Configurazione del tunneling ripartito per i client VPN sull'appliance ASA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Esempio di rete
Prodotti correlati
Convenzioni
Premesse
Configurazione del tunneling ripartito sull'appliance ASA
Configurare ASA 7.x con Adaptive Security Device Manager (ASDM) 5.x
Configurare ASA 8.x con ASDM6.x
Configurazione di ASA 7.x e versioni successive tramite CLI
Configurazione di PIX 6.x tramite la CLI
Verifica
Connessione con il client VPN
Visualizza registro client VPN
Test dell'accesso LAN locale con ping
Risoluzione dei problemi
Limitazione del numero di voci in un ACL con tunnel suddiviso
Informazioni correlate

Introduzione

In questo documento viene descritto il processo per consentire ai client VPN di accedere a Internet durante il tunneling in un'appliance di sicurezza Cisco ASA serie 5500.

Prerequisiti

Requisiti

In questo documento si presume che sull'appliance ASA esista già una configurazione VPN ad accesso remoto funzionante. Fare riferimento a <u>PIX/ASA 7.x come server VPN remoto usando</u> <u>l'esempio di configurazione ASDM</u>, se non ne è già stato configurato uno.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Security Appliance Software versione 7.x e successive
- Cisco Systems VPN Client versione 4.0.5
- Adaptive Security Device Manager (ASDM)



Nota: questo documento contiene anche la configurazione PIX 6.x CLI compatibile con Cisco VPN client 3.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Il client VPN si trova su una tipica rete SOHO e si connette tramite Internet all'ufficio principale.



Esempio di rete

Prodotti correlati

Questa configurazione può essere utilizzata anche con il software Cisco PIX serie 500 Security Appliance versione 7.x.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

In questo documento viene spiegato dettagliatamente come consentire ai client VPN di accedere a Internet mentre sono tunneling in un'appliance di sicurezza Cisco Adaptive Security Appliance (ASA) serie 5500. Questa configurazione consente ai client VPN di accedere in modo sicuro alle risorse aziendali tramite IPsec, garantendo al contempo l'accesso non protetto a Internet.



Nota: il tunneling completo è considerato la configurazione più sicura in quanto non consente l'accesso simultaneo del dispositivo a Internet e alla LAN aziendale. Un compromesso tra il tunneling completo e il tunneling suddiviso permette ai client VPN solo l'accesso alla LAN locale. Per ulteriori informazioni, fare riferimento all'<u>esempio di configurazione PIX/ASA 7.x: Allow Local LAN Access for VPN Clients</u>.

In uno scenario di base tra client VPN e ASA, tutto il traffico proveniente dal client VPN viene crittografato e inviato all'ASA, a prescindere dalla destinazione. In base alla configurazione e al numero di utenti supportati, tale configurazione può richiedere un uso intensivo della larghezza di banda. Il tunneling ripartito può ridurre questo problema in quanto consente agli utenti di inviare solo il traffico destinato alla rete aziendale attraverso il tunnel. Tutto il resto del traffico, come la messaggistica istantanea, la posta elettronica o la navigazione casuale, viene inviato a Internet tramite la LAN locale del client VPN.

Configurazione del tunneling ripartito sull'appliance ASA

Configurare ASA 7.x con Adaptive Security Device Manager (ASDM) 5.x

Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling suddiviso per gli utenti del gruppo.

1. Scegliere Configurazione > VPN > Generale > Criteri di gruppo e selezionare i Criteri di gruppo in cui abilitare l'accesso LAN locale. Quindi fare clic su Modifica .



2. Andare alla scheda Configurazione client.

General IPSec Client Configuration Client Firewall	Hardware Client NA	IC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its value fro	om the default group policy.
General Client Parameters Cisco Client Parameter	Microsoft Client Para	ameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔽 Inherit	v.
Split Tunnel Network List:	🔽 Inherit	▼ Manage
Address pools		
Velieble Pools	Δ.	esimed Boole (un to 6 entries)
Available FOUS	^ ^ ^	sagreu Pools (up to Clerities)
	Add>>	
	< <remove< td=""><td></td></remove<>	

3. Deselezionare la casella Eredita per Criteri tunnel suddivisi e scegliere Tunnel Network List Below.

career far ar oup to ney thin taney tpri			
Name: hillvalleyvpn			
General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN	
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.	
	1		
General Client Parameters Cisco Client Parameters	Microsoft Client	Parameters	1
Banner	☑ Inherit	Edit Banner	
	1 million		
Default Domain:	🔽 Inherit		
Colit Tunnel DNC Manage (analog definited)	-		
Spit Tunnei DNS Names (space deimited).	iv innent	1	
Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks	
		Tunnel All Networks	
Split Tunnel Network List:	🔽 Inherit	Tunnel Network List Below	l
- Advess pode			
			l
Avaïable Pools		Assigned Pools (up to 6 entries)	l
	Add>>		I
	< <remove< td=""><td>i l</td><td></td></remove<>	i l	

Deselezionare la casella di controllo Eredita per Elenco reti tunnel suddivise, quindi fare clic su Gestisci per avviare Gestione ACL.

nternal Group Policy: hillvalley v pn		
Name: hilvalleyvpn		
eneral IPSec Client Configuration Client Firewall	Hardware Client	
andrai (17360) andra den ingen andra (Calori, Filleyrai)	Thank ware client	
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Parameters	s Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	I∕ Inherit	J
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 İnherit	None Manage
Address pools		
🔽 Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add≽⊳	
	< <remove< td=""><td>1</td></remove<>	1

In Gestione ACL, selezionare **Aggiungi > Aggiungi ACL...** per creare un nuovo elenco degli accessi.

ACL Manager					1. 1.	<u>(</u>)		X
Stendard AG. Edended	ACL.							
◆ Add → 📑 545. 🎁	arkte 🕈	4 美術	BL -					1
Add AGL	dress	Action		Description				
BLASHACE. 10								
The insert Atter.								

Specificare un nome per l'ACL e fare clic su OK.

•	ACL Manager		_			<u>×</u>
	Add - Eden	066ACL 首 05355 카 - 4	X % 85 -	•		
	No	Address	Adlon	Description		
			Add ACL	Tell Trend Link	X	
			ox.	Carca	Here	
	Rule Flow Diagram		34	inside outsi	te ja	×
				🔶 🗸 deny	•	
			OK	Cancel	Pep	

Dopo aver creato l'ACL, selezionare Add > Add ACE. .per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).



Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.0.1.0/24.

a.

Scegliere Autorizza .

b.

Scegliere un indirizzo IP di 10.0.1.0

c.

Selezionare una maschera di rete di 255.255.255.0.

d.

(Facoltativo) Fornire una descrizione.

Fate clic su > OK.

a ACC STRUMES	2
Standard ACL Extended ACL	
◆ Add - Ⅲ (-2: ① Delete + 4 🐰 🛍 🛍 -	
No Address Action Desolution	
Spit_Turnel_List	
🕼 Add AKE	
- Action	
Action 🗣 Power 💌	
Hort/Hertwork	
P Address: 10010	
Hetwask: 255.255.255.0	
Description	
The carpone memory company rate.	
OK Carca Heap	
Ruie Row Diagram	x
3	

Per uscire da Gestione ACL, fare clic su OK.

•

e.



Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.

Nerre: PilvaReyrpn General PSac Clerit Configuration Clerit Pirewall Hardware Clerit NAC WeivVPil Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters General Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters Elst Elstrongen	Neme: Neme: General IPSic Clert Configuration Clert Preveal Hardware Clert NAC WebVPN Check an inhert checkbox to let the corresponding setting take its value from the default group policy. General Clert Parameters Clecc Clert Parameters Microsoft Clert Parameters Banner: IP Innel IP Innel Eff Parver. Default Donveix IP Innel IP Innel IP Parver. Spit Tunnel DMS Names (space definited): IP Innel Ip Innel Network Llet: IP Innel IP Innel INT INNEL Manage Address pools Address pools Address Address (pools (poils Fiertnes)) Address Immediate Pools Address Fools (poils Fiertnes) Address Address Address Immediate Pools Address Intert In	Edit Internal Group Policy: hillvalleyvpn		
General PSec Clert Configuration Clert Reswall Hardware Clert NAC WebWPN Check as Inherit checkbox to let the corresponding setting take its value from the default group policy. General General Edr. Borner. Default Clert Parameters Cloco Clert Parameters Microsoft Clert Parameters Biorner. Default Dowar Inherit Edr. Borner. Default Dowar Inherit Edr. Borner. Spit Tunnel DNS Nemes (space definited): Inherit Turnel Network List Below Inherit Spit Tunnel Policy: Inherit Spit Turnel Network List Below Inherit Addresse pools Cutsite_cryptional None - Addresse pools Cutsite_cryptional None - Addresse pools Cutsite_cryptional Cutsite_cryptional Inherit Cutsite_cryptional Cutsite_cryptional Addresse pools Cutsite_cryptional Cutsite_cryptional Inherit Cutsite_cryptional Cutsite_cryptional Inherit Cutsite_cryptional Cutsite_cryptional Inherit Cutsite_cryptional Cutsite_cryption Inherit </th <th>Operand [PSec] Clerk Configuration Clerk Firewall Hardware Clerk [NAC] Web/VPN Check an Inhert checkbox to let the corresponding setting take its value from the default group policy. Central Clerk Parameters Claco Clerk Parameters Banner: Inhert Default Domain: Inhert Spit Tunnel DNS Names (space definited): Inhert Spit Tunnel Policy: Inhert Spit Tunnel Network Liet: Inhert Address pools Address pools Address pools Address Address pools Address Inhert Address pools Inhert Inhert</th> <th>New New Pillesterre</th> <th></th> <th></th>	Operand [PSec] Clerk Configuration Clerk Firewall Hardware Clerk [NAC] Web/VPN Check an Inhert checkbox to let the corresponding setting take its value from the default group policy. Central Clerk Parameters Claco Clerk Parameters Banner: Inhert Default Domain: Inhert Spit Tunnel DNS Names (space definited): Inhert Spit Tunnel Policy: Inhert Spit Tunnel Network Liet: Inhert Address pools Address pools Address pools Address Address pools Address Inhert Address pools Inhert Inhert	New New Pillesterre		
General PSec Clerct Contiguration Clerct Firewall Handware Clerct NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Clerct Parameters Clerct Parameters General Clerct Parameters Clerct Parameters Microsoft Clerct Parameters Edit Dorver. Berner: Image: Image: Image: Edit Dorver. Default Dorver. Image: Image: Image: Image: Split Tunnel DNS Names (space delimited): Image: Image: Image: Image: Split Tunnel Network List: Image: Image: Image: Image: Image: Address pools Clerct Parameters Address pools Clerct Parameters Address pools Clerct Parameters Manage: Address pools Clerct Parameters Address Clerct Parameters Address Clerct Parameters Manage: Address pools Clerct Parameters Address Clerct Parameters Manage: Image: Address pools Clerct Parameters Address Clerct Parameters Image: Image:	General PSec Clerct Contiguration Clerct Firewall Hardware Clert NAC WebVPN Check an Inhert checkbox to let the corresponding setting take its value from the default group policy. General Clerct Parameters Cloco Clert Parameters Microsoft Clert Parameters Banner: Image: Image: Edit Parameters Default Domain: Image: Image: Image: Split Tunnel DNS Names (space delimited): Imment Tunnel Network List Below Image: Split Tunnel Policy: Imment Imment Image: Image: Address pools Imment Edit Store - Set Manage: Image: Image: Address pools Edit Store - Set Edit Store - Set Edit Store - Set Image: Image: Address pools Edit Store - Set Edit Store - Set Edit Store - Set Edit Store - Set Image: Image: Address pools Edit Store - Set Edit Store - Set Image: Image:<	mane. parrancjipri		
Check as Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Cloco Client Parameters Benner: Image: Edr Borner. Default Domain: Imherit Spit Tunnel DNS Names (space delimited): Imherit Spit Tunnel Policy: Imherit Spit Tunnel Network List: Imherit Addresse pools Odd Kinger Pools Addresse pools Odd Kinger Pools Addresse pools Control List Addresse pools Control List Addresse pools Control List Control List Control List Addresse pools Control List Control List Control List	Check an inherit checkbox to let the corresponding setting take its value from the defauit group policy. Central Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters Banner: Defauit Donvein: Defauit Donvein: Defauit Donvein: Split Tunnel DMS Names (space delivited): Split Tunnel Network List: Split Tunnel Network List: None Address pools Nordiste Epoils Addres Addres Addres Cool (op to 5 entres) Addres ddres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addres Addre	General IPSec Client Configuration Client Firewal	Hardware Client	NAC WebVPN
Ceneral Client Parameters Cisco Client Parameters Berner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Spit Tunnel Network List: Inherit Address pools Address pools Address pools Address pools Address pools Address Address pools Address Address pools Address	Central Clert Parameters Disco Clert Parameters Banner: Inhert Default Donvain Inhert Spit Tunnel DNS Names (space delinited): Inhert Spit Tunnel Policy: Inhert Spit Tunnel Network List: Inhert Address pools Stit Tunnel List Address pools Address Address Address Address Address Address Address	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Berner: Inhest Detaut Domein: Inhest Spit Tunnel DAS Nenes (space delinited): Inhest Spit Tunnel Policy: Inhest Spit Tunnel Network List: Inhest Spit Tunnel Network List: Inhest Address pools Inhest Address pools Address Address pools Address Address pools Address Address pools Address	Berner: Inherit Detault Donveix Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Address pools Spit Tunnel List Address Address Address Spit Tunnel Network Dist Distributed	General Clent Parameters Cloco Clent Parameter	s Microsoft Client	Parameters
Berner: Image: Convert Default Donveix Image: Convert Spit Tunnel DNS Names (space delimited): Immerit Spit Tunnel Policy: Immerit Spit Tunnel Policy: Immerit Spit Tunnel Network List: Immerit Address pools Immerit Address pools Outside_cryptomax Address pools Address Address Address Address Address Address Address	Berner: Image: Edit Edite Default Donveix Image: Im	,		
Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Intent: Spit Tunnel Network List: Intent: Address pools Address pools Address Address <td>Default Domain: Spit Turnel DNS Names (space delimited): Spit Turnel Policy: Inherit Spit Turnel Network List: Inherit Spit Turnel Network Spit Turnel Network Inherit Spit Turnel Network Inherit Spit Turnel Network Spit Tur</td> <td>Banner.</td> <td>🔽 Inhert</td> <td>Edt Borner</td>	Default Domain: Spit Turnel DNS Names (space delimited): Spit Turnel Policy: Inherit Spit Turnel Network List: Inherit Spit Turnel Network Spit Turnel Network Inherit Spit Turnel Network Inherit Spit Turnel Network Spit Tur	Banner.	🔽 Inhert	Edt Borner
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Inherit Address pools Address Address Inherit Address Address Inherit Address Inherit Inhe	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Inherit Address pools Address	Destauit Downein:	E interit	
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Inherit Spit Tunnel Network List: Inherit Address pools Address po	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List Inherit Address pools Ad	L-C-MARK DAMINGS	1. BERN	
Spit Tunnel Policy: Spit Tunnel Network List: Inhert: Address pools: Address pools: Address pools: Address pools: Address pool: Address pool: <tr< td=""><td>Spit Turnel Policy: Spit Turnel Network List: Intent Spit Turnel Network List: Intent Address pools tr< td=""><td>Split Tunnel DNS Names (space delimited):</td><td>P Inherit</td><td></td></tr<></td></tr<>	Spit Turnel Policy: Spit Turnel Network List: Intent Spit Turnel Network List: Intent Address pools Address pools <tr< td=""><td>Split Tunnel DNS Names (space delimited):</td><td>P Inherit</td><td></td></tr<>	Split Tunnel DNS Names (space delimited):	P Inherit	
Spit Tunnel Network List: Address pools	Spit Tunnel Network List Address pools Address Address <td>Split Tunnel Policy:</td> <td>[] Interit</td> <td>Turnel Network List Below</td>	Split Tunnel Policy:	[] Interit	Turnel Network List Below
Spit Turnel Network List: Address pools Address pools <t< td=""><td>Spit Tunnel Network List: Address pools Address A</td><td></td><td></td><td></td></t<>	Spit Tunnel Network List: Address pools Address A			
Address pools Address pools Available Pools Address A	Address pade Interit Available Pade Address Address pade Available Pade Address Addre	Spilt Tunnel Network List:	[Inhert	Splt_TurneU Manage
Available Roots Accigned Roots (up to 6 ontries)	Image: Sector	-Address pools		Spit_Turnel_List
Available Pools Addree	Available Pools Addree collemove	F interit		outside_cryptomap ⁵
Addree	Addive	Avaitable Pools		Assigned Pools (up to 6 entries)
< diemone			Addres	1
			collemone	il l
				1

Per tornare alla configurazione di Criteri di gruppo, fare clic su OK.

٠

i 💼 Bi	dit Int	ernal Grou	p Policy: hillvalle	ayvpn				×
	No	me pi	livaleyvpn					
	Gen	eral PSec	Client Configuratio	n Client Firewal H	ardware Client	NAC WebVPN		
	a	heck an Inha	nt checkbox to let t	he corresponding set	ing take its valu	e from the default group p	olicy.	
	G	enerai Client	Parameters Cloco	o Client Parameters 1	Vicrosoft Client	Parametora		
		Banner:			🖂 Inherit	Est Envie		
		Default Dor	main:		🖂 inherit			
		Spit Tunne	DNS Names (spac	e delmited):	🖓 inherit			
		Split Tunne	i Policy:		T interit	Turnel Network List Be	ow 💌	
		Split Tunne	Network List:		[Inherit	Spit_Turnel_L ¥	Manage	
		-Address p	ools				1	

Per inviare i comandi all'appliance ASA, fare clic su Apply e quindi su Send (se necessario).

٠



Configurare ASA 8.x con ASDM 6.x

Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling suddiviso per gli utenti del gruppo.

Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo e scegliere i Criteri di gruppo in cui abilitare l'accesso LAN locale. Quindi fare clic su Modifica.

A total (Col ca) Contract			
A HOD COL Delete			
Name	Type	Tunneling Protocol	
DRtGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N(A
OfftGrpPolicy (System Default) Defaultgroup	Internal	L2TP-IPSec, IPSec, webvpn Inherited	N/A

Fare clic su Tunneling ripartito.

📬 Edit Internal Group Policy:	y: hivalleyvpn	
General Servers Advanced -12 Browser Proxy B-SSL VPN Client -19 Prec Client	Split tunneling network lists distinguish networks that require traffic to go through the tunnel require tunneling. The security appliance makes split tunneling distions on the basis of a net ACL that consists of list of addresses on the private network. DNS Names: 🔽 Inherit Policy: 🔽 Inherit	l and those that do no teoric list, which is an
Clent Access Rule Clent Firewal	Network List: 🖂 [inherit]	· Matega
151511414 54015	Intercept DHCP Configuration Message from Micosoft Clients	
	Intercept: 🔽 Inherit C 🕬 C No	
	Subnet Mask (Optional): 0.0.0.0	Y

Deselezionare la casella **Eredita** per Criteri tunnel suddivisi e scegliere **Elenco reti tunnel di seguito**.

ſ	Edit Internal Group Policy:	: hivalleyvpn	
	General Gervers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and the require tunneling. The security appliance makes split tunneling decisions on the basis of a network list ACL that consists of list of addresses on the private network.	se that do no , which is an
	-IE Browster Procy (E)-53L VPN Client	DNS Names: 🖂 Inhant Turnel Network List Below	
	 Orec Clent Clent Access Rule Clent Preval 	Network List: 17 Inherit Tunnel Al Network List Delaw	Managa
	- Hardware Client	Exclude Network Ust Below	-
		Intercept UNCP Configuration Plessage from Pacoson Cliencs	<u> </u>
		prior to XP, DHCP Intercept provides the domain name and subnet mask.	

Deselezionare la casella di controllo Eredita per Elenco reti tunnel suddivise, quindi fare clic su Gestisci per avviare Gestione ACL.

f	Edit Internal Group Policy:	i hiralleyvpn
	General Servers Ə. Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
	- 22 Browser Prozy - 35, VPN Client	DNS Names: 🖓 Inherit
		Pokcy: Inherit Turnel Network List Berow * Network List: Enherit None * Manage)
	Hardware Clenk	Intercept DHCP Configuration Message from Micosoft Clients
		DHCP Intercept lets Microsoft XP clents use split tunneling with the security appliance. For Windows clents prior to XP, DHCP Intercept provides the domain name and subnet mask.
		Intercept: 🔽 Inherit - C. No.
		Subret Mask (Optiona): 0.0.0.0

In Gestione ACL, selezionare Aggiungi > Aggiungi ACL... per creare un nuovo elenco degli accessi.



Specificare un nome per l'ACL e fare clic su OK.

•

Standard ACL Exter	ided ACL	4 X Pa 18	L +	
No. 1	Address J	V do mili la	Description	F
	Act, Nar	ACL ne: Split_Turnel_Ust	Help	

Una volta creato l'ACL, scegliere **Aggiungi > Aggiungi ACE...** per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).



Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.0.1.0/24.

a.

Fare clic sul pulsante di opzione Autorizza.

b.

Scegliere l'indirizzo di rete con maschera 10.0.1.0/24.

c.

(Facoltativo) Fornire una descrizione.

d.

Fare clic su OK.

📫 ACL Manager					
Standard ACL Extended AC	1				
🗢 Add 👻 🔟 Edt 📋 🕻	Selote 🕈 🗲 👗	Ra 10, -			
No Addr	ess Action		Description		
Split_Turnel_List					
	- A 44 AFT			and the second se	-
	1 HOU HEE				
	Action: (* Permit (Deny			
	Address: 10.0.1.0/24			17	
	Description:				
	The Corporate natwork b	whind the ASA			
	1				
		OK.	Cancel	Help	
			and 1		

Per uscire da Gestione ACL, fare clic su OK.

ACL Manager				and the second second	
Standard ACL Extend	ind act 1				
A ALL PARTY	and the second s		Des atta		
🏶 Add 🔹 🥑 Edt	Delete 7	* *	•B III -		
No	Address	Action		Description	
E Split_Tunnel_List			-		inter and
1 1 10.0.1	0/24	Permit	The Corpora	ste network behind	the ASA
			(Con)	i and i	in the second

Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.

Clent Access Rule Clent Presail Hardware Clent Hardware Clent Intercept DHCP Config Spit_Turnel_List DHCP Intercept lets Microsoft XP clents use spit turneling with the security appliance. For Windows clents prior to XP, DHCP Intercept provides the domain name and subnet mask.	5	Colt Internal Group Policy General General Advanced Colt Turneling E Browser Proxy B-SS, VPN Client G-TEsec Client	hivelicyvpn Spik tunneling retwork lists distinguish networks that require traffic to go through the tunnel and those that or require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is ACL that consists of list of addresses on the private network. DNS Names: Image: Image: Tunnel Network List Delow Policy: Image: Tunnel Network List Delow	lo ne s an
Intercept: 🔽 Inherit - C No.		- Clent Access Rule - Clent Freeval - Hardware Clent	Network List:	*

Per tornare alla configurazione di Criteri di gruppo, fare clic su OK.

•

	Edit Internal Group Polic	y: hivalleyvpn		
	General Servers Advanced	Split tunneling network list require tunneling. The sec ACL that consists of list of	s distinguish networks that require traffic to go through the tunn unity appliance makes split tunneling decisions on the basis of a r addresses on the private network.	el and those that do not setwork list, which is an
	IE Browser Proxy	045 Names: 🔽 Inherit		
i⊞-SSL VPN Clent ⊞-IPsec Clent	Policy: 🕅 Inherit	Tunnel Network List Below	*	
	NetworkList: 🗖 Inherit	Split_Tunnel_List	* Manage	
	Intercept DHCP Confi	guration Message from Micosoft Clients		
	DHCP Intercept lets Micr prior to XP, DHCP Interc	cooft XP clients use split tunneling with the security appliance. Fr apt provides the domain name and subnet mask.	or Windows clients	
		Intercept: 🖂 Inherit	C Yes C No	
			Submet Maski (Optional): 0.0.0.0	Ψ.

Per inviare i comandi all'appliance ASA, fare clic su Apply e quindi su Send (se necessario).

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored intermexternally on a RADBUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Туре	Tunneling Protocol	
OfbGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N(A -
Defaultgroup	Internal	Inherited	N/A
ivalleyvpn	Internal	svc, IPSec	N/A -

Configurazione di ASA 7.x e versioni successive tramite CLI

Anziché utilizzare ASDM, è possibile completare i seguenti passaggi nella CLI dell'ASA per consentire il tunneling suddiviso sull'appliance ASA:



Nota: la configurazione del tunneling con split CLI è la stessa per entrambe le appliance ASA 7.x e 8.x.

Accedere alla modalità di configurazione.

<#root>

٠

ciscoasa>

enable

Password: ******* ciscoasa#

configure terminal

ciscoasa(config)#

Creare l'elenco degli accessi che definisce la rete dietro l'appliance ASA.

<#root>

•

ciscoasa(config)#

access-list Split_Tunnel_List remark The corporate network behind the ASA.

ciscoasa(config)#

access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

Accedere alla modalità di configurazione di Criteri di gruppo per il criterio che si desidera modificare.

<#root>

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

Specificare i criteri per il tunnel suddiviso. In questo caso il criterio è specificato tramite tunneling.

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

Specificare l'elenco degli accessi al tunnel suddiviso. In questo caso, l'elenco è Split_Tunnel_List.

<#root>

٠

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split_Tunnel_List

Immettere questo comando

٠

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

Associare i Criteri di gruppo al gruppo di tunnel

<#root>

•

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

Uscire dalle due modalità di configurazione.

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

٠

Salvare la configurazione nella memoria RAM non volatile (NVRAM) e premere **Invio** quando richiesto per specificare il nome del file di origine.

<#root>

ciscoasa#

copy running-config startup-config

Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec) ciscoasa#

Configurazione di PIX 6.x tramite la CLI

Attenersi alla seguente procedura:

٠

Creare l'elenco degli accessi che definisce la rete dietro al PIX.

<#root>

PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

• Creare un gruppo vpn **vpn3000** e specificare l'ACL del tunnel suddiviso come mostrato:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



Nota: per ulteriori informazioni sulla configurazione della VPN di accesso remoto per PIX 6.x, fare riferimento a <u>Cisco Secure PIX</u> <u>Firewall 6.x e Cisco VPN Client 3.5 per Windows con autenticazione RADIUS IAS Microsoft Windows 2000 e 2003</u>.

Verifica

Per verificare la configurazione, completare la procedura descritta in queste sezioni.

Connessione con il client VPN

Visualizza registro client VPN

Test dell'accesso LAN locale con ping

Connessione con il client VPN

•

•

•

Connettere il client VPN a VPN Concentrator per verificare la configurazione.

Connection Entries Status Certificates Log Cisco Status Cisco <td< th=""><th>👌 VPN Client - Version 4.0.5 (Rel)</th><th></th><th></th></td<>	👌 VPN Client - Version 4.0.5 (Rel)		
Import Import New Import Import Modily Delete Import	Connection Entries Status Certificates Log	Options Help	
Connection Entries Certificates Log Connection Entry Host Transport Hillvalleyypin 172.22.1.160 IPSec/UDP	Connect New Import Mi	odity Delete	Cisco Systems
Connection Entry Transport hillvalleyvpn 172.22.1.160	Connection Entries Certificates Log		
hilveleyvpn 172.22.1.160 IPSecAUDP	Connection Entry	Host	Transport
	hilvaleyvpn	172.22.1.160	IPSec/UDP
	a		

Selezionare la voce di connessione dall'elenco e fare clic su Connetti.

Immettere le credenziali.

👌 VPN Client U	er Authen	tication l	for "hillvalle;	yvpn"	×
Cisco Systems	<u>U</u> sername: <u>P</u> assword:	marty	OK		Cancel

Scegliere **Stato > Statistiche...** per visualizzare la finestra Dettagli tunnel, in cui è possibile esaminare i dettagli del tunnel e verificare il flusso del traffico.

•

•

unnel Details	Route Details	Firewal	
Address Info	rmation	Connection Information	1
Client:	10.0.1.50	Entry:	hillvalley2
Server	172.22.1.160	Time:	0 day(s), 00:00.25
Bytes		Crypto	
Received:	0	Encryption:	168-bit 3-DES
Sent	1494	Authentication:	HMAC-SHA1
Packets		Transport	
Encrypted:	9	Transparent Tunneling	Inactive
Decrypted	0	Local LAN:	Disabled
Discarded:	0	Compression:	None
Bypassed:	159		
			Reset
			Close

Per visualizzare le route che il client VPN sta proteggendo verso l'appliance ASA, andare alla scheda Dettagli route.

Nell'esempio, il client VPN sta proteggendo l'accesso a 10.0.1.0/24, mentre tutto il resto del traffico non è crittografato e non viene inviato attraverso il tunnel.

👌 VPN Client 🖇	Statistics			×
Tunnel Details	Route Details Frew	al		
Local LAN Rou	ites 🗟	Secured Rou	tes	
Network	Subnet Mask	Network	Subnet Mask	
		10.0.1.0	255.255.255.0	

Visualizza registro client VPN

Quando si esamina il registro del client VPN, è possibile determinare se è impostato o meno il parametro che specifica la suddivisione del tunneling. Per visualizzare il log, andare alla scheda Log nel client VPN. Quindi fare clic su **Log Settings** (Impostazioni registro) per regolare i dati registrati. Nell'esempio, IKE è impostato su **3 - Alta** mentre tutti gli altri elementi del log sono impostati su **1 - Bassa**.

VPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO STATEMS
Connection Entries Certificates Log	
Cisco Systems VPN Client Version 4.0.5 [Ref/C Copyright (C) 1999-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2	
Not connected.	

Cisco Systems VPN Client Version 4.0.5 (Rel) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2

1 14:20:09.532 07/27/06 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 172.22.1.160.

!--- Output is supressed

18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator

19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy).

20 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion Prevention Security Agent, Capability= (Are you There?).

21 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160

22 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160

23 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.160

24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010

MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 26 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 27 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x630000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x000000130 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0mask = 255.255.255.0protocol = 0src port = 0dest port=0 !--- Output is supressed.

Test dell'accesso LAN locale con ping

Per verificare che il client VPN sia configurato per il tunneling suddiviso quando è tunneling all'ASA, è possibile usare anche il comando **ping** sulla riga di comando di Windows. La LAN locale del client VPN è 192.168.0.0/24 e sulla rete è presente un altro host con indirizzo IP 192.168.0.3.

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
```

Risoluzione dei problemi

Limitazione del numero di voci in un ACL con tunnel suddiviso

È presente una restrizione relativa al numero di voci in un ACL usato per il tunnel suddiviso. Si consiglia di non utilizzare più di 50-60 voci ACE per una funzionalità soddisfacente. È consigliabile implementare la funzionalità di subnet per coprire un intervallo di indirizzi IP.

Informazioni correlate

- <u>PIX/ASA 7.x come server VPN remoto con configurazione ASDM</u>
- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).