date dall'opzione minimal, sono inclusi il numero di serie e il nome dell'oggetto di ogni certificato.
- **complete**: oltre alle informazioni date dall'opzione minimal, sono inclusi il numero di serie e il nome dell'oggetto di ogni certificato.

URL database

Immettere la posizione in cui il server CA scriverà i dati di registrazione dei certificati. Se non viene specificata alcuna posizione, i dati di registrazione dei certificati verranno scritti sulla memoria flash per impostazione predefinita.

Ad esempio, per scrivere i dati di registrazione dei certificati su un server tftp, immettere tftp://mytftp. Per ripristinare l'URL del database sulla memoria flash, immettere nvram.

Archivio database

Scegliere **pem** per creare l'archivio in formato pem oppure **pkcs 12** per creare l'archivio in formato pkcs12.

Nome utente database

Immettere il nome utente per l'archivio di database nel campo Nome utente database. Il nome utente e la password verranno utilizzati per autenticare il server sul database.

Password di database e Conferma password

Immettere la password nel campo Password di database, quindi reimmetterla nel campo Conferma password.

Durate

Impostare la durata o il tempo prima della scadenza degli elementi associati al server CA. Per impostare la durata di un elemento specifico, selezionarlo nell'elenco a discesa Durata e immettere un valore nel campo Durata.

È possibile impostare la durata per i seguenti elementi:

- **Certificato**: certificati emessi dal server CA. La durata viene immessa in giorni e deve essere compresa tra 1 e 1825. Se non viene immesso alcun valore, un certificato scade dopo un anno. Se viene immesso un nuovo valore, influisce solo sui certificati creati dopo l'impostazione del nuovo valore.
- **CRL**: l'elenco dei certificati revocati (Certificate Revocation List) relativo ai certificati emessi dal server CA. La durata viene immessa in ore e deve essere compresa tra 1 e 336. Se non viene immesso alcun valore, un CRL scade dopo 168 ore (una settimana).
- **Richiesta di registrazione**: richieste di certificato aperte esistenti nel database di registrazione, escluse quelle ricevute tramite SCEP. La durata viene immessa in ore e deve essere compresa tra 1 e 1000. Se non viene immesso alcun valore, una richiesta di registrazione aperta scade dopo 168 ore (una settimana).

Procedura guidata server CA: Chiavi RSA

l server CA utilizza chiave RSA pubbliche e private per crittografare i dati e per firmare i certificati. SDM genera automaticamente una nuova coppia di chiavi assegnandole il nome del server CA. È possibile modificare il modulo e il tipo di chiave, oltre che rendere la chiave esportabile. È necessario immettere una passphrase da utilizzare per ripristinare il server CA.

Etichetta

Il campo è di sola lettura. SDM utilizza il nome del server CA come nome della coppia di chiavi.

Modulo

Immettere il valore relativo al modulo della chiave. Per un valore compreso tra 512 e 1024 immettere un valore intero multiplo di 64, mentre per un valore superiore a 1024, è possibile immettere 1536 o 2048. Se si immette un valore superiore a 512, la generazione della chiave può richiedere almeno un minuto.

Il modulo determina la dimensione della chiave. Più è grande il modulo, maggiore sarà la sicurezza della chiave; tuttavia, occorre più tempo per generare le chiavi con un modulo grande e le operazioni di crittografia/decrittazione necessitano di un tempo maggiore se le chiavi sono più grandi.

Tipo

Per impostazione predefinita, Cisco SDM crea una coppia di chiavi con funzionalità generali che viene utilizzata sia per la crittografia sia per la firma. Se si desidera che Cisco SDM generi coppie di chiavi separate per crittografare e per firmare i documenti, scegliere **Chiavi utilizzate**. Cisco SDM genererà tali chiavi per la crittografia e per la firma.

Chiave esportabile

Se si desidera che la chiave del server CA sia esportabile, selezionare **Chiave esportabile**.

Passphrase e Conferma passphrase

Immettere nel campo Passphrase una passphrase da utilizzare per ripristinare il server CA dal backup. Reimmettere la stessa passphrase nel campo Conferma passphrase.

Apri firewall

La finestra Apri firewall viene visualizzata quando è necessario modificare una configurazione firewall per consentire la comunicazione tra il CDP e il server Server CA. Selezionare l'interfaccia e selezionare la casella **Modifica** per permettere a SDM di modificare il firewall di consentire questo traffico. Fare clic su **Dettagli** per visualizzare l'ACE da aggiungere al firewall.

Procedura guidata server CA: Riepilogo

La finestra di riepilogo visualizza le informazioni che sono state immesse nelle schermate della procedura guidata in modo da poterle esaminare prima di inviarle al router. Di seguito viene visualizzato un riepilogo di esempio:

```
------------------------------------------------------------
Configurazione server CA
------------------------------------------------------------
Nome server CA: CASvr-a
Concedi:Manuale
CDP URL:http://192.27.108.92/snrs.com
Nome comune (nc):CS1841
Unità aziendale (ua): Supporto IT
Azienda (a): Acme Enterprises.
Stato (st): CA
Paese (p): US

------------------------------------------------------------
Configurazione avanzata server CA
------------------------------------------------------------
URL database:nvram
Archivio database:pem
Nome utente database:crossi
Password database:*********

------------------------------------------------------------
Chiavi RSA:
------------------------------------------------------------
Il server CA genererà automaticamente la coppia di chiavi RSA con i
seguenti valori predefiniti:-
Modulo:1024
Tipo di chiave: Finalità generale
Chiave esportabile: No
Passphrase configurata: ******


------------------------------------------------------------
Voci dei controlli di accesso (ACE) di pass-through del firewall per
le interfacce:
------------------------------------------------------------

FastEthernet0/0
    permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

Il riepilogo visualizzato contiene quattro sezioni: Configurazione server CA, Configurazione avanzata server CA, Chiavi RSA e Pass-through di firewall. Il nome di questo server CA è CAsvr-a. I certificati verranno concessi manualmente. Le informazioni sui certificati verranno archiviate nella nvram, in formato PEM. SDM genererà una coppia di chiavi per finalità generale con il modulo predefinito 1024. La chiave non sarà esportabile. Verrà configurato un ACE per consentire il traffico tra il router e l'host CDP con l'indirizzo IP 192.27.108.92.

Gestisci server CA

Da questa finestra è possibile avviare e arrestare il server CA, accettare e rifiutare richieste di certificati e revocare certificati. Se occorre modificare la configurazione del server CA, è possibile disinstallare il server da questa finestra e tornare alla finestra Crea server CA per creare la configurazione necessaria.

Nome

Visualizza il nome del server. È quello che è stato definito alla creazione del server.

Icona Stato

Se il server CA è in esecuzione, vengono visualizzate le parole In esecuzione e un'icona verde. Se il server CA non è in esecuzione, vengono visualizzate la parola Arrestato e un'icona rossa.

Avvia server

Il pulsante Avvia server viene visualizzato se il server è stato arrestato. Fare clic su **Avvia server** per avviare il server CA.

Arresta server

Il pulsante Arresta server viene visualizzato se il server è in esecuzione; fare clic su **Arresta server** se è necessario arrestare il server CA.

Esegui backup server

Fare clic su **Esegui backup server** per eseguire il backup delle informazioni di configurazione del server sul PC. Immettere la posizione del backup nella finestra di dialogo visualizzata.

Disinstalla server

Fare clic per disinstallare il server CA dal router Cisco IOS. La configurazione del server CA e i relativi dati verranno rimossi. Se è stato eseguito il backup del server CA prima di disinstallarlo, è possibile ripristinarne i dati solo dopo la creazione di un nuovo server CA. Vedere Crea server CA.

Dettagli server CA

La tabella Dettagli server CA fornisce l'istantanea della configurazione del server CA. Nella tabella che segue vengono mostrate delle informazioni di esempio.

Nome elemento	Valore elemento
Durata certificato CA	1095 giorni
URL CDP	http://192.168.7.5
Durata CRL	168 ore
Durata certificato	365 giorni
Livello database	Minimo
URL database	nvram:
Durata richiesta di registrazione	168 ore
Concedi	Manuale
Nome ente emittente	CN=CertSvr
Modalità	Autorità di certificazione
Nome	CertSvr

Per la descrizione di questi elementi, vedere Procedura guidata server CA: Informazioni sull'autorità di certificazione e Opzioni avanzate.

Eseguire il backup del server CA

È possibile eseguire il backup su PC dei file contenenti le informazioni del Server CA. La finestra Eseguire il backup del server CA riporta i file che verranno inclusi nel backup. I file elencati devono essere presenti nella NVRAM del router perché il backup riesca.

Scegliere **Sfoglia** e specificare la cartella del PC in cui verrà eseguito il backup dei file del server CA.

Gestisci server CA - Finestra Ripristina

Se è stato eseguito il backup ed è stato disinstallato un Server CA, è possibile ripristinarne la configurazione sul router facendo clic sul pulsante **Ripristina server CA**. È necessario fornire il nome del server CA, l'URL di database completo e la passphrase di backup utilizzata nella configurazione iniziale. Quando si ripristina il server CA, è possibile modificare le impostazioni di configurazione.

Ripristina server CA

Se è stato eseguito il backup della configurazione di un Server CA disinstallato, è possibile ripristinarlo immettendo le informazioni relative ad esso nella finestra Ripristina server CA. È possibile modificare le impostazioni del server facendo clic su **Modifica impostazioni server CA prima del ripristino**. Per eseguire il backup del server o modificare le impostazioni del server è necessario fornire il nome, il formato file, l'URL di database e la passphrase.

Nome server CA

Immettere il nome del server CA di cui è stato eseguito il backup.

Formato file

Scegliere il formato file specificato nella configurazione del server: PEM o PKCS12.

URL completo

Immettere l'URL di database del router fornito al momento della configurazione del server CA. Si tratta della posizione in cui il server CA scriverà i dati di registrazione dei certificati. Vengono forniti di seguito due esempi di URL:

```
nvram:/mycs_06.p12
tftp://192.168.3.2/mycs_06.pem
```

Passphrase

Immettere la passphrase immessa al momento della configurazione del server CA.

Copia file server CA da PC

Selezionare la casella di controllo **Copia file server CA da PC** se si desidera copiare nella nvram del router le informazioni del server di cui è stato eseguito il backup sul PC.

Modifica impostazioni server CA prima del ripristino

Per modificare le impostazioni di configurazione del server CA prima di ripristinare il server, fare clic su **Modifica impostazioni server CA prima del ripristino**. Per informazioni sulle impostazioni modificabili, vedere Procedura guidata server CA: Informazioni sull'autorità di certificazione e Procedura guidata server CA: Chiavi RSA.

Modifica impostazioni server CA: scheda Generale

In questa finestra è possibile modificare le impostazioni generali di configurazione del server CA. Non è possibile cambiare il nome del server CA. Per informazioni sulle impostazioni modificabili, vedere Procedura guidata server CA: Informazioni sull'autorità di certificazione.

Modifica impostazioni server CA: scheda Avanzate

IN questa finestra è possibile modificare le impostazioni avanzate del server CA. Per informazioni su queste impostazioni, vedere Opzioni avanzate.

Gestisci server CA - Server CA non configurato

Questa finestra viene visualizzata quando si fa clic su **Gestisci server CA** ma non è configurato alcun server CA. Fare clic su **Crea server CA** e completare la procedura guidata per configurare un server CA sul router.

Gestisci certificati

Facendo clic su VPN > Infrastruttura a chiave pubblica > Autorità di certificazione > Gestisci certificati vengono visualizzate la scheda Richieste in sospeso e la scheda Certificati revocati. Per visualizzare gli argomenti della guida relativi a queste schede, fare clic sui seguenti collegamenti:

- Richieste in sospeso
- Certificati revocati

Richieste in sospeso

In questa finestra viene visualizzato l'elenco delle richieste di registrazione di certificati inviate dai client al server CA. La parte superiore della finestra contiene le informazioni e i controlli del server CA. Per informazioni sull'arresto, l'avvio e la disinstallazione del server CA, vedere Gestisci server CA.

È possibile scegliere una richiesta di registrazione di certificato presente nell'elenco per poi scegliere di emetterla (accettarla), respingerla o eliminarla. Le azioni disponibili dipendono dallo stato della richiesta di registrazione di certificato scelta.

Seleziona tutto

Scegliere **Seleziona tutto** per selezionare tutte le richieste di certificato in sospeso. Quando tutte le richieste sono selezionate, facendo clic su **Concedi** si accettano tutte le richieste. Facendo clic su **Rifiuta** quando tutte le richieste sono selezionate, tutte le richieste vengono rifiutate.

Concedi

Fare clic su **Concedi** per concedere il certificato al client richiedente.

Nota La finestra del server CA non visualizza gli ID dei certificati concessi. Se è necessario revocare un certificato, si dovrà richiedere l'ID del certificato all'amministratore del client per cui è stato emesso il certificato. L'amministratore del client potrà determinare l'ID del certificato immettendo il comando Cisco IOS sh crypto pki cert.

Elimina

Fare clic su **Elimina** per rimuovere la richiesta di registrazione di certificato dal database.

Rifiuta

Fare clic su **Rifiuta** per rifiutare la richiesta di registrazione di certificato.

Aggiorna

Fare clic su **Aggiorna** per aggiornare l'elenco di richieste di registrazione di certificato con le ultime modifiche.

Area delle richieste di registrazione di certificato

L'area delle richieste di registrazione di certificato presenta le seguenti colonne:

ID richiesta: numero univoco assegnato alla richiesta di registrazione di certificato.

Stato: stato corrente della richiesta di registrazione di certificato. Può essere In sospeso (nessuna decisione), Concesso (certificato emesso), Rifiutato (richiesta negata).

Impronta digitale: identificativo digitale univoco del cliente.

Nome oggetto: nome oggetto nella richiesta di registrazione.

Di seguito viene riportato un esempio di richiesta di registrazione.

ID richiesta	Stato	Impronta digitale	Nome oggetto
1	In sospeso	serialNumber=FTX0850Z0GT+ hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FDBBB5E8BA

Revoca certificato

Fare clic su **Revoca certificato** per visualizzare una finestra di dialogo che consente di immettere l'ID del certificato da revocare.

Nota L'ID del certificato non corrisponde sempre a quello della richiesta, visualizzato nelle finestre del server CA. Potrebbe essere necessario richiedere l'ID del certificato da revocare all'amministratore del client per cui è stato concesso il certificato. Per informazioni su come l'amministratore del client potrà determinare l'ID del certificato, vedere Richieste in sospeso.

Certificati revocati

Questa finestra visualizza l'elenco dei certificati emessi e revocati. È possibile revocare solo i certificati emessi. La parte superiore della finestra contiene le informazioni e i controlli del server CA. Per informazioni sull'arresto, l'avvio e la disinstallazione del server CA, vedere Gestisci server CA.

L'elenco dei certificati presenta le seguenti colonne:

- **N. serie certificato**: numero univoco assegnato al certificato. Questo numero viene visualizzato in formato esadecimale. Ad esempio, il numero di serie decimale 1 viene visualizzato come 0x01.
- **Data di revoca**: ora e data di revoca del certificato. Se un certificato è stato revocato 41 minuti e 20 secondi dopo la mezzanotte del 6 febbraio 2007, la data di revoca viene visualizzata nel formato 00:41:20 UTC Feb 6 2007.

Revoca certificato

Fare clic su **Revoca certificato** per visualizzare una finestra di dialogo che consente di immettere l'ID del certificato da revocare.

Nota L'ID del certificato non corrisponde sempre a quello della richiesta, visualizzato nelle finestre del server CA. Potrebbe essere necessario richiedere l'ID del certificato da revocare all'amministratore del client per cui è stato concesso il certificato. Per informazioni su come l'amministratore del client potrà determinare l'ID del certificato, vedere Richieste in sospeso.

Revoca certificato

In questa finestra è possibile revocare i certificati concessi da questo server CA.

ID certificato

Immettere l'ID del certificato da revocare.

Nota L'ID del certificato non corrisponde sempre a quello della richiesta, visualizzato nelle finestre del server CA. Potrebbe essere necessario richiedere l'ID del certificato da revocare all'amministratore del client per cui è stato concesso il certificato. Per informazioni su come l'amministratore del client potrà determinare l'ID del certificato, vedere Richieste in sospeso.

CAPITOLO 19

Cisco IOS SSL VPN

Cisco IOS SSL VPN fornisce una connettività con accesso remoto VPN SSL (Secure Socket Layer) da quasi tutte le posizioni abilitate a Internet utilizzando esclusivamente un browser Web e la corrispondente crittografia SSL nativa. In questo modo le società sono in grado di estendere le reti aziendali protette a tutti gli utenti autorizzati, fornendo una connettività con accesso remoto alle risorse aziendali da qualsiasi posizione abilitata a Internet.

Cisco IOS SSL VPN inoltre abilita l'accesso dai computer non di proprietà dell'azienda, compresi il computer di casa, le postazioni Internet e gli hotspot wireless, laddove un reparto IT non è in grado di distribuire e gestire facilmente il software client VPN necessario per le connessioni VPN IPSec.

Esistono tre modalità di accesso VPN SSL: senza client, thin client e con client per il full tunnel e tutte e tre sono supportate da Cisco SDM. Di seguito la descrizione di ognuna:

- **Clientless VPN SSL**. La modalità senza client fornisce l'accesso protetto alle risorse Web private nonché l'accesso ai contenuti Web. Permette di accedere alla maggior parte dei contenuti utilizzati in genere all'interno di un browser Web, quali l'accesso intranet e gli strumenti in linea che utilizzano un'interfaccia Web.
- **Thin Client VPN SSL** (applet Java di inoltro su porta). La modalità thin client consente di estendere le funzionalità di crittografia del browser Web per attivare l'accesso remoto alle applicazioni basate su TCP, ad esempio POP3, SMTP, IMAP, Telnet e SSH.

- **Full Tunnel Client VPN SSL**. La modalità client per il full tunnel offre un supporto completo per le applicazioni grazie al software client VPN SSL per Cisco IOS VPN SSL scaricato dinamicamente. Con il client per il full tunnel per Cisco IOS SSL VPN, Cisco fornisce un client di tunneling VPN SSL leggero, configurato centralmente e facile da supportare, che consente un accesso di connettività a livello di rete virtualmente a qualsiasi applicazione.

Contesti Cisco IOS SSL VPN, gateway e criteri descrive il funzionamento combinato dei componenti di una configurazione di Cisco IOS SSL VPN.

Per i collegamenti ai documenti Cisco IOS SSL VPN, fare clic su Collegamenti Cisco IOS SSL VPN sul sito Web di Cisco.

Collegamenti Cisco IOS SSL VPN sul sito Web di Cisco

In questo argomento della Guida vengono elencati i collegamenti correnti che forniscono le informazioni più utili riguardo a Cisco IOS SSL VPN.

L'indirizzo riportato di seguito consente l'accesso ai documenti relativi a Cisco IOS SSL VPN. È opportuno tornare di tanto in tanto su tale collegamento per conoscere le informazioni aggiornate.

www.cisco.com/go/iosSSLVPN

Le modalità di configurazione del server AAA con il protocollo RADIUS per Cisco IOS SSL VPN sono illustrate all'indirizzo riportato di seguito.

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Crea VPN SSL

È possibile utilizzare le procedure guidate Cisco IOS SSL VPN per la creazione di una nuova Cisco IOS SSL VPN oppure per l'aggiunta di nuovi criteri o nuove funzionalità a una Cisco IOS SSL VPN esistente.

Fare clic su Cisco IOS SSL VPN per avere una panoramica delle funzioni supportate da Cisco SDM. Contesti Cisco IOS SSL VPN, gateway e criteri descrive il modo in cui interagiscono i componenti di una configurazione Cisco IOS SSL VPN.

Per i collegamenti ai documenti Cisco IOS SSL VPN, fare clic su Collegamenti Cisco IOS SSL VPN sul sito Web di Cisco.

Attività preliminari

Prima di procedere alla configurazione di VPN SSL Cisco IOS, è necessario configurare AAA e certificati sul router. In quest'area della finestra sarà visualizzata una notifica dell'eventuale mancanza di una o entrambe le configurazioni pertinenti e in tal caso sarà indicato un collegamento per consentirne il relativo completamento. Quando tutte le configurazioni preliminari saranno state completate, sarà possibile tornare alla presente finestra e iniziare la configurazione di Cisco IOS SSL VPN.

Cisco SDM attiva AAA senza immissioni da parte dell'utente. Cisco SDM consente di generare chiavi pubbliche e private per il router e di registrarle con una Certification Authority per ottenere i certificati digitali. Per maggiori informazioni vedere la sezione Infrastruttura a chiave pubblica. In alternativa è possibile configurare un'autocertificazione permanente, per cui non è necessaria l'approvazione da parte di una CA. Per maggiori informazioni sulla funzionalità di autocertificazione permanente, fare riferimento al collegamento indicato di seguito:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Assicurarsi che l'intero URL sia presente nel campo di collegamento del browser in uso.

Crea una nuova VPN SSL

Selezionare questa opzione per creare una nuova configurazione di VPN SSL Cisco IOS. La procedura guidata consente di creare una VPN SSL Cisco IOS con un solo criterio utente e una serie limitata di funzioni. Al termine di questa creazione guidata, è possibile utilizzare altre procedure guidate per configurare ulteriori criteri e funzionalità per VPN SSL Cisco IOS. Per creare configurazioni VPN SSL Cisco IOS aggiuntive, tornare a questa procedura.

Quando si configura per la prima volta una VPN SSL Cisco IOS in Cisco SDM su di un router, viene creato un contesto VPN SSL Cisco IOS, viene configurato un gateway e viene creato un criterio di gruppo. Al termine della procedura guidata, fare clic su **Modifica VPN SSL** per visualizzare la configurazione e conoscere il funzionamento dei componenti di VPN SSL Cisco IOS. Per una maggiore comprensione della configurazione iniziale, fare clic su Contesti Cisco IOS SSL VPN, gateway e criteri.

Aggiungi un nuovo criterio a un VPN SSL esistente per un nuovo gruppo di utenti

Selezionare questa opzione per aggiungere un nuovo criterio a una configurazione VPN SSL Cisco IOS esistente per un nuovo gruppo di utenti. La disponibilità di più criteri consente di definire serie di funzionalità differenti per i vari gruppi di utenti. Ad esempio, si potrebbe definire un criterio specifico per l'ufficio tecnico e un altro per le vendite.

Configura funzionalità avanzate per una VPN SSL esistente

Selezionare questa opzione per configurare funzionalità avanzate per un criterio VPN SSL Cisco IOS esistente. È necessario specificare il contesto in cui è configurato il criterio.

Pulsante Avvia attività selezionata

Scegliere questo pulsante per avviare la configurazione selezionata. Nel caso in cui non sia possibile completare l'attività scelta, si riceverà un messaggio di avviso. Se è necessario portare a termine un'attività preliminare, verrà indicato il tipo di attività e il procedimento per completarla.

Autocertificazione permanente

Le informazioni richieste per un'autocertificazione permanente possono essere fornite in questa finestra di dialogo. Tramite il server HTTPS verrà generato un certificato con le informazioni fornite, che sarà utilizzato nell'handshake SSL. Le autocertificazioni permanenti sono conservate nella configurazione anche in caso di ricaricamento del router e vengono introdotte nel corso dell'handshake SSL. I nuovi utenti devono accettare manualmente questi certificati. Questa operazione non è necessaria per gli utenti che l'abbiano già eseguita una volta, anche in caso di ricaricamento del router.

Per maggiori informazioni sulla funzionalità di autocertificazione permanente, fare riferimento al collegamento indicato di seguito:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Assicurarsi che l'intero URL sia presente nel campo di collegamento del browser in uso.

Nome

Cisco SDM inserisce in questo campo il nome del certificato del router. Se lo si desidera, è possibile modificare il nome, che corrisponderà al nome dell'oggetto utilizzato per la richiesta del certificato.

Lunghezza della chiave RSA

Cisco SDM inserisce in questo campo il valore 512. Se lo si desidera, è possibile specificare una chiave più lunga, ad esempio 1024. Il valore della lunghezza della chiave deve corrispondere a un multiplo di 64.

Oggetto

Fornire le informazioni per i campi dell'area oggetto. Per maggiori informazioni su questi campi, vedere Altri attributi dell'oggetto.

Pulsante Genera

Dopo avere inserito le informazioni in questa finestra, fare clic su **Genera** per creare l'autocertificazione permanente tramite il router.

Pagina iniziale

Nella finestra iniziale di tutte le procedure guidate sono elencate le rispettive attività di cui la procedura consente il completamento. Consultare queste informazioni per verificare l'utilizzo della procedura idonea. Nel caso in cui non si stia utilizzando la procedura opportuna, fare clic su **Annulla** per tornare alla finestra Crea VPN SSL e scegliere quella corretta.

Dopo aver inserito tutte le informazioni richieste per la procedura guidata, queste vengono visualizzate nella finestra di riepilogo. Per visualizzare i comandi CLI Cisco IOS da inoltrare al router, fare clic su **Annulla** per uscire dalla procedura guidata e passare a **Modifica > Preferenze** e selezionare **Eseguire l'anteprima dei comandi prima dell'inoltro al router.** Riavviare quindi la procedura guidata e immettere le informazioni richieste. Durante l'inoltro della configurazione al router, viene visualizzata una finestra aggiuntiva in cui sono indicati i comandi CLI Cisco IOS che vengono inviati.

Gateway VPN SSL

Un gateway VPN SSL Cisco IOS fornisce l'indirizzo IP e il certificato digitale per il Contesto VPN SSL in cui è utilizzato. In questa finestra è possibile inserire le informazioni per un gateway e i dati che consentiranno agli utenti l'accesso al portale.

Campi Indirizzo IP e Nome

Utilizzare questi campi per creare l'URL mediante il quale gli utenti avranno accesso alla pagina del portale VPN SSL Cisco IOS. Nell'elenco di indirizzi IP sono contenuti gli indirizzi di tutte le interfacce router configurate, nonché tutti i gateway VPN SSL Cisco IOS esistenti. È possibile utilizzare l'indirizzo IP di un'interfaccia router se corrisponde a un indirizzo pubblico raggiungibile dai client prestabiliti oppure utilizzare un altro indirizzo IP pubblico raggiungibile dai client.

Quando si immette un indirizzo IP mai utilizzato per un gateway, viene creato un nuovo gateway.

Casella di controllo Allow Cisco SDM access through *IP Address (Consenti accesso a SDM mediante indirizzo IP)*

Selezionare questa casella se si desidera continuare ad accedere a Cisco SDM da questo indirizzo IP. Questa casella di controllo viene visualizzata all'immissione dell'indirizzo IP attualmente utilizzato per accedere a Cisco SDM.

Nota Selezionando questa casella di controllo, l'URL richiesto per l'accesso a Cisco SDM sarà modificato dopo l'inoltro della configurazione al router. Rivedere l'area delle informazioni in basso alla finestra per sapere quale URL utilizzare. Cisco SDM colloca un collegamento a tale URL su desktop del PC, utilizzabile per gli accessi futuri a Cisco SDM.

Certificato digitale

Se si crea un nuovo gateway, selezionare il certificato digitale che il router presenterà ai client al momento dell'accesso al gateway. Se invece si è scelto l'indirizzo IP di un gateway esistente, il router utilizzerà il certificato digitale configurato per quel determinato gateway e di conseguenza questo campo non viene attivato.

Area informazioni

Quando vengono inserite le informazioni nei campi Indirizzo IP e Nome, quest'area contiene l'URL che gli utenti immetteranno. È necessario fornire questo URL agli utenti ai quali è destinata la VPN SSL Cisco IOS.

Se è stato selezionato **Consenti l'Cisco SDM accesso tramite *indirizzo IP***, l'URL da utilizzare per gli accessi futuri Cisco SDM viene riportato in quest'area. Cisco SDM colloca un collegamento a tale URL sul desktop del PC dopo aver inviato la configurazione Cisco IOS SSL VPN al router.

Autenticazione utente

Utilizzare questa finestra per specificare la modalità con cui il router deve eseguire l'autenticazione utente. Il router può autenticare gli utenti VPN SSL Cisco IOS in locale oppure inviare la richiesta di autenticazione ai server AAA remoti.

Pulsante Server AAA esterno

Fare clic su questo pulsante se si desidera che il router utilizzi un server AAA per l'autenticazione degli utenti VPN SSL Cisco IOS. Il router utilizzerà i server AAA elencati in questa finestra. Se non è configurato alcun server, è possibile configurarli in questa finestra. Per utilizzare questa opzione, è necessario che almeno un server AAA sia configurato sul router.

Pulsante In locale su questo router

Fare clic su questo pulsante se si desidera che il router proceda all'autenticazione degli utenti in locale. Il router autenticherà tutti gli utenti visualizzati nella finestra. Se sul router non è stato ancora configurato alcun utente, è possibile aggiungerli in questa finestra.

Pulsante Prima su un server AAA esterno, quindi in locale su questo router

Fare clic su questo pulsante se si desidera che, per l'autenticazione degli utenti, il router utilizzi in primo luogo un server AAA e in caso di tentativo non riuscito passi all'autenticazione in locale. Nel caso in cui l'utente non sia configurato o sul server AAA oppure in locale sul router, non sarà possibile autenticarlo.

Pulsante Utilizzare l'elenco dei metodi di autenticazione AAA

Fare clic su questo pulsante se si desidera che il router utilizzi un elenco di metodi per l'autenticazione. Un elenco di questo tipo comprende i metodi di autenticazione che possono essere utilizzati. Il router tenta il primo metodo di autenticazione dell'elenco. Se l'autenticazione non riesce, il router tenta il successivo metodo dell'elenco e continua in questo modo fino ad autenticazione effettuata o fino alla fine dell'elenco.

Elenco Server AAA configurati per questo router

L'elenco contiene i server AAA utilizzati dal router per l'autenticazione degli utenti. Se si è scelto di autenticare gli utenti mediante i server AAA, in questo elenco deve essere compreso il nome o l'indirizzo IP di almeno un server. Utilizzare il pulsante **Aggiungi** per aggiungere le informazioni per un nuovo server. Per gestire le configurazioni AAA sul router, uscire dalla procedura guidata, fare clic su **Attività aggiuntive**, quindi selezionare il nodo AAA nella struttura della attività aggiuntive. Se è stato selezionato il pulsante **In locale su questo router**, questo elenco non sarà visualizzato.

Creare gli account utente in locale su questo router

Inserire in questo elenco gli utenti che devono essere autenticati dal router. Utilizzare i pulsanti **Aggiungi e Modifica** per gestire gli utenti sul router. Se è stato selezionato il pulsante **Server AAA esterno**, questo elenco non sarà visualizzato.

Configura siti Web intranet

In questa finestra è possibile configurare gruppi di siti Web intranet a cui si desidera che i client abbiano accesso. Questi collegamenti saranno visualizzati nel portale che appare nel momento in cui gli utenti accedono a VPN SSL Cisco IOS.

Colonne Azione ed Elenco URL

Quando si aggiunge un criterio a un contesto VPN SSL Cisco IOS esistente, è possibile che nella tabella visualizzata vengano mostrati degli elenchi URL. Scegliere **Seleziona** se per il criterio si desidera utilizzare uno degli elenchi URL visualizzati.

Per creare un nuovo elenco, fare clic su **Aggiungi** e inserire le informazioni richieste nella finestra di dialogo visualizzata. Utilizzare i tasti **Modifica** ed **Elimina** per modificare o rimuovere gli elenchi URL presenti nella tabella.

Aggiungi o Modifica URL

In questa finestra è possibile aggiungere o modificare le informazioni per un collegamento VPN SSL Cisco IOS.

Etichetta

L'etichetta appare nel portale visualizzata al momento dell'accesso alla VPN SSL Cisco IOS. Ad esempio, è possibile utilizzare l'etichetta del calendario della contabilità del personale per la creazione di un collegamento al calendario di riepilogo dei giorni di paga e ferie retribuite.

Collegamento URL

Inserire o modificare l'URL del sito Web intranet aziendale per il quale si desidera consentire l'accesso agli utenti.

Personalizza portale VPN SSL

L'aspetto del portale dipende dalle impostazioni specificate in esso. È possibile scegliere tra i temi predefiniti elencati e ottenere un'anteprima dell'aspetto del portale con l'utilizzo di tali temi.

Tema

Selezionare il nome di un tema predefinito.

Anteprima

In quest'area viene mostrato come appare il portale a seconda del tema selezionato. È possibile visualizzare le anteprime di diversi temi, per stabilire quale utilizzare.

Configurazione pass-through di VPN SSL

Affinché gli utenti possano connettersi all'intranet, è necessario aggiungere le voci ACE (Access Control Entry) alle configurazioni di firewall e NAC (Network Access Control), per consentire al traffico SSL di raggiungere l'intranet. Cisco SDM è in grado di configurare le voci ACE in questione o può farlo l'utente selezionando **Firewall e ACL > Modifica ACL/Criterio firewall** e apportando le modifiche richieste.

Se si sta utilizzando la procedura guidata VPN SSL Cisco IOS, fare clic su **Consenti l'utilizzo di VPN SSL con NAC e firewall** se si desidera configurare tali ACE in Cisco SDM. Fare clic su **Visualizza dettagli** per visualizzare le voci ACE che saranno create automaticamente in Cisco SDM. Di seguito è indicato un esempio di una delle possibili voci create tramite Cisco SDM:

```
permit tcp any host 172.16.5.5 eq 443
```

Durante la modifica di un contesto VPN SSL Cisco IOS, Cisco SDM visualizza le interfacce interessate e le rispettive voci ACL applicate. Fare clic su **Modifica** per permettere a Cisco SDM di aggiungere le voci all'ACL, in modo da consentire il passaggio del traffico SSL attraverso il firewall. Fare clic su **Dettagli** per visualizzare la voce aggiunta da Cisco SDM. La voce sarà simile a quella sopra indicata.

Criterio utente

Questa finestra consente di scegliere una VPN SSL Cisco IOS esistente e aggiungervi un nuovo criterio. Ad esempio, si potrebbe creare una VPN SSL Cisco IOS come Aziendale e definire l'accesso intranet per un nuovo gruppo di utenti denominato Ufficio tecnico.

Seleziona VPN SSL esistente

Scegliere la VPN SSL Cisco IOS per il quale si desidera creare un nuovo gruppo di utenti. I criteri precedentemente configurati per quella VPN SSL Cisco IOS sono visualizzati in una casella sotto l'elenco. È possibile fare clic su uno di questi criteri per visualizzarne i dettagli. Per maggiori informazioni vedere la sezione Dettagli del criterio di gruppo VPN SSL: Nome criterio.

Nome del nuovo criterio

Immettere il nome che si desidera attribuire al nuovo gruppo di utenti. Nell'area sotto questo campo sono elencati i criteri di gruppo già esistenti per questa VPN SSL Cisco IOS.

Dettagli del criterio di gruppo VPN SSL: Nome criterio

In questa finestra sono visualizzati i dettagli di un criterio VPN SSL Cisco IOS esistente.

Servizi

In quest'area sono elencati i servizi per i quali il criterio è configurato, ad esempio la manipolazione dell'URL e Cisco Secure Desktop.

URL esposti agli utenti

In quest'area sono elencati gli URL intranet esposti agli utenti governati da questo criterio.

Server esposti agli utenti

In quest'area vengono visualizzati gli indirizzi IP dei server per inoltro su porta utilizzati dal criterio configurato.

Server WINS

In quest'area vengono visualizzati gli indirizzi IP dei server WINS utilizzati dal criterio configurato.

Seleziona gruppo utente VPN SSL

Scegliere in questa finestra la VPN SSL Cisco IOS e il gruppo utente associato per i quali si desidera configurare i servizi avanzati.

SSL VPN

Scegliere la VPN SSL Cisco IOS a cui il gruppo utente è associato da questo elenco.

Gruppo utenti

Scegliere il gruppo utente per il quale si desidera configurare le funzionalità avanzate. Il contenuto dell'elenco è basato sulla VPN SSL Cisco IOS scelta.

Seleziona funzionalità avanzate

Scegliere in questa finestra le funzionalità che si desidera configurare. Nella procedura guidata vengono visualizzate le finestre che consentono di configurare le funzionalità scelte.

Ad esempio, facendo clic su Thin client (inoltro su porta), Cisco Secure Desktop e Common Internet File System (CIFS), saranno visualizzate le relative finestre di configurazione.

È necessario selezionare almeno una funzionalità da configurare.

Thin client (inoltro su porta)

A volte, per comunicare con i server intranet, è indispensabile che le workstation eseguano le applicazioni client. Ad esempio i server IMAP (Internet Mail Access Protocol) o SMPT (Simple Mail Transfer Protocol) possono richiedere l'esecuzione di applicazioni client da parte delle workstation per inviare o ricevere i messaggi di posta elettronica. La funzionalità thin client, conosciuta anche come inoltro su porta, consente di eseguire il download di un'applet di piccole dimensioni insieme al portale, in modo che la workstation remota sia messa in comunicazione con il server intranet.

Nella finestra vengono elencati i server e i numeri di porta configurati per la rete intranet. Utilizzare il pulsante **Aggiungi** per aggiungere un indirizzo IP del server e il numero di porta. Utilizzare i pulsanti **Modifica** ed **Elimina** per apportare delle modifiche alle informazioni nell'elenco e rimuovere i dati relativi a un server.

L'elenco creato viene visualizzato nel portale al momento dell'accesso dei client.

Aggiunta o modifica di un server

In questa finestra è possibile aggiungere o modificare le informazioni relative a un server.

Indirizzo IP del server

Immettere l'indirizzo IP o il nome host del server.

Porta del server in cui il servizio è in ascolto

Immettere la porta su cui il server è in ascolto per questo servizio. Il numero di porta può essere prestabilito a seconda del servizio, ad esempio il numero standard per Telnet è 23. In alternativa è possibile specificare un numero di porta non standard, per cui sia stata creata una mappa porte-applicazioni (PAM, Port-to-Application Map). Ad esempio, avendo stabilito 2323 come numero di porta non standard per Telnet e dopo aver creato una voce PAM per quella porta sul server in questione, è possibile immettere 2323 in questa finestra.

Porta sul PC client

Cisco SDM immette un numero in questo campo, a partire da 3000. All'aggiunta di una nuova voce, Cisco SDM aumenta il numero di una cifra. Utilizzare le voci che Cisco SDM ha inserito in questo campo.

Descrizione

Inserire una descrizione della voce. Ad esempio, se si aggiunge una voce che consente agli utenti di stabilire una connessione telnet con un server all'indirizzo 10.10.11.2, è possibile inserire “Connessione Telnet con 10.10.11.2”. La descrizione inserita viene visualizzata nel portale.

Ulteriori informazioni

Per maggiori informazioni, consultare il collegamento. È possibile visualizzare subito le informazioni facendo clic su Maggiori informazioni sui server per l'inoltro su porta.

Maggiori informazioni sui server per l'inoltro su porta

L'inoltro su porta consente agli utenti remoti VPN SSL Cisco IOS di connettersi alle porte statiche sui server tramite indirizzi IP privati sulla rete intranet aziendale. Ad esempio, è possibile configurare l'inoltro su porta su un router per consentire agli utenti remoti l'accesso via Telnet a un server sulla rete intranet aziendale. Per la configurazione dell'inoltro su porta sono necessarie le seguenti informazioni:

- L'indirizzo IP del server.
- Il numero di porta statico sul server.
- Il numero di porta remota per il PC client. Nella finestra di dialogo, Cisco SDM consente di fornire un numero di porta protetto per l'utilizzo.

Per consentire agli utenti di utilizzare Telnet per connettersi a un server con l'indirizzo IP 10.0.0.100 (numero di porta 23), ad esempio, è necessario creare una voce di mappatura delle porte con le seguenti informazioni:

Indirizzo IP del server: 10.0.0.100

Porta del server alla quale si connette l'utente: 23

Porta sul PC client: Valore fornito in Cisco SDM. 3001 per questo esempio.

Descrizione: Accesso Telnet VPN SSL al server a. Questa descrizione sarà inserita nel portale.

Quando il browser del client si connette al router del gateway, viene eseguito il download dell'applet del portale sul PC client. In questa applet è contenuto l'indirizzo IP e il numero di porta statico del server e il numero di porta utilizzato dal PC client. L'applet consente le seguenti operazioni:

- Creazione di una mappatura sul PC client relativa al traffico della porta 23 in 10.0.0.100 all'indirizzo IP loopback del PC 127.0.0.1, porta 3001.
- Ascolto sulla porta 3001, indirizzo IP 127.0.0.1

Quando si esegue un'applicazione che consente la connessione alla porta 23 in 10.0.0.100, la richiesta viene inviata alla porta 3001 dell'indirizzo 127.0.0.1. L'applet del portale, in ascolto su quella porta e a quell'indirizzo IP, acquisisce la richiesta e la invia attraverso il tunnel VPN SSL Cisco IOS al gateway. Il router del gateway la inoltra al server all'indirizzo 10.0.0.100 e rimanda il traffico di ritorno al PC.

Full tunnel

I client per il full tunnel devono eseguire il download del software per il full tunnel e ottenere un indirizzo IP dal router. L'utilizzo di questa finestra consente di configurare il pool di indirizzi IP che i client per il full tunnel otterranno al momento dell'accesso e consente di specificare il percorso del bundle di installazione per il full tunnel.

Nota Se il bundle di installazione del software non è già installato, la memoria flash del router presente deve essere sufficiente per l'installazione da parte di Cisco SDM al termine della procedura guidata.

Casella di controllo Attiva full tunnel

Selezionare questa casella di controllo per consentire al router di eseguire il download del software del client per il full tunnel nel PC dell'utente e di rendere attivi gli altri campi in questa finestra.

Pool di indirizzi IP

Specificare il pool di indirizzi IP che sarà ottenuto dai client per il full tunnel. Nel campo è possibile immettere il nome di un pool esistente oppure è possibile fare clic sul pulsante a destra del campo e scegliere **Seleziona un pool di IP esistente** per ricercare nell'elenco dei pool. Per creare un nuovo pool, scegliere **Crea un nuovo pool IP** e completare la finestra di dialogo visualizzata. Il pool di indirizzi scelto o creato deve contenere gli indirizzi nell'intranet aziendale.

Casella di controllo Mantenere installato il software del client per il full tunnel sul PC del client

Selezionare questa casella di controllo se si desidera mantenere il software per il full tunnel sul PC del client dopo la disconnessione. Se la casella di controllo non viene selezionata, i client eseguiranno il download del software tutte le volte che verrà stabilita una comunicazione con il gateway.

Casella di controllo Installa client per il full tunnel

Selezionare questa casella di controllo per consentire di installare il software del client per il full tunnel in questa fase. È possibile installare anche il software del client quando si modifica VPN SSL Cisco IOS.

Il software del client per il full tunnel deve essere installato sul router per consentire ai client di eseguire il download e stabilire una connettività di tipo full tunnel. Se il software per il full tunnel è stato installato con Cisco SDM, il percorso viene visualizzato automaticamente nel campo Percorso, come illustrato in Esempio 19-1.

Esempio 19-1 Pacchetto per il full tunnel installato su router

```
flash:sslclient-win-1.0.2.127.pkg
```

In Esempio 19-1, il bundle di installazione per il full tunnel viene caricato nella memoria flash del router. Se il dispositivo principale del router è un disco o uno slot, il percorso visualizzato inizierà con `diskn` o `slotn`.

Se il campo è vuoto, è necessario individuare il bundle di installazione per consentire a Cisco SDM di caricarlo sul dispositivo principale del router oppure eseguire il download del bundle di installazione del software da Cisco.com facendo clic sul collegamento Eseguire il download dell'ultimo..., nella parte inferiore della finestra. Attraverso questo collegamento viene visualizzata la seguente pagina Web:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Nota Per acquisire il software dai siti di download dei software di Cisco, potrebbero essere necessari un nome utente e una password CCO. Per ottenere queste credenziali, fare clic su **Registra** nella parte superiore di qualsiasi pagina Web di Cisco.com e fornire le informazioni richieste. L'ID utente e la password verranno inviati tramite posta elettronica.

Per informazioni sull'individuazione del bundle di installazione del software per il full tunnel, fare clic su Individuazione del bundle di installazione per Cisco SDM e fornire un percorso da utilizzare per Cisco SDM.

Pulsante Avanzate

Fare clic su questo pulsante per configurare le opzioni avanzate, quali la suddivisione tunnel, lo split DNS e le impostazioni Microsoft Internet Explorer dei client.

Individuazione del bundle di installazione per Cisco SDM

La procedura riportata di seguito consente di individuare i bundle di installazione del software per Cisco SDM per utilizzare quel percorso nella configurazione di Cisco IOS SSL VPN oppure, se necessario, caricare il software sul router.

Nota Per acquisire il software dai siti di download dei software di Cisco, potrebbero essere necessari un nome utente e una password CCO. Per ottenere queste credenziali, fare clic su **Registra** nella parte superiore di qualsiasi pagina Web di Cisco.com e fornire le informazioni richieste. L'ID utente e la password verranno inviati tramite posta elettronica.

Passo 1 Controllare il campo **Percorso**. Se il percorso del bundle di installazione è indicato in quel campo, non saranno necessarie altre operazioni. Cisco SDM configura il router per il download del software da quel percorso. In Esempio 19-2 viene visualizzato un percorso relativo a un bundle di installazione del software.

Esempio 19-2 Pacchetto per il full tunnel installato su router

```
flash:sslclient-win-1.0.2.127.pkg
```

Passo 2 Se il campo Percorso è vuoto, fare clic sul pulsante **...**, a destra del campo, per specificare il percorso del software.

Passo 3 Se il software è installato sul router, scegliere **File system del router** e ricercare il file.

Se il software è installato nel PC, scegliere **Risorse del computer** e ricercare il file.

Cisco SDM consente di collocare il file system del router o il percorso del PC specificato nel campo Percorso.

Passo 4 Se il software non è installato nel router o nel PC, è necessario eseguire il download sul PC e quindi fornire il percorso per il file in questo campo.

a. Fare clic sul collegamento Eseguire il download dell'ultimo... nella finestra. Viene effettuata la connessione alla pagina di download relativa al software desiderato.

b. Nella pagina Web visualizzata, potrebbero essere disponibili pacchetti software per piattaforme Cisco IOS e altre piattaforme. Fare doppio clic sulla versione più recente del software per piattaforme Cisco IOS di cui eseguire il download e fornire il nome utente e la password CCO quando vengono richiesti.

c. Eseguire il download del pacchetto sul PC.

d. Nella procedura guidata VPN SSL Cisco IOS, fare clic sul pulsante **...** a destra del campo Percorso, scegliere **Risorse del computer** nella finestra di selezione del percorso visualizzata; e spostarsi alla directory nella quale è stato posizionato il file.

e. Selezionare il file del bundle di installazione e fare clic su **OK** nella finestra di selezione del percorso. Cisco SDM colloca il percorso nel campo Percorso. Negli esempi viene illustrato un bundle di installazione presente sul desktop del PC.

Esempio 19-3 Pacchetto per il full tunnel installato su router

```
C:\Documents and Settings\nome
utente\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco SDM consente l'installazione del software sul router dalla directory del PC specificata quando si inoltra la configurazione al router facendo clic su **Fine**.

Attiva Cisco Secure Desktop

Il router consente di installare Cisco Secure Desktop sul PC quando l'utente accede a VPN SSL Cisco IOS. Le transazioni Web possono creare sul PC cookie, file di cronologia del browser, allegati e-mail e altri file dopo la disconnessione. Cisco Secure Desktop crea una partizione protetta sul desktop e utilizza un algoritmo del Department of Defense per rimuovere i file al termine della sessione.

Installare Cisco Secure Desktop

I client devono eseguire il download del bundle di installazione del software Cisco Secure Desktop dal router. Se il software è stato installato con Cisco SDM, il percorso viene visualizzato automaticamente nel campo **Percorso**, come illustrato in Esempio 19-4.

Esempio 19-4 Pacchetto Cisco Secure Desktop installato su router

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

In Esempio 19-4, il bundle di installazione di Cisco Secure Desktop viene caricato nella memoria flash del router. Se il dispositivo principale del router è un disco o uno slot, il percorso visualizzato inizierà con `diskn` o `slotn`.

Se il campo è vuoto, è necessario individuare il bundle di installazione per consentire a Cisco SDM di caricarlo sul dispositivo principale del router oppure eseguire il download del bundle di installazione del software da Cisco.com facendo clic sul collegamento **Eseguire il download dell'ultimo...** nella parte inferiore della finestra. Il collegamento conduce alla seguente pagina Web:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Nota Per acquisire il software dai siti di download dei software di Cisco, potrebbero essere necessari un nome utente e una password CCO. Per ottenere queste credenziali, fare clic su **Registra** nella parte superiore di qualsiasi pagina Web di Cisco.com e fornire le informazioni richieste. L'ID utente e la password verranno inviati tramite posta elettronica.

Per informazioni sull'individuazione del bundle di installazione del software Cisco Secure Desktop, fare clic su Individuazione del bundle di installazione per Cisco SDM e fornire un percorso utilizzato da Cisco Cisco SDM.

Common Internet File System

Il sistema CIFS (Common Internet File System) consente ai client di ricercare, accedere e creare file, in modalità remota, su file server basati su Microsoft Windows utilizzando un'interfaccia del browser Web.

Server WINS

I server WINS (Windows Internet Naming Service) di Microsoft gestiscono il database in cui vengono mappati gli indirizzi IP del client ai corrispondenti nomi NetBIOS. Immettere gli indirizzi IP dei server WINS nella rete in questa casella. Utilizzare i punti e virgola (;) per separare gli indirizzi.

Ad esempio, per immettere gli indirizzi IP 10.0.0.18 e 10.10.10.2, è necessario immettere 10.0.0.18;10.10.10.2 in questa casella.

Autorizzazioni

Specificare le autorizzazioni da concedere agli utenti.

Attiva Citrix senza client

Citrix senza client consente agli utenti di eseguire applicazioni, quali Microsoft Word o Excel, su server remoti allo stesso modo in cui vengono eseguiti su server locali, senza software client sul PC. Il software Citrix deve essere installato su uno o più server in una rete raggiungibile dal router.

Server Citrix

Per creare un nuovo elenco, fare clic su **Aggiungi** e inserire le informazioni richieste nella finestra di dialogo visualizzata. Utilizzare i tasti **Modifica** ed **Elimina** per modificare o rimuovere gli elenchi URL presenti nella tabella.

Riepilogo

Questa finestra visualizza un riepilogo della configurazione VPN SSL Cisco IOS creata. Fare clic su **Fine** per trasferire la configurazione sul router oppure fare clic su **Indietro** per tornare a una finestra della procedura guidata e apportare le modifiche desiderate.

Per visualizzare i comandi CLI da inoltrare al router, passare a **Modifica > Preferenze** e selezionare **Eseguire l'anteprima dei comandi prima dell'inoltro al router.**

Modifica VPN SSL

La finestra Modifica VPN SSL consente di modificare o di creare configurazioni di Cisco IOS SSL VPN. Nella parte superiore della scheda vengono elencati i contesti Cisco IOS SSL VPN configurati. Nella parte inferiore vengono visualizzati i dettagli relativi a quel contesto.

Fare clic su Cisco IOS SSL VPN per l'anteprima delle funzioni Cisco IOS SSL VPN supportate da Cisco SDM.

Per i collegamenti ai documenti Cisco IOS SSL VPN, fare clic su Collegamenti Cisco IOS SSL VPN sul sito Web di Cisco.

Fare clic su Contesti Cisco IOS SSL VPN, gateway e criteri per la descrizione dell'interazione dei componenti di una configurazione Cisco IOS SSL VPN.

Contesti VPN SSL

In quest'area vengono visualizzati i contesti Cisco IOS SSL VPN configurati sul router. Selezionare un contesto in quest'area per visualizzarne le informazioni nella parte inferiore della finestra. Per aggiungere un nuovo contesto, fare clic su **Aggiungi** e immettere le informazioni nella finestra di dialogo visualizzata. Per modificare un contesto, selezionarlo e fare clic su **Modifica**. Per rimuovere un contesto e i criteri di gruppo associati, selezionarlo e fare clic su **Elimina**.

È possibile attivare un contesto non in servizio selezionandolo e facendo clic su **Attiva**. Per rendere un contesto fuori servizio, selezionarlo e fare clic su **Disattiva**.

Le informazioni riportate di seguito vengono visualizzate per ciascun contesto.

Nome

Nome del contesto Cisco IOS SSL VPN. Se il contesto è stato creato nella procedura guidata Cisco IOS SSL VPN, il nome è la stringa immessa nella finestra Nome e indirizzo IP.

Gateway

Nel gateway utilizzato dal contesto è contenuto l'indirizzo IP e il certificato digitale che verrà utilizzato dal contesto Cisco IOS SSL VPN.

Dominio

Se è stato configurato un dominio per il contesto, verrà visualizzato in questa colonna. Se viene configurato un dominio, sarà necessario immettere quel dominio nel browser Web per accedere al portale.

Stato

Sono contenute icone per l'identificazione veloce dello stato.

Stato amministrativo

Descrizione testuale dello stato.

- In Servizio: contesto in servizio. Gli utenti specificati nei criteri configurati nel contesto possono accedere al relativo portale Cisco IOS SSL VPN.
- Non in servizio: contesto non in servizio. Gli utenti specificati nei criteri configurati nel contesto non possono accedere al relativo portale Cisco IOS SSL VPN.

Esempio di visualizzazione

Nella tabella riportata di seguito viene illustrato un esempio di visualizzazione dei contesti Cisco IOS SSL VPN.

Nome	Gateway	Dominio	Stato	Stato amministrativo
WorldTravel	Gateway1	wtravel.net		In servizio
A+Insurance	Gateway2	aplus.com		Non in servizio

Dettagli sul contesto VPN SSL: *Nome*

In quest'area vengono visualizzati i dettagli relativi al contesto con il nome *nome* selezionato nella parte superiore della finestra. È possibile modificare le impostazioni visualizzate facendo clic su **Modifica** nella parte superiore della finestra.

Contesto VPN SSL

Questa finestra consente di aggiungere o modificare un contesto Cisco IOS SSL VPN.

Nome

Immettere il nome di un nuovo contesto oppure scegliere il nome di un contesto esistente per modificarlo.

Gateway associato

Per configurare un nuovo gateway per il contesto, selezionare un gateway esistente oppure fare clic su **Crea gateway**. Nel gateway è contenuto l'indirizzo IP e il certificato digitale utilizzati per questo contesto. Per ciascun gateway è richiesto un indirizzo IP pubblico univoco.

Dominio

Se si dispone di un dominio per il contesto, immetterlo in questo campo. Gli utenti Cisco IOS SSL VPN potranno utilizzare il nome di questo dominio nell'accesso al portale, invece di un indirizzo IP. Un esempio è azienda.com.

Elenco di autenticazione

Per autenticare gli utenti per questo contesto, scegliere l'elenco metodi AAA.

Dominio di autenticazione

Immettere il nome di dominio da aggiungere al nome utente prima dell'invio per l'autenticazione. Questo dominio deve corrispondere al dominio utilizzato nel server AAA per gli utenti che verranno autenticati per questo contesto.

Casella di controllo Attiva contesto

Selezionare questa casella di controllo se si desidera che il contesto sia attivo al termine della configurazione. Non è necessario ritornare a questa finestra per disattivare il contesto attivato. È possibile attivare e disattivare singoli contesti nella scheda Modifica VPN SSL.

Numero massimo di utenti

Immettere il numero massimo di utenti a cui è consentito utilizzare questo contesto contemporaneamente.

Nome VRF

Immettere il nome VRF (Routing and Forwarding) VPN per questo contesto. Il nome VRF deve essere già stato configurato sul router.

Criterio di gruppo predefinito

Selezionare il criterio che si desidera utilizzare come criterio di gruppo predefinito. Il criterio di gruppo predefinito verrà utilizzato per gli utenti non inclusi negli altri criteri configurati sul server AAA.

Designa interfacce interne ed esterne

Un'ACL applicata a un'interfaccia su cui è configurata una connessione Cisco IOS SSL VPN può bloccare il traffico SSL. Cisco SDM può modificare automaticamente l'ACL in modo da consentire il passaggio di questo tipo di traffico attraverso il firewall. Tuttavia, è necessario indicare quale interfaccia è l'interfaccia interna (trusted) e quale invece quella esterna (untrusted) per la creazione in Cisco SDM della voce ACE (Access Control Entry) che consentirà al traffico appropriato di attraversare il firewall.

Se l'interfaccia elencata è trusted, selezionare **Interna**, in caso contrario selezionare **Esterna**.

Seleziona un gateway

Questa finestra consente di selezionare un gateway esistente. Questa finestra fornisce le informazioni necessarie per determinare il gateway da selezionare. In essa vengono visualizzati i nomi e gli indirizzi IP di tutti i gateway, il numero di contesti associati a ciascuno e se il gateway è attivo o meno.

Contesto: Criteri di gruppo

In questa finestra vengono visualizzati i criteri di gruppo configurati per il contesto Cisco IOS SSL VPN scelto. Per gestire questi criteri di gruppo, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

Per ciascun criterio, in questa finestra viene indicato il nome del criterio e se tale criterio è il criterio di gruppo predefinito ovvero il criterio assegnato a un utente non incluso in altri criteri. È possibile cambiare il criterio di gruppo ritornando alla finestra Contesto e selezionando un criterio differente come quello predefinito.

Fare clic su un criterio nell'elenco per visualizzare i dettagli sul criterio nella parte inferiore della finestra. Per una descrizione di questi dettagli, fare clic sui collegamenti riportati di seguito

Criterio di gruppo: scheda Generale

Criterio di gruppo: scheda Senza client

Criterio di gruppo: scheda Thin client

Criterio di gruppo: scheda Client VPN SSL (full tunnel)

Fare clic qui per ulteriori informazioni

Per informazioni importanti, fare clic sul collegamento nella finestra. Per acquisire tali informazioni da questa pagina della Guida, fare clic su Maggiori informazioni sui criteri di gruppo.

Maggiori informazioni sui criteri di gruppo

I criteri di gruppo Cisco IOS SSL VPN consentono di definire il portale e i collegamenti per gli utenti inclusi nei criteri. Quando un utente remoto immette l'URL Cisco IOS SSL VPN fornito, il router deve determinare il criterio di appartenenza dell'utente in modo da visualizzare il portale configurato per quel criterio. Se sul router è configurato soltanto un criterio Cisco IOS SSL VPN, l'autenticazione degli utenti avverrà a livello locale oppure utilizzando un server AAA e successivamente verrà visualizzato il portale.

Tuttavia, se sono configurati più criteri, il router deve affidarsi a un server AAA per determinare il criterio da utilizzare ogni volta che un utente remoto tenta di accedere. Se sono stati configurati più criteri di gruppo Cisco IOS SSL VPN, è necessario configurare almeno un server AAA per il router ed è necessario configurare un criterio su quel server per ciascun gruppo di utenti per il quale è stato creato un criterio Cisco IOS SSL VPN I nomi dei criteri nel server AAA devono essere uguali ai nomi dei criteri di gruppo configurati sul router e devono essere configurati con le credenziali degli utenti membri del gruppo.

Ad esempio, se un router è stato configurato con autenticazione locale per Bob Smith ed è stato configurato soltanto il criterio di gruppo Vendite, sarà visualizzabile solo un portale quando l'utente Bob Smith tenta di effettuare l'accesso. Tuttavia, se sono presenti tre criteri di gruppo Cisco IOS SSL VPN configurati, ovvero Vendite, Campo e Produzione, il router non sarà in grado di determinare autonomamente il criterio di gruppo di cui è membro Bob Smith. Se un server AAA è configurato con le informazioni appropriate per quei criteri, il router può contattare quel server e ricevere le informazioni sull'appartenenza di Bob Smith al gruppo Vendite. Successivamente il router visualizzerà il portale corrispondente al gruppo Vendite.

Per informazioni sulla configurazione del server AAA, consultare la sezione “Configuring RADIUS Attribute Support for SSL VPN” nel documento *SSL VPN Enhancements* nel seguente collegamento:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Criterio di gruppo: scheda Generale

Nella creazione di un nuovo criterio di gruppo, è necessario immettere le informazioni in ciascun campo della scheda Generale.

Nome

Immettere un nome per il criterio di gruppo, ad esempio Ufficio tecnico, Risorse umane o Marketing.

Timeout

Timeout idle: immettere il numero di secondi in cui il client può restare inattivo prima del termine della sessione.

Timeout sessione: immettere il numero massimo di secondi per sessione, indipendentemente dall'attività nella sessione.

Casella di controllo Rendere questo criterio di gruppo predefinito per il contesto

Selezionare questa casella di controllo se si desidera impostare questo criterio di gruppo come predefinito, ovvero il criterio assegnato a un utente non incluso in altri criteri. Se si seleziona questa casella di controllo, questo criterio verrà visualizzato come criterio predefinito nella finestra Criterio di gruppo.

Criterio di gruppo: scheda Senza client

Citrix senza client consente agli utenti di eseguire applicazioni su server remoti così come avviene con i server locali, senza dover installare il software client su sistemi remoti che utilizzano queste applicazioni. Il software Citrix deve essere installato su uno o più server in una rete raggiungibile dal router.

Immettere le informazioni desiderate per consentire ai client Cisco IOS SSL VPN di utilizzare Citrix senza client.

Ricerca sul Web senza client

Selezionare uno o più elenchi URL da visualizzare nel portale che verrà visualizzato dagli utenti di questo gruppo. Se si desidera analizzare un elenco URL, scegliere un nome dall'elenco e fare clic su **Visualizza**. Gli URL presenti nell'elenco specificato verranno visualizzati nel portale.

Se si desidera limitare gli utenti per gli URL presenti nell'elenco ed evitare che questi immettano altri URL, fare clic su **Nascondi barra degli URL nella pagina del portale**.

Attiva CIFS

Scegliere questa opzione se si desidera consentire ai membri del gruppo di ricercare i file sui server MS Windows nella rete aziendale. È necessario specificare l'elenco dei server WINS che consentirà la visualizzazione dei file appropriati a questi utenti. Per verificare il contenuto di un elenco di server WINS, scegliere l'elenco e fare clic su **Visualizza**.

Per consentire ai membri del gruppo di leggere i file, fare clic su **Lettura**. Per consentire ai membri del gruppo di modificare i file, fare clic su **Scrittura**.

Per rendere disponibile questa funzionalità, configurare almeno un elenco di server WINS per questo contesto Cisco IOS SSL VPN.

Criterio di gruppo: scheda Thin client

Per configurare Thin client, indicato anche come inoltro su porta, per i membri di questo gruppo, definire le impostazioni nella scheda.

Per attivare questa funzionalità, fare clic su **Attiva thin client** (**inoltro su porta**) e specificare un elenco di inoltri su porta. È necessario configurare almeno un elenco di inoltri su porta per il contesto Cisco IOS SSL VPN nel quale è configurato questo criterio di gruppo. Per esaminare l'elenco di inoltri su porta scelto, fare clic su **Visualizza**.

Criterio di gruppo: scheda Client VPN SSL (full tunnel)

Per consentire ai membri del gruppo di eseguire il download e utilizzare il software client per il full tunnel, definire le impostazioni nella scheda.

Nota È necessario specificare il percorso del software del client per il full tunnel facendo clic su **Pacchetti** nella struttura SSL VPN, specificando il percorso del bundle di installazione e selezionando **Installa**.

Attivare le connessioni full tunnel selezionando **Attiva** dall'elenco. Se si desidera richiedere le connessioni full tunnel, selezionare **Richiesto**. Se si seleziona **Richiesto**, le comunicazioni senza client e thin client funzioneranno soltanto se il software client Cisco IOS SSL VPN è stato installato correttamente sul PC client.

Pool di indirizzi IP dal quale verrà assegnato l'indirizzo IP ai client

Ai client che stabiliscono una comunicazione full tunnel viene assegnato un indirizzo IP mediante il router. Specificare il nome del pool oppure fare clic sul pulsante **...** per creare un nuovo pool dal quale il router può assegnare gli indirizzi.

Casella di controllo Mantenere installato il software del client per il full tunnel sul PC del client

Selezionare questa casella di controllo se si desidera mantenere il software per il full tunnel sul PC del client dopo la disconnessione. Se la casella di controllo non viene selezionata, i client eseguiranno il download del software tutte le volte che verrà stabilita una comunicazione con il gateway.

Campo Tasto di rinegoziazione

Immettere il numero di secondi dopo il quale il tunnel deve essere arrestato in modo che possa essere negoziata una nuova chiave SSL e ristabilito il tunnel.

ACL per limitare l'accesso degli utenti di questo gruppo alle risorse aziendali

È possibile scegliere o creare un'ACL che specifichi le risorse nella rete aziendale che verranno limitate ai membri del gruppo.

Il client della pagina principale deve riconoscere quando un browser Web viene aperto con il software per il full tunnel installato

Immettere l'URL della pagina principale da visualizzare ai client per il full tunnel di questo gruppo.

Timeout DPD (Dead Peer Detection)

Il DPD (Dead Peer Detection) consente a un sistema di rilevare un peer che non risponde. È possibile impostare timeout separati che possono essere utilizzati dal router per rilevare i client e i server che non rispondono. Per entrambi, l'intervallo è compreso tra 0 e 3600 secondi.

Pulsante Configura server DNS e WINS

Fare clic su questo pulsante per visualizzare la finestra di dialogo Server DNS e WINS, che consente di fornire gli indirizzi IP dei server DNS e WINS nel sito intranet aziendale utilizzato dai client per l'accesso agli host e ai servizi intranet.

Pulsante Configura opzioni tunnel avanzate

Fare clic su questo pulsante per visualizzare la finestra di dialogo Opzioni tunnel avanzate che consente di configurare le impostazioni di tunnel per la gestione dello split tunnel, lo split DNS e le impostazioni del server proxy per i client che utilizzano Microsoft Internet Explorer.

Opzioni tunnel avanzate

Le impostazioni configurate in questa finestra di dialogo consentono di controllare il traffico crittografato, di specificare i server DNS nell'intranet aziendale e di specificare le impostazioni del server proxy da inviare ai browser dei client.

Suddivisione tunnel

La crittografia di tutto il traffico del tunnel potrebbe richiedere un numero eccessivo di risorse di sistema. La suddivisione tunnel consente di specificare le reti con traffico da crittografare e di esentare dalla crittografia il traffico verso altre reti. È possibile specificare il traffico di tunnel da crittografare oppure specificare il traffico che *non* deve essere crittografato e consentire al router di crittografare ogni altro tipo di traffico di tunnel. È possibile creare soltanto un elenco; il traffico incluso e quello escluso si escludono a vicenda.

Fare clic su **Includi traffico** e utilizzare i tasti **Aggiungi**, **Modifica** ed **Elimina** per creare un elenco di reti di destinazione con traffico da crittografare. Oppure fare clic su **Escludi traffico** e creare un elenco delle reti di destinazione il cui traffico *non* deve essere crittografato.

Fare clic su **Escludi LAN locali** per escludere in modo esplicito dalla crittografia il traffico di client destinato alle LAN a cui è connesso il router. In caso di stampanti in rete in queste LAN, è necessario utilizzare questa opzione.

Maggiori informazioni sulla suddivisione tunnel.

Split DNS

Se si desidera che i client Cisco IOS SSL VPN utilizzino il server DNS nella rete aziendale soltanto per risolvere domini specifici, è possibile immettere tali domini in quest'area. Tali domini devono essere all'interno dell'intranet aziendale. Separare ciascuna voce con un punto e virgola e non utilizzare i ritorni a capo. Di seguito è riportato un elenco di esempi di voci:

azienda.com;dev-lab.net;extranet.net

I client devono utilizzare i server DNS forniti dai relativi ISP per risolvere tutti gli altri domini.

Impostazioni Proxy Browser

Le impostazioni presenti in quest'area sono inviate ai browser Microsoft Internet Explorer dei client con le connessioni per il full tunnel. Queste impostazioni non avranno alcun effetto se i client utilizzano un browser differente.

Non utilizzare proxy server

Selezionare per indicare ai browser dei client Cisco IOS SSL VPN di non utilizzare un server proxy.

Rileva automaticamente impostazioni proxy

Selezionare se si desidera che nei browser dei client Cisco IOS SSL VPN sia effettuata la rilevazione automatica delle impostazioni dei server proxy.

Bypass delle impostazioni proxy per gli indirizzi locali

Selezionare per collegare i client a indirizzi locali in grado di ignorare le impostazioni proxy normali.

Server proxy

Immettere l'indirizzo IP del server proxy e il numero di porta per il servizio fornito in questi campi. Ad esempio, se il server proxy supporta le richieste FTP, immettere l'indirizzo IP del server proxy e il numero di porta 21.

Non usare un server proxy per gli indirizzi che iniziano con

Per evitare che i client utilizzino server proxy durante l'invio di traffico a reti o indirizzi IP specifici, è possibile inserirli in questo campo. Per separare ciascuna voce, utilizzare il punto e virgola. Ad esempio, se non si desidera che i client utilizzino un server proxy nel corso della connessione di un server alle reti 10.10.0.0 o 10.11.0.0, immettere 10.10;10.11. È possibile immettere un numero qualsiasi di reti.

Server DNS e WINS

Immettere gli indirizzi IP dei server DNS e WINS aziendali che verranno inviati ai client Cisco IOS SSL VPN. I client Cisco IOS SSL VPN utilizzeranno tali server per accedere agli host e ai servizi della intranet aziendale.

Fornire gli indirizzi per i server DNS primario e secondario e i server WINS.

Maggiori informazioni sulla suddivisione tunnel

Quando una connessione Cisco IOS SSL VPN viene configurata con un client remoto, tutto il traffico inviato e ricevuto dal client può attraversare il tunnel Cisco IOS SSL VPN, incluso il traffico che non fa parte dell'intranet aziendale. In questo modo le prestazioni della rete si riducono. La suddivisione tunnel consente di specificare il traffico per il tunnel Cisco IOS SSL VPN, mentre tutti gli altri tipi di traffico possono restare senza protezione ed essere gestiti da altri router.

Nell'area suddivisione tunnel è possibile specificare il traffico da *includere* in Cisco IOS SSL VPN ed escludere in modo predefinito il resto del traffico oppure è possibile specificare il traffico da *escludere* da Cisco IOS SSL VPN e includere in modo predefinito il resto del traffico.

Ad esempio, se l'organizzazione utilizza gli indirizzi di rete 10.11.55.0 e 10.12.55.0, aggiungere questi indirizzi di rete all'elenco delle reti di destinazione e fare clic sul pulsante di scelta **Includi traffico**. Tutti gli altri tipi di traffico Internet, ad esempio il traffico relativo a Google o Yahoo, vengono indirizzati direttamente a Internet.

Potrebbe risultare più pratico escludere il traffico verso determinate reti dal tunnel Cisco IOS SSL VPN. In tal caso, aggiungere gli indirizzi di tali reti all'elenco delle reti di destinazione e fare clic sul pulsante di scelta **Escludi traffico**. Tutto il traffico destinato alle reti nell'elenco Reti di destinazione viene inviato tramite percorsi non protetti e tutto il resto del traffico viene invitato tramite il tunnel Cisco IOS SSL VPN.

In caso di stampanti in reti LAN locali che si desidera utilizzare durante la connessione a Cisco IOS SSL VPN, è necessario fare clic su **Escludi LAN locali** nell'area Suddivisione tunnel.

Nota L'elenco delle reti di destinazione presente nell'area Suddivisione tunnel potrebbe contenere già degli indirizzi di rete. Le impostazioni di traffico definite nell'area Suddivisione tunnel hanno la precedenza su tutte le impostazioni già configurate per le reti elencate.

Server DNS e WINS

Immettere gli indirizzi IP dei server DNS e WINS aziendali che verranno inviati ai client Cisco IOS SSL VPN. I client Cisco IOS SSL VPN utilizzeranno tali server per accedere agli host e ai servizi della intranet aziendale.

Fornire gli indirizzi per i server DNS primario e secondario e i server WINS.

Contesto: Impostazioni HTML

Le impostazioni configurate in questa finestra consentono di controllare l'aspetto del portale per il contesto Cisco IOS SSL VPN selezionato.

Seleziona tema

È possibile specificare l'aspetto del portale selezionando un tema predefinito invece di selezionare automaticamente ciascun colore. Quando si seleziona un tema, le impostazioni relative a quel tema vengono visualizzate nei campi associati al pulsante **Personalizza**.

Pulsante Personalizza

Fare clic su questo pulsante se si desidera selezionare ciascun colore utilizzato nel portale e specificare un messaggio di accesso e un titolo. In caso di selezione di un tema predefinito, i valori relativi a quel tema vengono visualizzati nei campi di questa sezione. È possibile modificare questi valori; i valori immessi vengono utilizzati nel portale per il contesto selezionato. Le modifiche apportate in questa finestra influiscono soltanto sul portale in fase di creazione senza apportare variazioni ai valori predefiniti del tema.

Messaggio di accesso

Immettere il messaggio di accesso che verrà mostrato ai client quando il browser visualizzerà il portale. Ad esempio:

```
Benvenuto nella rete nome dell'azienda. Disconnettersi se non si è
utente autorizzato.
```

Titolo

Immettere il titolo che si desidera assegnare al portale. Ad esempio:

```
Pagina di accesso alla rete nome dell'azienda
```

Colore di sfondo per il titolo

Il valore predefinito per il colore di sfondo visualizzato sotto il titolo è #9999CC. Modificare il valore facendo clic sul pulsante **...** e selezionando un colore diverso.

Colore di sfondo per i titoli secondari

Il valore predefinito per il colore di sfondo visualizzato sotto il titolo è #9729CC. Modificare il valore facendo clic sul pulsante **...** e selezionando un colore diverso oppure immettendo il valore esadecimale di un colore diverso.

Colore del testo

Il valore predefinito per il colore del testo è bianco. Modificare il valore facendo clic sulla freccia giù **...** e selezionando un colore diverso.

Colore del testo secondario

Il valore predefinito per il colore del testo secondario è nero. Modificare il valore facendo clic sulla freccia giù **...** e selezionando un colore diverso.

File del logo

Se si desidera visualizzare un logo nel portale, fare clic sul pulsante **...** per ricercare il logo nel PC in uso. Il logo viene salvato nella memoria flash del router quando si sceglie **OK** e verrà visualizzato nell'angolo superiore sinistro del portale.

Pulsante Anteprima

Fare clic su questo pulsante per visualizzare un'anteprima dell'aspetto del portale con il tema predefinito o i valori personalizzati specificati.

Seleziona colore

Fare clic su **Base** per selezionare un colore predefinito, oppure fare clic su **RGB** per creare un colore personalizzato.

Base

Selezionare il colore che si desidera utilizzare dalla tavolozza sulla sinistra. Il colore selezionato viene visualizzato nel quadrato grande sul lato destro della finestra di dialogo.

RGB

Utilizzare i cursori Rosso, Verde e Blu in combinazione per creare un colore personalizzato. Il colore creato viene visualizzato nel quadrato grande sul lato destro della finestra di dialogo.

Contesto: Elenchi server dei nomi NetBIOS

Visualizzare tutti gli elenchi server dei nomi NetBIOS configurati per il contesto Cisco IOS SSL VPN selezionato in questa finestra. Il sistema CIFS utilizza i server NetBIOS per visualizzare il file system di Microsoft Windows aziendale per gli utenti Cisco IOS SSL VPN.

Ciascun elenco server di nomi configurato per il contesto viene visualizzato nell'area **Elenchi server di nomi NetBIOS**. Per gestire questi elenchi, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. Per visualizzare il contenuto dell'elenco nell'area corrispondente **Dettagli del del server dei nomi NetBIOS**, fare clic su un nome dell'elenco.

Aggiungi o modifica elenco server di nomi NetBIOS

Creare o gestire un elenco server dei nomi NetBIOS in questa finestra. È necessario immettere un nome per ogni elenco creato e fornire l'indirizzo IP, il timeout e il numero di tentativi da effettuare per ciascun server nell'elenco. In ogni elenco deve essere presente un server designato come server principale.

Ciascun server nell'elenco viene visualizzato in questa finestra di dialogo, con lo stato principale, il timeout e i valori dei tentativi.

Aggiungi o modifica un server NBNS

È necessario immettere l'indirizzo IP di ciascun server, con il numero di secondi di attesa del router prima di effettuare di nuovo il tentativo di connessione al server, e il numero di tentativi da effettuare per contattare il server.

Se si desidera che questo server sia il primo dell'elenco ad essere contattato dal router, selezionare **Rendere principale questo server**.

Contesto: Elenchi di inoltro su porta

Configurare gli elenchi di inoltro su porta per il contesto selezionato in questa finestra. Gli elenchi possono essere associati a qualsiasi criterio di gruppo configurato nel contesto selezionato. Negli elenchi di inoltro su porta sono indicati i servizi applicazione TCP ai client Cisco IOS SSL VPN.

Nella parte superiore della finestra vengono visualizzati gli elenchi di inoltro su porta configurati per il contesto selezionato. Fare clic su un nome di elenco per visualizzare i dettagli relativi all'elenco nella parte inferiore della finestra.

Nella finestra viene visualizzato l'indirizzo IP, il numero di porta utilizzato, il numero di porta corrispondente del client e una descrizione in caso di immissione di uno di questi.

Aggiungi o modifica elenco di inoltro su porta

Creare e gestire gli elenchi di inoltro su porta in questa finestra. A ciascun elenco deve essere assegnato un nome e deve contenere almeno una voce di server. Utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** per creare, modificare e rimuovere le voci dall'elenco.

Contesto: Elenchi di URL

Gli elenchi di URL specificano i collegamenti che possono essere visualizzati nel portale per gli utenti di un gruppo particolare. Configurare uno o più elenchi URL per ciascun contesto; quindi, utilizzare le finestra dei criteri di gruppo per associare questi elenchi a criteri di gruppo specifici.

Nella parte superiore della finestra sono visualizzati tutti gli elenchi di URL configurati per il contesto. Nella parte inferiore della finestra è visualizzato il contenuto dell'elenco selezionato. Per ciascun elenco, è indicata l'intestazione visualizzata nella parte superiore dell'elenco di URL e ciascun URL presente nell'elenco.

Per creare e gestire gli elenchi di URL, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

Aggiungi o modifica un elenco URL

È necessario immettere un nome per ciascun elenco di URL e il testo dell'intestazione che verrà visualizzato nella parte superiore dell'elenco di URL.

Il testo dell'intestazione deve descrivere il contenuto in generale dei collegamenti presenti nell'elenco. Ad esempio, se un elenco di URL fornisce l'accesso alle pagine Web sui programmi per la salute e quelle sulle assicurazioni, è possibile utilizzare il testo dell'intestazione `Vantaggi`.

Utilizzare il pulsante **Aggiungi** per creare una nuova voce per l'elenco e i pulsanti **Modifica** ed **Elimina** per gestire l'elenco. Ciascuna voce aggiunta viene visualizzata nell'area elenco.

Contesto: Cisco Secure Desktop

Cisco Secure Desktop consente di crittografare cookie, file di cronologia del browser, file temporanei e allegati e-mail che potrebbero causare problemi di protezione se non crittografati. Al termine di una sessione di Cisco IOS SSL VPN, Cisco Secure Desktop rimuove i dati utilizzando un algoritmo di pulitura Department of Defense.

Fare clic su **Attiva Cisco Secure Desktop** per consentire a tutti gli utenti del contesto di eseguire il download e di utilizzare **Cisco Secure Desktop**. Se il bundle di installazione per il software non viene trovato nel router, in questa finestra viene visualizzato un messaggio.

Per caricare il bundle di installazione di Cisco Secure Desktop sul router, fare clic su Pacchetti nella struttura Cisco IOS SSL VPN e seguire le istruzioni riportate nella finestra.

Gateway VPN SSL

Questa finestra visualizza i gateway Cisco IOS SSL VPN configurati sul router e consente di modificare i gateway esistenti e configurarne di nuovi. Un gateway Cisco IOS SSL VPN è il portale utente alla rete di protezione.

Gateway VPN SSL

In quest'area della finestra vengono elencati i gateway Cisco IOS SSL VPN configurati sul router. È indicato il nome e l'indirizzo IP del gateway, il numero di contesti configurati per utilizzare il gateway e lo stato del gateway.


Gateway attivo e in servizio.


Gateway disattivato e fuori servizio.

Fare clic su un gateway per visualizzare i dettagli relativi nella parte inferiore della finestra. Attivare un gateway **Disattivato** selezionandolo e facendo clic su **Attiva**. Rendere un gateway attivo fuori servizio selezionandolo e facendo clic su **Disattiva**. Per modificare un gateway, selezionarlo e fare clic sul pulsante **Modifica**. Per rimuovere un gateway, selezionarlo e fare clic sul pulsante **Elimina**.

Dettagli del gateway VPN SSL

In quest'area della finestra sono visualizzati i dettagli di configurazione del gateway selezionato nella parte superiore della finestra e i nomi dei contesti Cisco IOS SSL VPN configurati per l'utilizzo del gateway.

Per maggiori informazioni sui dettagli di configurazione del gateway, fare clic su Aggiungi o modifica gateway VPN SSL. Per maggiori informazioni sui contesti, fare clic su Contesto VPN SSL.

Aggiungi o modifica gateway VPN SSL

In questa finestra è possibile creare o modificare un gateway Cisco IOS SSL VPN.

Nome gateway

Il nome gateway identifica univocamente il gateway nel router e viene utilizzato per fare riferimento al gateway quando si configurano i contesti Cisco IOS SSL VPN.

Indirizzo IP

Selezionare o immettere l'indirizzo IP da utilizzare per il gateway. Questo indirizzo deve essere un indirizzo IP pubblico e non utilizzato da altri gateway nel router.

Certificato digitale

Selezionare il certificato da inviare ai client Cisco IOS SSL VPN per l'autenticazione SSL.

Casella di controllo Reindirizzamento HTTP

Deselezionare questa casella di controllo se non si desidera utilizzare il reindirizzamento HTTP. Il reindirizzamento HTTP reindirizza automaticamente le richieste HTTP alla porta 443, utilizzata per la comunicazione Cisco IOS SSL VPN protetta.

Casella di controllo Attiva gateway

Deselezionare questa casella di controllo se non si desidera attivare il gateway. È possibile anche attivare e disattivare il gateway dalla finestra Gateway VPN SSL.

Pacchetti

Questa finestra consente di ottenere i bundle di installazione del software che devono essere scaricati nei client Cisco IOS SSL VPN per supportare le funzionalità Cisco IOS SSL VPN e di caricare tali bundle nel router. Questa finestra può essere utilizzata anche per rimuovere i bundle di installazione installati in precedenza.

Seguire la procedura descritta nella finestra per scaricare i bundle di installazione da Cisco.com nel PC in uso e successivamente copiarli sul router. Per ottenere un bundle di installazione, iniziare con il Passaggio 1 facendo clic sul collegamento al sito del download.

Nota Per l'accesso ai siti di download è richiesto un nome utente e una password CCO (Cisco Connection Online). Se non si dispone di tali requisiti, fare clic su Registra nella parte superiore di una qualsiasi pagina Web di Cisco.com e completare il modulo visualizzato. Il nome utente e la password verranno inviati tramite posta elettronica.

Se i bundle di installazione sono stati caricati in precedenza sul PC o sul router, completare i passaggi 2 e 3 per specificare il percorso corrente dei bundle di installazione e copiarli nella memoria flash del router.

Fare clic sul pulsante **...** in ciascuna sezione per specificare il percorso corrente del bundle di installazione.

Dopo avere specificato il percorso corrente e la posizione nella quale si desidera copiare il bundle nella memoria flash del router, fare clic su **Installa**.

Al termine del caricamento dei bundle sul router, nella finestra verranno visualizzate le informazioni relative al nome, la versione e la data di creazione del pacchetto. Se con il pacchetto è disponibile uno strumento di amministrazione, nella finestra viene visualizzato un pulsante che consente di eseguire questo strumento.

Il bundle di installazione del client Cisco IOS SSL VPN è disponibile al seguente collegamento:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Il bundle di installazione Cisco Secure Desktop è disponibile al seguente collegamento:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Installa Pacchetto

Specificare il percorso corrente di un bundle di installazione ricercandolo in questa finestra. Se il bundle di installazione è già presente sul router, fare clic su **Router** ed eseguirne la ricerca. Se il bundle è già presente sul PC, fare clic su **Risorse del computer** ed eseguirne la ricerca. Dopo avere specificato il percorso corrente del bundle di installazione, scegliere **OK**.

Il percorso verrà visualizzato nella finestra Pacchetti.

Contesti Cisco IOS SSL VPN, gateway e criteri

Cisco SDM fornisce un metodo facile per configurare le connessioni Cisco IOS SSL VPN per gli utenti remoti. Tuttavia, la terminologia utilizzata per questa tecnologia potrebbe creare confusione. Nell'argomento della Guida sono illustrati i termini Cisco IOS SSL VPN utilizzati nelle finestre di configurazione Cisco SDM e viene descritto il funzionamento combinato dei componenti di Cisco IOS SSL VPN. Viene fornito anche un esempio dell'utilizzo della procedura guidata Cisco IOS SSL VPN e delle finestre di modifica di Cisco SDM.

Prima di descrivere singolarmente ciascun componente, è opportuno considerare quanto segue:

- Un contesto Cisco IOS SSL VPN è in grado di supportare più criteri di gruppo.
- Ciascun contesto deve disporre di un gateway associato.
- Un gateway può supportare più contesti.
- Se nel router sono presenti più criteri di gruppo, per l'autenticazione deve essere utilizzato un server AAA.

Contesti Cisco IOS SSL VPN

Un contesto Cisco IOS SSL VPN identifica le risorse necessarie per supportare i tunnel VPN SSL tra i client remoti e l'intranet aziendale o privata, e supporta più criteri di gruppo. Un contesto Cisco IOS SSL VPN fornisce le seguenti risorse:

- Un gateway Cisco IOS SSL VPN associato che fornisce un indirizzo IP raggiungibile dai client e un certificato utilizzato per stabilire una connessione protetta.
- Mezzi di autenticazione. È possibile autenticare gli utenti localmente oppure utilizzando i server AAA.
- Le impostazioni di visualizzazione HTML per il portale che fornisce i collegamenti alle risorse di rete.
- Elenchi di inoltro su porta che consentono l'utilizzo di applet del thin client su client remoti. Ciascun elenco deve essere configurato per l'utilizzo in uno specifico criterio di gruppo.
- Elenchi URL contenenti i collegamenti alle risorse nell'intranet aziendale. Ciascun elenco deve essere configurato per l'utilizzo in uno specifico criterio di gruppo.
- Elenchi server dei nomi NetBIOS. Ciascun elenco deve essere configurato per l'utilizzo in uno specifico criterio di gruppo.

Queste risorse sono disponibili quando si configurano i criteri di gruppo Cisco IOS SSL VPN.

Un contesto Cisco IOS SSL VPN è in grado di supportare più criteri di gruppo. Un contesto Cisco IOS SSL VPN può essere associato a un solo gateway.

Gateway Cisco IOS SSL VPN

Un gateway Cisco IOS SSL VPN fornisce un indirizzo IP raggiungibile e il certificato per uno o più contesti Cisco IOS SSL VPN. Ciascun gateway configurato su un router deve essere configurato con il relativo indirizzo IP; gli indirizzi IP non possono essere condivisi tra i gateway. È possibile utilizzare l'indirizzo IP dell'interfaccia di un router oppure un altro indirizzo IP raggiungibile, se disponibile. Per utilizzare i gateway, è necessario configurare un certificato digitale oppure un'autocertificazione. Tutti i gateway nel router possono utilizzare lo stesso certificato.

Sebbene un gateway possa funzionare per più contesti Cisco IOS SSL VPN, è opportuno tenere in considerazione le limitazioni delle risorse e la raggiungibilità dell'indirizzo IP.

Criteri Cisco IOS SSL VPN

I criteri di gruppo Cisco IOS SSL VPN consentono di soddisfare le esigenze di gruppi di utenti differenti. Le esigenze di accesso alle differenti risorse di rete di un gruppo di tecnici, che lavora in modalità remota, sono diverse da quelle del personale addetto alle vendite che opera nel settore. La collaborazione con l'organizzazione richiede l'accesso a determinate informazioni da parte dei partner commerciali e dei rivenditori esterni; tuttavia, è importante assicurarsi di non consentire l'accesso a informazioni riservate o ad altre risorse non necessarie. La creazione di un criterio diverso per ciascuno di questi gruppi consente di fornire agli utenti remoti le risorse necessarie e di impedire a tali utenti di accedere ad altre risorse.

Quando si configura un criterio di gruppo, è possibile effettuare la selezione fra le risorse disponibili configurate per il contesto associato al criterio, quali gli elenchi URL, gli elenchi di inoltro su porta e gli elenchi server dei nomi NetBIOS.

Se sul router sono configurati più criteri di gruppo, sarà necessario configurare il router per l'utilizzo di un server AAA per autenticare gli utenti e per determinare il criterio di gruppo al quale appartiene un determinato utente. Per maggiori informazioni fare clic su Maggiori informazioni sui criteri di gruppo.

Esempio

In questo esempio, l'utente seleziona **Crea un nuovo VPN SSL** e utilizza la procedura guidata per creare la prima configurazione di Cisco IOS SSL VPN sul router. Al termine della procedura guidata, sarà stato creato un nuovo contesto, un gateway e un criterio di gruppo. Nella tabella riportata di seguito sono presenti le informazioni immesse dall'utente in ciascuna finestra della procedura guidata e la configurazione creata in Cisco SDM mediante tali informazioni.

Finestra Procedura guidata Cisco IOS SSL VPN	Configurazione
Finestra Crea una nuova VPN SSL	
L'area Attività preliminari indica che i certificati digitali non sono configurati sul router. L'utente seleziona **autocertificazione** e configura un certificato nella finestra di dialogo Autocertificazione permanente. Non viene modificato il nome fornito in Cisco SDM, Router_Certificate. L'utente seleziona **Crea una nuova VPN SSL**.	In Cisco SDM viene configurata un'autocertificazione denominata “Router_Certificate” che potrà essere utilizzata in tutte le configurazioni Cisco IOS SSL VPN.
Finestra Indirizzo IP e Nome	
L'utente immette le informazioni riportate di seguito: Indirizzo IP - 172.16.5.5 Nome: Asia Selezionare **Attiva l'accesso SDM protetto mediante 192.168.1.1**. Certificato: **Router_Certificate**	In Cisco SDM viene creato un contesto denominato “Asia”. In Cisco SDM viene creato un gateway denominato “gateway 1” nel quale è utilizzato l'indirizzo IP 172.16.5.5 e Router_Certificate. Questo gateway può essere associato ad altri contesti Cisco IOS SSL VPN. Sarà possibile accedere al portale immettendo Cisco IOS SSL VPN http://172.16.5.5/Asia. Se il gateway è associato a contesti aggiuntivi, per tali contesti verrà utilizzato lo stesso indirizzo IP nell'URL. Ad esempio, se il contesto Europa è configurato anche per utilizzare il gateway 1, sarà possibile accedere al portale immettendo https://172.16.5.5/Europa. Dopo che la configurazione è stata inoltrata al router, sarà necessario immettere http://172.16.5.5:4443 per avviare Cisco SDM utilizzando questo indirizzo IP. Inoltre, in Cisco SDM viene avviata la configurazione del primo criterio di gruppo denominato criterio 1.

Finestra Procedura guidata Cisco IOS SSL VPN	Configurazione
Finestra Autenticazione utente	
L'utente sceglie **In locale su questo router**. Viene aggiunto un account utente all'elenco esistente.	In Cisco SDM viene creato l'elenco di autenticazione "sdm_vpn_xauth_ml_1". Questo elenco verrà visualizzato nella finestra Contesti Cisco IOS SSL VPN al termine della procedura guidata. Gli utenti indicati nella finestra Autenticazione utente sono membri di questo elenco di autenticazione e saranno governati dal criterio 1.
Finestra Configura siti Web intranet	
L'utente configura l'elenco URL Ulist_1. L'intestazione è "Taiwan".	L'elenco di URL con intestazione Taiwan verrà mostrato nel portale visualizzata dagli utenti in "sdm_vpn_xauth_ml_1" al momento dell'accesso. L'elenco URL sarà disponibile per la configurazione in altri criteri di gruppo configurati nel contesto "Asia".
Finestra Attiva full tunnel	
L'utente fa clic su **Attiva full tunnel** e seleziona un pool di indirizzi predefinito. Non sono configurate opzioni avanzate.	Nei PC client verrà eseguito il download del software del client per il full tunnel quando si accede per la prima volta e viene stabilito un full tunnel tra il PC e il router al momento dell'accesso al portale.
Finestra Personalizza portale VPN SSL	
L'utente seleziona **Ocean Breeze**.	In Cisco SDM vengono configurate le impostazioni di visualizzazione HTTP con questo schema colori. Quando gli utenti del criterio 1 effettuano l'accesso, viene visualizzato il portale relativo a queste impostazioni. Queste impostazioni vengono applicate anche a tutti i criteri configurati nel contesto "Asia". È possibile personalizzare le impostazioni di visualizzazione HTTP nella finestra Modifica VPN SSL al termine della procedura guidata.
Finestra Configurazione pass-through di VPN SSL	
L'utente seleziona **Consenti l'utilizzo di VPN SSL con NAC e Firewall**	In Cisco SDM viene aggiunto un'ACL con la seguente voce. `permit tcp any host 172.16.5.5 eq 443`

Finestra Procedura guidata Cisco IOS SSL VPN	Configurazione
Finestra Riepilogo	
Nella finestra Riepilogo sono illustrate le informazioni visualizzate a destra. È possibile visualizzare altri dettagli nelle finestre Modifica VPN SSL.	Nome criterio VPN SSL: criterio 1 Nome gateway VPN SSL: gateway 1 Elenco metodi per autenticazione utente: Locale Configurazione full tunnel Stato SVC: Sì Pool di indirizzi IP: Pool 1 Suddivisione tunnel: Disattivato Split DNS: Disattivato Installa client per il full tunnel: Attivato

Quando questa configurazione viene inoltrata, il router dispone di un contesto Cisco IOS SSL VPN denominato Asia, di un gateway denominato gateway 1 e di un criterio di gruppo denominato criterio 1. Queste informazioni vengono visualizzate nella finestra Modifica VPN SSL come mostrato nella seguente tabella:

Nome	Gateway	Dominio	Stato	Stato amministrativo
Asia	gateway 1	Asia		In servizio

Dettagli relativi al contesto VPN SSL Asia:

Nome elemento	Valore elemento
Criteri di gruppo	
criterio 1	
Servizi	Manipolazione URL, Full tunnel
URL esposti agli utenti	http://172.16.5.5/pricelist
	http://172.16.5.5/catalog
Server esposti agli utenti	<Nessuno>
Server WINS	<Nessuno>

Il criterio 1 fornisce il servizio Cisco IOS SSL VPN di base della manipolazione dell'URL e specifica che è stato stabilito un full tunnel tra i client e il router. Non sono configurate altre funzionalità. È possibile aggiungere funzionalità al criterio 1, quali Thin client e Common Internet File System, scegliendo **Configura funzionalità avanzate per un VPN SSL esistente**, selezionando **Asia** e **criterio 1** nella finestra Seleziona gruppo utente Cisco IOS SSL VPN e scegliendo le funzionalità nella finestra delle funzionalità avanzate. In questa procedura guidata è possibile configurare anche elenchi URL aggiuntivi.

È possibile creare un nuovo criterio di gruppo nel contesto "Asia" scegliendo **Aggiungi un nuovo criterio a un VPN SSL esistente per un nuovo gruppo di utenti**.

È possibile personalizzare le impostazioni e i criteri configurati per il contesto "Asia" selezionando Asia nell'elenco dei contesti e facendo clic su **Modifica**. Nella finestra per la modifica del contesto Asia VPN SSL viene visualizzata una struttura che consente di configurare maggiori risorse per il contesto e di modificare e configurare criteri aggiuntivi. Le impostazioni per il gateway 1 possono essere modificate selezionando **Gateway VPN SSL** nel nodo VPN SSL, selezionando il gateway 1 e facendo clic su **Modifica**.

Informazioni aggiuntive

Gli argomenti della sezione relativa alle informazioni aggiuntive illustrano attività di configurazione comuni associate a questa funzionalità.

Come verificare il funzionamento di Cisco IOS SSL VPN?

Il metodo migliore per determinare che un contesto Cisco IOS SSL VPN fornisca l'accesso configurato per gli utenti è effettuare una configurazione come utente e tentare di accedere a tutti i siti Web e ai servizi da fornire agli utenti per i quali è stato configurato il contesto. Utilizzare la procedura riportata di seguito come guida nell'esecuzione di questa prova.

Passo 1 Verificare che le credenziali da utilizzare siano incluse in tutti i criteri appropriati nel server AAA.

Passo 2 Se possibile, aprire una sessione Cisco SDM per il router per monitorare il traffico Cisco IOS SSL VPN che verrà creato. Se il PC per la prova del contesto Cisco IOS SSL VPN non è collegato a una rete con accesso a Cisco SDM, tale operazione deve essere effettuata in un altro PC. Passare a **Monitor > Stato VPN > VPN SSL**.

Passo 3 Immettere l'URL relativo a ciascuno dei portali Web configurate per questo contesto Cisco IOS SSL VPN. Verificare che ciascuna pagina presenti l'aspetto configurato e che tutti i collegamenti specificati negli elenchi degli URL relativi al criterio siano visualizzati nella pagina.

Passo 4 Verificare tutti i collegamenti e i servizi disponibili per gli utenti inclusi in questo criterio. Se uno dei criteri da verificare consente il download di Cisco Secure Desktop o del software del client per il full tunnel, immettere gli URL ai portali Web per quei criteri e fare clic sui collegamenti che richiederanno il download di questo software. Verificare che il download del software venga eseguito in modo corretto e che sia possibile accedere ai servizi destinati agli utenti attraverso questi collegamenti.

Passo 5 Se una sessione Cisco SDM viene stabilita prima di iniziare la verifica, fare clic sul ramo del contesto da verificare e consultare le statistiche relative al traffico Cisco IOS SSL VPN nella finestra Cisco IOS SSL VPN.

Passo 6 Sulla base dei risultati delle verifiche, ritornare a Cisco SDM se necessario e correggere i problemi di configurazione riscontrati.

Come configurare una Cisco IOS SSL VPN dopo aver configurato un firewall?

Se il firewall è già stato configurato, è possibile comunque utilizzare le procedure guidate Cisco IOS SSL VPN in Cisco SDM per creare contesti e criteri Cisco IOS SSL VPN. Cisco SDM convalida i comandi CLI Cisco IOS SSL VPN generati rispetto alla configurazione esistente sul router. L'utente viene informato nel caso in cui venga rilevata una configurazione del firewall esistente da modificare in modo da consentire il passaggio del traffico Cisco IOS SSL VPN. È possibile consentire a Cisco SDM di apportare le modifiche necessarie al firewall oppure lasciare il firewall intatto e apportare manualmente le modifiche accedendo a **Configura > Firewall e ACL > Modifica firewall ACL** e immettendo le dichiarazioni che consentono il passaggio del traffico Cisco IOS SSL VPN attraverso il firewall.

Come associare un'istanza VRF a un contesto Cisco IOS SSL VPN?

Le istanze VFR (Routing and Forwarding) VPN consentono di gestire una tabella di routing e una tabella di inoltro su porta per una VPN. È possibile associare un'istanza VRF o un nome con un contesto Cisco IOS SSL VPN passando a **Configura > VPN > VPN SSL > Modifica VPN SSL**. Selezionare il contesto a cui si desidera associare un'istanza VRF quindi fare clic su **Modifica**. Selezionare il nome dell'istanza VRF nella finestra di dialogo visualizzata.

Nota L'istanza VRF deve essere già stata configurata sul router.

CAPITOLO 20

Risoluzione dei problemi della rete VPN

Cisco SDM è in grado di risolvere i problemi delle connessioni VPN configurate. Cisco SDM esegue dei test di connessione e, in caso di errore, suggerisce le azioni da intraprendere per correggere il problema.

Il seguente collegamento fornisce informazioni sulla risoluzione dei problemi della rete VPN mediante interfaccia della riga di comando (CLI).

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/useguide/u13_rtrb.htm

Risoluzione dei problemi della rete VPN

Questa finestra viene visualizzata durante la risoluzione dei problemi di una connessione VPN site-to-site, di un tunnel GRE su IPSec, di una connessione remota Easy VPN oppure una connessione server Easy VPN.

Nota La risoluzione dei problemi della rete VPN non prenderà in considerazione più di due peer per una VPN site-to-site, per un tunnel GRE su IPSec o per una connessione remota Easy VPN.

Dettagli tunnel

Questa casella fornisce i dettagli relativi al tunnel VPN.

Interfaccia

L'interfaccia dalla quale viene configurata la rete VPN.

Peer

L'indirizzo IP o il nome host dei dispositivi presenti all'altra estremità della connessione VPN.

Riepilogo

Fare clic su questo pulsante per visualizzare un riepilogo delle informazioni relative alla risoluzione dei problemi.

Dettagli

Fare clic su questo pulsante per visualizzare i dettagli delle informazioni relative alla risoluzione dei problemi.

Attività

In questa colonna sono visualizzate le attività legate alla risoluzione dei problemi.

Stato

Consente di visualizzare lo stato di ciascuna attività di risoluzione dei problemi, contrassegnato dalle icone e dagli avvisi riportati di seguito:


La connessione è attiva.


La connessione non è attiva.


La verifica ha avuto esito positivo.


La verifica ha avuto esito negativo.

Motivi errore

Questa casella indica le possibili cause dell'errore del tunnel VPN.

Azioni consigliate

In questa casella vengono fornite possibili azioni per risolvere il problema.

Pulsante Chiudi

Fare clic sul pulsante per chiudere la finestra.

Pulsante Verifica client specifico

Il pulsante è attivo se si sta eseguendo la verifica delle connessioni per un server Easy VPN configurato sul router. Fare clic sul pulsante e specificare il client per cui si desidera eseguire la verifica della connessione.

Il pulsante è disattivo nelle seguenti circostanze:

- La verifica di base non viene eseguita oppure non è stato completata correttamente.
- L'immagine IOS non supporta i comandi di debug richiesti.
- La vista utilizzata per avviare Cisco SDM non dispone dei privilegi amministrativi.

Tabella riassuntiva funzioni

Funzione	Procedura
Risoluzione di problemi della connessione VPN.	Fare clic sul pulsante **Avvia**. Quando la verifica è in esecuzione, l'etichetta del pulsante **Avvia** diventerà **Arresta**. Si ha quindi la possibilità di interrompere la risoluzione dei problemi durante la fase di verifica.
Salvataggio del report di verifica	Fare clic sul pulsante **Salva report** per salvare il report della verifica in formato HTML. Il pulsante è disattivo quando la verifica è in corso.

Risoluzione dei problemi della rete VPN - Specificare client Easy VPN

Questa finestra consente di specificare il client Easy VPN di cui si desidera eseguire il debug.

Indirizzo IP

Immettere l'indirizzo IP del client Easy VPN di cui si desidera eseguire il debug.

Attendi richiesta per X minuti

Inserire il tempo massimo durante il quale il server Easy VPN deve attendere le richieste del client Easy VPN.

Pulsante Continua

Dopo aver selezionato il tipo di generazione del traffico, fare clic sul pulsante per continuare la verifica.

Pulsante Chiudi

Fare clic sul pulsante per chiudere la finestra.

Risoluzione dei problemi della rete VPN - Genera traffico

Da questa finestra si può generare del traffico di VPN site-to-site o Easy VPN ai fini del debug. È possibile lasciare che Cisco SDM generi traffico VPN, oppure generare attivamente del traffico VPN.

Il traffico VPN della connessione è definito come segue

In questo campo viene elencato il traffico VPN nell'interfaccia.

Azione

La colonna indica se il tipo di traffico è autorizzato nell'interfaccia.

Origine

Indirizzo IP di origine

Destinazione

Indirizzo IP di destinazione

Servizio

In questa colonna viene elencato il tipo di traffico nell'interfaccia.

Registro

Questa colonna indica se per questo tipo di traffico è stata attivata la registrazione.

Attributi

Tutti gli attributi supplementari definiti.

Genera traffico VPN tramite SDM

Selezionare questa opzione se si desidera che sia Cisco SDM a generare il traffico VPN nell'interfaccia per il debug.

Nota Cisco SDM non genererà il traffico nel caso in cui il traffico del tunnel VPN è originato da una lista ACL senza IP oppure quando la vista CLI applicata non è quella di amministrazione.

Immettere un indirizzo IP di host nella rete di origine

Immettere l'indirizzo host nella rete di origine.

Immettere un indirizzo IP di host nella rete di destinazione

Immettere l'indirizzo IP di host nella rete di destinazione.

Il traffico VPN verrà generato dalla rete di origine

Selezionare questa opzione se si desidera generare il traffico VPN dalla rete di origine.

Tempo di attesa

Immettere il tempo in secondi durante il quale il server Easy VPN Server resta in attesa che venga generato il traffico. Assicurarsi di impostare una durata tale da consentire all'utente di passare ad altri sistemi per generare il traffico.

Pulsante Continua

Dopo aver selezionato il tipo di generazione del traffico, fare clic sul pulsante per continuare la verifica.

Pulsante Chiudi

Fare clic sul pulsante per chiudere la finestra.

Risoluzione dei problemi della rete VPN - Generare traffico GRE

La schermata appare durante la generazione del traffico GRE su IPSec.

Genera traffico VPN tramite SDM

Selezionare questa opzione se si desidera che sia Cisco SDM a generare il traffico VPN nell'interfaccia per il debug.

Immettere indirizzo IP del tunnel remoto

Immettere l'indirizzo IP del tunnel GRE remoto. Non utilizzare l'indirizzo dell'interfaccia remota.

Il traffico VPN verrà generato dalla rete di origine

Selezionare questa opzione se si desidera generare il traffico VPN dalla rete di origine.

Tempo di attesa

Immettere il tempo in secondi durante il quale il server Easy VPN Server resta in attesa che venga generato il traffico. Assicurarsi di impostare una durata tale da consentire all'utente di passare ad altri sistemi per generare il traffico.

Pulsante Continua

Dopo aver selezionato il tipo di generazione del traffico, fare clic sul pulsante per continuare la verifica.

Pulsante Chiudi

Fare clic sul pulsante per chiudere la finestra.

Avviso Cisco SDM: SDM consente di eseguire i debug del router…

Questa finestra appare quando Cisco SDM è pronto a iniziare la risoluzione avanzata dei problemi. La risoluzione avanzata dei problemi include l'invio dei comandi di debug al router in attesa dei risultati e, successivamente, l'eliminazione di tali comandi per non compromettere ulteriormente le prestazioni del router.

Questo messaggio viene visualizzato poiché il processo può durare alcuni minuti e potrebbe influire sulle prestazioni del router.

CAPITOLO 21

Security Audit

La funzionalità Security Audit consente di esaminare le configurazioni del router esistente e aggiorna il router per una maggiore protezione del router e della rete. Basato sulla funzionalità Cisco IOS AutoSecure, Security Audit consente di eseguire verifiche e fornisce supporto nella configurazione di quasi tutte le funzioni AutoSecure. Per un elenco completo delle funzioni esaminate da Security Audit e per un elenco delle poche funzioni AutoSecure non supportate da Security Audit, vedere l'argomento Cisco SDM e Cisco IOS AutoSecure.

La funzionalità opera in due modalità: la Procedura guidata di Security Audit, che consente di scegliere quali potenziali modifiche di configurazione relative alla protezione implementare nel router, e Blocco rapido, che apporta automaticamente tutte le modifiche di configurazione relative alla protezione consigliate.

Esegui Security Audit

Con questa opzione è possibile avviare la procedura guidata di Security Audit. La procedura consente di verificare la configurazione del router per determinare se esistono potenziali problemi di protezione, quindi visualizza una schermata che permette di indicare quali di questi problemi si desidera risolvere. Una volta determinati, al router verranno apportate le modifiche necessarie per la risoluzione.

Per fare in modo che Cisco SDM esegua Security Audit e risolva i problemi rilevati

Passo 1 Nel frame a sinistra, selezionare **Security Audit**.

Passo 2 Fare clic su **Esegui Security Audit**.

Viene visualizzata la pagina iniziale della procedura guidata.

Passo 3 Fare clic su **Avanti>**.

Viene visualizzata la pagina Configurazione dell'interfaccia di Security Audit.

Passo 4 Per utilizzare la procedura è necessario conoscere quali interfacce del router sono connesse alle rete interna e quali sono connesse all'esterno della rete. Per ogni interfaccia elencata, selezionare la casella di controllo **Interna** o **Esterna** per indicare dove connettere l'interfaccia.

Passo 5 Fare clic su **Avanti>**.

La procedura guidata consente di verificare la configurazione del router per determinare quali possibili problemi di protezione possono esistere. Viene visualizzata una schermata che mostra lo stato dell'azione, elencando tutte le opzioni di configurazioni da verificare e se la configurazione del router corrente supera o meno tali verifiche.

Se si desidera salvare il report in un file, fare clic su **Salva report**.

Passo 6 Fare clic su **Chiudi**.

Viene visualizzata la schermata Scheda report di Security Audit che mostra un elenco dei possibili problemi legati alla protezione.

Passo 7 Selezionare le caselle **Correggi** accanto ai problemi che si desidera risolvere tramite Cisco Router and Security Device Manager (Cisco SDM). Per una descrizione del problema e un elenco dei comandi Cisco IOS che verranno aggiunti alla configurazione, fare clic sulla descrizione del problema per visualizzare la relativa pagina della Guida.

Passo 8 Fare clic su **Avanti>**.

Passo 9 Nella procedura guidata possono essere visualizzate una o più schermate che richiedono informazioni per la risoluzione di determinati problemi. Immettere le informazioni come richiesto e fare clic su **Avanti>** in ognuna di queste schermate.

Passo 10 Nella pagina Riepilogo della procedura viene visualizzato un elenco di tutte le modifiche di configurazione che verranno apportate in Security Audit. Fare clic su **Fine** per trasmettere le modifiche al router.

Blocco rapido

Con questa opzione è possibile verificare potenziali problemi di protezione della configurazione del router, e apportare automaticamente tutte le modifiche di configurazione necessarie per la risoluzione dei problemi rilevati. Le condizioni esaminate e, se necessario, corrette sono riportate di seguito.

- Disattiva servizio Finger
- Disattiva servizio PAD
- Disattiva il servizio TCP Small Servers
- Disattiva il servizio UDP Small Servers
- Disattiva servizio server BOOTP IP
- Disattiva servizio identificazione IP
- Disattiva CDP
- Disattiva route di origine IP
- Attiva servizio di crittografia password
- Attiva TCP Keepalive per le sessioni telnet in ingresso
- Attiva TCP Keepalive per le sessioni telnet in uscita
- Attiva i numeri di sequenza e gli indicatori data ora per le operazioni di debug
- Attiva IP CEF
- Disattiva ARP gratuiti IP
- Imposta la lunghezza minima della password a meno di 6 caratteri
- Imposta la frequenza di errore di autenticazione a meno di 3 tentativi
- Imposta ora di attesa TCP Syn
- Imposta banner
- Attivazione della registrazione
- Imposta attivazione password segreta
- Disattiva SNMP
- Imposta intervallo pianificazione
- Imposta allocazione pianificazione
- Imposta utenti

- Attiva impostazioni Telnet
- Attiva modalità NetFlow Switching
- Disattiva reindirizzamenti IP
- Disattiva ARP proxy IP
- Disattiva Broadcast IP
- Disattiva servizio MOP
- Disattiva IP non raggiungibili
- Disattiva risposta maschera IP
- Disattiva IP non raggiungibili su interfacce NULL
- Attiva Unicast RPF su tutte le interfacce esterne
- Attiva firewall su tutte le interfacce esterne
- Imposta classe di accesso per il servizio server HTTP
- Imposta classe di accesso sulle linee VTY
- Attiva SSH per l'accesso al router

Pagina iniziale

In questa schermata è descritta la procedura guidata di Security Audit e le modifiche che si tenta di apportare alla configurazione del router mediante tale procedura.

Pagina Selezione di interfaccia

In questa schermata viene visualizzato un elenco di tutte le interfacce e viene richiesto di identificare quali interfacce del router sono “esterne”, ovvero, le interfacce che sono connesse a reti non protette, ad esempio a Internet. Identificando quali interfacce sono esterne, con Configurazione protezione è possibile sapere su quali interfacce configurare le funzionalità di protezione firewall.

Colonna Interfaccia

In questa colonna sono elencate tutte le interfacce del router.

Colonna Esterna

Nella colonna viene visualizzata una casella di controllo per ogni interfaccia elencata nella colonna Interfaccia. Selezionare la casella di controllo di ogni interfaccia connessa a una rete esterna alla propria, ad esempio a Internet.

Colonna Interna

Nella colonna viene visualizzata una casella di controllo per ogni interfaccia elencata nella colonna Interfaccia. Selezionare la casella di controllo per ogni interfaccia connessa direttamente alla rete locale, e quindi protetta da Internet tramite firewall.

Pagina Scheda report

Nella pagina popup viene visualizzato un elenco delle modifiche di configurazione consigliate che, se apportate, aumentano la protezione della rete. Il pulsante **Salva**, attivato dopo aver eseguito tutti i controlli, consente di salvare la scheda report in un file che si può stampare o inviare tramite posta elettronica. Selezionando **Chiudi** viene visualizzata una finestra di dialogo in cui sono elencati i problemi di protezione rilevati e le potenziali configurazioni di protezione che possono essere annullate da Cisco SDM.

Pagina Correggi

In questa pagina sono visualizzate le modifiche di configurazione consigliate nella pagina Scheda report. Utilizzare l'elenco **Selezionare un'opzione** per visualizzare i problemi di protezione risolvibili da Cisco SDM o le configurazioni di protezione che possono essere annullate da Cisco SDM.

Selezionare un'opzione: Risolvere i problemi di protezione

Nella schermata Scheda report viene visualizzato un elenco delle modifiche di configurazione consigliate che aumentano la protezione del router e della rete. I potenziali problemi di protezione nella configurazione del router sono elencati nella colonna a sinistra. Per maggiori informazioni su un problema potenziale, fare clic sul problema. Nella Guida in linea verrà visualizzata una descrizione più dettagliata del problema e le modifiche di configurazione suggerite. Per risolvere tutti i problemi potenziali, fare clic su **Correggi tutto** e selezionare **Avanti>** per continuare. Per risolvere un singolo problema di protezione, selezionare la casella di controllo **Correggi** accanto al problema e fare clic su **Avanti>** per continuare la procedura guidata. Con Security Audit è possibile correggere i problemi selezionati, raccogliendo ulteriori dati dall'utente quando necessario, e quindi di visualizzare un elenco dei comandi della nuova configurazione che verrà aggiunta a quella del router.

Correggi tutto

Fare clic su questo pulsante per inserire un segno di spunta accanto a tutti i potenziali problemi di protezione elencati nella schermata Scheda report.

Selezionare un'opzione: Annulla configurazioni di protezione

Quando si seleziona quest'opzione, Cisco SDM visualizza le configurazioni di protezione che possono essere annullate. Per fare in modo che Cisco SDM annulli tutte le configurazioni di protezione, fare clic su **Annulla tutto**. Per specificare una configurazione di protezione da annullare, selezionare la casella **Annulla** posizionata accanto alla voce. **Fare clic su Avanti>** dopo aver specificato quali configurazioni di protezione annullare. È necessario selezionarne almeno una.

Annulla tutto

Fare clic su questo pulsante per inserire un segno di spunta accanto a tutte le configurazioni di protezione che possono essere annullate da Cisco SDM.

Per visualizzare le configurazioni di protezione che si possono annullare con Cisco SDM, fare clic su

Configurazioni di protezione annullabili in Cisco SDM

Soluzione di alcuni problemi da parte di Cisco SDM, ma annullamento di altre configurazioni di protezione

Se si desidera risolvere alcuni problemi di protezione con Cisco SDM ma annullare altre configurazioni di protezione non necessarie, si può utilizzare la procedura guidata di Security Audit. Eseguire la procedura una prima volta, per specificare i problemi da correggere e, una seconda volta, per poter selezionare le configurazioni di protezione da annullare.

Disattiva servizio Finger

Security Audit consente di disattivare il servizio finger, quando possibile. Il servizio viene utilizzato per scoprire quali utenti sono connessi a un dispositivo di rete. Sebbene queste informazioni non siano altamente riservate, talvolta potrebbero essere utili a un utente malintenzionato.

Inoltre, il servizio Finger può essere utilizzato in un determinato tipo di attacco di negazione del servizio (DoS, Denial-of-Service) detto “Finger of death” che comporta l'invio di una richiesta Finger a un determinato computer ogni minuto, ma senza mai disconnettersi.

La configurazione che verrà trasmessa al router per disattivare il servizio Finger è riportata di seguito:

```
no service finger
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva servizio PAD

Security Audit consente di disattivare tutti i comandi PAD (Packet Assembler/Disassembler) e le connessioni tra i dispositivi PAD e i server di accesso, quando possibile.

La configurazione che verrà trasmessa al router per disattivare il servizio PAD è riportata di seguito:

```
no service pad
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva il servizio TCP Small Servers

Security Audit consente di disattivare i servizi secondari, quando possibile. Per impostazione predefinita, i dispositivi Cisco che eseguono Cisco IOS versione 11.3 o precedente offrono “servizi secondari” quali echo, chargen e discard. Questa tipologia di servizio, per impostazione predefinita, è disattivata in Cisco IOS versione 12.0 e successiva. Tali servizi, in particolar modo le versioni UDP (User Datagram Protocol), raramente sono utilizzati per scopi leciti, tuttavia possono essere utilizzati per avviare DoS e altri attacchi altrimenti impediti dal filtro pacchetti.

Un utente malintenzionato potrebbe, ad esempio, inviare un pacchetto DNS (Domain Name System), falsificando l'indirizzo origine con quello di un server DNS, che altrimenti sarebbe raggiungibile, e utilizzando come porta origine, la porta di servizio DNS (porta 53). Se un tale pacchetto venisse inviato alla porta echo UDP del router, risulterebbe che il pacchetto DNS sarebbe stato inviato dal router al server in questione. Nessun controllo degli elenchi di accesso in uscita verrebbe applicato al pacchetto, dal momento che verrebbe considerato come generato localmente dal router stesso.

Sebbene gran parte degli abusi dei servizi secondari possa essere evitata o resa meno pericolosa utilizzando elenchi di accesso anti-spoofing, i servizi dovrebbero essere quasi sempre disattivati su qualsiasi router che fa parte di un firewall o che si trova in un punto della rete critico a livello di protezione. Dal momento che i servizi sono utilizzati raramente, la politica migliore, di solito, consiste nel disattivarli su tutti i router di qualsiasi descrizione.

La configurazione che verrà trasmessa al router per disattivare il servizio TCP Small Servers è riportata di seguito:

```
no service tcp-small-servers
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva il servizio UDP Small Servers

Security Audit consente di disattivare i servizi secondari, quando possibile. Per impostazione predefinita, i dispositivi Cisco che eseguono Cisco IOS versione 11.3 o precedente offrono “servizi secondari” quali echo, chargen e discard. Questa tipologia di servizio, per impostazione predefinita, è disattivata in Cisco IOS versione 12.0 e successiva. Tali servizi, in particolar modo le versioni UDP, raramente sono utilizzati per scopi leciti, tuttavia possono essere utilizzati per avviare DoS e altri attacchi altrimenti impediti dal filtro pacchetti.

Un utente malintenzionato potrebbe, ad esempio, inviare un pacchetto DNS (Domain Name System), falsificando l'indirizzo origine con quello di un server DNS, che altrimenti sarebbe raggiungibile, e utilizzando come porta origine, la porta di servizio DNS (porta 53). Se un tale pacchetto venisse inviato alla porta echo UDP del router, risulterebbe che il pacchetto DNS sarebbe stato inviato dal router al server in questione. Nessun controllo degli elenchi di accesso in uscita verrebbe applicato al pacchetto, dal momento che verrebbe considerato come generato localmente dal router stesso.

Sebbene gran parte degli abusi dei servizi secondari possa essere evitata o resa meno pericolosa utilizzando elenchi di accesso anti-spoofing, i servizi dovrebbero essere quasi sempre disattivati su qualsiasi router che fa parte di un firewall o che si trova in un punto della rete critico a livello di protezione. Dal momento che i servizi sono utilizzati raramente, la politica migliore, di solito, consiste nel disattivarli su tutti i router di qualsiasi descrizione.

La configurazione che verrà trasmessa al router per disattivare il servizio UDP Small Servers è riportata di seguito:

```
no service udp-small-servers
```

Disattiva servizio server BOOTP IP

Security Audit consente di disattivare il servizio BOOTP (Bootstrap Protocol), quando possibile. Grazie a BOOTP, i router e i computer possono configurare automaticamente le informazioni Internet necessarie da un server gestito centralmente all'avvio, includendo il download del software Cisco IOS. Di conseguenza, BOOTP può essere potenzialmente utilizzato da un utente malintenzionato per scaricare una copia del software Cisco IOS di un router.

Inoltre, il servizio BOOTP è vulnerabile ad attacchi DoS; pertanto dovrebbe essere disattivato o filtrato mediante un firewall anche per questo motivo.

La configurazione che verrà trasmessa al router per disattivare il servizio BOOTP è riportata di seguito:

```
no ip bootp server
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva servizio identificazione IP

Security Audit consente di disattivare il supporto di identificazione, quando possibile. Grazie a questo supporto è possibile richiedere l'identificazione di una porta TCP. Questa funzionalità consente a un protocollo non protetto di segnalare l'identificazione di un client che inizializza una connessione TCP e un host che risponde alla connessione. Il supporto consente di connettere una porta TCP su un host, emettere una semplice stringa di testo per richiedere informazioni e ricevere una risposta con una stringa.

È pericoloso consentire, a un qualsiasi sistema su un segmento connesso direttamente, di sapere che il router è un dispositivo Cisco e di determinare il numero di modello e la versione software Cisco IOS in esecuzione. Queste informazioni possono essere utilizzate per progettare attacchi contro il router.

La configurazione che verrà trasmessa al router per disattivare il servizio di identificazione IP è riportata di seguito:

```
no ip identd
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva CDP

Security Audit consente di disattivare CDP (Cisco Discovery Protocol), quando possibile. CDP è un protocollo proprietario utilizzato dai router Cisco per essere in grado di identificarsi reciprocamente su un segmento LAN. Questa funzionalità risulta pericolosa in quanto consente a un qualsiasi sistema su un segmento connesso direttamente di sapere che il router è un dispositivo Cisco e di determinare il numero di modello e la versione software Cisco IOS in esecuzione. Queste informazioni possono essere utilizzate per progettare attacchi contro il router.

La configurazione che verrà trasmessa al router per disattivare CDP è riportata di seguito:

```
no cdp run
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva route di origine IP

Security Audit consente di disattivare il routing di origine IP, quando possibile. Il protocollo IP supporta le opzioni di routing di origine che consentono al mittente di un datagramma IP di controllare la route che il datagramma intraprende verso la destinazione finale e, generalmente anche la route di risposta. Queste opzioni raramente sono utilizzate per scopi leciti nelle reti. Alcune implementazioni IP precedenti non elaborano i pacchetti di routing di origine correttamente. Un arresto anomalo dei computer che eseguono queste implementazioni potrebbe verificarsi inviando loro datagrammi con opzioni di routing di origine.

Disattivando il routing di origine IP, un router Cisco non sarà mai in grado di inoltrare un pacchetto IP con un'opzione di routing di origine.

La configurazione che verrà trasmessa al router per disattivare il routing di origine IP è riportata di seguito:

```
no ip source-route
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Attiva servizio di crittografia password

Security Audit consente di attivare la crittografia password, quando possibile. Questa funzionalità consente al software Cisco IOS di crittografare le password, i dati segreti CHAP (Challenge Handshake Authentication Protocol) e altre informazioni simili che sono salvate nel relativo file di configurazione. Questa funzionalità è utile per impedire la lettura delle password a utenti occasionali che, ad esempio, osservano lo schermo da dietro le spalle di un amministratore.

La configurazione che verrà trasmessa al router per attivare la crittografia password è riportata di seguito:

```
service password-encryption
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Attiva TCP Keepalive per le sessioni telnet in ingresso

Security Audit consente messaggi TCP Keepalive per le sessioni Telnet in ingresso e in uscita, quando possibile. Con l'attivazione di TCP Keepalive, il router genera messaggi Keepalive periodici che consentono di rilevare ed eliminare le connessioni Telnet interrotte.

La configurazione che verrà trasmessa al router per attivare TCP Keepalive per le sessioni Telnet in ingresso è riportata di seguito:

```
service tcp-keepalives-in
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Attiva TCP Keepalive per le sessioni telnet in uscita

Security Audit consente messaggi TCP Keepalive per le sessioni Telnet in ingresso e in uscita, quando possibile. Con l'attivazione di TCP Keepalive, il router genera messaggi Keepalive periodici che consentono di rilevare ed eliminare le connessioni Telnet interrotte.

La configurazione che verrà trasmessa al router per attivare TCP Keepalive per le sessioni Telnet in uscita è riportata di seguito:

```
service tcp-keepalives-out
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Attiva i numeri di sequenza e gli indicatori data ora per le operazioni di debug

Security Audit consente l'attivazione dei numeri di sequenza e degli indicatori data ora per le operazioni di debug, e i messaggi registro, quando possibile. Gli indicatori data ora e i messaggi registro indicano la data e l'ora in cui è stato generato un messaggio. I numeri di sequenza indicano la sequenza in cui sono stati generati i messaggi con indicatori data ora identici. Queste informazioni rappresentano un importante strumento per diagnosticare potenziali attacchi.

La configurazione che verrà trasmessa al router per attivare gli indicatori data ora e i numeri di sequenza è riportata di seguito:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

Attiva IP CEF

Security Audit consente il CEF (Cisco Express Forwarding) o il DCEF (Distributed Cisco Express Forwarding), quando possibile. Poiché non è necessario creare voci nella cache quando il traffico arriva a destinazioni nuove, il funzionamento del CEF è più prevedibile di altre modalità quando presentato con grandi volumi di traffico indirizzati a più destinazioni. I router configurati per il CEF offrono prestazioni migliori contro attacchi SYN rispetto a router che utilizzano la cache tradizionale.

La configurazione che verrà trasmessa al router per attivare CEF è riportata di seguito:

```
ip cef
```

Disattiva ARP gratuiti IP

Security Audit consente di disattivare le richieste di ARP (Address Resolution Protocol) gratuiti IP, quando possibile. Un ARP gratuito è un broadcast ARP in cui gli indirizzi MAC di origine e di destinazione sono uguali, ed è utilizzato principalmente da un host per fornire alla rete informazioni sul relativo indirizzo IP. Un messaggio ARP gratuito falsificato può causare un'archiviazione non corretta delle informazioni relative alla mappatura della rete, provocandone un malfunzionamento.

La configurazione che verrà trasmessa al router per disattivare gli ARP gratuiti è riportata di seguito:

```
no ip gratuitous-arps
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Imposta la lunghezza minima della password a meno di 6 caratteri

Security Audit consente di configurare il router in modo che richieda una lunghezza minima della password di sei caratteri, quando possibile. Uno dei metodi utilizzato dagli utenti malintenzionati per forzare le password è tentare tutte le combinazioni di caratteri possibili fino a quando la password non viene scoperta. Le password più lunghe hanno esponenzialmente più combinazioni di caratteri possibili, rendendo il metodo di attacco più difficile.

Con questa modifica di configurazione tutte le password del router, incluse le password utente, di attivazione, crittografata, di console, AUX, TTY e VTY devono avere una lunghezza minima di sei caratteri. La modifica di configurazione verrà eseguita solo se la versione di Cisco IOS in esecuzione sul router supporta questa funzionalità.

La configurazione che verrà trasmessa al router è riportata di seguito:

```
security passwords min-length <6>
```

Imposta la frequenza di errore di autenticazione a meno di 3 tentativi

Security Audit consente di configurare il router in modo che possa bloccare l'accesso dopo tre tentativi non riusciti, quando possibile. Un metodo per forzare le password, detto attacco con “dizionario”, consiste nell'utilizzare un software che tenta l'accesso con le parole di un dizionario. Questa configurazione blocca l'accesso al router per 15 secondi dopo tre tentativi non riusciti, disattivando il metodo di attacco con dizionario. Oltre a bloccare l'accesso al router, dopo i tre tentativi viene generato un messaggio registro che avvisa l'amministratore dei tentativi di accesso non riusciti.

La configurazione, che verrà trasmessa al router per bloccarne l'accesso dopo tre tentavi non riusciti, è riportata di seguito:

```
security authentication failure rate <3>
```

Imposta ora di attesa TCP Syn

Security Audit consente di impostare l'ora di attesa TCP Syn a 10 secondi, quando possibile. Questo valore è utile per superare attacchi SYN Flooding, una forma di attacco DoS. Una connessione TCP richiede un collegamento in tre fasi per stabilire inizialmente la connessione. La richiesta di connessione viene inviata dal richiedente, il riconoscimento viene inviato dal ricevente e l'accettazione di quel riconoscimento viene inviata dal mittente. Una volta completate le tre fasi, la connessione è ultimata e può iniziare il trasferimento dei dati. Un attacco SYN Flooding invia ripetute richieste di connessione a un host, ma non invia mai l'accettazione di riconoscimenti che completano le connessioni, creando sempre più connessioni incomplete nell'host. Poiché il buffer per le connessioni incomplete è solitamente di dimensione inferiore rispetto a quello delle connessioni completate, tale situazione può comportare l'utilizzo eccessivo e la disattivazione dell'host. Impostando l'ora di attesa TCP Syn a 10 secondi, una connessione incompleta viene chiusa dal router dopo 10 secondi, impedendo l'intensificarsi di connessioni incomplete nell'host.

La configurazione che verrà trasmessa al router per impostare l'ora di attesa TCP Syn a 10 secondi è riportata di seguito:

```
ip tcp synwait-time <10>
```

Imposta banner

Security Audit consente di configurare un testo per il banner, quando possibile. In alcune legislazioni, il procedimento giudiziario civile e/o penale di utenti dolosi che interferiscono con i sistemi è reso più semplice se viene fornito un banner che informi gli utenti non autorizzati a non eseguire tale operazione in quanto non consentita. In altre legislazioni, può essere vietato controllare le attività anche di utenti non autorizzati a meno che non ne sia stata notificata l'intenzione. Il testo per banner rappresenta un metodo per eseguire questa notifica.

La configurazione che verrà trasmessa al router per creare un testo per il banner è riportata di seguito, sostituendo <*company name*>, <*administrator email address*> e <*administrator phone number*> con i valori appropriati inseriti in Security Audit:

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Attivazione della registrazione

Security Audit consente di attivare la registrazione con gli indicatori data ora e i numeri di sequenza, quando possibile. Dal momento che fornisce informazioni dettagliate sugli eventi di rete, la registrazione è una funzione fondamentale per riconoscere e rispondere agli eventi di protezione. Gli indicatori data ora e i numeri di sequenza forniscono informazioni circa la data, l'ora e la sequenza in cui gli eventi si verificano nella rete.

La configurazione che verrà trasmessa al router per attivare e configurare la registrazione è riportata di seguito, sostituendo <*log buffer size*> e <*logging server ip*> con i valori appropriati immessi in Security Audit:

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

Imposta attivazione password segreta

Security Audit consente di configurare il comando **enable secret** di Cisco IOS per una maggiore protezione delle password, quando possibile. Il comando **enable secret** è utilizzato per impostare la password che concede l'accesso amministrativo privilegiato al sistema Cisco IOS. Il comando **enable secret** utilizza un algoritmo di crittografia (MD5) per proteggere tale password, molto più sicuro del comando **enable password** precedente. Questa crittografia più avanzata è un mezzo essenziale per proteggere la password del router e, di conseguenza, l'accesso alla rete.

La configurazione che verrà trasmessa al router per configurare il comando è riportata di seguito:

```
enable secret <>
```

Disattiva SNMP

Security Audit consente di disattivare SNMP (Simple Network Management Protocol), quando possibile. SNMP è un protocollo di rete che fornisce una funzionalità per recuperare e inoltrare dati sulle prestazioni e sui processi della rete. È utilizzato ampiamente per il monitoraggio del router e frequentemente per le modifiche di configurazione del router. La versione 1 del protocollo, tuttavia, che è la più comune, rappresenta spesso un rischio per la protezione per i motivi riportati di seguito.

- Il protocollo utilizza stringhe di autenticazione (password), dette *stringhe di comunità*, che sono archiviate e inviate nella rete in testo normale.
- La maggior parte delle implementazioni SNMP inviano quelle stringhe ripetutamente come parte di un polling periodico.
- È un protocollo di transizione basato su datagrammi facilmente falsificabile.

Dal momento che SNMP può essere utilizzato per recuperare una copia della tabella di routing della rete e altre informazioni riservate sulla rete, se ne consiglia la disattivazione, se non è necessario. Security Audit richiede la disattivazione di SNMP all'inizio.

La configurazione che verrà trasmessa al router per disattivare SNMP è riportata di seguito:

```
no snmp-server
```

Imposta intervallo pianificazione

Security Audit consente di configurare l'intervallo di pianificazione nel router, quando possibile. Quando un router trasferisce rapidamente un gran numero di pacchetti, è possibile che impieghi così tanto tempo per rispondere agli interrupt provenienti dalla interfacce di rete da non poter eseguire altre operazioni. Alcuni flussi di pacchetti molto veloci possono causare questa condizione, rendendo possibile l'arresto dell'accesso amministrativo al router, che risulta molto pericoloso se il dispositivo subisce un attacco. La regolazione dell'intervallo pianificazione garantisce che l'accesso gestione al router è sempre disponibile, generando l'esecuzione di processi di sistema nel router dopo l'intervallo di tempo specificato, anche quando l'utilizzo della CPU è al massimo.

La configurazione che verrà trasmessa al router per regolare l'intervallo pianificazione è riportata di seguito:

```
scheduler interval 500
```

Imposta allocazione pianificazione

Nei router che non supportano il comando **scheduler interval**, Security Audit consente di configurare il comando **scheduler allocate**, quando possibile. Quando un router trasferisce rapidamente un gran numero di pacchetti, è possibile che impieghi così tanto tempo per rispondere agli interrupt provenienti dalla interfacce di rete da non poter eseguire altre operazioni. Alcuni flussi di pacchetti molto veloci possono causare questa condizione, rendendo possibile l'arresto dell'accesso amministrativo al router, che risulta molto pericoloso se il dispositivo subisce un attacco. Il comando **scheduler allocate** garantisce una percentuale di processi CPU del router per attività diverse dallo switching di rete, quali i processi di gestione.

La configurazione che verrà trasmessa al router per impostare la percentuale di allocazione pianificazione è riportata di seguito:

```
scheduler allocate 4000 1000
```

Imposta utenti

Security Audit consente di proteggere le linee console, AUX, vty e tty configurando account utente Telnet per autenticare l'accesso a queste linee, quando possibile. Security Audit visualizzerà una finestra di dialogo che consente di definire gli account e le password degli utenti per queste porte.

Attiva impostazioni Telnet

Security Audit consente di proteggere le linee console, AUX, vty e tty implementando le seguenti configurazioni, quando possibile:

- Configura i comandi **transport input** e **transport output** per definire quali protocolli si possono utilizzare per la connessione a queste reti.
- Imposta il valore exec-timeout su 10 minuti nelle linee console e AUX, causando la disconnessione di un utente amministrativo da queste linee dopo 10 minuti in cui non è stata registrata alcuna attività.

La configurazione che verrà trasmessa al router per proteggere le linee console, AUX, VTY e TTY è riportata di seguito:

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Attiva modalità NetFlow Switching

Security Audit attiva NetFlow Switching, quando possibile. NetFlow Switching è una funzionalità di Cisco IOS che potenzia le prestazioni routing durante l'utilizzo delle liste di controllo degli accessi (ACL) e altre funzionalità che creano e migliorano la protezione della rete. NetFlow identifica flussi di pacchetti di rete in base agli indirizzi IP di origine e di destinazione e ai numeri di porta TCP. Di conseguenza, è possibile utilizzare solo il pacchetto iniziale di un flusso per confrontarlo con le liste ACL e per altri controlli di protezione, piuttosto di dover utilizzare tutti i pacchetti nel flusso di rete. In questo modo le prestazioni sono migliorate, consentendo di utilizzare tutte le funzioni di protezione del router.

La configurazione che verrà trasmessa al router per attivare NetFlow è riportata di seguito:

```
ip route-cache flow
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva reindirizzamenti IP

Security Audit consente di disattivare i messaggi di reindirizzamento ICMP (Internet Message Control Protocol), quando possibile. ICMP supporta il traffico IP inoltrando informazioni sui percorsi, le route e le condizioni della rete. I messaggi reindirizzati ICMP sono impiegati per configurare i nodi terminali affinché utilizzino un router specifico per raggiungere una determinata destinazione. In una rete IP correttamente gestita, il router trasmette messaggi di questo tipo solo agli host appartenenti alle proprie subnet locali. Inoltre, nessun messaggio reindirizzato viene inviato dai nodi terminali né può transitare in più di un hop di rete. Tuttavia, violando queste regole, è possibile mettere a rischio i sistemi di protezione della rete. La disattivazione dei messaggi reindirizzati ICMP non comporta alcun impatto sulle prestazioni della rete e rappresenta un metodo efficace per eliminare questo tipo di rischio.

La configurazione che verrà trasmessa al router per disattivare i messaggi di reindirizzamento ICMP è riportata di seguito:

```
no ip redirects
```

Disattiva ARP proxy IP

Security Audit consente di disattivare proxy ARP (Address Resolution Protocol), quando possibile. Il protocollo ARP è utilizzato nelle reti per convertire gli indirizzi IP in indirizzi MAC. Di norma il protocollo ARP funziona in un'unica LAN. Tuttavia, se esiste un router che funziona da proxy per le richieste ARP, tali richieste possono essere effettuate anche fra più segmenti di LAN. Poiché questa soluzione rappresenta una violazione dei meccanismi di protezione delle LAN, i proxy ARP devono essere utilizzati solo fra due LAN aventi un uguale livello di protezione e solo se necessario.

La configurazione che verrà trasmessa al router per disattivare proxy ARP è riportata di seguito:

```
no ip proxy-arp
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva Broadcast IP

Security Audit consente di disattivare i broadcast IP, quando possibile. Un broadcast IP è un datagramma trasmesso all'indirizzo broadcast di una subnet alla quale il mittente non è connesso in modo diretto. Tale tipo di broadcast è instradato attraverso la rete come flusso di pacchetti unicast finché non arriva alla subnet di destinazione, dove viene convertito in un broadcast a livello di collegamento. A causa della natura dell'architettura degli indirizzamenti IP, solo l'ultimo router della catena, ovvero quello connesso direttamente alla subnet di destinazione, può identificare in modo definitivo un broadcast diretto. I broadcast diretti sono talvolta utilizzati per fini leciti ma ciò si verifica raramente al di fuori del settore dei servizi finanziari.

I broadcast IP sono utilizzati negli attacchi DoS di tipo smurf assai noti e diffusi e possono anche essere impiegati per altri attacchi dello stesso tipo. Gli attacchi di tipo smurf si basano sull'invio di richieste echo ICMP da un indirizzo mittente falsificato verso un indirizzo a broadcast diretto. Tutti gli host appartenenti alla subnet di destinazione reagiscono a tali richieste inviando una risposta al mittente falsificato. L'invio di un flusso continuo di richieste di questo tipo provoca un flusso di risposte ancora più intenso e in grado di inondare completamente l'host di cui è stato falsificato l'indirizzo.

Se si disattiva questa opzione, il broadcast IP, anziché essere convertito in broadcast a livello di collegamento quando raggiunge tale livello, viene invece scartato.

La configurazione che verrà trasmessa al router per disattivare i Broadcast IP è riportata di seguito:

```
no ip directed-broadcast
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva servizio MOP

Security Audit consente di disattivare MOP (Maintenance Operations Protocol) su tutte le interfacce Ethernet, quando possibile. Il protocollo è utilizzato per fornire informazioni sulla configurazione al router durante le comunicazioni con reti DECNet ed è vulnerabile a diversi attacchi.

La configurazione che verrà trasmessa al router per disattivare il servizio MOP sulle interfacce Ethernet è riportata di seguito:

```
no mop enabled
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva IP non raggiungibili

Security Audit consente di disattivare i messaggi ICMP (Internet Message Control Protocol) host non raggiungibili, quando possibile. ICMP supporta il traffico IP inoltrando informazioni sui percorsi, le route e le condizioni della rete. L'invio di messaggi di questo tipo avviene quando un router riceve un pacchetto di tipo nonbroadcast in cui si utilizza un protocollo sconosciuto oppure quando riceve un pacchetto che non è in grado di inoltrare poiché non conosce alcun percorso per raggiungere la destinazione finale. Di conseguenza, questi messaggi possono essere impropriamente utilizzati per ottenere illecitamente informazioni sulla mappatura della rete.

La configurazione che verrà trasmessa al router per disattivare i messaggi ICMP host non raggiungibili è riportata di seguito:

```
int <all-interfaces>
no ip unreachables
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva risposta maschera IP

Security Audit consente di disattivare i messaggi di risposta maschera ICMP (Internet Message Control Protocol), quando possibile. ICMP supporta il traffico IP inoltrando informazioni sui percorsi, le route e le condizioni della rete. I messaggi di risposta maschera ICMP si utilizzano quando occorre comunicare a un dispositivo di rete la subnet mask di una determinata subnet della rete. I messaggi sono inviati da dispositivi di rete che sono a conoscenza di tali informazioni. Di conseguenza, questi messaggi possono essere impropriamente utilizzati per ottenere illecitamente informazioni sulla mappatura della rete.

La configurazione che verrà trasmessa al router per disattivare i messaggi di risposta maschera ICMP è riportata di seguito:

```
no ip mask-reply
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Disattiva IP non raggiungibili su interfacce NULL

Security Audit consente di disattivare i messaggi ICMP (Internet Message Control Protocol) host non raggiungibili, quando possibile. ICMP supporta il traffico IP inoltrando informazioni sui percorsi, le route e le condizioni della rete. L'invio di messaggi di questo tipo avviene quando un router riceve un pacchetto di tipo nonbroadcast in cui si utilizza un protocollo sconosciuto oppure quando riceve un pacchetto che non è in grado di inoltrare poiché non conosce alcun percorso per raggiungere la destinazione finale. Dal momento che l'interfaccia NULL è un raccoglitore di pacchetti inutilizzabili, i pacchetti inoltrati a questa interfaccia verranno sempre annullati e, se non disattivata, genererà messaggi host non raggiungibili. In tal caso, se l'interfaccia NULL è utilizzata per bloccare un attacco DoS, questi messaggi congestionano la rete locale. La disattivazione di questi messaggi evita una situazione simile. Inoltre, poiché tutti i pacchetti bloccati sono inoltrati all'interfaccia NULL, un utente malintenzionato che riceve messaggi host non raggiungibili potrebbe utilizzare questi pacchetti per determinare la configurazione della lista di controllo degli accessi (ACL).

Se nel router è configurata l'interfaccia “NULL 0”, Security Audit trasmetterà la configurazione riportata di seguito al router, per disattivare i messaggi ICMP host non raggiungibili per i pacchetti annullati o per i pacchetti instradati all'interfaccia NULL, nel modo seguente:

```
int null 0
no ip unreachables
```

Questa correzione può essere annullata. Per informazioni sulla modalità fare clic su Annullamento delle correzioni di Security Audit.

Attiva Unicast RPF su tutte le interfacce esterne

Security Audit consente di attivare l'inoltro del percorso inverso unicast (RPF) su tutte le interfacce connesse a Internet, quando possibile. RPF è una funzionalità con la quale il router è in grado di controllare l'indirizzo di origine di qualsiasi pacchetto sulla base dell'interfaccia attraverso la quale il pacchetto ha raggiunto il router. Se l'interfaccia di input non è un percorso possibile dell'indirizzo origine in base alla tabella di routing, il pacchetto verrà eliminato. La verifica dell'indirizzo di origine è utilizzata per superare lo spoofing IP.

Questa funzionalità è consentita solo quando il routing è simmetrico. Se la rete è progettata in modo che il traffico dall'host A all'host B possa prendere un percorso diverso dal traffico dall'host B all'host A, il controllo avrà sempre esito negativo e la comunicazione tra i due host non sarà possibile. Questo tipo di routing asimmetrico è comune nella struttura di base di Internet. Assicurarsi che la rete non utilizzi un routing asimmetrico prima di attivare questa funzionalità.

Inoltre, Unicast RPF può essere attivato solo quando IP CEF (Cisco Express Forwarding) è attivato. Security Audit consentirà di verificare la configurazione del router per vedere se IP CEF è attivato. In caso contrario, Security Audit ne consiglia l'attivazione e attiverà la funzionalità quando il consiglio viene accettato. Se IP CEF non è attivato tramite Security Audit o altro modo, Unicast RPF non verrà attivato.

Per attivare Unicast RPF, la configurazione riportata di seguito verrà trasmessa al router per ogni interfaccia connessa all'esterno della rete privata, sostituendo *<outside interface>* con l'identificatore di interfaccia:

```
interface <outside interface>
ip verify unicast reverse-path
```

Attiva firewall su tutte le interfacce esterne

Se l'immagine Cisco IOS in esecuzione sul router include il set di funzioni Firewall, Security Audit consentirà l'attivazione di CBAC (Context-Based Access Control) nel router, quando possibile. CBAC, un componente del set di funzioni Firewall di Cisco IOS, consente di filtrare i pacchetti in base alle informazioni a livello di applicazione. Tali informazioni possono riguardare i tipi di comandi che vengono eseguiti all'interno della sessione. Ad esempio, se nella sessione viene rilevato un comando che non è supportato, al pacchetto può essere negato l'accesso.

CBAC consente di migliorare la protezione delle applicazioni TCP e UDP (User Datagram Protocol) che utilizzano porte conosciute, come la porta 80 per HTTP o la porta 443 per SSL (Secure Sockets Layer). L'operazione viene eseguita analizzando dettagliatamente gli indirizzi di origine e di destinazione. Senza il componente CBAC, il traffico di applicazioni avanzate è consentito solo scrivendo liste di controllo degli accessi (ACL). Questo approccio lascia le porte firewall aperte, in questo modo la maggior parte degli amministratori tende a negare tutto il traffico dell'applicazione. Con CBAC attivato, tuttavia, è possibile permettere il traffico multimediale e di altre applicazioni in maniera protetta aprendo il firewall quando necessario e chiudendolo in tutte le altre occasioni.

Per attivare CBAC, in Security Audit verranno utilizzate le schermate Crea firewall di Cisco SDM per generare una configurazione firewall.

Imposta classe di accesso per il servizio server HTTP

Security Audit consente di attivare il servizio HTTP nel router con una classe di accesso, quando possibile. Il servizio HTTP consente la configurazione remota e il monitoraggio mediante un browser Web, ma è limitato in termini di protezione in quanto invia una password in testo non codificato nella rete durante il processo di autenticazione. Per questo motivo, Security Audit limita l'accesso a questo servizio configurando una classe che consente l'accesso solo dai nodi di rete connessi direttamente.

La configurazione che verrà trasmessa al router per attivare il servizio HTTP con una classe di accesso è riportata di seguito:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Imposta classe di accesso sulle linee VTY

Security Audit consente di configurare una classe di accesso per le linee vty, quando possibile. Poiché le connessioni vty permettono l'accesso remoto al router, dovrebbero essere limitate solo ai nodi di rete conosciuti.

La configurazione che verrà trasmessa al router per configurare una classe di accesso per le reti vty è riportata di seguito:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Inoltre, a ogni linea vty, verrà applicata la seguente configurazione:

```
access-class <std-acl-num>
```

Attiva SSH per l'accesso al router

Se l'immagine Cisco IOS in esecuzione nel router è un'immagine crittografica (un'immagine che utilizza la crittografia DES a 56 bit ed è soggetta a limitazioni di esportazione), Security Audit consentirà di implementare le configurazioni riportate di seguito per proteggere l'accesso Telnet, quando possibile:

- Attivare SSH (Enable Secure Shell) per l'accesso Telnet. SSH consente una maggiore protezione all'accesso Telnet.
- Impostare il valore di timeout di SSH a 60 secondi, in questo modo le connessioni SSH incomplete verranno interrotte dopo 60 secondi.
- Impostare il numero massimo di tentativi di accesso SSH non riusciti a due prima di bloccare l'accesso al router.

La configurazione che verrà trasmessa al router per proteggere le funzioni di accesso e di trasferimento file è riportata di seguito:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Nota Una volta apportate le modifiche sopra indicate, è necessario specificare la dimensione della chiave del modulo SSH e generare la chiave. Per eseguire l'operazione, utilizzare la pagina SSH.

Attiva AAA

AAA, acronimo di Authentication, Authorization, and Accounting, di Cisco IOS è uno schema di architettura per configurare in modo coerente un set di tre funzioni di protezione indipendenti. Esso esegue i servizi di autenticazione, autorizzazione e accounting in modo modulare.

Per evitare di non riuscire più ad accedere al router, Cisco SDM esegue le seguenti attività precauzionali durante l'abilitazione dell'AAA:

- Configurare l'autenticazione e l'autorizzazione per le linee VTY

  Per l'autenticazione e l'autorizzazione verrà utilizzato il database locale.

- Configurare l'autenticazione per la console

  Per l'autenticazione verrà usato il database locale.

- Modificare l'autenticazione HTTP per utilizzare il database locale

Schermata di riepilogo della configurazione

In questa schermata viene visualizzato un elenco di tutte le modifiche di configurazione che verranno trasmesse alla configurazione del router, in base ai problemi di protezione selezionati per la correzione nella schermata Scheda report.

Cisco SDM e Cisco IOS AutoSecure

AutoSecure è una funzionalità di Cisco IOS che, come Cisco SDM, consente una configurazione più semplice delle funzionalità di protezione nel router, in modo da fornire alla rete una protezione migliore. Cisco SDM implementa quasi tutte le configurazioni supportate da AutoSecure.

Funzionalità AutoSecure implementate in Cisco SDM

Le funzionalità AutoSecure elencate di seguito sono implementate in questa versione di Cisco SDM. Per una spiegazione di questi servizi e delle funzionalità, fare clic sui seguenti collegamenti:

- Disattiva SNMP
- Disattiva servizio Finger
- Disattiva servizio PAD
- Disattiva il servizio TCP Small Servers
- Disattiva servizio server BOOTP IP

- Disattiva servizio identificazione IP
- Disattiva CDP
- Disattiva route di origine IP
- Disattiva reindirizzamenti IP
- Disattiva ARP proxy IP
- Disattiva Broadcast IP
- Disattiva servizio MOP
- Disattiva IP non raggiungibili
- Disattiva IP non raggiungibili su interfacce NULL
- Disattiva risposta maschera IP
- Attiva servizio di crittografia password
- Disattiva IP non raggiungibili su interfacce NULL
- Disattiva IP non raggiungibili su interfacce NULL
- Imposta la lunghezza minima della password a meno di 6 caratteri
- Attiva IP CEF
- Attiva firewall su tutte le interfacce esterne
- Imposta utenti
- Attivazione della registrazione
- Attiva firewall su tutte le interfacce esterne
- Imposta la lunghezza minima della password a meno di 6 caratteri
- Attiva firewall su tutte le interfacce esterne
- Imposta utenti
- Imposta utenti
- Imposta utenti
- Attiva Unicast RPF su tutte le interfacce esterne
- Attiva firewall su tutte le interfacce esterne

Funzionalità AutoSecure non implementate in Cisco SDM

Le funzionalità AutoSecure elencate di seguito non sono implementate in questa versione di Cisco SDM.

- Disattivazione di NTP: in base all'input, AutoSecure consentirà di disattivare il protocollo NPT (Network Time Protocol), se non è necessario. In caso contrario, NPT verrà configurato con l'autenticazione MD5. Cisco SDM non supporta la disattivazione di questo protocollo.
- Configurazione di AAA: se il servizio AAA (Authentication, Authorization, and Accounting) non è configurato, AutoSecure ne consente la configurazione locale e richiede la configurazione di un database di nome utente e password locale nel router. Cisco SDM non supporta la configurazione di AAA.
- Impostazione dei valori SPD: Cisco SDM non consente l'impostazione dei valori SPD (Selective Packet Discard).
- Attivazione di TCP Intercept: Cisco SDM non consente l'attivazione di TCP Intercept.
- Configurazione di ACL anti-spoofing su interfacce esterne: AutoSecure consente di creare tre elenchi di accesso denominati, utilizzati per impedire indirizzi origine anti-spoofing. Cisco SDM non supporta la configurazione di queste ACL.

Funzionalità AutoSecure implementate diversamente in Cisco SDM

- Disattiva SNMP: Cisco SDM consentirà di disattivare SNMP ma, diversamente da AutoSecure, non fornisce un'opzione per configurare la versione 3 di SNMP.
- Attiva SSH per l'accesso al router: Cisco SDM consentirà di attivare e configurare SSH sulle immagini crittografate di Cisco IOS ma, diversamente da AutoSecure, non permetterà l'attivazione di SCP (Service Control Point) o la disattivazione di altri servizi di accesso e di trasferimento file, ad esempio FTP.

Configurazioni di protezione annullabili in Cisco SDM

Nella tabella sono elencate le configurazioni di protezione che possono essere annullate da Cisco SDM.

Configurazione protezione	Interfaccia CLI equivalente
Disattiva servizio Finger	No service finger
Disattiva servizio PAD	No service pad
Disattiva il servizio TCP Small Servers	No service tcp-small-servers no service udp-small-servers
Disattiva servizio server BOOTP IP	No ip bootp server
Disattiva servizio identificazione IP	No ip identd
Disattiva CDP	No cdp run
Disattiva route di origine IP	No ip source-route
Attiva modalità NetFlow Switching	ip route-cache flow
Disattiva reindirizzamenti IP	no ip redirects
Disattiva ARP proxy IP	no ip proxy-arp
Disattiva Broadcast IP	no ip directed-broadcast
Disattiva servizio MOP	No mop enabled
Disattiva IP non raggiungibili	int <all-interfaces> no ip unreachables
Disattiva risposta maschera IP	no ip mask-reply
Disattiva IP non raggiungibili su interfacce NULL	int null 0 no ip unreachables
Attiva servizio di crittografia password	service password-encryption
Attiva TCP Keepalive per le sessioni telnet in ingresso	service tcp-keepalives-in
Attiva TCP Keepalive per le sessioni telnet in uscita	service tcp-keepalives-out
Disattiva ARP gratuiti IP	no ip gratuitous arps

Annullamento delle correzioni di Security Audit

Cisco SDM consente di annullare la correzione di questa protezione. Se si desidera che Cisco SDM rimuova questa configurazione di protezione, eseguire la procedura guidata di Security Audit. Nella finestra Scheda report, selezionare l'opzione **Annulla configurazioni di protezione**, porre un segno di spunta accanto a questa configurazione e ad altre configurazioni che si desidera annullare e fare clic su **Avanti>**.

Schermata Aggiungi o modifica account Telnet/SSH

Questa schermata consente di aggiungere un nuovo account utente o di modificare un account utente esistente per l'accesso Telnet e SSH al router.

Nome utente

Immettere il nome utente per il nuovo account in questo campo.

Password

Immettere la password per il nuovo account in questo campo.

Conferma password

Reimmettere la password del nuovo account in questo campo per la conferma. La voce in questo campo deve corrispondere a quella nel campo della password.

Pagina Configurare gli account utente per l'accesso a Telnet/SSH

Questa schermata consente di gestire gli account utente che dispongono dell'accesso Telnet o SSH (Secure Shell) al router. La tabella riportata in questa schermata visualizza ogni account utente Telnet, elencando il nome utente dell'account e visualizzando asterischi per rappresentare la password dell'account. Si noti che questa schermata viene visualizzata solo se non è già stato configurato alcun account utente; pertanto la tabella nella schermata è sempre vuota quando viene visualizzata all'inizio.

Casella di controllo Attiva autorizzazione per telnet

Selezionare questa casella per attivare l'accesso Telnet e SSH al router. Deselezionare questa casella per disattivare l'accesso Telnet e SSH al router.

Pulsante Verifica tunnel...

Fare clic su questo pulsante per visualizzare la schermata Aggiungi account utente che consente di aggiungere un account assegnandogli un nome utente e una password.

Pulsante Verifica tunnel...

Fare clic su un account utente nella tabella per selezionarlo e fare clic su questo pulsante per visualizzare la schermata Modifica account utente che consente di modificare il nome utente e la password dell'account selezionato.

Pulsante Elimina

Fare clic su un account utente nella tabella per selezionarlo e fare clic su questo pulsante per eliminare l'account selezionato.

Pagina Attiva password crittografata e Banner

In questa schermata è possibile immettere una nuova password crittografata e un testo del banner per il router.

La password crittografata è una password che fornisce l'accesso a livello amministratore a tutte le funzioni del router. È di essenziale importanza che la password crittografata sia protetta e difficile da forzare. La lunghezza minima deve essere di sei caratteri; si consiglia di includere sia caratteri alfabetici che numerici, e di non utilizzare una parola che possa essere trovata in un dizionario, o che potrebbe essere un'informazione personale che qualcuno potrebbe essere in grado di scoprire.

Il testo per il banner verrà visualizzato ogni volta che un utente si connette al router tramite Telnet o SSH. Il testo del banner è un importante fattore di protezione in quanto è un metodo per notificare agli utenti non autorizzati che l'accesso al router è vietato. In alcune legislazioni, tale azione è perseguibile civilmente e/o penalmente.

Nuova password

Immettere la nuova password crittografata in questo campo.

Reimmettere la nuova password

Reimmettere la nuova password crittografata in questo campo per la verifica.

Banner accesso

Immettere il testo del banner che si desidera configurare nel router.

Pagina di registrazione

In questa schermata è possibile configurare il registro del router creando un elenco di server syslog a cui devono essere inoltrati i messaggi del registro, e impostando il livello di registrazione che determina la gravità minima che deve avere un tale messaggio perché venga acquisito.

Tabella Indirizzo IP/nome host

In questa tabella viene visualizzato un elenco di host a cui inoltrare i messaggi di registro del router. Questi host devono essere server syslog che possono acquisire e gestire i messaggi di registro del router.

Pulsante Verifica tunnel...

Fare clic su questo pulsante per visualizzare la schermata Indirizzo IP/Nome host che consente di aggiungere un server syslog all'elenco immettendo il relativo indirizzo IP o il nome host.

Pulsante Verifica tunnel...

Fare clic su un server syslog nella tabella per selezionarlo e fare clic su questo pulsante per visualizzare la schermata Indirizzo IP/Nome host che consente di modificare l'indirizzo IP o il nome host del server syslog selezionato.

Pulsante Elimina

Fare clic su un server syslog nella tabella per selezionarlo e fare clic su questo pulsante per eliminare il server syslog dalla tabella.

Campo Impostazione livello registrazione

In questo campo, selezionare il livello minimo di gravità in base al quale un messaggio di registro del router venga acquisito e inoltrato ai server syslog nella tabella in questa schermata. Il livello di gravità di un messaggio di registro viene visualizzato sotto forma di numero da 1 a 7, con i numeri più bassi utilizzati per indicare gli eventi più gravi. Di seguito viene fornita la descrizione dei livelli di gravità.

- 0: emergenze

  Sistema inutilizzabile

- 1: avvisi

  È necessaria un'azione immediata

- 2: critico

  Condizioni critiche

- 3: errori

  Condizioni di errore

- 4: avvertenze

  Condizioni di avvertenza

- 5: notifiche

  Condizione normale ma significativa

- 6: informativo

  Messaggio unicamente informativo

- 7: debug

  Messaggi di debug

CAPITOLO 22

Routing

Nella finestra Routing vengono visualizzate le route statiche configurate, e le route configurate dei protocolli RIP (Routing Internet Protocol), OSPF (Open Shortest Path First) ed EIGRP (Extended Interior Gateway Routing Protocol). Da questa finestra è possibile rivedere le route, aggiungerne altre, modificare quelle esistenti ed eliminarle.

Nota In questa finestra verranno visualizzate le route statiche e dinamiche configurate per i tunnel GRE su IPSec. Se si elimina una voce di routing utilizzata per il tunnel GRE su IPSec in questa finestra, la route non sarà più disponibile per il tunnel.

Routing statico

Rete di destinazione

Si tratta della rete a cui la route statica fornisce un percorso.

Inoltro

Si tratta dell'interfaccia o dell'Indirizzo IP attraverso cui i pacchetti devono essere inviati per raggiungere la rete di destinazione.

Opzionale

In quest'area viene indicato se l'unità di misura distanza è stata immessa e se la route è designata come permanente.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di una route statica	Fare clic su **Aggiungi** e creare la route statica finestra Route statica.
Modifica di una route statica.	Selezionare la route statica e fare clic su **Modifica**. Modificare le informazioni relative alla route nella finestra Route statica IP. Se una route configurata non è supportata da SDM, il pulsante Modifica è disattivato.
Eliminazione di una route statica.	Selezionare la route statica e fare clic su **Elimina**. Quindi, confermare l'eliminazione nel messaggio di avviso visualizzato.
Eliminazione di tutte le route statiche.	Fare clic su **Elimina tutto**. Quindi, confermare l'eliminazione nel messaggio di avviso visualizzato.

Nota

- Se viene rilevata una voce di route statica precedentemente configurata e con l'interfaccia per l'hop successivo configurata come “Null”, la voce di route statica sarà di sola lettura.
- Se viene rilevata una voce di route statica precedentemente configurata con le opzioni “tag” o “nome”, la voce sarà di sola lettura.
- Se si sta configurando un router Cisco 7000 e l'interfaccia utilizzata per l'hop successivo non è supportata, la route sarà di sola lettura.
- Le voci di sola lettura non possono essere modificate o eliminate con SDM.

Routing dinamico

In questa parte della finestra è possibile configurare le route dinamiche RIP, OSPF e EIGRP.

Nome elemento

Se non è stata configurata nessuna route dinamica, in questa colonna verrà visualizzato il testo RIP, OSPF e EIGRP Se sono state configurate una o più route, nella colonna saranno elencati i nomi dei parametri per il tipo di routing configurato.

Protocollo di routing	Parametri della configurazione
RIP	Versione RIP, rete, interfaccia passiva
OSPF	ID processo
EIGRP	Numero sistema autonomo

Valore elemento

In questa colonna vengono visualizzati la scritta “Attivato” e i valori della configurazione se è stato configurato un tipo di routing. Viene invece visualizzata la scritta “Disattivato” se non è stato configurato alcun protocollo di routing.

Tabella riassuntiva funzioni

Funzione	Procedura
Configurazione di una route RIP.	Selezionare la scheda RIP e fare clic su **Modifica**. Quindi, configurare la route nella finestra Route dinamica RIP.
Configurazione di una route OSPF.	Selezionare la scheda OSPF e fare clic su **Modifica**. Quindi, configurare la route nella finestra visualizzata.
Configurazione di una route EIGRP.	Selezionare la scheda EIGRP e fare clic su **Modifica**. Quindi, configurare la route nella finestra visualizzata.

Aggiungi o Modifica IP route statica

Utilizzare questa finestra per aggiungere o modificare una route statica.

Rete di destinazione

Immettere le informazioni sull'indirizzo della rete di destinazione in questi campi.

Prefisso

Immettere l'indirizzo IP della rete di destinazione. Per maggiori informazioni vedere Configurazioni delle interfacce disponibili.

Maschera prefisso

Immettere la subnet mask per l'indirizzo di destinazione.

Impostazione come route predefinita

Selezionare questa casella per impostare questa route come predefinita. Una route predefinita consente di inoltrare tutti i pacchetti sconosciuti in uscita attraverso questa route.

Inoltro

Specificare come inoltrare i dati alla rete di destinazione.

Interfaccia

Fare clic su **Interfaccia** per selezionare l'interfaccia del router che consente di inoltrare il pacchetto alla rete remota.

Indirizzo IP

Fare clic su **Indirizzo IP** per immettere l'indirizzo IP del successivo hop del router che consente di ricevere e di inoltrare il pacchetto alla rete remota.

Opzionale

È possibile fornire un'unità di misura distanza per questa route e indicarla come route permanente.

Unità di misura distanza route

Immettere il valore della distanza da registrare nella tabella di routing. I valori validi sono compresi tra 1 e 255.

Route permanente

Selezionare questa casella per impostare questa voce di route statica come permanente. Le route permanenti non vengono eliminate anche se l'interfaccia viene chiusa o se il router non consente la comunicazione con il router successivo.

Aggiungi o Modifica route RIP

Utilizzare la finestra per aggiungere o modificare una route RIP (Routing Internet Protocol).

Versione RIP

I valori sono versione RIP 1, versione RIP 2 e Impostazione predefinita. Selezionare la versione supportata dall'immagine Cisco IOS in esecuzione sul router. Se si seleziona la versione 1, il router consente di inviare i pacchetti RIP versione 1 e di ricevere i pacchetti versione 1. Se si seleziona la versione 2, il router consente di inviare i pacchetti RIP versione 2 e di ricevere i pacchetti versione 2. Se si seleziona Impostazione predefinita, il router consente di inviare i pacchetti versione 1 e di ricevere i pacchetti versione 1 e versione 2.

Elenco reti IP

Immettere le reti in cui attivare RIP. Fare clic su **Aggiungi** per aggiungere una rete. Fare clic su **Elimina** per eliminare una rete dall'elenco.

Elenco interfacce disponibili

In questo elenco sono visualizzate le interfacce disponibili.

Rendere l'interfaccia passiva

Selezionare la casella vicina all'interfaccia se non si desidera inviare aggiornamenti a quelle successive. L'interfaccia riceverà comunque gli aggiornamenti del routing.

Add or Edit an OSPF Route

Utilizzare la finestra per aggiungere o modificare una route OSPF (Open Shortest Path First).

ID processo OSPF

Questo campo può essere modificato dopo aver attivato OSPF ed è disattivato quando il routing OSPF viene attivato. L'ID processo consente di identificare il processo di routing OSPF del router verso altri router.

Elenco reti IP

Immettere le reti per le quali si desidera creare delle route. Fare clic su **Aggiungi** per aggiungere una rete. Fare clic su **Elimina** per eliminare una rete dall'elenco.

Rete

L'indirizzo della rete di destinazione per questa route. Per maggiori informazioni vedere Configurazioni delle interfacce disponibili.

Maschera

La subnet mask utilizzata nella rete.

Area

Il numero dell'area OSPF per la rete. Ogni router di una particolare area OSPF mantiene un database topologico per quell'area.

Nota Se viene rilevato un routing OSPF precedentemente configurato che include comandi “area”, la tabella Elenco reti IP sarà di sola lettura e non potrà essere modificata.

Elenco interfacce disponibili

In questo elenco sono visualizzate le interfacce disponibili.

Rendere l'interfaccia passiva

Selezionare la casella vicina all'interfaccia se non si desidera inviare aggiornamenti a quelle successive. L'interfaccia riceverà comunque gli aggiornamenti del routing.

Aggiungi

Fare clic su **Aggiungi** per fornire un indirizzo IP, una maschera di rete e un numero di area nella finestra Indirizzo IP.

Modifica

Fare clic su **Modifica** per modificare un indirizzo IP, una maschera di rete e un numero di area nella finestra Indirizzo IP.

Add or Edit EIGRP Route

Utilizzare questa finestra per aggiungere o eliminare una route EIGRP (Extended IGRP).

Numero sistema autonomo

Il numero di sistema autonomo viene utilizzato per identificare il processo di routing EIGRP del router verso altri router.

Elenco reti IP

Immettere le reti per le quali si desidera creare delle route. Fare clic su **Aggiungi** per aggiungere una rete. Fare clic su **Elimina** per eliminare una rete dall'elenco.

Elenco interfacce disponibili

In questo elenco sono visualizzate le interfacce disponibili.

Rendere l'interfaccia passiva

Selezionare la casella vicina all'interfaccia se non si desidera inviare aggiornamenti a quelle successive. L'interfaccia non riceverà e non invierà aggiornamenti routing.

Precauzione Se si rende un'interfaccia passiva, EIGRP elimina lo scambio dei pacchetti Hello tra i router comportando la perdita della relazione con quelli successivi. Questa azione non solo blocca la notifica degli aggiornamenti routing, ma elimina anche gli aggiornamenti routing in ingresso.

Aggiungi

Fare clic su **Aggiungi** per aggiungere un indirizzo IP della rete di destinazione all'elenco reti.

Elimina

Selezionare un indirizzo IP e fare clic su **Elimina per rimuovere un indirizzo IP** dall'elenco reti.

CAPITOLO 23

Network Address Translation

NAT, acronimo di Network Address Translation, è un formato trusted di conversione indirizzi che estende la capacità di indirizzamento fornendo sia conversioni di indirizzi statici, sia conversioni di indirizzi dinamici. NAT consente a un host, che non dispone di un indirizzo IP registrato valido, di comunicare con altri host tramite Internet. Gli host possono utilizzare indirizzi privati o indirizzi assegnati a un'altra azienda; in entrambi i casi, NAT consente di continuare a utilizzare questi indirizzi, che non sono pronti per il collegamento a Internet, ma sono in grado di comunicare con host via Internet.

Procedure guidate di traduzione degli indirizzi di rete

Per la creazione di una regola NAT (Network Address Translation) si può utilizzare una procedura guidata. Scegliere una delle seguenti procedure guidate:

- NAT di base

  Scegliere la procedura guidata NAT di base se si vuole connettere la propria rete ad Internet (o all'esterno) e la propria rete dispone di client ma non di server. Osservare il diagramma d'esempio visualizzato sulla destra quando si sceglie **NAT di base**. Se la propria rete è composta soltanto da PC che necessitano di un accesso ad Internet, scegliere **NAT di base** e fare clic sul pulsante **Avvia**.

- NAT avanzato

  Scegliere la procedura guidata NAT avanzato quando si vuole connettere la propria rete ad Internet (o all'esterno) *e* permettere ai propri server di risultare accessibili da host esterni (host in internet). Osservare il diagramma d'esempio visualizzato sulla destra quando si sceglie **NAT avanzato**. Se la propria rete comprende server e-mail, server web o altri tipi di server e si desidera che essi accettino le connessioni provenienti da Internet, scegliere **NAT avanzato** e fare clic sul pulsante **Avvia**.

Nota Se non si vuole che i propri server accettino connessioni da Internet, è possibile utilizzare la procedura guidata NAT di base.

Configurazione guidata NAT di base: Pagina iniziale

La finestra d'introduzione NAT di base mostra in che modo funziona la configurazione guidata per la connessione ad Internet di una o più LAN senza server.

Configurazione guidata NAT di base: connessione

Scegliere un'interfaccia

Dal menu a tendina scegliere l'interfaccia che si collega ad Internet. Questa è l'interfaccia WAN del router.

Scegliere le reti

L'elenco delle reti disponibili mostra le reti collegate al proprio router. Scegliere quali reti condivideranno l'interfaccia WAN nella configurazione NAT che si imposta. Per scegliere una rete selezionare la casella di controllo corrispondente nella lista delle reti disponibili.

Nota Non scegliere una rete connessa all'interfaccia WAN che viene impostata con questa configurazione NAT. Rimuovere tale rete dalla configurazione NAT deselezionando la casella di controllo corrispondente.

L'elenco visualizza le seguenti informazioni per ciascuna rete:

- Gamma di indirizzi IP assegnati alla rete
- Interfaccia LAN di rete
- Commenti immessi sulla rete

Per rimuovere una rete dalla configurazione NAT deselezionare la casella di controllo corrispondente.

Nota Se in Cisco SDM viene rilevato un conflitto tra la configurazione NAT e una configurazione VPN esistente per l'interfaccia WAN, quando l'utente fa clic su **Avanti** viene visualizzata una finestra di dialogo di avvertimento.

Riepilogo

Questa finestra mostra la configurazione NAT creata e consente di salvare la configurazione. Il riepilogo sarà simile al seguente:

```
Interfaccia connessa a Internet o al proprio fornitore di servizi
Internet:
    FastEthernet0/0

Intervalli di indirizzi IP che condividono la connessione a Internet:
    Da 108.1.1.0 a 108.1.1.255
    Da 87.1.1.0 a 87.1.1.255
    Da 12.1.1.0 a 12.1.1.255
    Da 10.20.20.0 a 10.20.20.255
```

Se si è utilizzata la configurazione guidata NAT avanzato, sarà anche possibile vedere informazioni simili alle seguenti:

```
Regole NAT per i server:
    Traduci TCP 10.10.10.19 TCP porta 6080 in un indirizzo IP
dell'interfaccia FastEthernet0/0 TCP porta 80
    Traduci TCP 10.10.10.20 TCP porta 25 in 194.23.8.1 TCP porta 25
```

Configurazione guidata NAT avanzato: Pagina iniziale

La finestra d'introduzione NAT avanzato mostra in che modo funziona la configurazione guidata per la connessione ad Internet delle proprie LAN e dei propri server.

Configurazione guidata NAT avanzato: connessione

Scegliere un'interfaccia

Dal menu a tendina scegliere l'interfaccia che si collega ad Internet. Questa è l'interfaccia WAN del router.

Indirizzi IP pubblici aggiuntivi

Fare clic su **Aggiungi** per immettere gli indirizzi IP pubblici di propria proprietà. Tali indirizzi IP potranno essere assegnati ai server della propria rete che si desiderano rendere disponibili su Internet.

Per eliminare un indirizzo IP dall'elenco, selezionare tale indirizzo e fare clic sul pulsante **Elimina**.

Aggiungi indirizzo IP

Immettere un indirizzo IP di propria proprietà. Tali indirizzi IP potranno essere assegnati ai server della propria rete che si desidera rendere disponibili su Internet.

Configurazione guidata NAT avanzato: reti

Scegliere le reti

L'elenco delle reti disponibili mostra le reti collegate al proprio router. Scegliere quali reti condivideranno l'interfaccia WAN nella configurazione NAT che si imposta. Per scegliere una rete selezionare la casella di controllo corrispondente nella lista delle reti disponibili.

Nota Non scegliere una rete connessa all'interfaccia WAN che viene impostata con questa configurazione NAT. Rimuovere tale rete dalla configurazione NAT deselezionando la casella di controllo corrispondente.

L'elenco visualizza le seguenti informazioni per ciascuna rete:

- Gamma di indirizzi IP assegnati alla rete
- Interfaccia LAN di rete
- Commenti immessi sulla rete

Per rimuovere una rete dalla configurazione NAT deselezionare la casella di controllo corrispondente.

Per aggiungere alla lista una rete non direttamente connessa al proprio router, fare clic su **Aggiungi network**.

Nota Se Cisco SDM non consente di selezionare la casella di controllo accanto ad una rete per cui si desidera configurare una regola NAT significa che l'interfaccia associata a tale rete è stata già designata come interfaccia NAT. Questo stato sarà indicato dalla parola *Designata* nella colonna Commenti. Se si desidera configurare una regola NAT per tale interfaccia, uscire dalla procedura guidata, fare clic su **Modifica NAT**, fare clic su **Indica interfacce NAT** e deselezionare l'interfaccia. Quindi tornare alla procedura per configurare la regola NAT.

Aggiungi rete

Si può aggiungere una rete alla lista delle reti rese disponibili nella procedura guidata NAT avanzato. È necessario disporre dell'indirizzo IP e della subnet mask della rete. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Indirizzo IP

Immettere l'indirizzo IP di rete.

Subnet Mask

Immettere la subnet mask in questo campo o scegliere il numero di bit dal campo a scorrevole sulla destra. Mediante la subnet mask il router è in grado di stabilire quali bit dell'indirizzo IP definiscono l'indirizzo di rete e quali bit definiscono invece l'indirizzo host.

Configurazione guidata NAT avanzato: Indirizzi IP pubblici del server

Questa finestra consente di convertire gli indirizzi IP pubblici negli indirizzi privati dei server interni che si desidera rendere disponibili su Internet.

Questa lista elenca porte (se utilizzate) e indirizzi IP privati, e porte (se utilizzate) e indirizzi convertiti corrispondenti.

Per modificare l'ordine dell'elenco sulla base degli indirizzi IP privati, fare clic sull'intestazione di colonna **Indirizzo IP privato**. Per modificare l'ordine dell'elenco sulla base degli indirizzi pubblici, fare clic sull'intestazione di colonna **Indirizzo IP pubblico**.

Pulsante Aggiungi

Per aggiungere una regola di traduzione per il server, fare clic su **Aggiungi**.

Pulsante Modifica

Per modificare una regola di traduzione per il server, selezionarla nell'elenco e fare clic su **Modifica**.

Pulsante Elimina

Per cancellare una regola di traduzione, selezionarla nell'elenco e fare clic su **Elimina**.

Aggiungi o Modifica regola di traduzione

In questa finestra è possibile immettere o modificare le informazioni di traduzione dell'indirizzo IP per un server.

Indirizzo IP privato

Immettere l'indirizzo IP che il server utilizza nella rete interna. Questo è un indirizzo IP che non può essere utilizzato esternamente su Internet.

Indirizzo IP pubblico

Dal menu a tendina, scegliere gli indirizzi IP pubblici nei quali l'indirizzo IP privato del server verrà convertito. Gli indirizzi IP che compaiono nel menu a tendina includono l'indirizzo IP del router dell'interfaccia WAN e qualsiasi indirizzo IP pubblico posseduto immesso nella finestra delle connessioni (vedere Configurazione guidata NAT avanzato: connessione).

Tipo di server

Scegliere uno dei seguenti tipi di server dal menu a tendina:

- Server Web

  Un host HTTP che serve pagine HTML o altre per il WWW.

- Server E-mail

  Un server SMTP per l'invio di posta Internet.

- Altro

  Un server che non è un server web o e-mail, ma che richiede la traduzione delle porte per la fornitura del servizio. Questa scelta attiva il campo Porta tradotta e il menu a tendina Protocollo.

Se non si sceglie un tipo di server tutto il traffico diretto agli all'IP pubblico scelto per il server sarà instradato su tale indirizzo e non verrà effettuata alcuna traduzione delle porte.

Porta originale

Immettere il numero di porta usato dal server per accettare le richieste dalla rete interna.

Porta tradotta

Immettere il numero di porta usato dal server per accettare le richieste di servizio da Internet.

Protocollo

Scegliere **TCP** o **UDP** per il protocollo utilizzato dal server con le porte originali e le porte convertite.

Configurazione guidata NAT avanzato: conflitto ACL

Se questa finestra viene visualizzata in Cisco SDM è stato rilevato un conflitto tra la configurazione NAT ed un'ACL esistente sull'interfaccia WAN. Questa ACL può far parte di una configurazione del firewall, una configurazione della VPN o di un'altra funzione.

Scegliere di modificare la configurazione NAT per rimuovere il conflitto o scegliere di *non* modificare la configurazione NAT. Se si sceglie di *non* modificare la configurazione NAT, il conflitto può causare l'interruzione del funzionamento di altre funzioni configurate.

Visualizza dettagli

Fare clic sul pulsante **Visualizza dettagli** per vedere le modifiche proposte nella configurazione NAT per risolvere il conflitto. Questo pulsante non è attivato per tutti i conflitti tra le funzioni.

Dettagli

In questa finestra sono elencate le modifiche che verranno apportate da Cisco SDM sulla configurazione NAT per la risoluzione dei conflitti tra la NAT e altre funzioni configurate sulla stessa interfaccia.

Regole NAT

Nella finestra Regole NAT è possibile visualizzare le regole NAT, visualizzare i pool di indirizzi e impostare i timeout di conversione. Inoltre, da questa finestra è possibile indicare le interfacce come interfacce interne o esterne.

Per maggiori informazioni sui parametri NAT, seguire il collegamento Ulteriori informazioni sul protocollo NAT.

Indica interfacce NAT

Consente di indicare le interfacce come interne o esterne. La NAT utilizza le designazioni interna/esterna come punti di riferimento quando interpreta le regole di traduzione. Le interfacce interne sono quelle connesse alle reti private servite dal router. Le interfacce esterne connettono alla rete WAN o a Internet. Le interfacce interne ed esterne designate sono elencate sopra l'elenco delle regole NAT.

Pool di indirizzi

Scegliere questo pulsante per configurare o modificare i pool di indirizzi. I pool di indirizzi sono utilizzati con la conversione di indirizzi dinamici. Il router può assegnare dinamicamente gli indirizzi dal pool, quando richiesto. Se un indirizzo non è più necessario, viene restituito al pool.

Timeout di conversione

Quando il NAT dinamico è configurato, le voci di conversione dispongono di un periodo di timeout dopo il quale scadono o sono rimossi dalla tabella di conversione. Fare clic su questo pulsante per configurare i valori di timeout per le voci di conversione NAT e altri valori.

Regole NAT

In quest'area sono visualizzate le interfacce interne ed esterne indicate e le regole NAT che sono state configurate.

Interfacce interne

Le interfacce interne sono le interfacce che connettono alle reti private servite dal router. L'indicazione interna è utilizzata da NAT durante l'interpretazione di una regola di conversione NAT. È possibile indicare le interfacce come interne selezionando **Indica interfacce NAT**.

Interfacce esterne

Le interfacce esterne sono le interfacce del router che connettono alla rete WAN o a Internet. L'indicazione esterna è utilizzata da NAT durante l'interpretazione di una regola di conversione NAT. È possibile indicare le interfacce come esterne selezionando **Indica interfacce NAT**.

Indirizzo originale

È l'indirizzo privato o il set di indirizzi utilizzato nella rete LAN.

Indirizzo convertito

È l'indirizzo valido o l'intervallo di indirizzi utilizzato in Internet o nella rete esterna.

Tipo di regola

Le regole sono regole di conversione dell'indirizzo statico o regole di conversione dell'indirizzo dinamico.

Conversione di indirizzi statici. Consente agli host con indirizzi privati di accedere a Internet e di essere pubblicamente accessibili da tale rete. Questo tipo di conversione consente di abbinare staticamente un indirizzo IP privato a un indirizzo pubblico o globale. Se si desidera fornire la conversione statica a dieci indirizzi privati, creare una regola statica distinta per ciascun indirizzo.

Conversione di indirizzi dinamici. Esistono due metodi di indirizzamento dinamico tramite NAT. Il primo consente di abbinare più indirizzi privati a un indirizzo pubblico singolo e ai numeri di porta delle sessioni host per determinare a quale host instradare il traffico di ritorno. Il secondo metodo utilizza i pool di indirizzi nominati. In questi pool sono contenuti gli indirizzi pubblici. Quando da un host con indirizzo privato viene richiesto di stabilire una comunicazione esterna alla rete LAN, viene fornito un indirizzo pubblico da tale pool. Quando l'indirizzo non è più necessario, viene restituito al pool.

Duplica voce selezionata durante l'aggiunta

Se si desidera utilizzare una regola esistente come base per una regola nuova che si desidera creare, scegliere la regola e selezionare questa casella di controllo. Quando si fa clic su **Aggiungi**, gli indirizzi nella regola prescelta sono visualizzati nella finestra Aggiungi regola di conversione indirizzi. È possibile modificare questi indirizzi per ottenere quelli necessari per la nuova regola, invece di digitare l'indirizzo completo in ciascun campo.

Tabella riassuntiva funzioni

Funzione	Procedura
Indicazione delle interfacce interne ed esterne. Per eseguire NAT nel router è necessario indicare almeno un'interfaccia interna e una esterna.	Fare clic su **Indica interfacce NAT** e indicare le interfacce come interne o esterne nella finestra Impostazioni interfaccia NAT. Le interfacce possono essere indicate come interfacce interne o esterne anche nella finestra Interfaccia e connessioni.
Aggiunta, modifica o eliminazione un pool di indirizzi. Le regole dinamiche possono utilizzare i pool di indirizzi per assegnare gli indirizzi ai dispositivi, quando richiesto.	Fare clic su **Pool indirizzi** e configurare le informazioni relative al pool nella finestra di dialogo.
Impostare il timeout di conversione.	Fare clic su **Timeout di conversione** e impostare il timeout nella finestra Timeout di conversione.
Aggiunta di una regola NAT.	Fare clic su **Aggiungi** e creare la regola NAT nella finestra Aggiungi regola di conversione indirizzi. Se si desidera utilizzare una regola NAT esistente come modello per la nuova regola, scegliere la regola, fare clic su **Duplica voce selezionata durante l'aggiunta** e scegliere **Aggiungi**.
Modifica di una regola NAT.	Scegliere la regola NAT da modificare, fare clic su **Modifica** e modificare la regola nella finestra Modifica regola di conversione indirizzi.

Funzione	Procedura
Eliminazione di una regola NAT.	Scegliere la regola NAT che si desidera eliminare e fare clic su **Elimina**. È necessario confermare l'eliminazione della regola nel messaggio di avviso visualizzato.
Visualizzare o modificare mappe di instradamento. Se nel router sono configurate connessioni VPN, gli indirizzi IP locali nella rete VPN devono essere protetti dalle conversioni NAT. Se sono configurati VPN e NAT, Cisco Router and Security Device Manager (Cisco SDM) crea route map per proteggere gli indirizzi IP dalla conversione in una VPN. Inoltre "route map" vengono configurate mediante l'uso della CLI (Command-Line Interface). È possibile visualizzare le route map configurate e modificare la regola di accesso che utilizzano.	Fare clic su **Visualizza route map**.
Reperimento di informazioni su come eseguire attività di configurazione correlate.	Visualizzare una delle seguenti procedure: • Come configurare un pass-through NAT per una connessione VPN? • Come configurare il protocollo NAT in un'interfaccia non supportata? • Come configurare un pass-through NAT per un firewall?

Nota Molte condizioni fanno sì che regole NAT configurate in precedenza compaiano come di sola lettura nell'elenco delle Regole di conversione degli indirizzi della rete. Le regole NAT di sola lettura non sono modificabili. Per maggiori informazioni, vedere l'argomento della Guida Motivi per i quali Cisco SDM non è in grado di modificare una regola NAT.

Indica interfacce NAT

Utilizzare questa finestra per indicare le interfacce interne ed esterne che si desidera utilizzare nelle conversioni NAT. Le indicazioni interna ed esterna sono utilizzate da NAT durante l'interpretazione delle regole di conversione, dal momento che le conversioni sono eseguite da interna a esterna o da esterna a interna.

Una volta designate queste interfacce sono utilizzate in tutte le regole di traduzione NAT. Le interfacce indicate sono visualizzate al di sopra dell'elenco Regole NAT nella finestra principale NAT.

Interfaccia

In questa colonna sono elencate tutte le interfacce del router.

Interna (trusted)

Consente di indicare un'interfaccia come interfaccia interna. Tali interfacce sono solitamente connesse a una rete LAN servita dal router.

Esterna (untrusted)

Consente di indicare un'interfaccia come interfaccia esterna. Tali interfacce sono solitamente connesse alla rete WAN aziendale o a Internet.

Impostazioni timeout di conversione

Quando si configurano le regole di conversione NAT dinamico, le voci di conversione dispongono di un periodo di timeout dopo il quale scadono o sono rimosse dalla tabella di conversione. Impostare i valori di timeout per le varie conversioni in questa finestra.

Timeout DNS

Immettere il numero di secondi dopo i quali le connessioni ai server DNS scadono.

Timeout ICMP

Immettere il numero di secondi dopo il quale il flusso ICMP (Internet Control Message Protocol) va in timeout. Il valore predefinito è 60 secondi.

Timeout PPTP

Immettere il numero di secondi dopo il quale il flusso PPTP (Point-to-Point Tunneling Protocol) della NAT va in timeout. Il valore predefinito è 86400 secondi (24 ore).

Timeout NAT dinamico

Immettere il numero massimo di secondi per la durata di conversioni NAT dinamici.

Numero massimo di voci NAT

Immettere il numero massimo di voci NAT nella tabella di conversione.

Timeout flusso UDP

Immettere il numero massimo di secondi per la durata delle conversioni dei flussi UDP (User Datagram Protocol). Il valore predefinito è 300 secondi (5 minuti).

Timeout flusso TCP

Immettere il numero massimo di secondi per la durata delle conversioni dei flussi TCP (Transmission Control Protocol). Il valore predefinito è 86400 secondi (24 ore).

Pulsante Reimposta

Facendo clic su questo pulsante si reimpostano la conversione e i parametri di timeout ai loro valori di default.

Modifica route map

Quando VPN e NAT sono entrambi configurati in un router, i pacchetti che solitamente soddisfano i criteri di una regola IPSec non hanno più questa caratteristica, se i relativi indirizzi IP sono convertiti da NAT. In questo caso, i pacchetti verranno inviati senza essere crittografati. Cisco SDM può creare route map per impedire a NAT di convertire gli indirizzi IP che si desidera preservare.

Sebbene Cisco SDM crei le route map solo per limitare l'azione di NAT, tali mappe possono essere utilizzate anche per altri scopi. Se sono create tramite l'interfaccia CLI, le route map saranno visibili anche in questa finestra.

Nome

Il nome della route map.

Voci di route map

In questa casella sono elencate le voci di route map.

Nome

Il nome della voce della route map.

Numero di sequenza

Il numero di sequenza della route map.

Azione

Le route map create da Cisco SDM sono configurate con la parola chiave **permit**. Se il campo contiene il valore **deny**, la route map è stata creata tramite l'interfaccia CLI.

Elenchi di accesso

Gli elenchi di accesso che specificano il traffico a cui applicare la route map.

Per modificare una voce di route map

Scegliere la voce, fare clic su **Modifica** e modificare la voce nella finestra Modifica voce di route map.

Modifica voce di route map

Questa finestra viene utilizzata per modificare l'elenco di accessi specificato in una voce di route map.

Nome

Un campo di sola lettura che contiene il nome della voce della route map.

Numero di sequenza

Un campo di sola lettura che contiene il numero di sequenza della route map. Se una route map è creata da Cisco SDM, il numero di sequenza viene assegnato automaticamente.

Azione

Le opzioni sono **permit** o **deny**. Le route map create da Cisco SDM sono configurate con la parola chiave **permit**. Se il campo contiene il valore **deny**, la route map è stata creata tramite l'interfaccia CLI.

Elenchi di accesso

In quest'area sono visualizzati gli elenchi di accesso associati alla voce. Tali elenchi sono utilizzati dalla route map per determinare quale traffico proteggere dalla conversione NAT.

Per modificare un elenco di accesso in una voce di route map

Scegliere l'elenco di accesso e fare clic su **Modifica**. Quindi modificare l'elenco nella finestra visualizzata.

Pool di indirizzi

Nella finestra Pool di indirizzi sono visualizzati i pool di indirizzi che possono essere utilizzati per la conversione NAT dinamico.

Nome pool

Il campo contiene il nome del pool di indirizzi. Utilizzare questo nome per fare riferimento al pool durante la configurazione di una regola NAT dinamico.

Indirizzo

Nel campo è contenuto l'intervallo di indirizzi IP nel pool. I dispositivi i cui indirizzi IP corrispondono alla regola di accesso specificata nella finestra Aggiungi regola di conversione indirizzi verranno forniti di indirizzi IP privati da questo pool.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiungere un pool di indirizzi alla configurazione del router.	Fare clic su **Aggiungi** e configurare il pool nella finestra Aggiungi pool di indirizzi. Se si desidera utilizzare un pool esistente come modello per la nuova regola, scegliere il pool, selezionare **Duplica voce selezionata durante l'aggiunta** e fare clic su **Aggiungi**.
Modifica di un pool di indirizzi esistente.	Scegliere la voce del pool, fare clic su **Modifica** e modificare la configurazione del pool nella finestra Modifica pool di indirizzi.
Eliminazione di un pool di indirizzi.	Selezionare la voce del pool, fare clic su **Elimina** e confermare l'eliminazione nel messaggio di avviso visualizzato.

Nota Se Cisco SDM rileva che un pool di indirizzi NAT, configurato precedentemente, utilizza la parola chiave “type”, tale pool sarà di sola lettura e non potrà essere modificato.

Aggiungi o Modifica pool di indirizzi

Utilizzare questa finestra per specificare un pool di indirizzi per la conversione di indirizzi dinamici, un indirizzo per la modalità PAT (Port Address Translation) o un pool per la rotazione del bilanciamento del carico TCP.

Nome pool

Immettere il nome del pool di indirizzi

Modalità PAT (Port Address Translation)

Possono verificarsi casi in cui, quando la maggior parte degli indirizzi del pool è stata assegnata, tale pool possa essere sul punto di esaurirsi. In tali circostanze, per soddisfare ulteriori richieste di indirizzi, è possibile utilizzare PAT con un singolo indirizzo IP. Selezionare questa casella di controllo se si desidera che il router utilizzi PAT quando il pool sta per esaurirsi.

Indirizzo IP

Immettere l'indirizzo IP con il numero più basso nell'intervallo nel campo a sinistra e quello con il numero più alto nel campo a destra. Per maggiori informazioni vedere Configurazioni delle interfacce disponibili.

Maschera di rete

Immettere la subnet mask o il numero di bit di rete che specificano il numero di bit di rete contenuto nei bit degli indirizzi IP.

Aggiungi o Modifica regola di conversione indirizzi statici - Da interna a esterna

Usare questo argomento della guida quando si è scelto Da esterna a interna nella finestra Modifica regola statica di conversione indirizzi.

Utilizzare la finestra per aggiungere o modificare la regola di conversione indirizzi statici. Se si sta modificando una regola, i campi tipo di regola (statico o dinamico) e direzione sono disattivati. Se occorre modificare queste impostazioni, eliminare la regola e quindi crearla nuovamente utilizzando le impostazioni desiderate.

Il NAT è utilizzato da due tipi di traduzione di indirizzo: statico semplice e statico esteso.

Nota Se si crea una regola NAT per convertire gli indirizzi dei dispositivi che fanno parte di una rete VPN, Cisco SDM richiede di consentire la creazione di una route map che protegga tali indirizzi dalla conversione tramite NAT. Se la conversione degli indirizzi dei dispositivi in una rete VPN viene consentita, gli indirizzi convertiti non corrisponderanno alla regola IPSec utilizzata nel criterio corrispondente e il traffico verrà inviato non crittografato. Le route map create tramite Cisco SDM o utilizzando l'interfaccia CLI possono essere visualizzate facendo clic sul pulsante **Visualizza route map** nella finestra NAT.

Direzione

In questo argomento della Guida è descritta la modalità di utilizzo dei campi Aggiungi regola di conversione indirizzi quando viene selezionata l'opzione **Da interna a esterna**.

Da interna a esterna

Scegliere questa opzione per convertire gli indirizzi privati nella rete LAN in indirizzi validi in Internet o nella Intranet aziendale. È possibile scegliere questa opzione se si utilizzano indirizzi privati nella rete LAN che non sono globalmente univoci in Internet.

Converti da interfaccia

Quest'area mostra le interfacce da cui i pacchetti che richiedono la conversione dell'indirizzo giungono nel router. Nell'area sono forniti campi per specificare l'indirizzo IP di un singolo host o un indirizzo di rete e una subnet mask che rappresentano gli host in una rete.

Interfacce interne

Se per la direzione è stato scelto **Da interna a esterna**, in quest'area sono elencate le interfacce interne indicate.

Nota Quando nell'area non è indicato alcun nome di interfaccia, chiudere la finestra Aggiungi regola di conversione indirizzi, fare clic su **Indica interfacce NAT** nella finestra NAT e indicare le interfacce del router come interne o esterne. Quindi, tornare a questa finestra e configurare la regola NAT.

Indirizzo IP

Eseguire una delle seguenti operazioni:

- Se si desidera creare una mappatura statica uno-a-uno tra l'indirizzo di un singolo host e un indirizzo convertito, noto come *indirizzo globale interno*, immettere l'indirizzo IP per l'host. Non immettere una subnet mask nel campo Maschera di rete.
- Se si desidera creare una mappatura *n*-a-*n* tra gli indirizzi privati in una subnet e gli indirizzi globali interni corrispondenti, immettere qualsiasi indirizzo valido dalla subnet di cui si desidera la conversione degli indirizzi e immettere una maschera di rete nel campo successivo.

Maschera di rete

Se si desidera che Cisco SDM traduca gli indirizzi di una subnet, immettere la maschera della subnet. Cisco SDM determina il numero di rete e di subnet e il set di indirizzi da tradurre dall'indirizzo IP e dalla maschera forniti.

Converti in interfaccia

Quest'area mostra le interfacce da cui i pacchetti con gli indirizzi convertiti escono dal router. Vi sono compresi anche i campi per la specifica dell'indirizzo convertito e altre informazioni.

Interfacce esterne

Se per la direzione è stato scelto **Da interna a esterna**, in quest'area sono elencate le interfacce esterne indicate.

Tipo

- Scegliere **Indirizzo IP** se si desidera convertire l'indirizzo nell'indirizzo definito nel campo Indirizzo IP.
- Scegliere **Interfaccia** se si desidera che l'indirizzo *Converti da* utilizzi l'indirizzo di un'interfaccia del router. L'indirizzo *Converti da* verrà convertito nell'indirizzo IP assegnato all'interfaccia specificata nel campo Interfaccia.

Interfaccia

Questo campo è attivato se nel campo Tipo è selezionata l'opzione Interfaccia. Nel campo sono elencate le interfacce nel router. Scegliere l'interfaccia in cui convertire l'indirizzo interno locale nell'indirizzo IP.

Nota Se nel campo Tipo è selezionata l'opzione **Interfaccia**, sono supportate solo le conversioni che reindirizzano le porte TCP/IP. La casella di controllo Porta di reindirizzamento è selezionare automaticamente e non può essere deselezionata.

Indirizzo IP

Questo campo è attivato se nel campo Tipo è stato scelto **Indirizzo IP**. Eseguire una delle seguenti operazioni:

- Se si desidera creare una mappatura uno-a-uno tra un singolo indirizzo locale interno e un singolo indirizzo globale interno, immettere l'indirizzo globale interno in questo campo.
- Se si desidera eseguire la mappatura degli indirizzi locali interni di una subnet agli indirizzi globali interni corrispondenti, immettere in questo campo qualsiasi indirizzo IP che si desidera utilizzare nella conversione. La maschera di rete immessa nell'area *Converti da* verrà utilizzata per calcolare i rimanenti indirizzi globali interni.

Nota Se non si immette la maschera di rete in tale area, Cisco SDM esegue un'unica conversione.

Porta di reindirizzamento

Selezionare questa casella di controllo se si desidera includere le informazioni sulla porta per il dispositivo interno nella conversione. In questo modo è possibile utilizzare lo stesso indirizzo IP per più dispositivi, purché la porta specificata per ciascun dispositivo sia differente. È necessario creare una voce separata per ciascuna mappatura porta per questo indirizzo "tradotto".

Fare clic su **TCP** se si tratta di un numero di porta TCP; selezionare **UDP** se si tratta di un numero di porta UDP.

Nel campo Porta originale immettere il numero di porta del dispositivo interno.

Nel campo Porta tradotta immettere il numero di porta che il router deve utilizzare per questa conversione.

Scenari della configurazione

Fare clic su Scenari di conversione degli indirizzi statici per visualizzare esempi che descrivono la modalità di utilizzo dei campi di questa finestra.

Aggiungi o Modifica regola di conversione indirizzi statici - Da esterna a interna

Usare questo argomento della guida quando si è scelto Da esterna a interna nella finestra Modifica regola statica di conversione indirizzi.

Utilizzare la finestra per aggiungere o modificare la regola di conversione indirizzi statici. Quando si modifica una regola, il tipo di regola (statica o dinamica) e la direzione sono disattivati. Se occorre modificare queste impostazioni, eliminare la regola e quindi crearla nuovamente utilizzando le impostazioni desiderate.

Il NAT è utilizzato da due tipi di traduzione di indirizzo: statico semplice e statico esteso.

Nota Se si crea una regola NAT per convertire gli indirizzi dei dispositivi che fanno parte di una rete VPN, Cisco SDM richiede di consentire la creazione di una route map che protegga tali indirizzi dalla conversione tramite NAT. Se la conversione degli indirizzi dei dispositivi in una rete VPN viene consentita, gli indirizzi convertiti non corrisponderanno alla regola IPSec utilizzata nel criterio corrispondente e il traffico verrà inviato non crittografato. Le route map create tramite Cisco SDM o utilizzando l'interfaccia CLI possono essere visualizzate facendo clic sul pulsante **Visualizza route map** nella finestra NAT.

Direzione

Scegliere la direzione del traffico per questa regola.

Da esterna a interna

Scegliere questa opzione per convertire gli indirizzi in ingresso in indirizzi che saranno validi nella rete LAN. Ciò può essere necessario quando si uniscono più reti e si deve creare un solo insieme di indirizzi in ingresso compatibile con un insieme esistente sulla LAN servita dal router.

In questo argomento della Guida è descritta la modalità di utilizzo dei rimanenti campi una volta selezionato Da esterna a interna.

Converti da interfaccia

Quest'area mostra le interfacce da cui i pacchetti che richiedono la conversione dell'indirizzo giungono nel router. Nell'area sono forniti campi per specificare l'indirizzo IP di un singolo host o un indirizzo di rete e una subnet mask che rappresentano gli host in una rete.

Interfacce esterne

Se è stato scelto **Da esterna a interna**, in quest'area sono elencate le interfacce esterne indicate.

Nota Quando nell'area non è indicato alcun nome di interfaccia, chiudere la finestra Aggiungi regola di conversione indirizzi, fare clic su **Indica interfacce NAT** nella finestra NAT e indicare le interfacce del router come interne o esterne. Quindi, tornare a questa finestra e configurare la regola NAT.

Indirizzo IP

Eseguire una delle seguenti operazioni:

- Se si desidera creare una mappatura statica uno-a-uno tra l'indirizzo globale esterno di un singolo host remoto e un indirizzo convertito, noto come *indirizzo locale esterno*, immettere l'indirizzo IP per l'host remoto.
- Se si desidera creare una mappatura *n*-a-*n* tra gli indirizzi in una subnet remota verso gli indirizzi di tipo locale esterno corrispondenti, immettere qualsiasi indirizzo valido dalla subnet di cui si desidera la conversione degli indirizzi e immettere una maschera di rete nel campo successivo.

Maschera di rete

Se si desidera che Cisco SDM traduca gli indirizzi di una subnet remota, immettere la maschera della subnet. Cisco SDM determina il numero di rete e di subnet e il set di indirizzi da tradurre dall'indirizzo IP e dalla maschera forniti.

Converti in interfaccia

Quest'area mostra le interfacce da cui i pacchetti con gli indirizzi convertiti escono dal router. Vi sono compresi anche i campi per la specifica dell'indirizzo convertito e altre informazioni.

Interfacce interne

Se è stato scelto **Da esterna a interna**, in quest'area sono elencate le interfacce interne indicate.

Indirizzo IP

Eseguire una delle seguenti operazioni:

- Se si crea una mappatura uno-a-uno tra un singolo indirizzo globale esterno e un singolo indirizzo locale esterno, immettere l'indirizzo locale esterno in questo campo.
- Se si desidera eseguire la mappatura degli indirizzi di tipo globale esterno di una subnet remota verso gli indirizzi di tipo locale esterno corrispondenti, immettere in questo campo qualsiasi indirizzo IP che si desidera utilizzare nella conversione. La maschera di rete immessa nell'area Converti da interfaccia verrà utilizzata per calcolare i rimanenti indirizzi di tipo locale esterno.

Nota Se non si immette la maschera di rete in tale area, Cisco SDM esegue un'unica conversione.

Porta di reindirizzamento

Selezionare questa casella di controllo se si desidera includere le informazioni sulla porta per il dispositivo esterno nella conversione. In questo modo è possibile utilizzare la conversione statica estesa e lo stesso indirizzo IP per più dispositivi, purché la porta specificata per ciascun dispositivo sia differente.

Fare clic su **TCP** se si tratta di un numero di porta TCP; selezionare **UDP** se si tratta di un numero di porta UDP.

Nel campo Porta originale, immettere il numero di porta del dispositivo esterno.

Nel campo Porta tradotta immettere il numero di porta che il router deve utilizzare per questa conversione.

Scenari della configurazione

Fare clic su Scenari di conversione degli indirizzi statici per visualizzare esempi che descrivono la modalità di utilizzo dei campi di questa finestra.

Aggiungi o Modifica regola di conversione indirizzi dinamici - Da interna a esterna

Usare questo argomento della guida quando è stata scelta la direzione Da interna a esterna nella finestra Aggiungi o Modifica regola di conversione indirizzi dinamici.

In questa finestra aggiungere o modificare una regola di conversione indirizzi. Se si sta modificando una regola, i campi tipo di regola (statico o dinamico) e direzione sono disattivati. Se occorre modificare queste impostazioni, eliminare la regola e quindi crearla nuovamente utilizzando le impostazioni desiderate.

Una regola di conversione indirizzi dinamici abbina gli host agli indirizzi in maniera dinamica, utilizzando gli indirizzi contenuti in un pool di indirizzi che sono globalmente univoci nella rete di destinazione. Il pool è definito specificando un intervallo di indirizzi a cui viene attribuito un nome univoco. Gli indirizzi disponibili nel pool (ovvero quelli non utilizzati per le conversioni statiche o per l'indirizzo IP della rete WAN) sono utilizzati dal router configurato per le connessioni a Internet o ad altre reti esterne. Quando un indirizzo non è più utilizzato, viene restituito al pool di indirizzi da assegnare dinamicamente in un secondo momento a un altro dispositivo.

Nota Se si crea una regola NAT per convertire gli indirizzi dei dispositivi che fanno parte di una rete VPN, Cisco SDM richiede di consentire la creazione di una route map che protegga tali indirizzi dalla conversione tramite NAT. Se la conversione degli indirizzi dei dispositivi in una rete VPN viene consentita, gli indirizzi convertiti non corrisponderanno alla regola IPSec utilizzata nel criterio corrispondente e il traffico verrà inviato non crittografato.

Direzione

Scegliere la direzione del traffico per questa regola.

Da interna a esterna

Scegliere questa opzione se si vogliono convertire gli indirizzi privati sulla LAN in indirizzi pubblici (univoci al livello globale) su Internet o nell'intranet dell'organizzazione.

In questo argomento della Guida è descritta la modalità di utilizzo dei rimanenti campi una volta selezionato Da interna a esterna.

Converti da interfaccia

Quest'area mostra le interfacce da cui i pacchetti che richiedono la conversione dell'indirizzo giungono nel router. In essa sono compresi i campi per la specifica degli indirizzi IP di un host singolo, o un indirizzo di rete e una subnet mask che rappresenta gli host di una rete.

Interfacce interne

Se per la direzione è stato scelto **Da interna a esterna**, in quest'area sono elencate le interfacce interne indicate.

Nota Quando nell'area non è indicato alcun nome di interfaccia, chiudere la finestra Aggiungi regola di conversione indirizzi, fare clic su **Indica interfacce NAT** nella finestra NAT e indicare le interfacce del router come interne o esterne. Quindi, tornare a questa finestra e configurare la regola NAT.

Regola di accesso

Le regole di conversione NAT dinamico utilizzano le regole di accesso per specificare gli indirizzi da convertire. Se si sceglie **Da interna a esterna**, gli indirizzi sono di tipo locale interno. Immettere il nome o il numero della regola di accesso che definisce gli indirizzi da convertire. In caso contrario, fare clic sul pulsante **...** e scegliere una regola d'accesso esistente oppure creare una nuova regola di accesso da usare.

Converti in interfaccia

Quest'area mostra le interfacce da cui i pacchetti con gli indirizzi convertiti escono dal router. Vi sono compresi anche i campi per la specifica dell'indirizzo convertito.

Interfacce esterne

Se la direzione scelta è **Da interna a esterna**, in quest'area sono elencate le interfacce esterne indicate.

Tipo

Scegliere **Interfaccia** se si desidera che l'indirizzo *Converti da* utilizzi l'indirizzo di un'interfaccia del router. Questi indirizzi verranno convertiti nell'indirizzo specificato nel campo Interfaccia mentre la modalità PAT verrà utilizzata per distinguere ciascun host nella rete. Scegliere **Pool di indirizzi** se si desidera la conversione degli indirizzi in indirizzi definiti in un pool di indirizzi configurati.

Interfaccia

Se si sceglie **Interfaccia** nel campo Tipo, questo campo elenca le interfacce sul router. Scegliere l'interfaccia in cui convertire gli indirizzo interno locale nell'indirizzo IP. La modalità PAT verrà utilizzata per distinguere ciascun host nella rete.

Pool di indirizzi

Se nel campo Tipo si sceglie l'opzione **Pool di indirizzi**, è possibile immettere il nome di un pool di indirizzi configurati in questo campo; in alternativa, è possibile fare clic su **Pool di indirizzi** per selezionare o creare un pool di indirizzi.

Scenari della configurazione

Fare clic su Scenari di conversione degli indirizzi dinamici per visualizzare esempi che descrivono la modalità di utilizzo dei campi di questa finestra.

Aggiungi o Modifica regola di conversione indirizzi dinamici - Da esterna a interna

Usare questo argomento della guida quando è stata scelta la direzione Da esterna a interna nella finestra Aggiungi o Modifica regola di conversione indirizzi dinamici.

In questa finestra aggiungere o modificare una regola di conversione indirizzi. Se si sta modificando una regola, i campi tipo di regola (statico o dinamico) e direzione sono disattivati. Se occorre modificare queste impostazioni, eliminare la regola e quindi crearla nuovamente utilizzando le impostazioni desiderate.

Una regola di conversione indirizzi dinamici abbina gli host agli indirizzi in maniera dinamica, utilizzando gli indirizzi contenuti in un pool di indirizzi che sono globalmente univoci nella rete di destinazione. Il pool è definito specificando un intervallo di indirizzi a cui viene attribuito un nome univoco. Gli indirizzi disponibili nel pool (ovvero quelli non utilizzati per le conversioni statiche o per l'indirizzo IP della rete WAN) sono utilizzati dal router configurato per le connessioni a Internet o ad altre reti esterne. Quando un indirizzo non è più utilizzato, viene restituito al pool di indirizzi da assegnare dinamicamente in un secondo momento a un altro dispositivo.

Nota Se si crea una regola NAT per convertire gli indirizzi dei dispositivi che fanno parte di una rete VPN, Cisco SDM richiede di consentire la creazione di una route map che protegga tali indirizzi dalla conversione tramite NAT. Se la conversione degli indirizzi dei dispositivi in una rete VPN viene consentita, gli indirizzi convertiti non corrisponderanno alla regola IPSec utilizzata nel criterio corrispondente e il traffico verrà inviato non crittografato.

Direzione

Scegliere la direzione del traffico per questa regola.

Da esterna a interna

Scegliere questa opzione per convertire gli indirizzi in ingresso in indirizzi che saranno validi nella rete LAN. Ciò può essere necessario quando si uniscono più reti e si deve creare un solo insieme di indirizzi in ingresso compatibile con un insieme esistente sulla LAN servita dal router.

In questo argomento della Guida è descritta la modalità di utilizzo dei rimanenti campi una volta selezionato Da esterna a interna.

Converti da interfaccia

Quest'area mostra le interfacce da cui i pacchetti che richiedono la conversione dell'indirizzo giungono nel router. In essa sono compresi i campi per la specifica degli indirizzi IP di un host singolo, o un indirizzo di rete e una subnet mask che rappresenta gli host di una rete.

Interfacce esterne

Se è stato scelto **Da esterna a interna**, in quest'area sono elencate le interfacce esterne indicate.

Nota Quando nell'area non è indicato alcun nome di interfaccia, chiudere la finestra Aggiungi regola di conversione indirizzi, fare clic su **Indica interfacce NAT** nella finestra NAT e indicare le interfacce del router come interne o esterne. Quindi, tornare a questa finestra e configurare la regola NAT.

Regola di accesso

Le regole di conversione NAT dinamico utilizzano le regole di accesso per specificare gli indirizzi da convertire. Se si sceglie **Da esterna a interna**, gli indirizzi sono di tipo globale esterno. Immettere il nome o il numero della regola di accesso che definisce gli indirizzi da convertire. In caso contrario, fare clic sul pulsante **...** e scegliere una regola d'accesso esistente oppure creare una nuova regola di accesso da usare.

Converti in interfaccia

Quest'area mostra le interfacce da cui i pacchetti con gli indirizzi convertiti escono dal router. Vi sono compresi anche i campi per la specifica dell'indirizzo convertito.

Interfacce interne

Se è stato scelto **Da esterna a interna**, in quest'area sono elencate le interfacce interne indicate.

Tipo

Scegliere **Interfaccia** se si desidera che l'indirizzo *Converti da* utilizzi l'indirizzo di un'interfaccia del router. Questi indirizzi verranno convertiti nell'indirizzo specificato nel campo Interfaccia mentre la modalità PAT verrà utilizzata per distinguere ciascun host nella rete. Scegliere **Pool di indirizzi** se si desidera la conversione degli indirizzi in indirizzi definiti in un pool di indirizzi configurati.

Interfaccia

Se si sceglie **Interfaccia** nel campo Tipo, questo campo elenca le interfacce sul router. Scegliere l'interfaccia in cui convertire gli indirizzo interno locale nell'indirizzo IP. La modalità PAT verrà utilizzata per distinguere ciascun host nella rete.

Pool di indirizzi

Se nel campo Tipo si sceglie l'opzione Pool di indirizzi, è possibile immettere il nome di un pool di indirizzi configurati in questo campo; in alternativa, è possibile fare clic su **Pool di indirizzi** per selezionare o creare un pool di indirizzi.

Scenari della configurazione

Fare clic su Scenari di conversione degli indirizzi dinamici per visualizzare esempi che descrivono la modalità di utilizzo dei campi di questa finestra.

Come . . .

In questa sezione sono contenute le procedure delle attività non contemplate nella procedura guidata.

Come configurare la Traduzione degli indirizzi per il traffico dall'esterno all'interno

La procedura guidata NAT consente di configurare la regola NAT (Network Address Translation) per convertire indirizzi dall'interno all'esterno. Per configurare una regola NAT per convertire gli indirizzi dall'esterno all'interno, osservare le indicazioni di una delle seguenti sezioni:

- Aggiungi o Modifica regola di conversione indirizzi dinamici - Da esterna a interna
- Aggiungi o Modifica regola di conversione indirizzi statici - Da esterna a interna

Come si configura la NAT con una LAN e diverse WAN?

La procedura guidata NAT consente di configurare una regola NAT (Network Address Translation) tra un'interfaccia LAN sul router e un'interfaccia WAN. Per configurare NAT tra un'interfaccia LAN sul router e più interfacce WAN, utilizzare la procedura guidata NAT per configurare una regola di conversione indirizzi tra l'interfaccia LAN sul router e un'interfaccia WAN. Seguire quindi le indicazioni fornite in una delle seguenti sezioni:

- Aggiungi o Modifica regola di conversione indirizzi statici - Da interna a esterna
- Aggiungi o Modifica regola di conversione indirizzi dinamici - Da interna a esterna

Ogni volta che si aggiunge una nuova regola di traduzione degli indirizzi usando le indicazioni di queste sezioni, scegliere la stessa interfaccia LAN ed una nuova interfaccia WAN. Ripetere questa procedura per tutte le interfacce che si desidera configurare con regole di conversione degli indirizzi.

Come . . .

CAPITOLO 24

IPS Cisco IOS

Il Cisco IOS Sistema prevenzioni intrusioni (IPS Cisco IOS) consente di gestire la prevenzione delle intrusioni sui router che utilizzano Cisco IOS versione 12.3(8)T4 o versioni successive. IPS Cisco IOS consente di controllare e di prevenire le intrusioni confrontando il traffico con le firme delle minacce note e bloccando il traffico al momento del rilevamento di una minaccia.

Cisco SDM consente di controllare l'applicazione di IPS Cisco IOS nelle interfacce, di importare e modificare i file SDF (Signature Definition File) da Cisco.com e di configurare l'azione che IPS Cisco IOS deve intraprendere se rileva una minaccia.

Schede IPS

Usare le schede nella parte superiore della finestra IPS per accedere all'area in cui si deve lavorare.

- Crea IPS – Selezionare questa opzione per passare alla procedura di creazione guidata delle regola IPS per creare una nuova regola IPS Cisco IOS.
- Modifica IPS – Consente di modificare le regole IPS Cisco IOS e applicarle alle interfacce o rimuoverle da esse.
- Dashboard protezione – Consente di visualizzare la tabella Minacce principali e distribuire le firme associate a tali minacce.
- Migrazione IPS – Se il router esegue un'immagine di Cisco IOS versione 12.4(11)T o versione successiva, è possibile migrare le configurazioni IPS Cisco IOS create con le versioni precedenti di Cisco IOS.

Regole IPS

Una regola IPS Cisco IOS specifica un'interfaccia, il tipo e la direzione del traffico che deve essere esaminato e la posizione del file SDF (Signature Definition File) utilizzato dal router.

Crea IPS

Da questa finestra è possibile eseguire la procedura guidata di creazione delle regole IPS.

La procedura guidata richiede l'immissione delle seguenti informazioni:

- L'interfaccia di applicazione della regola.
- La direzione del traffico cui applicare IPS Cisco IOS (in ingresso, in uscita o entrambe le direzioni).
- La posizione del file SDF (Signature Definition File).

Per le immagini di Cisco IOS 12.4(11) o versioni successive, viene anche chiesto di inserire le seguenti informazioni:

- La posizione in cui memorizzare i file contenenti le modifiche apportate alla configurazione IOS IPS. Un file che memorizza questo tipo di informazioni viene definito file delta.
- La chiave pubblica da utilizzare per l'accesso alle informazioni nei file delta.
- La categoria della firma. La categoria di firme di base è adatta ai router con meno di 128 MB di memoria flash. La categoria di firme avanzata è adatta ai router con più di 128 MB di memoria flash.

Lo scenario di utilizzo illustra una configurazione in cui viene utilizzata una regola IPS Cisco IOS. Dopo aver creato la regola IPS Cisco IOS e aver recapitato la configurazione al router, è possibile modificare la regola facendo clic sulla scheda **Modifica IPS**.

Per ulteriori informazioni sul IPS Cisco IOS, consultare la documentazione disponibile al seguente indirizzo:

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Fare clic sul pulsante **Avvia la procedura guidata regola IPS**.

Crea IPS: Pagina iniziale

Questa finestra fornisce un riepilogo delle attività da eseguire quando si completa la procedura guidata di creazione delle regole IPS.

Fare clic su **Avanti** per iniziare la configurazione di una regola IPS Cisco IOS.

Crea IPS: Seleziona interfacce

Selezionare le interfacce sulle quali si desidera applicare la regola IPS Cisco IOS specificando se la regola deve essere applicata al traffico in ingresso o in uscita. Se si selezionano entrambe le caselle di controllo, In ingresso e In uscita, la regola viene applica al traffico in entrambe le direzioni.

Ad esempio: le impostazioni seguenti applicano la regola IPS Cisco IOS al traffico in ingresso nell'interfaccia BRI 0 e su entrambe le direzioni di traffico, in ingresso e in uscita, nell'interfaccia FastEthernet 0.

Nome interfaccia	In ingresso	In uscita
BRI 0	Selezionare	—
FastEthernet 0	Selezionare	Selezionare

Crea IPS: Posizione SDF

IPS Cisco IOS esamina il traffico confrontandolo con le firme contenute nel file SDF (Signature Definition File). Il file SDF può essere posizionato nella memoria flash del router o su un sistema remoto raggiungibile dal router. È possibile specificare diverse posizioni del file SDF in modo che se non è in grado di contattare la prima posizione il router può tentare altre posizioni finché non ottiene il file SDF.

Utilizzare le opzioni **Aggiungi**, **Elimina**, **su** e **Sposta giù** per aggiungere e rimuovere elementi o modificarne l'ordine nella lista delle posizioni SDF che il router può cercare di contattare per ottenere un SDF. Il router comincia con la prima voce e va avanti lungo la lista finché non ottiene un file SDF.

Le immagini Cisco IOS che supportano IPS Cisco IOS contengono firme incorporate. Se si seleziona la casella di controllo nella parte inferiore della finestra, il router userà le definizioni incorporate soltanto se non può ottenere un SDF da una qualsiasi altra posizione contenuta nell'elenco.

Crea IPS: File delle firme

Il file delle firme IPS Cisco IOS contiene informazioni sulle firme predefinite presenti in ogni aggiornamento del file su Cisco.com. Le modifiche apportate a questa configurazione vengono salvate in un file delta. Per motivi di sicurezza, il file delta deve disporre di firma digitale. Specificare il percorso del file delle firme, nonché il nome e il testo della chiave pubblica che verranno utilizzati per firmare il file delta in questa finestra.

Questo argomento della Guida descrive la finestra File delle firme visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

Specificare il file delle firme da utilizzare con IPS IOS.

Se il file delle firme è già presente sul PC, sulla memoria flash del router o su un sistema remoto, fare clic su **Specificare il file di firme da utilizzare con IPS IOS** per visualizzare una finestra di dialogo in cui è possibile specificare il percorso del file delle firme.

Richiedere l'ultimo file delle firme al sito Web di Cisco e salvarlo PC

Fare clic su **Richiedere l'ultimo file delle firme al sito Web di Cisco e salvarlo PC** se il file delle firme non è ancora presente sul PC o sulla memoria flash del router. Fare clic su **Sfoglia** per specificare il percorso in cui salvare il file delle firme, quindi fare clic su **Download** per avviare il download del file. Cisco SDM esegue il download del file delle firme nel percorso specificato.

Configura chiave pubblica

Le modifiche apportate alla configurazione della firma vengono salvate nel file delta. Il file delta deve disporre di firma digitale con chiave pubblica. La chiave può essere ottenuta da Cisco.com ed è possibile incollare le informazioni nei campi Nome e Chiave.

Nota Se la chiave pubblica è già stata aggiunta alla configurazione mediante Cisco IOS CLI, è comunque necessario specificare la chiave pubblica in questa schermata. Dopo aver completato la Procedura guidata regola IPS Cisco IOS, è possibile passare a **Modifica impostazioni > globali IPS**. Nella schermata Impostazioni globali, è possibile fare clic su **Modifica** nell'area Modifica prerequisiti IPS, quindi fare clic su **Chiave Pubblica** per visualizzare la finestra di dialogo Chiave pubblica. In tale finestra, è possibile eliminare le chiavi pubbliche non più necessarie.

Seguire questi passaggi per inserire le informazioni della chiave pubblica nei campi Nome e Chiave.

Passo 1 Utilizzare il collegamento riportato di seguito per ottenere la chiave pubblica:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Passo 2 Eseguire il download della chiave sul PC.

Passo 3 Copiare il testo che segue la dicitura “named-key” (chiave con nome) nel campo Nome. Se per esempio la riga di testo compreso il nome è la seguente:

```
named-key realm-cisco.pub signature
```

copiare `realm-cisco.pub signature` nel campo Nome:

Passo 4 Copiare il testo compreso tra la dicitura `key-string` e la parola `quit` nel campo Chiave. Questo è un esempio di testo:

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

Crea IPS: Posizione di configurazione e Categoria

Specificare un percorso di memorizzazione delle informazioni di firma che verranno utilizzate da IPS Cisco IOS. Le informazioni consistono nel file delle firme e nel file delta creato quando vengono apportate modifiche alle informazioni di firma.

Questo argomento della Guida descrive la finestra Posizione di configurazione visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

Posizione di configurazione

Fare clic sul pulsante a destra del campo Posizione di configurazione per visualizzare una finestra di dialogo che consente di specificare un percorso. Dopo avere immesso le informazioni in questa finestra di dialogo, in questo campo Cisco SDM visualizza il percorso a tale posizione.

Scegli categoria

Dal momento che la memoria del router e le limitazioni delle risorse possono impedire l'utilizzo di tutte le firme disponibili, esistono due categorie di firme:**di base** e **avanzata**. Nel campo Scegli categoria, scegliere la categoria che consentirà a IPS Cisco IOS di essere eseguito in modo efficace sul router. La categoria di base è adatta ai router con meno di 128 MB di memoria flash disponibile. La categoria avanzata è adatta ai router con più di 128 MB di memoria flash disponibile.

Aggiungi o Modifica posizione di configurazione

Specificare un percorso di memorizzazione delle informazioni di firma e il file delta che verranno utilizzati da IPS Cisco IOS.

Specifica posizione di configurazione nel router

Per specificare un percorso sul router, fare clic sul pulsante a destra del campo Nome directory e scegliere la directory in cui memorizzare le informazioni di configurazione.

Nota Se il router dispone di un file system basato su LEFS, non sarà possibile creare una directory nella memoria del router. In tal caso, viene utilizzato flash: come posizione di configurazione.

Specifica posizione di configurazione tramite URL

Per specificare un percorso su un sistema remoto, specificare il protocollo e il percorso dell'URL richiesto per raggiungere la posizione. Se ad esempio si desidera specificare l'URL http://172.27.108.5/ips-cfg, immettere 172.27.108.5/ips-cfg.

Nota Non includere il protocollo nel percorso immesso. Cisco SDM aggiunge il protocollo automaticamente. Se viene immesso il protocollo, Cisco SDM visualizza un messaggio di errore.

Nei campi N. di tentativi e Timeout, specificare il numero di tentativi che il router può eseguire per contattare il sistema remoto e il tempo di attesa della risposta prima di interrompere i tentativi di contatto.

Selezione della directory

Scegliere la cartella in cui memorizzare le informazioni di configurazione. Per creare una nuova cartella, fare clic su **Nuova cartella**, specificare un nome nella finestra di dialogo visualizzata, selezionarla e fare clic su **OK**.

File delle firme

Specificare il percorso del file delle firme che verrà utilizzato da IPS Cisco IOS.

Specificare il file delle firme sulla memoria flash

Se il file delle firme si trova sulla memoria flash del router, fare clic sul pulsante a destra del campo. Cisco SDM visualizza i nomi del file delle firme del formato corretto selezionabili.

Specificare il file delle firme tramite URL

Se il file delle firme si trova su un sistema remoto, selezionare il protocollo da utilizzare e immettere il percorso al file. Se ad esempio il file delle firme IOS-S259-CLI.pkg si trova all'indirizzo 10.10.10.5 e si utilizzerà il protocollo FTP, selezionare **ftp** come protocollo e immettere

```
10.10.10.5/IOS-S259-CLI.pkg
```

Nota Non includere il protocollo nel percorso immesso. Cisco SDM aggiunge il protocollo automaticamente. Se viene immesso il protocollo, Cisco SDM visualizza un messaggio di errore. Inoltre, se si utilizza un URL, è necessario specificare il nome del file in modo che sia conforme alla convenzione di denominazione di file IOS-Snnn-CLI.pkg, così come per il file utilizzato nell'esempio precedente.

Specificare il file delle firme su PC

Se il file delle firme si trova sul PC, fare clic su **Sfoglia**, navigare alla cartella contenente il file e selezionare il nome del file. È necessario scegliere un pacchetto specifico per Cisco SDM di formato sigv5-SDM-S*xxx*.zip; ad esempio, sigv5-SDM-S260.zip.

Crea IPS: Riepilogo

Questo è un esempio di una visualizzazione di riepilogo di IPS Cisco IOS su un router su cui è in esecuzione una versione di Cisco IOS precedente alla 121.4(11)T.

```
Interfaccia selezionata: FastEthernet 0/1

IPS Scanning Direction (Direzione di scansione IPS): Entrambi

Posizione del file SDF (Signature Definition File): flash//sdmips.sdf

Built-in enabled (Attivazione firme incorporate): Sì
```

In questo esempio, IPS Cisco IOS è attivato nell'interfaccia FastEthernet 0/1 e il traffico viene esaminato in entrambe le direzioni. Il file SDF è denominato sdmips.sdf ed è situato nella memoria flash del router. Il router è configurato per l'uso delle definizioni delle firme incorporate nell'immagine Cisco IOS utilizzata dal router.

Crea IPS: Riepilogo

La finestra di riepilogo visualizza le informazioni che sono state immesse in modo da poterle esaminare prima di trasmettere le modifiche al router.

Questo argomento della Guida descrive la finestra di riepilogo visualizzata se sul router è in esecuzione Cisco IOS versione 12.4(11)T o versioni successive. Di seguito viene presentato un esempio di finestra di riepilogo.

```
La regola IPS verrà applicate al traffico in uscita sulle seguenti interfacce.
     FastEthernet0/1
La regola IPS verrà applicate al traffico in entrata sulle seguenti interfacce.
     FastEthernet0/0
Percorso del file delle firme:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Chiave pubblica:
       30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Posizione di configurazione
     flash:/configloc/
Categoria di firme selezionata:
     avanzata
```

In questo esempio, il criterio IPS Cisco IOS viene applicato alle interfacce FastEthernet 0/0 e FastEthernet 0/1. Il file delle firme si trova sul PC. La posizione di configurazione si trova sulla memoria flash del router, nella directory chiamata configloc.

Modifica IPS

In questa finestra è possibile visualizzare i IPS Cisco IOS pulsanti per la configurazione e la gestione dei criteri di IPS Cisco IOS, dei messaggi di protezione, delle firme e altro.

Pulsante Criteri IPS

Fare clic per visualizzare la finestra Modifica IPS dalla quale è possibile attivare o disattivare il sistema IPS Cisco IOS su un'interfaccia e visualizzare informazioni sulle modalità di applicazione da parte di IPS Cisco IOS. Se si attiva IPS Cisco IOS su un'interfaccia, è possibile specificare su quale traffico effettuare il rilevamento delle intrusioni.

Pulsante Impostazioni globali

Fare clic per visualizzare la finestra Modifica IPS: Impostazioni globali da cui è possibile configurare le impostazioni che influenzano il funzionamento complessivo del sistema IPS Cisco IOS.

Aggiornamento automatico

Questo pulsante viene visualizzato se l'immagine Cisco IOS sul router è di versione 12.4(11)T o successiva. L'Aggiornamento automatico consente di configurare il router in modo da ottenere automaticamente gli aggiornamenti di firma più recenti da Cisco Security Center. Per maggiori informazioni vedere Modifica IPS: Aggiornamento automatico.

Configurazione SEAP

Questo pulsante viene visualizzato se l'immagine Cisco IOS sul router è di versione 12.4(11)T o successiva. SEAP (Signature Event Action Processing) fornisce il controllo massimo sull'IOS IPS mediante funzioni di filtraggio e di sostituzione avanzate.

Pulsante Messaggi SDEE

I messaggi SDEE (Secure Device Event Exchange) comunicano i dati relativi all'inizializzazione e al funzionamento di IPS Cisco IOS. Fare clic per visualizzare la finestra Modifica IPS: Messaggi SDEE, da cui è possibile rivedere i messaggi SDEE e filtrarli per visualizzare solo i messaggi di errore, di stato o di avviso.

Pulsante Firme

Fare clic per visualizzare la finestra Modifica IPS: Firme dove è possibile gestire le firme nel router.

Pulsante NM-CIDS

Questo pulsante è visibile se nel router è installato un modulo di rete CIDS (Cisco Intrusion Detection System). Fare clic per gestire il modulo IDS.

Modifica IPS: Criterio IPS

Questa finestra visualizza lo stato del sistema IPS Cisco IOS per tutte le interfacce del router e consente di attivare e disattivare IPS Cisco IOS nelle interfacce.

Interfacce

Utilizzare questo elenco per filtrare le interfacce visualizzate nell'area dell'elenco interfacce. Scegliere una delle opzioni seguenti:

- Tutte le interfacce: tutte le interfacce del router.
- Interfacce IPS: interfacce in cui è stato attivato IPS Cisco IOS.

Pulsante Attiva

Fare clic su questo pulsante per attivare IPS Cisco IOS nell'interfaccia selezionata. È possibile specificare le direzioni di traffico alle quali applicare IPS Cisco IOS e gli elenchi di controllo di accesso (ACL, Access Control List) da utilizzare per definire il tipo di traffico da analizzare. Per maggiori informazioni vedere la sezione Attiva o Modifica IPS nell'interfaccia.

Pulsante Modifica

Fare clic su questo pulsante per modificare le caratteristiche del sistema IPS Cisco IOS applicate all'interfaccia selezionata.

Pulsante Disattiva

Fare clic su questo pulsante per disattivare IPS Cisco IOS nell'interfaccia selezionata. Un menu di scelta rapida indica le direzioni di traffico a cui IPS Cisco IOS è stato applicato ed è possibile selezionare la direzione per la quale si desidera disattivare IPS Cisco IOS. Se si disattiva IPS Cisco IOS in un'interfaccia a cui era applicato, Cisco SDM rimuove tutte le associazioni tra le regole IPS Cisco IOS e l'interfaccia.

Pulsante Disattiva tutto

Fare clic su questo pulsante per disattivare IPS Cisco IOS in tutte le interfacce in cui era attivato. Se si disattiva IPS Cisco IOS in un'interfaccia a cui era applicato, Cisco SDM rimuove tutte le associazioni tra le regole IPS Cisco IOS e l'interfaccia.

Nome interfaccia

Nome dell'interfaccia Ad esempio: Serial0/0 oppure FE0/1.

IP

Questa colonna può contenere i seguenti tipi di indirizzo IP:

- Configurato: l'indirizzo IP dell'interfaccia.
- Client DHCP: l'interfaccia riceve un indirizzo IP da un server DHCP (Dynamic Host Configuration Protocol).
- Negoziato: l'interfaccia riceve un indirizzo IP tramite negoziazione con il dispositivo remoto.
- Senza numero: il router utilizza uno degli indirizzi IP di un pool fornito dal provider di servizi per il router in uso e per i dispositivi sulla LAN.
- Non applicabile: al tipo di interfaccia non può essere assegnato un indirizzo IP.

IPS in ingresso/IPS in uscita

- Attivato: IPS Cisco IOS è attivato per questa direzione di traffico.
- Disattivato: IPS Cisco IOS non è attivato per questa direzione di traffico.

Stato VFR

Stato VFR (Virtual Fragment Reassembly). I valori possibili sono:

- On: VFR è attivato.
- Off: VFR è disattivato.

IPS Cisco IOS non può identificare il contenuto di frammenti IP né può raccogliere informazioni sulla porta da un frammento per verificarne la corrispondenza con una firma. I frammenti possono quindi attraversare la rete senza essere analizzati o senza la creazione di una lista di controllo degli accessi (ACL) dinamica.

VFR consente al firewall Cisco IOS di creare le liste di controllo degli accessi dinamiche appropriate, proteggendo quindi la rete da attacchi a frammentazione.

Descrizione

Descrizione della connessione, se è stata aggiunta

Dettagli filtro IPS

Se non è stato applicato alcun filtro al traffico, quest'area risulta vuota. Se è stato applicato un filtro, il nome o il numero della lista di controllo degli accessi viene indicato tra parentesi.

Pulsanti Filtro in ingresso/Filtro in uscita

Consentono di visualizzare le voci del filtro applicato al traffico in ingresso o in uscita.

Descrizione dei campi

Azione: indica se il traffico autorizzato o bloccato.

 Consente il traffico di origine.

 Impedisce il traffico di origine.

Origine: un indirizzo host o di rete o qualsiasi host o rete.

Destinazione: un indirizzo host o di rete o qualsiasi host o rete.

Servizio: tipo di servizio filtrato: IP, TCP, UDP, IGMP o ICMP.

Registro: indica se il traffico bloccato viene registrato.

Attributi: opzioni configurate utilizzando l'interfaccia CLI.

Descrizione: qualsiasi descrizione fornita.

Attiva o Modifica IPS nell'interfaccia

Utilizzare questa finestra per selezionare le interfacce nelle quali si desidera attivare il rilevamento delle intrusioni e di scegliere i filtri IPS necessari per l'analisi del traffico.

Pulsanti In ingresso, In uscita e Entrambi

Utilizzare questi pulsanti per specificare se IPS Cisco IOS verrà attivato solo sul traffico in ingresso, solo su quello in uscita o su entrambi.

Filtro in ingresso

(Opzionale) Immettere il nome o il numero della regola di accesso che specifica il traffico in ingresso da analizzare. La lista di controllo degli accessi (ACL) specificata verrà visualizzata nella finestra di configurazione delle regole IPS quando si seleziona l'interfaccia alla quale è associata. Per cercare una regola di accesso o crearne una nuova, fare clic sul **pulsante**…

Filtro in uscita

(Opzionale) Immettere il nome o il numero della regola di accesso che specifica il traffico in uscita da analizzare. La lista di controllo degli accessi (ACL) specificata verrà visualizzata nella finestra di configurazione delle regole IPS quando si seleziona l'interfaccia alla quale è associata. Per cercare una regola di accesso o crearne una nuova, fare clic sul pulsante **...**.

... Pulsante

Consente di specificare un filtro. Facendo clic, viene visualizzato un menu con le seguenti opzioni:

- Choose an existing rule (Scegli regola esistente). Per maggiori informazioni vedere la sezione Selezionare una regola.
- Crea una nuova regola. Per maggiori informazioni vedere la sezione Aggiungi o modifica regola.
- Nessuno (cancella associazione regole). Questa opzione consente di rimuovere un filtro da una direzione di traffico a cui era stato applicato.

Attiva il controllo dei frammenti nell'interfaccia

(Attivato per impostazione predefinita). Selezionare questa opzione se si desidera che il firewall Cisco IOS controlli i frammenti IP nell'interfaccia. Per maggiori informazioni vedere la sezione Stato VFR.

Attiva il controllo dei frammenti nelle altre interfacce

Se si attiva il controllo dei frammenti per il traffico in uscita, il router deve analizzare anche il traffico in ingresso verso le interfacce che inviano traffico in uscita all'interfaccia che si sta configurando. Specificare queste interfacce di seguito.

Se si seleziona il pulsante di opzione In ingresso, quest'area non viene visualizzata.

Specificare il file delle firme

La finestra Specificare il file delle firme contiene le informazioni sulla versione SDF utilizzata dal router e consente di aggiornare il file SDF a una versione più recente. Per specificare un nuovo file SDF, fare clic sul pulsante **...** vicino al campo File delle firme e specificare un nuovo file nella finestra visualizzata.

Modifica IPS: Impostazioni globali

Questa finestra consente di visualizzare e configurare le impostazioni globali per Cisco IPS. Questo argomento della Guida descrive le informazioni visualizzate se è in esecuzione una versione di immagine Cisco IOS precedente alla 12.4(11)T.

Tabella Impostazioni globali

Questa tabella nella finestra Impostazioni globali consente di visualizzare le impostazioni globali correnti e i relativi valori. Fare clic su **Modifica** per modificare i valori.

Nome elemento	Valore elemento
Syslog	Se questa opzione è attivata, le notifiche vengono inviate al server syslog specificato nelle proprietà di sistema.
SDEE	Acronimo di Security Device Event Exchange. Se quest'opzione è attivata, verranno generati eventi SDEE.
Eventi SDEE	Indica il numero degli eventi SDEE da memorizzare nel buffer del router.
Registrazione SDEE	Numero di registrazioni SDEE contemporanee.

Opzioni motore	Le opzioni motore sono: • Errore chiuso: per impostazione predefinita, mentre Cisco IOS compila una nuova firma per un determinato motore, autorizza il passaggio di pacchetti senza cercare il motore corrispondente. Se attivata, questa opzione provoca la perdita dei pacchetti da parte di Cisco IOS durante il processo di compilazione. • Utilizza firme incorporate (come backup): se IPS Cisco IOS non riesce a trovare firme o a caricarle da posizioni specifiche, vengono utilizzate le firme incorporate di Cisco IOS per attivare IPS Cisco IOS. L'opzione è attivata per impostazione predefinita. • Nega azione sull'interfaccia IPS: opzione consigliata quando il router esegue il bilanciamento del carico. Una volta attivata, questa opzione determina l'attivazione da parte di IPS Cisco IOS delle ACL sulle interfacce IPS Cisco IOS piuttosto che sulle interfacce da cui proviene il traffico di attacco.
Eventi shun	Questa opzione utilizza il parametro Shun Time, che indica l'intervallo di tempo nel quale le azioni shun hanno validità. Un'azione shun si verifica se un host o una rete viene aggiunto a una ACL per negarne il traffico.

Posizioni SDF configurate

La posizione di una firma è un URL che fornisce un percorso a un file SDF. Per trovare un file SDF, il router tenta di contattare la prima posizione dell'elenco. In caso di esito negativo, prova con le posizioni seguenti, finché non trova un file SDF.

Pulsante Aggiungi

Consente di aggiungere un URL all'elenco.

Pulsante Modifica

Consente di modificare la posizione specificata.

Pulsante Elimina

Consente di eliminare la posizione specificata.

Pulsanti Sposta su e Sposta giù

Consentono di modificare l'ordine di preferenza degli URL elencati.

Ricarica firme

Consente di compilare nuovamente le firme in tutti i motori firma. Durante la ricompilazione delle firme in un motore firme, Cisco IOS non potrà utilizzare le firme di quel motore per la scansione dei pacchetti.

Modifica impostazioni globali

Consente di modificare le impostazioni che riguardano il funzionamento generale di IPS Cisco IOS in questa finestra e nelle schede Syslog e SDEE e Motore globale.

Attiva notifica Syslog (scheda Syslog e SDEE)

Selezionare questa casella di controllo per consentire al router di inviare avvisi, eventi e messaggi di errore a un server syslog. Per il funzionamento del metodo di notifica occorre identificare un server syslog nelle proprietà di sistema.

SDEE (scheda Syslog e SDEE)

Immettere il numero di registrazioni SDEE contemporanee, comprese nell'intervallo da 1 a 3, nel campo **Numero di registrazioni SDEE contemporanee**. Per registrazione SDEE si intende un flusso in tempo reale di eventi SDEE.

Nel campo **Maximum number of SDEE alerts to store** (Numero massimo di avvisi SDEE da archiviare) immettere il numero massimo di avvisi SDEE che si desidera far archiviare dal router, in un intervallo compreso tra 10 e 2000. Per archiviare più avvisi è necessario l'utilizzo di una maggiore memoria del router.

Nel campo **Maximum number of SDEE messages to store** (Numero massimo di messaggi SDEE da archiviare) immettere il numero massimo di messaggi SDEE che si desidera far archiviare dal router, in un intervallo compreso tra 10 e 500. Per archiviare più messaggi è necessario l'utilizzo di una maggiore memoria del router.

Attiva chiusura per errore motore (scheda Motore globale)

Per impostazione predefinita, il software Cisco IOS compila una nuova firma per un determinato motore mentre autorizza il passaggio di pacchetti senza cercare il motore corrispondente. Attivare questa opzione per determinare la perdita dei pacchetti da parte del software Cisco IOS durante il processo di compilazione.

Utilizza firme incorporate (come backup) (scheda Motore globale)

Se IPS Cisco IOS non riesce a trovare le firme o a caricarle dalla posizione specificata, è possibile utilizzare le firme incorporate di Cisco IOS per attivare IPS Cisco IOS. L'opzione è attivata per impostazione predefinita.

Attiva Nega azione sull'interfaccia IPS (scheda Motore globale)

Questa opzione è applicabile se le azioni di firma sono configurate su “denyAttackerInline” o “denyFlowInline”. Per impostazione predefinita, IPS Cisco IOS applica le ACL alle interfacce da cui proviene il traffico di attacco e non alle interfacce IPS Cisco IOS. L'attivazione di questa opzione consente a IPS Cisco IOS di applicare le ACL direttamente alle interfacce IPS Cisco IOS e non alle interfacce che hanno ricevuto originariamente il traffico di attacco. Non attivare questa impostazione se il router non sta eseguendo il bilanciamento del carico. In caso contrario, se ne consiglia l'attivazione.

Timeout (scheda Motore globale)

Questa opzione consente di impostare il numero di minuti, in un intervallo compreso tra 0 e 65.535, durante i quali le azioni shun hanno validità. Il valore predefinito è 30 minuti. Un'azione shun si verifica se un host o una rete viene aggiunto a una ACL per negarne il traffico.

Aggiungi o Modifica posizione firma

Specifica la posizione da cui IPS Cisco IOS deve caricare un SDF. Per specificare più posizioni SDF, aprire nuovamente questa finestra di dialogo e immettere le informazioni su un altro SDF.

Specificare SDF nel router

Specifica la parte della memoria del router in cui si trova il file SDF tramite il menu a tendina Percorso. Ad esempio: il menu potrebbe visualizzare le voci *disk0*, *usbflash1*, e *flash*. Selezionare quindi il nome file facendo clic sulla freccia giù vicino al campo Nome file o immettere nel campo il nome del file.

Specifica SDF utilizzando l'URL

Se il file SDF è situato su un sistema remoto è possibile specificare l'URL in cui si trova.

Protocollo

Selezionare il protocollo che il router deve utilizzare per ottenere l'SDF, ad esempio *http* o *https*.

URL

Immettere l'URL nella forma indicata di seguito:

percorso-al-file-SDF

Nota Il protocollo selezionato dal menu Protocollo viene visualizzato alla destra del campo URL. *Non* immettere nuovamente il protocollo nel campo URL.

Il seguente URL è fornito come un esempio del formato. *Non* è un URL valido per un file SDF e include il protocollo per mostrare tutto URL:

```
https://172.16.122.204/mysigs/vsensor.sdf
```

Salvataggio automatico

Fare clic su questa opzione se si desidera che il router salvi automaticamente l'SDF in caso di crash del router. In questo modo si elimina la necessità di riconfigurare IPS Cisco IOS con questo SDF quando il router torna in funzione.

Modifica IPS: Messaggi SDEE

In questa finestra sono elencati i messaggi SDEE ricevuti dal router. I messaggi SDEE vengono generati quando sono apportate modifiche alla configurazione IPS Cisco IOS.

Messaggi SDEE

Scegliere il tipo di messaggio SDEE da visualizzare:

- Tutto— Vengono visualizzati i messaggi di errore, di stato e di avviso SDEE.
- Errore— Vengono visualizzati soltanto i messaggi di errore SDEE.
- Stato— Vengono visualizzati soltanto i messaggi di stato SDEE.
- Avvisi— Vengono visualizzati soltanto i messaggi di avviso SDEE.

Seleziona per

Consente di selezionare il messaggio SDEE per la ricerca.

Criterio

Consente di immettere la stringa di ricerca.

Pulsante Vai

Fare clic su questo pulsante per avviare la ricerca della stringa immessa nel campo Criterio.

Tipo

I tipi sono: Errore, Stato e Avvisi. Fare clic su Testo dei messaggi SDEE per visualizzare gli eventuali messaggi SDEE.

Ora

Indica l'ora di ricezione del messaggio.

Descrizione

Visualizza la descrizione presente.

Pulsante Aggiorna

Consente di verificare se ci sono nuovi messaggi SDEE.

Pulsante Chiudi

Consente di chiudere la finestra Messaggi SDEE.

Testo dei messaggi SDEE

Di seguito sono elencati i possibili messaggi SDEE:

Messaggi di stato IDS

Messaggio di errore

```
ENGINE_BUILDING: %s - %d signatures - %d of %d engines
```

Descrizione Si attiva quando IPS Cisco IOS inizia la creazione del micromotore firme (SME).

Messaggio di errore

```
ENGINE_BUILD_SKIPPED: %s - there are no new signature
definitions for this engine
```

Descrizione Si attiva quando non ci sono definizioni di firma o modifiche alle definizioni di firma esistenti in un sistema di rilevamento intrusioni SME.

Messaggio di errore

```
ENGINE_READY: %s - %d ms - packets for this engine will be
scanned
```

Descrizione Si attiva quando un sistema IDS SME è stato creato ed è pronto per analizzare i pacchetti.

Messaggio di errore

```
SDF_LOAD_SUCCESS: SDF loaded successfully from %s
```

Descrizione Si attiva quando viene completato il caricamento di un file SDF da una determinata posizione.

Messaggio di errore

```
BUILTIN_SIGS: %s to load builtin signatures
```

Descrizione Si attiva quando il router carica le firme incorporate.

Messaggi di errore IDS

Messaggio di errore

```
ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s
```

Descrizione Si attiva quando IPS Cisco IOS non riesce a costruire uno dei motori dopo il caricamento di un file SDF. Per ogni errore del motore viene inviato un messaggio. Ciò significa che il motore del sistema IPS Cisco IOS non ha completato l'importazione delle firme per il motore specificato nel messaggio. La causa più probabile del problema è la memoria insufficiente. Se ciò avviene, la nuova firma importata che appartiene a questo motore viene annullata da IPS Cisco IOS.

Messaggio di errore

```
SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d
```

Descrizione Si attiva quando un file SDF non esegue correttamente l'analisi.

Messaggio di errore

```
SDF_PARSE_FAILED: failed to %s SDF from %s
```

Descrizione Si attiva quando il caricamento di un file SDF non viene completato.

Messaggio di errore

```
DISABLED: %s - IDS disabled
```

Descrizione IDS è stato disattivato. Il messaggio ne indica la causa.

Messaggio di errore

```
SYSERROR: Unexpected error (%s) at line %d func %s() file %s
```

Descrizione Si attiva in caso di errore di sistema interno imprevisto.

Modifica IPS: Impostazioni globali

Sono disponibili numerose opzioni di configurazione di IPS Cisco IOS con l'immagine Cisco IOS 12.4(11)T e versioni successive. Tali opzioni sono descritte in questo argomento della Guida. I controlli su schermo e le opzioni di configurazione disponibili nelle versioni di Cisco IOS precedenti alla 12.4(11)T, quali Syslog e le impostazioni globali SDEE, sono descritte in Modifica IPS: Impostazioni globali.

Questo argomento della Guida descrive la finestra Impostazioni globali visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

Opzioni motore

Le opzioni motore disponibili con Cisco IOS 12.4(11)T e immagini di versioni successive sono le seguenti:

- Errore chiuso: per impostazione predefinita, mentre Cisco IOS compila una nuova firma per un determinato motore, autorizza il passaggio di pacchetti senza cercare il motore corrispondente. Se attivata, questa opzione provoca la perdita dei pacchetti da parte di Cisco IOS durante il processo di compilazione.
- Nega azione sull'interfaccia IPS : opzione consigliata quando il router esegue il bilanciamento del carico. Una volta attivata, questa opzione determina l'attivazione da parte di IPS Cisco IOS delle ACL sulle interfacce IPS Cisco IOS piuttosto che sulle interfacce da cui proviene il traffico di attacco.

Modifica tabella prerequisiti IPS

In questa tabella sono visualizzate le informazioni sul metodo di provisioning del router per IPS Cisco IOS. Fare clic su **Modifica** per modificare questi valori. I dati campione della seguente tabella indicano che la posizione di configurazione si trova nella directory configloc nella memoria flash, che il router utilizza la categoria di base di firme e che la chiave pubblica è stata configurata in modo da consentire al router di accedere alle informazioni nella directory configloc.

Nome elemento	Valore elemento
Posizione di configurazione	flash:/configloc/
Categoria selezionata	di base
Chiave pubblica	Configurata

Modifica impostazioni globali

La finestra di dialogo Modifica impostazioni globali contiene una scheda Syslog e SDEE e una scheda Motore globale. Fare clic sul seguente collegamento per le informazioni che si desidera visualizzare:

- Scheda Syslog e SDEE
- Scheda Motore globale

Scheda Syslog e SDEE

La finestra di dialogo Syslog e SDEE visualizzata se il router utilizza un'immagine Cisco IOS 12.4(11)T o versione successiva, consente di configurare le notifiche e i parametri syslog per le registrazioni, gli eventi e i messaggi SDEE.

Attiva notifica Syslog

Selezionare questa casella di controllo per consentire al router di inviare avvisi, eventi e messaggi di errore a un server syslog. Per il funzionamento del metodo di notifica occorre identificare un server syslog nelle proprietà di sistema.

SDEE

Immettere il numero delle registrazioniSDEE contemporanee, nell'intervallo 1–3, nel campo Numero di registrazioni SDEE contemporanee. Per registrazione SDEE si intende un flusso in tempo reale di eventi SDEE.

Nel campo Maximum number of SDEE alerts to store (Numero massimo di avvisi SDEE da archiviare), immettere il numero massimo di avvisi SDEE che si desidera far archiviare dal router, in un intervallo compreso tra 10 e 2000. Per archiviare più avvisi è necessario l'utilizzo di una maggiore memoria del router.

Nel campo Maximum number of SDEE messages to store (Numero massimo di messaggi SDEE da archiviare), immettere il numero massimo di messaggi SDEE che si desidera far archiviare dal router, in un intervallo compreso tra 10 e 500. Per archiviare più messaggi è necessario l'utilizzo di una maggiore memoria del router.

Scheda Motore globale

La finestra di dialogo Motore globale visualizzata se il router utilizza un'immagine Cisco IOS 12.4(11)T o versione successiva, consente di configurare le impostazioni descritte nelle seguenti sezioni.

Attiva chiusura per errore motore

Per impostazione predefinita, mentre il software Cisco IOS compila una nuova firma per un determinato motore, autorizza il passaggio di pacchetti senza cercare il motore corrispondente. Attivare questa opzione per determinare la perdita dei pacchetti da parte del software Cisco IOS durante il processo di compilazione.

Attiva Nega azione sull'interfaccia IPS

Questa opzione è applicabile se le azioni di firma sono configurate su “denyAttackerInline” o “denyFlowInline”. Per impostazione predefinita, IPS Cisco IOS applica le ACL alle interfacce da cui proviene il traffico di attacco e non alle interfacce IPS Cisco IOS. L'attivazione di questa opzione consente a IPS Cisco IOS di applicare le ACL direttamente alle interfacce IPS Cisco IOS e non alle interfacce che hanno ricevuto originariamente il traffico di attacco. Non attivare questa impostazione se il router non sta eseguendo il bilanciamento del carico. In caso contrario, se ne consiglia l'attivazione.

Modifica prerequisiti IPS

La finestra di dialogo Modifica prerequisiti IPS contiene schede per le seguenti categorie di informazioni. Fare clic su un collegamento per le informazioni che si desidera visualizzare:

- Scheda Posizione di configurazione
- Scheda Selezione categoria
- Scheda Chiave pubblica

Scheda Posizione di configurazione

Se sul router è stata configurata una posizione di configurazione, questo può essere modificato. Se sul router non è stata configurata una posizione di configurazione, fare clic su Aggiungi e configurarne uno. Il pulsante Aggiungi è disattivato se è già stata configurata una posizione di configurazione. Il pulsante Modifica è disattivato se è non è stata configurata alcuna posizione di configurazione. Per maggiori informazioni vedere la sezione Crea IPS: Posizione di configurazione e Categoria.

Scheda Selezione categoria

Se si specifica una categoria di firma, SDM configura il router con un set secondario di firme appropriate per una quantità specifica di memoria del router. È inoltre possibile rimuovere una configurazione di categoria esistente per rimuovere i vincoli di categoria durante la selezione delle firme.

Configura categoria

Fare clic su **Configura categoria** e scegliere **di base** o **avanzata**. La categoria di base è adatta ai router con meno di 128 MB di memoria flash disponibile. La categoria avanzata è adatta ai router con più di 128 MB di memoria flash disponibile.

Elimina categoria

Per rimuovere la configurazione di categoria, fare clic su **Elimina categoria**.

Scheda Chiave pubblica

Questa finestra di dialogo visualizza le chiavi pubbliche configurate per IPS Cisco IOS. Da questa finestra è possibile aggiungere o eliminare le chiavi. Per aggiungere una chiave, fare clic su **Aggiungi** e configurare la chiave nella finestra di dialogo visualizzata.

Per rimuovere una chiave, selezionare il nome della chiave e fare clic su **Elimina**.

Aggiungi chiave pubblica

È possibile copiare il nome della chiave e la chiave stessa dal seguente sito di Cisco.com:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Copiare il nome della chiave e incollarlo nel campo Nome di questa finestra di dialogo. Copiare quindi la chiave dallo stesso percorso e incollarla nel campo Chiave. Per le istruzioni dettagliate che illustrano in modo preciso quali parti di testo copiare e incollare, consultare Configura chiave pubblica.

Modifica IPS: Aggiornamento automatico

Gli aggiornamenti del file delle firme vengono pubblicati su Cisco.com. Cisco SDM può eseguire il download dell'aggiornamento del file delle firme specificato dall'utente o eseguire automaticamente il download dell'aggiornamento del file delle firme più recente con pianificazione predefinita.

Questo argomento della Guida descrive la finestra Aggiornamento automatico visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

Prima di configurare l'aggiornamento automatico

Prima di configurare l'aggiornamento automatico, è necessario sincronizzare l'orologio del router con quello del PC. A questo scopo, completare i seguenti passaggi:

Passo 1 Andare ad **Configura** > **Attività aggiuntive** > **Proprietà router** > **Data/Ora**.

Passo 2 Nella finestra Data/Ora, fare clic su **Modifica impostazioni**.

Passo 3 Selezionare l'opzione **Sincronizza con l'orologio del PC locale**, quindi fare clic sul pulsante **Sincronizza**.

Passo 4 Chiudere la finestra di dialogo.

Download del file delle firme da Cisco.com

Per fare in modo che Cisco SDM esegua il download di un file delle firme specifico da Cisco.com al proprio PC, specificare il file di cui Cisco SDM deve eseguire il download e specificare il percorso di salvataggio. Il pacchetto di firme in uso visualizza la versione attualmente utilizzata da IPS Cisco IOS. È necessario eseguire un accesso CCO per eseguire il download dei file delle firme e ottenere altre informazioni dalle pagine Web the IPS Cisco IOS di Cisco.com.

Per eseguire il download del file delle firme più recente, fare clic su **Ottieni file più recente**. Fare clic su **Sfoglia** per specificare il percorso di salvataggio del file, quindi fare clic su **Download** per salvare il file sul PC.

Per sfogliare i file disponibili prima del download, fare clic su **Elenca i file disponibili per il download**. Fare quindi clic sul pulsante a destra del campo Elenco di pacchetti di firme. Fare clic su **Aggiorna** nel menu contestuale per sfogliare l'elenco di file disponibili. Per visualizzare il file readme, fare clic su **Mostra readme**. Scegliere il file desiderato e utilizzare i pulsanti **Sfoglia** e **Download** per salvarlo sul PC.

Aggiornamento automatico

Fare clic su **Attiva Aggiornamento automatico** per fare in modo che Cisco SDM ottenga automaticamente gli aggiornamenti dal server remoto specificato dall'utente.

Impostazioni URL aggiornamento automatico IPS

Immettere il nome utente e la password per l'accesso al server, quindi immettere l' URL al file di aggiornamento nei campi Impostazioni URL aggiornamento automatico IPS. Questo è un esempio di URL:

```
tftp//:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

Pianifica

Specificare una pianificazione per il recupero da parte del router dell'aggiornamento da un server. È possibile specificare più valori in ciascuna colonna per indicare un intervallo o per indicare più valori temporali. Per specificare che si desidera recuperare l'aggiornamento dal server all'1:00 a.m. di ogni giorno, dalla Domenica al Sabato, scegliere i valori nella seguente tabella.

Minuto	Ora	Data	Giorno
0	1	Selezionare 1 e 31.	Selezionare le caselle da Domenica a Giovedì.

Fare clic su **Applica modifiche** per inviare al router le modifiche apportate nei campi Aggiornamento automatico. Fare clic su **Annulla modifiche** per rimuovere i dati immessi in tali campi.

Modifica IPS: Configurazione SEAP

IPS Cisco IOS disponibile con Cisco IOS 12.4(11)T o versioni successive implementa il SEAP (Signature Event Action Processing). Questa finestra descrive le funzionalità SEAP configurabili. Per iniziare con la configurazione, fare clic su uno dei pulsanti sotto il pulsante Configurazione SEAP.

È possibile configurare le impostazioni SEAP di IPS Cisco IOS se sul router è in esecuzione Cisco IOS 12.4(11)T e versioni successive.

Modifica IPS: Configurazione SEAP: Classificazione valore di destinazione

La classificazione del valore di destinazione (TVR, Target Value Rating) è un valore definito dall'utente che rappresenta il valore percepito dell'host di destinazione. Ciò consente all'utente di aumentare il rischio di un evento associato a un sistema critico e di ridurre l'enfasi del rischio di un evento su una destinazione di valore ridotto.

Utilizzare i pulsanti a destra delle colonne Classificazione valore di destinazione e Indirizzo IP di destinazione per aggiungere, rimuovere e modificare le voci di destinazione. Fare clic su **Seleziona tutto** per evidenziare automaticamente tutte le classificazioni del valore di destinazione. Fare clic su **Aggiungi** per visualizzare una finestra di dialogo in cui creare una nuova voce TVR. Fare clic su **Modifica** per modificare le informazioni relative all'indirizzo IP di una voce.

Colonna Classificazione valore di destinazione

La destinazione può essere valutata come Alta, Bassa, Media, Critica o Nessun valore. Una volta creata una voce di destinazione, la classificazione non può essere modificata. Se si deve cambiare la classificazione, è necessario eliminare la voce di destinazione e ricrearla usando la classificazione desiderata.

Colonna Indirizzo IP di destinazione

L'indirizzo IP di destinazione può essere un indirizzo IP singolo o un intervallo di indirizzi IP. Nel seguente esempio vengono riportate due voci: una è una voce di indirizzo IP singolo e l'altra è un intervallo di indirizzi.

Classificazione valore di destinazione	Indirizzo IP di destinazione
Alta	192.168.33.2
Media	10.10.3.1-10.10.3.55

Applica modifiche

Dopo avere immesso le informazioni desiderate nella finestra Classificazione valore di destinazione, fare clic su **Applica modifiche**. Il pulsante **Applica Modifiche** è disabilitato se non sono presenti modifiche da inviare al router.

Annulla modifiche

Per cancellare le informazioni immesse nella finestra Classificazione valore di destinazione e non inviarle al router, fare clic su **Annulla modifiche**. Il pulsante Annulla Modifiche è disabilitato se non sono presenti modifiche in attesa di essere inviate al router.

Aggiungi classificazione valore destinazione

Per aggiungere una voce TVR, scegliere la classificazione del valore di destinazione e immettere un indirizzo IP di destinazione o un intervallo di indirizzi IP.

Classificazione valore di destinazione (TVR)

La destinazione può essere valutata come Alta, Bassa, Media, Critica o Nessun valore. Una volta utilizzata una classificazione per un voce di destinazione, non è possibile utilizzarla per le altre voci. Di conseguenza, immettere nella stessa voce tutte le destinazioni a cui si desidera assegnare la stessa classificazione.

Indirizzi IP di destinazione

È possibile immettere un indirizzo IP singolo o un intervallo di indirizzi, come riportato nel seguente esempio:

```
192.168.22.33
10.10.11.4-10.10.11.55
```

Gli indirizzi IP immessi vengono visualizzati nella finestra Classificazione valore di destinazione.

Modifica IPS: Configurazione SEAP: Sostituzioni azione evento

Le sostituzioni di azioni evento consentono di modificare le azioni associate a un evento in base alla Classificazione rischio (RR, Risk Rating) di tale evento. Ciò avviene assegnando un intervallo RR per ciascuna azione evento. Se si verifica un evento e l'RR ricade nell'intervallo definito, l'azione viene aggiunta all'evento. Le sostituzioni di azioni evento rappresentano un modo per aggiungere azioni evento in modo globale senza dovere configurare singolarmente ogni firma.

Utilizza sostituzioni azioni evento

Selezionare la casella Utilizza sostituzioni azioni evento per fare in modo che IPS Cisco IOS utilizzi le sostituzioni di azioni evento. È possibile aggiungere o modificare le sostituzioni di azioni evento sia che queste siano attivate sul router o meno.

Seleziona tutti

Il pulsante Seleziona tutto funziona con i pulsanti Attiva, Disattiva ed Elimina. Per attivare o disattivare tutte le sostituzioni di azioni evento, fare clic su **Seleziona tutto**, quindi su **Attiva** o **Disattiva**. Per rimuovere tutte le sostituzioni di azioni evento, fare clic su **Seleziona tutto**, quindi su **Elimina**.

Pulsanti Aggiungi e Modifica

Fare clic su **Aggiungi** per visualizzare una finestra di dialogo in cui immettere le informazioni relative a una sostituzione di azioni evento. Scegliere una sostituzione di azioni evento e fare clic su **Modifica** per modificare le informazioni relative a una sostituzione di azioni evento.

Elimina

Fare clic su **Elimina** per rimuovere le sostituzioni di azioni evento selezionate o per rimuoverle tutte nel caso sia stato fatto clic su **Seleziona tutto**.

Attiva e Disattiva

I pulsanti Attiva e Disattiva consentono di attivare o disattivare le sostituzioni di azioni evento. Scegliere una sostituzione di azioni evento o fare clic su **Seleziona tutto** per attivare o disattivare tutte le sostituzioni di azioni evento.

Applica modifiche

Dopo avere immesso le informazioni desiderate nella finestra Sostituzioni azioni evento, fare clic su **Applica modifiche**. Il pulsante **Applica Modifiche** è disabilitato se non sono presenti modifiche da inviare al router.

Annulla modifiche

Per cancellare le informazioni immesse nella finestra Sostituzione azioni evento e non inviarle al router, fare clic su **Annulla modifiche**. Il pulsante **Annulla modifiche** è disabilitato se non sono presenti modifiche in attesa di essere inviate al router.

Aggiungi o Modifica sostituzione azioni evento

Per aggiungere una sostituzione di azioni evento, scegliere l'azione evento, attivarla o disattivarla e specificare l'intervallo RR. Se si sta apportando una modifica, non è possibile modificare l'azione evento.

Azione evento

Scegliere una delle seguenti azioni evento:

- Deny Attacker Inline**:** impedisce la trasmissione di questo pacchetto e di quelli successivi dall'indirizzo dell'autore dell'attacco per un periodo di tempo determinato (solo in linea).
- Deny Connection Inline**:** impedisce la trasmissione di questo pacchetto e di quelli successivi sul flusso TCP (solo in linea).
- Deny Packet Inline**:** impedisce la trasmissione del pacchetto.
- Produce Alert**:** scrive un <evIdsAlert> nel registro eventi.
- Reset TCP Connection**:** invia reimpostazioni TCP per deviare e terminare il flusso TCP.

Attivato

Fare clic su **Sì** per attivare la sostituzione di azioni evento o su **No** per disattivarla. È anche possibile attivare o disattivare le sostituzioni di azioni evento nella finestra Sostituzione azioni evento.

Classificazione rischio

Immettere il limite minimo dell'intervallo RR nella casella Min e quello massimo nella casella Max. Se il valore RR di un evento ricade nell'intervallo specificato, IPS Cisco IOS aggiunge la sostituzione specificata dall'Azione evento. Se ad esempio a Impedisci connessione in linea è assegnato un intervallo RR di 90-100 e si verifica un evento con RR 95, IPS Cisco IOS risponde impedendo la connessione in linea.

Modifica IPS: Configurazione SEAP: Filtri azione evento

I filtri di azione evento consentono a IPS Cisco IOS di eseguire singole azioni in risposta a un evento senza dover eseguire tutte le azioni o dover rimuovere l'intero evento. I filtri agiscono rimuovendo azioni da un evento. Un filtro che rimuove tutte le azioni da un evento consuma di fatto l'evento. I filtri di azione evento vengono elaborati come un elenco ordinato. È possibile spostare i filtri in alto o in basso nell'elenco per fare in modo che il router elabori un filtro prima di altri.

La finestra Filtri azione evento visualizza i filtri di azione evento configurati e consente di riordinare l'elenco di filtri in modo che IPS Cisco IOS li elabori nell'ordine desiderato.

Utilizza filtri azione evento

Selezionare **Utilizza filtri Azione evento** per attivare l'utilizzo dei filtri di azione evento. È possibile aggiungere, modificare e rimuovere i filtri di azione evento e riorganizzare l'elenco in modo che il router elabori i filtri nel caso il filtraggio di azione evento sia attivato o meno.

Area Elenco filtri azione evento

Per la descrizione delle colonne dell'area Elenco filtri azione evento, consultare Aggiungi o Modifica filtro azioni evento.

Pulsanti Elenco filtri azione evento

I pulsanti dell'Elenco filtri azione evento consentono di creare, modificare e rimuovere i filtri di azione evento e di posizionare ciascun filtro di azione evento nell'ordine desiderato nell'elenco. I pulsanti vengono descritti nelle sezioni seguenti.

Seleziona tutto

Il pulsante **Seleziona tutto** è utilizzabile con i pulsanti **Attiva**, **Disattiva** ed **Elimina**. Per attivare o disattivare tutti i filtri di azione evento, fare clic su **Seleziona tutto**, quindi su **Attiva** o **Disattiva**. Per rimuovere tutti i filtri di azione evento, fare clic su **Seleziona tutto**, quindi su **Elimina**.

Aggiungi

Fare clic su **Aggiungi** per aggiungere un filtro di azione evento alla fine dell'elenco. Viene visualizzata una finestra di dialogo che consente di immettere i dati del filtro.

Inserisci prima

Per inserire un nuovo filtro di azione evento prima di uno esistente, selezionare la voce di filtro esistente e fare clic su **Inserisci prima**. Viene visualizzata una finestra di dialogo che consente di immettere i dati del filtro.

Inserisci dopo

Per inserire un nuovo filtro di azione evento dopo di uno esistente, selezionare la voce di filtro esistente e fare clic su **Inserisci dopo**. Viene visualizzata una finestra di dialogo che consente di immettere i dati del filtro.

Sposta su

Scegliere un filtro di azione evento e fare clic su **Sposta su** per spostare il filtro verso l'alto nell'elenco.

Sposta giù

Scegliere un filtro di azione evento e fare clic su **Sposta giù** per spostare il filtro verso il basso nell'elenco.

Modifica

Fare clic su **Modifica** per modificare un filtro di azione evento scelto.

Attiva

Fare clic su **Attiva** per attivare un filtro di azione evento scelto. Per attivare tutti i filtri di azione evento, fare prima clic su **Seleziona tutto**, quindi su **Attiva**.

Disattiva

Fare clic sul pulsante **Disattiva** per disattivare un filtro di azione evento scelto. Per disattivare tutti i filtri di azione evento, fare prima clic su **Seleziona tutto**, quindi su **Disattiva**.

Elimina

Fare clic sul pulsante **Elimina** per eliminare un filtro di azione evento scelto. Per eliminare tutti i filtri di azione evento, fare prima clic su **Seleziona tutto**, quindi su **Elimina**.

Applica modifiche

Dopo avere immesso le informazioni desiderate in questa finestra, fare clic su **Applica modifiche**. Il pulsante Applica Modifiche è disabilitato se non sono presenti modifiche da inviare al router.

Annulla modifiche

Per cancellare le informazioni immesse in questa finestra e non inviarle al router, fare clic su **Annulla modifiche**. Il pulsante Annulla modifiche è disattivato se non sono presenti modifiche in attesa di essere inviate al router.

Aggiungi o Modifica filtro azioni evento

Le seguenti informazioni descrivono i campi delle finestre di dialogo Aggiungi e Modifica filtro azione evento.

Nome

SDM fornisce i nomi dei filtri di azione evento a partire da Q00000, e aumentando la parte numerica del nome di 1 per ogni filtro di azione evento aggiunto. È anche possibile immettere il nome desiderato. Quando si modifica un filtro di azione evento, il campo Nome è di sola lettura.

Attivato

Fare clic su **Sì** per attivare il filtro di azione evento o su **No** per disattivarlo. È anche possibile attivare o disattivare i filtro di azione evento nella finestra Filtro azione evento.

ID firma

Per ID firma, immettere un intervallo di ID di firma compreso tra 900 e 65535 oppure immettere un ID singolo compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 988-5000.

ID firma secondaria

Per ID firma secondaria, immettere un intervallo di ID firma secondaria compreso tra 0 e 255 oppure immettere un ID firma secondaria singolo compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 70-200.

Indirizzo autore attacco

Per Indirizzo autore attacco, immettere un intervallo di indirizzi compreso tra 0.0.0.0 e 255.255.255.255 oppure immettere un indirizzo singolo compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 192.168.7.0-192.168.50.0.

Porta autore attacco

Per Porta autore attacco, immettere un intervallo di numeri di porta compreso tra 0 e 65535 oppure immettere un singolo numero di porta compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 988-5000.

Indirizzo vittima

Per Indirizzo vittima, immettere un intervallo di indirizzi compreso tra 0.0.0.0 e 255.255.255.255 oppure immettere un indirizzo singolo compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 192.168.7.0-192.168.50.0.

Porta vittima

Per Porta vittima, immettere un intervallo di numeri di porta compreso tra 0 e 65535 oppure immettere un singolo numero di porta compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 988-5000.

Classificazione rischio

Per Classificazione rischio, immettere un intervallo RR compreso tra 0 e 100.

Azioni da sottrarre

Fare clic sulle azioni da sottrarre dagli eventi corrispondenti. Per sottrarre più di un'azione dagli eventi corrispondenti, tenere premuto il tasto **Ctrl** durante la scelta degli eventi aggiuntivi. Tutti gli eventi scelti per questo filtro vengono elencati nella finestra Filtri azione evento.

Arresta se corrispondente

Se si desidera che IPS Cisco IOS venga arrestato se un evento corrisponde a questo filtro di azione evento, fare clic su **Sì**. Se si desidera che IPS Cisco IOS valuti gli eventi corrispondenti rispetto agli altri filtri restanti, fare clic su **No**.

Commenti

È possibile aggiungere commenti descrittivi della finalità del filtro. Questo campo è opzionale.

Modifica IPS: Firme

IPS Cisco IOS impedisce le intrusioni confrontando il traffico con le firme degli attacchi noti. Le immagini Cisco IOS che supportano IPS Cisco IOS dispongono di firme integrate utilizzabili ed è anche possibile fare in modo che IPS Cisco IOS importi le firme che deve utilizzare il router durante l'analisi del traffico. Le firme importate sono immagazzinate in un file SDF (Signature Definition File).

Questa finestra consente di visualizzare le firme IPS Cisco IOS configurate nel router. È possibile aggiungere firme personalizzate o importare firme dai file SDF (Signature Definition File) scaricati dal sito Web Cisco.com. È possibile anche modificare, eliminare, attivare e disattivare firme.

IPS Cisco IOS viene consegnato con un SDF che contiene firme utilizzabili dal router. Per ulteriori informazioni sull'SDF consegnato con IPS Cisco IOS e sulle modalità di utilizzo da parte di IPS Cisco IOS, fare clic File di definizione firme fornito da IPS.

Albero firme

L'albero firme consente di filtrare la lista delle firme sulla destra secondo il tipo di firme che si vogliono visualizzare. Scegliere prima il ramo del tipo generale di firma che si vuole visualizzare. La lista delle firme visualizza le firme configurate disponibili per il tipo scelto. Se alla sinistra di un ramo compare il segno più (+) sono presenti sottocategorie utilizzabili per migliorare il filtro. Fare clic sul segno + per espandere il ramo e selezionare la sottocategoria di firme che si desidera visualizzare. Se l'elenco delle firme è vuoto non ci sono firme configurate disponibili per il tipo scelto.

Ad esempio: se si desidera visualizzare tutte le firme degli attacchi, fare clic sul ramo **Attacco**. Se si desidera vedere le sottocategorie che si possono utilizzare per la visualizzazione delle firme di attacco, fare clic sul segno + accanto alla cartella Attacco. Se si desidera visualizzare le firme DoS (Denial of Service), fare clic sulla cartella **DoS**.

Pulsante Importa

Fare clic per importare un file definizione firme dal PC o dal router. Dopo aver specificato il file, IPS Cisco IOS visualizza le firme disponibili nel file e l'utente può scegliere le firme che desidera importare nel router. Per ulteriori informazioni sul metodo di scelta delle firme da importare vedere Importare firme.

Nota È possibile importare le firme dal router se il router ha un sistema di file basato sul DOS.

Gli SDF sono disponibili presso Cisco. Per scaricare un file SDF visitare il sito Web Cisco all'indirizzo (è necessario l'ID di accesso):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup (in lingua inglese)

Cisco gestisce un centro avvisi in grado di fornire informazioni sulle minacce emergenti. Per maggiori informazioni vedere la sezione Cisco Security Center.

Elenco Seleziona per e Criterio

Gli elenchi a discesa Seleziona per e Criterio consentono di ottenere una diversa visualizzazione in base ai tipi di firme che si desidera visualizzare. Scegliere innanzitutto i criteri nell'elenco a discesa Seleziona per, quindi scegliere il valore corrispondente nell'elenco a discesa Criterio.

Ad esempio: se si seleziona **Motore** nell'elenco Seleziona per, l'elenco Criterio cambia in Motore ed è possibile scegliere tra i motori disponibili, come **Atomic.ICMP** e**Service.DNS**.

Se si seleziona **ID firma** o **Nome firma**, è necessario immettere un valore nel campo dei criteri.

Totale [*n*] Nuove [*n*] Eliminate [*n*]

Viene fornito il conteggio delle firme nuove e di quelle eliminate.

Seleziona tutti

Consente di selezionare tutte le firme nell'elenco.

Aggiungi

Fare clic su **Aggiungi** per eseguire una delle seguenti operazioni:

- **Aggiungi nuovo**: scegliere questa opzione per aggiungere una nuova firma, e fornire parametri firma nella finestra di dialogo visualizzata.
- **Duplica**: l'opzione di duplicazione è attiva se viene specificata una firma che non appartiene al motore codificato. È disattivata se la firma utilizza uno dei motori codificati di Cisco IOS.

Modifica

Consente di modificare i parametri della firma specificata.

Elimina

Fare clic su **Elimina** per contrassegnare le firme specificate per l'eliminazione dall'elenco. Per visualizzare le firme eliminate, fare clic su **Dettagli**. Per ulteriori informazioni sullo stato e la gestione di questo tipo di firme, vedere la sezione Firme contrassegnate per l'eliminazione.

Nota È possibile visualizzare e monitorare le firme OPACL TrendMicro, ma queste non possono essere modificate, eliminate, attivate o disattivate. Se è stata selezionata una firma OPACL TrendMicro, i pulsanti **Modifica**, **Elimina**, **Attiva** e **Disattiva** sono disattivati. Il Server di controllo degli incidenti di Cisco assume il controllo di queste firme.

Attiva

Fare clic su **Attiva** per attivare le firme specificate. Le firme attivate sono contraddistinte da un segno di spunta verde. Se una firma è stata disattivata e poi attivata, nella colonna ! viene visualizzata un'icona gialla di attesa per indicare che la modifica deve essere applicata al router.

Disattiva

Fare clic su **Disattiva** per disattivare le firme specificate. Le firme disattivate sono contrassegnate da un'icona rossa. Se la firma viene disattivata durante la sessione corrente, nella colonna ! viene visualizzata un'icona gialla di attesa per indicare che la modifica deve essere applicata al router.

Pulsante Riepilogo o Dettagli

Consente di visualizzare o nascondere le firme contrassegnate per l'eliminazione.

Elenco firme

Consente di visualizzare le firme recuperate dal router e quelle aggiunte da un file SDF.

Nota Le firme che sono state impostate per l'importazione e sono identiche alle firme distribuite non verranno importate e non saranno visualizzate nell'elenco delle firme.

È possibile filtrare l'elenco utilizzando i controlli di selezione.

Attivato	Le firme attivate sono contrassegnate da un segno di spunta verde. In questo caso quando viene rilevata la firma vengono eseguite le azioni specificate. Le firme disattivate sono contrassegnate da un'icona rossa. In questo caso le azioni sono disattivate e non vengono eseguite.
Avviso (!)	Questa colonna contiene l'icona gialla di attesa.  Questa icona è associata alle nuove firme o alle firme modificate che non sono state inviate al router.

ID firma	Indica l'ID numerico della firma. Ad esempio: l'ID della firma per ICMP Echo Reply è 2000.
ID SubSig	Indica l'ID della firma secondaria.
Nome	Indica il nome della firma. Ad esempio: ICMP Echo Reply.
Azione	Indica l'azione da eseguire quando viene rilevata una firma.
Filtro	Indica una lista di controllo degli accessi (ACL) associata alla firma corrispondente.
Gravità	Indica il livello di gravità dell'evento. I livelli di gravità sono informativa, bassa, media e alta.
Motore	Indica il motore a cui appartiene la firma.

Menu di scelta rapida (tasto destro)

Facendo clic con il tasto destro su una firma, Cisco SDM visualizza un menu di scelta rapida con le seguenti opzioni:

- Azioni: consente di selezionare le azioni da eseguire quando viene rilevata la corrispondenza di una firma. Per maggiori informazioni vedere la sezione Assegnazione di azioni.
- Imposta gravità su: consente di impostare il livello di gravità di una firma su: alta, media, bassa o informativa.
- Ripristina valori predefiniti: consente di ripristinare i valori predefiniti della firma.
- Rimuovi filtro: consente di rimuovere un filtro applicato alla firma.
- Guida in linea NSDB (è richiesto un account CCO): consente di visualizzare la guida in linea Network Security Data Base (NSDB).

Firme contrassegnate per l'eliminazione

Quest'area è visibile quando si preme il pulsante **Dettagli**. Questo pulsante consente di elencare le firme che sono state eliminate dall'elenco delle firme e quelle contrassegnate per l'eliminazione perché le firme importate sono impostate per la sostituzione delle firme già configurate nel router. Per maggiori informazioni vedere la sezione Procedura per l'importazione delle firme.

Le firme contrassegnate per l'eliminazione rimangono attive nella configurazione IPS Cisco IOS finché non si fa clic su **Applica modifiche**. Se si esce dalla finestra delle firme e si disattiva IPS Cisco IOS, le firme contrassegnate saranno eliminate alla riattivazione di IPS Cisco IOS.

Pulsante Annulla Elimina tutto

Consente di ripristinare tutte le firme nell'elenco delle firme contrassegnate come eliminate.

Pulsante Annulla Elimina

Consente di ripristinare determinate firme contrassegnate per l'eliminazione. Le firme non saranno più contrassegnate e verranno ripristinate nell'elenco delle firme attive.

Pulsante Applica modifiche

Consente di inviare al router le firme appena importate, quelle appena attivate o disattivate e le modifiche apportate alle firme. Dopo aver apportato le modifiche, l'icona gialla di attesa scompare dalla colonna contrassegnata dal segno di avviso ! Queste modifiche vengono salvate nella memoria flash del router nel file sdmips.sdf. Questo file viene creato automaticamente quando si seleziona **Applica modifiche**.

Nota Se si cerca di importare delle firme che sono tutte identiche alle firme distribuite, il pulsante **Applica modifiche** verrà disabilitato.

Pulsante Annulla modifiche

Consente di annullare le modifiche effettuate.

Nota Se si cerca di importare delle firme che sono tutte identiche alle firme distribuite, il pulsante **Annulla modifiche** verrà disabilitato.

Porta vittima

Per Porta vittima, immettere un intervallo di numeri di porta compreso tra 0 e 65535 oppure immettere un singolo numero di porta compreso in tale intervallo. Se si immette un intervallo, utilizzare un trattino (-) per separare il limite minore dell'intervallo da quello maggiore. Immettere ad esempio 988-5000.

Classificazione rischio

Per Classificazione rischio, immettere un intervallo RR compreso tra 0 e 100.

Azioni da sottrarre

Fare clic sulle azioni da sottrarre dagli eventi corrispondenti. Per sottrarre più di un'azione dagli eventi corrispondenti, tenere premuto il tasto **Ctrl** durante la scelta degli eventi aggiuntivi. Tutti gli eventi scelti per questo filtro vengono elencati nella finestra Filtri azione evento.

Arresta se corrispondente

Se si desidera che IPS Cisco IOS venga arrestato se un evento corrisponde a questo filtro di azione evento, fare clic su **Sì**. Se si desidera che IPS Cisco IOS valuti gli eventi corrispondenti rispetto agli altri filtri restanti, fare clic su **No**.

Commenti

È possibile aggiungere commenti descrittivi della finalità del filtro. Questo campo è opzionale.

Modifica IPS: Firme

IPS Cisco IOS impedisce le intrusioni confrontando il traffico con le firme degli attacchi noti. Le immagini Cisco IOS che supportano IPS Cisco IOS dispongono di firme integrate utilizzabili da IPS Cisco IOS ed è anche possibile fare in modo che IPS Cisco IOS importi le firme che deve utilizzare il router durante l'analisi del traffico. Le firme importate sono immagazzinate in un file SDF (Signature Definition File).

Questo argomento della Guida descrive la finestra Firme visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

La finestra Firme consente di visualizzare le firme di IPS Cisco IOS configurate sul router. È possibile aggiungere firme personalizzate o importare firme dai file SDF (Signature Definition File) scaricati dal sito Web Cisco.com. È possibile anche modificare, attivare, disattivare, ritirare e annullare il ritiro delle firme.

Albero firme

L'albero firme consente di filtrare l'elenco di firme a destra in base al tipo di firma che si desidera visualizzare. Scegliere prima il ramo del tipo generale di firma che si vuole visualizzare. La lista delle firme visualizza le firme configurate disponibili per il tipo scelto. Se alla sinistra di un ramo compare il segno più (+) sono presenti sottocategorie utilizzabili per migliorare il filtro. Fare clic sul segno + per espandere il ramo e selezionare la sottocategoria di firme che si desidera visualizzare. Se l'elenco delle firme è vuoto non ci sono firme configurate disponibili per il tipo scelto.

Ad esempio: se si desidera visualizzare tutte le firme degli attacchi, fare clic sul ramo **Attacco**. Se si desidera vedere le sottocategorie che si possono utilizzare per la visualizzazione delle firme di attacco, fare clic sul segno + accanto alla cartella Attacco. Se si desidera visualizzare le firme DoS (Denial of Service), fare clic sulla cartella **DoS**.

Pulsante Importa

Fare clic per importare un file definizione firme dal PC o dal router. Dopo aver specificato il file, IPS Cisco IOS visualizza le firme disponibili nel file e l'utente può scegliere le firme che desidera importare nel router. Per ulteriori informazioni sul metodo di scelta delle firme da importare vedere Importare firme.

Nota È possibile importare le firme dal router se il router ha un sistema di file basato sul DOS.

Gli SDF sono disponibili presso Cisco. Per scaricare un file SDF visitare il sito Web Cisco all'indirizzo (è necessario l'ID di accesso):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup (in lingua inglese)

Cisco gestisce un centro avvisi in grado di fornire informazioni sulle minacce emergenti. Per maggiori informazioni vedere la sezione Cisco Security Center.

Elenco Seleziona per e Criterio

Gli elenchi a discesa Seleziona per e Criterio consentono di ottenere una diversa visualizzazione in base ai tipi di firme che si desidera visualizzare. Scegliere innanzitutto i criteri nell'elenco a discesa Seleziona per, quindi scegliere il valore corrispondente nell'elenco a discesa Criterio.

Ad esempio: se si seleziona **Motore** nell'elenco Seleziona per, l'elenco Criterio cambia in Motore ed è possibile scegliere tra i motori disponibili, come **Atomic.ICMP** e **Service.DNS**.

Se si seleziona **ID firma** o **Nome firma**, è necessario immettere un valore nel campo dei criteri.

Totale [*n*]

Viene fornito il numero totale di firme presenti sul router.

Seleziona tutti

Consente di selezionare tutte le firme nell'elenco.

Elenco Seleziona per e Criterio

Gli elenchi a discesa Seleziona per e Criterio consentono di ottenere una diversa visualizzazione in base ai tipi di firme che si desidera visualizzare. Scegliere innanzitutto i criteri nell'elenco a discesa Seleziona per, quindi scegliere il valore corrispondente nell'elenco a discesa Criterio.

Ad esempio: se si seleziona **Motore** nell'elenco Seleziona per, l'elenco Criterio cambia in Motore ed è possibile scegliere tra i motori disponibili, come **Atomic.ICMP** e **Service.DNS**.

Se si seleziona **ID firma** o **Nome firma**, è necessario immettere un valore nel campo dei criteri.

Totale [*n*]

Viene fornito il numero totale di firme presenti sul router.

Seleziona tutti

Consente di selezionare tutte le firme nell'elenco.

Disattiva

Fare clic su **Disattiva** per disattivare la firma specificata. Le firme disattivate sono contrassegnate da un'icona rossa. Se la firma viene disattivata durante la sessione corrente, nella colonna ! viene visualizzata un'icona gialla di attesa per indicare che la modifica deve essere applicata al router.

Ritiro

Fare clic su **Ritiro** per evitare che una firma venga compilata per la scansione.

Annulla ritiro

Fare clic su **Annulla ritiro** per fare in modo che una firma venga compilata per la scansione.

Elenco firme

Visualizza le firme recuperate dal router ed eventuali firme aggiunte da un SDF.

Nota Le firme che sono state impostate per l'importazione e sono identiche alle firme distribuite non verranno importate e non saranno visualizzate nell'elenco delle firme.

È possibile filtrare l'elenco utilizzando i controlli di selezione.

Attivato	Le firme attivate sono contrassegnate da un segno di spunta verde. In questo caso quando viene rilevata la firma vengono eseguite le azioni specificate. Le firme disattivate sono contrassegnate da un'icona rossa. In questo caso le azioni sono disattivate e non vengono eseguite.
Avviso (!)	Questa colonna contiene l'icona gialla di attesa.  Questa icona è associata alle nuove firme o alle firme modificate che non sono state inviate al router.
ID firma	Indica l'ID numerico della firma. Ad esempio: l'ID della firma per ICMP Echo Reply è 2000.
ID SubSig	Indica l'ID della firma secondaria.
Nome	Indica il nome della firma. Ad esempio: ICMP Echo Reply.
Azione	Indica l'azione da eseguire quando viene rilevata una firma.
Gravità	Indica il livello di gravità dell'evento. I livelli di gravità sono informativa, bassa, media e alta.
Classificazione di fedeltà	La classificazione di fedeltà della firma.
Ritirata	Un valore vero o falso. Vero se la firma è stata ritirata. Falso in caso contrario. Le firme ritirate non sono compilate.
Motore	Indica il motore a cui appartiene la firma.

Menu di scelta rapida (tasto destro)

Facendo clic con il tasto destro su una firma, Cisco SDM visualizza un menu di scelta rapida con le seguenti opzioni:

- Azioni: consente di selezionare le azioni da eseguire quando viene rilevata la corrispondenza di una firma. Per maggiori informazioni vedere la sezione Assegnazione di azioni.
- Classificazione di fedeltà: fare clic per immettere una classificazione di fedeltà per la firma.
- Imposta gravità su: consente di impostare il livello di gravità di una firma su: alta, media, bassa o informativa.
- Ripristina valori predefiniti: consente di ripristinare i valori predefiniti della firma.
- Guida in linea NSDB (è richiesto un account CCO): consente di visualizzare la guida in linea Network Security Data Base (NSDB).

Applica modifiche

Fare clic su **Applica modifiche** per inviare al router le firme appena importate, quelle appena attivate o disattivate e le modifiche apportate alle firme. Dopo aver apportato le modifiche, l'icona gialla di attesa scompare dalla colonna contrassegnata dal segno di avviso ! Queste modifiche vengono salvate nella memoria flash del router nel file sdmips.sdf. Questo file viene creato automaticamente quando si seleziona **Applica modifiche**.

Nota Se si cerca di importare delle firme che sono tutte identiche alle firme distribuite, il pulsante **Applica modifiche** verrà disabilitato.

Annulla modifiche

Fare clic su **Annulla modifiche** per annullare le modifiche effettuate.

Nota Se si cerca di importare delle firme che sono tutte identiche alle firme distribuite, il pulsante **Annulla modifiche** verrà disabilitato.

Modifica firma

Utilizzare i campi nella finestra di dialogo Modifica firma per modificare la firma selezionata. Le modifiche vengono memorizzate in un file delta salvato nella memoria flash del router. Gli elementi delle firme vengono descritti nelle seguenti sezioni.

Questo argomento della Guida descrive la finestra Modifica firme visualizzata se il router esegue Cisco IOS 12.4(11)T e versioni successive.

ID firma

Valore numerico univoco assegnato alla firma. Questo valore consente a IPS Cisco IOS di identificare una determinata firma.

ID firma secondaria

Valore numerico univoco assegnato alla firma secondaria. L'ID firma secondaria viene utilizzato per identificare una versione più granulare di una firma complessa.

Gravità avviso

Scegliere uno dei valori seguenti per categorizzare la gravità dell'avviso: Alta, Media, Bassa o Informativa.

Classificazione di fedeltà firma

La classificazione di fedeltà della firma è un valore impostato dall'autore della firma per quantificare l'affidabilità della firma nel generare veri positivi. Questo valore è impostato prima che la firma venga distribuita e può essere modificato quando i dati di prestazioni della firma sono disponibili.

Promiscuous Delta

Il delta promiscuo è un fattore sottratto dalla classificazione rischio (RR) di un evento se il router funziona in modalità promiscua. Il Delta promiscuo viene sottratto dall'RR ogni volta che viene generato un avviso se il sistema è distribuito in modalità promiscua.

Nota Sebbene il delta promiscuo possa essere riconfigurato in base a una firma, si consiglia di non modificare alcuna opzione predefinita di delta promiscuo.

Descrizione firma

La descrizione della firma comprende il nome e la versione della firma, eventuali noti di avviso disponibili dal Cisco Security Center, i commenti dell'utente e altre informazioni.

Motore

Il motore firme associato a questa firma. Un motore comunemente utilizzato è l'Atomic IP con nome.

La casella Motore contiene i campi che consentono di configurare un'ampia gamma di parametri di firma. È ad esempio possibile specificare l'azione da intraprendere se la firma è associata e viene generato un evento, è possibile specificare il protocollo di livello 4 da ispezionare per gli eventi corrispondenti a questa firma, nonché specificare i parametri IP, quali lunghezza dell'intestazione e tipo di servizio.

Event Counter

I controlli nella casella Event Counter consentono di specificare i parametri descritti nelle seguenti sezioni.

Event Count

Numero di volte che un evento deve verificarsi prima che venga generato un avviso.

Event Count Key

Tipo di informazioni da utilizzare per considerare un evento come verificatosi. Se ad esempio si scelgono gli indirizzi sia dall'**autore dell'attacco che quello della vittima e le relative porte**, ogni volta che sono disponibili questi 4 elementi di informazione per un evento, il conteggio aumenta di 1. Se si sceglie l'**indirizzo dell'autore dell'attacco**, sarà necessaria solo tale parte di informazione.

Event Interval

Numero di secondi tra l'invio degli eventi al registro eventi. Se si seleziona **Sì**, viene visualizzato un campo aggiuntivo che consente di immettere il numero di secondi.

Alert Frequency

La finalità del parametro di frequenza avviso è quella di ridurre il volume di avvisi scritti nel registro eventi.

Summary Mode

Sono disponibili quattro modalità: Fire All, Fire Once, Summarize e Global Summarize. La modalità di riepilogo viene modificata dinamicamente per adattare il volume di avvisi corrente. È ad esempio possibile configurare la firma su Visualizza tutti ma dopo il raggiungimento di una determinata soglia, viene avviato il riepilogo.

Summary Key

Tipo di informazioni da utilizzare per determinare quando creare il riepilogo. Se ad esempio si scelgono **sia l'indirizzo dell'autore dell'attacco che quello della vittima e le relative porte**, ogni volta che sono disponibili queste 4 informazioni per un evento, viene avviato il riepilogo. Se si sceglie **l'indirizzo dell'autore dell'attacco**, sarà necessaria solo questa informazione.

Specifica soglia riepilogo globale

È possibile specificare le soglie numeriche da utilizzare per determinare quando riepilogare gli eventi nel registro eventi. Se si sceglie **Sì**, è possibile specificare la soglia di riepilogo globale e un intervallo di riepilogo.

Stato

È possibile specificare se la firma deve essere attivata, disattivata o ritirata nella casella Stato. Inoltre, la casella Stato può visualizzare le firme rese obsolete.

Selezione dei file

Questa finestra consente di caricare un file dal proprio router. In questa finestra si possono vedere soltanto i file di tipo DOSFS.

Il lato sinistro della finestra visualizza una struttura ad albero espandibile che rappresenta il sistema delle directory della memoria flash del proprio router Cisco e dei dispositivi USB collegati a tale router.

Il lato destro della finestra visualizza un elenco dei nomi dei file e delle directory che si trovano nella directory specificata nel lato sinistro della finestra. Qui è inoltre visibile la dimensione in byte e la data e l'ora dell'ultima modifica di ciascun file o directory.

È possibile scegliere un file da caricare nell'elenco sul lato destro della finestra. Sotto l'elenco dei file, è disponibile il campo Nome file che contiene il percorso completo del file specificato.

Nota Se si sta scegliendo un file di configurazione per il provisioning del router, questo deve essere un file CCCD o avere l'estensione .cfg.

Nome

Fare clic su **Nome** per ordinare alfabeticamente i file e le directory in base al loro nome. Facendo di nuovo clic su **Nome**, l'ordine viene invertito.

Dimensioni

Fare clic su **Dimensioni** per disporre in ordine di dimensione i file e le directory. La dimensione delle directory misura sempre zero byte, anche quando esse non sono vuote. Facendo di nuovo clic su **Dimensioni**, l'ordine viene invertito.

Ora di modifica

Fare clic su **Ora di modifica** per disporre in ordine secondo la data e l'ora di modifica. Facendo di nuovo clic su **Ora di modifica** l'ordine viene invertito.

Assegnazione di azioni

Questa finestra contiene le azioni che possono essere intraprese quando viene rilevata la corrispondenza di una firma. Le azioni disponibili dipendono dalla firma. Di seguito vengono elencate quelle più comuni:

- **alarm**: genera un messaggio di allarme. Simili a **produce-verbose-alert**.
- **deny-attacker-inline**: crea un'ACL che rifiuta tutto il traffico proveniente dall'indirizzo IP considerato dal sistema dal sistema IPS Cisco IOS come l'origine dell'attacco. Simile a **denyAttackerInline**.
- **deny-connection-inline**: consente di eliminare il pacchetto e tutti i pacchetti futuri su questo flusso TCP. Simile a **produce-alert** e **denyFlowInline**.
- **deny-packet-inline**: impedisce la trasmissione del pacchetto (solo in linea). Simile a **drop**.
- **denyAttackerInline**: crea un'ACL che rifiuta tutto il traffico proveniente dall'indirizzo IP considerato dal sistema dal sistema IPS Cisco IOS come l'origine dell'attacco. Simile a **deny-attacker-inline**.
- **denyFlowInline**: crea un'ACL che rifiuta tutto il traffico dall'indirizzo IP che è considerato l'origine dell'attacco 5-tuple (ip src, porta src, ip dst, porta dst e protocollo 14). denyFlowInline è più granulare rispetto a denyAttackerInline Simile a **produce-alert** e **deny-connection-inline**.
- **drop**: consente di eliminare il pacchetto di attacco. Simile a **deny-packet-inline**.
- **produce-alert**: genera un avviso. Simile a **denyFlowInline** e **deny-connection-inline**.
- **produce-verbose-alert**: genera un avviso con include un dump codificato del pacchetto di attacco. Simile ad **alarm**.
- **reset**: reimposta la connessione e consente di eliminare il pacchetto di attacco. Simile a **reset-tcp-connection**.
- **reset-tcp-connection**: invia TCP RESETS per terminare il flusso TCP. Simile a **reset**.

Importare firme

Utilizzare la finestra Importa IPS per importare nel PC le firme da un file SDF o di altro tipo. Le informazioni contenute in questa finestra indicano quali firme sono disponibili nell'SDF e quali di esse sono già installate nel proprio router.

Procedura per l'importazione delle firme

Per impostare le firme, seguire i passaggi seguenti:

Passo 1 Utilizzare l'albero firme e gli elenchi a discesa Seleziona per e Criterio per visualizzare le firme che si desidera importare.

Nell'elenco delle firme, deselezionare la casella di controllo **Importa** per le firme che *non* si desidera importare. Se si desidera deselezionare la casella di controllo **Importa** per tutte le firme, fare clic sul pulsante **Deseleziona tutti**, che diventa il pulsante **Seleziona tutti**.

Passo 2 Selezionare la casella di controllo **Non importare firme che sono definite come disattivate** se non si desidera impedire l'importazione di firme il cui utilizzo potrebbe ridurre le prestazioni del router.

Passo 3 Fare clic sul pulsante **Unisci** per unire le firme importate con quelle già configurate nel router oppure il pulsante **Sostituisci** per sostituire le firme già configurate.

Per maggiori informazioni, vedere Pulsante Unisci e Pulsante Sostituisci.

Passo 4 Fare clic sul pulsante **Applica modifiche** nella finestra Modifica IPS per distribuire le firme importate.

È possibile modificare le firme importate prima della loro distribuzione. Le firme che sono state impostate per l'importazione e sono identiche alle firme distribuite non verranno importate. Se tutte le firme importate sono identiche alle firme distribuite, il pulsante **Applica modifiche** verrà disattivato.

Albero firme

Per una descrizione dell'albero firme, fare clic sul seguente collegamento: Albero firme. È possibile utilizzare l'albero firme di questa finestra per assemblare le firme che si desidera importare, categoria per categoria.

Ad esempio: è possibile aggiungere le firme dalla categoria OS e dalla categoria Servizio. Per fare questo si può scegliere il ramo **OS** dell'albero e qualsiasi altro ramo della parte dell'albero desiderata, come il ramo UNIX o il ramo Windows. Una volta visualizzati i tipi di firma che si vogliono importare si possono effettuare le selezioni nell'area elenco firme. Quindi scegliere il ramo **Servizio** e selezionare le firme di servizio desiderate.

Elenco Seleziona per e Criterio

Gli elenchi a discesa Seleziona per e Criterio consentono di filtrare la visualizzazione in base ai tipi di firme che si desidera visualizzare. Scegliere innanzitutto i criteri nell'elenco a discesa Seleziona per, quindi scegliere il valore corrispondente nell'elenco a destra (l'elenco dei criteri).

Ad esempio: se si seleziona **Motore** nell'elenco Seleziona per, l'elenco dei criteri viene etichettato Motore ed è possibile scegliere tra i motori disponibili, come **Atomic.ICMP** e**Service.DNS**.

Se si seleziona **ID firma** o **Nome firma**, è necessario immettere un valore nel campo dei criteri.

Area elenco firme

L'elenco delle firme visualizza le firme disponibili nell'SDF sulla base dei criteri selezionati nell'albero delle firme. Il testo delle firme già individuate nel router di destinazione viene visualizzato in blu.

L'area elenco firme consta di tre colonne:

- ID firma: identifica il valore numerico univoco assegnato alla firma. Questo valore consente a IPS Cisco IOS di identificare una determinata firma.
- Nome: indica il nome della firma. Ad esempio: *FTP Improper Address*.
- Gravità: Alta, Media, Bassa o Informativa.

- Distribuito: visualizza *Sì* se la firma è già distribuita nel router. visualizza *No* se la firma non è ancora distribuita nel router.
- Importa: contiene una casella di controllo per ciascuna firma. Volendo importare la firma selezionare questa casella di controllo.

Nota Tutte le firme importate da un file SDF o un file zip con nome IOS-S*xxx*.zip possono essere visualizzate nell'elenco delle firme. Quando le firme vengono importate da un file zip con un nome diverso, verranno visualizzate solo le firme individuate tramite gli elenchi a discesa Seleziona per e Criterio.

Pulsante Unisci

Consente di unire le firme che si vogliono importare con quelle che sono già configurate nel router.

Pulsante Sostituisci

Consente di sostituire le firme che si vogliono importare con quelle che sono già configurate nel router. Le firme che sono già configurate nel router, ma che *non* sono presenti nell'elenco delle firme in corso di importazione, vengono contrassegnate per l'eliminazione ed elencate in **Firme contrassegnate per l'eliminazione** in **Modifica IPS > Firme**. Per maggiori informazioni vedere la sezione Firme contrassegnate per l'eliminazione.

Aggiunta, modifica o duplicazione di una firma

Questa finestra contiene i campi e i valori descritti nella sezione Definizioni dei campi. I campi possono variare in base alla firma, quindi questo non rappresenta un elenco esaustivo di tutti i campi che possono essere visualizzati.

Definizioni dei campi

Nelle finestre Aggiungi, Modifica e Duplica firma si trovano i seguenti campi:

- **SIGID**; valore numerico univoco assegnato alla firma. Questo valore consente a IPS Cisco IOS di identificare una determinata firma.
- **SigName**: identifica il nome assegnato alla firma.

- **SubSig**: identifica il valore numerico univoco assegnato alla firma secondaria. L'ID SubSig viene utilizzato per identificare una versione più granulare di una firma complessa.
- **AlarmInterval**: gestione speciale di eventi temporizzati. Utilizzare AlarmInterval Y con MinHits X per avvisi X con intervallo in secondi Y.
- **AlarmSeverity**: gravità dell'avviso per la firma.
- **AlarmThrottle**: tecnica utilizzata per l'attivazione di avvisi.
- **AlarmTraits**: dettagli definiti dall'utente che descrivono ulteriormente la firma.
- **ChokeThreshold**: valore limite di avvisi per intervallo che determina il passaggio automatico alla modalità AlarmThrottle. Se si definisce ChokeThreshold, IPS Cisco IOS passa automaticamente alla modalità AlarmThrottle se una quantità elevata di avvisi viene visualizzata nel ThrottleInterval.
- **Attivato**: identifica se la firma è stata attivata o meno. Una firma deve essere attiva perché il sistema IPS Cisco IOS possa proteggere dal traffico da essa specificato.
- **EventAction**: identifica le azioni eseguite da IPS Cisco IOS quando la firma viene generata.
- **FlipAddr**: True se nel messaggio di avviso l'indirizzo di origine e di destinazione e porte ad essi associate, sono state scambiati. False se non si è verificato alcuno scambio (impostazione predefinita).
- **MinHits**: specifica il numero minimo di accessi alla firma prima che il messaggio di avviso sia inviato. L'accesso è l'apparenza della firma sulla chiave dell'indirizzo.
- **SigComment**: testo di commento o descrizione della firma.
- **SigVersion**: indica la versione della firma.
- **ThrottleInterval**: numero di secondi che definiscono un intervallo Alarm Throttle. È utilizzato con il parametro AlarmThrottle per ottimizzare i delimitatori speciali di avvisi.
- **WantFrag**: il valore True consente l'ispezione solo di pacchetti frammentati. il valore False consente l'ispezione solo di pacchetti non frammentati. Selezionare “Non definito” per consentire l'ispezione di entrambi i tipi di pacchetti, frammentati e non frammentati.

Cisco Security Center

Il Cisco Security Center fornisce informazioni e collegamenti alle firme IPS Cisco IOS disponibili per proteggere la rete dalle minacce emergenti. I rapporti e i download delle firme sono disponibili al seguente collegamento (è richiesto l'accesso):

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

File di definizione firme fornito da IPS

Per fare in modo che il router abbia a disposizione tutte le firme che la sua memoria può contenere, Cisco SDM viene consegnato con uno dei seguenti file SDF:

- 256MB.sdf - Se la quantità di RAM disponibile è superiore a 256 MB. Il file 256MB.sdf contiene 500 firme.
- 128MB.sdf - Se la quantità di RAM disponibile è compresa tra 128 MB e 256 MB. Il file 128MB.sdf contiene 300 firme.
- attack-drop.sdf - Se la quantità di RAM disponibile è pari a 127 MB o inferiore. Il file attack-drop.sdf contiene 82 firme.

Se sul router è in esecuzione Cisco IOS versione12.4(11)T o successiva, è necessario utilizzare un file SDF il cui formato del nome sia sigv5-SDM-S*xxx*.zip; ad esempio, sigv5-SDM-S260.zip.

Nota Per poter utilizzare tutti i motori firme disponibili nei motori 256MB.sdf e 128MB.sdf, il router deve eseguire Cisco IOS versione 12.3(14)T o successiva. Se il router utilizza una versione precedente, non tutti i motori firma saranno disponibili.

Per utilizzare un file SDF nella memoria del router, stabilire quale SDF è stato installato e poi configurare IPS Cisco IOS perché ne faccia uso. Le procedure seguenti illustrano come fare questo.

Determinare quale file SDF è presente in memoria

Per determinare quale file SDF si trova nella memoria del router, aprire una sessione Telnet del router e immettere il comando **show flash.** Si otterrà qualcosa di simile a quanto segue:

```
Directory flash del sistema:
File  Lunghezza   Nome/stato
  1   10895320  c1710-k9o3sy-mz.123-8.T.bin
  2   1187840  ips.tar
  3   252103   attack-drop.sdf
  4   1038     home.shtml
  5   1814     sdmconfig-1710.cfg
  6   113152   home.tar
  7   758272   es.tar
  8   818176   common.tar
[14028232 byte utilizzati, 2486836 disponibili, 16515068 totali]
16384 Kb della scheda System flash del processo (Lettura/Scrittura)
```

In questo esempio il file attack-drop.sdf si trova nella memoria router Su certi router, come quelli provvisti di file system su disco, utilizzare **dir** per visualizzare il contenuto della memoria del router.

Configurazione di IPS per l'uso di un SDF

Perché IPS Cisco IOS utilizzi il file SDF presente nella memoria del router, eseguire le operazioni seguenti:

Passo 1 Fare clic su **Impostazioni globali**.

Passo 2 Nell'elenco delle posizioni SDF configurate fare clic su **Aggiungi**.

Passo 3 Nella finestra di dialogo visualizzata, fare clic su **Specifica SDF in flash** e immettere il nome del file SDF.

Passo 4 Fare clic su **OK** per chiudere la finestra di dialogo.

Dashboard protezione

Dashboard protezione consente di mantenere il router aggiornato con le firme per le minacce più recenti. Prima di poter distribuire le firme utilizzando Dashboard protezione, è necessario che IPS Cisco IOS sia configurato nel router.

Tabella Minacce principali

La tabella Minacce principali visualizza le più recenti e importanti minacce ricevute da Cisco se lo stato delle firme associate indica che sono disponibili per la distribuzione o sotto esame. Alcune di queste minacce sono associate con le firme che possono essere distribuite al router. Il testo delle firme già individuate nel router viene visualizzato in blu.

Per ricevere le minacce principali più recenti, fare clic sul pulsante **Aggiorna elenco minacce principali**.

Nota Non è possibile aggiornare le minacce principali utilizzando il pulsante **Aggiorna** di Cisco SDM o il comando Aggiorna del browser.

La tabella delle minacce principali presenta le colonne seguenti:

- **Device Status** (Stato dispositivo) indica se la firma associata alla minaccia è già stata attivata nel router. Nella colonna Device Status (Stato dispositivo) può venire visualizzato il simbolo seguente:

  Indica che la firma è già stata attivata nel router.

  Indica che la firma non è disponibile nel router oppure è disponibile ma *non* è stata attivata.

- **ID firma** è un numero univoco che identifica la firma associata alla minaccia.
- **ID SubSig** è un numero univoco che identifica la firma secondaria. Se la firma associata alla minaccia non presenta una firma secondaria, il valore di **ID SubSig** è 0.
- **Nome** è il nome attribuito alla minaccia.

- **Urgency** (Priorità) indica se il livello della minaccia è elevato (manutenzione prioritaria) o normale (manutenzione standard).
- **Threat Status** (Stato minaccia) indica se la firma associata alla minaccia è già stata disponibile o se si trova ancora sotto esame.
- **Deploy** (Distribuzione) contiene caselle di controllo che possono essere selezionate se la firma associata alla minaccia è disponibile per la distribuzione.

Select SDF (Seleziona SDF)

Fare clic sul pulsante **Sfoglia** e selezionare il file SDF Cisco IOS da utilizzare. Il file SDF Cisco IOS deve trovarsi sul PC. Il formato del nome del file dipende dalla versione di Cisco IOS in esecuzione sul router.

- Se sul router è in esecuzione un'immagine Cisco IOS precedente alla 12.4(11)T, il file SDF deve disporre di un nome con formato IOS-S*xxx*.zip, in cui *xxx* rappresenta un numero di tre cifre. Ad esempio: un file SDF IPS Cisco IOS potrebbe essere denominato IOS-S193.zip.
- Se sul router è in esecuzione un'immagine Cisco IOS di versione 12.4(11)T o successiva, il file SDF deve disporre di un nome con formato sigv5-SDM-S*xxx*.zip; per esempio, sigv5-SDM-S260.zip

La posizione del file SDF Cisco IOS selezionato viene visualizzata nel campo della posizione del file SDF. Questa campo è di sola lettura.

Dopo aver scaricato un file SDF Cisco IOS per la prima volta, Cisco SDM memorizza la posizione del file. Quando Dashboard protezione verrà nuovamente caricato, Cisco SDM selezionerà il file SDF Cisco IOS più recente sulla base del numero di tre cifre nel nome del file.

Nota Il file SDF Cisco IOS con il numero a tre cifre più elevato è il file Cisco IOS più recente.

Distribuzione delle firme dalla tabella Minacce principali

Prima di cercare di distribuire le firme dalla tabella Minacce principali, assicurarsi di aver:

- configurato IPS Cisco IOS sul router
- scaricato su PC il file Cisco IOS più recente

Per distribuire le firme dalla tabella Minacce principali, seguire la procedura seguente:

Passo 1 Per essere certi di disporre dell'elenco delle minacce più aggiornato, fare clic sul pulsante **Aggiorna elenco minacce principali**.

Passo 2 Nella colonna Deploy (Distribuzione) selezionare la casella di controllo corrispondente ad ognuna delle firme delle minacce principali che si desidera distribuire dalla tabella Minacce principali.

È possibile selezionare solo le minacce principali con stato **Signature available** (Firma disponibile). Le firme disponibili contrassegnate con un'icona rossa nella colonna Applied (Applicato) vengono automaticamente impostate per la distribuzione.

Passo 3 Fare clic sul pulsante **Sfoglia** e selezionare il file Cisco IOS più recente per essere sicuri di utilizzare il file delle firme più recente.

Questa operazione potrebbe essere necessaria se la posizione dell'ultimo file SDF è stata modificata dall'ultima volta in cui era stata impostata in Dashboard protezione o se il formato o il nome è diverso da IOS-S*xxx*.zip, dove *xxx* è un numero a tre cifre

Passo 4 Fare clic sul pulsante **Distribuisci firme** per distribuire al router le firme selezionate.

Se una delle firme selezionate non viene individuata nel file Cisco IOS, viene visualizzato un avviso. È tuttavia possibile continuare a distribuire tutte le firme individuate. Al termine della distribuzione nel router, le firme vengono attivate automaticamente e aggiunte all'elenco delle firme attive del router.

Migrazione IPS

Se si dispone di una configurazione IPS Cisco IOS che si desidera migrare su IPS Cisco IOS disponibile in Cisco IOS 12.4(11)T o versioni successive, è possibile utilizzare la procedura di migrazione guidata IPS.

Nota Se il router utilizza un'immagine di Cisco IOS versione 12.4(11)T o versione successiva, è necessario migrare una configurazione creata prima di questa versione se si desidera utilizzare IPS Cisco IOS sul proprio router. Se la configurazione non viene migrata, i comandi della configurazione non verranno modificati ma IPS Cisco IOS non funzionerà.

Fare clic sul pulsante **Avvia la procedura guidata Migrazione IPS** per iniziare il processo di migrazione.

Procedura guidata migrazione: Pagina iniziale

La schermata iniziale della procedura guidata di migrazione elenca le attività di cui la procedura consente il completamento. Se non si desidera eseguire la procedura guidata di migrazione IPS, fare clic su **Annulla**.

La procedura guidata di migrazione IPS è disponibile se sul router è in esecuzione Cisco IOS 12.4(11)T e versioni successive.

Procedura guidata migrazione: scelta del file delle firme di backup IOS IPS

Il file di backup contiene le informazioni IPS Cisco IOS che verranno migrate. Il file può essere un file SDF (Signature Definition File), ad esempio attack-drop.sdf o 128MB.sdf. Se si apportano modifiche alle informazioni di firme, ad esempio la disattivazione di firme o la modifica degli attributi di firme specifiche, i record delle modifiche apportate vengono memorizzate in un file a parte. Se è stato utilizzato Cisco SDM per apportare modifiche, Cisco SDM le salva nel file denominato sdmips.sdf nella memoria flash del router. Se sono state apportate modifiche manualmente, è possibile assegnare al file un altro nome e salvarne una copia di backup sul PC.

Fare clic sul pulsante **...** vicino al campo del file di backup per visualizzare una finestra di dialogo che consente di accedere al file di backup sulla memoria flash del router o sul PC.

File delle firme

Specificare il percorso del file delle firme di backup in questa finestra di dialogo.

Specificare il file delle firme sulla memoria flash

Se il file delle firme di backup si trova sulla memoria flash, fare clic sul pulsante freccia in giù vicino a questo campo e selezionare il file.

Specificare il file delle firme sul PC

Se il file delle firme di backup si trova sul PC, fare clic su **Sfoglia** vicino a questo campo e selezionare il file.

Dimensione heap Java

Cisco SDM visualizza la finestra Dimensione heap Java se la dimensione heap Java è troppo piccola per supportare una funzionalità SDM. Completare la seguente procedura per impostare il valore di dimensione heap riportato nella finestra.

Passo 1 Uscire da Cisco SDM.

Passo 2 Fare clic su **Start > Pannello di controllo > Java**.

Passo 3 Aprire la finestra di dialogo Java Runtime Settings (Impostazioni Java Runtime). La posizione di questa finestra varia in base alla versione.

a. Fare clic sulla scheda **Advanced** (Avanzate). Individuare la finestra di dialogo Java Runtime Settings (Impostazioni Java Runtime) e passare al Passo 4. Se la finestra di dialogo non è disponibile nella scheda Advanced (Avanzate), procedere l punto b.

b. Fare clic sulla scheda **Java**. Individuare la finestra di dialogo Java Runtime Settings (Impostazioni Java Runtime). Fare clic sul pulsante **View** (Visualizza) se necessario per visualizzare la finestra di dialogo e procedere al Passo 4.

Passo 4 Nella colonna Java Runtime Parameters (Parametri Java Runtime), immettere il valore riportato nella finestra. Se ad esempio nella finestra viene indicato di utilizzare il valore `-Xmx256m`, immettere tale valore nella colonna Java Runtime Parameters (Parametri Java Runtime). Nella seguente tabella sono riportati degli esempi di valori.

Nome prodotto	Versione	Percorso	Parametri Java Runtime
JRE	1.5.0_08	C:\Program Files\java\jre1.5.0_08	-Xmx256m

Passo 5 Fare clic su **OK** nella finestra di dialogo Java Runtime Settings (Impostazioni Java Runtime).

Passo 6 Fare clic su **Apply** (Applica) nel pannello di controllo Java, quindi fare clic su **OK**.

Passo 7 Riavviare Cisco SDM.

CAPITOLO 25

Gestione del modulo di rete

Se il router dispone di moduli di rete che sono gestiti da altre applicazione, come un IDS (Intrusion Detection System), Secure Router Device Manager (Cisco SDM) è in grado di avviare tali applicazioni.

Gestione modulo di rete IDS

Se nel router è installato un modulo di rete IDS di Cisco, in questa finestra sono visualizzate le relative informazioni di base sullo stato. Se il modulo di rete IDS è stato configurato, sarà possibile avviare anche il software IDM (Intrusion Detection Device Manager) del modulo di rete IDS e selezionare da questa finestra le interfacce del router che si desidera monitorare tramite il modulo di rete IDS.

Se Cisco SDM rileva che il modulo di rete IDS non è stato configurato, viene richiesto di aprire una sessione nel modulo di rete in modo che sia possibile configurarlo. È possibile utilizzare Telnet o SSH per la sessione.

Pulsanti di controllo Modulo di rete IDS

Da questa finestra Cisco SDM consente di emettere un numero di comandi di base al modulo di rete IDS.

Ricarica

Consente di ricaricare il sistema operativo del modulo di rete IDS.

Reimposta

Consente di eseguire la reimpostazione dell'hardware del modulo di rete IDS. Si consiglia di utilizzare il pulsante Reimposta solo per il ripristino dello stato Failed o dopo aver arrestato il modulo di rete IDS.

Arresta

Consente di arrestare il modulo di rete IDS. Prima di rimuovere il modulo dal router eseguire sempre un arresto.

Avvia IDM

Consente di avviare il software IDM nel modulo IDS. Quando si avvia il software, in Cisco SDM è visualizzata una finestra di dialogo che richiede l'indirizzo IP dell'interfaccia Fast Ethernet esterna del modulo IDS. Quando Cisco SDM ottiene l'indirizzo corretto, viene visualizzata una finestra IDM. Per ulteriori informazioni sulla finestra di dialogo vedere la sezione Determinazione dell'Indirizzo IP.

Per maggiori informazioni sulla modalità di esecuzione dell'applicazione IDM, consultare la documentazione disponibile al seguente indirizzo:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm (in inglese)

Aggiorna

Consente di aggiornare la visualizzazione dello stato.

Stato del Modulo di rete IDS

In quest'area è visualizzato lo stato generale del modulo di rete IDS e sono contenute le informazioni riportate di seguito.

- Modulo di servizio: il nome del modulo di rete.
- Stato: lo stato del modulo di rete. Gli stati possibili sono: Steady, Shutdown e/o Failed.
- Versione software: la versione del software IDM in esecuzione nel modulo.
- Modello: il numero di modello del modulo di rete.
- Memoria: la quantità di memoria disponibile nel modulo di rete.

Impostazioni dell'interfaccia di monitoraggio NM IDS

In quest'area della finestra sono visualizzate le interfacce del router il cui traffico è stato inviato al modulo di rete IDS per il monitoraggio.

	Un'icona del segno di spunta accanto al nome dell'interfaccia indica che il modulo di rete IDS monitora il traffico su quell'interfaccia.
	Un'icona rossa con una X accanto al nome dell'interfaccia indica che il modulo di rete IDS non monitora il traffico su quell'interfaccia.

Configura

Consente di aggiungere o rimuovere le interfacce da questo elenco. Quando si fa clic su **Configura**, Cisco SDM verifica che il modulo di rete IDS sia stato configurato e che il router disponga di tutte le impostazioni di configurazione necessarie per comunicare con tale modulo. Se alcune configurazioni non sono pronte, Cisco SDM visualizza un elenco di controllo che mostra le voci configurate e quelle non configurate. È possibile fare clic sulle voci non configurate per completare l'operazione, quindi far verificare nuovamente a Cisco SDM che tali voci siano state configurate in modo che sia possibile aggiungere o rimuovere interfacce dall'elenco Impostazioni dell'interfaccia del Modulo di rete IDS.

Indirizzo IP dell'interfaccia del sensore IDS

Cisco SDM deve comunicare con il modulo di rete IDS tramite l'indirizzo IP dell'interfaccia Fast Ethernet interna del modulo. La finestra viene visualizzata se Cisco SDM non è in grado di rilevare l'indirizzo IP, e consente di fornirne uno senza l'intervento di Cisco SDM. Se il modulo di rete IDS è stato configurato con un indirizzo IP statico o configurato come IP senza numero in un'altra interfaccia con un indirizzo IP, tale finestra non verrà visualizzata.

L'immissione di un indirizzo IP in questa finestra può creare un'interfaccia loopback nuova. Queste interfacce possono essere visualizzate nella finestra Interfacce e connessioni. L'indirizzo IP immesso verrà visualizzato solo dal router; pertanto può essere costituito da qualsiasi indirizzo che si desidera utilizzare.

Indirizzo IP

Immettere un indirizzo IP da utilizzare per l'interfaccia sensore IDS. Cisco SDM effettuerà le seguenti operazioni:

- Creazione di un'interfaccia loopback. Se disponibile, è utilizzato il numero 255, in caso contrario, si ricorrerà a un altro numero. L'interfaccia loopback sarà elencata nella finestra Interfacce e connessioni.
- Configurazione dell'interfaccia loopback con l'indirizzo IP immesso.
- Configurazione dell'IP senza numero del modulo di rete IDS nell'interfaccia loopback.
- Se il modulo di rete IDS è già stato configurato con un IP senza numero in un'interfaccia loopback esistente, ma l'interfaccia non dispone di un indirizzo IP valido, all'interfaccia loopback viene fornito l'indirizzo IP immesso in questa finestra.

Determinazione dell'Indirizzo IP

Cisco SDM visualizza questa finestra quando è necessario determinare l'indirizzo IP di un modulo di rete che si vuole gestire. Normalmente è l'indirizzo IP dell'interfaccia Ethernet esterna del modulo di rete. Cisco SDM ricorda l'indirizzo utilizzato l'ultima volta che è stata eseguita l'applicazione di gestione, può cercare di scoprire l'indirizzo IP, oppure può accettare un indirizzo impostato in questa finestra.

Selezionare un metodo e fare clic su **OK**. Se il metodo selezionato non ha esito positivo, è possibile selezionare un altro metodo.

Utilizza ultimo indirizzo IP di Cisco SDM conosciuto

Fare clic per far sì che Cisco SDM utilizzi l'indirizzo IP che ha utilizzato l'ultima volta che è stata eseguita l'applicazione di gestione di questo modulo di rete. Se l'indirizzo IP del modulo non è stato modificato da quando l'applicazione è stata eseguita per l'ultima volta, e non si vuole che Cisco SDM cerchi di scoprire l'indirizzo usare questa opzione.

Rilevamento indirizzo IP da parte di Cisco SDM

Fare clic per fare in modo che Cisco SDM cerchi di scoprire l'indirizzo IP del modulo di rete. Si può utilizzare quest'opzione se non si conosce l'indirizzo IP, e se non si è certi che l'ultimo indirizzo utilizzato da Cisco SDM per mettersi in contatto con il modulo di rete sia ancora corretto.

Specificare

Se si conosce l'indirizzo IP del modulo di rete, scegliere questa opzione ed immettere l'indirizzo. Tale indirizzo verrà memorizzato da Cisco SDM e sarà possibile selezionare **Utilizza ultimo indirizzo IP di SDM conosciuto** al successivo avvio del modulo di rete.

Elenco di controllo della configurazione NM IDS

Questa finestra è visualizzata una volta selezionato **Configura** nella finestra Gestione Modulo rete IDS per specificare le interfacce del router di cui occorre analizzare il traffico, ma al modulo di rete IDS o al router manca un'impostazione di configurazione necessaria per la comunicazione dei due dispositivi. Nella finestra sono visualizzate le impostazioni di configurazione necessarie e, in alcuni casi, è possibile completare la configurazione all'interno di Cisco SDM.


Un'icona del segno di spunta nella colonna Azione indica che l'impostazione di configurazione è stata eseguita.

Un'icona X nella colonna Azione indica che per consentire la comunicazione tra il router e il modulo di rete IDS, è necessario eseguire l'impostazione di configurazione.

Interfaccia sensore NM IDS

Se questa riga contiene un'icona X nella colonna Azione, l'interfaccia del sensore NM IDS non è stata configurata con un indirizzo IP. Fare doppio clic sulla riga e immettere l'indirizzo IP del sensore IDS nella finestra di dialogo visualizzata. L'indirizzo IP del sensore IDS è l'indirizzo utilizzato da Cisco SDM e dal router durante la comunicazione con il modulo di rete IDS. Questo indirizzo può essere privato, ovvero, nessun host diverso dal router sul quale è installato potrà raggiungere l'indirizzo.

Data e ora

Se questa riga contiene un'icona X nella colonna Azione, le impostazioni dell'orologio del router non sono state configurate. Fare doppio clic sulla riga e immettere le impostazioni relative all'ora e alla data nella finestra Proprietà data e ora.

Impostazione IP CEF

Se questa riga contiene un'icona X nella colonna Azione, il CEF (Cisco Express Forwarding) non è stato attivato nel router. Fare doppio clic sulla riga e selezionare **Sì** per attivare IP CEF nel router.

Configurazione iniziale NM IDS

Se questa riga contiene un'icona X nella colonna Azione, Cisco SDM ha rilevato che l'indirizzo IP predefinito del modulo di rete IDS non è stato modificato. Fare doppio clic sulla riga: Cisco SDM richiederà di aprire una sessione per il modulo IDS e di completare la configurazione. Per questa sessione è possibile utilizzare Telnet o SSH.

Per ulteriori informazioni sulla configurazione del modulo IDS, consultare la documentazione disponibile al seguente indirizzo:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm (in inglese)

Aggiorna

Dopo aver corretto le impostazioni di configurazione, è possibile selezionare questo pulsante per aggiornare l'elenco di controllo. Se l'icona X rimane nella colonna Azione, l'impostazione di configurazione non è stata ancora eseguita.

Configurazione monitoraggio dell'interfaccia NM IDS

Utilizzare questa finestra per selezionare le interfacce del router di cui si desidera monitorare il traffico mediante il modulo di rete IDS.

Interfacce monitorate

In questo elenco sono contenute le interfacce di cui si desidera monitorare il traffico mediante il modulo di rete IDS. Per aggiungere un'interfaccia all'elenco, selezionarne una dall'elenco Interfacce disponibili e fare clic sulla freccia a sinistra (<<). Per rimuovere un'interfaccia dell'elenco, selezionarla e fare clic sulla freccia a destra (>>).

Interfacce disponibili

In questo elenco sono contenute le interfacce il cui traffico non è correntemente monitorato dal modulo di rete IDS. Per aggiungere un'interfaccia all'elenco Interfacce monitorate, selezionarla e fare clic sulla freccia a sinistra (<<).

Accesso al modulo di rete

Immettere il nome utente e la password necessari per accedere al modulo di rete. Queste credenziali potrebbero essere diverse da quelle richieste per accedere al router.

Funzione non disponibile

Questa finestra viene visualizzata quando si tenta di configurare una funzione che non è supportata dall'immagine Cisco IOS nel router. Se si vuole utilizzare questa funzione, ottenere da Cisco.com un'immagine Cisco IOS che la supporti.

Selezione interfaccia modulo switch

Questa finestra viene visualizzata quando ci sono più di uno modulo switch installato sul router, e consente di selezionare quello che si desidera gestire. Fare clic sul pulsante di selezione accanto al modulo switch che si vuole gestire e fare clic su **OK**.

CAPITOLO 26

Qualità del servizio (QoS)

La procedura guidata QoS consente a un amministratore di rete di attivare il criterio QoS sulle interfacce WAN del router. Questo criterio può anche essere attivato sulle interfacce e sui tunnel VPN IPSec. La pagina relativa alla modifica del criterio QoS consente all'amministratore di modificare i criteri creati tramite la procedura guidata.

Crea criterio QoS

La procedura guidata QoS consente a un amministratore di rete di attivare il criterio QoS (Quality of Service) sulle interfacce WAN del router. Questo criterio può anche essere attivato sulle interfacce e sui tunnel VPN IPSec.

Il criterio QoS viene applicato al traffico in uscita dall'interfaccia.

Scheda Crea criterio QoS

Fare clic su questa scheda per aggiungere un nuovo criterio QoS.

Scheda Modifica il criterio QoS

Fare clic su questa scheda per modificare un criterio QoS esistente.

Pulsante Avvia procedura guidata QoS

Fare clic su questo pulsante per avviare la procedura guidata QoS. La procedura guidata QoS consente di configurare i criteri QoS sulle interfacce WAN.

Procedura guidata QoS

Questa finestra fornisce un riepilogo delle informazioni necessarie quando si completa la procedura guidata dei criteri QoS.

Fare clic su **Avanti** per iniziare la configurazione di un criterio QoS.

Selezione interfaccia

Scegliere in questa finestra l'interfaccia su cui configurare il criterio QoS. In questa finestra sono elencate le interfacce WAN e le interfacce per cui non è stato configurato un criterio QoS in uscita. L'elenco contiene le interfacce VPN, ma non le interfacce utilizzate per i client Easy VPN né le interfacce che già dispongono di un criterio QoS. Il criterio QoS non è supportato nei client Easy VPN.

Pulsante Dettagli

Fare clic per visualizzare i dettagli relativi alla configurazione dell'interfaccia selezionata. Nella finestra sono visualizzati l'indirizzo IP e la subnet mask dell'interfaccia, il nome delle regole di accesso e dei criteri applicati all'interfaccia e le connessioni per cui l'interfaccia è utilizzata.

Contrassegno DSCP (attendibile):

Fare clic per utilizzare i contrassegni DSCP (Differentiated Services Code Point) per la classificazione del traffico. I dispositivi di rete Cisco quali telefoni IP e switch aggiungono contrassegni DSCP ai pacchetti. La configurazione del DSCP sul router consente l'utilizzo dei contrassegni per la classificazione del traffico. Se l'immagine Cisco IOS del router non supporta i contrassegni DSCP, questa opzione non verrà visualizzata.

Rilevamento del protocollo NBAR (non attendibile)

Fare clic per utilizzare il rilevamento del protocollo NBAR (Networked Based Application Recognition) per la classificazione del traffico. Quando un'applicazione viene riconosciuta e classificata da NBAR, una rete può richiamare servizi specifici per l'applicazione. NBAR garantisce l'utilizzo ottimale della larghezza di banda classificando i pacchetti e applicando la Qualità del servizio (QoS) al traffico classificato. Se l'immagine Cisco IOS del router non supporta il rilevamento del protocollo NBAR, questa opzione non verrà visualizzata.

Generazione criteri QoS

Utilizzare questa finestra per allocare la larghezza di banda a vari tipi di traffico diretto all'interfaccia selezionata. Il valore percentuale immesso rappresenta 10000 Kbps. Se ad esempio viene immesso 5%, viene allocata una larghezza di banda di 5000 Kbps. Il valore percentuale totale per tutti i tipi di traffico (escluso Massimo sforzo) non può superare il 75%.

- Voce: traffico vocale. Il valore predefinito è 33% della banda.
- Segnalazione chiamate: segnalazione necessaria per il controllo del traffico vocale. Il valore predefinito è 5% della banda.
- Routing: traffico generato da questo e altri router per la gestione dell'instradamento dei pacchetti. Il valore predefinito è 5% della banda.
- Gestione: Telnet, SSH e altro traffico generato per la gestione del router. Il valore predefinito è 5% della banda.
- Transazionale: ad esempio il traffico generato per le applicazioni retail o per gli aggiornamenti del database. Il valore predefinito è 5% della banda.
- Massimo sforzo: banda restante per l'altro traffico, ad esempio il traffico e-mail. Il valore predefinito è 47% della banda. Il valore di Massimo sforzo viene aggiornato in modo dinamico in base alla percentuale totale degli altri tipi di traffico.

Riepilogo della configurazione QoS

In questa finestra è visualizzato un riepilogo del criterio QoS creato in base alle scelte effettuate durante la procedura guidata. Questa mappa di criteri verrà associata all'interfaccia selezionata. Ogni classe configurata dalla procedura guidata QoS SDM viene riportata in riepilogo in questa schermata. Di seguito viene riportata una visualizzazione parziale che mostra l'interfaccia a cui è associato il criterio, il tipo di classificazione (NBAR o DSCP), il nome del criterio e molte delle classi QoS create.

```
Interfaccia:  FastEthernet0/0

Classificazione:  DSCP

Nome criterio: SDM-QoS-Policy-1
```

```
Dettagli criterio

------------------------------------------------------------------------
Nome classe: SDM-Voice-1
------------------------------------------------------------------------
Attivata: Sì
Corrispondenza DSCP: ef
Accodamento: LLQ
Percentuale di larghezza di banda: 33

------------------------------------------------------------------------
Nome classe: SDM-Signalling-1
------------------------------------------------------------------------
Attivata: Sì
Corrispondenza DSCP: cs3,af31
Accodamento: CBWFQ (Class Based Weighted Fair Queue)
Percentuale di larghezza di banda: 5

------------------------------------------------------------------------
Nome classe: SDM-Routing-1
------------------------------------------------------------------------
Attivata: Sì
Corrispondenza DSCP: cs6
Accodamento: CBWFQ (Class Based Weighted Fair Queue)
Percentuale di larghezza di banda: 5

------------------------------------------------------------------------
Nome classe: class-default
------------------------------------------------------------------------
Attivata: Sì
Corrispondenza protocolli:
Accodamento: FQ (Fair Queue)
Rilevamento casuale: Sì

------------------------------------------------------------------------
Nome classe: SDM-Streaming-Video-1
------------------------------------------------------------------------
Attivata: No
Corrispondenza DSCP: cs4
```

Modifica il criterio QoS

La finestra **Modifica il criterio QoS** consente di visualizzare e modificare i criteri QoS configurati e associare i criteri alle interfacce del router.

Elenco nomi criterio

Scegliere un nome di criterio QoS in questo elenco per visualizzarne i dettagli.

Interfaccia

Se il criterio visualizzato è associato a un'interfaccia, viene visualizzato il nome dell'interfaccia, ad esempio FastEthernet 0/0.

Associazione

Fare clic per modificare l'associazione del criterio QoS con un'interfaccia. Se il criterio è attualmente associato a un'interfaccia, è possibile dissociarlo o modificare la direzione del traffico a cui esso è applicato. Il pulsante Associazione viene disattivato se nel campo Interfaccia viene visualizzata un'interfaccia seriale frame-relay.

Pulsanti Classe QoS

I pulsanti presenti in alto all'area Elenco classi consente di modificare e riordinare le informazioni della classe per il criterio

- Pulsante Aggiungi: consente di aggiungere una classe QoS al criterio.
- Pulsante Modifica: selezionare una classe e fare clic su questo pulsante per modificarla nella finestra di dialogo visualizzata. Il pulsante Modifica è disattivato se viene selezionata una classe QoS in sola lettura.
- Pulsante Elimina: selezionare una classe e fare clic su questo pulsante per rimuoverla da questo criterio. Il pulsante Elimina è disattivato se viene selezionata una classe QoS in sola lettura.
- Pulsante Taglia: selezionare una classe e fare clic su questo pulsante per rimuoverla dalla posizione corrente nell'elenco. Utilizzare il pulsante Incolla per inserire la classe nella posizione desiderata. Il pulsante Taglia è disattivato se viene selezionata una classe QoS in sola lettura.

- Pulsante Copia: selezionare una classe e fare clic su questo pulsante per copiarne le informazioni. Il pulsante Copia è disattivato se viene selezionata una classe QoS in sola lettura.
- Pulsante Incolla: consente di modificare le informazioni della classe copiate e assegnare alla classe un nuovo nome. Se si sceglie **Aggiungi classe al criterio**, la classe verrà aggiunta con i relativi criteri attivati. Il pulsante Incolla è disattivato se viene selezionata una classe QoS in sola lettura.
- Pulsante Sposta su: selezionare una classe e fare clic su questo pulsante per spostarla verso l'alto nell'elenco. Questo pulsante consente di spostare solo le classi attive. Il pulsante Sposta su è disattivato se viene selezionata una classe QoS in sola lettura.
- Pulsante Sposta giù: selezionare una classe e fare clic su questo pulsante per spostarla verso il basso nell'elenco. Questo pulsante consente di spostare solo le classi attive. Il pulsante Sposta giù è disattivato se viene selezionata una classe QoS in sola lettura.

Visualizzazione elenco di classi

La finestra Modifica il criterio QoS visualizza i dettagli delle classi QoS che compongono il criterio selezionato.

Colonna Icona

La prima colonna può contenere un'icona che indica lo stato del criterio QoS.

Se questa icona viene visualizzata accanto alla classe QoS, la classe è in sola lettura e non può essere modificata, eliminata o spostata in altra posizione all'interno dell'elenco di classi.

Nome classe

Indica il nome della classe QoS. In Cisco SDM i nomi delle classi QoS sono predefiniti.

Attivato

Un segno di spunta verde sta a indicare che la classe è attivata. Un'icona rossa con una X bianca indica che la classe non è stata attiva per questo criterio. Per attivare una classe, fare clic su **Modifica** e attivare la classe nella finestra Modifica classe QoS.

Corrispondenza

Indica se la classe QoS ricerca corrispondenze a **Qualsiasi** o **Tutti** i valori DSCP selezionati. Se si sceglie **Qualsiasi**, il traffico dovrà soddisfare solo uno dei criteri di corrispondenza. Se si sceglie **Tutti**, il traffico dovrà soddisfare tutti i criteri di corrispondenza. I valori DSCP scelti vengono visualizzati nella colonna DSCP.

Classificazione

In questa sezione della visualizzazione sono incluse seguenti colonne:

- DSCP: valori scelti come possibile corrispondenza.
- Protocolli: indica i protocolli inclusi nella classe QoS. Una classe QoS di tipo traffico video può comprendere protocolli quali CUSeeMe, Netshow e VDOLive. Una classe QoS di tipo instradamento può comprendere protocolli quali BGP, EIGRP e OSPF.
- ACL: nome o il numero dell'ACL che specifica il traffico a cui viene applicata questa classe QoS.

Azione

In questa sezione della visualizzazione sono incluse seguenti colonne:

- Accodamento: questa colonna elenca il tipo di accodamento, che può essere CBWFQ (Class Based Weighted Fair Queuing), LLQ (Low Latency Queuing) o FQ (Fair Queuing) e visualizza la larghezza di banda allocata alla classe.
- Imposta DSCP: valore DSCP assegnato a questo tipo di traffico dalla classe QoS.
- Elimina: la colonne visualizza **Sì** se questo tipo di traffico deve essere eliminato o **No** se non deve essere eliminato.

Pulsanti Applica modifiche e Annulla modifiche

Le modifiche apportate in questa finestra non vengono inviate immediatamente al router. Per inviare le modifiche apportate, fare clic su **Applica modifiche**. Se non si desidera inviare al router le modifiche effettuate in questa finestra, fare clic su **Annulla modifiche**.

Associa o dissocia il criterio QoS

Utilizzare questa finestra per modificare le associazioni di un criterio QoS con le interfacce del router.

Colonna Interfaccia

In questa colonna sono elencate le interfacce del router.

Nota Se si seleziona l'interfaccia utilizzata da SDM per comunicare con il router, la connessione tra l' SDM e il router viene interrotta.

Colonna In ingresso

Selezionare la casella in questa colonna per associare il criterio QoS al traffico in ingresso sull'interfaccia scelta.

Colonna In uscita

Selezionare la casella in questa colonna per associare il criterio QoS al traffico in uscita sull'interfaccia scelta.

Aggiungi o Modifica classe QoS

È possibile creare e modificare le classi di traffico QoS e specificare se la classe deve essere aggiunta al criterio QoS.

Aggiungi classe al criterio

Selezionare questa opzione per includere questa classe QoS al criterio QoS. Se questa opzione non è selezionata, la classe QoS sarà contrassegnata come Disattivata nella finestra Modifica il criterio QoS.

Nome classe

Se si sta modificando una classe esistente, il nome della classe QoS viene visualizzato in questo campo. È necessario immettere un nome di classe se si sta aggiungendo una nuova classe a un criterio o incollare le informazioni dalla classe QoS copiata.

Valore predefinito classe

Questa opzione viene visualizzata se non esiste alcun valore predefinito di classe nel criterio QoS. Fare clic su **Valore predefinito classe** per aggiungere un valore predefinito classe (la classe predefinita) invece di crearne una nuova. Sono presenti vari parametri di configurazione non impostabili come valore predefinito classe:

- Casella Classificazione: non è possibile specificare i criteri di classificazione.
- Casella Azione: non è possibile specificare il traffico da scartare. È inoltre possibile specificare solo il valore FR (Fair Queuing) da utilizzare.

Classificazione

Scegliere i tipi di elementi e i valori di cui si desidera che il router esamini il traffico. Se si sceglie Tutti, il traffico dovrà soddisfare tutti i criteri. Se si sceglie Qualsiasi, il traffico dovrà soddisfare un solo criterio. È necessario specificare un tipo di valore nell'elenco e fare clic su **Modifica** per specificarne i valori. Per specificare la classe è ad esempio http, edonkey e smtp, scegliere **Protocollo** e fare clic su **Modifica**. Scegliere quindi i protocolli nella finestra di dialogo Modifica valori protocollo corrispondenza e fare clic su **OK**. I protocolli scelti vengono visualizzati nella colonna Valore dell'elenco Classificazione.

Se si desidera che la classe corrisponda al traffico definito in un ACL, fare clic su **Regola di accesso**, quindi su **Modifica**. Nella finestra di dialogo visualizzata, è possibile scegliere un ACL esistente, crearne uno nuovo o cancellare le associazioni esistenti, nel caso si stia modificando una classe QoS.

Azione

Scegliere l'azione che il router dovrà intraprendere in caso di corrispondenza del traffico con i valori DSCP specificati.

- **Elimina**: elimina il traffico. Se si sceglie **Elimina**, le altre opzioni nell'area Azione vengono disattivate.
- **Imposta DSCP**: consente di scegliere il valore DSCP a cui reimpostare il traffico.
- **Accodamento**: l'LLQ è disponibile se il traffico utilizza il protocollo RTP e il valore DSCP è EF. In caso contrario, l'opzione LLQ non è disponibile. Se si sta aggiungendo o modificando la classe predefinita (class-default), è disponibile solo l'FQ (Fair Queuing).
- **Percentuale di larghezza di banda**: il valore percentuale immesso viene utilizzato come percentuale assoluta della larghezza di banda totale sull'interfaccia.
- **Percentuale di rimanente di larghezza di banda**: il valore percentuale immesso viene utilizzato come percentuale relativa della larghezza di banda totale sull'interfaccia. È ad esempio possibile specificare il 30% della larghezza di banda disponibile da allocare a una classe e il 60% della larghezza di banda da allocare a un'altra classe QoS. Per utilizzare questa opzione, tutte le altre classi devono utilizzare questa stessa opzione. L'opzione **Percentuale di rimanente di larghezza di banda** è disattivata se è stato selezionato **LLQ**.
- **Rilevamento casuale**: attiva il WRED (Weighted Random Early Detection) e il DWRED (Distributed WRED) sul router. Questa opzione è disattivata se è stato selezionato **LLQ**. Il RED scarta i pacchetti nei momenti di congestione del traffico, comunicando all'host di origine di ridurre il tasso di trasmissione.

Modifica valori DSCP corrispondenza

Per aggiungere un valore DSCP all'elenco di corrispondenza, scegliere un valore dalla colonna **Valori DSCP disponibili** a sinistra e fare clic sul pulsante a doppia freccia in alto per aggiungerlo alla colonna **Valori DSCP selezionati**. Per rimuovere un valore dalla colonna **Valori DSCP selezionati**, scegliere il valore e fare clic sul pulsante a doppia freccia in basso.

Modifica valori protocollo corrispondenza

Per aggiungere un protocollo a una classe, scegliere un protocollo dalla colonna Valori Protocollo disponibili a sinistra e fare clic sul pulsante a doppia freccia in alto per aggiungerlo alla colonna Valori protocollo selezionati. Per rimuovere un protocollo dalla colonna Protocolli selezionati, scegliere il protocollo e fare clic sul pulsante a doppia freccia in basso.

Aggiungi protocolli personalizzati

In questa finestra è possibile aggiungere protocolli personalizzati non disponibili nella finestra Modifica valori protocollo corrispondenza. Per definire un protocollo personalizzato, attenersi alla seguente procedura:

Passo 1 Selezionare il nome del protocollo personalizzato dall'elenco Nome.

Passo 2 Selezionare se verrà utilizzato come protocollo TCP o UDP.

Passo 3 Definire i numeri di porta che utilizzerà. Immettere un numero di porta nel campo Numero nuova porta e fare clic su **Aggiungi** per aggiungerlo all'elenco dei numeri di porte. Per rimuovere un numero di porta dall'elenco, scegliere il numero e fare clic su **Rimuovi**.

Modifica ACL corrispondenza

Scegliere **Seleziona regola esistente (ACL)** o **Create nuova regola (ACL) e selezionare**. Vengono visualizzate finestre di dialogo aggiuntive che consentono di creare una regola o di selezionarne una esistente. Per cancellare le associazioni di regole esistenti, scegliere **Nessuno (cancella associazioni)**.

Modifica valori DSCP corrispondenza

Per aggiungere un valore DSCP all'elenco di corrispondenza, scegliere un valore dalla colonna **Valori DSCP disponibili** a sinistra e fare clic sul pulsante a doppia freccia in alto per aggiungerlo alla colonna **Valori DSCP selezionati**. Per rimuovere un valore dalla colonna **Valori DSCP selezionati**, scegliere il valore e fare clic sul pulsante a doppia freccia in basso.

CAPITOLO 27

Controllo di ammissione della rete (NAC)

Il NAC (Network Admission Control) protegge le reti di dati dai virus informatici valutando lo stato di salute delle workstation client, assicurando che esse ricevano gli aggiornamenti delle firme dei virus più recenti e controllando il loro accesso alla rete.

Il NAC opera con il software antivirus per valutare la condizione di un client, chiamata *posture* del client, prima di consentire l'accesso alla rete da parte del client. Il NAC assicura che i client della rete dispongano di definizioni aggiornate dei virus che non sono state infettate. Se il client richiede un aggiornamento delle definizioni il NAC lo dirige in modo da completare l'aggiornamento. Se il client è stato compromesso o se sulla rete si sta verificando la diffusione di un virus, il NAC mette il client in un segmento di rete sotto quarantena fino al completamento della disinfezione.

Per maggiori informazioni sul NAC fare clic sui seguenti collegamenti.

- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Scheda Crea NAC

La scheda Crea NAC e la procedura guidata NAC si usano per creare un criterio NAC e associarlo con un'interfaccia. Dopo avere creato il criterio NAC è possibile modificarlo facendo clic su **Modifica NAC** e scegliendolo nell'elenco dei criteri.

La configurazione NAC del router è soltanto una parte di una implementazione completa del NAC. Fare clic su Altre attività in un'implementazione NAC per apprendere quali sono le attività da eseguire su altri dispositivi per implementare il NAC.

Pulsante Attiva AAA

Authentication, Authorization e Accounting (AAA) devono essere attivi sul router prima di poter configurare il NAC. Se AAA non è attivato, fare clic sul pulsante **Attiva AAA**. Se AAA è già stato configurato sul router, questo pulsante non è visualizzato.

Pulsante Avvia procedura guidata NAC

Fare clic su questo pulsante per avviare la configurazione guidata del NAC. La procedura guidata divide la configurazione del NAC in una serie di schermate in ciascuna delle quali si completa una singola attività di configurazione.

Elenco Come

Se si vuole creare una configurazione non prevista da questa procedura guidata, fare clic sul pulsante accanto a questo elenco. Vi sono elencati altri tipi di configurazione che si possono voler eseguire. Per apprendere come creare una delle configurazioni elencate, scegliere tale configurazione e fare clic su **Vai**.

Altre attività in un'implementazione NAC

Un'implementazione NAC completa comprende i seguenti passi di configurazione:

Passo 1 Installare e configurare il software CTA (Cisco Trust Agent) sugli host della rete. Ciò fornisce agli host un agente posture in grado di rispondere alle richieste EAPoUDP del router. Seguire i collegamenti alla fine di questi passi per ottenere il software CTA e apprendere come installarlo e configurarlo.

Passo 2 Installare e configurare un server EAPoUDP di autenticazione AAA. Questo server deve essere un server ACS Cisco Secure (Acces Control Server) che utilizza il protocollo RADIUS. È necessario il software Secure Access Control Server Cisco versione 3.3. Seguire i collegamenti alla fine di questi passi per apprendere come installare e configurare ACS.

Passo 3 Installare e configurare un server di convalida e riparazione.

Per gli utenti registrati di Cisco.com, è possibile scaricare il software CTA (Cisco Trust Agent) dal seguente collegamento:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

Il documento del collegamento seguente spiega come installare e configurare il software CTA su un host.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

Il documento del collegamento seguente contiene una panoramica del processi di configurazione.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

I documenti dei collegamenti seguenti spiegano come installare e configurare Cisco Secure ACS per Windows Server versione 3.3.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

Pagina iniziale

La procedura guidata NAC consente di fare quanto segue:

- Scegliere l'interfaccia su cui si deve attivare il NAC—Gli host che cercano di accedere alla rete mediante questa interfaccia sono sottoposti al processi di convalida NAC.
- Configurare i server criteri NAC—I criteri di controllo di ammissione sono configurati su questi server, che il router contatta quando un host della rete cerca di accedere alla rete. È possibile specificare informazioni per più server. I server criteri NAC usano il protocollo RADIUS.
- Configurare un elenco eccezioni NAC—Host come stampanti, telefoni IP e alcuni host senza agenti di posture installati possono ignorare il processo NAC. Host con indirizzi IP statici e altri dispositivi che possono essere identificati in un elenco eccezioni e gestiti usando un criterio eccezioni associato. Gli host possono essere identificati mediante i loro indirizzi MAC o i loro tipi di dispositivo.
- Configurare un criterio per host senza agente—È possibile usare un criterio residente su un server Cisco Secure ACS per la gestione degli host senza un agente di posture installato. Quando il server Cisco Secure ACS riceve un pacchetto da un host senza agente, esso risponde inviando il criterio per gli host senza agente. La configurazione di un criterio host senza agente è utile quando ci sono degli host privi di agente con indirizzi dinamici, come i client DHCP.
- Configurazione di NAC per l'Accesso remoto: l'accesso deve essere consentito agli host che utilizzano Cisco SDM per gestire il router. La procedura guidata consente di specificare indirizzi IP per la gestione remota in modo che Cisco SDM possa modificare l'ACL del NAC per consentire l'accesso al router per gli host con tali indirizzi.

La configurazione del NAC sul router è l'ultimo passo di una configurazione NAC. Prima di configurare il router con questa funzionalità, completare i passi descritti nel collegamento seguente: Altre attività in un'implementazione NAC.

Server criteri NAC

I criteri di ammissione del NAC sono configurati e conservati in un database che risiede sui server RADIUS che eseguono Cisco Secure ACS versione 3.3. Il router deve convalidare le credenziali degli host della rete comunicando con il server RADIUS. Usare questa finestra per fornire le informazioni necessarie perché il router possa contattare tali server RADIUS. Ciascun server RADIUS specificato deve disporre di Cisco Secure ACS (Access Control Server) software versione 3.3 installato e configurato.

Scegliere l'origine Client RADIUS

La configurazione dell'origine RADIUS consente di specificare l'indirizzo IP dell'origine da inviare in pacchetti RADIUS collegati per il server RADIUS. Per maggiori informazioni su un'interfaccia, scegliere l'interfaccia e fare clic sul pulsante **Dettagli**.

L'indirizzo IP di origine nei pacchetti RADIUS inviati dal router deve essere configurato come l'indirizzo IP NAD del Cisco ACS Versione 3.3 o successiva.

Se si seleziona l'opzione **Il router sceglie l'origine**, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo dell'interfaccia attraverso la quale i pacchetti RADIUS escono dal router.

Se si sceglie un'interfaccia, l'indirizzo IP di origine nei pacchetti RADIUS sarà l'indirizzo dell'interfaccia che si sceglie come origine del client RADIUS.

Nota Il software Cisco IOS consente la configurazione di una sola interfaccia origine RADIUS sul router. Se il router ha già un'origine RADIUS configurata e si sceglie un'origine diversa, l'indirizzo IP collocato nei pacchetti inviati al server RADIUS diventa l'indirizzo IP della nuova origine e pertanto può non corrispondere all'indirizzo IP NAD configurato sul Cisco ACS.

Pulsante Dettagli

Se si desidera un'istantanea delle informazioni su un'interfaccia prima di sceglierla, fare clic sul pulsante **Dettagli**. Questa schermata mostra l'indirizzo IP e la subnet mask, le regole di accesso e le Inspection Rule applicate all'interfaccia, il criterio IPSec e il criterio QoS applicato, e se sull'interfaccia è presente una configurazione di Easy VPN.

Colonne IP Server, Timeout, e Parametri

Le colonne IP Server, Timeout, e Parametri contengono informazioni che il router utilizza per contattare un server RADIUS. Se non ci sono informazioni sul server RADIUS associate all'interfaccia scelta, queste colonne sono vuote.

Casella di controllo Usa per NAC

Selezionare questa casella di controllo se si vuole usare il server RADIUS elencato per il NAC. Il server deve disporre dei criteri di controllo ammissione richiesti configurati in modo che NAC sia in grado di usare il server.

Pulsanti Aggiungi, Modifica, ed Esegui ping

Per fornire informazioni su un server RADIUS, fare clic sul pulsante **Aggiungi** e immettere le informazioni nella schermata visualizzata. Scegliere una riga e fare clic su **Modifica** per modificare le informazioni sul server RADIUS. Scegliere una riga e fare clic su **Esegui ping** per testare la connessione tra il router e il server RADIUS.

Nota Quando si esegue una prova ping, immettere l'indirizzo IP dell'interfaccia origine RADIUS nel campo origine della finestra di dialogo del ping. Se è stata scelta l'opzione **Il router sceglie l'origine**, non è necessario indicare alcun valore nel campo origine della finestra di dialogo del ping.

I pulsanti **Modifica** ed **Esegui ping** sono disattivati quando non sono disponibili informazioni sul server RADIUS per l'interfaccia selezionata.

Selezione interfaccia

Scegliere in questa finestra l'interfaccia su cui si deve attivare il NAC. Scegliere l'interfaccia tramite cui gli host si collegano alla rete.

Fare clic sul pulsante **Dettagli** per visualizzare i criteri associati all'interfaccia scelta. La finestra visualizza i nomi delle ACL applicate al traffico in entrata e in uscita su questa interfaccia.

Se un'ACL in entrata è già presente sull'interfaccia, Cisco SDM utilizza tale ACL per il NAC aggiungendo le dichiarazioni di permesso appropriate per il traffico EAPoUDP. Se l'indirizzo IP dell'interfaccia su cui si sta applicando il NAC fosse 192.55.22.33, una dichiarazione di consenso d'esempio potrebbe essere la seguente:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

La dichiarazione di permesso che Cisco SDM aggiunge usa il numero di porta 21862 per il protocollo EAPoUDP. Se gli host di rete eseguono EAPoUDP su un numero di porta, si deve modificare questa voce ACL perché usi il numero di porta usato da tale host.

Se sull'interfaccia specificata non è configurato un ACL per il traffico in ingresso, si può fare in modo che Cisco SDM applichi un ACL all'interfaccia. Si può scegliere un criterio raccomandato o un criterio che esegue semplicemente il monitoraggio delle posture riportate dal NAC.

- **Convalida rigorosa** (**raccomandata**): Cisco SDM applica un'ACL che rifiuta tutto il traffico (**deny ip any any**). L'ammissione sulla rete è determinata dal processo di convalida NAC. Per impostazione predefinita tutto il traffico è rifiutato tranne il traffico dimostratosi valido sulla base del criterio configurato sul server criteri NAC.
- **Controlla posture NAC**: Cisco SDM applica un'ACL che permette tutto il traffico (**permit ip any any**). Dopo il processo di convalida NAC il router può ricevere criteri dal server NAC che rifiutano l'accesso a certi host. È possibile utilizzare l'impostazione **Controlla posture NAC** per determinare l'impatto della configurazione NAC sulla rete. Fatto questo, è possibile modificare i criteri del server criteri NAC e riconfigurare il NAC sul router perché usi la **Convalida rigorosa** cambiando l'ACL applicata all'interfaccia in **deny ip any any** per mezzo della funzione Criterio firewall di Cisco SDM.

Elenco eccezioni NAC

È possibile identificare gli host cui si deve consentire di ignorare il processo di convalida NAC. Solitamente gli host come le stampanti, i telefoni IP e gli host privi di agenti posture di NAC installati vengono aggiunti a questo elenco eccezioni.

Se sulla propria rete ci sono host privi di indirizzo statico si raccomanda che questi vengano immessi nel criterio degli host senza agenti, e non nell'elenco eccezioni NAC. Il criterio eccezioni NAC può non funzionare correttamente se l'indirizzo IP dell'host cambia.

Se si utilizza la procedura guidata NAC e non si vuole configurare un elenco eccezioni NAC, si può fare clic su **Avanti** senza immettere informazioni in questa finestra. In alternativa o come complemento all'elenco eccezioni NAC la procedura guidata consente di configurare un criterio host senza agenti in un'altra finestra.

Colonne Indirizzo IP/Indirizzo MAC/Tipo di dispositivo, Indirizzo/Dispositivo e Criterio

Queste colonne contengono informazioni sugli host presenti nell'elenco eccezioni. Gli host possono essere identificati mediante i loro indirizzi IP, i loro indirizzi MAC o i tipi di dispositivo cui appartengono. Se identificato come indirizzo, l'indirizzo IP o MAC di un host viene visualizzato nella riga accanto al nome del criterio che governa l'accesso dell'host alla rete.

Aggiunta, modifica, e eliminazione di pulsanti

Creare l'elenco delle eccezioni facendo clic su **Aggiungi** e immettendo le informazioni su un host. È possibile usare ripetutamente il pulsante **Aggiungi** finché necessario.

Scegliere una riga e fare clic su **Modifica** per modificare le informazioni su un host. Fare clic su **Elimina** per rimuovere le informazioni su un host da questa finestra. I pulsanti Aggiungi e Elimina sono disattivati se in questo elenco non ci sono informazioni.

Aggiungi o Modifica voce elenco eccezioni

Aggiungere o modificare le informazioni di un elenco eccezioni in questa finestra.

Elenco tipi

Gli host sono scelti secondo il modo in cui vengono identificati. Questo elenco contiene le seguenti selezioni:

- Indirizzo IP—Scegliere questo tipo se si vuole identificare l'host con il suo indirizzo IP.
- Indirizzo MAC—Scegliere questo tipo se si vuole identificare l'host con il suo indirizzo MAC.
- Telefono IP Cisco—Scegliere questo tipo se si vogliono includere nell'elenco eccezioni i telefoni IP Cisco nella rete.

Campo Specificare indirizzo

Se si sceglie indirizzo IP o indirizzo MAC come o tipo di host, immettere qui l'indirizzo. Se si seleziona un tipo di dispositivo questo campo è disattivato.

Campo Criterio

Se si conosce il nome del criterio di eccezione, immetterlo in questo campo. Fare clic sul pulsante con i puntini di sospensione e a destra del campo Criterio per scegliere un criterio o visualizzare una finestra di dialogo in cui creare un nuovo criterio.

Scegli un criterio eccezioni

Selezionare il criterio che si desidera applicare all'host. Quando si sceglie un criterio l'URL di redirezione specificato per il criterio appare in un campo di sola lettura e le voci della regola di accesso del criterio sono visualizzate.

Se non ci sono criteri disponibili nell'elenco, fare clic su **Annulla** per tornare alla schermata della procedura guidata e scegliere l'opzione che consente di aggiungere un criterio.

Selezionare dall'elenco il criterio che si desidera applicare all'host sottoposto ad eccezione. Se nell'elenco non ci sono criteri, fare clic su **Annulla** per tornare alla procedura guidata. Quindi scegliere **Crea un nuovo criterio** e selezionarlo nella finestra Aggiungi all'elenco eccezioni.

Reindirizza URL: campo URL

Questo campo di sola lettura visualizza l'URL associato al criterio scelto. Gli host cui viene applicato questo criterio sono reindirizzati a questa URL quando cercano di accedere alla rete.

Anteprima della regola d'accesso

Le colonne Azione, Origine, Destinazione e Servizio mostrano le voci ACL nella regola di accesso associata al criterio. Questo colonne sono vuote se per questo criterio non sono stati configurate ACL.

Aggiungi criterio di eccezione

Immettere un nuovo criterio di eccezione in questa finestra.

Per creare un nuovo criterio di eccezione, immettere un nome per il criterio e specificare una regola di accesso che definisca gli indirizzi IP cui gli host presenti nell'elenco eccezioni possono accedere, o immettere un URL di redirezione. L'URL di redirezione deve contenere informazioni di riparazione che consentono agli utenti di aggiornare i loro file di definizione dei virus. È necessario fornire o un nome di regola di accesso o un URL di reindirizzamento. È possibile specificare entrambe le cose.

Campo Nome

Immettere in questo campo il nome del criterio. I nomi di criterio non possono contenere spazi o punti interrogativi. La lunghezza massima del nome è di 256 caratteri.

Campo Regola di accesso

Immettere il nome o numero della regola di accesso che si vuole utilizzare o fare clic sul pulsante a destra di questo campo per trovare la regola di accesso con sfogliando le cartelle o creare una nuova regola di accesso. la regola di accesso deve contenere voci di consenso che specificano gli indirizzi IP cui gli host dell'elenco eccezioni possono connettersi. La regola di accesso deve essere chiamata ACL; le ACL prive di numerazione non sono supportate.

Campo URL reindirizzamento

Immettere un URL che contenga le informazioni di riparazione per la rete. Queste informazioni possono contenere informazione per il download di file di definizioni dei virus.

Un URL di riparazione potrebbe essere simile al seguente:

`http://172.23.44.9/update`

Di solito gli URL di reindirizzamento sono nella forma `http://URL` o `https://URL`.

Criterio host agentless

Se sul server Cisco Secure ACS è presente un host privo di agente, il router può utilizzare questo criterio per gestire gli host senza agenti di posture installati. Questo metodo di gestione degli host senza agenti può essere utilizzato come alternativa o come complemento di un elenco eccezioni NAC. Se si sta usando la procedura guidata NAC e non si deve configurare un criterio host senza agenti, si può fare clic su **Avanti** senza immettere informazioni in questa finestra.

Casella di controllo Autentica host senza agenti

Selezionare questa casella per indicare che si desidera utilizzare il criterio host senza agenti del server Cisco Secure ACS.

Campi nome utente e password

Alcune immagini software Cisco IOS richiedono la comunicazione di un nome utente e una password insieme alla richiesta al server Cisco Secure ACS. In tal caso immettere il nome utente e la password configurati a questo fine sul server Cisco Secure ACS. Se l'immagine Cisco IOS non richiede questa informazione questi campi non sono visualizzati.

Configurazione di NAC per l'Accesso remoto

La configurazione di NAC per l'accesso remoto consente di modificare le ACL create dalla configurazione NAC, in modo esse consentano il traffico di Cisco SDM. Specificare gli host che devono usare Cisco SDM per collegarsi al router.

Attiva la gestione remota di Cisco SDM

Selezionare questa casella di controllo per attivare la gestione remota di Cisco SDM sull'interfaccia nominata.

Campi Host/Indirizzo rete

Se si vuole che Cisco SDM modifichi l'ACL per consentire al traffico Cisco SDM l'accesso attraverso un solo host, scegliere **Indirizzo Host** e immettere l'indirizzo IP di un host. Scegliere l'**Indirizzo di rete** e immettere l'indirizzo di una rete e una subnet mask per consentire il traffico di Cisco SDM dagli host su tale rete. L'host o la rete deve essere accessibile dall'interfaccia specificata. Scegliere **Any** (Qualsiasi) per consentire il traffico Cisco SDM da qualsiasi host connesso alle interfacce specificate.

Modifica firewall

Cisco SDM controlla ogni ACL applicata all'interfaccia specificata in questa configurazione in modo da determinare se viene bloccato il traffico consentito attraverso il firewall in modo da rendere efficace la funzione configurata.

Ciascuna interfaccia è elencata con il servizio correntemente bloccato su tale interfaccia e l'ACL che la sta bloccando. Se si desidera che Cisco SDM modifichi l'ACL per consentire il traffico elencato, fare clic sulla casella **Modifica** della riga appropriata. Se si vuole vedere la voce che Cisco SDM aggiungerà all'ACL, fare clic sul pulsante **Dettagli**.

Nella seguente tabella FastEthernet0/0 è stata configurata per il NAC. Questa interfaccia è configurata con i servizi indicati nella colonna Servizio.

Interfaccia	Servizio	ACL	Azione
FastEthernet0/0	RADIUS Server	101 (IN INGRESSO)	[ ] Modifica
FastEthernet0/0	DNS	100 (IN INGRESSO)	[ ] Modifica
FastEthernet0/0	DHCP	100 (IN INGRESSO)	[ ] Modifica
FastEthernet0/0	NTP	101 (IN INGRESSO)	[ ] Modifica
FastEthernet0/0	VPN	190 (IN INGRESSO)	[ ] Modifica

Finestra Dettagli

In questa finestra sono visualizzate le voci che Cisco SDM aggiungerà alle ACL per consentire i servizi per i servizi che si stanno configurando. La finestra potrebbe contenere una voce come la seguente:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

In tal caso, il traffico Web il cui numero di porta è maggiore di 1024 è consentito dall'host 10.77.158.84 sulla rete locale all' host 10.77.158.1

Riepilogo della configurazione

Questa finestra riepiloga le informazioni immesse e consente di esaminarle in una singola finestra. È possibile usare il pulsante Indietro per tornare ad una qualunque schermata precedente e modificare le informazioni. Fare clic su **Fine** per inviare la configurazione al router.

Ecco un esempio di riepilogo di configurazione NAC:

```
Interfaccia NAC:  FastEthernet0/1.42
Nome ammissione:  SDM_EOU_3


Interfaccia origine cliente AAA: FastEthernet0/1.40
Server criteri NAC 1:   10.77.158.54

Elenco eccezioni
-------------------------------------------------------------------------
Indirizzo/Dispositivo     Indirizzo IP        (22.22.22.2) appena
aggiunto
Dettagli criterio:
Nome criterio:          P55
       Reindirizza URL:  http://www.fix.com
        regola d'accesso:   test11

-------------------------------------------------------------------------


Criterio host senza agente attivo
Nome utente:  bill
Password:   ******
```

Nell'esempio i pacchetti RADIUS dovranno avere l'indirizzo IP della FastEthernet 0/1.40. Il NAC è attivato sulla FastEthernet 0/1.42 e il criterio NAC applicato dalla procedura guidata è SDM_EOU_3. Un host è stato nominato nell'elenco eccezioni, ed il suo accesso alla rete è controllato dal criterio eccezioni P55.

Scheda Modifica NAC

La scheda modifica NAC elenca i criteri NAC configurati sul router e consente di configurare altre impostazioni NAC. Per ciascuna interfaccia su cui si deve eseguire una convalida di postura deve essere configurato un criterio NAC.

Pulsante Timeout NAC

Il router e il client usano il protocollo EAPoUDP (Extensible Authentication Protocol over Unformatted Data Protocol) per lo scambio di informazioni sulla posture. I valori di default del timeout di EAPoUDP sono preconfigurati, ma possono essere modificati. Questo pulsante è disattivato se non ci sono criteri NAC configurati sul router.

Pulsante Criteri host senza agenti

Se sul server Cisco Secure ACS è presente un host privo di agente, il router può utilizzare questo criterio per gestire gli host senza agenti di posture installati. Questo metodo di gestione degli host senza agenti può essere utilizzato quando tali host non dispongono indirizzi IP statici. Questo pulsante è disattivato se non ci sono criteri NAC configurati sul router.

Aggiunta, modifica, e eliminazione di pulsanti

Questi pulsanti consentono di gestire l'elenco criteri NAC. Fare clic su **Aggiungi** per creare un nuovo criterio NAC. Usare i pulsanti Modifica e Elimina per modificare e rimuovere i metodi NAC. I pulsanti Modifica e Elimina sono disattivati se non ci sono criteri NAC configurati sul router.

Solo il pulsante Aggiungi resta attivato se non ci sono criteri NAC configurati sul router. Il pulsante Aggiungi è disattivato quando tutte le interfacce del router sono configurate con criteri NAC.

Elenco Criteri NAC

Il nome, l'interfaccia cui il criterio NAC è applicato, e la regola di accesso che definisce il criterio sono inclusi in questo elenco. Se si è attivato il NAC su un'interfaccia usando la procedura guidata Crea NAC, il criterio NAC predefinito SDM_EOU_1 è presente in questo elenco.

Componenti NAC

Questa finestra fornisce una breve descrizione dei componenti EAPoUDP che Cisco SDM consente di configurare.

Finestra Elenco eccezioni

Questo argomento segnaposto sarà rimosso quando il sistema guida del NAC sarà stato approntato. Questo argomento della guida è già stato scritto per la modalità procedura guidata. Per visualizzarlo, fare clic sul collegamento seguente:

Elenco eccezioni NAC

Finestra Criteri eccezioni

I criteri eccezione NAC controllano l'accesso alla rete degli host nell'elenco eccezioni. Un criterio eccezioni NAC contiene un nome, una regola di accesso e/o un URL di reindirizzamento. La regola di accesso specifica le destinazioni cui gli host governati dal criterio hanno accesso. Se un URL di reindirizzamento è specificato nel criterio, il criterio può inviare i client web su siti che contengono informazioni su come ottenere la più recente protezione antivirus disponibile.

Un esempio di una voce criteri NAC è illustrato nella seguente tabella:

Nome	Regola di accesso	URL reindirizzamento
NACLess	nac-rule	http://172.30.10/update

Le regole di accesso associate con i criteri NAC devono essere ACL estese, e devono avere un nome. Un esempio di regola di accesso che può essere usato in un criterio NAC è illustrato nella seguente tabella:

Azione	Origine	Destinazione	Servizio	Registro	Attributi
consenti	any	172.30.2.10	ip		

Questa regola consente a qualsiasi host governato dal criterio di inviare traffico IP all'indirizzo IP 172.30.2.10.

Aggiunta, modifica, e eliminazione di pulsanti

Fare clic sul pulsante **Aggiungi** per creare un nuovo criterio di eccezione. Usare il pulsante **Modifica** per modificare i criteri di eccezione esistenti e il pulsante **Elimina** per rimuovere i criteri di eccezione. I pulsanti Aggiungi e Elimina sono disattivati se in questo elenco non ci sono criteri di eccezione.

Timeout NAC

Configurare i valori di timeout che il router deve utilizzare per le comunicazioni EAPoUDP con gli host della rete. I valori minimo e massimo predefinito di tutte le impostazioni sono visualizzati nella seguente tabella.

Valore	Predefinito	Minimo	Massimo
Timeout periodo sospensione	180 secondi	60 secondi	86400 secondi
Timeout ritrasmissione	3 secondi	1 secondi	60 secondi
Timeout riconvalida:	36000 secondi	300 secondi	86400 secondi
Timeout richiesta di stato	300 secondi	30 secondi	1800 secondi

Selezione interfaccia

Scegliere l'interfaccia cui si devono applicare le impostazioni di timeout NAC.

Campo Timeout periodo di sospensione

Immettere il numero di secondi nei quali il router deve ignorare i pacchetti dai client che non sono riusciti ad autenticarsi.

Campo Timeout ritrasmissione

Immettere il numero di secondi che il router deve attendere prima di ritrasmettere messaggi EAPoUDP ai client.

Campo Timeout riconvalida

Il router interroga periodicamente l'agente posture sul client per determinare l'aderenza del client ai criteri di sicurezza. Immettere il numero di secondi che il router deve attendere tra le richieste.

Campo Timeout richiesta stato

Immettere il numero di secondi che il router deve attendere tra le richieste all'agente di posture sull'host.

Pulsante Ripristina configurazione predefinita

Facendo clic su questo pulsante si reimpostano la conversione e i parametri di timeout ai loro valori di default.

Casella di controllo Configura questi valori di timeout globalmente

Spuntare questa casella di controllo e per applicare questi valori a tutte le interfacce.

Configurare un criterio NAC

Un criterio NAC attiva il processo di convalida della posture su una interfaccia router, e può essere usato per specificare i tipi di traffico che sono esenti dalla convalida della posture nel processo di controllo dell'ammissione.

Campo Nome

Immettere un nome per il criterio.

Selezionare un elenco interfaccia

Scegliere l'interfaccia su cui si vuole applicare il criterio NAC. Selezionare un interfaccia che connette i clienti della rete al router.

Campo Regola di ammissione

Si può usare una regola di accesso per esentare del traffico specifico dall'avviare il processo di controllo di ammissione. Ciò non è obbligatorio. Immettere il nome del numero della regola di accesso che si vuole usare per la regola di ammissione. Si può anche fare clic sul pulsante a destra di questo campo per trovare la regola di accesso con sfogliando le cartelle o creare una nuova regola di accesso.

La regola di accesso deve contenere dichiarazione di rifiuto che specificano il traffico che è esentato dal processo di controllo di ammissione. Se la regola contiene solo dichiarazioni di rifiuto non viene avviata alcuna convalida della postura.

Ecco un esempio di voci ACL per una regola di ammissione NAC:

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any
```

La prima dichiarazione di rifiuto esenta il traffico con una destinazione alla porta 53 (domain) e la seconda dichiarazione esenta il traffico con destinazione alla porta 80 (www). La dichiarazione Consenti che termina l'ACL assicura che si verifichi la convalida di postura.

Informazioni aggiuntive

I seguenti argomenti contengono le procedure per l'esecuzione di attività che la procedura guidata Crea NAC non aiuta a completare.

Come si configura un Policy Server NAC?

Il router deve avere una connessione a un server ACS Cisco Secure dotato della versione 3.3 del software ACS. L'ACS deve essere configurato per usare il protocollo RADIUS per potere implementare il NAC. Il documento del collegamento seguente contiene una panoramica del processi di configurazione.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

I documenti dei collegamenti seguenti spiegano come installare e configurare Cisco Secure ACS per Windows Server versione 3.3.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

Come si installa e si configura un Agente di Posture su un host?

Per gli utenti registrati di Cisco.com, è possibile scaricare il software CTA (Cisco Trust Agent) dal seguente collegamento:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

Il documento del collegamento seguente spiega come installare e configurare il software CTA su un host.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

Le procedure d'installazione specifiche richieste per installare software agenti di posture di terze parti e il server di riparazione opzionale variano a seconda del software in uso. Consultare la documentazione dei fornitori per tutti i dettagli.

CAPITOLO 28

Proprietà router

La funzione Proprietà router consente di definire gli attributi generali del router, ad esempio il nome, il nome di dominio, la password, lo stato del protocollo SNMP (Simple Network Management Protocol), l'indirizzo del server DNS (Domain Name System), gli account utente, gli attributi di registro del router, le impostazioni del terminale virtuale (VTY), le impostazioni SSH e altre impostazioni di protezione per l'accesso al router.

Proprietà dispositivo

La schermata Proprietà dispositivo contiene informazioni sull'host, il dominio e la password del router.

Scheda Dispositivo

Nella scheda Dispositivo sono contenuti i campi riportati di seguito.

Host

Immettere il nome che si desidera assegnare al router.

Dominio

Immettere il nome di dominio dell'organizzazione. Se il nome di dominio non è noto, rivolgersi all'amministratore di rete.

Immettere il testo per il banner

Immettere il testo per il banner del router. Il testo verrà visualizzato ogni volta che un utente accede al router. Si raccomanda che il banner di testo comprenda un messaggio indicante che l'accesso non autorizzato è proibito.

Scheda Password

La scheda Password contiene i campi riportati di seguito.

Attiva password crittografata

Cisco Router and Security Device Manager (Cisco SDM) supporta l'attivazione della password crittografata. La funzione consente di controllare gli utenti che dispongono dell'autorizzazione per immettere comandi di configurazione nel router. Si raccomanda fortemente di impostare e attivare una password segreta. La password non sarà leggibile nella finestra Proprietà del Dispositivo di Cisco SDM, e sarà aggiunta in forma criptata nel file di configurazione del router. Pertanto è consigliabile tenere traccia della password nel caso possa essere dimenticata.

La versione di Cisco IOS in esecuzione nel router può supportare l'opzione Attiva password. Tale opzione è simile all'opzione Attiva password crittografata, ma la password è crittografata nel file di configurazione. Se l'opzione Attiva password viene configurata utilizzando l'interfaccia della riga di comando (CLI), essa verrà ignorata qualora sia stata configurata una password crittografata.

Password corrente

Se è già stata impostata una password, questo campo conterrà asterischi (*).

Immetti nuova password

Immettere la nuova password in questo campo.

Reimmetti nuova password

Reimmettere la stessa password immessa nel campo Nuova password.

Data e ora - Proprietà orologio

Utilizzare questa schermata per visualizzare e modificare le impostazioni relative all'ora e alla data del router.

Data/Ora

Le impostazioni della data e dell'ora del router vengono visualizzate nel lato destro della barra di stato di Cisco SDM. Le impostazioni di quest'area della finestra Proprietà orologio non vengono aggiornate.

Origine ora router

Questo campo può contenere i valori riportati di seguito.

- NTP: il router riceve le informazioni sull'ora da un server NTP.
- Configurazione utente: i valori relativi a data e ora vengono impostati manualmente tramite Cisco SDM o interfaccia CLI.
- Nessuna origine ora: il router non è configurato con le impostazioni di data e ora.

Cambia impostazioni

Utilizzare questa schermata per visualizzare e modificare le impostazioni relative all'ora e alla data del router.

Proprietà data e ora

Usare questa finestra per impostare la data e l'ora del router. È possibile lasciare che Cisco SDM sincronizzi le impostazioni col PC oppure impostarle manualmente.

Sincronizza con l'orologio del computer locale

Consente a Cisco SDM di sincronizzare le impostazioni della data e dell'ora del router con quelle del computer.

Sincronizza

Fare clic per consentire a Cisco SDM di sincronizzare le impostazioni di data e ora. Cisco SDM consente di regolare automaticamente le impostazioni di data e ora solo quando viene scelta l'opzione **Sincronizza**. Cisco SDM non esegue automaticamente una nuova sincronizzazione con il computer locale durante le sessioni successive. Il pulsante è disattivato se non è stata selezionata l'opzione **Sincronizza con l'orologio del computer locale**.

Nota È necessario specificare le impostazioni Fuso orario e Daylight Savings (Ora legale) nel computer locale prima di avviare Cisco SDM, in modo da consentire a Cisco SDM la ricezione delle impostazioni corrette quando viene premuto il pulsante **Sincronizza**.

Modifica data e ora

Utilizzare quest'area per configurare manualmente le impostazioni relative all'ora e alla data. Scegliere il mese e l'anno dagli elenchi a discesa e il giorno del mese nel calendario. I campi nell'area Ora richiedono l'immissione di valori nel formato 24 ore. È possibile scegliere il fuso orario in base all'ora di Greenwich (GMT) oppure sfogliare l'elenco delle principali città che rientrano nel fuso orario dell'utente.

Se si desidera che il router regoli automaticamente le impostazioni per l'ora legale e l'ora solare, selezionare **Passa automaticamente all'ora legale**.

Applica

Consente di applicare le impostazioni della data e dell'ora configurate nei campi Data, Ora e Fuso orario.

NTP

NTP (Network Time Protocol) consente ai router presenti nella rete di sincronizzare le proprie impostazioni orarie con un server NTP. Un gruppo di client NTP che riceve le informazioni relative alla data e all'ora da un'origine unica avrà impostazioni orarie più coerenti. La finestra consente di visualizzare le informazioni configurate nel server NTP, di aggiungere nuove informazioni o di modificare ed eliminare quelle esistenti.

Nota Se il router non supporta i comandi NTP, questo ramo non verrà visualizzato nell'elenco Proprietà router.

Indirizzo IP

Indirizzo IP di un server NTP.

Se l'organizzazione non dispone di un server NTP, potrebbe essere necessario utilizzare un server pubblicamente disponibile, quale il server descritto al seguente URL:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Interfaccia

L'interfaccia mediante la quale il router comunicherà con il server NTP.

Preferire

Nella colonna viene visualizzato **Sì** se il server NTP è stato designato come server NTP preferito. I server NTP preferiti vengono contattati prima dei server che non rientrano nell'elenco. È possibile indicare più di un server NTP preferito.

Aggiungi

Fare clic sull'opzione per aggiungere informazioni sul server NTP.

Modifica

Fare clic per modificare una configurazione server NTP specificata.

Elimina

Fare clic per cancellare una configurazione server NTP specificata.

Aggiungi o modifica dettagli server NTP

Aggiungere o modificare le informazioni relative a un server NTP in questa finestra.

Indirizzo IP

Immettere o modificare l'indirizzo IP del server NTP.

Preferire

Selezionare la casella se il server NTP deve essere configurato come server preferito.

Interfaccia

Scegliere l'interfaccia che verrà utilizzata per accedere al server NTP. È possibile utilizzare il comando CLI **show IP routes** per determinare quale interfaccia dispone di una route verso questo server NTP.

Nota Verrà creata una regola di accesso estesa per il traffico sulla porta 123, che verrà applicata all'interfaccia scelta in questa finestra. Se per l'interfaccia è già disponibile una regola di accesso, in Cisco SDM verranno aggiunte delle definizioni per consentire il traffico della porta 123 su questa interfaccia. Se la regola esistente è una regola di accesso standard, Cisco SDM esegue una modifica in una regola estesa per consentire di specificare il tipo e la destinazione del traffico.

Chiave di autenticazione

Selezionare questa casella se il server NTP utilizza una chiave di autenticazione e immettere le informazioni richieste nei campi. Le informazioni immesse devono corrispondere alle informazioni relative alla chiave del server NTP.

Numero chiave

Immettere il numero della chiave di autenticazione. L'intervallo di numeri della chiave è compreso tra 0 e 4294967295.

Valore chiave

Immettere la chiave utilizzata dal server NTP. Il valore della chiave può includere qualsiasi lettera dalla A alla Z, in caratteri maiuscoli o minuscoli, ma non può contenere più di 32 caratteri.

Conferma valore chiave

Inserire nuovamente il valore della chiave per confermarne la correttezza.

SNTP

Questa finestra viene visualizzata nei router Cisco 830. SNTP (Simple Network Time Protocol) è una versione meno complessa di NTP (Network Time Protocol). NTP consente ai router della rete di sincronizzare le impostazioni di data e ora con un server NTP. Un gruppo di client NTP che riceve le informazioni relative alla data e all'ora da un'origine unica avrà impostazioni orarie più coerenti. La finestra consente di visualizzare le informazioni configurate nel server NTP, di aggiungere nuove informazioni o di modificare ed eliminare quelle esistenti.

Nota Se il router non supporta i comandi NTP, questo ramo non verrà visualizzato nell'elenco Proprietà router.

Proprietà

Il nome definito dal sistema per il server NTP.

Valore

L'indirizzo IP del server NTP.

Aggiungi

Fare clic sull'opzione per aggiungere informazioni sul server NTP.

Modifica

Fare clic per modificare una configurazione server NTP specificata.

Elimina

Fare clic per cancellare una configurazione server NTP specificata.

Aggiungi dettagli server NTP

Immettere l'indirizzo IP di un server NTP in questa finestra.

Nota Verrà creata una regola di accesso estesa per il traffico sulla porta 123, che verrà applicata all'interfaccia scelta in questa finestra. Se per l'interfaccia è già disponibile una regola di accesso, in Cisco SDM verranno aggiunte delle definizioni per consentire il traffico della porta 123 su questa interfaccia. Se la regola esistente è una regola di accesso standard, Cisco SDM esegue una modifica in una regola estesa per consentire di specificare il tipo e la destinazione del traffico.

Indirizzo IP

Immettere l'indirizzo IP del server NTP in formato decimale separato da punti. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Registrazione

Utilizzare questa finestra per attivare la registrazione dei messaggi di sistema e per specificare gli host di registrazione nei quali verranno conservati i registri. È possibile specificare il livello di registrazione dei messaggi che si vogliono inviare e raccogliere ed immettere il nome host o l'indirizzo IP di più host di registrazione.

Indirizzo IP/Nome host

Fare clic su **Aggiungi** e immettere l'indirizzo IP o il nome host di un host di rete al quale si desidera che il router invii i messaggi di registrazione per l'archiviazione. I pulsanti **Modifica** ed **Elimina** consentono di modificare le informazioni immesse e di eliminare le voci.

Specificare il tipo di messaggi che verranno inviati agli host di registrazione, scegliendo il livello di registrazione nell'elenco a discesa **Livello di registrazione**. Per maggiori informazioni vedere la sezione Livello di registrazione.

Livello di registrazione

Nell'elenco a discesa **Livelli di registrazione** sono disponibili i seguenti livelli di registrazione:

- emergenze (0)
- avvisi (1)
- critici (2)
- errori (3)
- avvertimenti (4)
- notifiche (5)
- informativi (6)
- di debug (7)

Nel registro vengono raccolti tutti i messaggi del livello prescelto e tutti i messaggi dei livelli inferiori oppure il router invia tutti i messaggi del livello prescelto e quelli dei livelli inferiori agli host di registrazione. Se si sceglie, ad esempio, il livello notifiche (5), nel registro verranno raccolti o inviati i messaggi inclusi dal livello 0 al livello 5. I messaggi di registrazione del firewall richiedono un livello di registrazione di debug (7), mentre i messaggi del registro di protezione dell'applicazione richiedono un livello informativo (6).

Registrazione nel buffer

Se si desidera che i messaggi di sistema siano registrati sul buffer del router, fare clic sulla casella di controllo **Buffer di registrazione** nella casella di dialogo visualizzata in Cisco SDM quando si fa clic su **Modifica**, quindi immettere la dimensione del buffer nel campo Dimensione del buffer. Maggiore è il buffer, maggiore il numero di voci che è possibile registrare prima che quelle meno recenti vengano cancellate per far spazio alle nuove. Tenere presente che è necessario equilibrare le esigenze di registrazione e le prestazioni del router.

Specificare il tipo di messaggi che verranno raccolti nel registro scegliendo il livello di registrazione nell'elenco a discesa **Livello di registrazione**. Per maggiori informazioni vedere la sezione Livello di registrazione.

SNMP

Questa finestra consente di attivare il protocollo SNMP, impostare le stringhe di comunità SNMP e immettere le informazioni sul gestore del trap SNMP.

Attiva SNMP

Selezionare questa casella di controllo per attivare il supporto SNMP. Deselezionare questa casella per disattivare il supporto SNMP. SNMP è attivato per impostazione predefinita.

Stringa di comunità

Le stringhe di comunità SNMP rappresentano password incorporate per l'accesso a un MIB (Management Information Base). I MIB immagazzinano dati sul funzionamento del router e sono destinati ad essere disponibili per gli utenti remoti autenticati. I due tipi di stringhe di comunità sono le stringhe di comunità “pubbliche”, che forniscono un accesso di sola lettura a tutti gli oggetti nel MIB tranne le stringhe di comunità, e le stringhe di comunità “private” che forniscono un accesso di lettura-scrittura a tutti gli oggetti nel MIB tranne le stringhe di comunità.

La tabella delle stringhe di comunità elenca tutte le stringhe di comunità configurate e i rispettivi tipi. Utilizzare il pulsante **Aggiungi** per visualizzare la finestra di dialogo Aggiungi stringa di comunità e creare nuove stringhe di comunità. Fare clic sui pulsanti **Modifica** o **Elimina** per modificare o eliminare le stringhe di comunità selezionate nella tabella.

Ricevitore trap SNMP

Immettere gli indirizzi IP e le stringhe di comunità dei ricevitori trap SNMP, ovvero gli indirizzi presso i quali dovrebbero essere inviate le informazioni trap. Si tratta in genere degli indirizzi IP delle stazioni di gestione SNMP che monitorano il dominio. Consultare l'amministratore del sito per verificare che l'indirizzo IP sia valido.

Fare clic sui pulsanti **Aggiungi**, **Modifica** o **Elimina** per amministrare le informazioni del ricevitore trap.

Posizione server SNMP

Campo di testo che può essere utilizzato per immettere la posizione del server SNMP. Non si tratta di un parametro di configurazione che influirà sull'operatività del router.

Contatto server SNMP

Campo di testo che può essere utilizzato per immettere le informazioni di contatto della persona che gestisce il server SNMP. Non si tratta di un parametro di configurazione che influirà sull'operatività del router.

NetFlow

Questa finestra indica come è configurato il router per controllare i talker principali NetFlow sulle interfacce in cui è configurato NetFlow. Per maggiori informazioni su questo argomento, vedere Talker NetFlow.

È possibile controllare i parametri NetFlow sul router e visualizzare le statistiche sui talker principali in **Controllo > Stato dell'interfaccia** e in **Controllo > Stato traffico > N flussi traffico principali**. Se *non* si attivano i talker principali NetFlow, verranno controllati i primi dieci talker principali.

Talker NetFlow

In questa finestra è possibile configurare il monitoraggio NetFlow e visualizzare i talker principali.

Attiva talker principali

Selezionare la casella di controllo **Attiva talker principali** per attivare il controllo dei talker principali sulle interfacce con NetFlow configurato.

Talker principali

Impostare il numero dei talker principali nella casella numerica **Talker principali**. Scegliere un numero incluso nell'intervallo 1–200. In Cisco SDM i dati verranno rilevati e registrati fino al numero di talker principali specificato.

Timeout cache

Impostare il timeout, in millisecondi, per la cache dei talker principali nella casella numerica **Timeout cache**. Scegliere un numero incluso nell'intervallo 1–3600000. Quando viene raggiunto il timeout, la cache dei talker principali verrà aggiornata.

Ordina per

Scegliere come ordinare i talker principali, selezionando byte o pacchetti nell'elenco a discesa **Ordina**.

Accesso al router

La finestra illustra le funzioni incluse nell'accesso al router.

Account utente - Configurare gli account utente per l'accesso al router

Questa finestra consente di definire gli account e le password che consentiranno agli utenti di autenticarsi quando accedono al router tramite HTTP, Telnet, PPP o altri sistemi.

Nome utente

Nome dell'account utente specificato.

Password

La password dell'account utente, visualizzata con asterischi (*).

Nota La password utente non è uguale alla password crittografata configurata nella scheda Proprietà dispositivo - Password. Le password utente consentono all'utente specificato di accedere al router e immettere un insieme limitato di comandi.

Livello di privilegio

Il livello di privilegio per l'utente specificato.

Nome vista

Se all'account utente è stata associata una vista CLI, in questa colonna ne viene visualizzato il nome. Le viste definiscono l'accesso utente a Cisco SDM in base al ruolo dell'utente. Per maggiori informazioni fare clic su Associa una vista all'utente.

Nota Se Cisco SDM viene avviato con una vista definita dall'utente o con una vista modificata definita da Cisco SDM, Cisco SDM opererà in modalità Controllo e l'utente disporrà di privilegi di sola lettura. Le funzioni Cisco SDM disponibili per il controllo dipendono dai comandi disponibili nella vista. Non tutte le funzioni potrebbero essere disponibili per il controllo da parte dell'utente.

Tabella riassuntiva funzioni

Per:	Procedura:
Aggiunta di un nuovo account utente.	Fare clic su **Aggiungi**. Quindi aggiungere l'account nella finestra Aggiungi nome utente.
Modifica di un account utente.	Scegliere l'account utente e fare clic su **Modifica**. Quindi modificare l'account nella finestra Modifica nome utente.
Eliminazione di un account utente.	Scegliere l'account utente e fare clic su **Elimina**. Quindi confermare l'eliminazione nel messaggio di avviso visualizzato.

Aggiungi o modifica nome utente

Utilizzare i campi di questa finestra per aggiungere o modificare un account utente.

Nome utente

Immettere o modificare il nome utente in questo campo.

Password

Immettere o modificare la password in questo campo.

Conferma password

Immettere di nuovo la password in questo campo. Se la password e la password di conferma non sono uguali tra loro, quando si fa clic su **OK** viene visualizzato un messaggio d'errore.

Quando si fa clic su **OK**, le informazioni nuove o modificate relative all'account verranno visualizzate nella finestra Configurare gli account utente per l'accesso a Telnet.

Casella di controllo Crittografa password mediante algoritmo hash MD5

Selezionare questa casella se si desidera che la password venga crittografata utilizzando l'algoritmo unidirezionale Message Digest 5 (MD5), che fornisce una protezione avanzata.

Nota I protocolli che richiedono il recupero di password in testo non codificato, ad esempio CHAP, non possono essere utilizzati con le password crittografate tramite l'algoritmo MD5. La crittografia MD5 è irreversibile. Per ripristinare la password in testo non codificato, è necessario eliminare l'account utente e ricrearlo senza selezionare l'opzione **Crittografia password**.

Livello di privilegio

Immettere il livello di privilegio per l'utente specificato. Se tale opzione è applicata a un comando CLI, tale comando potrà essere eseguito soltanto da utenti con un livello di privilegio uguale o superiore a quello impostato per il comando stesso.

Associa una vista all'utente

Questo campo viene visualizzato quando si impostano gli account utente per l'accesso al router. Se si sta lavorando in un'altra area di Cisco SDM, il campo potrebbe non essere visibile.

Selezionare l'opzione **Associa una vista all'utente** se si vuole restringere l'accesso ad una vista specifica. Se si associa una vista con un utente per la prima volta, viene visualizzata la richiesta di immettere la password di vista. Questa opzione è disponibile soltanto nella pagina Accesso al router del diagramma di Attività aggiuntive.

Nome vista

Scegliere tra le seguenti la vista da associare a questo utente:

- SDM_Amministratore: un utente associato al tipo di vista SDM_Amministratore dispone dell'accesso totale a Cisco SDM e può eseguire tutte le operazioni supportate da Cisco SDM.
- SDM_Controllo: un utente associato a questo tipo di vista può controllare tutte le funzioni supportate da Cisco SDM. Non potrà inviare le configurazioni tramite Cisco SDM. Potrà invece spostarsi nelle diverse aree di Cisco SDM, ad esempio Interfacce e Connessioni, Firewall e VPN. Tuttavia, i componenti dell'interfaccia utente di queste aree saranno disattivati.
- SDM_Firewall: un utente associato al tipo di vista SDM_Firewall può usare le funzioni Firewall e Monitor di Cisco SDM. Può quindi configurare firewall e ACL tramite la procedura guidata Firewall, la Vista criterio firewall e l'Editor ACL. I componenti dell'interfaccia utente in altre aree saranno disattivati.
- SDM_EasyVPN_Remote: un utente associato al tipo di vista SDM_EasyVPN_Remote può usare le funzioni dell'Easy VPN Remote Cisco SDM. Può quindi creare connessioni EasyVPN Remote e modificarle. I componenti dell'interfaccia utente in altre aree saranno disattivati.

Dettagli

L'area **Associa una vista all'utente** visualizza i dettagli della vista specificata. Fare clic sul pulsante **Dettagli** per informazioni più dettagliate sulla vista specificata.

Password di vista

Quando si associa una vista con un utente per la prima volta, viene visualizzata la richiesta di immettere la password di vista per le viste definite in Cisco SDM. Utilizzare tale password per spostarsi tra le viste.

Immettere la password di vista

Immettere la password di vista nel campo Password di vista.

Impostazioni vty

In questa finestra sono visualizzate le impostazioni VTY del router. La colonna Proprietà contiene gli intervalli delle linee configurate e le proprietà configurabili per ogni intervallo. Le impostazioni delle proprietà sono contenute nella colonna Valore.

La tabella mostra le impostazioni VTY del router e contiene le colonne riportate di seguito.

- Intervallo linea: visualizza l'intervallo di connessioni VTY al quale si applicano le altre impostazioni della riga.
- Protocolli di input consentiti: indica i protocolli configurati per l'input. Può trattarsi dei protocolli Telnet, SSH o entrambi.
- Protocolli di output consentiti: indica i protocolli configurati per l'output. Può trattarsi dei protocolli Telnet, SSH o entrambi.
- EXEC Timeout: l'intervallo di inattività (in secondi) che deve trascorrere prima che una sessione venga chiusa.
- Classe di accesso in ingresso: il nome o il numero della regola di accesso applicata alla direzione in ingresso dell'intervallo di linea.
- Classe di accesso in uscita: il nome o il numero della regola di accesso applicata alla direzione in uscita dell'intervallo di linea.
- ACL - Se configurato, indica l'ACL associato alle connessioni VTY.

- Criterio di autenticazione: il criterio di autenticazione AAA associato alla linea VTY. Il campo è visualizzato se AAA è stato configurato nel router.
- Criterio di autorizzazione: il criterio di autorizzazione AAA associato alla linea VTY. Il campo è visualizzato se AAA è stato configurato nel router.

Nota Per utilizzare SSH come protocollo di ingresso o di uscita, attivarlo facendo clic su **SSH** nella struttura Attività aggiuntive e generando una chiave RSA.

Modifica linee VTY

In questa finestra è possibile modificare le impostazioni VTY del router.

Intervallo di linea

Immettere l'intervallo di linee VTY al quale si applicano le impostazioni specificate in questa finestra.

Timeout

Immettere l'intervallo di inattività (in secondi) che deve trascorrere prima che una connessione venga terminata.

Protocollo di input

Scegliere i protocolli di input selezionando le caselle di controllo appropriate.

Casella di controllo Telnet

Selezionare questa casella di controllo per attivare l'accesso Telnet al router.

Casella di controllo SSH

Selezionare questa casella di controllo per attivare l'accesso dei client SSH al router.

Protocollo di output

Scegliere i protocolli di output selezionando le caselle di controllo appropriate.

Casella di controllo Telnet

Selezionare questa casella di controllo per attivare l'accesso Telnet al router.

Casella di controllo SSH

Selezionare questa casella di controllo per consentire al router di comunicare con i client SSH.

Regola di accesso

È possibile associare le regole di accesso affinché filtrino il traffico in ingresso o in uscita nelle linee VTY incluse nell'intervallo.

In ingresso

Immettere il nome o il numero della regola di accesso che si desidera applicare per filtrare il traffico in ingresso oppure premere il pulsante per individuare la regola nell'elenco.

In uscita

Immettere il nome o numero della regola di accesso che si vuole utilizzare per il filtraggio del traffico in uscita, o fare clic sul pulsante per trovare la regola di accesso.

Autenticazione/autorizzazione

I campi sono visibili quando AAA è attivato nel router. È possibile attivare AAA facendo clic su **Attività aggiuntive > AAA > Attiva**.

Criterio di autenticazione

Scegliere il criterio di autenticazione che si desidera utilizzare per la linea VTY.

Criterio di autorizzazione

Scegliere il criterio di autorizzazione che si desidera utilizzare per la linea VTY.

Configura criteri di accesso gestione

Utilizzare questa finestra per rivedere i criteri di accesso gestione esistenti e scegliere i criteri da modificare. I criteri di accesso gestione consentono di specificare quali reti e host possono accedere all'interfaccia della riga di comando del router. Nel criterio è possibile definire quali protocolli possono essere utilizzati dall'host o dalla rete specificati e quale interfaccia del router gestirà il traffico.

Host/rete

Un indirizzo di rete o un indirizzo IP dell'host. Se viene fornito un indirizzo di rete, il criterio viene applicato a tutti gli host presenti nella rete. Se viene fornito un indirizzo di host, il criterio viene applicato a tale host.

L'indirizzo di rete viene mostrato nel formato numero di rete/bit di rete, come nell'esempio seguente:

```
172.23.44.0/24
```

Per maggiori informazioni sul formato e su come vengono utilizzati indirizzi IP e subnet mask, vedere Indirizzi IP e subnet mask.

Interfaccia di gestione

L'interfaccia del router utilizzata per il traffico di gestione.

Protocolli consentiti

Questa colonna elenca i protocolli che potranno essere utilizzati dagli host specificati nella comunicazione con il router. È possibile configurare i protocolli riportati di seguito.

- Cisco SDM: gli host specificati possono utilizzare Cisco SDM.
- Telnet: gli host specificati possono utilizzare Telnet per accedere alla CLI del router.
- SSH: gli host specificati possono utilizzare Secure Shell per accedere alla CLI del router.
- HTTP: gli host specificati possono utilizzare Hypertext Transfer Protocol per accedere al router. Se è stato specificato Cisco SDM, è necessario specificare anche HTTP o HTTPS.

- HTTPS: gli host specificati possono utilizzare Hypertext Transfer Protocol Secure per accedere al router.
- RCP: gli host specificati possono utilizzare Remote Copy Protocol per gestire i file del router.
- SNMP: gli host specificati possono utilizzare Simple Network Management Protocol per gestire il router.

Pulsante Aggiungi

Fare clic sul pulsante per aggiungere un criterio di gestione e specificare il criterio nella finestra Aggiungi criterio di gestione.

Pulsante Modifica

Fare clic sul pulsante per modificare un criterio di gestione e specificare il criterio nella finestra Modifica criterio di gestione.

Pulsante Elimina

Fare clic per eliminare un criterio di gestione specificato.

Pulsante Applica

Fare clic sul pulsante per applicare le modifiche apportate alla configurazione del router nella finestra Aggiungi o modifica criterio di gestione.

Pulsante Annulla modifiche

Fare clic sul pulsante per ignorare le modifiche apportate alla configurazione del router nella finestra Aggiungi o modifica criterio di gestione. Tutte le modifiche apportate vengono annullate e rimosse dalla finestra Configura criteri di accesso gestione.

Aggiungi o modifica criterio di gestione

Utilizzare la finestra per aggiungere o modificare un criterio di gestione.

Tipo

Specificare se l'indirizzo fornito è l'indirizzo di una rete o di un host.

Indirizzo IP/Subnet Mask

Se è stata specificata l'opzione **Rete** nel campo Tipo, immettere l'indirizzo IP di un host o l'indirizzo e la subnet mask della rete. Per maggiori informazioni vedere Indirizzi IP e subnet mask.

Interfaccia

Scegliere l'interfaccia mediante la quale si desidera consentire il traffico di gestione. Dovrebbe essere il percorso più diretto dall'host o dalla rete al router locale.

Protocolli di gestione

Specificare i protocolli di gestione consentiti per l'host o la rete.

Consenti SDM

Selezionare questa opzione per consentire all'host o alla rete specificati di accedere al sistema Cisco SDM. Selezionando questa casella vengono automaticamente attivati i protocolli indicati di seguito: Telnet, SSH, HTTP, HTTPS e RCP. La selezione dell'opzione non impedisce di consentire l'utilizzo di ulteriori protocolli.

Se si desidera consentire agli utenti l'utilizzo di protocolli sicuri per l'accesso a Cisco SDM, selezionare **Consenti solo protocolli di protezione**. Selezionando questa casella vengono automaticamente attivati i protocolli indicati di seguito: SSH, HTTPS, RCP. Se poi si seleziona un protocollo non protetto come Telnet, Cisco SDM deseleziona **Consenti solo protocolli di protezione**.

Specificare i singoli protocolli di gestione

Se si desidera specificare i singoli protocolli che potranno essere utilizzati dall'host o dalla rete, selezionare una qualsiasi delle caselle seguenti: Telnet, SSH, HTTP, RCP o SNMP.

Se Telnet e SSH non sono attivati (ovvero selezionati) nella finestra VTY e se SNMP non è attivato nella finestra Proprietà SNMP, Cisco SDM visualizza un messaggio che raccomanda di attivare tali protocolli qualora siano stati specificati in questa finestra.

Nota Le opzioni **Consenti solo protocolli di protezione** e **HTTPS** verranno disattivate se la versione di Cisco IOS del router non supporta HTTPS.

Messaggi di errore di Accesso gestione

La funzione Accesso gestione può generare i messaggi di errore indicati di seguito.

Messaggio di errore

```
Avviso SDM - ANY Not Allowed
```

Descrizione I criteri di gestione sono di sola lettura se una delle sue regole relative all'origine o alla destinazione contiene la parola chiave “any”. Tali criteri non possono essere modificati nella finestra Accesso gestione. Un criterio contenente la parola chiave “any” può costituire un rischio per la sicurezza per le seguenti ragioni:

- Se la voce “qualsiasi” è associata all'origine, essa consente l'ingresso al router del traffico proveniente da qualsiasi rete.
- Se la voce “qualsiasi” è associata alla destinazione, essa consente l'accesso a qualsiasi diramazione della rete supportata dal router.

Azione consigliata È possibile rimuovere la voce di accesso che causa la visualizzazione di questo messaggio scegliendo la regola nella finestra Regole e facendo clic su **Modifica**. In alternativa, nella finestra Interfacce e Connessioni, è possibile disassociare la regola dall'interfaccia cui essa è applicata.

Messaggio di errore

`Avviso SDM - Unsupported Access Control Entry`

Descrizione Un criterio di gestione è di sola lettura se all'interfaccia o alla linea VTY alla quale viene applicato il criterio di gestione sono associate voci di controllo di accesso non supportate. È possibile utilizzare la riga comandi per rimuovere le voci ACE non supportate, ovvero che contengono sintassi o parole chiave non supportate in Cisco SDM.

Messaggio di errore

`Avviso SDM - SDM Not Allowed`

Descrizione Questo messaggio viene visualizzato se non è ancora stato configurato alcun criterio di accesso gestione per consentire a un host o a una rete di accedere al sistema Cisco SDM nel router.

Azione consigliata È necessario fornire un criterio di questo tipo per rendere Cisco SDM accessibile nel router. Non è possibile spostarsi in altre funzioni o inviare comandi al router se non è stato configurato un criterio di accesso gestione che consenta a un host o a una rete di accedere al sistema Cisco SDM in esecuzione nel router.

Messaggio di errore

`Avviso SDM - Current Host Not Allowed`

Descrizione Questo messaggio viene visualizzato se non è stato configurato alcun criterio di accesso gestione per consentire all'host o alla rete correntemente in uso di accedere al sistema Cisco SDM nel router.

Azione consigliata È necessario creare un criterio di questo tipo per consentire all'host o alla rete correntemente in uso di accedere al sistema Cisco SDM in esecuzione nel router. In caso contrario, nel momento dell'invio della configurazione al router si interromperà la connessione al router stesso. Fare clic su **Sì** per aggiungere un criterio di accesso gestione per l'host o la rete correntemente in uso. Fare clic su **No** per proseguire senza aggiungere un criterio per l'host o la rete correntemente in uso. Durante l'invio del comando la connessione con il router verrà interrotta e sarà necessario accedere a Cisco SDM utilizzando un host o una rete differenti.

SSH

Il router implementa Secure Shell (SSH) Server, una funzione che consente a un client SSH di creare una connessione protetta e crittografata con un router Cisco. Tale connessione fornisce una funzionalità simile a quella di una connessione Telnet in ingresso, ma offre una crittografia avanzata da utilizzare con i metodi di autenticazione del software Cisco IOS. Il server SSH nel software Cisco IOS è in grado di funzionare con i client SSH disponibili pubblicamente e a livello commerciale. La funzione è disattivata se il router non utilizza una versione di Cisco IOS IPSec DES o 3DES e se il ramo SSH della struttura Attività facoltative non è visualizzato.

SSH utilizza una chiave crittografica RSA per cifrare i dati che viaggiano tra il router e il cliente SSH. La generazione della chiave RSA in questa finestra consente l'attivazione della comunicazione SSH tra il router e i client SSH.

Messaggi di stato

Crypto key is not set on this device

Questo messaggio viene visualizzato se nel dispositivo non è stata configurata alcuna chiave di crittografia. Se non è stata configurata una chiave, è possibile immettere la dimensione del modulo e quindi generare la chiave.

Chiave RSA impostata nel router

Questo messaggio viene visualizzato se è stata generata una chiave di crittografia. SSH è attivato nel router.

Pulsante Dimensione modulo chiave

Questo pulsante è visibile se non è stata generata nessuna chiave di crittografia. Fare clic sul pulsante e immettere la dimensione del modulo che si desidera assegnare alla chiave. Per un valore compreso tra 512 e 1024, immettere un valore intero multiplo di 64, mentre per un valore superiore a 1024, è possibile immettere 1536 o 2048. Se si immette un valore superiore a 512, la generazione della chiave può richiedere almeno un minuto.

Pulsante Genera chiave RSA

Fare clic sul pulsante per generare una chiave di crittografia per il router utilizzando la dimensione del modulo immessa. Se la chiave crittografica è stata già generata, questo pulsante è disattivato.

Configurazione DHCP

Questa finestra spiega in che modo si possono gestire le configurazioni DHCP sul proprio router.

Pool DHCP

In questa finestra sono visualizzati i pool DHCP configurati nel router.

Nome pool

Il nome del pool DHCP.

Interfaccia

L'interfaccia su cui il pool DHCP è configurato. I client applicati a questa interfaccia riceveranno gli indirizzi IP da questo pool DHCP.

Dettagli del pool DHCP *nome*

In quest'area sono riportati i dettagli relativi al pool identificato in *nome*.

- **Intervallo pool DHCP**: intervallo di indirizzi IP che possono essere assegnati ai client.
- **Indirizzo IP router predefinito**: se il router dispone di un indirizzo IP nella stessa subnet del pool DHCP, verrà visualizzato in questo campo.
- **Server DNS**: gli indirizzi IP dei server DNS che il router fornirà ai client DHCP.
- **Server WINS**: gli indirizzi IP dei server WINS che il router fornirà ai client DHCP.
- **Nome di dominio**: il nome di dominio configurato nel router.
- **Durata lease**: il periodo di tempo durante il quale il router assegnerà in lease l'indirizzo IP a un client.
- **Importa tutto**: l'opzione consente al router di importare i parametri di opzione DHCP nel database del server DHCP e di inviare anche queste informazioni ai client DHCP nella LAN al momento della richiesta degli indirizzi IP.

Aggiungi

Scegliere questa opzione per creare un nuovo pool DHCP. L'utente deve specificare il nome del pool DHCP, la rete del pool DHCP, la gamma indirizzi IP del pool DHCP, la durata del lease. Opzionalmente i server DNS, i server WINS, il nome di dominio e il default gateway possono essere configurati anche nel pool DHCP.

Modifica

Scegliere questa opzione per modificare un pool DHCP esistente.

Elimina

Scegliere questa opzione per eliminare un pool DHCP.

Stato pool DHCP

Fare clic su questo pulsante per vedere gli indirizzi IP rilasciati dal pool specificato. Se un pool DHCP contiene parametri diversi da rete del pool, gamma di indirizzi IP, Durata lease, server DNS, server WINS, nome di dominio e router predefinito, Cisco SDM mostra questo pool come di sola lettura. Se un pool contiene una gamma discontinua di indirizzi IP, esso viene visualizzato come di sola lettura.

Add or Edit DHCP Pool

Aggiungere o modificare un pool DHCP in questa finestra. Non è possibile modificare i pool predefiniti di Cisco SDM.

Nome pool DHCP

Immettere il nome del pool DHCP in questo campo.

Rete pool DHCP

Immettere la rete dalla quale verranno acquisiti gli indirizzi IP del pool, ad esempio 192.168.233.0. Non può trattarsi dell'indirizzo IP di un host singolo.

Subnet Mask

Immettere la subnet mask. La subnet mask di 255.255.255.0 fornisce 255 indirizzi IP.

Pool DHCP

Immettere gli indirizzi IP iniziale e finale dell'intervallo. Per esempio se la rete è 192.168.233.0 e la subnet mask è 255.255.255.0, l'indirizzo iniziale è 192.168.233.1 e quello finale è 192.168.233.254.

Lunghezza lease

Immettere la durata dell'assegnazione in lease ai client. È possibile specificare indirizzi di lease che non hanno scadenza, oppure specificare la durata del lease in giorni, ore e minuti. Non superare 365 giorni, 23 ore o 59 minuti.

Opzioni DHCP

Immettere le informazioni relative ai server DNS, ai server WINS, al nome di dominio e al router predefinito nei campi delle opzioni DHCP. I valori verranno inviati ai client DHCP quando questi invieranno la richiesta di un indirizzo IP.

Importa tutte le opzioni DHCP nel database server DHCP

Selezionare questa opzione per importare i parametri di opzione DHCP nel database del server DHCP e per inviare, inoltre, queste informazioni ai client DHCP nella LAN al momento della richiesta degli indirizzi IP.

Binding del DHCP

Questa finestra mostra il binding manuali del. Il binding manuale di assegnare sempre lo stesso indirizzo IP a un cliente specifico ogni volta che tale cliente richiede un indirizzo IP dai pool DHCP disponibili.

È anche possibile aggiungere nuovi binding, modificare o eliminare quelli esistenti.

Nome binding

Il nome assegnato al binding DHCP.

Host/Maschera IP

L'indirizzo IP e la maschera collegati al client.

Indirizzo MAC

L'indirizzo MAC di questo client.

Tipo

Il tipo di indirizzo MAC è uno dei seguenti:

- Ethernet

  Il client dispone di un indirizzo hardware.
- IEEE802

  Il client dispone di un indirizzo hardware.
- <Nessuno>

  Il client dispone di un identificatore del client.

Nome Client

Un nome opzionale assegnato al client.

Pulsante Aggiungi

Fare clic per aggiungere un nuovo binding DHCP manuale.

Pulsante Modifica

Fare clic per modificare il binding DHCP manuale specificato.

Pulsante Elimina

Fare clic per eliminare il binding DHCP manuale specificato.

Aggiungi o modifica binding DHCP

In questa finestra si possono aggiungere o modificare i binding DHCP manuali esistenti.

Nome

Immettere il nome che si desidera attribuire al binding DHCP. Durante la modifica del binding DHCP il campo nome è di sola lettura.

IP host

Immettere l'indirizzo IP che si vuole assegnare al client. L'indirizzo deve appartenere al pool DHCP disponibile per il client. Non immettere un indirizzo usato in un altro binding DHCP.

Maschera

Immettere la maschera utilizzata per l'indirizzo IP dell'host.

Identificatore

Fare clic sul menu a tendina e scegliere un metodo per identificare il client con un indirizzo MAC.

Indirizzo MAC

Immettere l'indirizzo MAC di questo client. Non immettere un indirizzo usato in un altro binding DHCP.

Tipo

Se si sceglie **Indirizzo hardware** dal menu a tendina Identificatore, scegliere **Ethernet** o **IEEE802** per impostare il tipo di indirizzo MAC del client.

Nome client (opzionale)

Immettere un nome per identificare il client. Il nome deve essere esclusivamente un nome di host, non un nome di tipo dominio. Ad esempio, *router* è un nome accettabile, ma *router.cisco.com* no.

Proprietà DNS

Il sistema DNS (Domain Name System) rappresenta un database di nomi host in Internet con i rispettivi indirizzi IP distribuiti in server DNS designati. Consente agli utenti della rete di fare riferimento agli host immettendo nomi invece di indirizzi IP, più difficili da ricordare. Utilizzare questa finestra per consentire l'utilizzo di server DNS per la conversione dei nomi host in indirizzi.

Attivare il nome host basato su DNS alla conversione degli indirizzi della casella di controllo.

Selezionare questa casella per attivare l'utilizzo di DNS nel router. Deselezionare questa casella se non si desidera utilizzare DNS.

Indirizzo IP DNS

Immettere gli indirizzi IP dei server DNS ai quali il router invierà le richieste DNS.

Fare clic sui pulsanti **Aggiungi**, **Modifica** o **Elimina** per gestire le informazioni relative agli indirizzi IP DNS.

Metodi DNS dinamici

Questa finestra visualizza un elenco dei metodi DNS dinamici.

Ciascun metodo DNS dinamico invierà con il suo aggiornamento anche il nome host e il nome di dominio configurati in **Configura > Attività aggiuntive > Proprietà router**. Tuttavia, se si crea un metodo DNS dinamico durante la configurazione di un'interfaccia WAN, è possibile sostituire il nome host e il nome di dominio configurati in **Configura > Attività aggiuntive > Proprietà router**. I nuovi nomi host e di dominio si applicheranno soltanto a tale metodo DNS dinamico.

Alcuni metodi dinamici DNS sono di sola lettura. Questi sono stati configurati nel software Cisco IOS mediante CLI e non possono essere modificati o eliminati. Per rendere modificabili questi metodi di sola lettura usare CLI per cambiare le opzioni di cache interno o gruppo host in HTTP o IETF.

Pulsante Aggiungi

Fare clic sul pulsante **Aggiungi** per creare un nuovo metodo DNS dinamico.

Pulsante Modifica

Per modificare un metodo DNS dinamico, sceglierlo dall'elenco dei metodi DNS dinamici esistenti e poi fare clic sul pulsante **Modifica**.

Pulsante Elimina

Per eliminare un metodo DNS dinamico, sceglierlo dall'elenco dei metodi DNS dinamici esistenti e poi fare clic sul pulsante **Elimina**.

Nota Se si cerca di eliminare un metodo DNS dinamico associato ad una o più interfacce, viene visualizzato un avviso.

Aggiungi o modifica metodo DNS dinamico

Questa finestra consente di aggiungere o modificare un metodo DNS dinamico. Impostare il tipo di metodo scegliendo tra **HTTP** e **IETF**.

HTTP

HTTP è un tipo di metodo DNS dinamico che aggiorna un provider di servizi DNS con modifiche dell'indirizzo IP dell'interfaccia associato.

Server

Se si usa HTTP, scegliere l'indirizzo del dominio del provider di servizi DNS dal menu a tendina.

Nome utente

Se si usa l'HTTP, immettere un nome utente per l'accesso al provider di servizi DNS.

Password

Se si usa l'HTTP, immettere una password per l'accesso al provider di servizi DNS.

IETF

IETF è un tipo di metodo DNS dinamico che aggiorna un provider di servizi DNS con modifiche dell'indirizzo IP dell'interfaccia associato.

Se si usa IETF, configurare un server DNS per il router in **Configura > Attività aggiuntive > DNS**.

CAPITOLO 29

Editor ACL

Le regole definiscono il modo in cui il router reagisce a un determinato tipo di traffico. Con Cisco SDM, è possibile creare regole di accesso che consentono al router di bloccare alcuni tipi di traffico e di consentirne altri, creare le regole di NAT che definiscono il traffico per la ricezione delle traduzioni di indirizzi e le regole IPSec che specificano il traffico da crittografare. Cisco SDM fornisce inoltre le regole predefinite utilizzate nelle configurazioni guidata, esaminabili e utilizzabili durante la creazione delle regole di accesso personalizzate. Inoltre, è possibile visualizzare le regole che non sono state create via Cisco SDM, dette regole definite esternamente, e le regole la cui sintassi non è supportata in Cisco SDM, dette regole non supportate.

Nella schermata Regole è possibile visualizzare un riepilogo delle regole definite nella configurazione del router e passare ad altre finestre che consentono di creare, modificare o eliminare le regole.

Categoria

In questo campo è specificato il tipo di regola. La scelta può essere effettuata tra una delle opzioni riportate di seguito.

Regole di accesso	Queste regole stabiliscono quali flussi di traffico possono accedere o uscire dalla rete e sono utilizzate dalle interfacce di router e dalle linee VTY che consentono agli utenti di accedere al router.
Regole NAT	Queste regole determinano il modo in cui gli indirizzi IP privati sono convertiti in indirizzi IP Internet validi.
Regole IPSec	Queste regole determinano quale traffico deve essere crittografato sulle connessioni protette.
Regole NAC	Regole che specificano gli indirizzi IP autorizzati dalla rete e quelli bloccati.
Regole firewall	Regole che possono specificare gli indirizzi di origine e destinazione, il tipo di traffico e se il traffico è consentito o meno.
Regole QoS	Regole che specificano il traffico che appartiene alla classe QoS a cui è associata la regola.
Regole non supportate	Si tratta delle regole che non sono state create via Cisco SDM e che non sono supportate in Cisco SDM. Queste regole sono di sola lettura e non possono essere modificate in Cisco SDM.
Regole definite esternamente	Si tratta delle regole che non sono state create via Cisco SDMma che sono supportate in Cisco SDM. Queste regole non possono essere associate ad alcuna interfaccia.
Regole Cisco SDM predefinite	Si tratta delle regole predefinite utilizzate nelle procedure guidate di Cisco SDM. Tali regole possono essere applicate nelle finestre Attività aggiuntive>Editor ACL.

N. regole

Indica il numero delle regole di questo tipo.

Descrizione

Questo campo contiene la descrizione della regola, se disponibile.

Configurazione delle regole

Per visualizzare la finestra relativa a un determinato tipo di regola, fare clic sulla categoria nella struttura delle regole. Quindi, creare e modificare la regola nella finestra visualizzata.

Nell'argomento della guida relativo a queste finestre sono contenute delle utili procedure di carattere generale. Nella sezione Procedure utili per regole di accesso e firewall sono contenute le procedure guidate relative ad altre attività.

Procedure utili per regole di accesso e firewall

In questa sezione sono contenute delle utili procedure.

- Come visualizzare l'attività del firewall?
- Come configurare un firewall in un'interfaccia non supportata?
- Come configurare un firewall dopo aver configurato una connessione VPN?
- Come consentire il traffico specifico mediante un'interfaccia DMZ?
- Come modificare un firewall esistente per consentire il traffico da una nuova rete o un nuovo host?
- Come configurare un pass-through NAT per un firewall?
- Come consentire il passaggio del traffico verso il concentratore Easy VPN attraverso il firewall?
- Come associare una regola a un'interfaccia?
- Come annullare l'associazione di una regola di accesso a un'interfaccia?
- Come eliminare una regola associata a un'interfaccia?
- Come creare una regola di accesso per un elenco Java?

Finestre delle regole

Nelle finestre di seguito elencate è possibile esaminare, creare, modificare ed eliminare le regole.

- Regole di accesso — Le regole di accesso in genere definiscono i flussi di traffico a cui si desidera consentire o bloccare l'ingresso o l'uscita dalla LAN. Tuttavia, è possibile utilizzare questo tipo di regole anche per altri scopi.
- Regole NAT — Le regole NAT sono utilizzate per specificare un set di indirizzi da convertire.
- Regole IPSec — Le regole IPSec sono regole estese utilizzate nei criteri IPSec al fine di specificare quali flussi di traffico si desidera crittografare nelle connessioni VPN.
- Finestra Regole NAC — Regole che specificano gli indirizzi IP autorizzati dalla rete e quelli bloccati.
- Finestra Regole firewall — Regole che possono specificare gli indirizzi di origine e destinazione, il tipo di traffico e se il traffico è consentito o meno.
- Finestra Regole Qos — Regole che specificano il traffico che appartiene alla classe QoS a cui è associata la regola.
- Finestra Regole non supportate — Le regole non supportate contengono sintassi o parole chiave non supportate in Cisco SDM. Benché possano influire sul funzionamento del router, le regole di questo tipo non possono essere modificate in Cisco SDM.
- Finestra Regole definite esternamente — Le regole definite esternamente sono regole create non utilizzando Cisco SDM.
- Finestra Regole Cisco SDM predefinite — Le regole predefinite di Cisco SDM sono regole di accesso predefinite. Queste regole sono utilizzate nelle configurazioni guidate iniziali e possono anche essere implementate nelle configurazioni create dall'utente.
- Finestra Regole NAC. Le regole vengono usate nel criterio eccezioni NAC per specificare gli host che sono esentati dal processo di convalida NAC. Esse vengono anche utilizzate per definire gli host o le reti per il controllo di ammissione.

Nella parte superiore della schermata sono elencate le regole di accesso configurate sul router. Questo elenco non contiene le regole Cisco SDM predefinite. Per visualizzare le regole predefinite di Cisco SDM, fare clic sul ramo **Regole SDM predefinite** della struttura Regole.

Nella parte inferiore della schermata sono invece elencate le Rule entry associate alla regola selezionata. Una Rule entry è composta dal criterio in base al quale consentire o bloccare il traffico in ingresso o in uscita e dall'azione da intraprendere nel caso in cui tale criterio venga soddisfatto. Se un flusso di traffico non soddisfa il criterio di una delle Rule entry elencate, tale flusso viene scartato.

Prima colonna

In questa colonna possono essere visualizzate delle icone che indicano lo stato di una regola.

Se una regola è di sola lettura, in questa colonna viene visualizzata l'icona corrispondente.

Nome/Numero

Indica il nome o il numero della regola di accesso.

I numeri compresi fra 1 e 99 sono utilizzati per identificare gli elenchi di accesso standard. I numeri compresi fra 100 e 199 sono utilizzati per identificare gli elenchi di accesso estesi. I nomi, in cui è possibile utilizzare anche i caratteri alfabetici, consentono di estendere l'intervallo degli elenchi di accesso standard oltre 99 e l'intervallo degli elenchi di accesso estesi oltre 199.

Utilizzata da

Indica il nome dell'interfaccia o i numeri VTY a cui è stata applicata la regola.

Tipo

Indica il tipo di regola (standard o estesa).

Le regole standard prevedono il confronto fra l'indirizzo IP di origine dei pacchetti e i criteri di indirizzo IP per determinare una corrispondenza. Il criterio di indirizzo IP della regola può essere un indirizzo IP singolo o parti di un indirizzo IP definite mediante una maschera carattere jolly.

Le regole estese possono analizzare una maggior quantità di campi di un pacchetto per determinare una corrispondenza. Tali regole consentono inoltre di esaminare gli indirizzi IP di origine e destinazione, il tipo di protocollo, le porte di origine e destinazione nonché altri campi di un pacchetto.

Le regole di accesso possono essere standard o estese. Le regole IPSec devono essere di tipo esteso in quanto devono essere in grado di specificare un tipo di servizio. Le regole definite esternamente e quelle non supportate possono essere standard o estese.

Descrizione

Questo campo contiene la descrizione della regola, se disponibile.

Prima colonna (nell'area delle Rule entry)

 Questa icona indica che il traffico è consentito.

 Questa icona indica che il traffico è bloccato.

Azione

Indica l'azione che il router deve eseguire quando all'interfaccia arriva un pacchetto che soddisfa i criteri inseriti nella Rule entry. Tale azione può essere di due tipi, Consenti o Nega.

- Consenti: per consentire il traffico che soddisfa i criteri della riga selezionata.
- Nega: per bloccare il traffico che soddisfa i criteri della riga selezionata.

Per maggiori informazioni sulle azioni di tipo Consenti e di tipo Nega relativamente a uno specifico tipo di regola, fare clic su Significato delle parole chiave Consenti e Nega.

Origine

Indica i criteri dell'indirizzo IP di origine che il traffico deve soddisfare. Questa colonna può contenere:

- Indirizzo IP e maschera carattere jolly. L'indirizzo IP specifica una rete e la maschera carattere jolly indica in che misura l'indirizzo IP della regola e quello del pacchetto devono corrispondere.
- La parola chiave **any.** Indica che l'indirizzo IP di origine può essere costituito da un indirizzo IP qualsiasi.
- Nome host.

Destinazione

Per le regole estese, indica i criteri dell'indirizzo IP di destinazione che il traffico deve soddisfare. L'indirizzo deve essere di una rete o di un host specifico. Questa colonna può contenere:

- Indirizzo IP e maschera carattere jolly. L'indirizzo IP specifica una rete e la maschera carattere jolly indica in che misura l'indirizzo IP della regola e quello del pacchetto devono corrispondere.
- La parola chiave **any.** Indica che l'indirizzo IP di origine può essere costituito da un indirizzo IP qualsiasi.
- Nome host.

Servizio

Per le regole estese, il servizio specifica il tipo di traffico che i pacchetti devono contenere per soddisfare la regola. Viene visualizzato il servizio, ad esempio echo-reply, seguito dal protocollo, quale ICMP. Una regola che consente o impedisce servizi multipli tra gli stessi endpoint deve contenere una voce per ciascun servizio.

Attributi

Questo campo può contenere altre informazioni sulla voce, come ad esempio se è stata attivata la registrazione.

Descrizione

Contiene una breve descrizione della voce.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta di una regola.	Fare clic su **Aggiungi** e creare la regola nella finestra visualizzata.
Modifica di una regola o di una Rule entry.	Selezionare la regola di accesso e fare clic su **Modifica**. Quindi, modificare la regola nella finestra Modifica regola.
Associazione di una regola a un'interfaccia.	Vedere la sezione Come associare una regola a un'interfaccia?
Eliminazione di una regola non associata a un'interfaccia.	Selezionare la regola di accesso e fare clic su **Elimina**.
Eliminazione di una regola associata a un'interfaccia.	Cisco SDM non consente di eliminare una regola associata a un'interfaccia. Per l'eliminazione è necessario innanzitutto dissociare la regola dall'interfaccia. Vedere la sezione Come eliminare una regola associata a un'interfaccia?
Reperimento di ulteriori informazioni.	Per maggiori informazioni su altre procedure, consultare la sezione Procedure utili per regole di accesso e firewall.

Aggiungi o modifica regola

Questa finestra consente di aggiungere o modificare una regola selezionata nella finestra Regole. È possibile rinominare o rinumerare la regola, aggiungere o cambiarne la descrizione, aggiungere, modificare, riordinare o eliminare le voci relative alla regola stessa.

Nome/Numero

Aggiungere o modificare il nome o il numero della regola.

Alle regole standard deve essere associato un numero compreso fra 1 e 99 o fra 1300 e 1999.

Alle regole estese deve essere associato un numero compreso nell'intervallo 100–199 or 2000–2699.

I nomi consentono di associare un'etichetta significativa alla regola di accesso.

Tipo

Selezionare il tipo di regola che si desidera aggiungere. Le regole standard consentono al router di analizzare l'host o la rete di origine nel pacchetto. Le regole estese consentono al router di analizzare l'host o la rete di origine, l'host o la rete di destinazione e il tipo di traffico contenuti nel pacchetto.

Descrizione

Inserire in questo campo una descrizione della regola. La descrizione non deve superare i 100 caratteri.

Elenco Rule entry

L'elenco mostra le voci che formano la regola. È possibile aggiungere nuove voci oppure modificare o eliminare voci esistenti. Si può inoltre riordinarle per cambiare l'ordine in base al quale vengono analizzate.

Si consiglia di seguire le seguenti istruzioni quando si creano nuove Rule entry:

- L'elenco deve contenere almeno un'istruzione di tipo consenti, altrimenti verrà bloccato tutto il traffico.
- L'ultima voce dell'elenco deve essere la voce di tipo consenti tutto o nega tutto.
- Le voci standard e le voci estese non possono essere utilizzate per la stessa regola.
- Non possono esistere voci duplicate all'interno della stessa regola.

Duplica

Fare clic su questo pulsante per utilizzare la voce selezionata come modello per una nuova voce. Ciò consente di risparmiare tempo e di ridurre gli errori. Ad esempio, per creare alcune Rule entry estesa che abbiano stessa origine e destinazione, ma protocolli o porte differenti, si può creare la prima voce utilizzando il pulsante Aggiungi. Dopo aver creato la prima voce, si può copiarla utilizzando il pulsante **Duplica** e modificare il campo relativo al protocollo o alla porta per creare una nuova voce.

Associazione interfaccia

Fare clic su **Associa** per applicare la regola a un'interfaccia.

Note Questo pulsante è attivo solo se si sta aggiungendo una regola nella finestra Regole di accesso.

Tabella riassuntiva funzioni

Funzione	Procedura
Aggiunta o modifica di una Rule entry.	Fare clic su **Aggiungi**, quindi creare la voce nella finestra visualizzata. Oppure scegliere **Modifica**, quindi modificare la voce nella finestra visualizzata.
Aggiunta di una Rule entry utilizzando una voce già esistente come modello.	Selezionare la voce che si desidera utilizzare come modello, fare clic su **Duplica**, quindi creare la voce nella finestra di dialogo visualizzata. Nella finestra di dialogo apparirà il contenuto della voce selezionata che si potrà modificare per creare una nuova voce.
Ordinamento delle Rule entry per l'analisi di determinate voci.	Selezionare la Rule entry, quindi fare clic sul pulsante **Sposta su** o **Sposta giù** per spostare la voce nella posizione desiderata.
Associazione di una regola a un'interfaccia.	Fare clic su **Associa** e selezionare l'interfaccia e la direzione nella finestra Associa a un'interfaccia. Se il pulsante **Associa** non è attivato, è possibile associare la regola a un'interfaccia facendo doppio clic sull'interfaccia nella finestra Interfacce e connessioni e utilizzando la scheda Associa.
Eliminazione di una Rule entry.	Selezionare la Rule entry e fare clic su **Elimina**. Quindi, confermare l'eliminazione nel messaggio di avviso visualizzato.
Maggiori informazioni sulle regole.	Consultare il sito Web di Cisco. Informazioni sugli elenchi di accesso IP sono disponibili all'indirizzo http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml (in lingua inglese)
Reperimento di ulteriori informazioni.	Per maggiori informazioni su altre procedure, consultare la sezione Procedure utili per regole di accesso e firewall

Associa a un'interfaccia

Questa finestra consente di associare una regola creata nella finestra Regole di accesso a un'interfaccia e di specificare se tale regola deve essere applicata al traffico in uscita o a quello in entrata.

Selezionare un'interfaccia

Selezionare l'interfaccia a cui applicare la regola.

Specificare una direzione

Fare clic su **In ingresso** se si desidera che il router verifichi i pacchetti in ingresso all'interfaccia. Il router confronterà i pacchetti con la regola prima di effettuare il routing e quindi accetterà o scarterà i pacchetti in base al tipo di regola (Consenti o Nega) configurato. Se si desidera che il router inoltri il pacchetto all'interfaccia in uscita prima di effettuare il confronto fra il pacchetto e le voci della regola di accesso, fare clic su **In uscita**.

Associazione di più regole alla stessa interfaccia

Se viene visualizzata una casella informativa in cui si avvisa che all'interfaccia è già associata un'altra regola di accesso con la stessa direzione, è possibile annullare l'operazione oppure continuare. In quest'ultimo caso, è possibile sia aggiungere le voci della nuova regola alla regola già associata all'interfaccia sia dissociare la regola precedente e associare all'interfaccia la nuova regola.

Tabella riassuntiva funzioni

Funzione	Procedura
Annullamento dell'operazione e conservazione dell'associazione fra l'interfaccia e la regola esistente.	Fare clic su **No**. L'associazione fra l'interfaccia e la regola esistente viene conservata e la regola creata nella finestra Aggiungi regola viene salvata. È possibile esaminare la regola esistente e la regola nuova e decidere se sostituire la regola esistente o se unire la regola esistente alle voci della nuova regola.
Continuare e unire le voci della regola creata alle voci della regola esistente.	Fare clic su **Sì**. Quando viene visualizzata la finestra in cui si chiede se si desidera unire o sostituire la regola esistente, fare clic su **Unisci**. Le voci della nuova regola vengono aggiunte dopo l'ultima voce della regola esistente. **Nota** Se la regola che si desidera unire non è compatibile con la regola esistente, sarà disponibile solo l'opzione per sostituire la regola esistente.
Sostituzione della nuova regola alla regola esistente.	Fare clic su **Sì**. Quando viene visualizzata la finestra in cui si chiede se si desidera unire o sostituire la regola esistente, fare clic su **Sostituisci**. La regola precedente non viene eliminata, viene soltanto dissociata dall'interfaccia e dalla direzione configurate in precedenza.

Aggiungere una Rule entry standard

Una Rule entry standard consente di autorizzare o bloccare il traffico proveniente da una determinata origine. L'origine può essere una rete o un host all'interno di una rete specifica. Si può creare un'unica Rule entry in questa finestra e, se necessario, è possibile ritornarvi per creare ulteriori voci.

Note Se un traffico non soddisfa i criteri in una delle Rule entry create viene bloccato in modo implicito. Per assicurarsi che il traffico che non si intende bloccare venga fatto passare, è consigliabile aggiungere in modo esplicito voci di tipo consenti alla regola che si sta configurando.

Azione

Selezionare l'azione che il router deve eseguire quando un pacchetto soddisfa i criteri inseriti nella Rule entry. Le possibilità sono **Consenti** e **Nega**. Il significato delle parole chiave Consenti e Nega varia in base al tipo di regola in cui vengono utilizzate. In Cisco SDM, le Rule entry standard possono essere utilizzate nelle regole di accesso, nelle regole NAT e negli elenchi di accesso associati a route map. Per maggiori informazioni sul significato delle parole chiave Consenti e Nega relativamente a un determinato tipo di regola, fare clic su Significato delle parole chiave Consenti e Nega.

Host/rete di origine

Indica i criteri dell'indirizzo IP di origine che il traffico deve soddisfare. I campi di quest'area variano sulla base del valore del campo Tipo.

Tipo

Selezionare una delle seguenti opzioni:

- Una rete. Selezionare se si desidera che l'azione si applichi a tutti gli indirizzi IP di una rete.
- Un nome host o indirizzo IP. Selezionare se si desidera che l'azione si applichi a un host o indirizzo IP specifico.
- Qualsiasi indirizzo IP. Selezionare se si desidera che l'azione si applichi a qualsiasi indirizzo IP.

Indirizzo IP

Se si è selezionato **una rete o un nome host o un indirizzo IP**, si deve immettere l'indirizzo IP in questo campo. Se l'indirizzo immesso è un indirizzo di rete, inserire una maschera carattere jolly per specificare le parti dell'indirizzo di rete di cui occorre verificare la corrispondenza.

Maschera

Se si è selezionato **una rete o un nome host o un indirizzo IP**, selezionare la maschera carattere jolly da questo elenco oppure immetterne una personalizzata. Uno 0 binario in una maschera carattere jolly indica che il relativo bit nell'indirizzo di rete di un pacchetto deve corrispondere in modo esatto. Un 1 binario in una maschera carattere jolly indica che non è necessario che il relativo bit nell'indirizzo di rete del pacchetto corrisponda.

Nome host/Indirizzo IP

Se si è selezionato **un nome host o un indirizzo IP** nel campo Tipo, immettere il nome o l'indirizzo IP dell'host. Se si immette un nome host il router deve essere configurato per l'uso di un server DNS.

Descrizione

Immettere una breve descrizione della voce in questo campo. La descrizione non deve superare i 100 caratteri.

Corrispondenze di registro per la voce

Se nelle proprietà di sistema si è specificato syslog, si può selezionare questa casella. In questo modo le corrispondenze saranno registrate nel registro di sistema.

Aggiungi Rule entry estesa

Una Rule entry estesa consente di bloccare o far passare il traffico in base alla sua origine e destinazione, al protocollo e al servizio specificati nel pacchetto.

Note Se un traffico non soddisfa i criteri in una delle Rule entry create viene bloccato in modo implicito. Per assicurarsi che il traffico che non si intende bloccare venga fatto passare, è consigliabile aggiungere in modo esplicito voci di tipo consenti alla regola che si sta configurando.

Azione

Selezionare l'azione che il router deve eseguire quando un pacchetto soddisfa i criteri inseriti nella Rule entry. Le possibilità sono **Consenti** e **Nega**. Quando si crea la voce di una regola IPSec le opzioni disponibili sono **Proteggi il traffico** e **Non proteggere**.

Il significato delle parole chiave Consenti e Nega varia in base al tipo di regola in cui vengono utilizzate. In Cisco SDM, le Rule entry estese possono essere utilizzate nelle regole di accesso, nelle regole NAT, nelle regole IPSec e negli elenchi di accesso associati a route map. Per maggiori informazioni sul significato delle parole chiave Consenti e Nega relativamente a un determinato tipo di regola, fare clic su Significato delle parole chiave Consenti e Nega.

Host/rete di origine

Indica i criteri dell'indirizzo IP di origine che il traffico deve soddisfare. I campi di quest'area variano sulla base del valore del campo Tipo.

Tipo

Selezionare una delle seguenti opzioni:

- Indirizzo IP specifico. Può essere un indirizzo di rete o l'indirizzo di un host specifico.
- Nome host.
- Qualsiasi indirizzo IP.

Indirizzo IP

Se si è selezionata l'opzione **Indirizzo IP specifico**, immettere la voce **Indirizzo IP** in questo campo. Se l'indirizzo immesso è un indirizzo di rete, inserire una maschera carattere jolly per specificare le parti dell'indirizzo di rete di cui occorre verificare la corrispondenza.

Maschera

Se si è selezionata l'opzione **Nome host o indirizzo IP**, scegliere la maschera carattere jolly da questo elenco o inserirne una personalizzata. Uno 0 binario in una maschera carattere jolly indica che il relativo bit nell'indirizzo di rete del pacchetto deve corrispondere in modo esatto. Un 1 binario in una maschera carattere jolly indica che non è necessario che il relativo bit nell'indirizzo di rete del pacchetto corrisponda.

Nome host

Se è stata selezionata la voce **Nome host** nel campo Tipo, immettere il nome dell'host.

Host/rete di destinazione

Indica i criteri dell'indirizzo IP di origine che il traffico deve soddisfare. I campi di quest'area variano sulla base del valore del campo Tipo.

Tipo

Selezionare una delle seguenti opzioni:

- Indirizzo IP specifico. Può essere un indirizzo di rete o l'indirizzo di un host specifico.
- Nome host.
- Qualsiasi indirizzo IP.

Maschera

Se è stata selezionata l'opzione **Nome host o indirizzo IP**, scegliere la maschera carattere jolly da questo elenco o inserirne una personalizzata. Uno 0 binario in una maschera carattere jolly indica che il relativo bit nell'indirizzo di rete del pacchetto deve corrispondere in modo esatto. Un 1 binario in una maschera carattere jolly indica che non è necessario che il relativo bit nell'indirizzo di rete del pacchetto corrisponda.

Nome host

Se è stata selezionata la voce **Nome host** nel campo Tipo, immettere il nome dell'host.

Descrizione

Immettere una breve descrizione della voce in questo campo. La descrizione non deve superare i 100 caratteri.

Protocollo e servizio

Selezionare il protocollo e il servizio a cui la voce deve applicarsi. Le informazioni da fornire variano da protocollo a protocollo. Fare clic sul protocollo per visualizzare le informazioni da fornire.

Porta di origine

Disponibile quando si seleziona TCP o UDP. Impostando questo campo il router applica un filtro alla porta di origine in un pacchetto. Di solito non è necessario impostare un valore della porta di origine per una connessione TCP. Se non si è sicuri di doverlo utilizzare, lasciare il campo impostato su **= any**.

Porta di destinazione

Disponibile quando si seleziona TCP o UDP. Impostando questo campo il router applica un filtro alla porta di destinazione in un pacchetto.

Tipi di protocolli	Informazioni da specificare nei campi Porta di origine e Porta di destinazione
TCP e UDP	Specificare la porta di origine e di destinazione per nome o numero. Se non è possibile reperire il nome o il numero, fare clic sul pulsante **...** e selezionare il valore desiderato nella finestra Servizio. Il campo accetta numeri di protocollo compresi tra 0 e 65535. • =. La Rule entry si applica al valore immesso nel campo a destra. • !=. La Rule entry si applica a qualsiasi valore tranne quello immesso nel campo a destra. • <. La Rule entry si applica a tutti i numeri di porta inferiori al numero immesso. • >. La Rule entry si applica a tutti i numeri di porta superiori al numero immesso. • Intervallo. La voce si applica all'intervallo di numeri di porta specificato nel campo a destra.

Tipi di protocolli	Informazioni da specificare nei campi Porta di origine e Porta di destinazione
ICMP	Specificare **qualsiasi** tipo di ICMP o specificare un tipo per nome o numero. Se non è possibile reperire il nome o il numero, fare clic sul pulsante **...** e selezionare il valore desiderato. Il campo accetta numeri di protocollo compresi tra 0 e 255.
IP	Specificare **qualsiasi** protocollo IP o specificare un protocollo per nome o numero. Se non è possibile reperire il nome o il numero, fare clic sul pulsante **...** e selezionare il valore desiderato. Il campo accetta numeri di protocollo compresi tra 0 e 255.

Nella sezione Servizi e porte è presente una tabella contenente i nomi e i numeri di porta disponibili in Cisco SDM.

Corrispondenze di registro per la voce

Se si è configurata il log dei messaggi firewall, è possibile selezionare questa casella di controllo e le voci corrispondenti saranno registrate nel file di log inviato al server syslog. Per maggiori informazioni, consultare il collegamento: Registro firewall.

Selezionare una regola

La finestra consente di selezionare una regola da utilizzare.

Categoria regola

Scegliere la categoria da cui si intende selezionare le regole. Le regole della categoria selezionata verranno visualizzate nella casella sotto l'elenco. Se la casella è vuota, per la categoria selezionata non sono state definite regole.

Nome/Numero

Indica il nome o il numero della regola.

Utilizzata da

Indica il modo in cui la regola viene utilizzata. Ad esempio, se la regola è stata associata ad un'interfaccia, indica il nome dell'interfaccia. Se la regola viene utilizzata in un criterio IPSec, indica il nome del criterio. Se invece la regola è stata usata da NAT, la colonna conterrà il valore NAT.

Descrizione

Indica la descrizione della regola.

Anteprima

In quest'area dello schermo verranno visualizzate le voci della regola selezionata.

Azione

Consenti o **Nega**. Per maggiori informazioni sulle azioni di tipo Consenti e di tipo Nega relativamente a uno specifico tipo di regola, consultare la sezione Significato delle parole chiave Consenti e Nega.

Origine

Indica i criteri dell'indirizzo IP di origine che il traffico deve soddisfare. Questa colonna deve contenere le seguenti voci:

- Indirizzo IP e maschera carattere jolly. L'indirizzo IP specifica una rete e la maschera carattere jolly indica in che misura l'indirizzo IP della regola e quello del pacchetto devono corrispondere.
- La parola chiave **any.** Indica che l'indirizzo IP di origine può essere costituito da un indirizzo IP qualsiasi.
- Nome host.

Destinazione

Per le regole estese, indica i criteri dell'indirizzo IP di destinazione che il traffico deve soddisfare. L'indirizzo deve essere di una rete o di un host specifico. Questa colonna deve contenere le seguenti voci:

- Indirizzo IP e maschera carattere jolly. L'indirizzo IP specifica una rete e la maschera carattere jolly indica in che misura l'indirizzo IP della regola e quello del pacchetto devono corrispondere.
- La parola chiave **any.** Indica che l'indirizzo IP di origine può essere costituito da un indirizzo IP qualsiasi.
- Nome host.

Servizio

Per le regole estese, il servizio specifica il tipo di traffico che i pacchetti devono contenere per soddisfare la regola. Viene visualizzato il servizio, ad esempio echo-reply, seguito dal protocollo, quale ICMP. Una regola che consente o impedisce servizi multipli tra gli stessi endpoint deve contenere una voce per ciascun servizio.

CAPITOLO 30

Mappatura porte-applicazioni

La PAM (Port-to-Application Mapping) consente di personalizzare i numeri di porta per i servizi e le applicazioni di rete. La PAM utilizza queste informazioni per supportare ambienti di rete che eseguono servizi utilizzando porte diverse da quelle solitamente associate con determinate applicazioni.

Le informazioni mantenute dalla PAM consentono l'esecuzione dei servizi supportati CBAC (Context-Based Access Control) su porte non standard. In precedenza il CBAC era limitato all'ispezione del traffico usando soltanto le porte usuali o registrate associate ad un'applicazione. Adesso la PAM consente agli amministratori di rete di personalizzare il controllo d'accesso alla rete per applicazioni e servizi specifici.

Mappatura porte-applicazioni

Questa finestra visualizza le mappature porte-applicazioni configurate sul router e consente di aggiungere, modificare e rimuovere voci PAM. Ciascuna riga della finestra visualizza una voce PAM e le voci sono raggruppate secondo i loro tipi.

Aggiunta, modifica, e eliminazione di pulsanti

Usare questi pulsanti per creare, aggiungere e rimuovere voci PAM. Facendo clic sul pulsante **Aggiungi** si creano voci che mappano i numeri di porta non standard sui nomi di protocollo. Facendo clic su **Modifica** si possono apportare modifiche sulle voci definite dagli utenti. Le voci col valore *Definito da sistema* nella colonna Tipo di protocollo non possono essere modificate né eliminate.

Colonna Protocollo applicazione

Questa colonna contiene il nome del protocollo applicazione, e i nomi dei tipi di protocollo. Per esempio le voci FTP e TFTP si trovano sotto il tipo di protocollo Trasferimento file.

Colonna Tipo di porta

Questo elenco viene visualizzato se il router sta eseguendo un'immagine di Cisco IOS che consente di specificare che questa voce di mappatura delle porte si applica al traffico TCP o UDP.

Colonna porta

Questa colonna contiene il numero di porta. Per esempio in questa colonna la voce definita dal sistema per HTTP presenterebbe la porta numero 80. Una voce definita da utente per HTTP potrebbe avere in questa colonna il numero di porta 8080 o un altro numero.

Colonna Tipo protocollo

Le righe in questa colonna visualizzano i seguenti valori:

- **Definito dall'utente**: la voce contiene una mappatura non standard tra un protocollo e un numero di protocollo. La voce potrebbe essere associata con un indirizzo IP di un host identificato da access control list (ACL) il cui numero è visualizzato nella colonna Elenco di Accesso.
- **Definito dal sistema**: la voce contiene una mappatura standard tra un protocollo e un numero di protocollo, come *tftp 69* o *smtp 25*. Le voci definite dal sistema non possono essere modificate o cancellate. Le voci definite dal sistema non contengono valori nell'Elenco di accesso perché si applicano a tutti gli host della rete.

Colonna Elenco di accesso

Una voce PAM si applica a un host singolo definito da una ACL standard. Questa colonna visualizza il numero delle ACL usate per identificare l'host al quale la voce PAM si applica. Se si vuole visualizzare l'ACL che identica l'host, scegliere **Attività aggiuntive > Editor ACL > Regole di accesso**. Quindi fare clic sul numero dell'ACL riportato in questa finestra.

Colonna Descrizione

Se è stata creata una descrizione della voce PAM, essa viene visualizzata in questa colonna.

Aggiungi o Modifica voce mappatura porte

È possibile aggiungere e modificare le voci di mappatura delle porte per i protocolli personalizzati o standard.

Campo protocollo

Quando si aggiunge una voce, specificare il protocollo facendo clic sul pulsante elenco (**...**) sulla destra e scegliere un protocollo definito dal sistema, oppure immettere il nome di un protocollo personalizzato. Non è possibile immettere nomi di protocolli personalizzati per i quali sono già presente mappature di porte.

Quando si modifica una voce il campo protocollo è disattivato. Se si deve cambiare il protocollo, eliminare la voce PAM e ricrearla usando le informazioni del protocollo desiderate.

Campo Descrizione

Questo campo viene visualizzato se il router sta eseguendo un'immagine di Cisco IOS che consente di specificare se questa voce di mappatura delle porte si applica al traffico TCP o UDP. È possibile inserire una descrizione facoltativa della voce di mappatura della porta. Le descrizioni sono utili quando si aggiungono voci per protocolli personalizzati o applicazioni speciali. Per esempio se si è creata una voce per un'applicazione database su misura denominata “orville” eseguita sull'host sf-5 si può immettere “orville-sf-5”.

Elenco Tipo porte

Questo elenco viene visualizzato se il router sta eseguendo un'immagine di Cisco IOS che consente di specificare che questa voce di mappatura delle porte si applica al traffico TCP o UDP. Scegliere **TCP** o **UDP**. L'impostazione predefinita è TCP.

Campo Numero porta

Immettere il numero di porta che si desidera mappare sul protocollo specificato. Se il router sta eseguendo un'immagine di Cisco IOS che consente di specificare se questa voce di mappatura delle porte si applica al traffico TCP o UDP, è possibile immettere più numeri di porta separati da virgole o gamme di numeri di porta uniti da trattini. Per esempio si potrebbero immettere tre numeri di porta non contigui come 310, 313, 318, o la gamma di porte 415-419.

Se il router non sta eseguendo un'immagine di Cisco IOS che consente di specificare se questa voce di mappatura delle porte si applica al traffico TCP o UDP è possibile immettere un solo numero di porta.

Campo host del servizio

Specificare l'indirizzo IP dell'host per il quale si applica questa mappatura porte. Se si necessita della stessa mappatura per un altro host, creare una voce PAM separata per tale host.

CAPITOLO 31

Firewall con criteri basati su zone

Il firewall con criteri basati su zone (ZPF, Zone-Policy Firewall) modifica l'interfaccia del firewall, passando da quella obsoleta a un modello di configurazione basato su zone più flessibile e comprensibile. Alle zone vengono assegnate delle interfacce e viene applicato un criterio di ispezione al traffico tra le zone. I criteri di interzona offrono flessibilità e livelli di dettaglio notevoli, grazie ai quali è possibile applicare vari criteri di ispezione a più gruppi host collegati alla stessa interfaccia del router.

I criteri del firewall vengono configurati mediante C3PL (Cisco Common Classification Policy Language) che utilizza una struttura gerarchica per la definizione dell'ispezione dei protocolli di rete e dei gruppi di host a cui l'ispezione viene applicata.

Per una descrizione dettagliata delle modalità di implementazione del firewall con criteri basati su zone, consultare *The Zone-Based Policy Firewall Design Guide* (Guida di implementazione del firewall con criteri basati su zone), disponibile sul sito cisco.com in **Support > Product Support > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Configure > Feature Guides** e facendo clic su Zone-Based Policy Firewall Design Guide. Il documento è disponibile al seguente collegamento:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Ordine delle attività di configurazione

Per configurare un firewall con criteri basati su zone è possibile seguire i seguente ordine di attività:

1. Definizione delle zone.
2. Definizione delle coppie di zone.
3. Definizione delle mappe di classi che descrivono il traffico a cui applicare il criterio se coinvolge una coppia di zone.
4. Definizione delle mappe di criteri per applicare le azioni al traffico della mappa di classi.
5. Applicazione delle mappe di criteri alle coppie di zone.
6. Assegnazione delle interfacce alle zone.

La sequenza delle attività non è fondamentale ma alcuni eventi devono essere completati in quest'ordine. Ad esempio, è necessario configurare una mappa di classi prima di assegnarla a una mappa di criteri. Allo stesso modo, non è possibile assegnare una mappa di criteri a una coppia di zone se non è stato configurato alcun criterio. Se si tenta di completare un'attività che si basa su un'altra parte della configurazione non ancora impostata, SDM impedirà di proseguire.

Finestra Zona

Una zona o una zona di protezione rappresenta un gruppo di interfacce a cui viene applicato un criterio di protezione. Le interfacce di una zona devono condividere funzioni e caratteristiche comuni. Ad esempio, due interfacce collegate alla LAN locale possono essere collocate in una zona di protezione e le interfacce collegate a Internet possono essere collocate in un'altra zona di protezione.

Per il traffico che coinvolge tutte le interfacce in un router, tutte le interfacce devono appartenere a una zona di protezione o all'altra. Non è necessario che tutte le interfacce del router facciano parte di zone di protezione.

Le Regole generali dei criteri basati su zone descrivono le regole che gestiscono il comportamento dell'interfaccia nel flusso di traffico tra interfacce appartenenti a una zona.

Questa finestra visualizza il nome di ciascuna zona di protezione, le interfacce in essa contenute e le coppie di zone associate a cui la zona appartiene. Una zona può appartenere a più coppie di zone.

Fare clic su **Aggiungi** per creare una nuova zona.

Fare clic su **Modifica** per scegliere interfacce diverse per una zona esistente.

Fare clic su **Elimina** per rimuovere una zona. Non è possibile eliminare una zona che appartiene a una coppia di zone.

Aggiunta o modifica di una zona

Per aggiungere una nuova zona, chiamata anche zona di protezione, immettere il nome della zona e scegliere le interfacce da includere in essa. L'elenco Interfaccia visualizza i nomi delle interfacce disponibili. Poiché è possibile collocare le interfacce fisiche solo in una zona, queste non vengono elencate nel caso in cui siano già state collocate in un'altra zona. Le interfacce virtuali, ad esempio le interfacce dialer o quelle di modello virtuale possono essere collocate in più zone e verranno sempre visualizzate nell'elenco.

Nota

- Il flusso di traffico in entrata o in uscita da questa interfaccia viene gestito dalla mappa di criteri associata alla zona.
- Un'interfaccia associata a tale zona può essere utilizzata per una VPN, DMVPN, Easy VPN, SSL VPN (VPN SSL) o per altri tipi di connessione da sito a sito il cui traffico potrebbe essere bloccato da un firewall. Se in questa finestra si associa un'interfaccia a una zona, SDM non crea alcuna ACL pass-through che consenta tale traffico. Il pass-through necessario per la mappa di criteri può essere configurato in due modi.
  - Passare a **Configura > Firewall e ACL > Modifica criterio firewall > Regola per nuovo traffico**. Nella finestra di dialogo visualizzata, specificare le informazioni relative agli indirizzi IP di origine e destinazione e il tipo di traffico di cui è consentito il passaggio attraverso il firewall. Nel campo Azione, selezionare **Consenti ACL**.
  - Passare a **Configura > C3PL > Mappa criteri > Ispezione protocollo**. Specificare una mappa di criteri di ispezione protocollo che consentirà il passaggio del traffico necessario attraverso il firewall.

Dopo aver creato una zona, è possibile modificare le interfacce ad essa associate ma non è possibile modificare il nome della zona.

Regole generali dei criteri basati su zone

L'appartenenza delle interfacce di rete del router alle zone è soggetta a varie regole che governano il comportamento dell'interfaccia, dal momento che è il traffico si sposta tra interfacce appartenenti a una zona.

- È necessario configurare una zona prima che ad essa vengano assegnate interfacce.
- Un'interfaccia può essere assegnata solo a una zona di protezione.
- Tutto il traffico in entrata e in uscita da un'interfaccia viene bloccato in modo implicito se l'interfaccia è assegnata a una zona, salvo il traffico in entrata e in uscita da altre interfacce della stessa zona e il traffico verso qualsiasi interfaccia del router.
- Per impostazione predefinita, il flusso di traffico è consentito in modo implicito tra le interfacce della stessa zona.
- Per consentire il traffico in entrata e in uscita da un'interfaccia appartenente a una zona, è necessario configurare un criterio che consenta o che ispezioni il traffico tra tale zona e le altre.
- La zona self è l'unica eccezione al criterio predefinito deny-all. Tutto il traffico verso una delle interfacce del router è consentito finché non viene bloccato in modo esplicito.
- Il flusso di traffico non è consentito tra un'interfaccia appartenente alla zona e un'interfaccia non appartenente alla zona.
- Le azioni relative all'autorizzazione, all'ispezione e allo scarto dei pacchetti possono essere applicate solo tra due zone.
- Le interfacce non assegnate a una zona agiscono come normali porte del router e possono utilizzare la configurazione classica di verifica di stato/CBAC.
- Se è necessario che un'interfaccia non faccia parte di un criterio di zona/firewall, potrebbe comunque essere necessario inserire l'interfaccia in una zona e configurare un criterio che autorizza tutto il traffico (un criterio fittizio) tra tale zona a la zona verso cui si desidera autorizzare il flusso del traffico.

- Come conseguenza di quanto appena detto, se il traffico può essere consentito tra tutte le interfacce in un router, tutte le interfacce devono appartenere al modello di zona (ciascuna interfaccia deve appartenere a una zona o all'altra).
- L'unica eccezione a quanto appena affermato che adotta un approccio predefinito di negazione del traffico è relativa al traffico in entrata e in uscita dal router, che è consentito per impostazione predefinita. È possibile configurare un criterio esplicito per limitare tale traffico.

Questo gruppo di regole è stato preso dal *The Zone-Based Policy Firewall Design Guide* (Guida di implementazione del firewall con criteri basati su zone) disponibile al seguente collegamento:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Coppie di zone

Una coppia di zone consente di specificare un criterio di firewall unidirezionale tra due zone di sicurezza. La direzione del traffico viene specificata immettendo una zona di protezione di origine e una di destinazione. Non è possibile definire la stessa zona come origine e destinazione.

Se si desidera consentire il flusso di traffico in entrambe le direzioni tra due zone, è necessario creare una coppia di zone per ciascuna direzione. Se si desidera consentire il flusso di traffico tra tutte le interfacce, è necessario configurare ciascuna interfaccia in una zona.

La seguente tabella riporta un esempio di quattro coppie di zone:

Coppia di zone	Origine	Destinazione	gruppo
LAN-out	zone-VLAN1	zone-FE1	inspection-policymap-a
LAN-in	zone-FE1	zone-VLAN1	inspection-policymap-b
Bkup-out	self	zone-BRI0	inspection-policymap-c
Bkup-in	zone-BRI0	self	inspection-policymap-c

LAN-out e LAN-in sono coppie di zone configurate per il flusso di traffico tra l'interfaccia LAN, VLAN1 e l'interfaccia FastEthernet 1. Ciascuna coppia di zone è controllata da un criterio diverso. Bkup-out e Bkup-in sono configurate per il traffico generato dal router. Lo stesso criterio controlla il traffico inviato da zone-BRI0 come traffico inviato dal router, rappresentato dalla zona self.

Fare clic su **Aggiungi** per creare una coppia di zone.

Fare clic su **Modifica** per modificare il criterio associato a una coppia di zone.

Fare clic su **Elimina** per rimuovere una coppia di zone.

Aggiunta o modifica di una coppia di zone

Per configurare una nuova coppia di zone, immettere un nome per la coppia di zone, una zona di origine da cui viene generato il traffico, una zona di destinazione a cui è diretto il traffico e il criterio che determina il tipo di traffico che può essere autorizzato tra le zone. Gli elenchi relativi alla zona di origine e alla zona di destinazione contengono le zone configurate sul router e la zona self. La zona self può essere utilizzata se si stanno configurando coppie di zone per il traffico originato dal router stesso o destinato al router stesso, ad esempio una coppia di zone configurata per il traffico SNMP. L'elenco Criterio contiene il nome di ogni Mappa criteri configurata sul router.

Se si sta aggiungendo una coppia di zone, è possibile modificare la mappa di criteri ma non il nome delle zone di origine e di destinazione.

Aggiunta di una zona

È possibile configurare un'interfaccia come appartenente a una zona di protezione dalla scheda Associazione della finestra di dialogo Modifica interfacce e connessioni. La zona aggiunta comprenderà l'interfaccia che si sta modificando come appartenente alla zona.

Nota

- Il flusso di traffico in entrata o in uscita da questa interfaccia viene gestito dalla mappa di criteri associata alla zona.
- Un'interfaccia associata a tale zona può essere utilizzata per una VPN, DMVPN, Easy VPN, SSL VPN (VPN SSL) o per altri tipi di connessione da sito a sito il cui traffico potrebbe essere bloccato da un firewall. Se in questa finestra si associa un'interfaccia a una zona, SDM non crea alcuna ACL pass-through che consenta tale traffico. Il pass-through necessario per la mappa di criteri può essere configurato in due modi.
  - Passare a **Configura > Firewall e ACL > Modifica criterio firewall > Regola per nuovo traffico**. Nella finestra di dialogo visualizzata, specificare le informazioni relative agli indirizzi IP di origine e destinazione e il tipo di traffico di cui è consentito il passaggio attraverso il firewall. Nel campo Azione, selezionare **Consenti ACL**.
  - Passare a **Configura > C3PL > Mappa criteri > Ispezione protocollo**. Specificare una mappa di criteri di ispezione protocollo che consentirà il passaggio del traffico necessario attraverso il firewall.

Nome zona

Immettere il nome della zona che si desidera aggiungere.

Seleziona una zona

Se sul router è stata configurata una zona di protezione, è possibile aggiungere l'interfaccia in fase di configurazione come appartenente alla zona.

Selezionare una zona per l'interfaccia

Selezionare la zona in cui includere l'interfaccia e fare clic su **OK**.

CAPITOLO 32

Autenticazione, autorizzazione e accounting

AAA, acronimo di Authentication, Authorization, and Accounting, di Cisco IOS è uno schema di architettura per configurare in modo co erente un set di tre funzioni di protezione indipendenti. Esso esegue i servizi di autenticazione, autorizzazione e accounting in modo modulare.

AAA di Cisco IOS offre i seguenti vantaggi:

- Flessibilità e controllo migliorati
- Scalabilità.
- Metodi di autenticazione standardizzati. Con Cisco SDM SDM è possibile configurare i metodi di autenticazione RADIUS (Remote Authentication Dialin User Service) e TACACS+ (Terminal Access Controller Access Control System Plus).

Finestra principale AAA

In questa finestra è fornita una vista riepilogo della configurazione AAA sul router. Per visualizzare ulteriori informazioni dettagliate o per modificare la configurazione AAA, fare clic sul nodo appropriato nella struttura AAA.

Attivare/disattivare AAA

AAA è attivato per impostazione predefinita. Se si fa clic su **Disattiva**, in Cisco SDM viene visualizzato un messaggio indicante che verranno apportate modifiche alla configurazione in modo da garantire l'accesso al router.
La disattivazione di AAA impedirà la configurazione del router come server Easy VPN e l'associazione di account utente con viste dell'interfaccia della riga di comando (CLI).

Server e gruppi AAA

In questo campo di sola lettura è visualizzato un conteggio di server e gruppi di server AAA. Il router inoltra le richieste di autenticazione, autorizzazione e accounting ai server AAA che sono organizzati in gruppi per fornire al router server alternativi da contattare qualora il primo server contattato non fosse disponibile.

Criteri di autenticazione

In questo campo di sola lettura sono elencati i criteri di autenticazione configurati. Tali criteri definiscono la modalità di identificazione degli utenti. Per modificare i criteri di autenticazione, fare clic sul nodo secondario **Accesso** in **Criteri di autenticazione** nella struttura AAA.

Criteri di autorizzazione

In questo campo di sola lettura sono elencati i criteri di autorizzazione configurati. **Tali criteri definiscono i metodi che sono utilizzati per permettere o negare un accesso dell'utente.** Per modificare i criteri di autorizzazione, fare clic su **Criteri di autorizzazione** nella struttura AAA.

Per modificare i criteri di autorizzazione (Autorizzazione Exec e Autorizzazione di rete), fare clic rispettivamente sui nodi secondari **Exec** e **Rete** nel nodo **Criteri di autorizzazione** nella struttura AAA.

Server e gruppi di server AAA

In questa finestra è fornita una descrizione dei server e dei gruppi di server AAA.

Finestra Server AAA

In questa finestra è possibile visualizzare un'istantanea delle informazioni sui server AAA che la configurazione del router utilizza. Per ciascun server sono visualizzati l'indirizzo IP, il tipo di server e altri parametri.

Impostazioni globali

Fare clic su questo pulsante per eseguire le impostazioni globali per i server TACACS+ e RADIUS. Nella finestra Modifica impostazioni globali è possibile specificare per quanto tempo provare a contattare un server AAA prima di passare a quello successivo, la chiave da utilizzare quando si contatta il server TACACS+ o RADIUS e l'interfaccia sulla quale verranno ricevuti i pacchetti TACACS+ o RADIUS. Queste impostazioni verranno applicate a tutti i server per i quali non sono state eseguite impostazioni specifiche del server.

Pulsante

Fare clic su questo pulsante per aggiungere un server TACACS+ o RADIUS all'elenco.

Pulsante

Fare clic su questo pulsante per modificare le informazioni sul server AAA selezionato.

Elimina...

Fare clic su questo pulsante per eliminare le informazioni sul server AAA selezionato.

Indirizzo IP del server

L'indirizzo IP del server AAA.

Tipo

Il tipo di server: TACACS+ o RADIUS.

Parametri

In questa colonna sono elencati il timeout, la chiave e altri parametri relativi a ciascun server.

Aggiungi o modifica server TACACS+

In questa finestra aggiungere o modificare le informazioni relative a un server TACACS+.

IP o host del server

Immettere l'indirizzo IP o il nome host del server. Se il router non è stato configurato per utilizzare un server DNS (Domain Name Service), immettere un indirizzo IP.

Connessione singola al server

Selezionare questa casella se si desidera che il router mantenga una singola connessione aperta al server TACACS+, piuttosto che aprire e chiudere una connessione TCP ogni volta che comunica con il server. Una singola connessione aperta risulta più efficiente in quanto consente al server TACACS+ di gestire un maggior numero di operazioni TACACS+.

Nota Questa opzione è supportata solo se sul server TACACS+ è in esecuzione CiscoSecure versione 1.0.1 o successiva.

Configurazione specifica del server

Selezionare questa casella se si desidera ignorare le impostazioni globali del server AAA e indicare il valore di timeout specifico di un server nonché la chiave di crittografia.

Timeout (secondi)

Immettere il numero di secondi durante i quali il router deve tentare di contattare questo server prima di passare a quello successivo nell'elenco dei gruppi. Se non si immette alcun valore, il router utilizzerà quello configurato nella finestra Impostazioni globali dei server AAA.

Configura chiave

Opzionale. Immettere la chiave da utilizzare per crittografare il traffico tra il router e il server. Se non si immette alcun valore, il router utilizzerà quello configurato nella finestra Impostazioni globali dei server AAA.

Nuova chiave/Conferma chiave

Immettere la chiave e inserirla nuovamente per la conferma.

Aggiungi o modifica server RADIUS

In questa finestra aggiungere o modificare le informazioni relative a un server RADIUS.

IP o host del server

Immettere l'indirizzo IP o il nome host del server. Se il router non è stato configurato per utilizzare un server DNS (Domain Name Service), immettere un indirizzo IP.

Porta di autorizzazione

Specificare la porta del server da utilizzare per le richieste di autorizzazione. Il valore predefinito è 1645.

Porta di accounting

Specificare la porta del server da utilizzare per le richieste di accounting. Il valore predefinito è 1646.

Timeout in secondi

Opzionale. Immettere il numero di secondi durante i quali il router deve tentare di contattare questo server prima di passare a quello successivo nell'elenco dei gruppi. Se non si immette alcun valore, il router utilizzerà quello configurato nella finestra Impostazioni globali dei server AAA.

Configura chiave

Opzionale. Immettere la chiave da utilizzare per crittografare il traffico tra il router e il server. Se non si immette alcun valore, il router utilizzerà quello configurato nella finestra Impostazioni globali dei server AAA.

Nuova chiave/Conferma chiave

Immettere la chiave e inserirla nuovamente per la conferma.

Modifica impostazioni globali

È possibile specificare le impostazioni di comunicazione che verranno applicate a tutte le comunicazioni tra il router e i server AAA di questa finestra. Qualsiasi impostazione di comunicazione eseguita per uno specifico router sostituirà le impostazioni effettuate in questa finestra.

Server TACACS+/server RADIUS

Fare clic sul pulsante appropriato per specificare il tipo di server per il quale si impostano i parametri globali. Se si seleziona Server TACACS+, i parametri verranno applicati a tutte le comunicazioni con i server TACACS+ che non hanno un set di parametri specifici del server. Se si seleziona Server RADIUS, i parametri verranno applicati a tutte le comunicazioni con i server RADIUS che non hanno un set di parametri specifici del server.

Timeout (secondi)

Immettere il numero di secondi di attesa per una risposta dal server RADIUS o TACACS+.

Chiave

Immettere la chiave di crittografia per tutte le comunicazioni tra il router e i server TACACS+ o RADIUS.

Selezionare l'interfaccia di origine

Selezionare questa casella se si desidera specificare una singola interfaccia su cui il router deve ricevere i pacchetti TACACS+ o RADIUS.

Interfaccia

Selezionare l'interfaccia del router sulla quale devono essere ricevuti dal router i pacchetti TACACS+ o RADIUS. Se la casella **Selezionare l'interfaccia di origine** non è selezionata, questo campo verrà disattivato.

Finestra Gruppi di server AAA

In questa finestra sono visualizzati i gruppi di server AAA configurati sul router. Se non è stato configurato alcun server, tale finestra risulta vuota.

Aggiunta, modifica, e eliminazione di pulsanti

Fare clic sul pulsante **Aggiungi** per creare un gruppo server RADIUS. Dopo aver creato questo gruppo, nella finestra vengono visualizzati il nome e i membri del gruppo. Fare clic su **Modifica** per modificare le informazioni sul gruppo server evidenziato. Fare clic su **Elimina** per rimuovere il gruppo server evidenziato.

Nome gruppo

Il nome del gruppo di server. I nomi di gruppo server consentono di usare un nome singolo per riferirsi a più server.

Tipo

Il tipo di server nel gruppo selezionato: TACACS+ o RADIUS.

Membri gruppo

Gli indirizzi IP o i nomi host dei server AAA del gruppo.

Aggiungi o modifica gruppo server AAA

In questa finestra è possibile creare o modificare un gruppo server AAA.

Nome gruppo

Immettere un nome per il gruppo.

Tipo di server

Selezionare il tipo di server: RADIUS o TACACS+.

Nota Questo campo potrebbe essere protetto e impostato su un tipo specifico, a seconda della configurazione che si sta eseguendo.

Selezionare i server da inserire in questo gruppo di server AAA

In questa area vengono elencati gli indirizzi IP di tutti i server AAA configurati sul router del tipo scelto, insieme alle porte di autorizzazione ed accounting utilizzate. Selezionare la casella **Seleziona** accanto ai server da aggiungere.

Criteri di autenticazione e autorizzazione

Le finestre Criteri di autenticazione e di autorizzazione riepilogano le informazioni dei criteri di autenticazione sul router.

Tipo di autenticazione

Il tipo di criteri di autenticazione.

Numero di criteri

Il numero di criteri di questo tipo.

Utilizzo

La descrizione dell'utilizzo di tali criteri.

Finestre autenticazione e autorizzazione?

Le finestre Accesso e le finestre di autorizzazione Exec e di Rete visualizzano gli elenchi di metodi usati per autenticare gli accessi, le richieste NAC e autorizzare il livello di comando Exec richiesto dalla rete. Da queste finestre è possibile esaminare e gestire questi elenchi di metodi.

Aggiunta, modifica, e eliminazione di pulsanti

Usare questi pulsanti per creare, aggiungere e rimuovere elenchi di metodi.

Nome elenco

Nome dell'elenco metodi. Un elenco metodi è un elenco sequenziale che descrive i metodi di autenticazione da richiedere per autenticare un utente.

Metodo 1

Il metodo che il router tenterà per primo. Se uno dei server in questo metodo autentica l'utente (invia una risposta PASS), l'autenticazione viene completata. Se un server restituisce una risposta FAIL, l'autenticazione non riesce. Se nessuno dei server risponde al primo metodo, il router utilizza quello successivo nell'elenco. I metodi possono essere disposti in ordine quando si crea o modifica un elenco di metodi.

Metodo 2, 3 e 4

I metodi che il router utilizza se i server cui viene fatto riferimento nel metodo 1 non rispondono. Se esistono meno di quattro metodi, le posizioni per le quali non è stato configurato alcun elenco sono mantenute vuote.

Autenticazione NAC

La finestra di autenticazione NAC visualizza gli elenchi di metodi EAPoUDP configurati sul router. Se per creare la configurazione NAC sul router è stata utilizzata la procedura guidata, questa finestra contiene la seguente voce:

Nome elenco	Metodo 1
predefinita	gruppo SDM_NAC_Group

È possibile specificare un elenco di metodi aggiuntivi in questa finestra se si desidera che il router provi altri metodi prima di fare ricorso all'ultimo metodo predefinito.

Aggiunta, modifica, e eliminazione di pulsanti

Usare questi pulsanti per creare, aggiungere e rimuovere elenchi di metodi.

Colonna Nome elenco

Nome dell'elenco metodi. Un elenco metodi è un elenco sequenziale che descrive i metodi di autenticazione da richiedere per autenticare un utente.

Colonna Metodo 1

Il metodo che il router tenterà per primo. Se uno dei server in questo metodo autentica l'utente (invia una risposta PASS), l'autenticazione viene completata. Se un server restituisce una risposta FAIL, l'autenticazione non riesce. Se nessuno dei server risponde al primo metodo, il router utilizza quello successivo nell'elenco. I metodi possono essere disposti in ordine quando si crea o modifica un elenco di metodi.

Colonne Metodo 2, 3 e 4

I metodi che il router utilizza se i server cui viene fatto riferimento nel metodo 1 non rispondono. Se esistono meno di quattro metodi, le posizioni per le quali non è stato configurato alcun elenco sono mantenute vuote.

Autenticazione 802.1x

La finestra di autenticazione 802.1x visualizza gli elenchi di metodi configurati per l'autenticazione 802.1. Se per creare la configurazione 802.1x è stata utilizzata la procedura guidata LAN, questa finestra contiene la seguente voce:

Nome elenco	Metodo 1
predefinita	group radius

Nota Non è possibile specificare altri elenchi metodi per la configurazione 802.1x.

Aggiunta, modifica, e eliminazione di pulsanti

Usare questi pulsanti per creare, aggiungere e rimuovere elenchi di metodi.

Colonna Nome elenco

Nome dell'elenco metodi. Un elenco metodi è un elenco sequenziale che descrive i metodi di autenticazione da richiedere per autenticare un utente.

Colonna Metodo 1

Il metodo che il router tenterà per primo. Se uno dei server in questo metodo autentica l'utente (invia una risposta PASS), l'autenticazione viene completata. Se un server restituisce una risposta FAIL, l'autenticazione non riesce. Se nessuno dei server risponde al primo metodo, il router utilizza quello successivo nell'elenco. I metodi possono essere disposti in ordine quando si crea o modifica un elenco di metodi.

Colonne Metodo 2, 3 e 4

I metodi che il router utilizza se i server cui viene fatto riferimento nel metodo 1 non rispondono. Se esistono meno di quattro metodi, le posizioni per le quali non è stato configurato alcun elenco sono mantenute vuote.

Aggiungi o modifica un elenco metodi per l'autorizzazione.

Un elenco metodi è un elenco sequenziale che descrive i metodi di autenticazione da richiedere per autenticare un utente. Gli elenchi metodi consentono di indicare uno o più protocolli di protezione da utilizzare per l'autenticazione, garantendo così un sistema di backup per l'autenticazione nel caso in cui il metodo iniziale abbia esito negativo.

Il software Cisco IOS utilizza il primo metodo elencato per autenticare gli utenti. Se tale metodo non riesce a rispondere, il software seleziona il metodo di autenticazione successivo nell'elenco metodi. Questo processo continua fino a quando non viene completata la comunicazione con un metodo di autenticazione elencato o finché tutti i metodi definiti nell'elenco metodi non sono esauriti.

È importante notare che il software Cisco IOS tenta l'autenticazione con il successivo metodo di autenticazione elencato solo in caso di mancata risposta dal metodo precedente. Se l'autenticazione ha esito negativo in qualsiasi punto del ciclo, ovvero il server di protezione o il database del nome utente locale risponde negando l'accesso dell'utente, il processo di autenticazione viene interrotto e non viene tentato nessun altro metodo di autenticazione.

Nome/Specificare

Selezionare il nome Predefinito nell'elenco Nome oppure selezionare Definito dall'utente e immettere un nome elenco metodi nel campo Specificare.

Metodi

Un metodo è un gruppo di server configurato. È possibile specificare e posizionare fino a quattro metodi nell'elenco nell'ordine in base al quale si desideri che il router li utilizzi. Il router tenterà il primo metodo nell'elenco. Se la richiesta di autenticazione riceve una risposta PASS o FAIL, il router non fornisce altre risposte. Se il router non riceve una risposta mediante il primo metodo, utilizza il successivo metodo nell'elenco e continua fino alla fine dell'elenco finché non riceve una risposta PASS o FAIL.

Aggiungi

Fare clic su questo pulsante per aggiungere un metodo all'elenco. Se non esiste alcun gruppo di server configurato da aggiungere, è possibile configurare un gruppo di server nella finestra visualizzata.

Elimina

Fare clic su questo pulsante per eliminare un metodo dall'elenco.

Sposta su/Sposta giù

Il router tenta i metodi nell'ordine in cui sono elencati in questa finestra. Fare clic su **Sposta su** per spostare un metodo in alto nell'elenco. Fare clic su **Sposta giù** per spostare un metodo più in basso nell'elenco.

Il metodo “none” sarà sempre l'ultimo dell'elenco, nessun altro metodo può essere spostato a un livello inferiore. È una limitazione di IOS che non accetta alcun nome di metodo dopo aver aggiunto “none” a un elenco metodi.

CAPITOLO 33

Provisioning del router

È possibile eseguire il provisioning del router usando un dispositivo USB collegato direttamente al router oppure tramite Secure Device Provisioning (SDP). Per essere disponibile in Cisco SDM, l'applicazione SDP deve essere supportata dalla versione Cisco IOS in uso.

Secure Device Provisioning

Questa finestra consente di utilizzare Secure Device Provisioning (SDP) per completare attività quali la registrazione del router con un server CA e la configurazione del router. Per trasferire l'applicazione SDP basata sul Web e completare il processo, fare clic su **Avvia SDP**.

Se è in corso l'ottenimento dei certificati, in Cisco SDM viene visualizzata la finestra Certificati in cui è possibile trovare i certificati dopo che questi sono stati ottenuti dal server CA.

Per informazioni sulla preparazione della registrazione SDP, vedere Suggerimenti per la risoluzione dei problemi relativi a SDP.

Per maggiori informazioni su SDP, fare clic sul seguente collegamento.

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332 (in inglese)

Nota Se il pulsante **Avvia SDP** non è disponibile, significa che la versione di Cisco IOS sul router non supporta l'applicazione SDP. Se il pulsante **Avvia SDP** è disattivato, significa che si è collegati a Cisco SDM come utente di visualizzazione senza privilegi amministrativi.

Provisioning del router da USB

Questa finestra indica se Cisco SDM ha rilevato un dispositivo token USB o flash USB connesso al router. Fare clic sul pulsante **Provisioning del router** per selezionare un file di configurazione dal token USB o dal dispositivo flash USB.

Se si sceglie di eseguire il provisioning del router in questo modo, il file di configurazione del token USB o del dispositivo flash USB viene unito alla configurazione in esecuzione sul router per creare un nuovo file di configurazione in esecuzione.

Provisioning del router da USB (caricamento di file)

Da questa finestra si può caricare un file di configurazione da un token USB o flash USB connesso al router. Il file sarà unito con il file di configurazione in esecuzione del router per creare un nuovo file di configurazione.

Per caricare un file di configurazione attenersi ai passaggi seguenti:

Passo 1 Scegliere il tipo di dispositivo dal menu a tendina.

Passo 2 Immettere il nome del file di configurazione in Nome file, includendo l'intero percorso, oppure fare clic su **Sfoglia** per scegliere il file nella finestra Selezione file.

Passo 3 Se il tipo di dispositivo è un token USB, immettere la password per l'accesso al token nel PIN Token.

Passo 4 Per visionare il file in anteprima, fare clic su **Anteprima file** e visualizzare il contenuto del file nel riquadro dei dettagli.

Passo 5 Fare clic su **OK** per caricare il file prescelto.

Suggerimenti per la risoluzione dei problemi relativi a SDP

Utilizzare queste informazioni prima della registrazione tramite Secure Device Provisioning (SDP) per preparare la connessione tra il router e il server di certificazione. Se si verificano problemi di registrazione, è possibile rivedere tutte queste attività in modo da localizzare il problema.

Istruzioni

- Dopo aver avviato SDP, ridurre a icona la finestra del browser di questo argomento della guida per visualizzare l'applicazione Web SDP.
- Per la configurazione del router con SDP, è necessario eseguirla subito dopo aver configurato la connessione WAN.
- Una volta completate le modifiche apportate alla configurazione in SDP, ritornare a Cisco SDM e fare clic su Aggiorna nella barra degli strumenti per visualizzare lo stato del punto di attendibilità nella finestra Certificati router della struttura Componenti VPN.

Suggerimenti per la risoluzione dei problemi

Questi suggerimenti implicano delle attività preliminari da eseguire sul router e sul server CA locali. È necessario comunicare questi requisiti all'amministratore del server CA assicurando quanto segue:

- Il router locale e il server CA dispongono reciprocamente della connettività IP. Il router locale deve essere in grado di eseguire il ping al server di certificazione che, a sua volta, deve essere in grado di eseguire il ping al router locale.
- L'amministratore CA utilizza un browser Web che supporta JavaScript.
- L'amministratore del server CA ha attivato dei privilegi nel router locale.
- Il firewall del router locale consentirà il traffico in uscita e in ingresso dal server di certificazione.
- Se si configura un firewall nel router Petitioner e/o nel router Registrar, è necessario verificare che il firewall consenta il traffico HTTP o HTTPS del computer da cui viene avviata l'applicazione Cisco SDM/SDP.

Per maggiori informazioni su SDP, consultare la pagina Web indicata di seguito:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332 (in inglese)

CAPITOLO 34

C3PL (Cisco Common Classification Policy Language)

Il linguaggio C3PL (Cisco Common Classification Policy Language) rappresenta una sostituzione strutturata per i comandi di configurazione specifici delle funzionalità. Consente di creare criteri di traffico in base ad eventi, condizioni ed azioni. SDM utilizza il linguaggio C3PL per creare la Mappa criteri e la mappa classi descritte negli argomenti della Guida che seguono.

Mappa criteri

Le mappe criteri specificano le azioni da intraprendere quando il traffico corrisponde ai criteri stabiliti. I criteri e i tipi di traffico sono definiti nelle mappe classi associate a una mappa criteri. Perché un router possa utilizzare le informazioni di una mappa criteri e le mappe classi associate, la mappa criteri deve essere associata a una coppia di zone. Per ulteriori informazioni sulla configurazione di zone e coppie di zone, vedere Firewall con criteri basati su zone.

Finestre Mappa criteri

Utilizzare le finestre delle mappe criteri per esaminare, creare e modificare le mappe criteri per QoS, HTTP e altri tipi di traffico. Nella parte superiore della finestra vengono elencate le mappe criteri configurate, in quella inferiore vengono visualizzati i dettagli della mappa criteri evidenziata. Per modificare una mappa criteri o vederne una quantità maggiore di dettagli, fare clic su **Modifica** per visualizzare una finestra di dialogo in cui è possibile visualizzare informazioni e apportare modifiche.

Questo argomento della guida fornisce una descrizione generale delle finestre della mappa criteri con alcuni dati di esempio.

Aggiungi

Fare clic su **Aggiungi** per visualizzare una finestra di dialogo nella quale è possibile configurare una mappa criteri.

Modifica

Fare clic su **Modifica** per visualizzare una finestra di dialogo nella quale è possibile modificare la mappa criteri selezionata. Se non è stata configurata alcuna mappa criteri, il pulsante **Modifica** è disattivato.

Elimina

Fare clic su **Elimina** per rimuovere la mappa criteri selezionata.

Area dell'elenco mappe criteri

In questa area vengono elencate le mappe criteri configurate per il particolare protocollo o la particolare funzionalità. Selezionare una mappa criteri per visualizzare i dettagli nella parte inferiore dello schermo. Nell'esempio che segue vengono mostrati due criteri IM.

Nome mappa criteri	Descrizione
im-pmap-g	criterio ospite
im-pmap-e	criterio dipendente

Dettagli della mappa criteri

Nei dettagli della mappa criteri selezionata viene mostrata la configurazione della stessa. I dettagli visualizzati variano in base al tipo di mappa criteri.

HTTP, IM, P2P, IMAP e POP3 visualizzano le colonne nome classe corrispondenza, azione e registro. Nella tabella che segue vengono mostrati i dettagli di una mappa criteri IM. Il router blocca il traffico AOL ma consente tutti gli altri tipi di traffico IM.

Nome classe di corrispondenza	Azione	Registro
aol-cmap	Disattivato	Disattivato
class-default	Attivato	Disattivato

I dettagli delle mappe criteri di verifica protocollo, SMTP e SUNRPC includono le colonne Nome classe di corrispondenza e Azione. Nella tabella che segue vengono mostrati i dettagli di una mappa criteri SUNRPC.

Nome classe di corrispondenza	Azione
cmap-sunrpc1	Consenti
cmap-sunrpc2	Nessuno

Aggiungi o Modifica mappa criteri QoS

Utilizzare queste informazioni come ausilio per l'aggiunta o la modifica di una mappa criteri QoS.

Nome criterio e descrizione

Nella creazione di una nuova mappa criteri, immettere un nome e una descrizione nei relativi campi. Se si sta modificando una mappa criteri, questi campi sono di sola visualizzazione.

Colonne Mappa classe, Accodamento, Imposta DSCP ed Elimina

Queste colonne riepilogano le informazioni su ogni mappa classi della mappa criteri. L'esempio che segue si riferisce a una mappa classe vocale:

```
Voice-FastEthernet0/1  LLQ 70%    ef          No
```

Questa mappa classe utilizza l'LLQ (Low Latency Queuing) e il 70% della larghezza di banda per questa interfaccia. Il valore DSCP è impostato su ef e i pacchetti di questo tipo non vengono eliminati.

È possibile utilizzare i pulsanti **Aggiungi**, **Modifica**, **Elimina**, **Sposta su** e **Sposta giù** per modificare le informazioni della mappa classe di questo elenco.

Aggiungi mappa criteri di verifica protocollo

Le mappe criteri di verifica specificano l'azione che il router deve effettuare per il traffico che corrisponde ai criteri delle mappe classi associate. Il router può consentire il passaggio del traffico, eliminarlo e, se desidera, registrare l'evento, oppure verificare il traffico.

Il nome e la descrizione immessi saranno visibili nella finestra Verifica mappe criteri. Nelle colonne Mappa classe e Azione vengono visualizzate le mappe classi associate a questa mappa criteri insieme all'azione che il router deve effettuare per il traffico descritto dalla mappa classe. Fare clic su **Aggiungi** per aggiungere una nuova mappa classe all'elenco e configurare l'azione. Fare clic su **Modifica** per modificare le impostazioni di una mappa classe. Utilizzare i pulsanti **Sposta su** e **Sposta giù** per modificare l'ordine di valutazione delle mappe classi.

Mappa criteri Layer 7

Questa finestra consente di selezionare una mappa criteri Layer 7 da utilizzare per verificare un'applicazione selezionata. Nella finestra vengono visualizzate le mappe criteri disponibili per tale applicazione. Scegliere una mappa criteri e fare clic su **OK**.

Verifica di applicazione

I criteri di verifica di applicazione vengono applicati al Layer 7 del modello OSI, dove le applicazioni dell'utente inviano e ricevono messaggi che consentono alle applicazioni di offrire utili capacità. Dal momento che alcune applicazioni possono offrire capacità indesiderabili che potrebbero rendere il router vulnerabile, i messaggi associati a queste capacità devono essere filtrati per limitare le attività sui servizi delle applicazioni.

Il firewall con criteri basati su zone del software Cisco IOS offre la verifica e il controllo delle applicazioni sui seguenti servizi delle applicazioni: HTTP, SMTP, POP3, IMAP, SUNRPC, P2P e sulle applicazioni IMAP. Per maggiori informazioni, vedere i seguenti collegamenti:

- Aggiungi mappa classi di verifica HTTP
- Aggiungi o Modifica mappa classi SMTP
- Aggiungi o Modifica mappa classi POP3
- Aggiungi o Modifica mappa classi IMAP
- Aggiungi o Modifica mappa classi SUNRPC
- Aggiungi o Modifica mappa classi P2P
- Aggiungi o Modifica mappa classi IM

Configura verifica approfondita pacchetti

La verifica di Layer 7 (applicazioni) incrementa la verifica di Layer 4 con la capacità di riconoscere ed applicare azioni specifiche del servizio, ad esempio bloccando o consentendo in modo selettivo capacità di ricerca di file, trasferimento di file e chat di testo. Le capacità specifiche del servizio variano in base al servizio.

Nella creazione di una nuova mappa criteri, immettere un nome nel campo **Nome mappa criteri**. È inoltre possibile aggiungere una descrizione. Fare clic su **Aggiungi > Nuova mappa classi** per creare una nuova mappa classi point-to-point. Aggiungi o Modifica mappa classi P2P contiene le informazioni sulla creazione di questo tipo di mappa classi. Fare clic su **Aggiungi > valore predefinito classe** per aggiungere la mappa classi predefinita.

Quando nella tabella viene visualizzata la mappa classi, specificare l'azione che si desidera venga eseguita quando viene rilevata una corrispondenza e se si desidera che le corrispondenze vengano registrate. È possibile specificare **<Nessuna>**, **Reimposta** o **Consenti**. Nell'esempio seguente sono riportate mappe classi P2P per gnutella ed eDonkey.

Nome classe di corrispondenza	Azione	Registro
gnutellaCMap	Consenti	
eDonkeyCMap	Reimposta	X

Mappe classi

Le mappe classi definiscono il traffico selezionato da un firewall con criteri basati su zone (ZPF, Zone-Policy Based Firewall) per applicazioni di criteri. Le mappe classi di Layer 4 ordinano il traffico in base ai seguenti criteri:

- Gruppo di accesso: un ACL standard, esteso o con nome può essere utilizzato per filtrare il traffico in base agli indirizzi di origine e destinazione e ai numeri di porta di origine e destinazione.
- Protocollo: i protocolli Layer 4 (TCP, UDP e ICMP) e i servizi di applicazioni come HTTP, SMTP, DNS e così via. È possibile specificare qualunque servizio conosciuto o definito dall'utente, noto a PAM.
- Mappa classi: è possibile nidificare all'interno di un'altra mappa classi una mappa classi subordinata che offre criteri di corrispondenza aggiuntivi.
- No: il criterio no specifica che il traffico che non corrisponde a uno specifico servizio (protocollo), gruppo di accesso o mappa classi subordinata sarà selezionato per la mappa classi.

Le mappe classi possono essere applicate agli operatori “qualsiasi” o “tutti” per determinare la modalità di applicazione dei criteri di corrispondenza. Se si sceglie “qualsiasi”, il traffico dovrà soddisfare solo uno dei criteri di corrispondenza nella mappa classi. Se si sceglie “tutti”, il traffico dovrà soddisfare tutti i criteri di corrispondenza nella mappa classi per appartenere a tale classe.

Associa mappa classi

Per associare una mappa classi con una mappa criteri di verifica, completare le seguenti operazioni.

Passo 1 Specificare un nome di mappa classi facendo clic sul pulsante a destra del campo del nome e selezionando **Aggiungi mappa classi**, **Seleziona mappa classi** o **valore predefinito classe**.

Passo 2 Nella casella Azione, fare clic su **Trasmetti**, **Elimina** o **Verifica**. Se si fa clic su **Elimina**, è possibile selezionare **Registra** per registrare l'evento di eliminazione. Se si fa clic su **Verifica**, scegliere **Opzioni avanzate** per specificare le mappe parametri, i criteri di verifica o le azioni policing desiderate per il traffico di questa classe.

Passo 3 Scegliere **OK** per chiudere questa finestra di dialogo e tornare alla finestra di dialogo Aggiungi o Modifica mappa criteri di verifica protocollo.

Opzioni avanzate mappe classi

Quando si sceglie l'azione di verifica per il traffico, è possibile specificare mappe parametri, verifica delle applicazioni e policing ZPF.

Verifica mappa parametri

Verifica mappa parametri specifica i parametri di controllo di sessione e timeout UDP, TCP e DNS. È possibile selezionare una mappa parametri esistente. Se non è stata configurata alcuna mappa parametri, il campo è disattivato. Fare clic su **Visualizza** per visualizzare la mappa parametri selezionata senza uscire da questa finestra di dialogo.

Mappa parametri Filtri URL

Le mappe parametri filtri URL sono in grado di specificare i server URL Filtering e gli elenchi di URL locali. È possibile selezionare una mappa parametri esistente. Se non è stata configurata alcuna mappa parametri, il campo è disattivato. Fare clic su **Visualizza** per visualizzare la mappa parametri selezionata senza uscire da questa finestra di dialogo.

Attiva verifica applicazione

Un criterio di verifica applicazione specifica i tipo di dati da verificare nei pacchetti di una specifica applicazione. È possibile selezionare un criterio di verifica delle applicazioni esistente. Se non è configurato alcun criterio di verifica delle applicazioni, questo campo è disattivato. Fare clic su **Visualizza** per visualizzare il criterio di verifica delle applicazioni selezionato senza uscire da questa finestra di dialogo.

Police Rate e Burst

È possibile limitare il traffico a una specifica velocità e indicare un valore di burst. Il valore di Police Rate può essere compreso tra 8.000 e 2.000.000.000 bps. Il valore di Burst Rate può essere compreso tra 1.000 e 512.000.000 byte.

Mappa classi QoS

Utilizzare questa finestra per visualizzare e modificare le informazioni sulle mappe classi QoS. Le mappe classi QoS vengono utilizzate nelle mappe criteri QoS per definire i tipi di traffico.

Fare clic sul nome di una mappa classi per visualizzare i dettagli sulla stessa nell'area **Dettagli della mappa classi**.

I dettagli di una mappa classi mostrano i protocolli per i quali esiste una corrispondenza di definizione del traffico. Nell'esempio che segue vengono illustrati i dettagli di una mappa classi di segnalazione vocale:

```
Dettagli della mappa classi: SDMSignal-FastEthernet0/1

    Nome elemento                    Valore elemento
Corrispondenza protocolli            h323,rtcp
```

H.323 e RTCP sono i protocolli di segnalazione vocale per i quali deve esistere una corrispondenza.

Aggiungi o Modifica mappa classi QoS

Utilizzare queste informazioni come ausilio per l'aggiunta o la modifica di una mappa classi QoS. Se si aggiunge una nuova mappa classi QoS, fare clic sul pulsante a destra del campo del nome e scegliere **Aggiungi mappa classi** o **Seleziona mappa classi** dal menu di scelta rapida.

Per ulteriori informazioni sulle opzioni **Elimina**, **Imposta DSCP** e **Accodamento**, vedere Azione.

Aggiungi o Modifica mappa classi QoS

Immettere il nome e la descrizione della mappa classi QoS che si sta creando in modo da poterla identificare e utilizzare con facilità. Fare clic su Classificazione per la descrizione dei pulsanti **Qualsiasi**, **Tutti** e **Modifica** del riquadro Classificazione.

Seleziona mappa classi

Fare clic sul nome della mappa classi da scegliere, quindi fare clic su **OK**. La voce di mappa classi viene aggiunta alla finestra dalla quale è stata chiamata questa finestra di dialogo.

Verifica approfondita

La verifica approfondita consente di creare mappe classi per i parametri specifici di un'applicazione. Ad esempio, è possibile creare mappe classi per le applicazioni P2P comuni come eDonkey, gnutella e kazaa2.

Finestre Mappa classi e Gruppi di servizi applicazioni

Utilizzare le finestre delle mappe classi per esaminare, creare e modificare le mappe classi per protocolli come HTTP, SMTP e POP3. Nell'area Mappa classi della finestra vengono elencate le mappe classi configurate, nella parte inferiore vengono visualizzati i dettagli della mappa classi selezionata. Per modificare una mappa classi o visualizzare più dettagli, fare clic su **Modifica**; verrà visualizzata una finestra di dialogo che consente di visualizzare informazioni e apportare modifiche.

Aggiungi

Scegliere **Aggiungi** per creare una nuova mappa classi del tipo selezionato ed immetterne la configurazione nella finestra di dialogo visualizzata.

Modifica

Scegliere **Modifica** per modificare la configurazione della mappa classi selezionata.

Elimina

Scegliere **Elimina** per rimuovere la mappa classi selezionata. È possibile che vengano visualizzate finestre di dialogo inerenti se vi sono dipendenze associate a questa configurazione, ad esempio mappe classi subordinate o mappe parametri che potrebbero essere utilizzate da altre mappe classi.

Area Mappe classi

In quest'area vengono visualizzate le mappe classi configurate per il protocollo selezionato. Contiene i nomi delle mappe classi configurate e altre informazioni ad esse inerenti.

Mappe classi QoS

Le mappe classi QoS sono visualizzati in una tabella che contiene le colonne Nome mappa classi e Descrizione. Di seguito viene riportato un esempio di tabella.

Nome mappa classi	Descrizione
CMAP-DMZ	Mappa classi QoS FTP e HTTP
CMAP-3	Test

Mappe classi Verifica, HTTP, SMTP, SUN RPC, IMAP e POP3

Questi tipi di mappe classi hanno una colonna Nome mappa classe e una colonna Utilizzata da. Di seguito viene riportata una tabella di esempio per HTTP.

Nome mappa classi	Utilizzata da
http-rqst	pmap-5
http-rsp-body	pmap-5

Gruppi di servizi Instant Messaging e Gruppi di servizi applicazioni Peer-to-Peer

I gruppi di servizi Instant Messaging Service e i gruppi di servizi applicazioni Peer-to-Peer (P2P) hanno una colonna aggiuntiva, perché le mappe classi sono configurate per una specifica applicazione, ad esempio l'applicazione di instant messaging Yahoo! messenger o l'applicazione P2P gnutella. Nella tabella che segue vengono mostrati dati di esempio per i gruppi di servizi applicazioni P2P.

Nome mappa classi	Utilizzata da	Tipo mappa classi
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

Dettagli della mappa classi

Nell'area Dettagli della mappa classi viene mostrata la configurazione di una particolare mappa classi. Contiene una colonna Nome elemento e una colonna Valore elemento.

Nome elemento

Nome dell'impostazione di configurazione. Ad esempio, una mappa classi HTTP potrebbe avere impostazioni per Intestazione richiesta, Abuso porta e Violazione di protocollo.

Valore elemento

Valore dell'impostazione di configurazione. Ad esempio, il valore dell'impostazione Richiesta HTTP potrebbe essere Lunghezza > 500 e il flag Abuso porta potrebbe essere disattivato.

Altre informazioni su Dettagli della mappa classi

Per ulteriori informazioni sui dettagli della mappa classi visualizzati in queste finestre, fare clic sui seguenti collegamenti:

- Aggiungi o Modifica mappa classi QoS
- Aggiungi o Modifica mappa classi di verifica
- Aggiungi mappa classi di verifica HTTP
- Aggiungi o Modifica mappa classi IM
- Aggiungi o Modifica mappa classi P2P
- Aggiungi o Modifica mappa classi SMTP
- Aggiungi o Modifica mappa classi SUNRPC
- Aggiungi o Modifica mappa classi IMAP
- Aggiungi o Modifica mappa classi POP3

Aggiungi o Modifica mappa classi di verifica

La creazione di una mappa classi di verifica consente di rendere disponibile per la verifica una grande quantità di traffico. Immettere un nome per identificare questa mappa classe nel campo **Nome classe**. È inoltre possibile immettere una descrizione. Se si sta modificando una mappa classi non è possibile modificarne il nome. Dopo avere specificato le condizioni desiderate per la mappa classi, scegliere **OK**.

Definizione della corrispondenza della classe con una o con tutte le condizioni

Fare clic su **Qualsiasi** se la classe deve corrispondere a una o più condizioni scelte. Fare clic su **Tutte** se la classe deve corrispondere a tutte le condizioni.

Scelta dell'oggetto della corrispondenza della mappa classi di verifica

Individuare l'oggetto della corrispondenza della mappa classi nella colonna sinistra. Fare clic sul segno più (+) accanto a un nodo per visualizzare i nodi secondari. Ad esempio, fare clic su **HTTP** per visualizzare i nodi secondari http e https. Per scegliere un elemento, farvi clic quindi fare clic su **Aggiungi >>**. Per rimuovere un elemento che è stato aggiunto alla colonna di destra, farvi clic quindi fare clic su **<<Rimuovi**.

Modifica dell'ordine di corrispondenza

Se si sceglie la corrispondenza con qualsiasi condizione, è possibile che si desideri modificare l'ordine di corrispondenza degli elementi nella colonna destra. Per spostare un elemento dell'elenco verso l'alto, farvi clic quindi fare clic su **Su**. Per spostare un elemento dell'elenco verso il basso, farvi clic quindi fare clic su **Giù**. Quando si fa clic sul primo elemento dell'elenco, il pulsante **Su** è disattivato. Quando si fa clic sull'ultimo elemento dell'elenco, il pulsante **Giù** è disattivato.

Associa mappa parametri

In questa finestra di dialogo vengono visualizzate le mappe parametri che possono essere associate alla mappa classi. Fare clic sulla casella **Seleziona** accanto alla mappa parametri che si desidera associare alla mappa classi.

Aggiungi mappa classi di verifica HTTP

Le mappe classi di verifica HTTP consentono di rendere disponibile per la verifica una grande quantità di dati Richiesta HTTP, Risposta e Risposta alla richiesta.

Per creare una mappa classi di verifica HTTP, effettuare le seguenti operazioni:

Passo 1 Immettere un nome classe per identificare la mappa classi. È anche possibile immettere una descrizione che sarà visibile nella finestra Verifica mappe classi HTTP.

Passo 2 Fare clic sul ramo della struttura HTTP contenente il tipo di dati che si desidera rendere disponibili per la verifica. È possibile creare una mappa classi per le richieste HTTP, le risposte e per le risposte alle richieste.

Passo 3 Fare clic sul ramo secondario appropriato per specificare ulteriormente il tipo di dati da includere.

Passo 4 Configurare i dati della mappa classi nei campi visualizzati.

Passo 5 Specificare le condizioni di corrispondenza facendo clic su **Qualunque condizione seguente** se la mappa classi deve corrispondere solo a una o più condizioni. Fare clic su **Tutte le voci specificate di seguito** se la mappa classi deve corrispondere a tutte le condizioni specificate.

Intestazione richiesta HTTP

Immettere i criteri di mappa classi per gli attributi di intestazione richiesta HTTP.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza globale di intestazione di richiesta che non deve essere superata dai pacchetti, e specificare il numero di byte.

Conteggio maggiore di

Fare clic su questa casella se si desidera specificare un limite al numero totale di campi dell'intestazione di richiesta che i pacchetti non devono superare, e specificare il numero di campi.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Nome campo e opzioni di configurazione

È possibile includere campi all'interno dell'intestazione dei criteri di verifica e specificare lunghezza, conteggio e stringhe di cui verificare la presenza. Fare clic su **Aggiungi** per includere un campo e immettere i criteri nella finestra di dialogo visualizzata.

Campi di intestazione richiesta HTTP

Scegliere il tipo di campo di intestazione dall'elenco e specificare i criteri di ispezione per lo stesso.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza che il campo non deve superare e specificare il numero di byte. Ad esempio si potrebbe bloccare una richiesta il cui campo di cookie superi i 256 byte o il cui campo agente utente superi i 128 byte.

Conteggio maggiore di

Se si desidera specificare il numero di volte che questo campo può essere ripetuto nell'intestazione fare clic su questa casella e immettere un numero. Ad esempio, si potrebbe bloccare una richiesta con linee di intestazione con diverse lunghezze di contenuto immettendo il valore 1. Questo esempio è una misura efficace per prevenire l'uso illegale (smuggling) della sessione.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Campo di corrispondenza

Selezionare questa casella se si desidera che la mappa classi corrisponda al tipo di campo scelto.

Altri campi in questa finestra di dialogo

A seconda del campo di intestazione HTTP scelto, è possibile che in questa finestra di dialogo vengano visualizzati altri campi che consentono di specificare criteri aggiuntivi. Ad esempio, se si sceglie il campo del **tipo di contenuto**, è possibile verificare la presenza di mancate corrispondenze del tipo di contenuto tra richiesta e risposta, tipi di contenuto sconosciuti e violazioni di protocollo per quel tipo di contenuto particolare. Se si sceglie il campo della **codifica trasferimento**, è possibile verificare la presenza dei diversi tipi di compressione e codifica.

Corpo della richiesta HTTP

È possibile verificare la lunghezza e le stringhe di caratteri del corpo della richiesta HTTP.

Lunghezza

Selezionare questa casella e scegliere **Maggiore di (>)** per specificare il limite superiore di lunghezza del corpo della richiesta. Scegliere **Minore di (<)** per specificare un limite inferiore.

Espressioni regolari

Se si desidera verificare la presenza di stringhe, fare clic su questa casella e scegliere una mappa classi di espressioni regolari esistenti oppure crearne una nuova che corrisponderà alle stringhe oggetto della verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Argomenti di intestazione richiesta HTTP

È possibile verificare la lunghezza degli argomenti inviati in una richiesta oltre che verificare la presenza di stringhe che corrispondono alle espressioni regolari che sono state configurate.

Lunghezza maggiore di

Fare clic su questa casella e specificare il numero di byte che non deve essere superato dalla lunghezza totale degli argomenti dell'intestazione della richiesta.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Metodo HTTP

I metodi HTTP indicano lo scopo di una richiesta HTTP. Scegliere i metodi HTTP nella colonna **Elenco metodi** di cui si desidera eseguire la verifica e selezionare la casella **Seleziona** accanto al metodo.

Abuso porta richiesta

La porta HTTP 80 viene talvolta utilizzata da IM, P2P, tunnelling e altre applicazioni. Selezionare i tipi di abuso porta di cui si desidera verificare la presenza. È possibile verificare la presenza di qualsiasi tipo di abuso porta, dell'abuso porta da parte di applicazioni IM, da parte di applicazioni P2P e di tunnelling.

URI richiesta

Immettere i criteri URI (Universal Resource Identifier) da includere nella mappa classi.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza URI che il pacchetto non deve superare e specificare il numero di byte.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Esempio di utilizzo

Configurare una mappa classi HTTP per bloccare una richiesta il cui URI corrisponde a una delle espressioni regolari che seguono:

".*cmd.exe"

".*sex"

".*gambling"

Intestazione di risposta

Immettere i criteri delle intestazioni di risposta HTTP da includere nella mappa classi.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza di intestazione di risposta globale che non deve essere superata dai pacchetti, e specificare il numero di byte.

Conteggio maggiore di

Fare clic su questa casella se si desidera specificare un limite al numero totale di campi dell'intestazione di risposta che non deve essere superata dai pacchetti, e specificare il numero di campi.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Campi di intestazione richiesta

Scegliere il tipo di campo di intestazione dall'elenco e specificare i criteri di ispezione per lo stesso.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza di campo che il pacchetto non deve superare e specificare il numero di byte.

Conteggio maggiore di

Fare clic su questa casella se si desidera specificare un limite al numero totale di campi di questo tipo che il pacchetto non deve superare, e specificare il numero di campi.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Altri campi in questa finestra di dialogo

A seconda del campo di intestazione HTTP scelto, è possibile che in questa finestra di dialogo vengano visualizzati altri campi che consentono di specificare criteri aggiuntivi. Ad esempio, se si sceglie il campo del **tipo di contenuto**, è possibile verificare la presenza di mancate corrispondenze del tipo di contenuto tra richiesta e risposta, tipi di contenuto sconosciuti e violazioni di protocollo per quel tipo di contenuto particolare. Se si sceglie il campo della **codifica trasferimento**, è possibile verificare la presenza dei diversi tipi di compressione e codifica.

Campo di corrispondenza

Selezionare questa casella se si desidera che la mappa classi corrisponda al tipo di campo scelto.

Corpo della risposta HTTP

Specificare i criteri del corpo della risposta HTTP di cui verificare la presenza.

Applet Java nella risposta HTTP

Selezionare questa casella di controllo se si vuole verificare la presenza di applet Java nella risposta HTTP.

Lunghezza

Selezionare questa casella e scegliere **Maggiore di (>)** per specificare il limite superiore di lunghezza del corpo della risposta. Scegliere **Minore di (<)** per specificare un limite inferiore.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Linea di stato risposta HTTP

Fare clic su questa casella e specificare le espressioni regolari da confrontare con le linee di stato della risposta. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe per le quali si esegue la verifica.

Esempio di utilizzo

Configurare il router in modo che registri un avviso in seguito al tentativo di accedere a una pagina vietata. Una pagina vietata in genere contiene il codice stato 403 e la linea di stato ha l'aspetto “HTTP/1.0 403 page forbidden\r\n.”

L'espressione regolare in questo caso è la seguente:

```
[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403
```

La registrazione è specificata nella mappa criteri a cui è associata la mappa classi HTTP.

Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Criteri delle intestazioni di richiesta/risposta

Immettere i criteri di mappa classi le intestazioni di richiesta/risposta HTTP.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza globale dell'intestazione di richiesta/risposta che non deve essere superata dai pacchetti, e specificare il numero di byte.

Conteggio maggiore di

Fare clic su questa casella se si desidera specificare un limite al numero totale di campi dell'intestazione di richiesta/risposta che non deve essere superata dai pacchetti, e specificare il numero di campi.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe delle quali si verifica la presenza. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Campi di intestazione richiesta/risposta HTTP

Scegliere il campo di intestazione di richiesta/risposta HTTP da includere nella mappa classi.

Lunghezza maggiore di

Fare clic su questa casella se si desidera specificare una lunghezza di campo che il pacchetto non deve superare e specificare il numero di byte.

Conteggio maggiore di

Fare clic su questa casella se si desidera specificare un limite al numero totale di campi di questo tipo che il pacchetto non deve superare, e specificare il numero di campi.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe delle quali si verifica la presenza. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Altri campi in questa finestra di dialogo

A seconda del campo di intestazione HTTP scelto, è possibile che in questa finestra di dialogo vengano visualizzati altri campi che consentono di specificare criteri aggiuntivi. Ad esempio, se si sceglie il campo del **tipo di contenuto**, è possibile verificare la presenza di mancate corrispondenze del tipo di contenuto tra richiesta e risposta, tipi di contenuto sconosciuti e violazioni di protocollo per quel tipo di contenuto particolare. Se si sceglie il campo della **codifica trasferimento**, è possibile verificare la presenza dei diversi tipi di compressione e codifica.

Campo di corrispondenza

Selezionare questa casella se si desidera che la mappa classi corrisponda al tipo di campo scelto.

Corpo della richiesta/risposta

Il router può verificare la lunghezza del corpo della richiesta/risposta e la presenza di stringhe di testo specifiche all'interno dello stesso.

Lunghezza

Selezionare questa casella e scegliere **Maggiore di (>)** per specificare il limite superiore di lunghezza del corpo della richiesta/risposta. Scegliere **Minore di (<)** per specificare un limite inferiore.

Espressioni regolari

Fare clic su questa casella per specificare le espressioni regolari da confrontare. Scegliere una mappa classi di espressioni regolari esistente o crearne una nuova che corrisponderà alle stringhe delle quali si verifica la presenza. Per ulteriori informazioni sulla creazione di espressioni regolari, vedere Aggiungi o Modifica espressione regolare. Per esaminare una mappa esistente senza lasciare questa finestra di dialogo, selezionarla nell'elenco **Selezionare una mappa esistente**, quindi fare clic su **Visualizza**.

Violazione protocollo richiesta/risposta

Per verificare la presenza di violazioni del protocollo nelle richieste/risposte HTTP, fare clic su **Violazione di protocollo**.

Aggiungi o Modifica mappa classi IMAP

La creazione di una mappa classi per la verifica del protocollo IMAP (Internet Message Access Protocol) può aiutare a garantire che gli utenti utilizzino meccanismi di autenticazione protetta per non compromettere le credenziali utente.

Immettere un nome per identificare questa mappa classe nel campo **Nome classe**. È inoltre possibile immettere una descrizione. Se si sta modificando una mappa classi non è possibile modificarne il nome.

Fare clic su **Stringa di accesso in testo non codificato** per far verificare al router la presenza di accessi non protetti nel traffico IMAP.

Fare clic su **Comando di protocollo non valido** per far verificare al router la presenza di comandi non validi nel traffico IMAP.

Aggiungi o Modifica mappa classi SMTP

Le mappe classi SMTP (Simple Mail Transfer Protocol) consentono di limitare la lunghezza del contenuto e ottenere la conformità del protocollo.

Immettere un nome per identificare questa mappa classe nel campo **Nome classe**. È anche possibile inserire una descrizione nel campo.

Immettere il valore di **Quantità massima di dati consentita per il trasferimento** nel riquadro **Criteri di corrispondenza**.

Aggiungi o Modifica mappa classi SUNRPC

Le mappe classi SUNRPC (SUN Remote Procedure Call) consentono di specificare il numero del programma di cui si desidera che il router verifichi il traffico.

Immettere un nome per identificare questa mappa classe nel campo **Nome classe**. È inoltre possibile immettere una descrizione. Se si sta modificando una mappa classi non è possibile modificarne il nome.

Scegliere **Aggiungi** nel riquadro **Numero programma di corrispondenza** per aggiungere un numero di programma.

Aggiungi o Modifica mappa classi IM

Le mappe classi IM (Instant Messaging) consentono di specificare il tipo di Instant Messaging e di richiedere la verifica del traffico di tutti i servizi IM o del solo traffico del servizio chat di testo.

Nel campo **Tipo mappa classi** scegliere **aol** per America Online, **msnmsgr** per Microsoft Networks Messenger oppure **ymsgr** per Yahoo! Messenger.

Nel riquadro Criteri di corrispondenza, scegliere **Tutti i servizi** oppure **Servizi chat di testo** se si desidera che venga verificato solo il traffico della chat di testo.

Aggiungi o Modifica mappa classi P2P

Una mappa classi P2P (Point-to-Point) specifica un'applicazione P2P e i relativi criteri di corrispondenza. È possibile specificare una sola applicazione per mappa classi.

Nome classe

Immettere un nuovo nome classe per creare la nuova mappa classi. Facendo clic sul pulsante a destra del campo è possibile selezionare le mappe esistenti da modificare. È possibile modificare i criteri di corrispondenza per una mappa classi ma non il tipo di mappa classi.

Tipo mappa classi

È possibile creare una mappa classi P2P per i seguenti tipi di servizi P2P:

- **eDonkey**
- **fasttrack**
- **gnutella**
- **kazaa2**

Criteri e valore di corrispondenza

Scegliere **Aggiungi** per immettere i criteri di corrispondenza specificando il tipo di connessioni che la classe di traffico deve identificare.

immettere i criteri di corrispondenza specificando il tipo di connessioni che la classe di traffico deve identificare. È possibile specificare l'identificazione delle connessioni di trasferimento file in base alla classe di traffico per fasttrack, gnutella e kazaa2. Per eDonkey, è possibile specificare l'identificazione delle connessioni di trasferimento file, richieste nomefile (ricerca nome file) e chat di testo, in base alla classe di traffico. Il valore dei criteri di corrispondenza può essere rappresentato da qualsiasi espressione regolare. Ad esempio, per specificare l'identificazione di tutte le connessioni di trasferimento file, immettere *.

Aggiungi regola P2P

immettere i criteri di corrispondenza specificando il tipo di connessioni che la classe di traffico deve identificare. È possibile specificare l'identificazione delle connessioni di trasferimento file in base alla classe di traffico per fasttrack, gnutella e kazaa2. Per eDonkey, è possibile specificare l'identificazione delle connessioni di trasferimento file, richieste nomefile (ricerca nome file) e chat di testo, in base alla classe di traffico. Il valore dei criteri di corrispondenza può essere rappresentato da qualsiasi espressione regolare. Ad esempio, per specificare l'identificazione di tutte le connessioni di trasferimento file, immettere *.

Aggiungi o Modifica mappa classi POP3

La creazione di una mappa classi per la verifica del protocollo POP3 (Post Office Protocol versione 3) può aiutare a garantire che gli utenti utilizzino meccanismi di autenticazione protetta per non compromettere le credenziali utente.

Immettere un nome per identificare questa mappa classe nel campo **Nome classe**. È inoltre possibile immettere una descrizione. Se si sta modificando una mappa classi non è possibile modificarne il nome.

Fare clic su **Stringa di accesso in testo non codificato** per far verificare al router la presenza di accessi non protetti nel traffico POP3.

Fare clic su **Comando di protocollo non valido** per far verificare al router la presenza di comandi non validi nel traffico POP3.

Mappe parametri

Le mappe di parametri specificano il comportamento di verifica di ZPF (Zone-Policy Firewall), per parametri quali Protezione Denial-of-Service, timer di sessione e connessione e impostazioni di registrazione. Le mappe parametri vengono anche applicate con le mappe classi e criteri di Layer 7 per definire comportamenti specifici dell'applicazione come gli oggetti HTTP, i requisiti di autenticazione POP3 e IMAP e le altre informazioni specifiche dell'applicazione.

Finestre delle mappe parametri

Nelle finestre delle mappe parametri vengono elencate le mappe parametri configurati per informazioni protocollo, URL Filtering, espressioni regolari e altri tipi di mappe parametri. Se la mappa parametri è stata associata ad una mappa classi, il nome della mappa classi viene visualizzato nella colonna utilizzata da. I dettagli della mappa parametri selezionata vengono visualizzati nella parte inferiore della finestra. È possibile aggiungere, modificare ed eliminare mappe parametri. SDM informa se si tenta di eliminare una mappa parametri in uso da parte di una mappa classi.

Per ulteriori informazioni sui dettagli della mappa parametri visualizzati in queste finestre, fare clic sui seguenti collegamenti:

- Timeout e soglie per Verifica mappe parametri e CBAC
- Aggiungi o Modifica mappa parametri per informazioni protocollo
- Impostazioni generali di URL Filtering
- Aggiungi o Modifica un server di URL Filtering
- Elenco URL locali
- Aggiungi o Modifica espressione regolare

Aggiungi o Modifica mappa parametri per informazioni protocollo

Può essere necessario identificare i server per tipi particolari di applicazioni, ad esempio le applicazioni IM, in modo da poter limitare l'uso a una particolare attività come la chat di testo.

Nome mappa parametri

Immettere un nome che richiami l'uso di questa mappa parametri. Ad esempio, se si crea un elenco di server per i server di chat di testo Yahoo! Instant Messenger, si potrebbe utilizzare il nome ymsgr-pmap.

Dettagli server

Questa area dello schermo contiene l'elenco dei nomi server, degli indirizzi IP server o degli intervalli di indirizzi IP.

Aggiungi o Modifica voce server

È possibile fornire il nome host o l'indirizzo IP di un singolo server oppure un intervallo di indirizzi IP assegnati a un gruppo di server.

È possibile immettere un nome host nel campo **Nome** se il router è in grado di contattare un server DNS in rete per risolvere l'indirizzo IP del server. Se si desidera immettere l'indirizzo IP di un solo server, immetterlo nel campo **Indirizzo IP singolo**. Se più server utilizzano un intervallo di indirizzi IP, utilizzare il campo **Intervallo IP**. Immettere l'indirizzo IP con il numero più basso nell'intervallo nel campo a sinistra e quello con il numero più alto nel campo a destra. Ad esempio, per immettere l'intervallo compreso tra 103.24.5.67 e 99, immettere `103.24.5.67` nel campo a sinistra e `103.24.5.99` nel campo a destra.

Aggiungi o Modifica espressione regolare

Un'espressione regolare corrisponde a una stringa di testo letteralmente come stringa esatta, oppure tramite *metacaratteri*, consentendo di ottenere la corrispondenza di più varianti di una stringa di testo. È possibile utilizzare un'espressione regolare per ottenere la corrispondenza con il traffico di alcune applicazioni; ad esempio, è possibile ottenere la corrispondenza del testo all'interno di un pacchetto HTTP.

Le espressioni regolari create possono essere utilizzate ovunque occorra un'espressione regolare nelle schermate dei firewall con criteri basati su zone. Metacaratteri dell'espressione regolare riporta l'elenco dei metacaratteri delle espressioni regolari e la loro modalità di utilizzo.

Nome

Immettere un nome per identificare l'espressione regolare. Quando si modifica l'espressione regolare, il campo nome è di sola lettura.

Elenco modelli

Un'espressione regolare può contenere più modelli. Fare clic su **Aggiungi** per visualizzare una finestra di dialogo in cui immettere un nuovo modello di espressione regolare. Ogni modello creato viene automaticamente aggiunto all'elenco. Se è necessario copiare un modello da un'altra espressione regolare, fare clic su **Copia modello**, fare clic sul segno più (+) accanto al nome dell'espressione regolare, fare clic sul modello desiderato, quindi su **OK**.

```
parameter-map type regex ref_regex
pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"
parameter-map type regex host_regex
pattern "secure\.keenvalue\.com"
pattern "\.looksmart\.com"
parameter-map type regex usragnt_regex
pattern "Peer Points Manager"
```

Sostituire con tabella.

Aggiungi modello

Il modello immesso in questa finestra viene aggiunto alla fine della mappa parametri espressione regolare che si sta modificando. È possibile riordinare i modelli della mappa parametri nella finestra Modifica espressione regolare.

Modello

Immettere il modello che si desidera aggiungere all'espressione regolare.

Pulsante Guida

Fare clic per visualizzare la finestra di dialogo Genera espressione regolare che è utile nella creazione di un'espressione regolare. Se si fa clic su **Guida**, qualsiasi testo immesso nel campo **Modello** viene visualizzato nel campo Espressione regolare della finestra di dialogo Genera espressione regolare.

Genera espressione regolare

Nella finestra di dialogo Genera espressione regolare è possibile costruire un'espressione regolare con caratteri e metacaratteri. I campi che consentono di inserire i metacaratteri includono il metacarattere tra parentesi nel nome campo.

Genera snippet

In questa area è possibile creare snippet di testo di testo regolare oppure inserire un metacaratteri nel campo Espressione regolare.

- Inizia all'inizio della linea (^): indica che lo snippet deve partire dall'inizio della linea, utilizzando il metacarattere accento circonflesso (^). Accertarsi di inserire qualunque snippet con questa opzione all'inizio dell'espressione regolare.
- Specifica stringa di caratteri: immettere manualmente una stringa di testo.
  - Stringa di caratteri: immettere una stringa di testo.
  - Caratteri speciali di escape: se nella stringa di testo da utilizzare letteralmente sono stati immessi metacaratteri, selezionare questa casella per farli precedere dal carattere di escape barra rovesciata (\). Ad esempio, se si immette “esempio.com”, questa opzione lo converte in “esempio\.com”.
  - Ignora distinzione maiuscole/minuscole: se si desidera ottenere la corrispondenza indipendentemente dal fatto che i caratteri siano maiuscoli o minuscoli, questa casella di controllo consente di aggiungere automaticamente del testo a questo fine. Ad esempio, “gatti” viene convertito in “[gG][aA][tT][tT][iI]”.

Specifica carattere

Consente di specificare un metacarattere da inserire nell'espressione regolare.

- Nega carattere: indica che non deve essere trovata alcuna corrispondenza con il carattere identificato.
- Qualsiasi carattere: inserisce il metacarattere punto (.) a indicare la corrispondenza di qualsiasi carattere. Ad esempio, per **c.s** si ottiene la corrispondenza di cis, css, cas e di qualunque parola che contenga tali caratteri, ad esempio caspita.
- Set di caratteri: consente di inserire un set di caratteri. Il testo può corrispondere a qualsiasi carattere del set. I set includono:

  [0-9A-Za-z]

  [0-9]

  [A-Z]

  [a-z]

  [aeiou]

  [\n\f\r\t] (che rileva la corrispondenza di nuova riga, avanzamento foglio, ritorno a capo o tabulazione)

  Ad esempio, se si specifica [0-9A-Za-z], questo snippet rileverà la corrispondenza di qualsiasi carattere compreso tra A e Z (maiuscoli o minuscoli) o di qualsiasi cifra compresa tra 0 e 9.
- Carattere speciale: consente di inserire un carattere che richiede un carattere di escape, inclusi \, ?, *, +, |, ., [, (o ^. Il carattere di escape è la barra rovesciata (\), immessa automaticamente quando si seleziona questa opzione.
- Carattere spazio: i caratteri spazio includono \n (nuova riga), \f (avanzamento foglio, \r (ritorno a capo) o \t (tabulazione).
- Numero ottale a tre cifre: rileva la corrispondenza di un carattere ASCII come ottale (fino a tre cifre). Ad esempio, il carattere \040 rappresenta uno spazio. La barra rovesciata (\) viene immessa automaticamente.
- Numero esadecimale a due cifre: rileva la corrispondenza di un carattere ASCII utilizzando un carattere esadecimale (esattamente due cifre). La barra rovesciata (\) viene immessa automaticamente.
- Carattere specificato: consente di immettere qualsiasi carattere.

Anteprima snippet

Solo visualizzazione. Mostra lo snippet come verrà immesso nell'espressione regolare.

- Aggiungi snippet: consente di aggiungere lo snippet alla fine dell'espressione regolare.
- Aggiungi snippet come alternativa: Consente di aggiungere lo snippet alla fine dell'espressione regolare separato dal carattere (|), rilevando così la corrispondenza di entrambe le espressioni che separa. Ad esempio, **cane|gatto** consente di rilevare la corrispondenza di cane o di gatto.
- Inserisci snippet presso il cursore: consente di inserire lo snippet presso il cursore.

Espressione regolare

Questa area include il testo dell'espressione regolare che può essere sia immesso manualmente sia generato con gli snippet. È quindi possibile selezionare il testo nel campo Espressione regolare ed applicare un quantificatore alla selezione.

- Ricorrenze di selezione: selezionare il testo nel campo Espressione regolare, fare clic su una delle opzioni seguenti, quindi scegliere **Applica a selezione**. Ad esempio, se l'espressione regolare è "test me" e si applica l'opzione **Una o più volte**, l'espressione regolare cambia in "test (me)+".
  - Zero o una volte (?): un quantificatore che indica che l'espressione che lo precede deve essere presente 0 o 1 volta. Ad esempio, per **ca?ne** viene rilevata la corrispondenza di cne o di cane.
  - Una o più volte (+): un quantificatore che indica che l'espressione che lo precede è presente almeno una volta. Ad esempio, per **ca+ne** viene rilevata la corrispondenza di caane e di cane, ma non di cne.
  - Una o più volte (+): un quantificatore che indica che l'espressione che lo precede è presente almeno una volta. Ad esempio, per **ca+ne** viene rilevata la corrispondenza di caane e di cane, ma non di cne.
  - Qualsiasi numero di volte (*): un quantificatore che indica che l'espressione che lo precede è presente 0, 1 o qualsiasi numero di volte. Ad esempio, per **ca*ne** vengono rilevati cne, cane, caane e così via.
  - Almeno: ripetizione di almeno *x* volte. Ad esempio, per **ab(xy){2,}z** viene rilevata la corrispondenza di abxyxyz, abxyxyxyz, e così via.
  - Esattamente: ripeti esattamente *x* volte. Ad esempio, per **ab(xy){3}z** viene rilevata la corrispondenza di abxyxyxyz.
- Applica a selezione: consente di applicare il quantificatore alla selezione.

Metacaratteri dell'espressione regolare

Nell'elenco che segue vengono riportati i metacaratteri che presentano un significato speciale.

Carattere	Descrizione	Note
.	Punto	Consente di rilevare la corrispondenza di qualunque singolo carattere. Ad esempio, per **c.s** viene rilevata la corrispondenza di cis, css, cas e di qualunque parola che contenga tali caratteri, ad esempio caspita.
(*espressione*)	Espressione secondaria	L'espressione secondaria permette di separare i caratteri dai caratteri che li precedono e li seguono, in modo da poter utilizzare altri metacaratteri nella sottoespressione. Ad esempio, **t(u|r)e** consente di rilevare la corrispondenza di tue e di tre, ma **tu|re** consente di rilevare la corrispondenza di tu e di re. È anche possibile utilizzare una sottoespressione con quantificatori di ripetizione per differenziare i caratteri della ripetizione. Ad esempio, per **ab(xy){3}z** viene rilevata la corrispondenza di abxyxyxyz.
|	Alternativa	Consente di rilevare le due espressioni che separa. Ad esempio, **cane|gatto** consente di rilevare la corrispondenza di cane o di gatto.
?	Punto interrogativo	Quantificatore che indica che l'espressione che lo precede deve essere presente 0 o 1 volta. Ad esempio, per **ca?ne** viene rilevata la corrispondenza di cne o di cane. **Nota** È necessario immettere la combinazione **Ctrl+V** prima del punto interrogativo, altrimenti viene attivata la Guida.
*	Asterisco	Quantificatore che indica che l'espressione che lo precede deve essere presente zero, una o qualsiasi numero di volte. Ad esempio, per **ca*ne** vengono rilevati cne, cane, caane e così via.

Carattere	Descrizione	Note
+	Segno più	Quantificatore che indica che l'espressione che lo precede deve essere presente almeno una volta. Ad esempio, per **ca+ne** viene rilevata la corrispondenza di caane e di cane, ma non di cne.
{*x*}	Quantificatore di ripetizione	Esattamente: ripeti esattamente *x* volte. Ad esempio, per **ab(xy){3}z** viene rilevata la corrispondenza di abxyxyxyz.
{*x*,}	Quantificatore di ripetizioni minime	Ripeti almeno *x* volte. Ad esempio, per **ab(xy){2,}z** viene rilevata la corrispondenza di abxyxyz, abxyxyxyz, e così via.
[*abc*]	Classe di caratteri	Viene rilevata la corrispondenza di qualunque carattere tra parentesi. Ad esempio, per **[abc]** viene rilevata la corrispondenza di a, b o c.
[^*abc*]	Classe di caratteri negata	Consente di rilevare la corrispondenza di un singolo carattere che non è contenuto tra parentesi. Ad esempio, per **[^abc]** viene rilevata la corrispondenza di qualsiasi carattere diverso da a, b o c. Per **[^A-Z]** viene rilevata la corrispondenza di qualsiasi singolo carattere che non sia maiuscolo.
[*a-c*]	Classe di intervallo di caratteri	Viene rilevata la corrispondenza di qualunque carattere compreso nell'intervallo. Per **[a-z]** viene rilevata la corrispondenza di qualunque lettera minuscola. È possibile mescolare caratteri e intervalli: per **[abcq-z]** viene rilevata la corrispondenza di a, b, c, q, r, s, t, u, v, w, x, y, z, lo stesso per [**a-cq-z**]. Il trattino (-) si considera carattere letterale solo se è il primo o l'ultimo tra parentesi come nel caso **[abc-]** o **[-abc]**.
""	Virgolette	Consente di mantenere gli spazi che precedono o seguono la stringa. Ad esempio, in **" test"** viene mantenuto lo spazio prima della parole nella ricerca di corrispondenza.
^	Accento circonflesso	Specifica l'inizio della riga.

Carattere	Descrizione	Note
****	Carattere di escape	Quando utilizzato come metacarattere, consente di rilevare la corrispondenza di un carattere letterale. Ad esempio, per **\ [** viene rilevata la corrispondenza della parentesi quadra aperta.
carattere	Carattere	Quando il carattere non è un metacarattere, consente di rilevare la corrispondenza di un carattere letterale.
\r	Ritorno a capo	Consente di rilevare la corrispondenza di un ritorno a capo 0x0d.
\n	Nuova riga	Consente di rilevare la corrispondenza di un ritorno a capo 0x0a.
\t	Tabulazione	Consente di rilevare la corrispondenza di una tabulazione 0x09.
\f	Avanzamento foglio	Consente di rilevare la corrispondenza di un avanzamento foglio 0x0c.
\x*NN*	Numero esadecimale di escape	Consente di rilevare la corrispondenza di un carattere ASCII utilizzando un carattere esadecimale (esattamente due cifre).
NNN	Numero ottale di escape	Consente di rilevare la corrispondenza di un carattere ASCII come ottale (esattamente a tre cifre). Ad esempio, il carattere 040 rappresenta uno spazio.

CAPITOLO 35

URL Filtering

URL Filtering consente di controllare l'accesso ai siti Internet, permettendo o negando l'accesso a specifici siti Web in base alle informazioni contenute in un elenco di URL. È possibile impostare un elenco di URL locale sul router e utilizzare gli elenchi di filtri URL memorizzati sui server Websense o Secure Computing. URL Filtering viene abilitato durante la configurazione di un criterio di Protezione applicazioni.

Anche se sul router non è stato configurato nessun criterio di Protezione applicazioni, è comunque possibile gestire un elenco di URL locali e un elenco di server di URL Filtering quando viene creato un criterio che lo attiva.

In questo capitolo sono contenute le seguenti sezioni:

Per maggiori informazioni su URL Filtering, andare al seguente collegamento:

Firewall Websense URL Filtering (URL Filtering per il firewall Websense)

Per informazioni sull'utilizzo dei criteri di URL Filtering, fare clic su Precedenza di URL Filtering.

Finestra URL Filtering

In questa finestra sono visualizzate le impostazioni globali per URL Filtering sul router. L'elenco URL locale e l'elenco dei server di URL Filtering vengono gestiti nelle schermate Attività aggiuntive o nelle finestre Protezione applicazioni. Le impostazioni globali per URL Filtering possono essere gestite solo dalla finestra Attività aggiuntive. Per modificare questi valori, utilizzare il pulsante **Modifica impostazioni globali**.

Per una descrizione di ogni singola impostazione visualizzata in questa finestra, fare clic su Modifica impostazioni globali.

Per una descrizione delle funzioni per URL Filtering fornite da Cisco SDM, consultare le informazioni introduttive in URL Filtering.

Modifica impostazioni globali

Modificare le impostazioni globali per URL Filtering in questa finestra.

Nota È necessario che per il router sia stata attivata la registrazione in modo che possa segnalare gli avvisi dei filtri URL, i messaggi di registrazione controllo e i messaggi di sistema relativi al server di URL Filtering.

Modalità Consenti

Selezionare questa casella per permettere al router di passare alla modalità Consenti quando il router non è in grado di collegarsi a nessuno dei server di URL Filtering indicati nell'elenco dei server. Quando il router è nella modalità Consenti, viene consentito il passaggio di tutte le richieste HTTP se il router non è in grado di collegarsi a nessuno dei server indicati nell'elenco di server di URL Filtering. Per impostazione predefinita, la modalità Consenti è disattivata.

Avviso filtro URL

Selezionare questa casella per consentire al router di registrare i messaggi di avviso di URL Filtering. Nei messaggi di avviso di URL Filtering vengono segnalati alcuni eventi, ad esempio quando un server di URL Filtering è inattivo o quando una richiesta HTTP contenente un URL risulta troppo lunga per una richiesta di ricerca. Questa opzione è disattivata per impostazione predefinita.

Registrazione controllo

Selezionare questa casella per permettere al router di gestire una registrazione di controllo nel registro. Il router registrerà i messaggi di stato sulle richieste URL che indicano se una richiesta HTTP è stata permessa o negata e altri messaggi di registrazione controllo. Questa opzione è disattivata per impostazione predefinita.

Registro server URL Filtering

Selezionare questa casella per consentire al router di registrare nel registro i messaggi di sistema relativi al server di URL Filtering. Questa opzione è disattivata per impostazione predefinita.

Dimensione della cache

È possibile impostare le dimensioni massime della cache in cui vengono memorizzati gli indirizzi IP richiesti più di recente e il relativo stato di autorizzazione. La dimensione predefinita della cache è 5000 byte. L'intervallo è compreso tra 0 e 2147483647 byte. La cache viene cancellata ogni 12 ore.

N. massimo di richieste HTTP nel buffer

Consente di impostare il numero massimo di richieste HTTP in sospeso che il router è in grado di memorizzare nel buffer. Per impostazione predefinita, il router memorizza nel buffer fino a 1000 richieste. È possibile specificare da 1 a 2147483647 richieste.

N. massimo di risposte HTTP nel buffer

È possibile impostare il numero di risposte HTTP provenienti dai server di URL Filtering che il router è in grado di memorizzare nel buffer. Una volta raggiunto questo numero, il router scarta le ulteriori risposte. Il valore predefinito è 200. Sono ammessi valori da 0 a 20000.

Impostazioni generali di URL Filtering

Assegnare un nome al filtro URL, specificare il comportamento del router in caso di corrispondenza e configurare i parametri di dimensione del file di registro e della cache. È inoltre possibile specificare un'interfaccia di origine se non si desidera che la mappa di parametri di filtraggio URL venga applicata a tutte le interfacce del router.

Nome URL Filtering

Immettere il nome che rappresenterà il metodo di configurazione o di utilizzo del filtro URL. Se ad esempio viene specificata FastEthernet 1 come interfaccia di origine, è possibile impostare il nome `fa1-parmap`. Se un filtro utilizza un server di URL Filtering Websense all'indirizzo IP 192.128.54.23, è possibile specificare `websense23-parmap` come nome.

Modalità Consenti

Selezionare questa casella per permettere al router di passare alla modalità Consenti quando il router non è in grado di collegarsi a nessuno dei server di URL Filtering indicati nell'elenco dei server. Quando il router è nella modalità Consenti, viene consentito il passaggio di tutte le richieste HTTP se il router non è in grado di collegarsi a nessuno dei server indicati nell'elenco di server di URL Filtering. Per impostazione predefinita, la modalità Consenti è disattivata.

Avviso filtro URL

Selezionare questa casella per consentire al router di registrare i messaggi di avviso di URL Filtering. Nei messaggi di avviso di URL Filtering vengono segnalati alcuni eventi, ad esempio quando un server di URL Filtering è inattivo o quando una richiesta HTTP contenente un URL risulta troppo lunga per una richiesta di ricerca. Questa opzione è disattivata per impostazione predefinita.

Registrazione controllo

Selezionare questa casella per permettere al router di gestire una registrazione di controllo nel registro. Il router registrerà i messaggi di stato sulle richieste URL che indicano se una richiesta HTTP è stata permessa o negata e altri messaggi di registrazione controllo. Questa opzione è disattivata per impostazione predefinita.

Registro server URL Filtering

Selezionare questa casella per consentire al router di registrare nel registro i messaggi di sistema relativi al server di URL Filtering. Questa opzione è disattivata per impostazione predefinita.

Dimensione della cache

È possibile impostare le dimensioni massime della cache in cui vengono memorizzati gli indirizzi IP richiesti più di recente e il relativo stato di autorizzazione. La dimensione predefinita della cache è 5000 byte. L'intervallo è compreso tra 0 e 2147483647 byte. La cache viene cancellata ogni 12 ore.

N. massimo di richieste HTTP nel buffer

Consente di impostare il numero massimo di richieste HTTP in sospeso che il router è in grado di memorizzare nel buffer. Per impostazione predefinita, il router memorizza nel buffer fino a 1000 richieste. È possibile specificare da 1 a 2147483647 richieste.

N. massimo di risposte HTTP nel buffer

È possibile impostare il numero di risposte HTTP provenienti dai server di URL Filtering che il router è in grado di memorizzare nel buffer. Una volta raggiunto questo numero, il router scarta le ulteriori risposte. Il valore predefinito è 200. Sono ammessi valori da 0 a 20000.

Funzioni

La finestra Avanzate consente di scegliere l'interfaccia di origine. Scegliere l'interfaccia dall'elenco Interfaccia di origine.

Elenco URL locali

Se l'immagine Cisco IOS presente sul router supporta l'URL Filtering ma non sopporta lo ZPF (Zone-based Policy Firewall), è possibile mantenere un elenco di URL locali sul router. Questo elenco viene usato da tutti i criteri di Protezione applicazioni in cui è abilitato URL Filtering. Le immagini Cisco IOS dalla versione 12.4(9)T in poi supportano le funzionalità ZPF supportate da SDM. Nella configurazione ZPF, è possibile creare un elenco di URL locali per ciascuna mappa di parametri di URL Filtering.

Tramite Cisco SDM è possibile creare voci di elenco e importare tali voci da un elenco memorizzato sul PC. Quando un elenco di URL locali viene utilizzato in combinazione con i server di URL Filtering, le voci locali vengono utilizzate per prime. Per maggiori informazioni vedere la sezione Precedenza di URL Filtering.

Gestione dell'elenco degli URL locali

È possibile usare Cisco SDM per gestire un elenco di URL locali, con la possibilità di aggiungere ed eliminare le voci una per una, importare un elenco di URL dal PC e specificare le azioni che Cisco SDM dovrà eseguire con ciascuna voce. Utilizzare i pulsanti **Aggiungi** ed **Elimina** per gestire voci specifiche nell'elenco del router e fare clic sul pulsante **Importa elenco URL** per importare un elenco URL dal PC.

Nota Se una voce viene eliminata dall'elenco locale e il router è configurato per utilizzare i server di URL Filtering, le voci che corrispondono a quelle eliminate dall'elenco locale potrebbero tuttora esistere su tali server.

Per eliminare dal router tutte le voci, utilizzare il pulsante **Elimina tutto**. Se sul router non è configurato alcun elenco locale, il router deve affidarsi ai server di URL Filtering. Per recuperare in un secondo momento l'elenco URL eliminato in precedenza, utilizzare il pulsante **Esporta elenco URL** per salvare l'elenco URL sul PC prima di eliminare tutte le voci. Quando si salva un elenco URL sul PC, all'elenco viene attribuita all'estensione.CSV.

Importazione di elenchi di URL dal PC

Per importare un elenco di URL dal PC al router, fare clic sul pulsante **Importa elenco URL**. L'elenco URL selezionato deve avere l'estensione.txt o.CSV. Dopo avere selezionato l'elenco sul PC, in Cisco SDM viene visualizzata una finestra di dialogo che permette di specificare le azioni da eseguire con ciascuna voce dell'elenco. Per maggiori informazioni vedere la sezione Importa elenco URL.

Aggiunta o modifica di URL locali

In questa finestra è possibile modificare una voce URL dell'elenco di URL locali sul router. Specificare il nome completo o parziale di un dominio e scegliere se usare l'opzione **Consenti** o **Nega** per le richieste di questo URL.

Se si inserisce un nome completo di dominio, ad esempio www.dominio.com, tutte le richieste che includono questo nome di dominio, come www.dominio.com/notizie o www.dominio.com/indice verranno consentite o negate in base all'impostazione scelta in questa finestra di dialogo. Le richieste non verranno inviate ai server di URL Filtering configurati per essere utilizzati dal router.

Se si inserisce un nome parziale di dominio, ad esempio.dominio.com, tutte le richieste che terminano con questa stringa, come www.dominio.com/prodotti o wwwin.dominio.com/italiano, verranno consentite o negate in base all'impostazione scelta in questa finestra di dialogo. Le richieste non verranno inviate ai server di URL Filtering configurati per essere utilizzati dal router.

Importa elenco URL

In questa finestra di dialogo è possibile esaminare l'elenco URL che si sta importando dal PC al router e specificare le azioni da intraprendere con ciascuna voce. Se una voce URL visualizzata in questa finestra di dialogo non è già presente nel router, è possibile aggiungerla all'elenco sul router facendo clic su **Aggiungi**. Se una voce URL è già presente nel router ma si desidera sostituirla con la voce visualizzata nella finestra di dialogo, fare clic su **Sostituisci**.

Tutte le caselle nella colonna **Importa** sono selezionate per impostazione predefinita. Se vi sono voci che non si intende inviare al router, deselezionare le caselle accanto a tali voci. Per rimuovere i segni di spunta da tutte le caselle, fare clic su **Deseleziona tutti**. Facendo clic su **Seleziona tutti**, i segni di spunta verranno inseriti in tutte le caselle.

L'opzione **Aggiungi** aggiunge all'elenco degli URL tutte le voci selezionate non ancora presenti nell'elenco. Se si cerca di aggiungere una voce già presente nell'elenco URL, questa non verrà aggiunta anche se l'azione specificata per il dominio nella voce è diversa dall'azione già presente nell'elenco.

Utilizzare il pulsante **Sostituisci** per specificare un'altra azione per la voce già inclusa nell'elenco URL del router. Se la voce selezionata non è già inclusa nell'elenco del router, il comando **Sostituisci** non ha effetto.

Server di URL Filtering

Il router può inviare richieste HTTP ai server di URL Filtering in grado di memorizzare elenchi URL di maggiori dimensioni rispetto al router. Se il router è configurato con un elenco di server di URL Filtering, il router invia le richieste che non corrispondono alle voci dell'elenco locale ai server di URL Filtering a cui è collegato e consente o nega la richiesta in base alla risposta ricevuta dal server. Quando il server a cui è collegato è inattivo, il router contatta il server successivo nell'elenco fino a stabilire una connessione.

Gli elenchi sui server di URL Filtering possono essere usati insieme agli elenchi di URL locali. Per informazioni su come il router utilizza entrambe le risorse, fare clic su Precedenza di URL Filtering.

Fare clic su **Aggiungi** e scegliere **Secure Computing** o **Websense** per specificare il tipo di server da aggiungere.

Nota Il software Cisco IOS può usare solo un tipo di server di URL Filtering e non consente di aggiungere un server all'elenco se è di tipo diverso. Se, ad esempio, sul router è configurato un elenco di server di URL Filtering che contiene server Websense, verrà generato un messaggio di errore se si cerca di aggiungere un server Secure Computing all'elenco. Se attualmente l'elenco di server di URL Filtering contiene un tipo di server che si desidera modificare con l'altro tipo, è necessario eliminare tutte le voci server nell'elenco prima di aggiungere una voce del nuovo tipo.

In questa finestra è visualizzata la configurazione di ciascun server di URL Filtering presente nell'elenco. Per una descrizione di tutti i valori di configurazione, vedere Aggiungi o Modifica un server di URL Filtering.

Aggiungi o Modifica un server di URL Filtering

Specificare le informazioni sul server di URL Filtering Websense o Secure Computing.

Indirizzo IP/Nome host

Immettere l'indirizzo IP o il nome host del server. Se viene immesso un nome host, il router deve avere una connessione a un server DNS al fine di risolvere il nome host in un indirizzo IP.

Direzione

Se il server di URL Filtering fa parte della rete interna, scegliere **Interna**. Generalmente si tratta di una delle reti a cui sono collegate le interfacce LAN del router. Se il router si trova su una rete esterna, scegliere **Esterna**. Generalmente si tratta di una delle reti a cui sono collegate le interfacce WAN del router. Il valore predefinito è **Interna**.

Numero di porta

Contiene automaticamente il numero della porta predefinita per il tipo di server di URL Filtering che si sta aggiungendo. Se si aggiunge un server Websense, il valore predefinito è 15868, mentre se si aggiunge un server Secure Computing il valore predefinito è 4005. Cambiare questo numero e sostituirlo con il numero della porta a cui fa riferimento il server se tale numero risulta diverso da quello predefinito. Il campo accetta valori compresi tra 1 e 65535.

Numero ritrasmissioni

Campo facoltativo. Specificare il numero di volte in cui il router dovrà cercare di ritrasmettere la richiesta se non perviene alcuna risposta dal server. Il valore predefinito è 2 volte. Il campo accetta valori compresi tra 1 e 10.

Timeout ritrasmissione

Campo facoltativo. Specificare il numero di secondi in cui il router dovrà attendere una risposta dal server prima di ritrasmettere la richiesta. Il valore predefinito è 5 secondi.

Precedenza di URL Filtering

È necessario attivare URL Filtering in **Configura > Firewall e ACL > Protezione applicazioni > URL Filtering**, quindi fare clic su **Attiva URL Filtering**. Questa operazione può essere eseguita solo se sul router è stato configurato un criterio di protezione applicazioni.

Quando URL Filtering è attivato, il router determina come gestire una richiesta HTTP nel modo seguente:

- Se l'URL nella richiesta corrisponde a una voce presente sul router nell'elenco URL locali, il router consente o nega la richiesta in base a questa voce.
- Se l'URL nella richiesta non corrisponde a nessuna voce presente nell'elenco di URL locali, il router passa la richiesta HTTP al server di URL Filtering a cui è collegato. Consente o nega la richiesta a seconda delle informazioni restituite dal server.
- Se la modalità Consenti è disattivata e il router non è in grado di stabilire una connessione con un server di URL Filtering, il router negherà la richiesta. Per impostazione predefinita, la modalità Consenti è disattivata.
- Se la modalità Consenti è attivata e il router non è in grado di stabilire una connessione con un server di URL Filtering, il router consentirà la richiesta. La modalità Consenti viene abilitata nella finestra di dialogo Modifica impostazioni globali.

Sul router è possibile configurare solo un elenco URL e un elenco di server di URL Filtering. Tutti i criteri di Protezione applicazioni configurati utilizzano i medesimi elenco URL ed elenco di server di URL Filtering. Questi elenchi vengono gestiti nelle finestre Protezione applicazioni o tramite **Attività aggiuntive > URL Filtering**. Se vengono eliminati tutti i criteri di Protezione applicazioni, è comunque possibile gestire l'elenco URL e l'elenco dei server di URL Filtering nelle finestre Protezione applicazioni. Tuttavia, il router non esegue URL Filtering se questo non è attivato in un criterio di Protezione applicazioni.

CAPITOLO 36

Gestione della configurazione

Cisco SDM consente di modificare il file di configurazione del router e di ripristinare le impostazioni predefinite della configurazione del router. Poiché la modifica diretta del file di configurazione e il ripristino delle impostazioni predefinite del router possono comportare l'interruzione della connessione tra il computer e il router, leggere le sezioni relative a tutte le schermate in questa area di Cisco SDM della Guida in linea.

Modifica manuale del file di configurazione

Cisco SDM consente di modificare il file di configurazione del router mediante un editor di configurazione che può essere utilizzato per importare un file di configurazione oppure per immettere direttamente i comandi CLI Cisco IOS.

Cisco SDM supporta le parole chiavi e i comandi Cisco IOS più diffusi, tuttavia non è in grado di supportare tutti i comandi CLI. Per coloro che hanno familiarità con l'interfaccia a riga di comando di Cisco IOS e posseggono un'ottima conoscenza degli effetti che hanno i comandi di configurazione immessi sul funzionamento del router e della rete in cui è installato, l'utilizzo dell'editor di configurazione può risultare più immediato rispetto alle finestre di dialogo Cisco SDM. Se si desidera aggiungere una configurazione non supportata da Cisco SDM, è necessario utilizzare l'Editor configurazione oppure aprire mediante il router una sessione Telnet e utilizzare l'interfaccia CLI Cisco IOS.

L'utilizzo dell'Editor configurazione consente di evitare l'esecuzione della convalida Cisco SDM. Sebbene Cisco SDM restituisca i messaggi di errore IOS, non è in grado di confrontare le modifiche apportate alla configurazione con la configurazione in esecuzione, né di comunicare gli eventuali conflitti.
Ad esempio, se si utilizzano le finestre di dialogo Cisco SDM per immettere una configurazione VPN su un router già dotato di una configurazione di firewall, in Cisco SDM viene esaminato il firewall e stabilito quali istruzioni di tipo consenti devono essere aggiunte per attivare il passaggio del traffico VPN, inoltre è in grado di eseguire tale operazione automaticamente. Tuttavia, se si utilizza l'Editor configurazione, è necessario determinare i conflitti che possono verificarsi analizzando la configurazione esistente e apportare le modifiche aggiuntive necessarie per la risoluzione di tali conflitti. Inoltre, è necessario monitorare il funzionamento del router per verificare se il traffico viene gestito come richiesto.

Anche se non richiesto, si consiglia di consentire il backup della configurazione in esecuzione in Cisco SDM. Ogni volta che Cisco SDM esegue il backup, utilizza lo stesso nome di file e di conseguenza sovrascrive i file di backup precedenti.

Editor configurazione

L'Editor configurazione consente di visualizzare la configurazione in esecuzione e di apportarvi modifiche cambiando comandi specifici o sostituendo l'intero file di configurazione con un file importato dal proprio PC. Quando si effettuano le modifiche è possibile visualizzare la configurazione in esecuzione, in alternativa si può utilizzare l'intera finestra per visualizzare la configurazione che viene inviata al router.

Configurazione corrente

Per impostazione predefinita, questa casella consente di visualizzare la configurazione in esecuzione del router. È possibile nasconderla facendo clic su **Nascondi** nell'angolo superiore destro della finestra. Per visualizzare di nuovo la casella fare clic su **Mostra**.

Modifica configurazione

Questa casella consente di apportare modifiche. Per impostazione predefinita, la casella è vuota. È possibile immettere dati sulla configurazione in esecuzione del router, facendo clic su **Importa > configurazione in esecuzione**. È possibile immettere il file di configurazione nel PC, facendo clic su **Importa > configurazione da PC**. Aumentare le dimensioni della casella nascondendo la casella Configurazione corrente.

Unione alla configurazione in esecuzione

Se si desidera unire le modifiche effettuate nella casella Modifica configurazione alla configurazione in esecuzione sul router, fare clic su **Unisci a configurazione in esecuzione**. Le modifiche vengono inviate al router e diventano effettive non appena il router le riceve.

Sostituzione della configurazione in esecuzione

Se si desidera sostituire la configurazione in esecuzione con il contenuto della casella Modifica configurazione, fare clic su **Sostituisci configurazione in esecuzione**. Non utilizzare questo pulsante se prima nella casella Modifica configurazione non è stata inserita e modificata una configurazione importata dal router oppure una configurazione importata dal proprio PC.

Ripristina

Se, prima di utilizzare l'Editor configurazione, è stata salvata la configurazione in esecuzione, è possibile ripristinarla sul router facendo clic su questo pulsante. La configurazione ripristinata viene copiata sulla configurazione di avvio del router e quest'ultimo viene caricato di nuovo. Se non esiste alcuna copia di backup della configurazione del router, Cisco SDM visualizza un messaggio in cui viene indicato che non è possibile ripristinare la configurazione.

Ripristina impostazioni predefinite

È possibile ripristinare la configurazione del router secondo le impostazioni di fabbrica e salvare la configurazione corrente su un file da utilizzare in seguito. Se l'indirizzo IP della rete LAN del router è stato modificato rispetto al valore predefinito 10.10.10.1, si perderà la connessione tra il router e il computer poiché questo indirizzo IP ritornerà a 10.10.10.1 dopo il ripristino.

Nota

- La funzione Ripristina impostazioni predefinite non è supportata dai router Cisco 3620, 3640, 3640A e 7000.
- La funzione Ripristina impostazioni predefinite non è supportata quando è in esecuzione una copia di Cisco SDM installata sul computer.

Prima di iniziare, è necessario sapere come assegnare al computer un indirizzo IP statico nella subnet 10.10.10.0 in modo da riconnettersi al router dopo averlo ripristinato. La configurazione di fabbrica non include la configurazione del server DHCP del router e il router non fornirà alcun indirizzo IP al computer. Inoltre, la configurazione di fabbrica limita l'accesso HTTP o HTTPS al router, circoscrivendolo all'interfaccia LAN. è ammesso solo l'accesso proveniente dalla subnet interna definita su tale interfaccia. Una volta ottenuto l'accesso al router, è possibile modificare l'indirizzo IP predefinito del router e impostarlo in modo tale da consentire l'accesso remoto.

Come assegnare un indirizzo IP dinamico o statico al computer dopo il ripristino

Se si desidera utilizzare Cisco SDM dopo il ripristino, assegnare al computer un indirizzo IP statico o dinamico in base al tipo di router disponibile. Utilizzare la tabella riportata di seguito per determinare il tipo di indirizzo da assegnare al computer.

Router che richiedono indirizzi dinamici	Router che richiedono indirizzi statici
SB10x Cisco 83x, 85x, e 87x Cisco 1701, 1710 e 171x Cisco 180x e 181x	Cisco 1721, 1751, e 1760 Cisco 1841 Cisco 2600XM, e 2691 Cisco 28xx, 36xx, 37xx, e 38xx

Il processo per assegnare al computer un indirizzo IP statico o dinamico varia a seconda della versione di Microsoft Windows presente sul computer.

Nota Non riconfigurare il computer fino al ripristino del router.

Microsoft Windows NT

Dal pannello di controllo fare doppio clic sull'icona **Rete** per visualizzare la finestra Rete. Fare clic su **Protocolli**, selezionare la prima voce Protocollo TCP/IP e fare clic su **Proprietà**. Nella finestra Proprietà, selezionare l'adattatore Ethernet utilizzato per questa connessione. Fare clic su **Ottieni automaticamente un indirizzo IP** per ottenere un indirizzo IP dinamico. Per un indirizzo IP statico, fare clic su **Specificare un indirizzo IP**. Immettere l'indirizzo IP 10.10.10.2 o qualsiasi altro indirizzo nella subnet 10.10.10.0 maggiore di 10.10.10.1. Immettere la subnet 255.255.255.248. Fare clic su **OK**.

Microsoft Windows 98 e Microsoft Windows ME

Dal pannello di controllo fare doppio clic sull'icona **Rete** per visualizzare la finestra Rete. Fare doppio clic sulla voce Protocollo TCP/IP con l'adattatore Ethernet utilizzato per questa connessione per visualizzare **Proprietà** TCP/IP. Nella scheda indirizzo IP, fare clic su **Ottieni automaticamente un indirizzo IP** per ottenere un indirizzo IP dinamico. Per un indirizzo IP statico, fare clic su **Specificare un indirizzo IP**. Immettere l'indirizzo IP 10.10.10.2 o qualsiasi altro indirizzo nella subnet 10.10.10.0 maggiore di 10.10.10.1. Immettere la subnet 255.255.255.248. Fare clic su **OK**.

Microsoft Windows 2000

Dal Pannello di controllo, selezionare **Connessioni di rete e remote/Connessioni locali**. Selezionare l'adattatore Ethernet nel campo Connetti tramite. Selezionare Protocollo Internet e fare clic su Proprietà. Fare clic su **Ottieni automaticamente un indirizzo IP** per ottenere un indirizzo IP dinamico. Per un indirizzo IP statico, fare clic su **Specificare un indirizzo IP**. Immettere l'indirizzo IP 10.10.10.2 o qualsiasi altro indirizzo nella subnet 10.10.10.0 maggiore di 10.10.10.1. Immettere la subnet 255.255.255.248. Fare clic su **OK**.

Microsoft Windows XP

Fare clic su **Start**, selezionare **Impostazioni**, **Connessioni di rete** e quindi la connessione LAN da utilizzare. Fare clic su **Proprietà**, selezionare **Protocol Internet TCP/IP**, quindi fare clic sul pulsante **Proprietà**. Fare clic su **Ottieni automaticamente un indirizzo IP** per ottenere un indirizzo IP dinamico. Per un indirizzo IP statico, fare clic su **Specificare un indirizzo IP**. Immettere l'indirizzo IP 10.10.10.2 o qualsiasi altro indirizzo nella subnet 10.10.10.0 maggiore di 10.10.10.1. Immettere la subnet 255.255.255.248. Fare clic su **OK**.

Per ripristinare le impostazioni predefinite del router

Passo 1 Uscire da **Salva configurazione corrente sul computer** selezionato nella **Fase 1** della schermata**,** quindi specificare un nome per la configurazione del file. Cisco SDM specifica un percorso e un nome predefinito. Se lo si desidera, è possibile non modificare il nome.

Passo 2 Rivedere le informazioni nella casella Comprendere come eseguire nuovamente una connessione nella **Fase 2** della schermata in modo da stabilire una connessione al router dopo il ripristino. Se necessario, rivedere le informazioni in **Come assegnare un indirizzo IP dinamico o statico al computer dopo il ripristino.**

Passo 3 Fare clic su **Reimposta router**.

Passo 4 Fare clic su **Sì** per confermare il ripristino.

Passo 5 Seguire la procedura nella casella Comprendere come eseguire nuovamente una connessione nella **Fase 2** per la riconnessione.

Il ripristino del router alla configurazione predefinita riporta l'indirizzo IP dell'interfaccia interna del router a 10.10.10.1. La successiva volta che si accede al router tramite il browser, immettere l'indirizzo IP 10.10.10.1 nel campo posizione del browser.

Funzionalità non supportata

Questa finestra viene visualizzata se una funzionalità Cisco SDM non è supportata. Tale situazione può verificarsi nel caso in cui sul router sia in esecuzione un'immagine Cisco IOS che non supporta la funzionalità oppure Cisco SDM venga eseguito su un computer e non sia in grado di supportare la funzionalità.

CAPITOLO 37

Ulteriori informazioni...

Nelle seguenti sezioni vengono fornite ulteriori informazioni sugli argomenti descritti nella Guida in linea di Cisco SDM.

Indirizzi IP e subnet mask

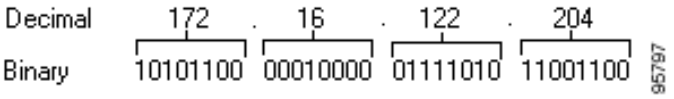
Di seguito vengono fornite informazioni sugli indirizzi IP e le subnet mask e viene indicato come utilizzare tali informazioni una volta immessi gli indirizzi e le maschere in Cisco SDM.

Spazio degli indirizzi IP versione 4 che corrisponde a 32 bit o a 4 byte. e viene utilizzato per definire i seguenti valori:

- Numero di rete
- Numero di subnet opzionale
- Numero host

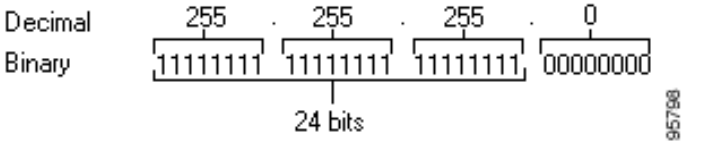
Nota Cisco SDM non supporta IP versione 6.

In Cisco SDM è necessario immettere gli indirizzi IP in formato decimale separato da punti. Questo formato rende gli indirizzi più semplici da leggere e da modificare mediante il raggruppamento di 32 bit in 4 ottetti che vengono visualizzati in formato decimale e separati da punti, ad esempio 172.16.122.204. L'indirizzo in formato decimale 172.16.122.204 rappresenta l'indirizzo IP binario mostrato nella figura riportata di seguito.



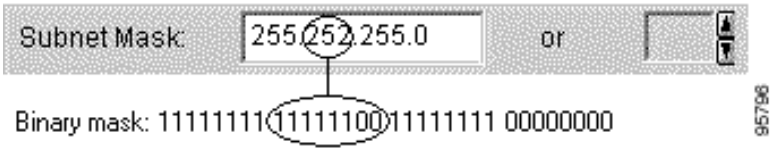
La subnet mask viene utilizzata per specificare la quantità dei 32 bit utilizzata per il numero di rete e di subnet, nel caso in cui quest'ultima sia presente. Si tratta di una maschera binaria con un bit per ciascuna posizione, utilizzata dai numeri di rete e di subnet e, come l'indirizzo IP, è caratterizzata da un valore a 32 bit, espresso in formato decimale. L'immagine seguente mostra una subnet mask immessa in Cisco SDM. Cisco SDM mostra la subnet mask e il numero equivalente di bit nella maschera.

Questi valori immessi da Cisco SDM rappresentano la maschera binaria mostrata nella figura seguente:



Nella subnet mask viene specificato che i primi 24 bit dell'indirizzo IP rappresentano il numero di rete e la subnet mask, mentre gli ultimi 8 bit rappresentano il numero host all'interno della rete e della subnet. È possibile immettere la maschera nel formato decimale separato da punti mostrato nel campo Subnet Mask oppure selezionare il numero di bit nel campo corrispondente. Una volta immesso o selezionato un valore in un campo, Cisco SDM regola automaticamente l'altro valore.

In Cisco SDM verrà visualizzato un messaggio di avviso nel caso in cui venga immessa una maschera decimale in zeri binari (0) nell'area di rete/subnet della maschera. Il campo relativo alla subnet mask riportato di seguito contiene un valore decimale in zeri binari (0) nella parte di numero di rete/subnet della maschera. Il campo dei bit a destra è vuoto per indicare che è stato immesso un valore non valido nel campo Subnet Mask.



Quando nelle finestre di Cisco SDM viene visualizzato un indirizzo di rete, l'indirizzo IP e la subnet mask relativi possono essere visualizzati nel formato indirizzo di rete/bit di subnet, come mostrato nell'esempio seguente:

```
172.28.33.0/24
```

L'indirizzo di rete nell'esempio è 172.28.33.0. Il numero 24 indica il numero di bit di subnet utilizzati ed è possibile considerarlo come un riferimento immediato alla subnet mask corrispondente di 255.255.255.0.

Gli indirizzi utilizzati nella rete Internet pubblica devono essere completamente univoci per il periodo di tempo in cui vengono utilizzati, mentre nelle reti private possono essere univoci solo per la rete o la subnet privata.

Gli indirizzi possono inoltre essere convertiti mediante l'utilizzo di schemi quali NAT e PAT, e possono essere temporaneamente assegnati mediante DHCP. È possibile utilizzare Cisco SDM per configurare i protocolli NAT, PAT e DHCP.

Campi Host e Rete

In questa sezione viene descritto come fornire informazioni sull'host o sulla rete nelle finestre che consentono di specificare un indirizzo host o di rete oppure un nome host.

Specificare la rete o l'host.

Tipo

La scelta può essere effettuata tra una delle opzioni riportate di seguito.

- **Una rete**: mediante la selezione di questa opzione, viene fornito un indirizzo di rete nel campo dell'indirizzo IP. La maschera carattere jolly consente di immettere un numero di rete corrispondente a più subnet.
- **Un nome host o indirizzo IP**: mediante la selezione di questa opzione, viene fornito un indirizzo IP host o un nome host nel campo successivo.
- **Qualsiasi indirizzo IP**: l'azione specificata viene applicata a qualsiasi host o rete.

Indirizzo IP/Maschera carattere jolly

Immettere un indirizzo di rete, quindi la maschera carattere jolly per specificare la parte dell'indirizzo di rete che deve corrispondere esattamente.

Ad esempio, se sono stati immessi un indirizzo di rete di 10.25.29.0 e una maschera carattere jolly di 0.0.0.255, verrà filtrato qualsiasi applet Java con un indirizzo di origine contenente 10.25.29. Se la maschera carattere jolly fosse 0.0.255.255, verrebbe filtrato qualsiasi applet Java con un indirizzo di origine contenente 10.25.

IP/Nome host

Questo campo viene visualizzato se è stata selezionata l'opzione **Un nome host o indirizzo IP** come Tipo. Se viene immesso un nome host, assicurarsi che nella rete si trovi un server DNS in grado di risolvere il nome host in un indirizzo IP.

Configurazioni delle interfacce disponibili

I tipi di configurazioni disponibili per ciascun tipo di interfaccia sono illustrati nella tabella riportata di seguito.

Se si è selezionato	È possibile aggiungere
Interfaccia Ethernet	• Connessione PPPoE • Interfaccia tunnel • Interfaccia loopback
Una delle seguenti interfacce: • Interfaccia Ethernet con una connessione PPPoE • Interfaccia dialer associata a una configurazione ADSL o G.SHDSL • Interfaccia seriale con configurazione PPP o HDLC • Interfaccia secondaria seriale con una configurazione Frame Relay • Interfaccia WAN non supportata	• Interfaccia tunnel • Interfaccia loopback

Interfaccia ATM senza incapsulamento	• Interfaccia ADSL • Interfaccia G.SHDSL • Tunnel o loopback per una delle interfacce sopra riportate
Interfaccia seriale	• Connessione Frame Relay • Connessione PPP • Interfaccia tunnel • Interfaccia loopback
Interfaccia secondaria ATM Interfaccia secondaria Ethernet Interfaccia dialer non associata a un'interfaccia ATM Loopback Tunnel	• Interfaccia tunnel • Interfaccia loopback

Pool di indirizzi DHCP

Gli indirizzi IP assegnati dal server DHCP vengono ottenuti da un pool comune configurato mediante l'indicazione dell'indirizzo IP iniziale e dell'indirizzo finale nell'intervallo.

L'intervallo di indirizzi specificato deve essere compreso tra i seguenti intervalli di indirizzi privati:

- Da 10.1.1.1 a 10.255.255.255
- Da 172.16.1.1 a 172.31.255.255

È inoltre necessario che l'intervallo di indirizzi specificato si trovi nella stessa subnet dell'indirizzo IP dell'interfaccia LAN. Nell'intervallo possono essere contenuti fino a 254 indirizzi. Nei seguenti esempi vengono riportati gli intervalli validi:

- Da 10.1.1.1 a 10.1.1.254 (considerando che l'indirizzo IP LAN si trova nella subnet 10.1.1.0)
- Da 172.16.1.1 a 172.16.1.254 (considerando che l'indirizzo IP LAN si trova nella subnet 172.16.1.0)

Il router viene configurato da Cisco SDM in modo da escludere automaticamente l'indirizzo IP dell'interfaccia LAN nel pool.

Indirizzi riservati

È necessario non utilizzare i seguenti indirizzi nell'intervallo degli indirizzi specificati:

- Indirizzo IP di rete/subnet
- Indirizzo broadcast nella rete

Significato delle parole chiave Consenti e Nega

È possibile utilizzare le voci delle regole nelle regole di accesso, NAT, IPSec e nelle regole di accesso associate alle route map. Il significato delle parole chiave Consenti e Nega varia in base al tipo di regola in cui vengono utilizzate.

Tipo di regola	Significato di Consenti	Significato di Nega
Regola di accesso	Consente l'ingresso o l'uscita del traffico corrispondente dall'interfaccia a cui è stata applicata la regola.	Consente l'eliminazione del traffico corrispondente.
Regola NAT	Consente di convertire l'indirizzo IP del traffico corrispondente nell'indirizzo locale interno o locale esterno specificato.	Non consente di convertire l'indirizzo.
regola IPSec (solo estesa)	Consente di crittografare il traffico con l'indirizzo corrispondente.	Non consente di crittografare il traffico, inviandolo quindi non crittografato.
Regola di accesso utilizzata nella route map	Consente di proteggere gli indirizzi corrispondenti dalla conversione NAT.	Non consente di proteggere gli indirizzi corrispondenti dalla conversione NAT.

Servizi e porte

In questa sezione vengono elencati i servizi che è possibile specificare nelle regole e i numeri di porta corrispondenti, con una breve descrizione per ciascun servizio.

La sezione è suddivisa nelle seguenti aree:

Servizi TCP

Servizio TCP	Numero di porta	Descrizione
bgp	179	Border Gateway Protocol. Il protocollo BGP consente lo scambio delle informazioni di accessibilità con altri sistemi che utilizzano il protocollo BGP.
chargen	19	Character Generator
cmd	514	Comandi remoti. Simili al comando exec con la differenza che cmd è dotato di un'autenticazione automatica.
daytime	13	Daytime
discard	9	Discard
domain	53	DNS (Domain Name Service). Sistema utilizzato nella rete Internet per la conversione dei nomi relativi ai nodi di rete negli indirizzi.
echo	7	Richiesta echo. Messaggio inviato una volta eseguito il comando ping.
exec	512	Esecuzione del processo remoto.
finger	79	Finger. Applicazione che consente di determinare se una persona possiede un account in un sito Internet particolare.
ftp	21	File Transfer Protocol. Protocollo di livello applicazione utilizzato per il trasferimento dei file tra i nodi di rete.

Servizio TCP	Numero di porta	Descrizione
ftp-data	20	Connessioni dati FTP.
gopher	70	Gopher. Sistema di accesso a documenti distribuiti.
hostname	101	Server di nomi host NIC (Network Information Center).
ident	113	Protocollo ident
irc	194	Internet Relay Chat. Protocollo a livello globale che consente agli utenti di scambiarsi messaggi di testo in tempo reale.
klogin	543	Accesso Kerberos. Kerberos rappresenta uno standard di sviluppo per l'autenticazione degli utenti di rete.
kshell	544	Shell Kerberos
login	513	Accesso
lpd	515	Line Printer Daemon. Protocollo utilizzato per l'invio di processi di stampa tra sistemi UNIX.
nntp	119	NNTP (Network News Transport Protocol)
pim-auto-rp	496	Protocol-Independent Multicast Auto-RP. PIM rappresenta un'architettura di routing multicast che consente l'aggiunta di routing IP multicast su reti IP esistenti.
pop2	109	Post Office Protocol versione 2. Protocollo utilizzato dalle applicazioni di posta elettronica del client per il recupero della posta dai server di posta.
pop3	110	Post Office Protocol versione 3.
smtp	25	Simple Mail Transport Protocol. Protocollo Internet per la fornitura di servizi di posta elettronica.
sunrpc	111	SUN Remote Procedure Call. Vedere rpc.
syslog	514	Registro eventi di sistema.

Servizi UDP

Servizio UDP	Numero di porta	Descrizione
biff	512	Servizio utilizzato dal sistema di posta per informare gli utenti sulla ricezione di nuovi messaggi di posta.
bootpc	69	Client BOOTP (Bootstrap Protocol).
bootps	67	Server BOOTP (Bootstrap Protocol).
discard	9	Discard
dnsix	195	Controllo del protocollo di protezione DNSIX.
domain	53	DNS (Domain Name Service).
echo	7	Vedere echo.
isakmp	500	Internet Security Association and Key Management Protocol.
mobile-ip	434	Registrazione IP mobile.
nameserver	42	Servizio nome IEN116 (obsoleto).
netbios-dgm	138	Servizio di datagrammi NetBios. NetBios (Network Basic Input Output System). Interfaccia API utilizzata da applicazioni per la richiesta di servizi da processi di rete di livello inferiore.
netbios-ns	137	Servizio di nomi NetBios.
netbios-ss	139	Servizio di sessioni NetBios.
ntp	123	Acronimo di Network Time Protocol. Protocollo TCP che assicura una sincronizzazione dell'ora locale precisa con riferimento agli orologi atomici e a stazioni radio che si trovano nella rete Internet.
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense-mode.
rip	520	Acronimo di Routing Information Protocol. Protocollo utilizzato per scambiare informazioni di route tra i router.
snmp	161	Acronimo di Simple Network Management Protocol. Protocollo utilizzato per monitorare e controllare i dispositivi di rete.
snmptrap	162	Trap SNMP. Notifica di gestione del sistema di alcuni eventi che si sono verificati nel sistema gestito in remoto.
sunrpc	111	SUN Remote Procedure Call. Le RPC rappresentano chiamate di procedura create o specificate dai client ed eseguite nei server, con i risultati restituiti al client attraverso la rete.

Servizio UDP	Numero di porta	Descrizione
syslog	514	Servizio di registro eventi di sistema.
tacacs	49	Terminal Access Controller Access Control System. Protocollo di autenticazione in grado di fornire l'autenticazione di accesso remoto e i servizi correlati, quali la registrazione.
talk	517	Talk. Protocollo inizialmente realizzato per la comunicazione tra terminali TTY, ora porta rendezvous da cui è possibile effettuare una connessione TCP.
tftp	69	Trivial File Transfer Protocol. Versione semplificata del protocollo FTP che consente il trasferimento dei file tra i nodi della rete.
time	37	Ora
who	513	Porta per database che consente di mostrare gli utenti che hanno effettuato l'accesso ai computer in una rete locale insieme alla media del carico del computer.
xdmcp	177	X-Display Manager Client Protocol. Protocollo utilizzato per le comunicazioni tra X-Display (client) e X Display Manager.
non500-isakmp	4500	Internet Security Association and Key Management Protocol. Parola chiave utilizzata quando è richiesta una porta NAT Traversal non permanente.

Tipi di messaggi ICMP

Messaggi ICMP	Numero di porta	Descrizione
alternate-address	6	Indirizzo host alternativo.
conversion-error	31	Inviato per segnalare un errore di conversione di datagrammi.
echo	8	Tipo di messaggio inviato una volta eseguito il comando ping.
echo-reply	0	Risposta a un messaggio (ping) di tipo echo-request.
information-reply	16	Obsoleto. Risposta a un messaggio inviato da un host per rilevare il numero della rete nella quale si trova. Sostituito da DHCP.
information-request	15	Obsoleto. Messaggio inviato da un host per rilevare il numero della rete nella quale si trova. Sostituito da DHCP.

Messaggi ICMP	Numero di porta	Descrizione
mask-reply	18	Risposta a un messaggio inviato da un host per rilevare la maschera della rete nella quale si trova.
mask-request	17	Obsoleto. Messaggio inviato da un host per rilevare la maschera della rete nella quale si trova.
mobile-redirect	32	Reindirizzamento host mobile. Inviato per informare un host mobile dell'esistenza di un nodo first-hop migliore nel percorso verso una destinazione.
parameter-problem	12	Messaggio generato in risposta a un pacchetto con problemi nell'intestazione corrispondente.
redirect	5	Inviato per informare un host dell'esistenza di un nodo first-hop migliore nel percorso verso una destinazione.
router-advertisement	9	Inviato periodicamente o in risposta a una richiesta di router.
router-solicitation	10	Messaggi inviati per richiedere ai router di generare rapidamente messaggi di notifica di router.
source-quench	4	Inviato quando lo spazio disponibile di buffer non è sufficiente per mettere in coda i pacchetti per la trasmissione a un hop successivo oppure inviato dal router di destinazione quando i pacchetti giungono troppo rapidamente per essere elaborati.
time-exceeded	11	Inviato per indicare che il campo relativo alla durata (TTL) del pacchetto ricevuto ha raggiunto lo zero.
timestamp-reply	14	Risposta alla richiesta di timestamp da utilizzare per la sincronizzazione tra due dispositivi.
timestamp-request	13	Richiesta di timestamp da utilizzare per la sincronizzazione tra due dispositivi.
traceroute	30	Messaggio inviato in risposta a un host dal quale è stata emessa una richiesta del comando traceroute.
unreachable	3	Destinazione non raggiungibile. Impossibile inviare il pacchetto per motivi che non riguardano la congestione.

Servizi IP

Servizi IP	Numero di porta	Descrizione
aahp	51	
eigrp	88	Acronimo di Extended Interior Gateway Routing Protocol. Versione avanzata del protocollo IGRP sviluppata da Cisco.
esp	50	Extended Services Processor.
icmp	1	Acronimo di Internet Control Message Protocol. Protocollo a livello di rete in grado di segnalare errori e di fornire altre informazioni relative all'elaborazione di pacchetti IP.
igmp	2	Acronimo di Internet Group Management Protocol. Protocollo utilizzato dagli host IP per segnalare le appartenenze di gruppo multicast corrispondenti ai router multicast adiacenti.
ip	0	Acronimo di Internet Protocol (protocollo Internet). Protocollo a livello di rete in grado di offrire un servizio di rete non orientato alla connessione.
ipinip	4	Incapsulamento IP-in-IP.
nos	94	Network operating system. Protocollo di sistema di file distribuito.
ospf	89	Acronimo di Open Shortest Path First. Algoritmo di routing gerarchico di tipo link-state.
pcp	108	Payload Compression Protocol.
pim	103	Protocol-Independent Multicast. PIM rappresenta un'architettura di routing multicast che consente l'aggiunta di routing IP multicast su reti IP esistenti.
tcp	6	Transmission Control Protocol. Protocollo di livello trasporto orientato alla connessione che consente una trasmissione di dati full-duplex trusted.
udp	17	User Datagram Protocol. Protocollo di livello trasporto non orientato alla connessione nello stack del protocollo TCP/IP.

Servizi che è possibile specificare nelle Inspection Rule

Protocollo	Descrizione
cuseeme	Protocollo per videoconferenze.
fragment	Consente di specificare che la verifica dei frammenti viene eseguita dalla regola.
ftp	Vedere ftp.
h323	Vedere H.323.
http	Vedere HTTP.
icmp	Vedere icmp.
netshow	NetShow. Protocollo per streaming video.
rcmd	Remote Command. Protocollo utilizzato quando i comandi vengono eseguiti in un sistema remoto da un sistema locale.
realaudio	RealAudio. Protocollo per streaming audio.
rpc	Remote Procedure Call. Le RPC rappresentano chiamate di procedura create o specificate dai client ed eseguite nei server, con i risultati restituiti al client attraverso la rete.
rtsp	Real-Time Streaming Protocol. Protocollo a livello di applicazione utilizzato per controllare l'invio di dati con proprietà in tempo reale.
sip	Acronimo di Session Initiation Protocol. Sip rappresenta un protocollo per la telefonia utilizzato per integrare i servizi di telefonia e di dati.
skinny	Protocollo per la telefonia che consente ai client della telefonia di essere conformi con H.323.
smtp	Vedere smtp.
sqlnet	Protocollo per i database abilitati alla rete.
streamworks	Protocollo StreamWorks. Protocollo per streaming video.
tcp	Vedere tcp.
tftp	Vedere tftp.
udp	Vedere udp.
vdolive	Protocollo VDOLive. Protocollo per streaming video.

Ulteriori informazioni sul protocollo NAT

In questa sezione vengono fornite informazioni sugli scenari che consentono il completamento delle finestre Regole NAT e altre informazioni in cui viene illustrato per quale motivo non è possibile modificare le regole NAT create mediante l'interfaccia CLI in Cisco SDM.

Scenari di conversione degli indirizzi statici

Negli scenari riportati di seguito viene mostrato come utilizzare le regole di conversione indirizzi statici.

Scenario 1

È necessario eseguire la mappatura di un indirizzo IP per un singolo host in un indirizzo pubblico. L'indirizzo dell'host è 10.12.12.3, quello pubblico è 172.17.4.8.

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Aggiungi regola di conversione indirizzi.

	Campi Converti da interfaccia		Campi Converti in interfaccia	
Statico/Dinamico	**Indirizzo IP**	**Net Mask**	**Indirizzo IP**	**Porta di reindirizzamento**
Statico	10.12.12.3	Lasciare vuoto	172.17.4.8	Lasciare non selezionato

Risultato

L'indirizzo di origine 10.12.12.3 viene convertito nell'indirizzo 172.17.4.8 nei pacchetti in uscita dal router. Se questa rappresenta la sola regola NAT nella rete, 10.12.12.3 sarà il solo indirizzo nella rete ad essere convertito.

Scenario 2

È necessario eseguire la mappatura di ciascun indirizzo IP in una rete in un indirizzo IP pubblico univoco e non creare una regola distinta per ciascuna mappatura. Il numero di rete di origine è 10.l2.12.0 e la rete di destinazione è 172.17.4.0. Tuttavia, in questo scenario, non è necessario conoscere i numeri di rete di origine o di destinazione. È sufficiente immettere gli indirizzi host e una maschera di rete.

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Aggiungi regola di conversione indirizzi.

	Campi Converti da interfaccia		Campi Converti in interfaccia	
Statico/Dinamico	**Indirizzo IP**	**Net Mask**	**Indirizzo IP**	**Porta di reindirizzamento**
Statico	10.12.12.35 (host)	255.255.255.0	172.17.4.8 (host)	Lasciare non selezionato

Risultato

Il protocollo NAT ricava l'indirizzo di rete del campo “Converti da” dall'indirizzo IP host e dalla subnet mask. Il protocollo NAT ricava l'indirizzo di rete del campo “Converti a” dalla net mask immessa nei campi “Converti da” e dall'indirizzo IP del campo “Converti a”. L'indirizzo IP di origine in qualsiasi pacchetto in uscita dalla rete originale viene convertito in un indirizzo nella rete 172.17.4.0.

Scenario 3

Si desidera utilizzare lo stesso indirizzo IP globale per diversi host nella rete trusted. Il traffico in ingresso sarà dotato di un numero di porta diverso basato sull'host di destinazione.

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Aggiungi regola di conversione indirizzi.

	Campi Converti da...		Campi Converti a...	
Statico/Dinamico	**Indirizzo IP**	**Net Mask**	**Indirizzo IP**	**Porta di reindirizzamento**
Statico	10.12.12.3	Lasciare vuoto	172.17.4.8	UDP Porta originale 137 Porta convertita 139

Risultato

L'indirizzo di origine 10.12.12.3 viene convertito nell'indirizzo 172.17.4.8 nei pacchetti in uscita dal router. Il numero di porta nel campo Porta di reindirizzamento viene cambiato da 137 a 139. Il traffico di ritorno dotato dell'indirizzo di destinazione 172.17.4.8 viene indirizzato al numero di porta 137 dell'host con l'indirizzo IP 10.12.12.3.

È necessario creare una voce distinta per ciascuna mappatura di host/porta che si desidera creare. È possibile utilizzare lo stesso indirizzo IP del campo "Converti a" in ciascuna voce, tuttavia è necessario immettere un indirizzo IP del campo "Converti da" diverso in ciascuna voce e un insieme di numeri di porta diverso.

Scenario 4

Si desidera che gli indirizzi di origine nel campo "Converti da" utilizzino l'indirizzo IP assegnato all'interfaccia Fast Ethernet 0/1 172.17.4.8 del router. Si desidera inoltre utilizzare lo stesso indirizzo IP globale per più host su una rete trusted. Il traffico in ingresso sarà dotato di un numero di porta diverso basato sull'host di destinazione. Nella tabella riportata di seguito viene illustrato l'utilizzo dei campi nella finestra Aggiungi regola di conversione indirizzi.

	Campi Converti da...		Campi Converti a...	
Statico/Dinamico	**Indirizzo IP**	**Net Mask**	**Indirizzo IP**	**Porta di reindirizzamento**
Statico	10.12.12.3	Lasciare vuoto	FastEthernet 0/1	UDP Porta originale 137 Porta convertita 139

Risultato

L'indirizzo di origine 10.12.12.3 viene convertito nell'indirizzo 172.17.4.8 nei pacchetti in uscita dal router. Il numero di porta nel campo Porta di reindirizzamento viene cambiato da 137 a 139. Il traffico di ritorno dotato dell'indirizzo di destinazione 172.17.4.8 e porta 139 viene indirizzato al numero di porta 137 dell'host con l'indirizzo IP 10.12.12.3.

Scenari di conversione degli indirizzi dinamici

Negli scenari riportati di seguito viene mostrato come utilizzare le regole di conversione indirizzi dinamici. Tali scenari sono validi sia nel caso in cui si selezioni una connessione dall'interno all'esterno o dall'esterno all'interno.

Scenario 1

Si desidera che gli indirizzi di origine nel campo “Converti da” utilizzino l'indirizzo IP assegnato all'interfaccia Fast Ethernet 0/1 172.17.4.8 del router. La modalità PAT (PAT) viene utilizzata per distinguere il traffico associato a host diversi. La regola ACL utilizzata per definire gli indirizzi “Converti da” viene configurata come mostrato di seguito:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

Quando è utilizzata in una regola NAT, tale regola di accesso consente a qualsiasi host nella rete 10.10.10.0 di ricevere la conversione dell'indirizzo, ad eccezione dell'host con l'indirizzo 10.10.10.1.

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Aggiungi regola di conversione indirizzi.

	Campi Converti da...	Campi Converti a...		
Statico/Dinamico	Regola ACL	Tipo	Interfaccia	Pool di indirizzi
Dinamico	7	Interfaccia	FastEthernet0/1	Disattivato

Risultato

L'indirizzo IP di origine del traffico proveniente da tutti gli host presenti nella rete 10.10.10.0 viene convertito in 172.17.4.8. La modalità PAT viene utilizzata per distinguere il traffico associato a host diversi.

Scenario 2

Si desidera che gli indirizzi host specificati in access-list 7 nello scenario precedente utilizzino gli indirizzi di un pool definito dall'utente. Se gli indirizzi nel pool vengono esauriti, si desidera che il router utilizzi la modalità PAT per soddisfare richieste aggiuntive per gli indirizzi del pool.

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Pool di indirizzi per questo scenario.

Nome pool	PAT (Port Address Translation)	Campi Indirizzo IP		Maschera di rete
Pool 1	Selezionato	172.16.131.2	172.16.131.10	255.255.255.0

Nella tabella riportata di seguito viene illustrato come vengono utilizzati i campi nella finestra Aggiungi regola di conversione indirizzi per questo scenario.

	Campi Converti da...	Campi Converti a...		
Statico/Dinamico	Regola ACL	Tipo	Interfaccia	Pool di indirizzi
Dinamico	7	Pool di indirizzi	Disattivato	Pool 1

Risultato

Gli indirizzi IP degli host nella rete 10.10.10.0 vengono convertiti in indirizzo IP nell'intervallo compreso tra 172.16.131.2 e 172.16.131.10. Se le richieste per la conversione degli indirizzi superano gli indirizzi disponibili in Pool 1, verrà utilizzato lo stesso indirizzo per soddisfare le richieste successive e la modalità PAT verrà utilizzata per distinguere gli host che utilizzano l'indirizzo.

Motivi per i quali Cisco SDM non è in grado di modificare una regola NAT

Una regola NAT precedentemente configurata sarà di sola lettura e non sarà configurabile quando una regola NAT statica viene configurata con una delle seguenti procedure:

- I comandi Cisco IOS **inside source static** e **destination**
- Il comando **inside source static network** con una delle parole chiavi “extendable”, “no-alias” o “no-payload”
- Il comando **outside source static network** con una delle parole chiavi “extendable”, “no-alias” o “no-payload”
- Il comando **inside source static tcp** con una delle parole chiavi “no-alias” o “no-payload”
- Il comando **inside source static udp** con una delle parole chiavi “no-alias” o “no-payload”
- Il comando **outside source static tcp** con una delle parole chiavi “no-alias” o “no-payload”
- Il comando **outside source static udp** con una delle parole chiavi “no-alias” o “no-payload”
- Il comando **inside source static** con una delle parole chiave “no-alias”, “no-payload”, “extendable”, “redundancy”, “route-map” o “vrf”
- Il comando **outside source static** con una delle parole chiave “no-alias”, “no-payload”, “extendable”o “add-route”
- Il comando **inside source static** con la parola chiave “esp”
- Il comando **inside source static** con il comando **interface**

Una regola dinamica NAT è configurata con l'interfaccia Loopback.

Ulteriori informazioni sul protocollo VPN

In queste sezioni vengono fornite ulteriori informazioni su VPN, DMVPN, IPSec e IKE.

Risorse sul sito Web Cisco.com

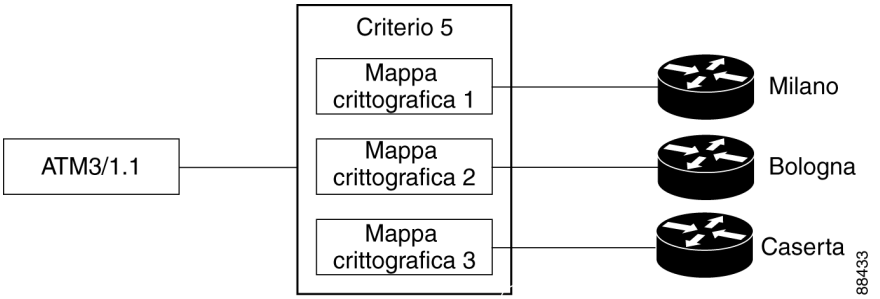
I seguenti collegamenti forniscono risorse del centro TAC di Cisco e altre informazioni sulle problematiche legate alla connessione VPN.

- How Virtual Private Networks Work
- Dynamic Multipoint IPSec VPNs
- TAC-authored articles on IPSec
- TAC-authored articles on Cisco SDM
- Security and VPN Devices
- IPSecurity Troubleshooting–Understanding and Using Debug Commands
- Field Notices

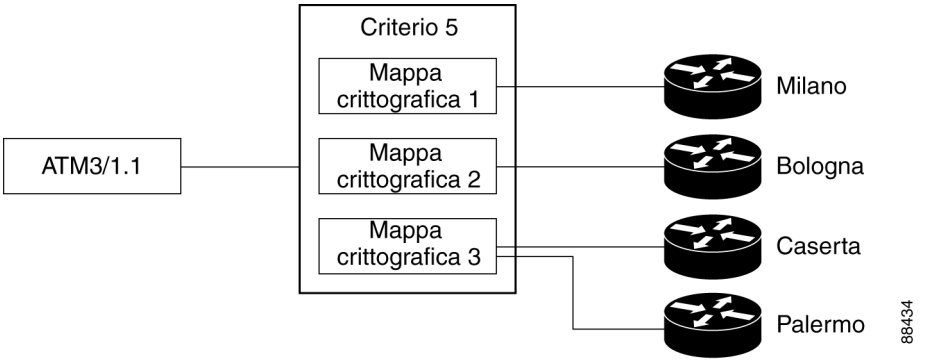
Ulteriori informazioni sulle connessioni VPN e i criteri IPSec

Una connessione VPN è un'associazione tra un'interfaccia di router e un criterio IPSec. L'elemento base di un criterio IPSec è rappresentato dalla mappa crittografica, che consente di specificare le seguenti voci: un set di trasformazione e altri parametri per controllare la crittografia, l'identità di uno o più peer e una regola IPSec che consente di specificare il traffico che verrà crittografato. È possibile che un criterio IPSec contenga più mappe crittografiche.

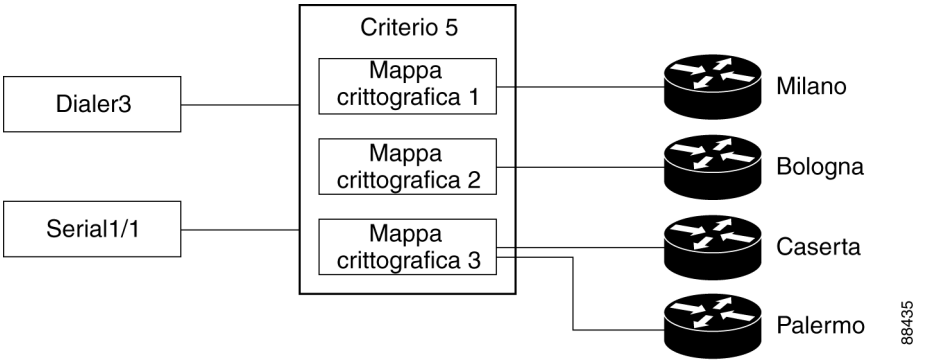
Nel diagramma seguente viene illustrata un'interfaccia (ATM 3/1.1) associata a un criterio IPSec, dotato di tre mappe crittografiche, ognuna delle quali indica un sistema peer diverso. L'interfaccia ATM 3/1 è pertanto associata a tre connessioni VPN.



Una mappa crittografica è in grado di specificare più di un peer per una connessione, in modo da garantire ridondanza. Nel diagramma seguente vengono mostrati la stessa interfaccia e lo stesso criterio, tuttavia dalla mappa crittografica CM-3 vengono indicati due peer: Topeka e Lawrence.



Un'interfaccia di router può essere associata solo a un criterio IPSec. Tuttavia, un criterio IPSec può essere associato a più interfacce di router e una mappa crittografica è in grado di specificare più peer per una connessione. Nel diagramma seguente vengono illustrate due interfacce di router associate a un criterio e una mappa crittografica da cui vengono indicati due peer.



In questa configurazione sono disponibili sei connessioni VPN, in quanto sia Dialer 3 che Serial 1/1 dispongono di connessioni verso Seattle, Chicago, Topeka e Lawrence. In Cisco SDM i collegamenti a Topeka e Lawrence vengono mostrati come una sola connessione per entrambe le interfacce.

Ulteriori informazioni sul protocollo IKE

Il protocollo IKE consente di gestire le seguenti attività:

- Autenticazione
- Negoziazione di sessioni
- Scambio della chiave
- Configurazione e negoziazione del tunnel IPSec

Autenticazione

L'autenticazione è probabilmente l'attività più importante svolta dal protocollo IKE e con ogni certezza la più complicata. Ogni volta che viene eseguita una negoziazione, è fondamentale conoscere con chi si sta effettuando una negoziazione. Il protocollo IKE è in grado di utilizzare diversi metodi per autenticare reciprocamente le parti coinvolte nella negoziazione.

- **Chiave precondivisa**: IKE utilizza una tecnica di hashing per assicurare che solo un utente in possesso della stessa chiave può aver inviato i pacchetti IKE.
- **Firme digitali RSA o DSS**: IKE utilizza la crittografia della firma digitale della chiave pubblica per verificare l'identità di ciascuna parte.
- **Crittografia RSA**: IKE utilizza uno dei due metodi per crittografare gran parte della negoziazione in modo da garantire che solo un'entità con la chiave privata corretta possa procedere con l'operazione.

Nota Cisco SDM supporta il metodo di autenticazione della chiave precondivisa.

Negoziazione di sessioni

Durante la negoziazione di sessioni, il protocollo IKE consente alle entità di negoziare il modo con cui eseguire l'autenticazione e con cui proteggere negoziazioni successive, ad esempio la negoziazione del tunnel IPSec. Vengono negoziati i seguenti elementi:

- **Metodo di autenticazione**: uno dei metodi di autenticazione sopra elencati.
- **Algoritmo dello scambio di chiave**: tecnica matematica per uno scambio protetto delle chiavi crittografiche su un supporto pubblico, ad esempio Diffie-Hellman. Le chiavi vengono utilizzate negli algoritmi della crittografia e della firma del pacchetto.
  - **Algoritmo di crittografia**: DES, 3DES o AES
  - **Algoritmo della firma del pacchetto**: MD5 o SHA-1

Scambio della chiave

IKE utilizza il metodo dello scambio della chiave negoziato (vedere la sezione "Negoziazione di sessioni" sopra riportata) per creare bit sufficienti di materiale di definizione delle chiavi crittografato in modo da proteggere le transazioni successive. Tale metodo assicura la protezione di ciascuna sessione IKE mediante un insieme di chiavi nuovo e sicuro.

Autenticazione, negoziazione di sessione e scambio delle chiavi costituiscono la fase 1 di una negoziazione IKE.

Configurazione e negoziazione del tunnel IPSec

Una volta che il protocollo IKE ha completato la negoziazione di un metodo sicuro per lo scambio di informazioni (fase 1), si utilizza tale protocollo per negoziare un tunnel IPSec. Tale operazione viene eseguita nella fase 2. Durante lo scambio, viene creato dal protocollo IKE materiale nuovo di definizione delle chiavi da utilizzare per il tunnel IPSec, mediante le chiavi della fase 1 IKE come base o eseguendo un nuovo scambio di chiavi. Inoltre, vengono negoziati algoritmi di autenticazione e di crittografia per il tunnel.

Ulteriori informazioni sulle IKE Policy

Quando ha inizio la negoziazione IKE, dal protocollo viene ricercata una IKE Policy identica per entrambi i peer. Dal peer, che avvia la negoziazione, verranno inviate tutte le relative policy al peer remoto, il quale a sua volta tenterà di trovare una corrispondenza mediante il confronto della propria policy con priorità elevata e le policy ricevute dell'altro peer. Il peer remoto procede con la verifica delle proprie policy in ordine di priorità (dalla più elevata) fino a quando non viene trovata una corrispondenza.

Si ha una corrispondenza quando entrambe le policy dei due peer possiedono crittografia, hashing, autenticazione e valori dei parametri Diffie-Hellman identici e quando dalla policy del peer remoto viene specificata una durata inferiore o uguale a quella della policy a confronto. Se la durata non è la stessa, verrà utilizzata quella più breve relativa alla policy del peer remoto.

Combinazioni di trasformazioni consentite

Per definire un set di trasformazioni, specificare una delle tre trasformazioni. Ciascuna trasformazione rappresenta un protocollo di protezione IPSec (AH o ESP) oltre all'algoritmo che si desidera utilizzare. Quando un set di trasformazione particolare viene utilizzato durante le negoziazioni per le Security Association IPSec, è necessario che l'intero set di trasformazione, ovvero la combinazione di protocolli, algoritmi e altre impostazioni, corrisponda a un set di trasformazione nel peer remoto.

Nella tabella seguente vengono elencate le selezioni di combinazioni delle trasformazioni consentite per i protocolli AH e ESP.

Trasformazione AH (*Effettuare una sola selezione*)	**Trasformazione crittografica ESP (*Effettuare una sola selezione*)**	**Trasformazione di autenticazione (*Effettuare una sola selezione*)**	**Trasformazione di compressione IP (*Effettuare una sola selezione*)**	**Esempi** *(Consentite fino a 3 trasformazioni)*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	1. ah-md5-hmac 2. esp-3des and esp-md5-hmac 3. ah-sha-hmac, esp-des e esp-sha-hmac

Nella tabella sottostante viene descritta ogni singola trasformazione.

Trasformazione	**Descrizione**
ah-md5-hmac	AH con algoritmo di autenticazione (variante HMAC) MD5.
ah-sha-hmac	AH con algoritmo di autenticazione (variante HMAC) SHA.
esp-des	ESP con algoritmo di crittografia DES a 56 bit.
esp-3des	ESP con algoritmo di crittografia DES a 168 bit (3DES o Triple DES).
esp-null	Algoritmo di crittografia Null.

Trasformazione	Descrizione
esp-seal	ESP con algoritmo di crittografia SEAL (Software Encryption Algorithm) della chiave di crittografia a 160 bit.
esp-md5-hmac	ESP con algoritmo di autenticazione (variante HMAC) MD5.
es-aes-128	ESP con AES (Advanced Encryption Standard). Crittografia con una chiave a 128 bit.
esp-aes-192	ESP con AES. Crittografia con chiave a 192 bit.
esp-aes-256	ESP con AES. Crittografia con chiave a 256 bit.
esp-sha-hmac	ESP con algoritmo di autenticazione (variante HMAC) SHA.
comp-lzs	Compressione IP con algoritmo LZS.

Esempi

Negli esempi seguenti vengono riportate le combinazioni delle trasformazioni consentite:

- ah-md5-hmac
- esp-des
- esp-3des e esp-md5-hmac
- ah-sha-hmac, esp-des e esp-sha-hmac
- comp-lzs

Motivi per i quali la configurazione di un'interfaccia seriale o di un'interfaccia secondaria può essere di sola lettura

Un'interfaccia secondaria o seriale precedentemente configurata sarà di sola lettura e non sarà configurabile nei seguenti casi:

- L'interfaccia è configurata mediante i comandi Cisco IOS **encapsulation ppp** e **ppp multilink ...** .
- L'interfaccia è configurata mediante i comandi **encapsulation hdlc** e **ip address negotiated**.
- L'interfaccia fa parte di SERIAL_CSUDSU_56K WIC.
- L'interfaccia fa parte di Sync/Async WIC configurato mediante il comando **physical-layer async**.
- L'interfaccia è configurata mediante il comando **encapsulation frame-relay** con un indirizzo IP nell'interfaccia principale.
- L'incapsulamento dell'interfaccia non è “hdlc”, “ppp” o “frame-relay”.
- Il comando **encapsulation frame-relay ...** contiene l'opzione **mfr ...** .
- L'interfaccia è configurata mediante il comando **encapsulation ppp**, tuttavia la configurazione PPP dispone di comandi non supportati.
- L'interfaccia è configurata mediante i comandi **encapsulation frame-relay** e **frame-relay map...** .
- L'interfaccia principale è configurata mediante i comandi **encapsulation frame-relay** e **frame-relay interface-dlci...** .
- L'interfaccia principale è configurata mediante il comando **encapsulation frame-relay** e l'interfaccia secondaria è configurata mediante il comando **frame-relay priority-dlci-group...** .
- L'interfaccia secondaria è configurata con il comando **interface-dlci ...** che contiene le parole chiave “ppp”, “protocol” o “switched”.
- Il tipo di interfaccia secondaria è “multipoint” invece di “point-to-point”.
- L'interfaccia secondaria è configurata mediante un incapsulamento diverso da “frame-relay”.

Motivi per i quali la configurazione di un'interfaccia ATM o di un'interfaccia secondaria può essere di sola lettura

Un'interfaccia secondaria o ATM precedentemente configurata sarà di sola lettura e non sarà configurabile nei seguenti casi:

- L'interfaccia dispone di un PVC con il comando **dialer pool-member**.
- L'interfaccia dispone di un PVC in cui il protocollo specificato nel comando **protocol** non è **ip**.
- L'interfaccia dispone di un PVC con più comandi **protocol ip**.
- L'incapsulamento in PVC non corrisponde a “aal5mux” né a “aal5snap”.
- Il protocollo di incapsulamento in aal5mux non è “ip”.
- L'indirizzo IP non è configurato nel PVC nel comando **protocol ip**.
- L'opzione “dial-on-demand” è configurata con il comando **pppoe-client**.
- Più PVC sono configurati nell'interfaccia.
- L'incapsulamento nel dialer associato è vuoto o non è “ppp”.
- Non è configurato alcun indirizzo IP nel dialer associato.
- È necessaria una rete VPDN, determinata dinamicamente dall'immagine di Cisco IOS, ma non è configurata per questa connessione.
- La modalità operativa è “CO” in un'interfaccia SHDSL (solo interfacce principali ATM).
- È configurato un indirizzo IP nell'interfaccia e questa non è configurata per PPPoE (solo interfacce secondarie ATM).
- L'interfaccia dispone di un indirizzo IP, tuttavia non dispone di un PVC associato.
- L'interfaccia dispone di un PVC, tuttavia non dispone di un indirizzo IP associato e non è configurata per PPPoE.
- Il comando **bridge-group** è configurato nell'interfaccia.
- L'interfaccia principale dispone di uno o più PVC e di una o più interfacce secondarie.
- L'interfaccia principale non è configurabile (solo interfacce secondarie ATM).
- Si tratta di un'interfaccia multipoint (solo interfacce secondarie ATM).

Motivi per i quali la configurazione di un'interfaccia Ethernet può essere di sola lettura

Un'interfaccia Ethernet LAN o WAN precedentemente configurata sarà di sola lettura e non sarà configurabile nei seguenti casi:

- L'interfaccia LAN è stata configurata come server DHCP con un indirizzo di supporto IP.

Motivi per i quali la configurazione di un'interfaccia ISDN BRI può essere di sola lettura

Un'interfaccia ISDN BRI precedentemente configurata sarà di sola lettura e non sarà configurabile nei seguenti casi:

- Un indirizzo IP è assegnato a un'interfaccia ISDN BRI.
- Nell'interfaccia ISDN BRI è configurato un incapsulamento diverso da ppp.
- Il comando **dialer-group** o **dialer string** è configurato nell'interfaccia ISDN BRI.
- Il comando **dialer pool-member** <*x*> è configurato nell'interfaccia ISDN BRI, tuttavia l'interfaccia dialer <*x*> corrispondente non è presente.
- Nell'interfaccia ISDN BRI sono configurati più comandi dialer pool-member.
- Il comando **dialer map** è configurato nell'interfaccia ISDN BRI.
- Nell'interfaccia dialer è configurato un incapsulamento diverso da ppp.
- Il comando **dialer-group** o **dialer-pool** non è configurato nell'interfaccia dialer.
- Nell'interfaccia dialer è configurato il comando **dialer-group** <*x*>, tuttavia il comando **dialer -list** <*x*> **protocol** non è configurato.
- Nell'interfaccia dialer è configurato il comando **dialer idle-timeout** <*num*> con la parola chiave opzionale (either/inbound).

- Nell'interfaccia dialer è configurato il comando **dialer string** con la parola chiave opzionale **class**.
- Nel caso in cui si stia utilizzando la connessione ISDN BRI come connessione di backup, una volta completata la configurazione di backup nel sistema Cisco SDM, la connessione verrà visualizzata come di sola lettura, se si verificano le condizioni seguenti:
  - La route predefinita attraverso l'interfaccia primaria è rimossa.
  - La route predefinita dell'interfaccia di backup non è configurata.
  - Il criterio ip local è rimosso.
  - **track /rtr** o **both** non è configurato.
  - Il comando route-map è rimosso.
  - Il comando access-list è rimosso o modificato, ad esempio modifica di tracking ip address.
  - Le interfacce supportate da Cisco SDM sono configurate mediante configurazioni non supportate.
  - Le interfacce primarie non sono supportate da Cisco SDM

Motivi per i quali la configurazione di un'interfaccia per modem analogico può essere di sola lettura

Un'interfaccia per modem analogico precedentemente configurata sarà di sola lettura e non sarà configurabile nei seguenti casi:

- Un indirizzo IP è assegnato all'interfaccia asincrona.
- Nell'interfaccia asincrona è configurato un incapsulamento diverso da ppp.
- Il comando **dialer-group** o **dialer string** è configurato nell'interfaccia asincrona.
- Async mode **interactive** è configurato nell'interfaccia asincrona.
- **dialer pool-member** <*x*> è configurato nell'interfaccia asincrona, tuttavia l'interfaccia dialer <*x*> corrispondente non è presente.
- Nell'interfaccia asincrona sono configurati più comandi dialer pool-member.
- Nell'interfaccia dialer è configurato un incapsulamento diverso da ppp.

- Il comando **dialer-group** o **dialer-pool** non è configurato nell'interfaccia dialer.
- Nell'interfaccia dialer è configurato il comando **dialer-group** <*x*>, tuttavia il comando **dialer -list** <*x*> **protocol** non è configurato.
- Nell'interfaccia dialer è configurato il comando **dialer idle-timeout** <*num*> con la parola chiave opzionale (either/inbound).
- Nella modalità di raccolta delle configurazioni delle linee, **modem inout** non è configurato.
- Nella modalità di raccolta delle configurazioni delle linee, **autoselect ppp** non è configurato.
- Nel caso in cui si stia utilizzando la connessione mediante modem analogico come connessione di backup, una volta completata la configurazione di backup nel sistema Cisco SDM, la connessione verrà visualizzata come di sola lettura, se si verificano le condizioni seguenti:
  - La route predefinita attraverso l'interfaccia primaria è rimossa.
  - La route predefinita dell'interfaccia di backup non è configurata.
  - Il criterio ip local è rimosso.
  - **track /rtr** o **both** non è configurato.
  - Il comando route-map è rimosso.
  - Il comando access-list è rimosso o modificato, ad esempio modifica di tracking ip address.
  - Le interfacce supportate da Cisco SDM sono configurate mediante configurazioni non supportate.
  - Le interfacce primarie non sono supportate da Cisco SDM

Scenario del caso di utilizzo del criterio firewall

Per informazioni sulla gestione dei criteri del firewall, compresi gli scenari dettagliati di distribuzione, consultare il documento disponibile al seguente collegamento:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration_09186a0080230754.pdf

Suggerimenti sulla configurazione di DMVPN

In questa sezione della Guida in linea vengono forniti dei suggerimenti su come procedere durante la configurazione dei router in una rete DMVPN.

Configurazione dell'hub come punto di partenza

Dal momento che per configurare gli spoke occorrono informazioni sull'hub, è necessario configurare dapprima quest'ultimo. Se si sta configurando un hub, è possibile utilizzare la funzione di configurazione dello spoke, disponibile nella finestra Riepilogo, per generare un file di testo contenente una procedura da inviare agli amministratori degli spoke in modo da configurarli con le informazioni relative all'hub corrette. Prima di iniziare a configurare uno spoke, è necessario ottenere le informazioni corrette relative all'hub.

Assegnazione degli indirizzi spoke

È necessario che tutti i router nella rete DMVPN si trovino nella stessa subnet; l'amministratore dell'hub deve pertanto assegnare gli indirizzi nella subnet ai router spoke per evitare conflitti di indirizzo e utilizzare sempre la stessa subnet mask.

Suggerimenti per la configurazione dei protocolli di routing per la rete DMVPN

Di seguito sono riportate alcune istruzioni che è necessario tener presente durante la configurazione dei protocolli di routing per la rete DMVPN. È anche possibile ignorarle, considerando tuttavia che Cisco SDM non è stato verificato in scenari diversi da quelli descritti da queste linee guida e che potrebbe non essere consentito modificare le configurazioni effettuate in Cisco SDM.

Tali suggerimenti sono elencati di seguito in ordine di importanza:

- Nel caso in cui sia presente un processo di routing in grado di notificare le reti interne, utilizzare tale processo per notificare le reti a DMVPN.
- Nel caso in cui sia presente un processo di routing in grado di notificare le reti di tunnel per VPN, ad esempio i tunnel GRE over IPSec, utilizzare tale processo per notificare le reti DMVPN.
- Nel caso in cui sia presente un processo di routing in grado di notificare le reti per le interfacce WAN, assicurarsi di utilizzare un numero di sistema autonomo o ID processo non utilizzati da tali interfacce per notificare le reti.
- Quando si configurano le informazioni di routing di DMVPN, Cisco SDM verifica se il numero di sistema autonomo (EIGRP) o l'ID area (OSPF) immesso è già utilizzato per notificare le reti dell'interfaccia fisica del router. Nel caso in cui il valore sia già in uso, Cisco SDM informa e suggerisce di utilizzare un nuovo valore o di selezionare un protocollo di routing diverso per notificare le reti in DMVPN.

Utilizzo di interfacce con configurazioni di tipo dialup

Se si seleziona un'interfaccia che utilizza una connessione di tipo dialup, è possibile che la connessione resti sempre attiva. Per stabilire se per l'interfaccia fisica selezionata è stata configurata una connessione di tipo dialup, ad esempio una connessione ISDN oppure asincrona, è possibile esaminare le interfacce supportate in Interfacce e connessioni.

Ping dell'hub prima di iniziare la configurazione degli spoke

Prima di configurare un router spoke, è necessario verificare la connettività dell'hub mediante l'esecuzione del comando ping. Se non è possibile effettuare tale operazione, è necessario eseguire la configurazione di una route all'hub.

Documenti di Cisco SDM

Le modalità di utilizzo di Cisco SDM sono descritte in una serie di documenti disponibili al seguente indirizzo:

http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/appnote/index.htm (in inglese)

CAPITOLO 38

Guida introduttiva

Cisco Router and Security Device Manager (Cisco SDM) è uno strumento software basato sul browser Internet di facile utilizzo progettato per configurare LAN, WAN, e funzionalità di protezione su un router. Cisco SDM è progettato per rivenditori e amministratori di rete di piccole e medie aziende con conoscenza delle nozioni di base delle reti LAN e della progettazione di reti di base.

Per una configurazione rapida ed efficiente di reti Ethernet, connettività WAN, firewall e reti VPN (Virtual Private Network), in Cisco SDM è richiesto il processo di configurazione con procedure guidate ovvero schermate in sequenza che analizzano la procedura di configurazione e forniscono un testo esplicativo. È quindi possibile modificare la configurazione di base creata per un maggior controllo sul router e sulla rete. Non è necessario aver utilizzato in precedenza dispositivi Cisco SDM o l'interfaccia della riga di comando (CLI) di Cisco.

Quando si avvia Cisco SDM, viene visualizzata la pagina principale, una finestra con le informazioni sulla panoramica del sistema e della configurazione circa l'hardware e il software del router, utile per determinare gli elementi da configurare. Una volta completata una configurazione, Cisco SDM consente di verificarla e risolvere problemi in modo da garantirne il funzionamento.

In Cisco SDM è inoltre disponibile una modalità di controllo che consente di osservare le prestazioni del router e di raccogliere le statistiche associate alle configurazioni effettuate nel router.

Le novità di questa versione

Questa versione supporta le seguenti nuove funzioni:

- Server Autorità di certificazione (CA): è possibile configurare il router come server Autorità di certificazione (CA) in modo che conceda i certificati agli host presenti nella rete. L'utilizzo di un server CA nella rete facilita la distribuzione della tecnologia VPN consentendo agli host locali di registrare i certificati dal server CA configurato e non da un server CA pubblico.
- Autenticazione 802.1x: è possibile configurare il router in modo che esegua l'autenticazione IEEE 802.1x, consentendo a un client di eseguire l'autenticazione utilizzando l'identità del computer anziché l'indirizzo IP.
- DVTI (Dynamic Virtual Tunnel Interfaces): DVTI consente di configurare una connessione Easy VPN utilizzando un'interfaccia virtuale. I tunnel virtuali dinamici forniscono un'interfaccia di accesso virtuale separata su richiesta per ogni connessione Easy VPN. La configurazione delle interfacce di accesso virtuale viene duplicata da una configurazione di modello virtuale che include la configurazione IPSec e le eventuali funzionalità software di Cisco IOS configurate sull'interfaccia di modello virtuale come QoS, NetFlow o ACL (elenchi di controllo di accesso).
- Firewall con criteri basato sulla zona: utilizza un modello di configurazione basato sulla zona, più flessibile dei firewall basati sulle interfacce. Alle zone vengono assegnate delle interfacce, quindi vengono inserite in coppie di zone per definire le interfacce di origine e destinazione del traffico. È possibile applicare criteri di verifica alle coppie di zone per governare il traffico che va dalle interfacce di origine a quelle di destinazione in una coppia di zone.
- Linguaggio C3PL (Cisco Common-Classification Policy Language):C3PL consente di creare criteri basati sulle classi. Le classi identificano i tipi di traffico, ad esempio il traffico P2P e IM. I criteri associano le classi di traffico e le azioni. Specificano l'azione che il router deve effettuare sul traffico di una classe particolare, ad esempio verificandolo, consentendone il passaggio oppure eliminandolo. Questi criteri possono essere applicati alle coppie di zone.

- Miglioramenti di IPS: i miglioramenti di Cisco IOS IPS disponibili con Cisco IOS versione 12.4(11)T sono supportati. È supportato un nuovo formato di file di definizione delle firme (SDF), come pure altre funzionalità quale il Processore azioni evento firma (SEAP, Signature Event Action Processor). Questo consente un maggiore controllo sul filtraggio, consentendo di creare i Filtri azioni evento firma (SEAF, Signature Event Action Filter) e assegnando le Sostituzioni azioni evento firma (SEAO, Signature Event Action Override).
- Miglioramenti QoS: QoS è stato migliorato per consentire di specificare i contrassegni di traffico DSCP o NBAR e di creare i criteri QoS utilizzando il linguaggio C3PL.

Per maggiori informazioni su questa versione vedere:

http://www.cisco.com/go/sdm

Fare clic sul collegamento General Information (in inglese) e quindi su Release Notes (in inglese).

Versioni di Cisco IOS supportate

Per determinare le versioni di Cisco IOS supportate da Cisco SDM, andare al seguente URL:

http://www.cisco.com/go/sdm

Fare clic sul collegamento Technical Documentation (in inglese) e quindi su Release Notes (in inglese).

CAPITOLO 39

Visualizzazione delle informazioni sul router

La modalità Controllo di Cisco Router and Security Device Manager (Cisco SDM) consente di visualizzare un'istantanea corrente delle informazioni sul router, le interfacce router, il firewall e tutte le connessioni VPN attive. È anche possibile visualizzare i messaggi del registro eventi del router.

Nota La finestra Controllo non viene aggiornata dinamicamente con le informazioni più recenti. Per visualizzare le informazioni che sono state modificate dopo la prima visualizzazione della finestra, fare clic su **Aggiorna**.

La modalità Controllo consente di esaminare il registro del router e di visualizzare i risultati dei comandi **show** di Cisco IOS. Per le funzioni della modalità Controllo basate su voci del registro, ad esempio le statistiche dei firewall, deve essere attivata la registrazione. La registrazione è attivata da Cisco SDM per impostazione predefinita, tuttavia l'impostazione può essere modificata tramite la finestra **Attività aggiuntive > Proprietà router > finestra Registrazione**. È possibile, inoltre, che occorra configurare una regola singola in modo che vengano generati eventi del registro. Per maggiori informazioni, vedere l'argomento della Guida Come visualizzare l'attività del firewall?

Funzione	Procedura
Visualizzazione di informazioni relative al router.	Dalla barra degli strumenti, fare clic su **Controlla**, quindi nel frame a sinistra fare clic su **Stato dell'interfaccia**. Nel campo Seleziona interfaccia, selezionare l'interfaccia per la quale si desiderano visualizzare le informazioni, quindi nel gruppo Elementi disponibili, selezionare le informazioni che si desidera visualizzare. Fare clic su **Mostra dettagli**.
Visualizzazione di grafici di utilizzo CPU o della memoria.	Nella barra degli strumenti, fare clic su **Controlla**. Nella pagina Panoramica sono inclusi grafici di utilizzo della CPU e della memoria.
Visualizzazione di informazioni relative al firewall.	Dalla barra degli strumenti, fare clic su **Controlla**, quindi nel frame a sinistra fare clic su **Stato del firewall**.
Visualizzazione di informazioni sulle connessioni VPN	Dalla barra degli strumenti, fare clic su **Controlla**, quindi nel frame a sinistra fare clic su **Stato VPN**. Selezionare la scheda per Tunnel IPSec, Tunnel DMVPN, Server Easy VPN o IKE SA.
Visualizzazione dei messaggi del registro eventi del router.	Dalla barra degli strumenti, fare clic su **Controlla**, quindi nel frame a sinistra fare clic su **Registrazione**.

Panoramica

Nella schermata Panoramica della modalità Controllo viene mostrata una panoramica dell'attività e delle statistiche del router e viene fornito un riepilogo delle informazioni contenute nelle altre schermate. Contiene inoltre le informazioni descritte in questo argomento della Guida.

Nota Se in questo argomento della Guida descritto nella schermata Panoramica non vi sono informazioni su una determinata funzione, significa che l'immagine Cisco IOS non supporta tale funzione. Ad esempio, se sul router è in esecuzione un'immagine Cisco IOS che non supporta le funzioni di protezione, le sezioni Stato del firewall e VPN non vengono visualizzate nella schermata.

Pulsante Avvia applicazione wireless

Se il router è dotato di interfacce radio, questo pulsante permette di controllare e configurare tali interfacce. Nella schermata della panoramica di controllo sono disponibili le informazioni sullo stato di queste interfacce. Tuttavia le interfacce radio non sono elencate nella finestra di stato dell'interfaccia di controllo.

Il pulsante non viene visualizzato se il router non dispone di interfacce radio.

Pulsante Aggiorna

Consente il recupero delle informazioni correnti dal router e l'aggiornamento delle statistiche visualizzate nella schermata.

Stato risorsa

Consente di visualizzare le informazioni di base sul router in uso. Nella schermata sono presenti i campi riportati di seguito.

Utilizzo CPU

In questo campo viene mostrata la percentuale di utilizzo della CPU.

Memoria utilizzata

In questo campo viene mostrata la percentuale di utilizzo della RAM.

Memoria flash utilizzata

In questo campo viene mostrata la quantità di memoria flash disponibile rispetto a quella installata sul router.

Stato dell'interfaccia

Consente di visualizzare le informazioni di base sulle interfacce installate sul router e il relativo stato.

Nota Nelle statistiche sono inclusi solo i tipi di interfaccia supportati da Cisco SDM. Le interfacce non supportate non saranno considerate.

Totale interfacce attive

Il numero totale delle interfacce attive del router.

Totale interfacce non attive

Il numero totale delle interfacce disattivate del router.

Interfaccia

Il nome dell'interfaccia.

IP

L'indirizzo IP dell'interfaccia.

Stato

Lo stato dell'interfaccia che può essere attivo o non attivo.

Utilizzo della larghezza di banda

La percentuale di larghezza di banda utilizzata.

Descrizione

La descrizione disponibile per l'interfaccia. È possibile che Cisco SDM aggiunga descrizioni quali $FW_OUTSIDE$ o ETH_LAN.

Gruppo Stato del firewall

Consente di visualizzare le informazioni di base sulle risorse del router. Nella schermata sono presenti i campi riportati di seguito.

Numero di accessi non consentiti dal firewall

In questo campo viene mostrato il numero dei messaggi del registro generati dai tentativi di connessione (da protocolli quali Telnet, HTTP, ping e altri) non consentiti dal firewall. Si noti che per generare una voce di registro di tentativo di connessione non consentito, è necessario che la regola di accesso che ha rifiutato il tentativo di connessione sia configurata per la creazione di voci di registro.

Registro firewall

Se attivato, in questo campo viene mostrato il numero delle voci di registro del firewall.

QoS

Il numero di interfacce associate a un criterio QoS.

Gruppo Stato VPN

Consente di visualizzare le informazioni di base sulle risorse del router. Nella schermata sono presenti i campi riportati di seguito.

Nr. di SA IKE aperte

In questo campo viene mostrato il numero di connessioni IKE(Security Associations)SA attualmente configurate e in esecuzione.

Nr. di tunnel IPSec aperti

In questo campo viene mostrato il numero di connessioni IPSec(Virtual Private Network) VPN attualmente configurate e in esecuzione.

Nr. di client DMVPN

Se il router è configurato come hub DMVPN, in questo campo viene mostrato il numero dei client DMVPN.

N. client VPN attivi

Se il router è configurato come server Easy VPN, in questo campo viene mostrato il numero di client remoti Easy VPN.

Gruppo Stato NAC

Visualizza un'istantanea sullo stato del NAC (Network Admission Control) sul router.

Campo Numero di interfacce con NAC attivato

Il numero di interfacce router su cui NAC è attivato.

Campo Numero di host convalidati

Il numero di host con agente posture che sono stati convalidati dal processo di controllo di ammissione.

Gruppo Registro

Consente di visualizzare le informazioni di base sulle risorse del router. Nella schermata sono presenti i campi riportati di seguito.

Voci di registro totali

In questo campo viene mostrato il numero totale delle voci memorizzate attualmente nel registro del router.

Elevata gravità

In questo campo viene mostrato il numero di voci del registro memorizzate che presentano un livello di gravità pari a 2 o inferiore. Questi messaggi richiedono attenzione immediata. Si noti che in caso di assenza di messaggi di elevata gravità l'elenco sarà vuoto.

Avviso

In questo campo viene mostrato il numero di voci del registro che presentano un livello di gravità pari a 3 o 4. Questi messaggi potrebbero indicare un problema di rete, tuttavia è probabile che non richiedano attenzione immediata.

Informativo

In questo campo viene mostrato il numero di voci del registro memorizzate che presentano un livello di gravità pari a 6 o superiore. Questi messaggi di informazione segnalano normali eventi di rete.

Stato dell'interfaccia

Nella schermata Stato dell'interfaccia viene visualizzato lo stato corrente delle diverse interfacce del router e il numero di pacchetti, byte o errori di dati che sono passati attraverso l'interfaccia selezionata. Le statistiche mostrate in questa schermata sono cumulative a partire dall'ultimo riavvio del router, dall'ultima reimpostazione dei contatori o dell'interfaccia selezionata.

Pulsante Sottoponi interfaccia a monitoraggio e Interrompi monitoraggio

Fare clic su questo pulsante per avviare o interrompere il controllo dell'interfaccia selezionata. La dicitura del pulsante cambia se Cisco SDM sta effettuando il monitoraggio dell'interfaccia oppure no.

Pulsante Verifica connessione

Per verificare la connessione selezionata, fare clic su questo pulsante. Viene visualizzata una finestra di dialogo che consente di specificare un host remoto verso cui eseguire un ping durante la connessione. Si viene quindi informati sull'esito della verifica. Se la verifica ha esito negativo, vengono fornite informazioni sulle probabili cause del problema e sulle procedure da eseguire per risolverlo.

Elenco interfacce

Selezionare da questo elenco l'interfaccia per la quale si desidera visualizzare le statistiche. Nell'elenco sono indicati il nome, l'indirizzo IP e la subnet mask, lo slot e la porta in cui si trova l'interfaccia e tutte le descrizioni Cisco SDM o utente immesse.

Gruppo Selezionare i tipi di grafico da controllare

Queste caselle di controllo rappresentano i dati per i quali Cisco SDM è in grado di mostrare le statistiche nell'interfaccia selezionata. I dati sono i seguenti:

- Input pacchetti: il numero di pacchetti ricevuti nell'interfaccia.
- Output pacchetti: il numero di pacchetti inviati dall'interfaccia.
- Utilizzo della larghezza di banda: la percentuale di larghezza di banda utilizzata dall'interfaccia, visualizzata come valore percentuale. Il modo in cui viene calcolata la percentuale della larghezza di banda è il seguente:

  Percentuale di larghezza di banda=(Kbit/s/lb) * 100,

  dove

  bit per secondo= ((modifica in input+modifica in output) * 8) / intervallo di polling

  Kbit/s= bit per secondo/1024

  lb=capacità della larghezza di banda dell'interfaccia

  Poiché le differenze tra byte in ingresso e in uscita possono essere calcolate solo dopo il secondo intervallo, nel grafico della percentuale di larghezza di banda viene mostrato l'utilizzo della larghezza di banda corretto a partire da tale intervallo. Per gli intervalli di polling e la visualizzazione degli intervalli vedere la sezione Visualizza intervallo.

- Input byte: il numero di byte ricevuti nell'interfaccia.
- Output byte: il numero di byte inviati dall'interfaccia.
- Errori in ingresso: il numero di errori che si verificano durante la ricezione dei dati nell'interfaccia.
- Errori in uscita: il numero di errori che si verificano durante l'invio dei dati dall'interfaccia.
- Flusso pacchetti: il numero di pacchetti contenuti nel flusso per l'interfaccia selezionata. Questi dati vengono visualizzati solo se sono stati configurati in precedenza in **Configura > Interfacce e connessioni > Modifica > Servizio applicazione** per l'interfaccia prescelta.
- Flusso byte: il numero di byte contenuti nel flusso per l'interfaccia selezionata. Questi dati vengono visualizzati solo se sono stati configurati in precedenza in **Configura > Interfacce e connessioni > Modifica > Servizio applicazione** per l'interfaccia prescelta.
- Totale flusso: il numero totale di flussi, da origini e destinazioni, per l'interfaccia selezionata. Questi dati vengono visualizzati solo se sono stati configurati in precedenza in **Configura > Interfacce e connessioni > Modifica > Servizio applicazione** per l'interfaccia prescelta.

Nota Se l'immagine Cisco IOS del router non supporta NetFlow, i contatori di flusso non saranno disponibili.

Per visualizzare le statistiche di uno di questi elementi:

Passo 1 Scegliere gli elementi da visualizzare selezionando le relative caselle di controllo.

Passo 2 Fare clic su **Controlla interfaccia** per visualizzare le statistiche di tutti i dati selezionati.

Area Stato dell'interfaccia

Visualizza intervallo

Questo campo a discesa consente di selezionare la quantità di dati mostrata per ogni elemento e la frequenza con cui i dati vengono aggiornati. Le opzioni presenti in questo campo sono le seguenti.

Nota Le frequenze di polling elencate sono approssimative e potrebbero essere leggermente diverse dai tempi elencati.

- Dati in tempo reale ogni 10 secondi. Selezionando questa opzione il polling del router continuerà al massimo per due ore, generando circa 120 dati.
- 10 minuti di dati raccolti ogni 10 secondi.
- 60 minuti di dati raccolti ogni minuto.
- 12 ore di dati raccolti ogni 10 minuti.

Nota Selezionando le ultime tra opzioni verrà recuperato un numero massimo di 60 dati. Una volta recuperati 60 dati, Cisco SDM continuerà il polling dei dati, sostituendo i dati più vecchi con quelli più recenti.

Mostra tabella/Nascondi tabella

Fare clic su questo pulsante per mostrare o nascondere i grafici delle prestazioni.

Pulsante Reimposta

Fare clic su questo pulsante per reimpostare su zero i conteggi delle statistiche dell'interfaccia.

Area Grafico

In quest'area vengono mostrati i grafici e i valori numerici relativi ai dati specificati.

Nota Selezionando le ultime tra opzioni verrà recuperato un numero massimo di 30 dati. Una volta recuperati 30 dati, Cisco SDM continuerà il polling dei dati, sostituendo i dati più vecchi con quelli più recenti.

Stato del firewall

In questa finestra vengono visualizzate le seguenti statistiche relative al firewall configurato nel router:

- Numero interfaccia configurata per verifica: il numero di interfacce sul router configurate in modo che il rispettivo traffico venga verificato da un firewall.
- Numero di pacchetti TCP: il numero totale di pacchetti TCP trasmessi tramite le interfacce configurate per la verifica.
- Numero di pacchetti UDP: il numero totale di pacchetti UDP trasmessi tramite le interfacce configurate per la verifica.
- Numero totale di connessioni attive: il numero di sessioni correnti.

Nella finestra Stato del firewall vengono inoltre visualizzate le sessioni con firewall attivo, in una tabella con le seguenti colonne:

- Indirizzo IP di origine: l'indirizzo IP dell'host di origine del pacchetto.
- Indirizzo IP di destinazione: l'indirizzo IP dell'host di destinazione del pacchetto.
- Protocollo: il protocollo di rete in esame.
- Numero corrispondenze: il numero di pacchetti che corrispondono alle condizioni del firewall.

Pulsante Aggiorna

Fare clic su questo pulsante per aggiornare le sessioni con firewall nella tabella e visualizzare i dati più recenti del router.

Stato firewall con criteri basati su zone

Se sul router è in esecuzione un'immagine Cisco IOS che supporta la funzione firewall con criteri basati su zone, è possibile visualizzare lo stato dell'attività del firewall per ciascuna coppia di zone configurata sul router.

Area Elenco criteri firewall

L'area di elenco dei criteri del firewall visualizza il nome del criterio, la zona di origine e quella di destinazione di ogni coppia di zone. Nella tabella che segue vengono mostrati dei dati di esempio di due coppie di zone.

Nome coppia di zone	Nome criterio	Zona di origine	Zona di destinazione
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

Nella tabella di esempio è presente una coppia di zone configurata per il traffico in entrata nella DMZ e per il traffico in uscita dalla DMZ.

Scegliere la coppia di zone di cui si desidera visualizzare le statistiche del firewall.

Visualizza intervallo

Scegliere una delle seguenti opzioni per specificare il metodo di raccolta dei dati:

- Dati in tempo reale ogni 10 secondi: i dati vengono rilevati ogni 10 secondi. Ogni contrassegno sull'asse orizzontale del grafico Pacchetti scartati e Pacchetti consentiti rappresenta un intervallo di 10 secondi.
- 60 minuti di dati raccolti ogni minuto: i dati vengono rilevati ogni minuto. Ogni contrassegno sull'asse orizzontale del grafico Pacchetti scartati e Pacchetti consentiti rappresenta un intervallo di 1 minuto.
- 12 ore di dati raccolti ogni 12 minuti: i dati vengono rilevati ogni 12 minuti. Ogni contrassegno sull'asse orizzontale del grafico Pacchetti scartati e Pacchetti consentiti rappresenta un intervallo di 12 minuti.

Criterio di monitoraggio

Fare clic su **Criterio di monitoraggio** per raccogliere i dati del firewall relativi al criterio selezionato.

Arresta monitoraggio

Fare clic su **Arresta monitoraggio** per terminare la raccolta dei dati del firewall.

Area Statistiche

Quest'area visualizza le statistiche del firewall per la coppia di zone selezionata. Controllare la visualizzazione in quest'area facendo clic sui nodi nella struttura sul lato sinistro. Le seguenti sezioni descrivono cosa viene visualizzato facendo clic su ciascun nodo.

Sessioni attive

Facendo clic su **Sessioni attive** viene visualizzato il tipo di traffico, l'indirizzo IP di origine e quello di destinazione del traffico ispezionato nella coppia di zone scelta.

Pacchetti eliminati

Per la coppia di zone scelta, facendo clic su **Pacchetti eliminati** viene visualizzato un grafico che mostra in numero complessivo di pacchetti scartati nell'intervallo di tempo scelto nell'elenco Intervallo di visualizzazione. I dati vengono raccolti sul traffico configurato come da scartare e registrato nella mappa di criteri Layer 4.

Pacchetti consentiti

Per la coppia di zone scelta, facendo clic su **Pacchetti consentiti** viene visualizzato un grafico che mostra in numero complessivo di pacchetti consentiti nell'intervallo di tempo scelto nell'elenco Intervallo di visualizzazione. I dati vengono raccolti sul traffico configurato con l'azione di autorizzazione nella mappa di criteri Layer 4.

Stato di VPN

In questa finestra viene visualizzata una struttura di connessioni VPN possibili sul router. Nella struttura delle connessioni VPN, è possibile scegliere una delle seguenti categorie VPN:

- Tunnel IPSec
- Tunnel DMVPN
- Easy VPN Server
- SA IKE
- Componenti VPN SSL

Per visualizzare le statistiche su una categoria VPN attiva, selezionare la categoria nella struttura delle connessioni VPN.

Tunnel IPSec

In questo gruppo vengono visualizzate le statistiche su ogni VPN IPSec configurato sul router. Ogni riga della tabella rappresenta una VPN IPSec. Le colonne della tabella e le informazioni in esse visualizzate sono le seguenti:

- Colonna Interfaccia

  L'interfaccia WAN del router sul quale è attivo il tunnel IPSec.
- Colonna Indirizzo IP locale

  L'indirizzo IP dell'interfaccia IPSec locale.
- Colonna Indirizzo IP remoto

  L'indirizzo IP dell'interfaccia IPSec remota.
- Colonna Peer

  L'indirizzo IP del peer remoto.
- Stato tunnel

  Lo stato corrente del tunnel IPSec. Di seguito sono riportati i valori possibili.
  - Attivo: il tunnel è attivo.
  - Disattivato: il tunnel non è attivo a causa di un errore o di un guasto hardware.
- Colonna Pacchetti di incapsulamento

  Il numero di pacchetti incapsulati sulla connessione VPN IPSec.

- Colonna Pacchetti di estrazione

  Il numero di pacchetti estratti sulla connessione VPN IPSec.
- Colonna Pacchetti errore inviati

  Il numero di errori che si sono verificati durante l'invio dei pacchetti.
- Colonna Pacchetti errore ricevuti

  Il numero di errori che si sono verificati durante la ricezione dei pacchetti.
- Colonna Pacchetti crittografati

  Il numero di pacchetti crittografati sulla connessione.
- Colonna Pacchetti decrittografati

  Il numero di pacchetti decrittografati sulla connessione.

Pulsante Controlla tunnel

Fare clic per controllare il tunnel IPSec scelto nella tabella Tunnel IPSec. Vedere Controllo di un tunnel IPSec.

Pulsante Verifica tunnel...

Consente di verificare il tunnel VPN selezionato. I risultati della verifica verranno visualizzati in un'altra finestra.

Pulsante Aggiorna

Fare clic su questo pulsante per aggiornare la tabella Tunnel IPSec e visualizzare i dati più recenti del router.

Controllo di un tunnel IPSec

Per controllare un tunnel IPSec, seguire la procedura riportata di seguito:

Passo 1 Nella tabella Tunnel IPSec, scegliere il tunnel IPSec da controllare.

Passo 2 Scegliere il tipo di informazioni da controllare selezionando le caselle di controllo in **Selezionare l'elemento da controllare**.

Passo 3 Tramite l'elenco a discesa **Visualizza intervallo**, scegliere l'intervallo di tempo per i grafici in tempo reale.

Tunnel DMVPN

In questo gruppo sono visualizzate le statistiche relative ai tunnel DMVPN. Ogni riga rappresenta un tunnel VPN.

- Colonna Subnet remota

  L'indirizzo di rete della subnet al quale il tunnel effettua la connessione.

- Colonna Tunnel IP remoto

  L'indirizzo IP del tunnel remoto. Si tratta dell'indirizzo IP privato assegnato al tunnel dal dispositivo remoto.

- Colonna Indirizzo IP dell'interfaccia pubblica del router remoto

  L'indirizzo IP dell'interfaccia pubblica (esterna) del router remoto.

- Colonna Stato

  Lo stato del tunnel DMVPN.

- Colonna Scadenza

  La data e l'ora di scadenza della registrazione del tunnel e il tunnel DMVPN che sarà chiuso.

Pulsante Controlla tunnel

Fare clic per controllare il tunnel DMVPN scelto nella tabella Tunnel DMVPN. Vedere Controllo di un tunnel DMVPN.

Pulsante Aggiorna

Fare clic su questo pulsante per aggiornare la tabella Tunnel DMVPN e visualizzare i dati più recenti del router.

Pulsante Reimposta

Fare clic per reimpostare i contatori delle statistiche relativi all'elenco dei tunnel. Vengono impostati su zero il numero di pacchetti incapsulati ed estratti, il numero di errori inviati e ricevuti e il numero di pacchetti crittografati e decrittografati.

Controllo di un tunnel DMVPN

Per controllare un tunnel DMVPN, seguire la procedura riportata di seguito:

Passo 1 Nella tabella Tunnel DMVPN, scegliere il tunnel da controllare.

Passo 2 Scegliere il tipo di informazioni da controllare selezionando le caselle di controllo in **Selezionare l'elemento da controllare**.

Passo 3 Tramite l'elenco a discesa **Visualizza intervallo**, scegliere l'intervallo di tempo per i grafici in tempo reale.

Easy VPN Server

In questo gruppo sono visualizzate le seguenti informazioni su ciascun gruppo di server Easy VPN:

- Il numero totale di client (nell'angolo in alto a destra)
- Nome gruppo
- Il numero di connessioni client

Pulsante Dettagli gruppo

Facendo clic su **Dettagli gruppo** verranno visualizzate le seguenti informazioni relative al gruppo selezionato.

- Nome gruppo
- Chiave
- Nome pool
- Server DNS
- Server WINS
- Nome di dominio
- ACL
- Server di backup
- Firewall di tipo Are-U-There
- Includi LAN locale

- Blocco gruppo
- Salva password
- Connessioni massime consentite nel gruppo
- Numero massimo di accessi per utente

Connessioni client nel gruppo

In quest'area vengono visualizzate le seguenti informazioni relative al gruppo selezionato.

- Indirizzo IP pubblico
- Indirizzo IP assegnato
- Pacchetti crittografati
- Pacchetti decrittografati
- Pacchetti in uscita eliminati
- Pacchetti in ingresso eliminati
- Stato

Pulsante Aggiorna

Fare clic su questo pulsante per visualizzare i dati correnti del router.

Pulsante Scollega

- Scegliere una riga nella tabella e fare clic su Disconnetti per lasciar cadere la connessione con il client.

SA IKE

In questo gruppo vengono visualizzate le seguenti statistiche su ogni SA IKE attiva configurata nel router.

- Colonna IP di origine

  L'indirizzo IP della SA IKE di origine del peer.

- Colonna IP di destinazione

  L'indirizzo IP del peer IKE remoto.

- Colonna Stato

  Lo stato corrente delle negoziazioni IKE. Sono possibili i seguenti stati:

  - MM_NO_STATE: è stata creata la SA ISAKMP (Internet Security Association and Key Management Protocol) ma non sono state ancora eseguite operazioni.
  - MM_SA_SETUP: i peer hanno concordato i parametri per la SA ISAKMP.
  - MM_KEY_EXCH: i peer si sono scambiate le chiavi pubbliche Diffie-Hellman e hanno generato un segreto condiviso. La SA ISAKMP resta non autenticata.
  - MM_KEY_AUTH: la SA ISAKMP è stata autenticata. Se il router ha avviato lo scambio, lo stato passa subito a QM_IDLE e inizia uno scambio in modalità rapida.
  - AG_NO_STATE: la SA ISAKMP è stata creata ma non sono state eseguite altre operazioni.
  - AG_INIT_EXCH: i peer hanno effettuato il primo scambio in modalità Aggressive; tuttavia la SA non è autenticata.
  - AG_AUTH: la SA ISAKMP è stata autenticata. Se il router ha avviato lo scambio, lo stato passa subito a QM_IDLE e inizia uno scambio in modalità rapida.
  - QM_IDLE: la SA ISAKMP è inattiva. Resta autenticata con il rispettivo peer e potrebbe essere utilizzata per successivi scambi in modalità rapida.

- Pulsante Aggiorna: fare clic su questo pulsante per aggiornare la tabella SA IKE e visualizzare i dati più recenti del router.
- Pulsante Cancella: selezionare una riga della tabella e fare clic su Cancella per cancellare la connessione SA IKE.

Componenti VPN SSL

Facendo clic sul pulsante Stato VPN il router comincia a controllare l'attività VPN SSL. In questa schermata vengono visualizzati i dati raccolti da tutti i contesti VPN SSL configurati sul router.

Per impostazione predefinita, questi dati vengono aggiornati ogni 10 secondi. Se 10 secondi è un intervallo troppo breve per visualizzare i dati prima dell'aggiornamento successivo, è possibile selezionare un intervallo di aggiornamento automatico ad **ogni minuto** per i **dati in tempo reale**.

Scegliere un contesto nella struttura VPN SSL per visualizzare i dati relativi al contesto e i dati per gli utenti configurati per tale contesto.

Risorse sistema

In quest'area viene visualizzata la percentuale di risorse di CPU e memoria utilizzate dal traffico VPN SSL in tutti i contesti.

N. utenti connessi

In questo grafico viene mostrato il numero di utenti attivi durante il periodo di tempo. Il numero massimo di utenti attivi da quando è iniziato il controllo viene visualizzato in alto nell'area del grafico. L'ora di inizio del controllo è indicata nell'angolo inferiore sinistro del grafico, mentre l'ora corrente è riportata nel centro, sotto al grafico.

Tabbed Area (Area schede)

Quest'area della finestra contiene le statistiche raccolte, organizzate in una serie di schede per semplificarne la visualizzazione.

Per una descrizione dei dati visualizzati nella scheda, fare clic su uno dei collegamenti sottostanti.

User Sessions (Sessioni utente)

Manipolazione URL

Inoltro su porta

CIFS

Full tunnel

Nota Se una funzione, ad esempio Inoltro su porta o Full tunnel, non è stata configurata sul router, nella scheda relativa a tale funzione non sarà visualizzato alcun dato.

Alcune statistiche vengono raccolte da capo ogni volta che il router aggiorna i dati di controllo. Altre statistiche, come le statistiche sul numero massimo di utenti attivi, vengono raccolte al momento dell'aggiornamento, ma vengono confrontate con gli stessi dati raccolti all'avvio del controllo. Il controllo di tutte le attività VPN, incluse le attività VPN SSL, ha inizio quando si fa clic sul pulsante **Stato VPN**.

Contesto VPN SSL

Questa schermata contiene lo stesso tipo di informazioni della schermata Componenti VPN SSL, ma vengono visualizzati solo i dati raccolti per il contesto prescelto. Per una descrizione delle informazioni visualizzate, fare clic su Componenti VPN SSL.

User Sessions (Sessioni utente)

In questa scheda sono visualizzate le seguenti informazioni sulle sessioni utente VPN SSL.

- Sessioni utente attive: il numero di sessioni utente VPN SSL di tutti i tipi attive da quando sono stati aggiornati i dati di controllo.
- Sessioni utente picco: il numero massimo di sessioni utente VPN SSL attive da quando è stato avviato il controllo.
- Connessioni TCP utente attive: il numero di sessioni utente VPN SSL basate su TCP attive da quando sono stati aggiornati i dati di controllo.
- Errori allocazione sessione: il numero di errori di allocazione verificatisi dall'inizio del controllo.
- Timeout sessione VPN: il numero di timeout verificatisi nella sessione VPN dall'inizio del controllo.
- Sessioni VPN cancellate dall'utente: il numero di sessioni VPN cancellate dagli utenti dall'inizio del controllo.
- Richieste in sospeso AAA: il numero di richieste AAA rimaste in sospeso da quando sono stati aggiornati i dati di controllo.
- Ora picco: la più lunga sessione utente registrata dall'inizio del controllo.
- Sessioni utente terminate: il numero di sessioni utente terminate dall'inizio del controllo.

- Errori autenticazione: il numero di sessioni la cui autenticazione è fallita dall'inizio del controllo.
- Timeout inattività VPN: il numero di timeout per inattività verificatisi dall'inizio del controllo.
- Limite utente contesto superato: il numero di volte, dall'inizio del controllo, in cui un utente ha cercato di avviare una sessione quando il limite di sessione del contesto era già stato raggiunto.
- Limite utente totale superato: il numero di volte, dall'inizio del controllo, in cui un utente ha cercato di avviare una sessione quando il limite di sessione totale era già stato raggiunto.

Manipolazione URL

In questa scheda sono visualizzati i dati sulle attività di manipolazione dell'URL. Per maggiori informazioni consultare il riferimento al comando disponibile al seguente indirizzo:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Inoltro su porta

In questa scheda vengono visualizzati i dati raccolti sulle attività di inoltro su porta. Per maggiori informazioni consultare il riferimento al comando disponibile al seguente indirizzo:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

In questa scheda vengono visualizzati i dati raccolti sulle richieste, risposte e connessioni CIFS. Per maggiori informazioni consultare il riferimento al comando disponibile al seguente indirizzo:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Full tunnel

Questa scheda contiene le informazioni sulle connessioni full tunnel tra client e server VPN SSL sull'intranet aziendale.

- Connessioni tunnel attive: il numero di connessioni full tunnel attive a partire dall'ultimo aggiornamento dei dati. I dati possono venire aggiornati ogni 10 secondi o ogni minuto.
- Ora picco connessioni attive: la connessione full tunnel di maggiore durata dall'inizio del controllo.
- Connessioni tunnel attive picco: il numero massimo di connessioni full tunnel attive dall'inizio del controllo.
- Connessioni tunnel non riuscite: il numero di tentativi di connessione full tunnel non riusciti dall'inizio del controllo.
- Connessioni tunnel riuscite: il numero di connessioni full tunnel instaurate correttamente dall'inizio del controllo.

Server:

- Pacchetti IP inviati al server: il numero di pacchetti IP ricevuti dai client full tunnel e inoltrati dal router ai server sull'intranet aziendale.
- Traffico IP inviato al server in byte: la quantità di traffico IP, espressa in byte, inoltrata dai client full tunnel ai server sull'intranet aziendale.
- Pacchetti IP ricevuti dal server: il numero di pacchetti IP che il router ha ricevuto dai server con connessioni full tunnel ai client.
- Traffico IP ricevuto dal server in byte: la quantità di traffico IP, espressa in byte, ricevuta dai server sull'intranet aziendale con connessioni full tunnel ai client.

Elenco di utenti

In questa finestra sono visualizzate le informazioni per il contesto scelto nella struttura Componenti VPN SSL. Poiché possono esservi più criteri di gruppo configurati per il contesto, ciascuno con i propri elenchi di URL e di server, questa schermata fornisce informazioni importanti su come i singoli utenti stanno utilizzando le rispettive connessioni VPN SSL.

Questa finestra permette di controllare il singolo uso di VPN SSL, scegliendo un utente e facendo clic sul pulsante **Scollega.**

Area Elenco di utenti

In quest'area sono elencati tutti gli utenti attivi di tutti i gruppi configurati per questo contesto. Nell'area sono visualizzate le seguenti informazioni:

- Nome di accesso utente: il nome utente autenticato con il server AAA.
- Indirizzo IP client: l'indirizzo IP VPN SSL assegnato all'utente per questa sessione. L'indirizzo IP viene ottenuto dal pool di indirizzi configurati per questo contesto.
- Contesto: il contesto VPN SSL in cui è stato configurato il criterio di gruppo per questo utente.
- Numero di connessioni: il numero di connessioni attive per l'utente. L'utente, ad esempio, può essere connesso a un server di posta e contemporaneamente sfogliare i file su un altro server collegato in rete.
- Data di creazione: la data in cui è stata creata la sessione.
- Ultimo utilizzo: ora e giorno in cui l'utente ha inviato del traffico per l'ultima volta tramite una connessione attiva.
- Cisco Secure Desktop: vero o falso. Indica se Cisco Secure Desktop è stato scaricato sul PC dell'utente.
- Nome gruppo: il nome del criterio di gruppo sotto al quale è stato configurato l'utente. I criteri di gruppo specificano l'elenco degli URL, i servizi disponibili per gli utenti, i server WINS disponibili per risolvere i nomi dei server e i server visualizzabili dall'utente quando sfoglia i file sull'intranet aziendale.
- Nome elenco di URL: il nome dell'elenco di URL che viene visualizzato nella pagina del portale dell'utente. L'elenco di URL è configurato per il gruppo a cui appartiene l'utente. Per maggiori informazioni vedere la sezione Criterio di gruppo: scheda Senza client.
- Timeout idle: il numero di secondi in cui una sessione può restare inattiva prima che venga terminata dal router. Questo valore è configurato per il gruppo a cui appartiene l'utente. Per maggiori informazioni vedere la sezione Criterio di gruppo: scheda Generale.
- Timeout sessione: il numero massimo di secondi in cui una sessione può restare attiva prima che venga terminata. Questo valore è configurato per il gruppo a cui appartiene l'utente. Per maggiori informazioni vedere la sezione Criterio di gruppo: scheda Generale.

- Nome dell'elenco di inoltro su porta: questo valore è configurato per il gruppo a cui appartiene l'utente. Per maggiori informazioni vedere la sezione Criterio di gruppo: scheda Thin client.
- WINS Name Service list name (Nome elenco WINS Name Service): questo valore è configurato per il gruppo a cui appartiene l'utente. Per maggiori informazioni vedere la sezione Criterio di gruppo: scheda Senza client.

Stato traffico

Questa finestra visualizza una struttura dei tipi di traffico che controllabili su un'interfaccia. Per poter controllare qualsiasi tipo di traffico, è necessario che sia abilitata almeno un'interfaccia.

Nella struttura Stato traffico, è possibile scegliere uno dei seguenti tipi di traffico:

- Talker principali NetFlow
- QoS
- Traffico applicazione/protocollo

  Per il controllo del traffico questo tipo utilizza il riconoscimento dell'applicazione basato sulla rete (NBAR).

Talker principali NetFlow

Se le statistiche NetFlow sono state abilitate per almeno un'interfaccia in **Configura > Interfacce e connessioni > Modifica interfaccia/connessione**, è possibile visualizzare le statistiche NetFlow. Nella struttura Stato traffico, scegliere **N flussi traffico principali > Protocolli principali** o **N flussi traffico principali > Talker principali** (origini a traffico elevato).

Nota Se l'immagine Cisco IOS del router non supporta NetFlow, le opzioni NetFlow non saranno disponibili nella struttura Stato traffico.

Protocolli principali

In questa finestra è visualizzata una tabella con le seguenti colonne:

- Protocollo: il protocollo in esame.
- Totale flussi: il numero totale di flussi associati a tale protocollo.
- Flussi/sec: i flussi attivi al secondo per il protocollo.
- Pacchetti/flusso: pacchetti trasmessi per flusso.
- Byte/pacchetto: byte per pacchetto trasmesso.
- Pacchetti/sec: pacchetti trasmessi per secondo.

Pulsante Aggiorna

Aggiorna la finestra con le informazioni correnti sui flussi.

Talker principali

In questa finestra è visualizzata una tabella con le seguenti colonne:

- **Indirizzo IP di origine**: l'indirizzo IP di origine del talker principale.

  Selezionare un indirizzo IP di origine per visualizzare ulteriori informazioni in **Stato flusso per indirizzo di origine**.
- **Pacchetti**: numero totale di pacchetti ricevuti dall'indirizzo IP di origine.
- **Byte**: numero totale di byte ricevuti dall'indirizzo IP di origine.
- **Flussi**: numero totale di flussi associati all'indirizzo IP di origine.

Nota Se l'opzione Talker principali NetFlow non è abilitata in **Configura > Attività aggiuntive > Proprietà router > NetFlow**, verranno visualizzate le statistiche per i primi dieci talker principali.

Stato flusso per indirizzo di origine

In questa tabella sono riportate le seguenti informazioni sul flusso associato all'indirizzo IP di origine selezionato:

- **Indirizzo IP di destinazione**: indirizzo IP di destinazione del talker principale.
- **Protocolli**: i protocolli utilizzati nei pacchetti scambiati con l'indirizzo IP di destinazione.
- **Numero di pacchetti**: il numero di pacchetti scambiati con l'indirizzo IP di destinazione.

Pulsante Aggiorna

Aggiorna la finestra con le informazioni correnti sui flussi.

QoS

La finestra Stato QoS consente di monitorare le prestazioni relative al traffico delle interfacce per cui è stato configurato il criterio QoS (vedere Associazione di un criterio QoS a un'interfaccia). Inoltre in questa finestra è possibile monitorare l'utilizzo della larghezza di banda e i byte inviati relativamente alle interfacce prive di una configurazione QoS. Il monitoraggio del traffico in ingresso nelle interfacce QoS mostra le statistiche solo a livello di protocollo. Per quanto riguarda le interfacce non QoS, il sistema provvede a creare delle statistiche a livello di protocollo per il traffico in entrambe le direzioni.

In questa finestra è possibile monitorare le statistiche di seguito riportate:

- Utilizzo della larghezza di banda per i tipi di traffico definiti in Cisco SDM.
  - Utilizzo della larghezza di banda per classe per ciascun tipo di traffico.
  - Utilizzo della larghezza di banda per protocollo e per classe.

  L'utilizzo della larghezza di banda è mostrato in Kbps.
- Quantità totale dei byte in ingresso e in uscita per ciascun tipo di traffico.
  - Quantità di byte in ingresso e in uscita per ciascuna classe definita nel tipo di traffico.
  - Quantità di byte in ingresso e in uscita per ciascun protocollo e per ogni classe.

Se il valore è maggiore di 1.000.000, il grafico può mostrare la quantità di byte come multiplo di 10^6. Se il valore è maggiore di 1.000.000.000, la quantità di byte può essere mostrata come multiplo di 10^9.

- Statistiche relative ai pacchetti scartati per ciascun tipo di traffico.

Interfaccia - IP/Maschera - Slot/Porta - Descrizione

In quest'area sono elencate le interfacce per cui sono stati configurati dei criteri QoS insieme ad altri dettagli informativi quali indirizzo IP e subnet mask, slot e porta (se applicabile). Infine, se disponibili, sono riportate delle descrizioni.

Selezionare in questo elenco l'interfaccia che si desidera monitorare.

Visualizza intervallo

Selezionare la frequenza di tempo secondo cui rilevare le statistiche:

- Subito - Le statistiche vengono rilevate non appena si fa clic su **Avvia monitoraggio**.
- Ogni minuto - Le statistiche vengono rilevate non appena si fa clic su **Avvia monitoraggio** e vengono aggiornate ogni minuto.
- Ogni 5 minuti - Le statistiche vengono rilevate non appena si fa clic su **Avvia monitoraggio** e vengono aggiornate ogni 5 minuti.
- Ogni ora - Le statistiche vengono rilevate non appena si fa clic su **Avvia monitoraggio** e vengono aggiornate ogni ora.

Avvia monitoraggio

Fare clic su questo pulsante per avviare il monitoraggio delle statistiche QoS.

Scelta dei parametri QoS da monitorare

Selezionare la direzione del traffico e il tipo di statistiche di cui si desidera effettuare il monitoraggio.

Direzione

Fare clic su **Input** oppure su **Output**.

Statistiche

Selezionare una delle seguenti opzioni:

- Larghezza di banda
- Byte
- Pacchetti scartati

Tutto il traffico - Traffico in tempo reale - Business-critical - Leggero

Cisco SDM visualizza le statistiche di tutte le classi di traffico sotto forma di grafico a barre, in base al tipo di statistica selezionato. Cisco SDM visualizza un messaggio al posto del grafico a barre se non sono presenti statistiche adeguate al tipo di traffico scelto.

Associazione di un criterio QoS a un'interfaccia

Passo 1 Andare a **Interfacce e connessioni > Modifica interfaccia/connessione**.

Passo 2 Dall'Elenco interfacce, scegliere l'interfaccia che si desidera associare a un criterio QoS.

Passo 3 Fare clic sul pulsante **Modifica**.

Passo 4 Fare clic sulla scheda **Servizio applicazione**.

Passo 5 Scegliere un criterio QoS dall'elenco a discesa **In ingresso** per associarlo al traffico in ingresso sull'interfaccia.

Passo 6 Scegliere un criterio QoS dall'elenco a discesa **In uscita** per associarlo al traffico in uscita sull'interfaccia.

Traffico applicazione/protocollo

Questa schermata permette di controllare il traffico dell'applicazione e del protocollo tramite il riconoscimento dell'applicazione basato sulla rete (NBAR), una funzione di rilevamento di protocollo e applicazione. La funzionalità NBAR viene usata per classificare i pacchetti, consentendo di gestire in maniera più efficiente il traffico di rete tramite un'interfaccia specifica.

Nota Se l'immagine Cisco IOS del router non supporta NBAR, la finestra di stato non sarà disponibile.

Attiva NBAR

Per visualizzare lo stato di NBAR per un'interfaccia specifica, è necessario che la funzione NBAR sia stata precedentemente abilitata sull'interfaccia. Per abilitare NBAR, seguire la procedura riportata di seguito:

Passo 1 Andare a **Interfacce e connessioni > Modifica interfaccia/connessione**.

Passo 2 Dall'Elenco interfacce, scegliere l'interfaccia per la quale si desidera abilitare NBAR.

Passo 3 Fare clic sul pulsante **Modifica**.

Passo 4 Fare clic sulla scheda **Servizio applicazione**.

Passo 5 Selezionare la casella di controllo **NBAR**.

Stato NBAR

Nella tabella di stato di NBAR sono visualizzate le statistiche riportate di seguito relative all'interfaccia selezionata nell'elenco a discesa **Selezionare un'interfaccia**:

- Numero pacchetti input: il numero di pacchetti del protocollo visualizzato, in ingresso sull'interfaccia selezionata.
- Numero pacchetti output: il numero di pacchetti del protocollo visualizzato, in uscita dall'interfaccia selezionata.
- Frequenza bit (bps): la velocità, espressa in bit al secondo, del traffico che passa attraverso l'interfaccia.

Stato NAC

Se il NAC è configurato sul router, Cisco SDM può visualizzare informazioni dell'istantanea sulle sessioni NAC del router, le interfacce su cui il NAC è configurato e le statistiche NAC dell'interfaccia selezionata.

La riga superiore della finestra visualizza il numero di sessioni NAC attive, il numero di sessioni NAC in corso di inizializzazione e un pulsante che consente di eliminare tutte le sessioni attive e in corso di inizializzazione.

La finestra elenca le interfacce del router con criteri NAC associati.

```
FastEthernet0/0    10.10.15.1/255.255.255.0   0
```

Facendo clic su una voce dell'interfaccia si visualizzano le informazioni restituite dagli agenti posture installati sugli host nella rete secondaria di tale interfaccia. Segue un esempio di informazioni dell'interfaccia:

```
10.10.10.5     Criterio EAP remoto    Infetto        12
```

10.10.10.1 è l'indirizzo IP dell'host. Criterio EAP remoto è il tipo di criterio di autenticazione in vigore. La posture corrente dell'host è Infettato, e sono passati 12 minuti da quando l'host ha completato il processo di controllo delle ammissioni.

Nota Quest'area della finestra non contiene dati se dall'host della rete selezionata non vengono restituite informazioni sulla posture.

I tipi di autenticazione sono:

- **Criterio di eccezione locale**: un criterio di eccezione configurato sul router e utilizzato per convalidare l'host.
- **Criterio EAP remoto**: l'host restituisce una posture e viene usato un criterio di eccezione assegnato da un server ACS.
- **Criterio d'accesso generico remoto**: l'host non ha un agente posture installato, quindi il server ACS assegna un criterio host senza agente.

L'agente posture sull'host possono ritornare i seguenti token di posture:

- **Sano**: l'host è privo di virus noti e dispone dei file di definizione aggiornati.
- **Controllo**: l'agente posture sta determinando se è stato installato l'ultimo file di definizione dei virus.

- **Quarantena**: sull'host non è installato l'ultimo file di definizione dei virus. L'utente è reindirizzato al sito di riparazione specificato che contiene le istruzioni per scaricare i file di definizione dei virus più aggiornati.
- **Infetto**: l'host è stato infettato da un virus noto. L'utente è reindirizzato a un sito di riparazione specificato per ottenere i file di definizione dei virus più aggiornati.
- **Sconosciuto**: la posture dell'host è sconosciuta.

Registri

In Cisco SDM sono disponibili i seguenti registri:

- Syslog: il registro del router.
- Registro firewall: se sul router è stato configurato un firewall, in questo registro vengono registrate le immissioni generate da tale firewall.
- Registro di Protezione dell'applicazione: se sul router è stato configurato il firewall di un'applicazione, in questo registro vengono registrate le immissioni generate da tale firewall.
- Registro messaggi SDEE: se SDEE è stato configurato sul router, in questo registro vengono registrati i messaggi SDEE.

Per aprire un registro, fare clic sulla scheda avente il nome del registro.

Syslog

Il router contiene un registro di eventi suddivisi in categorie in base al livello di gravità, simile a un servizio syslog di UNIX.

Nota Viene visualizzato il registro del router, anche se i messaggi del registro vengono inoltrati a un server syslog.

Registrazione buffer

In questa schermata viene mostrato se la registrazione buffer e quella syslog sono attivate. Se entrambe sono attivate viene visualizzato il testo “Attivato” Nella registrazione buffer una determinata quantità di memoria viene riservata per conservare i messaggi del registro. L'impostazione di questo campo non viene mantenuta se si riavvia il router. Per impostazione predefinita, la registrazione buffer è attivata con 4069 byte di memoria.

Host di registrazione

In questa finestra viene visualizzato l'indirizzo IP di tutti gli host syslog ai quali vengono inoltrati i messaggi del registro. Il campo è di sola lettura. Per configurare gli indirizzi IP degli host syslog, utilizzare la finestra **Attività aggiuntive > Proprietà router > Registrazione**.

Livello registrazione (Buffer)

In questa finestra viene mostrato il livello di registrazione configurato per il buffer sul router.

Numero di messaggi nel registro

In questa finestra viene mostrato il numero totale dei messaggi memorizzati nel registro del router.

Selezionare un livello di registrazione da visualizzare

Da questo campo, selezionare il livello di gravità dei messaggi che si desidera visualizzare nel registro. Se si modifica l'impostazione in questo campo, l'elenco dei messaggi del registro sarà aggiornato.

Registro

In questa finestra vengono visualizzati tutti i messaggi con il livello di gravità specificato nel campo Selezionare un livello di registrazione da visualizzare. Nel registro sono contenute le informazioni riportate di seguito.

- Colonna Gravità

In questa colonna viene mostrata la gravità dell'evento di registrazione, sottoforma di numero da 1 a 7, con i numeri più bassi utilizzati per indicare gli eventi più gravi. Di seguito viene fornita la descrizione dei livelli di gravità.

- 0: emergenze

  Sistema inutilizzabile
- 1: avvisi

  È necessaria un'azione immediata
- 2: critico

  Condizioni critiche
- 3: errori

  Condizioni di errore
- 4: avvertenze

  Condizioni di avvertenza
- 5: notifiche

  Condizione normale ma significativa
- 6: informativo

  Messaggio unicamente informativo
- 7: debug

  Messaggi di debug

- Colonna Ora

  In questa colonna viene mostrata l'ora in cui si è verificato l'evento del registro.
- Colonna Descrizione

  In questa colonna viene mostrata una descrizione dell'evento del registro.

Pulsante Aggiorna

Questo pulsante consente di aggiornare la finestra con le informazioni correnti sui dettagli del registro e le voci di registro più recenti.

Pulsante Clear Log (Cancella registro)

Questo pulsante consente di cancellare tutti i messaggi dal buffer del registro del router.

Pulsante Cerca

Viene aperta una finestra di ricerca. Nella finestra di ricerca, digitare il testo nel campo Cerca e fare clic sul pulsante **Trova** per visualizzare tutte le voci contenenti il testo cercato. Nelle ricerche *non* viene fatta distinzione tra lettere maiuscole e minuscole.

Registro firewall

Le voci di registro mostrate nella parte superiore di questa finestra sono determinate dai messaggi di registro generati dal firewall. Per consentire al firewall di generare voci di registro, è necessario configurare una regola di accesso singolo per la creazione di messaggi del registro nel momento in cui vengono richiamate. Per istruzioni sulle regole di configurazione dell'accesso per la generazione di messaggi di registro, vedere l'argomento della Guida Come visualizzare l'attività del firewall?

Affinché il log del firewall venga raccolto è necessario configurare il log sul router. Andare ad **Attività aggiuntive > Proprietà router > Registrazione**. Fare clic su **Modifica** e configurare la registrazione. Per ottenere i messaggi di registrazione del firewall si deve configurare un livello di debug (7).

Registro firewall

Il registro del firewall viene visualizzato se il router è configurato per gestire un registro dei tentativi di connessione negati dal firewall.

Numero di accessi non consentiti dal firewall

L'opzione consente di visualizzare il numero di tentativi di connessione rifiutati dal firewall.

Tabella Tentativi non consentiti dal firewall

L'opzione consente di visualizzare il numero di tentativi di connessione rifiutati dal firewall. In questa tabella sono incluse le seguenti colonne:

- Colonna Ora

  In questa colonna viene mostrata l'ora in cui il tentativo di connessione è stato rifiutato.

- Colonna Descrizione

  Contiene le seguenti informazioni relative ai tentativi non consentiti: nome accesso, nome o numero della regola di accesso, servizio, indirizzo di origine, indirizzo di destinazione e numero di pacchetti. Ad esempio:

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

Pulsante Aggiorna

Consente di eseguire il polling del router e di aggiornare le informazioni mostrate nella schermata.

Pulsante Cerca

Viene aperta una finestra di ricerca. Nel menu **Cerca** scegliere un tipo di ricerca e digitare il testo nel campo Cerca, quindi fare clic sul pulsante **Trova** per visualizzare le voci di registro che corrispondono alla ricerca.

Sono disponibili i seguenti tipi di ricerca:

- Indirizzo IP di origine: l'indirizzo IP di origine dell'attacco.

  È possibile specificare un indirizzo IP parziale.

- Indirizzo IP di destinazione: l'indirizzo IP di destinazione dell'attacco.

  È possibile specificare un indirizzo IP parziale.

- Protocollo: il protocollo di rete utilizzato per l'attacco.
- Testo: un testo qualunque trovato nella voce di registro.

Nelle ricerche *non* viene fatta distinzione tra lettere maiuscole e minuscole.

Visualizzazione degli attacchi principali

Nel menu a tendina Visualizza, scegliere uno dei seguenti metodi per visualizzare le informazioni sugli attacchi principali:

- Porte attacchi principali: gli attacchi principali in base alla porta di destinazione.
- Autori attacchi principali: in base all'indirizzo IP dell'autore dell'attacco.

Sotto al menu a tendina Visualizza è riportata una tabella contenente le voci sugli attacchi principali. Se nel menu a tendina Visualizza è stata scelta l'opzione Porte attacchi principali, nella tabella degli attacchi principali le voci verranno visualizzate con le seguenti colonne:

- Numero di porta: la porta di destinazione.
- Numero di attacchi: il numero di attacchi eseguiti sulla porta di destinazione.
- Numero di pacchetti negati: il numero di pacchetti a cui è stato negato l'accesso sulla porta di destinazione.
- Visualizza dettagli: un collegamento che apre una finestra contenente il registro completo degli attacchi eseguiti sulla porta selezionata.

Se nel menu a tendina Visualizza è stata scelta l'opzione Autori attacchi principali, nella tabella degli attacchi principali le voci verranno visualizzate con le seguenti colonne:

- Indirizzo IP autori attacco: l'indirizzo IP da cui provengono gli attacchi.
- Numero di attacchi: il numero di attacchi pervenuti dall'indirizzo IP.
- Numero di pacchetti negati: il numero di pacchetti pervenuti dall'indirizzo IP e ai quali è stato negato l'accesso.
- Visualizza dettagli: un collegamento che apre una finestra contenente il registro completo degli attacchi eseguiti dall'indirizzo IP selezionato.

Controllo del firewall con un account utente di "visualizzazione non amministrativo"

Il controllo del firewall richiede l'attivazione sul router della Registrazione in buffer. Se tale registrazione non è attivata, accedere a Cisco SDM mediante un account di visualizzazione di amministratore oppure utilizzando un account utente non basato sulla visualizzazione, con livello di privilegio 15, e configurare la registrazione.

Per configurare la registrazione in Cisco SDM, scegliere **Attività aggiuntive** > **Proprietà router** > **Registrazione**.

Registro di Protezione dell'applicazione

Se è stata attivato il log e si è specificato che quando il router rileva traffico da applicazioni o protocolli specificati devono essere generati degli allarmi, tali allarmi vengono raccolti in un log visibile mediante questa finestra.

Affinché le voci del Registro di Protezione dell'applicazione vengano raccolte è necessario configurare il logging sul router. Andare ad **Attività aggiuntive > Proprietà router > Registrazione**. Fare clic su **Modifica** e configurare la registrazione. Per ottenere i messaggi di registrazione del firewall è necessario configurare un livello di registrazione **informativo (6)** o superiore. Se la registrazione è già stata configurata per il **debug (7)**, il registro conterrà i messaggi del registro di protezione dell'applicazione.

Il seguente è un esempio di testo del log:

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

Pulsante Aggiorna

Questo pulsante consente di aggiornare la schermata con le informazioni correnti sui dettagli del registro e le voci di registro più recenti.

Pulsante Cerca

Viene aperta una finestra di ricerca. Nella finestra di ricerca, digitare il testo nel campo Cerca e fare clic sul pulsante **Trova** per visualizzare tutte le voci contenenti il testo cercato. Nelle ricerche *non* viene fatta distinzione tra lettere maiuscole e minuscole.

Registro messaggi SDEE

In questa finestra sono elencati i messaggi SDEE ricevuti dal router. I messaggi SDEE vengono generati quando sono apportate modifiche alla configurazione IPS.

Messaggi SDEE

Scegliere il tipo di messaggio SDEE da visualizzare:

- Tutto - Vengono visualizzati i messaggi di errore, di stato e di avviso SDEE.
- Errore - Vengono visualizzati soltanto i messaggi di errore SDEE.
- Stato - Vengono visualizzati soltanto i messaggi di stato SDEE.
- Avvisi - Vengono visualizzati soltanto i messaggi di avviso SDEE.

Pulsante Aggiorna

Consente di verificare se ci sono nuovi messaggi SDEE.

Pulsante Cerca

Viene aperta una finestra di ricerca. Nel menu **Cerca** scegliere un tipo di ricerca e digitare il testo nel campo Cerca, quindi fare clic sul pulsante **Trova** per visualizzare le voci di registro che corrispondono alla ricerca.

Sono disponibili i seguenti tipi di ricerca:

- Indirizzo IP di origine
- Indirizzo IP di destinazione
- Testo

Nelle ricerche *non* viene fatta distinzione tra lettere maiuscole e minuscole.

Ora

Indica l'ora in cui il messaggio è stato ricevuto.

Tipo

I tipi sono: Errore, Stato e Avvisi. Fare clic su Testo dei messaggi SDEE per visualizzare gli eventuali messaggi SDEE.

Descrizione

Visualizza la descrizione presente.

Stato IPS

Questa finestra viene visualizzata se il router utilizza un'immagine Cisco IOS che supporta IPS versione 4.x o precedente. In questa finestra è visualizzata una tabella con le statistiche sulle firme IPS, raggruppate per tipo di firma. Sono riportate le seguenti statistiche:

- **ID firma**: identificativo numerico della firma.
- **Descrizione**: descrizione della firma.
- **Valutazione rischio**: valore compreso tra 0 e 100 che rappresenta una quantificazione numerica del rischio associato a un particolare evento della rete.
- **Azione**: azione da eseguire quando viene rilevata la corrispondenza di un pacchetto con una firma.
- **Indirizzo IP di origine**: l'indirizzo IP dell'host di origine del pacchetto.
- **Indirizzo IP di destinazione**: l'indirizzo IP dell'host di destinazione del pacchetto.

- **Risultati**: il numero di pacchetti corrispondenti.
- **Numero eliminazioni**: il numero di pacchetti corrispondenti scartati.

Per ordinare le firme, fare clic sull'intestazione della colonna avente il nome di statistica della firma in base alla quale si desidera effettuare l'ordinamento.

Nota Se le firme vengono ordinate, potrebbero non risultare più raggruppate per tipo. Per ripristinare il raggruppamento delle firme per tipo, fare clic sul pulsante **Aggiorna**.

Totale firma attiva

Visualizza il numero totale di firme disponibili attive sul router.

Totale firma non attiva

Visualizza il numero totale di firme disponibili non attive sul router.

Pulsante Aggiorna

Fare clic per verificare e includere le statistiche sulle firme più recenti.

Pulsante Cancella

Fare clic per impostare su 0 tutti i contatori delle statistiche sulle firme.

Registro SDEE

Consente di visualizzare i messaggi SDEE. È anche possibile visualizzare tali messaggi facendo clic su **Controllo > Registrazione > Registro messaggi SDEE**.

Statistiche firma IPS

Questa finestra viene visualizzata se il router utilizza una configurazione IOS IPS 5.x. Le statistiche vengono visualizzate per ciascuna firma attiva nella configurazione IOS IPS. La parte superiore della finestra visualizza i totali di firma in modo da fornire un'istantanea della configurazione delle firme. Vengono forniti i seguenti totali:

- Totale firme
- Totale firme attivate
- Totale firme ritirate
- Totale firme compilate

Pulsanti Aggiorna e Cancella

Fare clic su **Aggiorna** per verificare e includere le statistiche sulle firme più recenti. Fare clic su **Cancella** per impostare su 0 tutti i contatori delle statistiche sulle firme.

Registro SDEE

Consente di visualizzare i messaggi SDEE. È anche possibile visualizzare tali messaggi facendo clic su **Controllo > Registrazione > Registro messaggi SDEE**.

Area elenco firme

L'ID firma, la Descrizione, il numero di risultati e il conteggio di scarto vengono visualizzati per tutte le firme. Se giunge un pacchetto che corrisponde alla firma, vengono anche elencati gli indirizzi IP di origine e destinazione.

Statistiche avvisi IPS

La finestra Statistiche avvisi IPS visualizza le statistiche di avvisi in formato codificato da colori per un riconoscimento più semplice. La parte superiore della schermata visualizza la legenda che illustra l'utilizzo dei colori nella schermata.

Colore	Spiegazione
ROSSO	L'evento che ha generato l'avviso ha un RR (Risk Rating, Classificazione rischio) alto nell'intervallo compreso tra 70 e 100.
MAGENTA	L'evento che ha generato l'avviso ha un RR (Risk Rating, Classificazione rischio) medio nell'intervallo compreso tra 40 e 69.
BLU	L'evento che ha generato l'avviso ha un RR (Risk Rating, Classificazione rischio) basso nell'intervallo compreso tra 0 e 39.

Facendo clic su un'intestazione di colonna, la visualizzazione viene riordinata in base ai valori del relativo parametro. Per esempio, facendo clic sull'intestazione **ID firma**, la visualizzazione viene ordinata nell'ordine numerico di ID firma crescente o decrescente. Nel seguente elenco viene descritta ciascuna colonna:

- **ID firma**: identificativo numerico della firma.
- **Descrizione**: descrizione della firma.
- Valutazione rischio: valore compreso tra 0 e 100 che rappresenta una quantificazione numerica del rischio associato a un particolare evento della rete.
- Azione evento: azione da eseguire da parte di IOS IPS quando si verifica una corrispondenza di un evento con una firma.
- Indirizzo IP di origine: l'indirizzo IP di origine del pacchetto.
- Indirizzo IP di destinazione: l'indirizzo IP di destinazione del pacchetto. Se il pacchetto è sospetto, l'Indirizzo IP di destinazione viene considerato come destinazione.
- Risultati: il numero di pacchetti corrispondenti.
- Numero eliminazioni: il numero di pacchetti corrispondenti scartati.
- Motore: il motore firme associato alla firma.

Stato autenticazione 802.1x

Area Autenticazione 802.1x sulle interfacce

Interfaccia

Autenticazione 802.1x

Riautenticazione

Area Client 802.1x

Indirizzo MAC client

Stato autenticazione

Interfaccia

CAPITOLO 40

Comandi del menu File

Nel menu File di Cisco Router and Security Device Manager (Cisco SDM) sono disponibili le opzioni riportate di seguito.

Salva configurazione in esecuzione su computer

Consente di salvare il file della configurazione del router in esecuzione in un file di testo del computer.

Invia configurazione al router

Questa finestra consente di inviare al router qualsiasi modifica della configurazione effettuata usando Cisco SDM. Le modifiche di configurazione apportate tramite Cisco SDM non avranno effetto sul router finché non viene inviata la configurazione.

Salva configurazione corrente nella configurazione d'avvio del router

Selezionare questa casella di controllo per fare in modo che Cisco SDM salvi la configurazione visualizzata nel file di configurazione in esecuzione del router e nel file di avvio. Il file di configurazione in esecuzione è temporaneo e viene cancellato dopo il riavvio del server. Salvando nella configurazione di avvio del router, le modifiche verranno mantenute dopo il riavvio.

Se si sta utilizzando Cisco SDM per configurare un router Cisco 7000, la casella di controllo **Salva configurazione corrente nella configurazione d'avvio del router** sarà disattivata se nella configurazione in esecuzione sono presenti comandi di **avvio di rete** o **avvio di host** con comandi di **configurazione di servizio**.

Annulla

Fare clic su questo pulsante per cambiare e chiudere la finestra di dialogo di Cisco SDM Invia a router.

Salva su file

Fare clic su questo pulsante per salvare le modifiche di configurazione visualizzate in un file di testo.

Scrivi nella configurazione d'avvio

Consente di scrivere il file di configurazione del router in esecuzione nella configurazione di avvio del router.

Se si utilizza Cisco SDM per configurare un router Cisco 7000, questa voce di menu sarà disattivata se nella configurazione in esecuzione sono presenti comandi **boot network** o **boot host** con i comandi **service config**.

Ripristina impostazioni predefinite

Vedere Ripristina impostazioni predefinite.

Gestione file

In questa finestra è possibile visualizzare e gestire i file di sistema nella memoria flash del proprio router Cisco e dei dispositivi USB collegati a tale router. Qui si possono vedere e gestire soltanto i file ti tipo DOSFS.

Il lato sinistro della finestra visualizza una struttura ad albero espandibile che rappresenta il sistema delle directory della memoria flash del proprio router Cisco e dei dispositivi flash USB collegati a tale router.

Il lato destro della finestra visualizza un elenco dei nomi dei file e delle directory che si trovano nella directory selezionata nel lato sinistro della finestra. Qui è inoltre visibile la dimensione in bytes e la data e l'ora dell'ultima modifica di ciascun file o directory.

È possibile scegliere un file da caricare nella lista sul lato destro della finestra e poi scegliere uno dei comandi sopra la lista.

Le directory (cartelle) possono essere rinominate o eliminate. È possibile copiare, incollare o eliminare uno o più file e rinominare i singoli file. In ogni caso vengono applicate le seguenti restrizioni:

- I file non possono essere incollati nella stessa directory in cui sono stati copiati.
- Se Cisco SDM viene richiamato dalla memoria flash del router, i file Cisco SDM non possono essere eliminati.

  È possibile eliminare i file Cisco SDM che sono copie oppure quando Cisco SDM viene richiamato da un PC.
- Se Cisco SDM viene richiamato dalla memoria flash del router, i file Cisco SDM non possono essere rinominati.

  È possibile rinominare i file Cisco SDM che sono copie oppure quando Cisco SDM viene richiamato da un PC.
- Se Cisco SDM viene richiamato dalla memoria flash del router, non è possibile sostituire un file Cisco SDM (vale a dire incollare un file copiato che abbia lo stesso nome).

  È possibile sostituire i file Cisco SDM che sono copie oppure quando Cisco SDM viene richiamato da un PC.
- I file del software Cisco IOS non possono essere rinominati.
- Le directory (cartelle) non possono essere copiate.

Se il router viene avviato da un server tftp, non viene applicata alcuna limitazione sull'uso del file.

Pulsante Aggiorna

Fare clic sul pulsante **Aggiorna** per caricare una nuova immagine delle directory e dei file della memoria flash del proprio router Cisco e dei dispositivi flash USB collegati a tale router.

Pulsante Formatta

Fare clic sul pulsante **Formatta** per riformattare la memoria flash del router Cisco o riformattare un dispositivo flash USB collegato a tale router. Il pulsante **Formatta** è attivato solo se un'icona che rappresenta la memoria flash o un dispositivo flash USB del proprio router Cisco è selezionata nel lato sinistro della finestra.

Precauzione La riformattazione della memoria flash del router Cisco o di un dispositivo flash connesso a tale router consente di *eliminare* tutti i file presenti nel file system.

Pulsante Nuova cartella

Fare clic sul pulsante **Nuova cartella** per creare una nuova directory nella directory che è stata scelta sul lato sinistro della finestra. I nomi dei folder non possono contenere spazi o punti interrogativi ("?").

Pulsante Carica file dal PC

Fare clic sul pulsante **Carica file dal PC** per aprire una finestra di selezione dei file sul PC locale. Scegliere un file da salvare sulla directory scelta sulla memoria flash del router Cisco o un dispositivo flash USB collegato a tale router. I file Cisco SDM e i file con nomi contenenti spazi non possono essere caricati usando Carica file dal PC.

I file Cisco SDM come Cisco SDM.tar non possono essere caricati usando Carica file dal PC. I file Cisco SDM devono essere caricati tramite **Strumenti > Aggiorna SDM**.

Se si usa Carica file dal PC per caricare un file immagine di avvio, questo non può essere salvato nella directory del file immagine di avvio corrente.

Pulsante copia

Scegliere un file dal lato destro della finestra e fare clic sul pulsante **Copia** per copiarlo.

Pulsante incolla

Dopo avere fatto clic sul pulsante **Copia** per copiare un file, fare clic sul pulsante **Incolla** per posizionare la copia del file in una directory diversa. Scegliere la directory di destinazione dal lato sinistro della finestra. Non è possibile posizionare una copia del file nella stessa directory del file originale.

Pulsante Rinomina

Scegliere un file o una directory dal lato destro della finestra e fare clic sul pulsante **Rinomina** per modificare il nome. I nomi non possono contenere spazi o punti interrogativi (“?”).

Pulsante Elimina

Scegliere un file o una directory dal lato destro della finestra e fare clic sul pulsante **Elimina** per eliminarlo. Un file con icona di sola lettura accanto ad esso non può essere selezionato.

Nome

Fare clic su **Nome** per disporre file e cartelle in ordine alfabetico in base al nome. Facendo di nuovo clic su **Nome**, l'ordine viene invertito.

Dimensioni

Fare clic su **Dimensione** per ordinare i file e le directory in base alle dimensioni. La dimensione delle directory misura sempre zero byte, anche quando esse non sono vuote. Facendo di nuovo clic su **Dimensione**, l'ordine viene invertito.

Ora di modifica

Fare clic su **Ora di modifica** per ordinare i file e le directory in base alla data e l'ora di modifica. Facendo di nuovo clic su **Ora di modifica** l'ordine viene invertito.

Rinomina

In questa finestra è possibile rinominare un file della memoria flash del proprio router Cisco o dei dispositivi USB collegati a tale router.

Immettere il nuovo nome file nel campo Nuovo nome. Il percorso per la posizione del file è visualizzato sopra al campo Nuovo nome.

Nuova cartella

In questa finestra è possibile nominare e creare un nuovo folder nel sistema delle directory della memoria flash del proprio router Cisco e dei dispositivi USB collegati a tale router.

Immettere il nome della nuova cartella nel campo Nome cartella. Il percorso per la posizione della cartella è visualizzato sopra al campo Nome cartella.

Salva SDF su PC

Se si sta lavorando in IPS è possibile salvare sul PC il file di definizione delle firme SDF su cui si sta lavorando. Spostarsi nella directory in cui si desidera salvare il file e fare clic su **Salva**.

Esci

Consente di uscire da Cisco Router and Security Device Manager.

Impossibile eseguire la compressione del contenuto della memoria flash

Questa finestra viene visualizzata quando il router non è in grado di eseguire una compressione del contenuto della memoria flash poiché non è mai stato sottoposto a un'operazione **erase flash:**. In questo argomento della Guida viene descritto come scaricare i file necessari prima di eseguire l'operazione **erase flash:**, come effettuare l'operazione **erase flash:**, come caricare di nuovo i file nel router e riconnettersi successivamente a Cisco SDM.

Se si esegue il comando **erase flash:** verranno eliminati Cisco SDM e l'immagine Cisco IOS dalla Memoria Flash del router e si interromperà la connessione al router. È necessario stampare i contenuti di questa sezione in modo da poter utilizzare tutte le istruzioni per avere un'immagine CISCO IOS e SDM.tar da CISCO.com e quindi installarli sul router.

Passo 1 Assicurarsi che il router sia collegato, altrimenti dopo l'operazione di **erase flash:** non sarà presente alcuna immagine Cisco IOS in memoria.

Nota Se dopo l'operazione del comando erase flash il router non è collegato, per il ripristino è possibile utilizzare la procedura al seguente indirizzo: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/sw_conf/37_swcf/appendc.htm#xtocid11 (in inglese)

Passo 2 Salvare la configurazione del router in esecuzione in un file del computer facendo clic su **File > Salva configurazione in esecuzione su computer** e immettendo un nome di file.

Passo 3 Preparare un server TFTP in cui è possibile salvare i file e copiarli nel router. È necessario disporre di un accesso in scrittura al server TFTP. Se si dispone di un'applicazione server TFTP, è possibile utilizzare il computer a tale scopo.

Passo 4 Utilizzare il comando **tftpcopy** per copiare l'immagine Cisco IOS, il file SDM.tar e il file SDM.shtml dalla memoria flash in un server TFTP:

copy flash: tftp://*indirizzo-server tftp/nome file*

Esempio:

```
copy flash: tftp://10.10.10.3/SDM.tar
```

Nota Se si preferisce scaricare un'immagine Cisco IOS, il file SDM.tar e il file SDM.shtml, seguire queste istruzioni per connettersi a Internet e scaricare un'immagine Cisco IOS, il file SDM.tar e il file SDM.shtml file supportati da Cisco SDM. Infine collocare questi file in un server TFTP.

a. Per ottenere un'immagine Cisco IOS dal Software Center di Cisco, fare clic sul seguente collegamento:

http://www.cisco.com/kobayashi/sw-center/ (in inglese)

b. Individuare un'immagine in grado di supportare le funzioni per la release 12.2(11)T o successive. Salvare il file nel server TFTP accessibile dal router.

c. Per i file SDM.tar e SDM.shtml utilizzare il collegamento riportato di seguito, quindi salvare questi file nel server TFTP.

http://www.cisco.com/go/sdm

Passo 5 Dal computer accedere al router con Telnet e immettere la modalità Attiva.

Passo 6 Immettere il comando **erase flash:** e confermare. L'immagine IOS del router, il file di configurazione, i file SDM.tar SDM.shtml vengono rimossi dalla memoria RAM non volatile (NVRAM).

Passo 7 Utilizzare il comando **tftpcopy** per copiare prima l'immagine IOS e poi il file SDM.tar dal server TFTP al router:

copy tftp://*tftp-server-indirizzo***/***nome file* **flash:**

Esempio:

```
copy tftp://10.10.10.3/ios_image_name flash:
! Sostituire nome_immagine_ios con il nome reale dell'immagine IOS
copy tftp://10.10.10.3/SDM.tar flash:
```

Passo 8 Avviare il browser Web e riconnettersi a Cisco SDM con lo stesso indirizzo IP utilizzato all'avvio della sessione Cisco SDM.

A questo punto, dopo l'esecuzione di **erase flash:** è possibile eseguire il comando **squeeze flash** se necessario.

CAPITOLO 41

Comandi del menu Modifica

Nel menu Modifica di Cisco Router and Security Device Manager (Cisco SDM) sono disponibili le opzioni riportate di seguito.

Preferenze

Questa schermata consente di configurare le opzionidi Cisco Router and Security Device Manager riportate di seguito.

Eseguire l'anteprima dei comandi prima dell'inoltro al router

Scegliere questa opzione se si vuole che Cisco SDM visualizzi una lista dei comandi di configurazione IOS Cisco generati prima che i comandi vengano inviati al router.

Salva file delle firme su flash

Scegliere questa opzione se si desidera che il file di definizione delle firme SDF, su cui si sta lavorando, sia salvato nella memoria flash del router, quando si fa clic su **Applica modifiche**.

Chiedere conferma prima di uscire da Cisco SDM

Impostazione predefinita in Cisco SDM. Selezionare questa opzione per consentire a Cisco SDM visualizzare una finestra di dialogo che chiede conferma prima di uscire da Cisco SDM.

Continuare a monitorare lo stato dell'interfaccia durante la modalità/attività di switching

Questo è il comportamento predefinito di Cisco SDM. Il monitoraggio dello stato delle interfacce da parte di Cisco SDM inizia quando si fa clic su **Controlla** e si seleziona **Stato dell'interfaccia**. Per fare in modo che Cisco SDM continui l'operazione anche se si lascia la modalità di controllo e si eseguono altre attività in Cisco SDM, selezionare questa casella di controllo e specificare il numero massimo di interfacce che si desidera monitorare tramite Cisco SDM. Il numero massimo è 4.

CAPITOLO 42

Comandi del menu Visualizza

Nel menu Visualizza di Cisco Router and Security Device Manager (Cisco SDM) sono disponibili le opzioni riportate di seguito.

Home

Consente di visualizzare la pagina principale di Cisco SDM, che fornisce informazioni sull'hardware e sul software del router nonché sulle configurazioni LAN, WAN, Firewall e VPN.

Configura

Consente di visualizzare la barra delle applicazioni di Cisco SDM, con cui è possibile eseguire configurazioni manuali e guidate delle interfacce, delle connessioni, dei firewall, delle ACL, del routing VPN e di altre attività.

Controlla

Consente di visualizzare la finestra Controlla di Cisco SDM, in cui è possibile consultare le statistiche sul router e la rete.

Configurazione in corso

Consente di visualizzare la configurazione corrente del router.

Mostra comandi

Consente di visualizzare la finestra di dialogo Mostra comandi, in cui è possibile eseguire i comandi **show** di Cisco IOS sul router, visualizzarne l'output e salvarlo sul PC. Il file di output viene salvato con il nome di file predefinito show_<*comando*>[*indirizzo_ip_router*].

La finestra di dialogo Mostra comandi può visualizzare l'output dei comandi **show** riportati di seguito.

- **show flash**: visualizza il contenuto della memoria Flash del router.
- **show startup-config**: visualizza il file di configurazione per l'avvio del router.
- **show access-lists**: visualizza tutti i comandi degli elenchi di controllo di accesso configurati sul router.
- **show diag**: visualizza le informazioni sull'hardware installato nel router.
- **show interfaces**: visualizza le informazioni sulla configurazione di ciascuna interfaccia e sui pacchetti trasferiti nell'interfaccia stessa.
- **show protocols**: visualizza le informazioni relative ai protocolli di rete configurati su ciascuna interfaccia.
- **show version**: visualizza le informazioni relative alla versione del software Cisco IOS installato sul router.
- **show tech-support**: mostra l'output di tutti gli altri comandi **show**.
- **show environment**: mostra le informazioni sull'alimentazione elettrica del router. Questo comando potrebbe non essere visualizzato nell'elenco a discesa **Mostra comandi** se non è supportato dal router.

Regole Cisco SDM predefinite

La finestra Regole Cisco SDM predefinite consente di visualizzare un elenco di tutte le regole predefinite configurate da Cisco SDM. Sul lato sinistro della finestra è inclusa una struttura ad albero in cui sono visualizzate le seguenti opzioni: Regole di accesso, Firewall, VPN - IKE Policy e VPN - Set di trasformazione. Per visualizzare le regole predefinite di queste opzioni, fare clic sull'opzione desiderata nella struttura (le regole predefinite appariranno sul lato destro). Per maggiori informazioni sulle regole, vedere le descrizioni che seguono.

Regole di accesso

Mostra tutte le regole ACL (Access Control List) predefinite e una breve descrizione di ciascuna.

Firewall

Mostra i criteri predefiniti di Protezione applicazioni predefiniti di Cisco SDM. Scegliere il criterio che si vuole visualizzare dalla lista nell'angolo superiore sinistro della finestra.

- SDM_HIGH—Questo criterio impedisce l'uso di Applicazioni di Instant Messaging e Point-to-Point sulla rete. Esso monitora il traffico HTTP e e-mail e blocca il traffico che non è conforme ai protocolli utilizzati. Permette il traffico TCP e UDP per le sessioni iniziate all'interno del firewall.
- SDM_MEDIUM—Questo criterio sottopone a monitoraggio l'uso di Applicazioni di Instant Messaging e Point-to-Point, e il traffico HTTP e email. Permette il traffico TCP e UDP per le sessioni iniziate all'interno del firewall.
- SDM_LOW—Questo criterio non effettua il monitoraggio del traffico delle applicazioni. Permette il traffico TCP e UDP per le sessioni iniziate all'interno del firewall.

VPN – IKE Policy

Consente di visualizzare le policy IKE (Internet Key Exchange) predefinite.

VPN - Set di trasformazione

Consente di visualizzare i set di trasformazione IPSec (IP Security).

Aggiorna

Consente di ricaricare le informazioni di configurazione dal router. Se uno dei comandi non è stato inviato, Cisco SDM visualizza un messaggio in cui si avvisa che in caso di aggiornamento, tutti i comandi non inviati verranno persi. Se si desidera inviare i comandi, fare clic su **No** in questa finestra, quindi scegliere **Invia** nella barra degli strumenti di Cisco SDM.

CAPITOLO 43

Comandi del menu Strumenti

Nel menu Comandi di Cisco Router and Security Device Manager (Cisco SDM) sono disponibili le opzioni riportate di seguito.

Esegui ping

Consente di visualizzare la finestra di dialogo Esegui ping, in cui è possibile inviare un messaggio ping a un altro dispositivo di rete. Per maggiori informazioni sull'uso della finestra Esegui ping, vedere la sezione Genera mirroring....

Telnet

Consente di visualizzare la finestra di dialogo Telnet di Windows, in cui è possibile connettersi al router e accedere all'interfaccia della riga di comando (CLI) di Cisco IOS mediante il protocollo Telnet.

Security Audit

Consente di visualizzare la finestra Security Audit di Cisco SDM. Per maggiori informazioni vedere la sezione Security Audit.

Impostazioni del PIN del token USB

Le impostazioni del PIN del token USB consente di impostare i PIN per i token USB connessi al router.

Selezionare un tipo di PIN

Scegliere **PIN utente** per impostare un PIN utente o **PIN amministratore** per impostare un PIN amministratore.

I PIN utente sono utilizzati per l'accesso al router. Se si collega un token USB a un router e il nome del token e il PIN utente corrispondono ad una voce in **Configura > VPN > Componenti VPN > Infrastruttura chiave pubblica > Token USB**, si viene automaticamente connessi a tale router.

I PIN amministratore sono usati per gestire le impostazioni dei token USB usando il software del produttore. Cisco SDM consente la modifica del USB amministratore di un token PIN se si può fornire il PIN amministratore corrente.

Nome del Token

Immettere il nome del token USB

Il nome del token è impostato dal produttore Per esempio, i token USB prodotti dalla Aladdin Knowledge Systems sono chiamati eToken.

È anche possibile utilizzare il nome “usbtoken*x*”, dove *x* è il numero della porta USB alla quale il token USB è connesso. Per esempio un token USB connesso alla porta USB 0 si chiamerà usbtoken0.

PIN corrente

Immettere il PIN utente o amministratore corrente. Se non si conosce il PIN corrente si deve usare il software del produttore del token USB per identificarlo.

Nuovo PIN

Immettere un nuovo PIN del token USB. Il PIN esistente sarà sostituito dal nuovo PIN. Il nuovo PIN deve contenere almeno 4 cifre.

Conferma PIN

Reimmettere il nuovo PIN per confermarlo.

Salva il nuovo PIN sul router

Selezionare la casella di controllo **Salva il nuovo PIN sul router** se si vuole salvare il nuovo PIN come voce in **Configura > VPN > Componenti VPN > Infrastruttura chiave pubblica > Token USB**. Se esiste già una voce con lo stesso nome in **Configura > VPN > Componenti VPN > Infrastruttura chiave pubblica > Token USB**, essa viene sostituita da quella nuova.

La casella di controllo **Salva il PIN sul router** è disponibile soltanto per i PIN utente.

Applicazione wireless

Se il router è dotato di interfacce radio, è possibile avviare l'Applicazione wireless per configurare e monitorare tali interfacce. Cisco SDM può semplificare la configurazione e la visualizzazione dell'indirizzo IP o i dettagli di bridging relativi a un'interfaccia radio ma è necessario utilizzare l'Applicazione wireless per impostare altri parametri di configurazione.

Aggiorna Cisco SDM

In Cisco SDM è possibile ottenere e installare automaticamente un aggiornamento.

Aggiorna Cisco SDM da Cisco.com

Cisco SDM può essere aggiornato direttamente dal sito Web di Cisco. Cisco SDM verifica la presenta di versioni disponibili e informa l'utente se esiste un aggiornamento rispetto alla versione installata sul router. È possibile aggiornare Cisco SDM mediante la procedura di aggiornamento guidata.

Per aggiornare Cisco SDM da Cisco.com:

Passo 1 Selezionare Aggiorna Cisco SDM da Cisco.com nel menu Strumenti per avviare la procedura di aggiornamento guidata.

Passo 2 Utilizzare la procedura guidata per scaricare i file Cisco SDM e copiarli nel router.

Aggiorna Cisco SDM dal computer locale

Cisco SDM può essere aggiornato utilizzando un file SDM.zip scaricato dal sito Web Cisco. Cisco SDM fornisce una procedura guidata di aggiornamento che copierà i file necessari sul router.

Per aggiornare Cisco SDM dal computer stesso in cui è installato Cisco SDM seguire la procedura riportata di seguito:

Passo 1 Scaricare il file sdm-v*nn*.zip dall'URL seguente:

`http://www.cisco.com/cgi-bin/tablebuild.pl/sdm`

Se esiste più di un file Cisco SDM.zip, scaricare la copia con il numero di versione più recente.

Passo 2 Utilizzare la procedura di aggiornamento guidata per copiare i file Cisco SDM dal computer al router.

Aggiorna Cisco SDM da CD

Se si dispone del CD di Cisco SDM, è possibile utilizzarlo per aggiornare la versione di Cisco SDM installata sul router mediante la procedura seguente:

Passo 1 Inserire il CD di Cisco SDM nell'unità CD-ROM del computer.

Passo 2 Selezionare **Aggiorna Cisco SDM da CD** e fare clic su **Aggiorna Cisco SDM** nella finestra Istruzioni generali dopo aver letto il testo.

Passo 3 Cisco SDM consentirà di individuare il file SDM-Updates.xml. nel CD. Una volta trovato, fare clic su **Apri**.

Passo 4 Seguire le istruzioni dell'installazione guidata.

Accesso CCO

Per accedere a questa pagina web è necessario fornire un accesso CCO. Indicare un nome utente e una password, quindi fare clic su OK.

Se non si dispone di un accesso CCO e di una password, è possibile ottenerli aprendo il browser e collegandosi al sito web di Cisco al seguente indirizzo:

http://www.cisco.com

Quando si apre la pagina web, fare clic su Registra e fornire le informazioni necessarie per ottenere un nome utente e una password. Quindi, ripetere questa operazione.

CAPITOLO 44

Comandi del menu ?

Nel menu ? di Cisco Router and Security Device Manager (Cisco SDM) sono disponibili le opzioni riportate di seguito.

Argomenti della Guida

Consente di visualizzare la Guida in linea di Cisco SDM. Il sommario della Guida in linea di Cisco SDM viene visualizzato nel frame di sinistra.

Cisco SDM su CCO

Consente di aprire un browser e di visualizzare la pagina Cisco SDM sul sito Web Cisco.com.

Matrice hardware/software

Consente di aprire un browser e di visualizzare una matrice dei modelli di router Cisco e delle versioni di immagine Cisco IOS per supportare l'utente nella selezione di un'immagine software Cisco IOS compatibile. Per l'accesso alla matrice, vengono richiesti un nome utente e una password di Cisco Connection Online.

Informazioni sul router...

Consente di visualizzare informazioni sull'hardware e sul software del router in cui è in esecuzione Cisco SDM.

Informazioni su Cisco SDM

Consente di visualizzare informazioni su Cisco SDM.

GLOSSARIO

Simboli e valori numerici

3DES DES triplo. Algoritmo di crittografia in cui vengono utilizzate tre chiavi di crittografia DES a 56 bit (ovvero 168 bit) in rapida successione. È disponibile anche una versione 3DES alternativa che consente di utilizzare solo due chiavi DES a 56 bit, dove una chiave viene utilizzata due volte, generando una lunghezza chiave pari a 112 bit. Opzione valida solo per gli Stati Uniti. Vedere DES.

802.1x 802.1x è uno standard IEEE per il controllo degli accessi a livello di supporto, che consente di autorizzare o negare la connettività di rete, di controllare l'accesso VLAN e applicare criteri di traffico, in base all'identità dell'utente o della macchina.

A

AAA Acronimo di Authentication, Authorization e Accounting (autenticazione, autorizzazione e accounting). Definito “A tripla”.

AAL5-MUX Acronimo di ATM Adaptation Layer 5 Multiplexing.

AAL5-SNAP Acronimo di ATM Adaptation Layer 5 Subnetwork Access Protocol.

ACE Acronimo di Access Control Entry (voce di controllo di accesso). Una voce è un'ACL che specifica un host o una rete di origine e se il traffico da tale host è consentito o meno. Un ACE può inoltre specificare un host o una rete di destinazione e il tipo di traffico.

ACL Acronimo di Access Control List (lista di controllo degli accessi). Informazioni su un dispositivo che specifica le entità alle quali è consentito l'accesso a tale dispositivo o alle reti sottostanti. Gli elenchi di controllo di accesso sono costituiti da una o più voci del controllo di accesso (ACE).

ACS Acronimo di Cisco Secure Access Control Server. Software Cisco che può implementare un server RADIUS o un server TACACS+. L'ACS viene utilizzato per memorizzare database di criteri utilizzati da Easy VPN, NAC e da altre funzioni che controllano l'accesso alla rete.

ADSL Acronimo di Asymmetric Digital Subscriber Line.

AH Acronimo di Authentication Header. Protocollo IPSec non recente e poco rilevante nella maggior parte delle reti rispetto al protocollo ESP, in quanto fornisce servizi di autenticazione ma non di crittografia. Viene utilizzato per garantire la compatibilità con i peer IPSec che non supportano il protocollo ESP, che fornisce invece entrambi i servizi di autenticazione e crittografia.

AH-MD5-HMAC Authentication Header con l'algoritmo hash MD5 (variante HMAC).

AHP Acronimo di Authentication Header Protocol. Protocollo in grado di fornire l'autenticazione host di origine e l'integrità dei dati. Tale protocollo non garantisce tuttavia la riservatezza.

AH-SHA-HMAC Authentication Header con l'algoritmo hash SHA (variante HMAC).

algoritmo Sequenza logica di processi per la risoluzione di un problema. Algoritmi di protezione relativi all'autenticazione o alla crittografia dei dati.

DES e 3DES rappresentano due esempi di algoritmi di crittografia dei dati.

Tra gli esempi di algoritmi di crittografia e decrittazione sono inclusi block cipher, CBC, null cipher e stream cipher.

Gli algoritmi di autenticazione includono hash, quali MD5 e SHA.

algoritmo hash Algoritmo utilizzato per generare un valore di hash, conosciuto anche come digest di messaggio, che garantisce che il contenuto del messaggio non venga modificato durante la trasmissione. I due tipi di algoritmi hash più diffusi sono Secure Hash Algorithm (SHA) e MD5.

AMI Acronimo di Alternate Mark Inversion.

ARP Acronimo di Address Resolution Protocol. Protocollo TCP/IP di livello inferiore che consente di eseguire la mappatura di un indirizzo hardware di nodi (definito *indirizzo MAC*) per l'indirizzo IP.

ASA Acronimo di Adaptive Security Algorithm. Abilita le connessioni unidirezionali (da interne a esterne) senza che sia necessaria una configurazione esplicita per ciascun applicazione o sistema interno.

ATM Acronimo di Asynchronous Transfer Mode. Standard internazionale per l'inoltro di cellule in cui più tipi di servizi (ad esempio, voce, video e dati) vengono trasferiti in cellule di lunghezza fissa (53 byte). Le cellule di lunghezza fissa consentono l'elaborazione di cellule in dispositivi hardware, riducendo pertanto eventuali ritardi di transito.

Attacco TCP SYN flooding Un attacco SYN flooding si verifica quando un hacker congestiona un server con una sequenza continua di richieste di connessione. Poiché questi messaggi presentano indirizzi di ritorno non raggiungibili, non è possibile effettuare alcuna connessione. Il risultante volume di connessioni aperte non risolte congestiona il server, che può rifiutarsi di servire le richieste provenienti dagli altri utenti. Di conseguenza risulta impossibile connettersi a un sito Web, accedere alla posta elettronica, utilizzare il servizio FTP e così via.

autenticare Verificare la veridicità di un'identità.

autenticazione In relazione alla protezione, si tratta di verificare l'identità di un utente o di un processo. L'autenticazione consente di stabilire l'integrità di un flusso di dati, garantendo che non sia stato alterato durante il tragitto e confermando l'origine del flusso di dati.

autenticazione dell'origine dati Funzione di un servizio di non-rifiuto.

B

bit di rete — In una subnet mask, numero di bit impostati sui numeri 1 binari. Una subnet mask di 255.255.255.0 è costituita da 24 bit di rete, in quanto i 24 bit della maschera sono impostati su 1. Una subnet mask di 255.255.248 invece è costituita da 17 bit di rete.

bit di subnet

subnet mask — Maschera di indirizzo a 32 bit utilizzata nel protocollo Internet per indicare i bit di un indirizzo IP utilizzati per l'indirizzo di rete e della subnet opzionale. Le subnet mask sono espresse in numeri decimali. La maschera 255.255.255.0 specifica che i primi 24 dell'indirizzo. Talvolta viene semplicemente definita maschera. Vedere anche maschera di indirizzo e indirizzo IP.

blocco — Sequenza di lunghezza fissa di bit.

block cipher — Algoritmo di crittografia in cui viene utilizzata una cifratura simmetrica a 64 bit per l'utilizzo con blocchi di dati di dimensione fissa. Vedere cipher.

BOOTP — Acronimo di Bootstrap Protocol. Protocollo utilizzato da un nodo di rete per stabilire l'indirizzo IP delle interfacce Ethernet per l'avvio della rete.

burst rate — Numero di byte che non deve essere superato da un burst di traffico.

C

C3PL — Acronimo di Cisco Common Classification Policy Language. C3PL è una sostituzione strutturata di comandi di configurazione specifici delle funzioni e consente alle funzioni configurabili di essere espresse in termini di eventi, condizioni e azioni.

CA — Acronimo di Certification Authority. Terza parte trusted che ha il compito di emettere e/o revocare certificati digitali. Può essere a volte definita come *notaio* o *autorità certificante*. Nell'ambito di un dominio di una Certification Authority specifica, è sufficiente disporre per ciascun dispositivo del certificato e della chiave pubblica di CA corrispondenti per autenticare qualsiasi altro dispositivo di tale dominio.

Certificato CA Certification Authority finale che firma i certificati delle CA secondarie. La CA principale dispone di un certificato autofirmato che contiene una propria chiave pubblica.

cache Archivio temporaneo di informazioni relative ad attività eseguite in precedenza che è possibile riutilizzare, riducendo pertanto i tempi di esecuzione delle attività.

caratteri di riempimento Nei sistemi di crittografia, il termine *caratteri di riempimento* si riferisce a caratteri, spazi vuoti, zeri e valori null casuali aggiunti all'inizio e alla fine di messaggi per compensare la rispettiva lunghezza effettiva o per soddisfare i requisiti della dimensione del blocco dati di alcune crittografie. Questi caratteri nascondono anche la posizione in cui ha inizio di fatto la codifica crittografica.

CBAC Acronimo di Context-Based Access Control. Protocollo che offre agli utenti interni un controllo di accesso protetto a ciascuna applicazione e a tutto il traffico dei perimetri di rete. CBAC consente di esaminare gli indirizzi di origine e destinazione e di tenere traccia di ogni stato di connessione dell'applicazione.

CDP Acronimo di Cisco Discovery Protocol. Protocollo per il rilevamento di dispositivi indipendenti da protocolli e supporti che viene eseguito su tutte le apparecchiature prodotte da Cisco inclusi router, server di accesso, bridge e switch. Mediante CDP, è possibile notificare la presenza di un dispositivo ad altri dispositivi, oltre a ricevere informazioni su altri dispositivi nella stessa LAN o nel sito remoto di una WAN.

CDP Certificate Revocation List Distribution Point (Punto di distribuzione elenchi di revoca certificati). Percorso dal quale è possibile recuperare un CRL (Certificate Revocation List). Solitamente un CDP è un URL HTTP o LDAP

CEP Acronimo di Certificate Enrollment Protocol. Protocollo per la gestione dei certificati. Consiste in un'implementazione precedente di Certificate Request Syntax (CRS), lo standard definito da Internet Engineering Task Force (IETF). CEP specifica la modalità di comunicazione di un dispositivo con una CA, incluse le modalità per recuperare la chiave pubblica della CA, registrare un dispositivo con la CA e recuperare l'elenco certificati revocati (CRL). Vengono utilizzati gli standard PKCS (Public Key Cryptography Standards) 7 e 10 come tecnologie di componenti principali. Il gruppo di lavoro relativo all'infrastruttura a chiave pubblica (PKIX) di IETF è impegnato nel definire gli standard di un protocollo specifico per tali funzionalità, CRS o equivalente. Una volta stabilito lo standard IETF, Cisco fornirà il proprio supporto. CEP è stato sviluppato congiuntamente da Cisco Systems e VeriSign, Inc.

certificato Vedere certificato digitale.

Certificato CA Certificato digitale concesso a una Certification Authority da parte di un'altra Certification Authority.

Certificato di firma Utilizzato per associare la firma digitale ai messaggi e ai documenti e per garantire che tali file arrivino a destinazione senza subire modifiche.

certificato digitale Rappresentazione digitale, firmata a livello di crittografia degli attributi di utenti o dispositivi che collegano una chiave a un'identità. Un certificato unico allegato a una chiave pubblica garantisce che la chiave non sia stata compromessa. Un certificato viene emesso e firmato da una Certification Authority trusted che associa una chiave pubblica al proprietario corrispondente. I certificati generalmente includono il nome, la chiave pubblica del proprietario, il numero di serie e la data di scadenza del certificato. È possibile tuttavia che siano disponibili anche altre informazioni. Vedere X.509.

Certificato X.509 Certificato digitale strutturato secondo le indicazioni dello standard X.509.

CET Acronimo di Cisco Encryption Technology. Crittografia proprietaria a livello di rete disponibile in Cisco IOS Release 11.2. CET garantisce la crittografia dei dati di rete a livello di pacchetti IP e consente di implementare gli standard seguenti: DH, DSS e DES a 40 e 56 bit.

CHAP Acronimo di Challenge Handshake Authentication Protocol. Funzionalità di protezione supportata su linee in cui si utilizza l'incapsulamento PPP per prevenire accessi non autorizzati. Con CHAP non è possibile prevenire un accesso non autorizzato, bensì tale protocollo consente di identificare l'estremità remota. In seguito il router o il server di accesso determina se l'utente è autorizzato a ottenere l'accesso. Vedere anche PAP.

chargen Acronimo di Character Generation. Mediante protocollo TCP, servizio che invia un continuo flusso di caratteri fino a quando non viene arrestato dal client. Mediante protocollo UDP, il server invia un numero casuale di caratteri a ogni invio di un datagramma da parte del client.

checksum Metodo di calcolo per il controllo dell'integrità dei dati trasmessi, ottenuto in base a una sequenza di ottetti che derivano da una serie di operazioni aritmetiche. Il destinatario ricalcola tale valore che viene quindi confrontato a scopo di verifica.

chiave Stringa di bit utilizzata per crittografare e decrittografare dati oppure per calcolare digest di messaggio.

chiave concordata Processo con cui due o più parti si accordano sull'utilizzo della stessa chiave simmetrica segreta.

chiave di sessione Chiave utilizzata una sola volta.

chiave distribuita Chiave di crittografia condivisa che viene suddivisa in più parti, ciascuna delle quali viene fornita a un diverso partecipante.

chiave precondivisa Uno dei tre metodi di autenticazione fornito in IPSec; gli altri due metodi sono RSA con crittografia nonce e firma RSA. Le chiavi precondivise consentono a più client di utilizzare segreti condivisi individuali per autenticare tunnel crittografati per un gateway tramite IKE. Chiavi di questo tipo sono comunemente utilizzate in reti di piccole dimensioni con un numero massimo di 10 client. Con le chiavi precondivise non è necessario l'utilizzo di CA per la protezione.

Lo scambio di chiavi Diffie-Hellman combina chiavi pubbliche e chiavi private per creare un segreto condiviso da utilizzare per l'autenticazione tra i peer IPSec. Il segreto condiviso può essere condiviso tra due o più peer. In ogni peer partecipante, è necessario specificare un segreto condiviso come parte di una IKE Policy. La distribuzione della chiave precondivisa avviene solitamente tramite un canale fuori banda protetto. Quando si utilizza una chiave precondivisa, se uno dei peer partecipanti non è configurato con la stessa chiave, il SA IKE non può essere stabilito. SA IKE è un prerequisito per un SA IPSec. È necessario configurare la chiave precondivisa in tutti i peer.

La certificazione digitale e le chiavi precondivise con caratteri jolly (che consentono l'utilizzo di un segreto condiviso a più client per autenticare tunnel crittografati per un gateway) sono alternative alle chiavi precondivise. La certificazione digitale e le chiavi precondivise con caratteri jolly offrono una scalabilità superiore alle chiavi precondivise.

chiave precondivisa Chiave segreta condivisa fra tutti gli utenti in una sessione di comunicazione basata su chiavi simmetriche.

chiave privata Vedere crittografia con chiave pubblica.

chiave RSA Coppia di chiavi asimmetriche RSA che forma un set di chiavi pubbliche e private corrispondenti.

chiave segreta Vedere chiave simmetrica.

chiave simmetrica Le chiavi simmetriche sono utilizzate per decrittografare le informazioni precedentemente crittografate.

chiavi asimmetriche Coppia di chiavi di crittografia correlate matematicamente. La chiave pubblica consente di crittografare le informazioni che possono essere decrittografate solo mediante la chiave privata e viceversa. La chiave privata inoltre assegna i dati che possono essere autenticati solo mediante la chiave pubblica.

ciclo di vita Vedere data di scadenza.

cipher Algoritmo di crittografia e decrittazione.

ciphertext Dati crittografati, illeggibili precedenti alla decrittazione.

Cisco SDM Cisco Router and Security Device Manager. Cisco SDM è uno strumento software basato sul browser Internet progettato per configurare LAN, WAN e funzionalità di protezione in un router. Per maggiori informazioni vedere la sezione Guida introduttiva.

classificazione di fedeltà Numero da 1 a 100 che indica l'affidabilità rispetto alla generazione di un avviso accurato da parte di una firma.

clear channel Canale tramite il quale è possibile trasferire il traffico non crittografato. Tali canali non offrono alcuna limitazione in merito alla protezione dei dati trasmessi.

cleartext Testo decrittografato, definito anche *plaintext* (testo normale).

CLI Acronimo di Command-Line Interface (interfaccia della riga di comando). Interfaccia primaria per l'impostazione dei comandi di configurazione e monitoraggio nel router. Per ulteriori informazioni sui comandi che è possibile immettere tramite l'interfaccia CLI, consultare la guida di configurazione del router in uso.

CNS Acronimo di Cisco Networking Services. Suite di servizi che supporta l'implementazione e la configurazione di reti scalabili, il monitoraggio di garanzia e la fornitura del servizio.

comp-lzs Algoritmo di compressione IP.

Configurazione, Config, file di configurazione File del router che contiene impostazioni, preferenze e proprietà che è possibile gestire mediante Cisco SDM.

connessione VPN VPN site-to-site. Collegamento costituito da un insieme di connessioni VPN fra peer. Gli attributi di definizione delle connessioni sono caratterizzati dalle seguenti informazioni di configurazione del dispositivo:

- Un nome di connessione
- Una IKE Policy e una chiave precondivisa (opzionale)
- Un peer IPSec
- Un elenco di una o più subnet remote o host protetti dalla connessione
- Una regola IPSec che definisce il traffico da crittografare
- Un elenco di set di trasformazione che definisce il modo in cui crittografare il traffico protetto
- Un elenco delle interfacce di rete del dispositivo con cui stabilire la connessione

Contesto VPN SSL Un contesto WebVPN fornisce le risorse necessarie per configurare un accesso protetto all'Intranet aziendale e ad altri tipi di reti private. Un contesto WebVPN deve comprendere un gateway WebVPN associato. Un contesto WebVPN può servire uno o più criteri di gruppo WebVPN.

controllo di accesso, regola del controllo di accesso Informazioni immesse durante la configurazione che consentono di specificare il tipo di traffico da autorizzare o negare in un'interfaccia. Per impostazione predefinita, viene negato il traffico non autorizzato in modo esplicito. Le regole del controllo di accesso sono costituite dalle voci del controllo di accesso (ACE).

conversione indirizzi Conversione di un indirizzo di rete e/o della porta in un altro indirizzo o porta di rete. Vedere anche Indirizzo IP, NAT, PAT, PAT statico.

cookie Funzionalità del browser Web che consente di archiviare o recuperare informazioni, quali le preferenze di un utente, nella memoria permanente. In Netscape e Internet Explorer, l'implementazione dei cookie avviene mediante il salvataggio di un piccolo file di testo nel disco rigido locale. Tale file può essere caricato al successivo avvio di un applet Java o visitando un sito Web. In questo modo, è possibile salvare tra le sessioni le informazioni univoche per un utente. La dimensione massima di un cookie è pari a circa 4 KB.

coppia di chiavi Vedere crittografia con chiave pubblica.

coppia di zone Una coppia di zone consente di specificare un flusso di traffico unidirezionali tra due zone di protezione. Vedere anche zona di protezione

CPE Acronimo di Customer Premises Equipment.

criterio di mirroring VPN

Criterio VPN su un sistema remoto che contiene valori compatibili con un criterio locale e che consente al sistema remoto di stabilire una connessione VPN con il sistema locale. Alcuni valori del criterio di mirroring devono corrispondere ai valori del criterio locale mentre invece altri valori, come ad esempio l'indirizzo IP del peer, devono essere l'opposto dei valori omologhi del criterio locale.

È possibile creare criteri di mirroring utilizzabili dagli amministratori remoti quando si configurano connessioni VPN tra siti. Per ulteriori informazioni sulla creazione di criteri di mirroring, vedere Genera mirroring....

Criterio gruppo VPN SSL

I criteri di gruppo WebVPN consentono di definire la pagina del portale e i collegamenti per gli utenti inclusi nei criteri. Un criterio di gruppo WebVPN viene configurato nel contesto WebVPN.

criterio IPSec

In Cisco SDM, un criterio IPSec è un set denominato di mappa crittografica associato a una connessione VPN.

crittografare

Convertire a livello crittografico testo normale in testo crittografato.

crittografia

Tecniche matematiche e scientifiche applicate per garantire che i dati siano riservati, autenticati, invariati e che non vengano rifiutati.

crittografia

Applicazione di un algoritmo specifico ai dati al fine di alterarne l'aspetto, rendendoli non leggibili a coloro che non dispongono dell'autorizzazione a visualizzare tali informazioni.

crittografia asimmetrica

Definito anche *sistema a chiave pubblica*, questo approccio consente a tutti gli utenti di ottenere l'accesso alla chiave pubblica di qualsiasi altro utente e pertanto di inviare un messaggio crittografato alla persona che utilizza la chiave pubblica.

crittografia con chiave pubblica

Nei sistemi di crittografia con chiave pubblica, gli utenti dispongono sia di una chiave pubblica che di una privata. Ogni chiave privata appartiene a un unico utente e non è condivisa. La chiave privata è utilizzata per generare una firma digitale univoca e per decrittografare le informazioni crittografate con la chiave pubblica. Viceversa, la chiave pubblica di un utente è disponibile a tutti per crittografare le informazioni destinate a quell'utente, o per verificare la firma digitale di quell'utente. Talvolta denominata codifica con chiave pubblica.

CRL Acronimo di Certification Revocation List (elenco certificati revocati). Elenco gestito e firmato da una Certificate Authority (CA) contenente tutti i certificati digitali non scaduti ma revocati.

CRL (Certificate Revocation List, elenco certificati revocati) X.509 Elenco di numeri di certificati revocati. Gli elenchi CRL X.509 sono conformi a una delle due definizioni di formattazione di CRL presentate nello standard X.509.

D

data di scadenza Data di un certificato o di una chiave che ne indica la scadenza. Una volta superata tale data, il certificato o la chiave non sarà più considerato trusted.

decrittazione Applicazione inversa di un algoritmo di crittografia ai dati crittografati, al fine di ripristinare i dati allo stato originale e non crittografato.

DES Acronimo di Data Encryption Standard. Algoritmo di crittografia standard sviluppato e definito da U.S. National Institute of Standards and Technology (NIST). Viene utilizzata una chiave di crittografia segreta a 56 bit. L'algoritmo DES è incluso in numerosi standard di crittografia.

DH, Diffie-Hellman Protocollo di crittografia a chiave pubblica che consente a due parti di stabilire un segreto condiviso su canali di comunicazione non protetti. Diffie-Hellman viene utilizzato in Internet Key Exchange (IKE) per stabilire delle chiavi di sessione. Tale protocollo è inoltre un componente di uno scambio di chiavi Oakley.

DHCP Acronimo di Dynamic Host Configuration Protocol. Fornisce un processo per l'assegnazione di indirizzi IP a host in maniera dinamica, affinché sia possibile riutilizzare gli indirizzi una volta che non sono più necessari.

digest Output di una funzione hash.

digest di messaggio Stringa di bit che rappresenta un blocco di dati di grandi dimensioni. Tale stringa definisce un blocco di dati, in base all'elaborazione del contenuto esatto mediante una funzione di hash a 128 bit. I digest di messaggio vengono utilizzati durante la creazione di firme digitali. Vedere hash.

DLCI Acronimo di Data-Link Connection Identifier (identificatore connessione collegamento dati). Nelle connessioni Frame Relay, identificatore di una specifica connessione di collegamento dati tra due endpoint.

DMVPN Acronimo di Dynamic Multipoint Virtual Private Network. Rete privata virtuale in cui i router sono disposti in base a una topologia hub and spoke logica e in cui gli hub dispongono di connessioni GRE su IPSec point-to-point. In DMVPN vengono utilizzati GRE e NHRP per abilitare il flusso di pacchetti alle destinazioni di rete.

DMVPN singola Router con una configurazione DMVPN singola che dispone di una connessione a un hub DMVPN e di un tunnel GRE configurato per le comunicazioni DMVPN. Gli indirizzi del tunnel GRE per topologie hub and spoke devono trovarsi sulla stessa subnet.

DMZ Acronimo di Demilitarized Zone (zona demilitarizzata). Area cuscinetto tra la rete Internet e le reti private. Può trattarsi di una rete pubblica generalmente utilizzata per server Web FTP e di posta elettronica a cui è possibile accedere da client esterni in Internet. Posizionando questi server ad accesso pubblico in una rete separata isolata, è possibile ottenere un ulteriore livello di protezione della rete interna.

DN Acronimo di Distinguished Name (nome distinto). Identificatore univoco per un cliente dell'autorità di certificazione, che viene incluso in ogni certificato del cliente ricevuto dall'autorità. Il nome DN generalmente include i seguenti dati relativi all'utente: il nome comune, il nome della società o dell'organizzazione, il codice del paese a due cifre, un indirizzo di posta elettronica di contatto, il numero di telefono, il numero del reparto e la città di residenza.

DNS Acronimo di Domain Name System (o Service). Servizio Internet che converte i nomi di dominio, composti da lettere, in indirizzi IP, composti invece da numeri.

DPD rilevamento peer inattivo. Il DPD determina se un peer è ancora attivo inviando regolarmente messaggi keepalive a cui è previsto che il peer risponda. Se il peer non risponde entro un determinato periodo di tempo, la connessione viene terminata.

DRAM Acronimo di Dynamic Random Access Memory. Memoria RAM che consente di archiviare informazioni in condensatori che necessitano di un aggiornamento periodico.

DSCP Acronimo di Differentiated Services Code Point. I contrassegni DSCP possono essere utilizzato per classificare il traffico di QoS. Vedere anche NBAR.

DSLAM Acronimo di Digital Subscriber Line Access Multiplexer.

DSS Acronimo di Digital Signature Standard (standard della firma digitale). Definito anche DSA *(Digital Signature Algorithm)*, l'algoritmo DSS rappresenta uno dei numerosi standard a chiave pubblica utilizzati per le firme di crittografia.

durata chiavi Attributo di una coppia di chiavi che consente di specificare un intervallo di tempo, durante il quale è da considerarsi valido il certificato che contiene il componente pubblico di tale coppia.

E

EAPoUDP Acronimo di Extensible Authentication Protocol over User Datagram Protocol. Talvolta abbreviato in EOU. Il protocollo utilizzato da un client e un NAD per eseguire una convalida posture.

Easy VPN Soluzione di gestione VPN centralizzata basata su Cisco Unified Client Framework. Easy VPN di Cisco è costituita da due componenti ovvero un client Cisco Easy VPN Remote e un server Cisco Easy VPN.

ECHO Vedere ping, ICMP.

eDonkey Noto anche come eDonkey 2000 o ED2K, è una rete di file sharing peer-to-peer molto diffusa. eDonkey implementa l'MFTP (Multisource File Transmission Protocol).

EIGRP Acronimo di Extended Interior Gateway Routing Protocol. Versione avanzata del protocollo IGRP sviluppata da Cisco Systems. Fornisce proprietà di convergenza ed un'efficienza operativa superiori, oltre a unire i vantaggi dei protocolli di tipo link-state con quelli dei protocolli di tipo distance-vector.

elenco eccezioni In una implementazione NAC un elenco di host con indirizzi statici a cui è consentito ignorare il processo NAC. Questi host vengono inseriti nell'elenco eccezioni perché non dispongono di alcun agente di posture installato oppure perché sono stampanti o telefoni IP Cisco.

ERR Acronimo di Event Risk Rating. L'ERR viene utilizzato per controllare il livello a cui l'utente sceglie di intraprendere delle azioni nel tentativo di ridurre al minimo i falsi positivi.

ESP Acronimo di Encapsulating Security Payload. Protocollo IPSec in grado di garantire l'integrità e la riservatezza dei dati. Definito anche protocollo ESP (Encapsulating Security Payload), fornisce le seguenti caratteristiche: riservatezza, autenticazione dell'origine dati, rilevamento risposta, integrità senza connessione, integrità di sequenza parziale e riservatezza del flusso di traffico limitato.

ESP_SEAL ESP con algoritmo di crittografia SEAL (Software Encryption Algorithm) con chiave a 160 bit. Funzionalità introdotta nella versione 12.3(7)T, che può essere utilizzata solo se nel router non è stata attivata la crittografia IPSec hardware.

esp-3des Trasformazione di ESP (Encapsulating Security Payload) mediante l'algoritmo di crittografia DES a 168 bit (3DES o DES triplo).

esp-des Trasformazione di ESP (Encapsulating Security Payload) mediante l'algoritmo di crittografia DES a 56 bit.

ESP-MD5-HMAC Trasformazione di ESP (Encapsulating Security Payload) mediante l'algoritmo di autenticazione SHA variante MD5.

esp-null Trasformazione di ESP (Encapsulating Security Payload) che non fornisce alcuna funzionalità di crittografia e riservatezza.

ESP-SHA-HMAC Trasformazione di ESP (Encapsulating Security Payload) mediante l'algoritmo di autenticazione SHA variante HMAC.

Ethernet Protocollo LAN ampiamente diffuso inventato da Xerox Corporation e sviluppato congiuntamente da Xerox, Intel e Digital Equipment Corporation. La tecnologia Ethernet utilizza il protocollo CSMA/CD e viene eseguita su una vasta gamma di tipi di cavi a 10 o 100 Mbit/s. Ethernet è simile alla serie standard IEEE 802.3.

F

fasttrack Rete di file-sharing in cui le funzioni di indicizzazione vengono assegnate in modo dinamico ai peer connessi, definiti supernodi.

file delta File creato da IPS Cisco IOS per la memorizzazione delle modifiche apportate alle firme.

finger Strumento software per stabilire se una persona dispone di un account in un sito Internet specifico. In molti siti non sono consentite richieste finger in ingresso.

fingerprint Impronta digitale (fingerprint) di un certificato CA che rappresenta la stringa di caratteri alfanumerici che proviene da un hash MD5 dell'intero certificato CA. Le entità che ricevono un certificato CA possono verificarne l'autenticità confrontandolo con l'impronta digitale nota. Tale attività di autenticazione ha lo scopo di garantire l'integrità delle sessioni di comunicazione impedendo attacchi di tipo “man-in-the-middle”.

firewall Uno o più router o server di accesso utilizzati come buffer tra qualsiasi rete pubblica connessa e una rete privata. Un router firewall utilizza elenchi di accesso e altri metodi per garantire la protezione della rete privata.

Firma Elemento di dati di IPS IOS che rileva uno schema specifico di abuso della rete.

firma digitale Metodo di autenticazione che consente di individuare facilmente la contraffazione dei dati e di prevenire un eventuale rifiuto. L'uso inoltre di firme digitali consente di verificare che una trasmissione ricevuta sia intatta. La firma digitale generalmente include l'indicatore dell'ora di trasmissione.

firme RSA Uno dei tre metodi di autenticazione fornito in IPSec; gli altri due metodi sono RSA con crittografia nonce e chiavi precondivise. Inoltre, uno dei tre algoritmi approvati da FIPS (Federal Information Processing Standards) per generare e verificare le firme digitali. Gli altri algoritmi approvati sono DSA e Elliptic Curve DSA.

Flash

Memoria Flash Chip di memoria che conserva dati senza necessità di alimentazione. Immagini software possono essere archiviate, avviate e scritte utilizzando la memoria Flash, se necessario.

Frame Relay Protocollo DLL commutato, standard del settore per la gestione di più circuiti virtuali mediante l'uso dell'incapsulamento HDLC tra i dispositivi connessi. Essendo più efficiente rispetto al protocollo X.25, quest'ultimo viene generalmente sostituito da Frame Relay.

FTP File Transfer Protocol. Componente dello stack del protocollo TCP/IP, utilizzato per il trasferimento di file tra host.

G

G.SHDSL Definito anche G.991.2, G.SHDSL è uno standard internazionale per DSL simmetrica, sviluppato da International Telecommunications Union. Tale standard consente l'invio e la ricezione di flussi di dati simmetrici ad alta velocità su una singola coppia di cavi in rame a velocità comprese tra 192 kbit/s e 2,31 Mbit/s.

gateway predefinito Ultimo gateway disponibile. Si tratta del gateway al quale viene indirizzato un pacchetto quando l'indirizzo di destinazione non corrisponde a nessuna voce della tabella di routing.

Gateway VPN SSL Un gateway WebVPN fornisce un indirizzo IP e un certificato per un contesto WebVPN. La

gestione chiavi Creazione, distribuzione, autenticazione e archiviazione delle chiavi di crittografia.

globale esterno Indirizzo IP assegnato a un host sulla rete esterna dal proprietario dell'host. Tale indirizzo è stato assegnato da spazio di rete o indirizzo instradabile a livello globale.

globale interno Indirizzo IP di un host all'interno della rete così come viene visualizzato nei dispositivi esterni alla rete.

gnutella Un protocollo di file sharing P2P decentralizzato. Se si utilizza un client Gnutella installato, gli utenti possono cercare, scaricare e caricare file via Internet.

GRE Acronimo di Generic Routing Encapsulation (incapsulamento di routing generico). Protocollo di tunneling sviluppato da Cisco che è in grado di incapsulare un'ampia gamma di tipi di pacchetti di protocollo all'interno di tunnel IP, creando un collegamento point-to-point virtuale ai router Cisco presso punti remoti su una rete IP. Collegando subnet con più protocolli in un ambiente backbone a protocollo singolo, il tunneling IP che utilizza il protocollo GRE consente l'espansione di rete in un ambiente backbone a protocollo singolo.

GRE su IPSec Tecnologia che utilizza IPSec per crittografare pacchetti GRE.

H

H.323 Standard che consente di effettuare servizi di videoconferenza su reti LAN e altre reti commutate a pacchetto, oltre a filmati via Internet.

hash Processo unidirezionale per convertire input di qualsiasi dimensione in output di checksum a dimensione fissa, definito *digest di messaggio* o semplicemente *digest*. Si tratta di un processo irreversibile e non adatto alla creazione o modifica di dati da includere in un digest specifico.

HDLC Acronimo di High Level Data Link Control. Protocollo DLL sincrono orientato al bit sviluppato da International Standards Organization (ISO). HDLC specifica un metodo di incapsulamento di dati in collegamenti seriali sincroni usufruendo di caratteri e checksum di frame.

headend Estremità di trasmissione upstream di un tunnel.

HMAC Acronimo di Hash-based Message Authentication Code. Meccanismo per l'autenticazione di messaggi mediante le funzioni relative all'hash crittografico. È possibile utilizzare HMAC con qualsiasi funzione iterativa dell'hash crittografico, ad esempio MD5, SHA-1, in associazione a una chiave condivisa segreta. L'efficienza della crittografia di HMAC dipende dalle proprietà della funzione hash sottostante.

HMAC-MD5 HMAC (Hash Message Authentication Code) con MD5 (RFC 2104). Versione con chiave di MD5 che consente a due parti di convalidare le informazioni trasmesse mediante un segreto condiviso.

host Computer, ad esempio un PC, o dispositivo di elaborazione, ad esempio un server, associato a un indirizzo IP individuale e facoltativamente a un nome. Nome di qualsiasi dispositivo disponibile in una rete TCP/IP dotato di indirizzo IP. Infine, qualsiasi dispositivo indirizzabile di una rete. Il termine *nodo* fa riferimento a dispositivi, quali router e stampanti, che in genere non vengono definiti *host*.

host proxy di registrazione Server proxy utilizzato per un server di registrazione dei certificati.

HTTP

HTTPS Acronimi di Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure. Protocollo utilizzato in browser e server Web per trasferire file, quali file grafici e di testo.

hub In una rete DMVPN, un hub consiste in un router con una connessione IPSec di tipo point-to-point a tutti i router spoke della rete. L'hub è il punto centrale logico di una rete DMVPN.

I

ICMP Acronimo di Internet Control Message Protocol. Protocollo Internet a livello rete che segnala i messaggi di errore e fornisce altre informazioni relative all'elaborazione di pacchetti IP.

identità del certificato Certificato X.509 che include le informazioni relative all'identità del dispositivo o dell'entità che possiede il certificato. Le informazioni di identificazione vengono quindi esaminate a ogni istanza successiva di verifica e autenticazione dei peer. È possibile tuttavia che le identità dei certificati siano vulnerabili agli attacchi di spoofing.

IDM Acronimo di IDS Device Manager. Software utilizzato per gestire un sensore IDS.

IDS Acronimo di Intrusion Detection System (sistema di rilevamento intrusioni). Cisco IPS è in grado di eseguire un'analisi in tempo reale del traffico di rete per individuare anomalie e violazioni, utilizzando una libreria di firme che è possibile confrontare con il traffico. Una volta individuate anomalie e attività non autorizzate, è possibile terminare la condizione, bloccare il traffico proveniente da attacchi host e inviare avvisi a IDM.

IEEE Acronimo di Institute of Electrical and Electronics Engineers.

IETF Acronimo di Internet Engineering Task Force.

IGMP Acronimo di Internet Group Management Protocol. Protocollo utilizzato in sistemi IPv4 per segnalare le appartenenze IP multicast a router multicast adiacenti.

IKE Acronimo di Internet Key Exchange. Protocollo standard per la gestione di chiavi utilizzato insieme a IPSec e altri standard. È possibile configurare IPSec anche senza il protocollo IKE, tuttavia quest'ultimo ne ottimizza le prestazioni grazie all'aggiunta di funzionalità, flessibilità e facilità di configurazione. IKE fornisce inoltre l'autenticazione di peer IPSec, la negoziazione di chiavi IPSec e di Security Association IPSec.

Prima che venga consentito il passaggio di traffico IPSec, ogni router/firewall/host deve essere in grado di verificare l'identità del peer. È possibile eseguire questa operazione manualmente immettendo chiavi precondivise in entrambi gli host o mediante un servizio CA. IKE è un protocollo ibrido che implementa lo scambio di chiavi Oakley e Skeme all'interno dello schema ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP, Oakley e Skeme sono protocolli di protezione implementati da IKE.

IM Acronimo di Instant Messaging. Servizio di comunicazione in tempo reale in cui entrambe le parti sono online nello stesso momento. I servizi di IM più noti sono Yahoo! Messenger (YM), Microsoft Networks Messenger e AOL Instant Messenger (AIM).

IMAP Acronimo di Internet Message Access Protocol. Protocollo utilizzato dai client per comunicare con un server di posta elettronica. Definito in RFC 2060, IMAP consente ai client di eliminare, modificare lo stato e gestire i messaggi sul server di posta elettronica, nonché di recuperarli.

incapsulamento Disposizione di dati in un'intestazione di protocollo specifica. I dati Ethernet, ad esempio, vengono inclusi in un'intestazione Ethernet specifica prima del transito in rete. Quando inoltre si effettua il bridging di reti diverse, l'intero frame viene semplicemente spostato da una rete a un'intestazione utilizzata dal protocollo DLL (Data Link Layer) dell'altra rete.

Indirizzo IP Spazio degli indirizzi IP versione 4 che corrisponde a 32 bit o a 4 byte. Tale spazio viene utilizzato per definire il numero host, di rete e della subnet opzionale. I 32 bit sono raggruppati in quattro ottetti (8 bit binari), rappresentati da 4 numeri decimali separati da punti. La parte dell'indirizzo utilizzata per indicare il numero host, di rete e della subnet è specificata dalla subnet mask.

Inspection Rule La regola CBAC consente la verifica nel router del traffico in uscita specificato, affinché sia possibile autorizzare un traffico di ritorno dello stesso tipo associato a una sessione iniziata nella rete LAN. Se è in funzione un firewall, è possibile che venga eliminato il traffico in ingresso associato a una sessione iniziata nel firewall, nel caso non sia stata configurata alcuna Inspection Rule.

integrità dei dati Presunta correttezza dei dati trasmessi, ovvero autenticità del mittente e assenza di alterazione dei dati.

interfaccia Connessione fisica tra una rete specifica e il router. L'interfaccia LAN del router viene connessa alla rete locale servita dal router, che dispone di una o più interfacce WAN connesse in Internet.

interfaccia fisica Interfaccia del router supportata da un modulo di rete installato nello chassis del router o che fa parte dell'hardware di base del router.

Interfaccia Layer 3 Le interfacce Layer 3 supportano l'instradamento all'interno della rete. Una VLAN è un esempio di interfaccia Layer 3 logica. Una porta Ethernet è un esempio di interfaccia Layer 3 fisica.

interfaccia logica Interfaccia creata unicamente durante la configurazione e che non rappresenta un'interfaccia fisica nel router. Le interfacce dialer e tunnel rappresentano due esempi di interfacce logiche.

Internet Rete globale in cui vengono utilizzati protocolli IP e Internet. Non si tratta di una rete LAN. Vedere anche Intranet.

Intranet Rete Intranet. LAN in cui vengono utilizzati protocolli IP e Internet, quali SNMP, FTP e UDP. Vedere anche rete, Internet.

IOS Software Cisco IOS. Software di Cisco Systems che fornisce funzionalità comuni di scalabilità e protezione per tutti prodotti dell'infrastruttura CiscoFusion. Cisco IOS consente l'installazione e la gestione centralizzate, integrate e automatiche delle reti, garantendo al contempo un supporto per una vasta gamma di protocolli, supporti multimediali, servizi e piattaforme.

IP Acronimo di Internet Protocol (protocollo Internet). Protocolli open-system, cioè non proprietari, più diffusi al mondo in quanto possono essere utilizzati per la comunicazione tra gruppi di reti interconnesse, oltre a essere ideali per le comunicazioni LAN e WAN.

IPS IOS

IPS Sistema prevenzione intrusioni (IPS) Cisco IOS. Sistema che consente di confrontare il traffico con un database completo di firme di intrusioni, di eliminare pacchetti relativi a intrusioni e di intraprendere ulteriori azioni in base al tipo di configurazione. Le firme sono incorporate in immagini IOS che supportano questa funzionalità, mentre firme aggiuntive possono essere memorizzate nei file remoti o locali delle firme.

IPSec Schema di standard aperti che garantisce riservatezza, integrità e autenticazione dei dati tra i peer partecipanti. Tali servizi di protezione vengono forniti a livello IP. IPSec utilizza IKE per gestire la negoziazione di protocolli e algoritmi basati sul criterio locale, oltre a generare le chiavi di crittografia e autenticazione da utilizzare. Infine IPSec consente di proteggere uno o più flussi di dati tra una coppia di host, di gateway di protezione oppure tra un gateway di protezione e un host.

IRB Acronimo di Integrated Routing and Bridging. IRB consente l'instradamento di un determinato protocollo fra interfacce del router e bridge group all'interno di un unico switch router.

ISAKMP Acronimo di Internet Security Association Key Management Protocol. Protocollo base per IKE che consente di autenticare peer di comunicazione, creare e gestire Security Association, oltre a definire tecniche per la generazione di chiavi.

K

kazaa2 Servizio di file sharing peer-to-peer.

key escrow (deposito chiavi) Terza parte trusted che dispone delle chiavi di crittografia.

key recovery (recupero chiavi) Metodo trusted mediante il quale è possibile decrittografare le informazioni crittografate, nel caso venga persa o distrutta la chiave di decrittazione.

L

L2TP Acronimo di Layer 2 Tunneling Protocol. Protocollo di rilevamento degli standard di Internet Engineering Task Force (IETF) definito in RFC 2661 che fornisce il tunneling del protocollo PPP. Basato sulle principali funzionalità dei protocolli L2F e PPTP, L2TP fornisce un metodo interoperabile, diffuso nel settore, per l'implementazione di VPDN. Nonostante L2TP sia proposto come alternativa al protocollo IPSec, a volte vengono anche utilizzati contemporaneamente per fornire servizi di autenticazione.

LAC Acronimo di L2TP Access Concentrator (concentratore di accessi L2TP). Dispositivo per l'interruzione delle chiamate ai sistemi remoti e per il tunneling di sessioni PPP tra sistemi remoti e LNS.

LAN Acronimo di Local Area Network (rete locale). Rete limitata a una zona circoscritta o a una organizzazione, in cui vengono generalmente, ma non necessariamente, utilizzati protocolli IP e Internet. Non si tratta della rete Internet globale. *Vedere anche* Intranet, rete, Internet.

LAPB Acronimo di Link Access Procedure, Balanced.

LBO Acronimo di Line Build Out (Linea in uscita).

LEFS Acronimo di low-end file system.

lifetime Security Association Durata prestabilita di una SA valida.

LLQ Acronimo di Low latency queuing.

LNS Acronimo di L2TP Network Server (server di rete L2TP). Dispositivo che consente di interrompere tunnel L2TP da dispositivi LAC e sessioni PPP a sistemi remoti mediante sessioni di dati L2TP.

locale esterno Indirizzo IP di un host esterno così come viene visualizzato nella rete interna. Non si tratta necessariamente di un indirizzo lecito, che è stato assegnato da uno spazio di indirizzi instradabile all'interno.

locale interno Indirizzo IP configurato e assegnato a un host all'interno della rete.

loopback In un test di loopback, i segnali inviati vengono reindirizzati all'origine da un punto qualsiasi del percorso di comunicazione. Tali test vengono spesso utilizzati per determinare l'utilizzabilità dell'interfaccia di rete.

M

MAC Acronimo di Message Authentication Code (codice di autenticazione messaggi). Checksum di crittografia del messaggio utilizzato per verificare l'autenticità del messaggio. Vedere hash.

mappa classi

Mappa criteri Una mappa criteri è composta di azioni configurate da intreprendere sul traffico. IL traffico viene definito nelle mappe di classi associate.

mappa crittografica In Cisco SDM, le mappe crittografiche consentono di specificare il traffico da proteggere mediante IPSec, dove inviare il traffico protetto da IPSec e quali set di trasformazione IPSec è necessario applicare al traffico.

mappa parametri Le mappe di parametri specificano il comportamento di ispezione di ZPF (Zone-Policy Firewall), per parametri quali Protezione Denial-of-Service, timer di sessione e connessione e impostazioni di registrazione. Le mappe di parametri vengono inoltre applicate con le mappe di classe Layer 7 e di criterio per la definizione dei criteri specifici di applicazioni, ad esempio oggetti HTTP, requisiti di autenticazione POP3 e IMAP e altre informazioni specifiche di applicazione.

maschera carattere jolly

Maschera di bit utilizzata nelle regole di accesso, IPSec e NAT per indicare le porzioni dell'indirizzo IP del pacchetto che devono corrispondere all'indirizzo IP contenuto nella regola. Una maschera carattere jolly contiene 32 bit, lo stesso numero di bit presente in un indirizzo IP. Se il valore di bit del carattere jolly è pari a 0, il bit in quella stessa posizione dell'indirizzo IP del pacchetto deve corrispondere al bit contenuto nell'indirizzo IP della regola. Se il valore è pari a 1, il bit corrispondente dell'indirizzo IP del pacchetto può essere 1 o 0, ossia il valore del bit è irrilevante. Una maschera carattere jolly di 0.0.0.0 indica che tutti i 32 bit contenuti nell'indirizzo IP del pacchetto devono corrispondere all'indirizzo IP presente nella regola. Una maschera carattere jolly di 0.0.255.0 indica che i primi 16 bit e gli ultimi 8 bit devono corrispondere, ma che al terzo ottetto può essere associato qualsiasi valore. Se l'indirizzo IP contenuto in una regola è 10.28.15.0 e la maschera è 0.0.255.0, l'indirizzo 10.28.88.0 corrisponde all'indirizzo IP della regola, mentre l'indirizzo IP 10.28.15.55 non corrisponde.

maschera

subnet mask

netmask

maschera di rete

Maschera di bit a 32 bit che indica come suddividere un indirizzo Internet in parti di rete, subnet e host. La maschera di rete dispone dei numeri uno (1) nelle posizioni bit incluse nell'indirizzo a 32 bit da utilizzare per le parti della rete e della subnet, mentre dispone di zeri (0) per la parte di host. La maschera deve contenere almeno la parte di rete standard (come stabilito dalla classe di indirizzo), mentre il campo della subnet deve essere adiacente alla parte di rete. La maschera è configurata mediante l'equivalente decimale del valore binario.

Esempi:

Decimale: 255.255.255.0
Binario: 11111111 11111111 11111111 00000000
I 24 bit iniziali indicano l'indirizzo di rete e della subnet, mentre gli ultimi 8 bit rappresentano l'indirizzo host.

Decimale: 255.255.255.248
Binario: 11111111 11111111 11111111 11111000
I 29 bit iniziali indicano l'indirizzo di rete e della subnet, mentre gli ultimi 3 bit rappresentano l'indirizzo host.

Vedere anche indirizzo IP, TCP/IP, host, host/rete.

MD5 Acronimo di Message Digest 5. Funzione di hashing unidirezionale che consente di creare un hash a 128 bit. MD5 e SHA (Secure Hashing Algorithm) sono variazioni di MD4 e vengono utilizzati per aumentare la protezione dell'algoritmo hash MD4. Cisco utilizza hash per l'autenticazione all'interno della struttura IPSec, Infine, MD5 consente di verificare l'integrità e di autenticare l'origine di una comunicazione.

MD5 Acronimo di Message Digest 5. Algoritmo hash unidirezionale che consente di creare un hash a 128 bit. MD5 e SHA (Secure Hashing Algorithm) sono variazioni di MD4 e vengono utilizzati per aumentare la protezione dell'algoritmo hash MD4. Cisco utilizza hash per l'autenticazione all'interno della struttura IPSec, oltre che per l'autenticazione di messaggi in SNMP v.2. MD5 consente di verificare l'integrità della comunicazione, di autenticare l'origine e di controllare la tempestività.

mGRE GRE multipoint.

modalità Aggressive Modalità utilizzata per stabilire SA ISAKMP per semplificare la negoziazione dell'autenticazione IKE (fase 1) tra due o più peer IPSec. Nonostante la modalità Aggressive sia più rapida della modalità principale, essa non è altrettanto sicura. Vedere modalità principale e modalità rapida.

modalità rapida In Oakley, nome del meccanismo utilizzato dopo aver stabilito una Security Association per negoziare le modifiche nei servizi di protezione, ad esempio nuove chiavi.

modulo di rete Scheda dell'interfaccia di rete installata nello chassis del router per aggiungere funzionalità al router. Esempi dei moduli di rete Ethernet e IDS.

motore firme Un motore di firme è un componente di IPS IOS progettato per fornire supporto a più firme di una determinata categoria. Un motore è composto da un componente di analisi e uno di ispezione. Ogni motore dispone di un set di parametri legali con intervalli o set di valori che è possibile autorizzare.

MTU Acronimo di Maximum Transmission Unit (unità di trasmissione massima). Dimensione massima dei pacchetti in byte che è possibile trasmettere o ricevere mediante un'interfaccia.

N

NAC Acronimo di Network Admission Control. Un metodo per controllare l'accesso alla rete e che ha la funzione di prevenire l'infiltrazione di virus. Utilizzando una serie di protocolli e prodotti software, NAC verifica la condizione degli host nel momento in cui tentano di accedere alla rete e gestisce la richieste sulla base della condizione dell'host, denominata anche *posture*. Gli host infetti possono essere messi in quarantena; per gli host privi di software antivirus aggiornato può essere avviata la richiesta di aggiornamento; agli host non infetti e dotati di software antivirus aggiornato può essere consentito l'accesso alla rete. Vedere anche ACL, posture e EAPoUDP.

NAD Acronimo di Network Access Device. In una implementazione NAC, il dispositivo che riceve da un host la richiesta di accedere alla rete. Un dispositivo NAD, generalmente un router, funziona insieme al software agente posture in esecuzione sull'host, un software antivirus e server ACS e di posture/convalida presenti nella rete per controllarne l'accesso al fine di prevenire un'infezione causata da virus.

NAS Acronimo di Access Server. Piattaforma di interfaccia tra Internet e la rete PSTN (Public Switched Telephone Network).

Gateway per la connessione di dispositivi asincroni a reti LAN o WAN mediante software di emulazione di terminale e di rete. Consente di eseguire routing sincrono e asincrono dei protocolli supportati.

NAT

Network Address Translation Acronimo di Network Address Translation. Meccanismo sviluppato per ridurre l'esigenza di disporre di indirizzi IP univoci. NAT consente a una organizzazione con indirizzi globali non univoci di connettersi a Internet trasferendo questi indirizzi in uno spazio di indirizzi instradabili globali.

NBAR Acronimo di Network-based Application Recognition. Metodo utilizzato per classificare il traffico di QoS.

negoziazione IKE Metodo per lo scambio protetto di chiavi private su reti non sicure.

NetFlow Funzionalità disponibile in alcuni router che consente di suddividere per categorie i pacchetti in ingresso nei flussi. Poiché è spesso possibile trattare i pacchetti inclusi in un flusso nello stesso modo, questa classificazione può essere utilizzata per ignorare alcune attività del router e velocizzare pertanto l'operazione di switching.

NHRP Acronimo di Next Hop Resolution Protocol. Protocollo client e server utilizzato in reti DMVPN, in cui il router hub rappresenta il server mentre gli spoke rappresentano i client. L'hub gestisce un database NHRP degli indirizzi dell'interfaccia pubblica di ogni spoke. All'avvio quindi ogni spoke registra l'indirizzo effettivo e richiede al database NHRP gli indirizzi effettivi degli spoke di destinazione per consentire la generazione di tunnel diretti.

nome di dominio Nome comune e facile da ricordare dato a un host in Internet che corrisponde al relativo indirizzo IP.

non crittografato Non sottoposto a crittografia.

NTP Acronimo di Network Time Protocol. Protocollo per la sincronizzazione degli orologi di sistema dei dispositivi di rete. Rappresenta un protocollo UDP.

NVRAM Acronimo di Non-volatile Random Access Memory.

O

Oakley Protocollo per la creazione di chiavi segrete che vengono utilizzate da parti autenticate, basate su Diffie-Hellman e progettate per essere compatibili con ISAKMP.

OFB Acronimo di Output Feedback. Funzione IPSec che consente di ripristinare output crittografato (generalmente, ma non necessariamente, con crittografia DES) in input originale. Il testo normale viene crittografato direttamente con la chiave simmetrica, creando un flusso di numeri pseudo-casuali.

OSPF Acronimo di Open Shortest Path First. Algoritmo di routing IGP gerarchico di tipo link-state proposto in sostituzione del protocollo RIP utilizzato in Internet. Tra le funzionalità del protocollo sono incluse routing a costi ridotti, a percorsi multipli e bilanciamento del carico.

P

P2P Vedere peer-to-peer.

PAD Acronimo di Packet Assembler/Disassembler. Dispositivo utilizzato per la connessione di dispositivi semplici (quali terminali in modalità carattere), che non supportano la funzionalità completa di un determinato protocollo, a una rete. I dispositivi PAD memorizzano i dati nel buffer e assemblano e disassemblano i pacchetti inviati a questi tipi di dispositivi finali.

PAM Acronimo di Port to Application Mapping. La PAM consente di personalizzare i numeri di porta TCP or UDP per i servizi o le applicazioni di rete. La PAM utilizza queste informazioni per supportare ambienti di rete che eseguono servizi utilizzando porte diverse da quelle solitamente associate con determinate applicazioni.

PAP Acronimo di Password Authentication Protocol. Protocollo di autenticazione che consente l'autenticazione reciproca dei peer trasmettendo la password e il nome host o il nome utente in formato crittografato. Vedere anche CHAP.

password Stringa (o altra origine dati) di caratteri protetta e segreta associata all'identità di un utente specifico o entità.

password per la revoca Password fornita a una CA quando si richiede la revoca del certificato digitale di un router. Talvolta denominata *password di verifica*.

PAT statico PAT (Port Address Translation) statico. Un indirizzo statico abbina un indirizzo IP locale a un indirizzo IP globale. Un PAT statico è un indirizzo statico che abbina una porta locale a una porta globale. Vedere anche PAT.

PAT

PAT dinamico Acronimo di Port Address Translation. PAT dinamico che consente la visualizzazione di sessioni in uscita originate da un indirizzo IP singolo. Con la modalità PAT attivata, il router sceglie un numero porta univoco dall'indirizzo IP PAT per ciascun slot (xlate) di conversione in uscita. Questa funzionalità è essenziale quando un provider di servizi Internet non può allocare indirizzi IP univoci sufficienti per le connessioni in uscita. Gli indirizzi del pool globale hanno sempre la precedenza sull'utilizzo di un indirizzo PAT.

peer In IKE, router che fungono da proxy per i partecipanti in un tunnel IKE. In IPSec, dispositivi o entità che comunicano in maniera protetta mediante lo scambio di chiavi o lo scambio di certificati digitali.

peer-to-peer Tipologia di architettura di rete in cui tutti gli host condividono funzionalità pressoché equivalenti. Chiamata anche P2P, la rete peer-to-peer è utilizzata da molte reti di file sharing.

PEM Formato Privacy Enhanced Mail. Formato di memorizzazione dei certificati digitali.

PFS Acronimo di Perfect Forward Secrecy. Proprietà di alcuni protocolli di chiavi concordate asimmetriche che consentono l'utilizzo di chiavi differenti in momenti diversi durante una sessione, per garantire che la compromissione di un'eventuale singola chiave non comprometta l'intera sessione.

ping Richiesta ICMP inviata tra host per determinare l'accessibilità di un host nella rete.

PKCS12 Acronimo di Public Key Cryptography Standard Number 12. Formato per la memorizzazione delle informazioni sui certificati digitali. Vedere anche PEM.

PKCS7 Acronimo di Public Key Cryptography Standard Number 7.

PKI Acronimo di Public-Key Infrastructure (infrastruttura a chiave pubblica). Sistema di Certification Authority (CA) e Registration Authority (RA) che fornisce supporto per l'utilizzo della crittografia di chiavi asimmetriche nella comunicazione dati mediante funzioni come gestione certificati, gestione archivio, gestione chiavi e gestione token.

In alternativa, qualsiasi standard per lo scambio di chiavi asimmetriche.

Questo tipo di scambio consente al destinatario di un messaggio di considerarne trusted la firma, e al mittente di crittografare il messaggio in modo appropriato per il destinatario. Vedere gestione chiavi.

Police Rate Numero di bit al secondo che non deve essere superato dal traffico.

policy IKE globale Dispositivo con un'unica IKE Policy, piuttosto che una policy per ogni singola interfaccia di tale dispositivo.

POP3 Post Office Protocol versione 3. Protocollo utilizzato per il recupero della posta dai server di posta.

posture In una implementazione NAC, la condizione di un host che tenta di accedere alla rete. Il software agente posture in esecuzione sull'host comunica con il NAD per segnalare la conformità dell'host con il criterio di protezione della rete.

PPP Acronimo di Point-to-Point Protocol (protocollo Point-to-Point). Protocollo che fornisce connessioni da router a router e da host alla rete su circuiti sincroni e asincroni. PPP dispone di meccanismi di protezione quali CHAP e PAP.

PPPoA Acronimo di Point-to-Point Protocol over Asynchronous Transfer Mode (ATM). Principalmente implementato come parte di ADSL, PPPoA si basa sulla RFC1483 nella modalità operativa LLC-SNAP (Logical Link Control-Subnetwork Access Protocol) o VC-Mux.

PPPoE Acronimo di Point-to-Point-Protocol over Ethernet. Protocollo PPP incapsulato in frame Ethernet. PPPoE consente la connessione di host in una rete Ethernet a host remoti mediante un modem a banda larga.

PPTP Acronimo di Point-to-Point Tunneling Protocol. Protocollo utilizzato per creare tunnel inizializzati da client incapsulando pacchetti in datagrammi IP per la trasmissione su reti basate su TCP/IP. Può essere utilizzato in alternativa ai protocolli di tunneling L2F e L2TP. Protocollo di proprietà Microsoft.

Profilo IKE Gruppo di parametri ISAKMP mappabili su vari tunnel IP Security.

protocollo L2F Acronimo di Layer 2 Forwarding Protocol. Protocollo che supporta la creazione di reti VPN di tipo dial-up protette in Internet.

pseudo-casuale Sequenza ordinata di bit che superficialmente appare simile alla sequenza casuale reale degli stessi bit. La chiave generata da un numero pseudo-casuale è detta nonce.

PVC Acronimo di Permanent Virtual Circuit (o Connection). Circuito virtuale stabilito in modo permanente. I circuiti PVC salvano la larghezza di banda associata alla connessione del circuito e la eliminano nei casi in cui determinati circuiti virtuali devono esistere per tutto il tempo. Nella terminologia ATM, connessione virtuale permanente.

Q

QoS Acronimo di Quality of Service (Qualità del servizio). Metodo per garantire la larghezza di banda a tipi specificati di traffico.

R

RA Acronimo di Registration Authority. Entità utilizzata come componente opzionale nei sistemi PKI per registrare o verificare alcune informazioni che le Certification Authority (CA) utilizzano durante l'emissione di certificati o l'esecuzione di altre funzioni di gestione certificati. La CA stessa può eseguire tutte le funzioni RA, ma generalmente sono gestite a parte. I doveri della Registration Authority variano notevolmente, ma possono includere l'assegnazione di nomi distinti, la distribuzione di token e l'esecuzione di funzioni di autenticazione personale.

RADIUS Acronimo di Remote Authentication Dial-In User Service. Un protocollo di autenticazione e accounting del server che utilizza UDP come protocollo di trasporto. Vedere anche TACACS+.

RCP Acronimo di Remote Copy Protocol. Protocollo che consente agli utenti di copiare i file in e da un file system in un host o server remoto nella rete. Il protocollo RCP utilizza TCP per garantire l'invio trusted dei dati.

regola Informazioni aggiunte alla configurazione per definire il criterio di protezione nel formato di istruzioni condizionali impiegate per impartire al router la modalità di azione in una particolare situazione.

regola implicita Regola di accesso creata automaticamente dal router in base a regole predefinite o come risultato di regole definite dall'utente.

regola IPSec Regola utilizzata per indicare il traffico protetto da IPSec.

regola standard In Cisco SDM, un tipo di regola di accesso o di regola NAT. Le regole standard confrontano l'indirizzo IP di origine di un pacchetto con i criteri del proprio indirizzo IP per determinare una corrispondenza. Tali regole utilizzano una maschera carattere jolly per definire quali porzioni dell'indirizzo IP devono corrispondere.

regole estese Tipo di regola di accesso. Le regole estese consentono di analizzare una maggiore quantità di campi di un pacchetto per determinare una corrispondenza. Tali regole consentono inoltre di esaminare gli indirizzi IP di origine e destinazione, il tipo di protocollo, le porte di origine e destinazione nonché altri campi di un pacchetto.

rete Gruppo di dispositivi di elaborazione che condividono una parte dello spazio dell'indirizzo IP e non rappresentano un singolo host. Una rete è costituita da più "nodi" o dispositivi con indirizzo IP, a cui viene fatto riferimento come *host*. Vedere anche Internet, Intranet, IP, LAN.

rifiuto Nei sistemi di crittografia, indica il rifiuto, da parte di una delle entità interessate da una comunicazione, di partecipare a tutta o a parte di quella comunicazione.

rilevamento risposta Funzionalità di protezione IPSec che combina i numeri di sequenza con l'autenticazione, in modo che il destinatario di una comunicazione può rifiutare pacchetti vecchi o duplicati al fine di evitare attacchi di risposta.

RIP Acronimo di Routing Information Protocol. Protocollo di routing che utilizza il numero di router che un pacchetto deve attraversare per raggiungere la destinazione, come metrica di routing.

riservatezza dei dati Risultato della crittografia dei dati che consente di evitare la divulgazione di informazioni a utenti, entità e processi non autorizzati. Tali informazioni possono riguardare dati a livello di applicazioni o parametri di comunicazione. Vedere riservatezza del flusso di traffico o analisi del traffico.

riservatezza del flusso di traffico o analisi del traffico Protezione dei dati al fine di impedire la diffusione non autorizzata dei parametri di comunicazione. Questa protezione impedisce agli utenti non autorizzati di accedere a informazioni quali gli indirizzi IP di origine e di destinazione, la lunghezza del messaggio e la frequenza di comunicazione

route Percorso all'interno di una rete.

route map Consente di controllare le informazioni aggiunte alla tabella di routing. Cisco SDM crea automaticamente route map per impedire la conversione NAT di specifici indirizzi di origine quando tale operazione impedirebbe ai pacchetti di soddisfare i criteri in una regola IPSec.

route statica Route esplicitamente configurata e immessa nella tabella di routing. Le route statiche hanno precedenza sulle route scelte dai protocolli di routing dinamico.

routing dinamico Routing che si adatta automaticamente alla topologia di rete o alle modifiche del traffico. Viene definito anche routing adattabile.

Routing RFC 1483 RFC1483 descrive due differenti metodi per il traffico di interconnessione della rete non orientato alla connessione su una rete ATM: PDU (Protocol Data Unit) instradate e PDU di bridge. Cisco SDM supporta la configurazione di routing RFC 1483 e consente di configurare due tipi di incapsulamento: AAL5MUX e AAL5SNAP.

AAL5MUX: l'incapsulamento AAL5 MUX supporta solo un singolo protocollo (IP o IPX) per PVC.

AAL5SNAP: l'incapsulamento AAL5 Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) supporta ARP Inverso e incorpora il protocollo LLC/SNAP che precede il datagramma del protocollo, consentendo più protocolli nello stesso PVC.

RPC Acronimo di Remote Procedure Call. Le RPC rappresentano chiamate di procedura che sono create o specificate dai client ed eseguite nei server, con i risultati restituiti ai client attraverso la rete. Vedere anche sistemi di elaborazione di tipo client/server.

RR Risk Rating (Classificazione rischio). L'RR è un valore compreso tra 0 e 100 che rappresenta una quantificazione numerica del rischio associato a un particolare evento della rete.

RSA Iniziali di Rivest, Shamir e Adelman, inventori di questa tecnica di scambio di chiavi crittografica basata sulla fattorizzazione di numeri grandi. RSA è anche il nome della tecnica stessa. RSA può essere utilizzato per la crittografia e l'autenticazione ed è inclusa in molti protocolli di protezione.

S

SA Acronimo di Security Association. Set di parametri di protezione concordati da due peer per proteggere una specifica sessione in un particolare tunnel. Le Security Association sono utilizzate sia da IKE che IPSec, sebbene le SA siano indipendenti l'una dall'altra.

Le SA IPSec sono unidirezionali e sono univoche in ciascun protocollo di protezione. Una SA IKE è utilizzata solo da IKE e, diversamente dalla SA IPSec, è bidirezionale. IKE negozia e stabilisce le SA per conto di IPSec. Anche un utente può stabilire manualmente SA IPSec.

Un set di SA è necessario per un pipe di dati protetto, uno per direzione per protocollo. Se, ad esempio, si dispone di un pipe che supporta ESP (Encapsulating Security Protocol) tra peer, un SA ESP è richiesto per ciascuna direzione. Le SA sono identificate univocamente dall'indirizzo di destinazione (endpoint IPSec), dal protocollo di protezione (AH o ESP) e dall'indice dei parametri di sicurezza (SPI).

SAID Acronimo di Security Association ID. Identificatore numerico per la SA di un dato collegamento.

salt Stringa di caratteri pseudo-casuale utilizzata per potenziare la complessità crittografica.

scambio chiavi Metodo mediante il quale due o più parti si scambiano chiavi di crittografia. Anche il protocollo IKE fornisce un metodo simile.

scambio di chiavi Diffie-Hellman Protocollo di crittografia a chiave pubblica che consente a due parti di stabilire un segreto condiviso su canali di comunicazione non protetti. Diffie-Hellman viene utilizzato in Internet Key Exchange (IKE) per stabilire delle chiavi di sessione. Tale protocollo è inoltre un componente di uno scambio di chiavi Oakley. Il software Cisco IOS supporta gruppi Diffie-Hellman a 768 e 1024 bit.

SDEE Acronimo di Security Device Event Exchange. Un protocollo di messaggio utilizzato per segnalare eventi legati alla sicurezza, ad esempio avvisi generati quando un pacchetto corrisponde alle caratteristiche di una firma.

SDF Acronimo di Signature Definition File. Un file, di solito in formato XML, che contiene le definizioni da utilizzare per caricare le firme su un dispositivo di protezione.

SDP Acronimo di Secure Device Provisioning. SDD utilizza Trusted Transitive Introduction (TTI) per semplificare l'implementazione dell'infrastruttura a chiave pubblica (PKI) tra due dispositivi finali, quali un client Cisco IOS e un server di certificati Cisco IOS.

SEAF Acronimo di Signature Event Action Filter (Filtro azioni evento firma). Filtro che consente di sottrarre azioni da un evento i cui parametri ricadono in quelli definiti. Ad esempio, è possibile creare un filtro SEAF per sottrarre l'azione Reset TCP Connection da un evento associato a un particolare indirizzo di autore di un attacco.

SEAO Acronimo di Signature Event Action Override (Sostituzione azioni evento firma). SEAO consente di assegnare un intervallo di classificiazione di rischio (RR) a un tipo di azione evento IPS, ad esempio un avviso. Se si verifica un evento con un RR nell'intervallo assegnato a un tipo di azione, l'azione viene aggiunta all'evento. In tal caso, verrebbe aggiunto un avviso all'evento.

SEAP Acronimo di Signature Event Action Processor (Processore azioni evento firma). SEAP consente il filtraggio e la sostituzione in base a una risposta ERR (Event Risk Rating) feedback.

Segreto condiviso Chiave crittografica.

sensore IDS Dispositivo hardware in cui viene eseguito Cisco IDS. I sensori IDS possono essere utilizzati come dispositivi autonomi o moduli di rete installati su router.

Server CA Server Autorità di certificazione. Host di rete utilizzato per emettere e/o revocare certificati digitali.

servizio di non-rifiuto Servizio di protezione di terze parti che consente di archiviare informazioni, per un successivo recupero, in merito all'origine e alla destinazione di tutti i dati inclusi in una comunicazione, senza che sia necessario archiviare i dati effettivi. Questa funzione può essere utilizzata per proteggere tutti i partecipanti alla comunicazione da rifiuti falsi da parte di qualsiasi partecipante che ha inviato o ricevuto informazioni.

set di trasformazione Combinazione valida di protocolli, algoritmi e impostazioni di protezione da applicare al traffico protetto utilizzando il protocollo IPSec. Durante la negoziazione dell'associazione della protezione IPSec, i peer concordano nell'utilizzare un particolare set di trasformazione per proteggere un determinato flusso di dati.

SFR Acronimo di Signature Fidelity Rating (Classificazione di fedeltà firma). Un valore associato alle capacità di una firma di operare in assenza di conoscenza specifica della destinazione.

SHA Acronimo di Secure Hashing Algorithm. Alcuni sistemi di crittografia utilizzano questo algoritmo come alternativa a MD5 per la creazione di firme digitali.

SHA-1 Acronimo di Secure Hashing Algorithm 1. Si tratta di un algoritmo che elabora un messaggio con un numero di bit inferiore 264, ricavandone un digest lungo 160 bit. Questo digest di notevoli dimensioni garantisce la protezione contro attacchi brute force di collisione e inversione. L'algoritmo SHA-1 [NIS94c] è una revisione dell'algoritmo SHA pubblicato nel 1994.

SIP Acronimo di Session Initiation Protocol. Consente di stabilire sessioni di gestione delle chiamate, in particolare di conferenze audio con due interlocutori, anche dette “chiamate”. Questo protocollo collabora con il protocollo SDP (Session Description Protocol) per l'indicazione delle chiamate. Il protocollo SDP specifica le porte del flusso multimediale. Tramite il protocollo SIP, il router è in grado di supportare qualsiasi gateway VoIP (Voice over IP) SIP e server proxy VoIP.

sistemi di elaborazione di tipo client/server Termine utilizzato per descrivere i sistemi di rete informatici (processi di elaborazione) distribuiti in cui le responsabilità sulle transazioni sono suddivise in due parti: client (front-end) e server (back-end). Definiti anche sistemi di elaborazione distribuiti. Vedere anche RPC.

SMTP Acronimo di Simple Mail Transfer Protocol. Protocollo Internet per la fornitura di servizi di posta elettronica.

SNMP Acronimo di Simple Network Management Protocol. Protocollo di gestione di rete utilizzato quasi esclusivamente nelle reti TCP/IP. SNMP consente di monitorare e controllare i dispositivi di rete e di gestire le configurazioni, la raccolta di statistiche, le prestazioni e la protezione.

Sostituzione azione evento

sostituzione azione evento Le sostituzioni di azioni evento vengono utilizzate in IOS IPS 5.x. Consentono di modificare le azioni associate a un evento in base all'RR (Risk Rating) di tale evento.

SPD Acronimo di Selective Packed Discard. Il metodo SPD dà priorità ai pacchetti del protocollo di routing e ad altri importanti keepalive di livello 2 relativi al controllo del traffico in caso di congestione di rete.

spoke In una rete DMVPN, un router spoke costituisce un endpoint logico della rete e dispone di una connessione IPSecpoint-to-point con un router hub DMVPN.

spoofing

spoof Invio di pacchetti la cui provenienza dichiarata non corrisponde alla provenienza effettiva. Lo spoofing è finalizzato a eludere i meccanismi di protezione di rete quali i filtri e gli elenchi di accesso.

SRB Acronimo di Source Route Bridging. Metodo di bridging creato da IBM e assai diffuso nelle reti di tipo token ring. Nelle reti SRB le route sono integralmente prestabilite in tempo reale prima di inviare i dati a destinazione.

SSH Acronimo di Secure Shell. Le applicazioni SSH sono eseguite su un livello di trasporto trusted, quale TCP/IP, in grado di garantire efficienti funzionalità di autenticazione e crittografia. Fino a cinque client SSH possono accedere contemporaneamente alla console del router.

SSL Acronimo di Secure Socket Layer. Tecnologia Web di crittografia utilizzata per garantire la protezione delle transazioni, quali ad esempio la trasmissione del numero di carta di credito durante un'operazione di commercio elettronico.

SSL VPN (VPN SSL) Acronimo di Secure Socket Layer Virtual Private Networks (Reti private virtuali su connettività con accesso remoto). VPN SSL è una funzione che consente ai router Cisco supportati di fornire l'accesso protetto dei client remoti alle risorse di rete creando un tunnel crittografico su Internet trami connessioni a banda larga o remote tramite ISP utilizzate dal client remoto.

stato, di stato, verifica di stato

I protocolli di rete prevedono la gestione di determinati dati, detti informazioni di stato, presso entrambe le estremità di una connessione di rete fra due host. Le informazioni di stato sono necessarie per implementare le caratteristiche di un protocollo, quali la trasmissione trusted dei pacchetti, l'invio in sequenza dei dati, il controllo di flusso e l'impiego di identificativi di transazione o di sessione. Parte delle informazioni di stato di un protocollo viene inviata in ogni pacchetto ogni volta che si utilizza tale protocollo. Ad esempio, un browser Web connesso a un server Web utilizza il protocollo HTTP e i protocolli di supporto TCP/IP. Ogni livello di protocollo aggiorna le informazioni di stato nei pacchetti inviati e ricevuti. I router verificano le informazioni di stato in ogni pacchetto in modo da garantire che tali informazioni siano aggiornate e valide per ognuno dei protocolli contenuti nel pacchetto. Questo meccanismo, detto verifica di stato, è finalizzato alla creazione di una solida protezione contro determinati tipi di attacchi informatici.

subnet

Rete IP che condivide un determinato indirizzo di subnet. Si tratta di reti IP arbitrariamente segmentate da un amministratore di rete al fine di fornire una struttura di routing gerarchica a più livelli, proteggendo contemporaneamente la subnet dalla complessità delle reti collegate. Vedere anche Indirizzo IP, Bit di subnet e Subnet mask.

subnet locale

Reti IP arbitrariamente segmentate da un amministratore di rete (mediante una subnet mask) al fine di fornire una struttura di routing gerarchica a più livelli, proteggendo contemporaneamente la subnet dalla complessità delle reti collegate. La subnet locale è quella associata all'estremità di trasmissione.

subnet remota

Reti IP arbitrariamente segmentate da un amministratore di rete (mediante una subnet mask) al fine di fornire una struttura di routing gerarchica a più livelli, proteggendo contemporaneamente la subnet dalla complessità delle reti collegate. La "subnet remota" è la subnet che *non* è associata all'estremità di una trasmissione.

SUNRPC

SUN Remote Procedure Call. L'RPC è un protocollo che consente ai client di eseguire programmi o routine su server remoti. SUNRPC è la versione di RPC distribuita in origine nella libreria SUN Open Network Computing (ONC).

T

T1 Collegamento in grado di trasmettere dati alla velocità di 1,5 Mb al secondo.

TACACS+ Terminal Access Controller Access Control System (Sistema di controllo accessi del controller di accessi terminale) Un protocollo di autenticazione e accounting del server che utilizza TCP come protocollo di trasporto.

tailend Estremità downstream di ricezione di un tunnel.

TCP Transmission Control Protocol. Protocollo di livello trasporto orientato alla connessione che consente una trasmissione di dati full-duplex trusted.

Telnet Protocollo di emulazione di terminale per reti TCP/IP quali ad esempio Internet. Telnet è utilizzato comunemente per il controllo remoto dei server Web.

testo normale Dati comuni, non crittografati.

TFTP Trivial File Transfer Protocol. Si tratta di un semplice protocollo utilizzato per il trasferimento dei file eseguito su UDP. Per ulteriori informazioni, consultare la RFC (Request For Comments) 1350.

trasformazione Descrizione di un protocollo di protezione e dei relativi algoritmi.

tunnel Canale virtuale configurato su una risorsa condivisa quale Internet e utilizzato per lo scambio di pacchetti dati incapsulati.

tunneling Processo di piping del flusso di dati di un protocollo attraverso un altro protocollo.

TVR Acronimo di Target Value Rating (Classificazione del valore di destinazione). Il TVR è un valore definito dall'utente che rappresenta il valore percepito dell'host di destinazione. Ciò consente agli utenti di aumentare la classificazione di rischio di un evento associato a un sistema critico e di ridurla per un evento su una destinazione di importanza inferiore.

U

UDP User Datagram Protocol. Protocollo del livello di trasporto nel contesto TCP/IP non orientato alla connessione e appartenente alla famiglia di protocolli Internet.

Unity Client Client di un server Easy VPN Unity.

URI Acronimo di Uniform Resource Identifier (Identificatore di risorsa uniforme). Tipo di identificatore formattato che incapsula il nome di un oggetto Internet e lo etichetta con un'identificazione dello spazio dei nomi, producendo un membro del set di nomi universale negli spazi dei nomi registrati e degli indirizzi che fanno riferimento ai protocolli o agli spazi dei nomi registrati. [RFC 1630]

URL Acronimo di Universal Resource Locator. Struttura di indirizzamento standardizzata che consente di accedere ai documenti ipertestuali e agli altri servizi forniti da un browser. Vengono forniti di seguito due esempi:

http://www.cisco.com.

ftp://10.10.5.1/netupdates/sig.xml

URL di registrazione Percorso HTTP a una Certification Authority che deve essere utilizzato dal router Cisco IOS durante l'invio di richieste di certificati. Tale URL include il nome DNS o un indirizzo IP e può essere seguito da un percorso completo agli script CA.

V

VCI Acronimo di Virtual Circuit Identifier. Percorso virtuale che può contenere più canali virtuali corrispondenti a singole connessioni. Il VCI identifica i canali in uso. La combinazione di VPI e VCI identifica una connessione ATM.

verifica Conferma dell'identità di un utente o di un processo.

VFR Acronimo di Virtual Fragment Reassembly. Consente al firewall IOS di creare dinamicamente ACL per bloccare dei frammenti IP. Questi spesso non contengono un numero di informazioni tale da poter essere filtrati da ACL statici.

VPDN Rete virtuale privata di tipo dial-up. Si tratta di un sistema che consente alle reti remote di tipo dial-in di essere accessibili dalle reti locali mediante una connessione diretta simulata. Questo tipo di rete utilizza i protocolli L2TP e L2F per stabilire la connessione di rete di livello 2 e dei livelli superiori con il gateway locale anziché il NAS (Network Access Server).

VPI Acronimo di Virtual Path Identifier. Identifica il percorso virtuale utilizzato in una connessione ATM.

VPN Acronimo di Virtual Private Network. Consente agli utenti di ottenere attraverso un'infrastruttura pubblica la stessa connettività che avrebbero utilizzando una rete privata. Le reti VPN consentono di proteggere la trasmissione del traffico IP su una rete pubblica TCP/IP sottoponendo a crittografia tutto il traffico scambiato fra le reti. La crittografia si basa sul tunneling e viene effettuata a livello IP.

VPN site-to-site Solitamente rete che connette due reti o subnet e che soddisfa alcuni altri specifici criteri, fra cui l'utilizzo di indirizzi IP statici su entrambe le estremità del tunnel, l'assenza di un software client VPN sulle stazioni terminali degli utenti e l'assenza di un hub VPN centrale (come da configurazioni VPN hub and spoke). Le reti VPN site-to-site non hanno la finalità di sostituire l'accesso di tipo dial-in da parte di utenti remoti o mobili.

VTI Acronimo di Virtual Template Interface (Interfaccia modello virtuale).

vty Acronimo di Virtual Type Terminal. In genere utilizzato come linea terminale virtuale.

W

WAN Acronimo di Wide Area Network. Rete che fornisce connettività a utenti localizzati in un'ampia area geografica e che spesso utilizza dispositivi di trasmissione forniti dai principali gestori di telefonia. Vedere anche LAN.

WINS Acronimo di Windows Internet Naming Service. Sistema Windows in grado di determinare l'indirizzo IP associato a un particolare computer connesso in rete.

X

X.509 Standard dei certificati digitali in cui si specifica la struttura dei certificati. I campi principali di tale standard sono ID, oggetto, date di validità, chiave pubblica e firma CA.

XAuth Autenticazione estesa IKE. XAuth consente a tutti i metodi di autenticazione AAA per il software Cisco IOS di eseguire l'autenticazione utente in una fase distinta, successiva allo scambio della prima fase di autenticazione IKE. Affinché l'utente sia autenticato, il nome elenco di configurazione AAA deve corrispondere a quello di Xauth.

L'autenticazione Xauth rappresenta un'estensione di IKE e non sostituisce l'autenticazione IKE.

Z

zona In un firewall con criteri basati su zone, una zona rappresenta un gruppo di interfacce con funzioni e caratteristiche simili. Se ad esempio le interfacce Ethernet 0/0 e Ethernet 0/1 sono entrambe connesse alla LAN, possono essere raggruppate in una zona che crea una

zona di protezione Gruppo di interfacce a cui è possibile applicare un criterio. Le zone di protezione sono composte da interfacce che condividono funzioni e caratteristiche simili. Per esempio, su un router le interfacce Ethernet 0/0 e Ethernet 0/1 possono essere connesse alla LAN locale. Queste due interfacce sono simili poiché rappresentano la rete interna, pertanto possono essere raggruppate in una zona per le configurazioni del firewall.

ZPF Acronimo di Zone-Based Policy Firewall (Firewall con criteri basati su zone). In una configurazione ZPF, le interfacce vengono assegnate delle interfacce e viene applicato un criterio di ispezione al traffico tra le zone.

INDICE

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W