ASA 8.X e versioni successive: Aggiunta o modifica di un elenco degli accessi tramite l'esempio di configurazione dell'interfaccia utente grafica di ASDM

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione](#)
[Esempio di rete](#)
[Aggiungi nuovo elenco accessi](#)
[Creazione di un elenco degli accessi standard](#)
[Creare una regola di accesso globale](#)
[Modifica elenco accessi esistente](#)
[Eliminare un elenco degli accessi](#)
[Esporta la regola di accesso](#)
[Esportare le informazioni dell'elenco accessi](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Questo documento spiega come usare Cisco Adaptive Security Device Manager (ASDM) per usare le liste di controllo degli accessi. Tra queste, la creazione di un nuovo elenco degli accessi, la modifica di un elenco degli accessi esistente e altre funzionalità relative agli elenchi degli accessi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco Adaptive Security Appliance (ASA) con versione 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) con versione 6.3.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.

Convenzioni

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

Premesse

Gli elenchi degli accessi vengono utilizzati principalmente per controllare il flusso del traffico attraverso il firewall. È possibile consentire o negare tipi specifici di traffico con elenchi degli accessi. Ogni elenco degli accessi contiene diverse voci di elenco degli accessi (ACE) che controllano il flusso di traffico da un'origine specifica a una destinazione specifica. In genere, l'elenco degli accessi è associato a un'interfaccia per notificare la direzione del flusso in cui deve cercare. Gli elenchi degli accessi sono classificati principalmente in due categorie generali.

1. Elenchi accessi in entrata
2. Elenchi accessi in uscita

Gli elenchi degli accessi in entrata si applicano al traffico che entra nell'interfaccia, mentre gli elenchi degli accessi in uscita si applicano al traffico che esce dall'interfaccia. La notazione in entrata/in uscita si riferisce alla direzione del traffico in termini di quell'interfaccia, ma non al movimento del traffico tra le interfacce di sicurezza superiore e inferiore.

Per le connessioni TCP e UDP non è necessario un elenco degli accessi per consentire la restituzione del traffico, in quanto l'appliance di sicurezza consente la restituzione di tutto il traffico per le connessioni bidirezionali stabilite. Per i protocolli senza connessione, ad esempio ICMP, l'appliance di sicurezza stabilisce sessioni unidirezionali, quindi è necessario disporre di elenchi degli accessi per applicare elenchi degli accessi alle interfacce di origine e di destinazione in modo da consentire l'ICMP in entrambe le direzioni, oppure è necessario abilitare il motore di ispezione ICMP. Il motore di ispezione ICMP tratta le sessioni ICMP come connessioni bidirezionali.

Da ASDM versione 6.3.X è possibile configurare due tipi di elenchi degli accessi.

1. Regole di accesso interfaccia
2. Regole di accesso globali

Nota: la regola di accesso fa riferimento a una singola voce dell'elenco degli accessi (ACE, Access List Entry).

Le regole di accesso all'interfaccia sono associate a qualsiasi interfaccia al momento della

creazione. Senza associarli a un'interfaccia, non è possibile crearli. Si tratta di un comportamento diverso rispetto all'esempio della riga di comando. Dalla CLI, è necessario creare prima l'elenco degli accessi con il comando **access list**, quindi associare l'elenco degli accessi a un'interfaccia con il comando **access-group**. ASDM 6.3 e versioni successive, l'elenco degli accessi viene creato e associato a un'interfaccia come un singolo task. Ciò si applica solo al traffico che attraversa quell'interfaccia specifica.

Le regole di accesso globale non sono associate ad alcuna interfaccia. Possono essere configurati tramite la scheda ACL Manager in ASDM e applicati al traffico in entrata globale. Vengono implementati quando esiste una corrispondenza basata sull'origine, la destinazione e il tipo di protocollo. Queste regole non vengono replicate su ciascuna interfaccia, consentendo di risparmiare spazio di memoria.

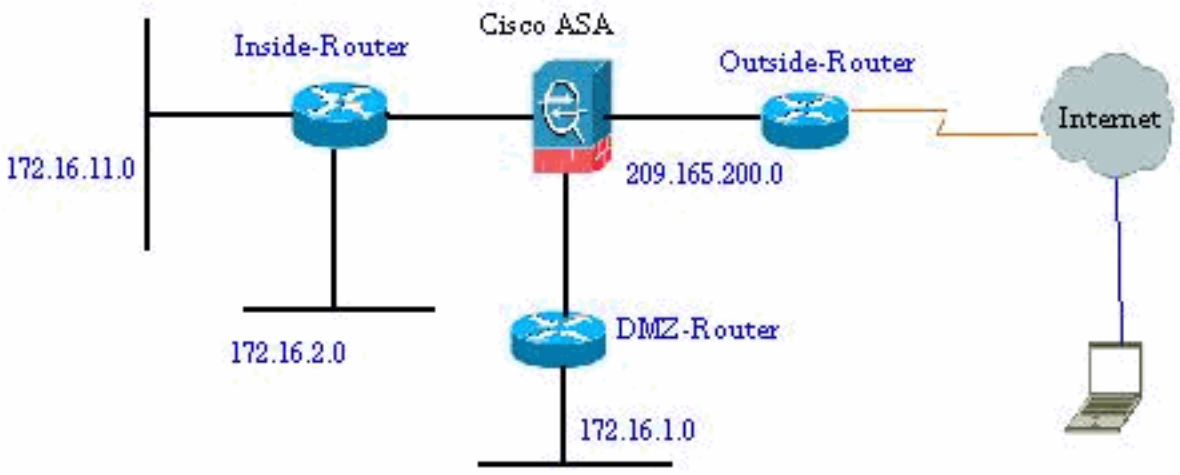
Quando devono essere implementate entrambe queste regole, le regole di accesso all'interfaccia hanno in genere la precedenza sulle regole di accesso globali.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

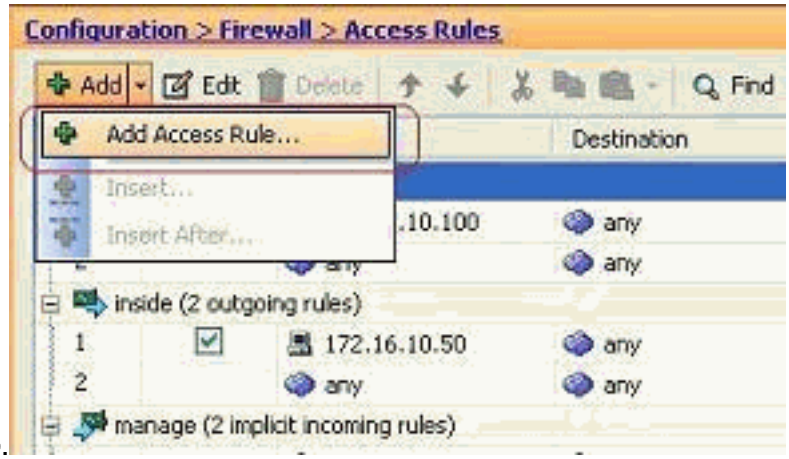
Nel documento viene usata questa impostazione di rete:



Aggiungi nuovo elenco accessi

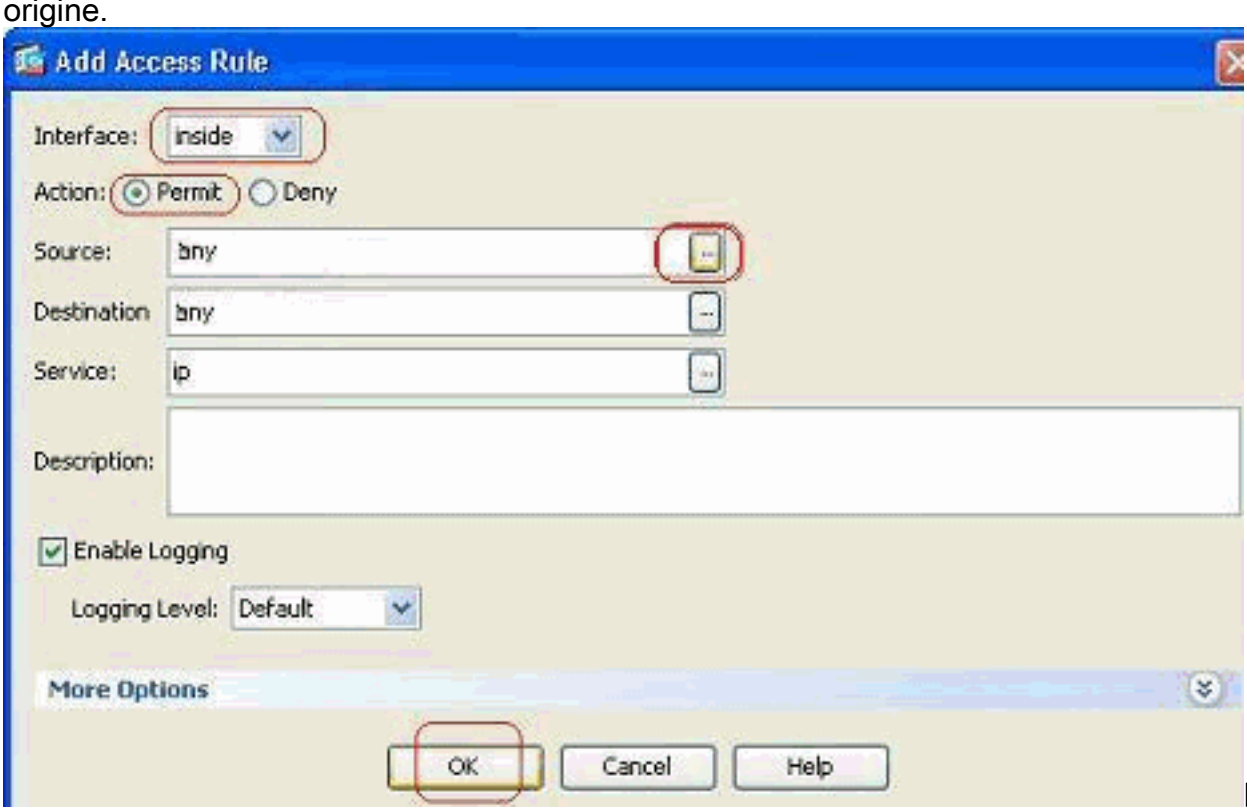
Per creare un nuovo elenco degli accessi con ASDM, completare i seguenti passaggi:

1. Scegliere **Configurazione > Firewall > Regole di accesso**, quindi fare clic sul pulsante



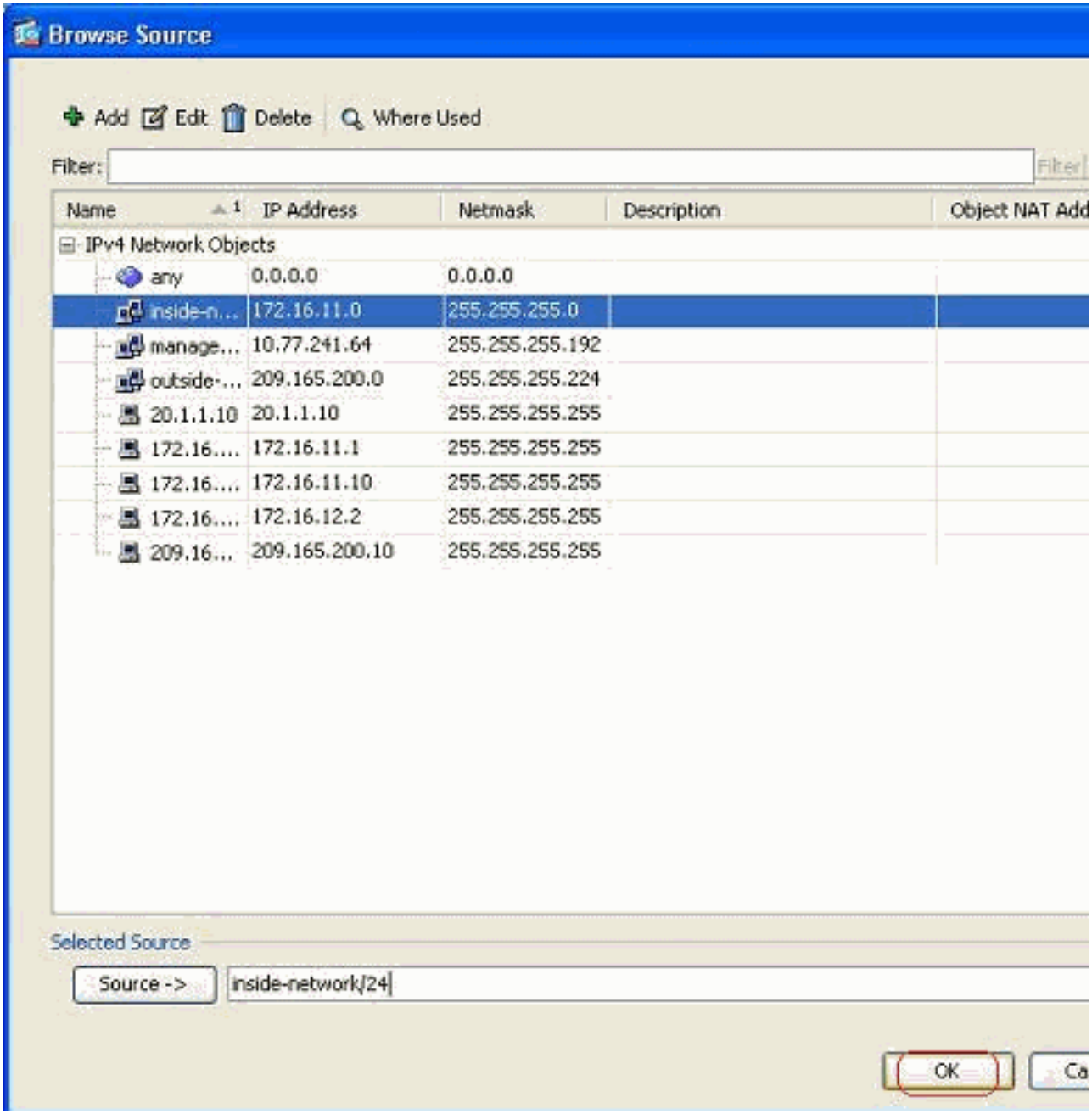
Aggiungi regola di accesso.

2. Selezionare l'interfaccia a cui deve essere associato l'elenco degli accessi, insieme all'azione da eseguire sul traffico, ad esempio consenti/nega. Quindi, fare clic sul pulsante **Details** (Dettagli) per selezionare la rete di origine.

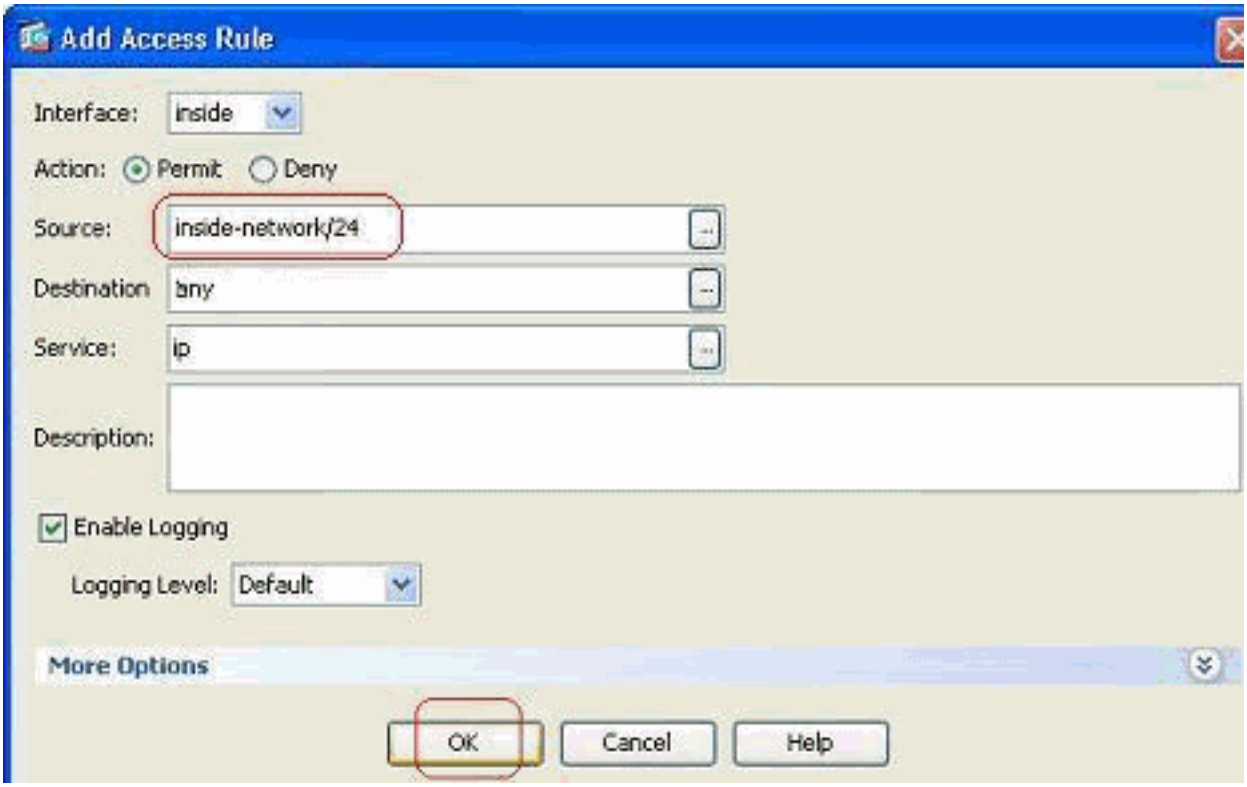


Nota: di seguito è riportata una breve spiegazione dei diversi campi visualizzati in questa finestra:**Interfaccia**: determina l'interfaccia a cui è associato l'elenco degli accessi.**Azione (Action)** - Determina il tipo di azione della nuova regola. Sono disponibili due opzioni. **Permit** consente tutto il traffico corrispondente e **Deny** blocca tutto il traffico corrispondente.**Origine**: questo campo specifica l'origine del traffico. Può trattarsi di un indirizzo IP singolo, di una rete, di un indirizzo IP di interfaccia del firewall o di un gruppo di oggetti di rete. Per selezionarli, usare il pulsante **Dettagli**.**Destinazione**: questo campo specifica l'origine del traffico. Può trattarsi di un indirizzo IP singolo, di una rete, di un indirizzo IP di interfaccia del firewall o di un gruppo di oggetti di rete. Per selezionarli, usare il pulsante **Dettagli**.**Servizio**: questo campo determina il protocollo o il servizio del traffico a cui viene applicato l'elenco degli accessi. È inoltre possibile definire un gruppo di servizi contenente un insieme di protocolli diversi.

3. Dopo aver fatto clic sul pulsante **Dettagli**, viene visualizzata una nuova finestra contenente gli oggetti di rete esistenti. Selezionare la **rete interna** e fare clic su **OK**.



4. Viene visualizzata di nuovo la finestra **Aggiungi regola di accesso**. Digitare **any** nel campo Destinazione. e fare clic su **OK** per completare la configurazione della regola di accesso.



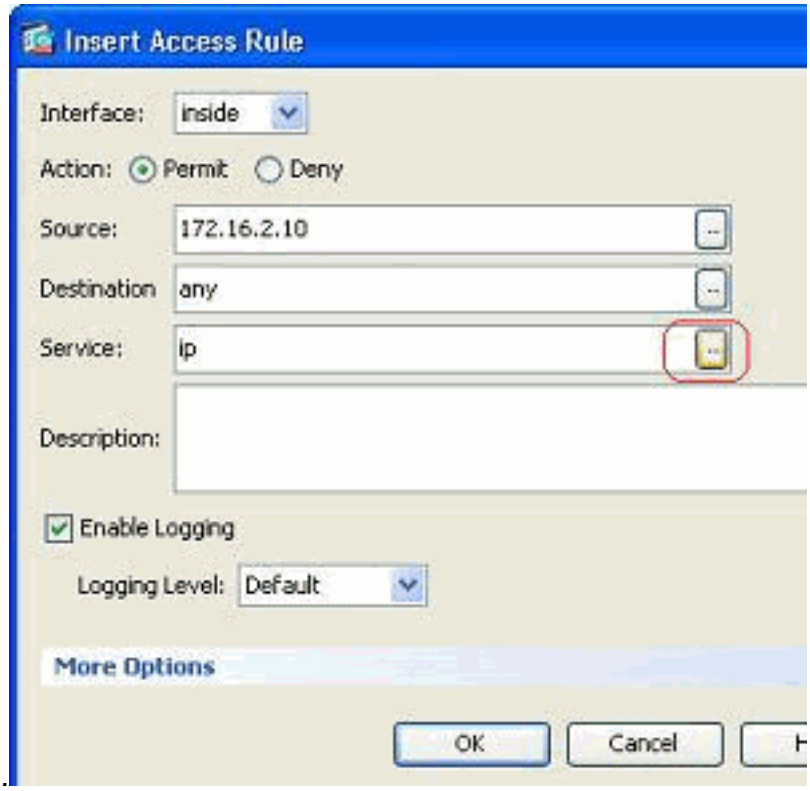
Aggiungere una regola di accesso prima di una regola esistente:

Completare la procedura seguente per aggiungere una regola di accesso immediatamente precedente a una regola di accesso già esistente:

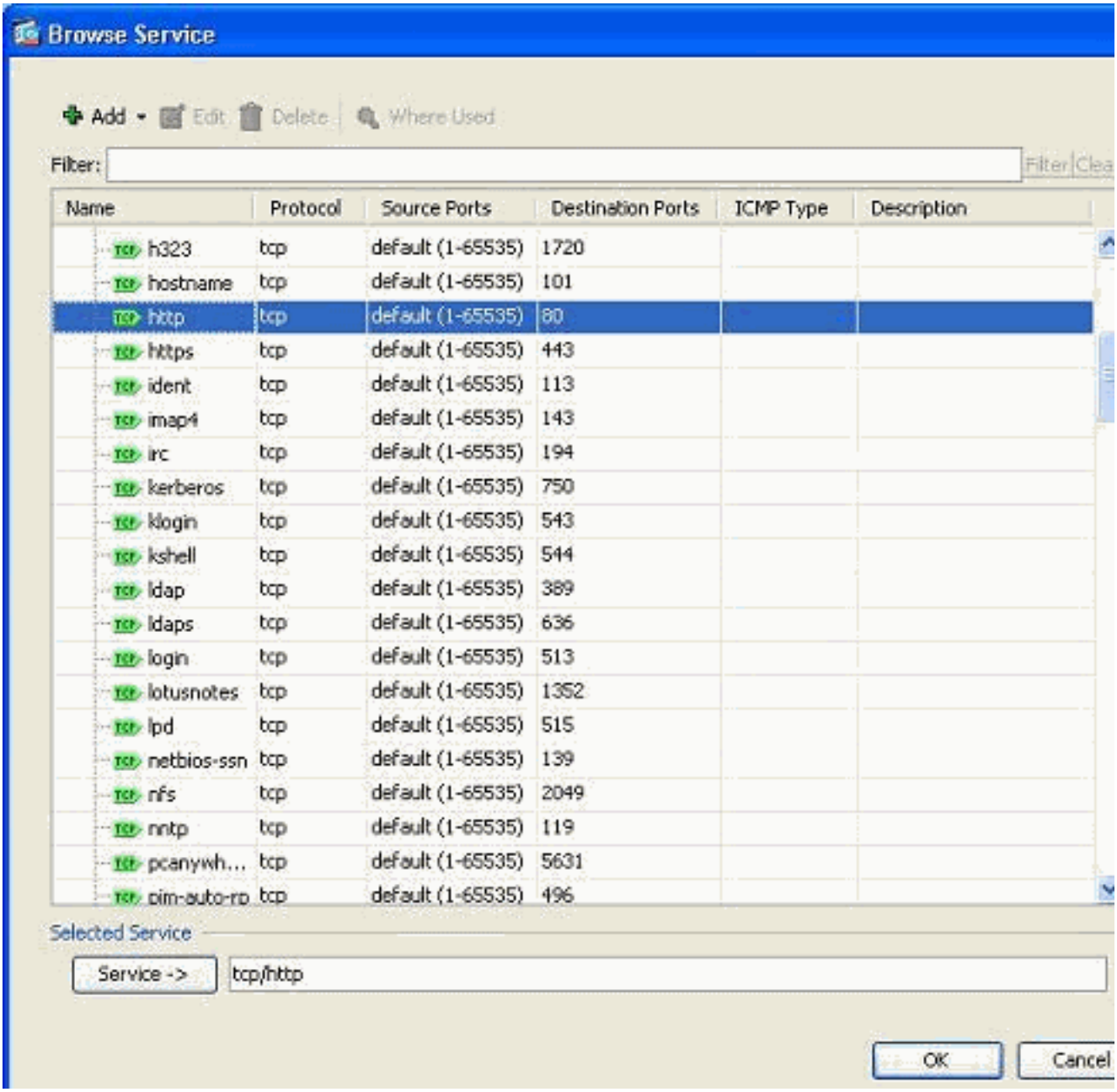
1. Selezionare la voce dell'elenco degli accessi esistente e fare clic su **Inserisci** dal menu a discesa **Aggiungi**

2. Scegliere l'origine e la destinazione, quindi fare clic sul pulsante **Dettagli** del campo Servizio

per scegliere il protocollo.



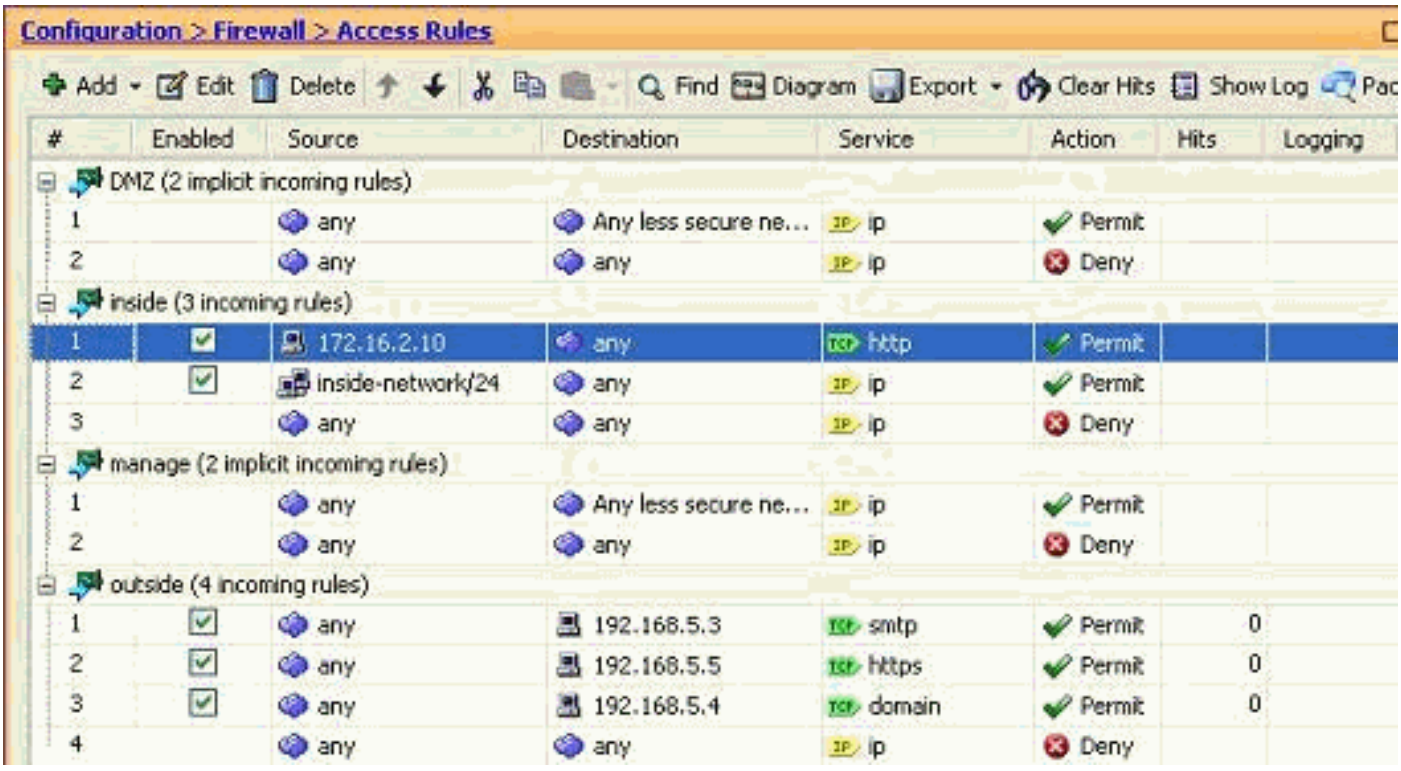
3. Scegliere HTTP come protocollo e fare clic su **OK**.



4. Viene visualizzata di nuovo la finestra Inserisci regola di accesso. Nel campo Servizio viene inserito **tcp/http** come protocollo selezionato. Per completare la configurazione della nuova voce dell'elenco degli accessi, fare clic su

OK.

Èora possibile osservare la nuova regola di accesso visualizzata prima della voce già esistente per la rete interna.

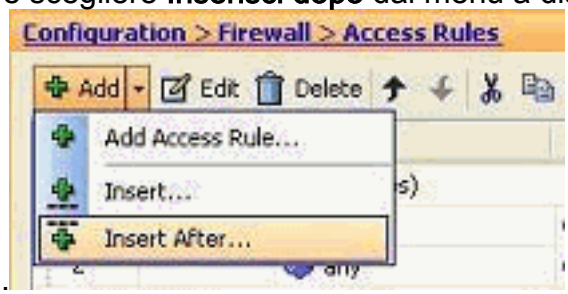


Nota: l'ordine delle regole di accesso è molto importante. Durante l'elaborazione di ciascun pacchetto da filtrare, l'ASA verifica se il pacchetto soddisfa uno dei criteri della regola di accesso in ordine sequenziale e, in caso di corrispondenza, implementa l'azione di tale regola di accesso. Quando una regola di accesso corrisponde, non passa ad altre regole di accesso e le verifica di nuovo.

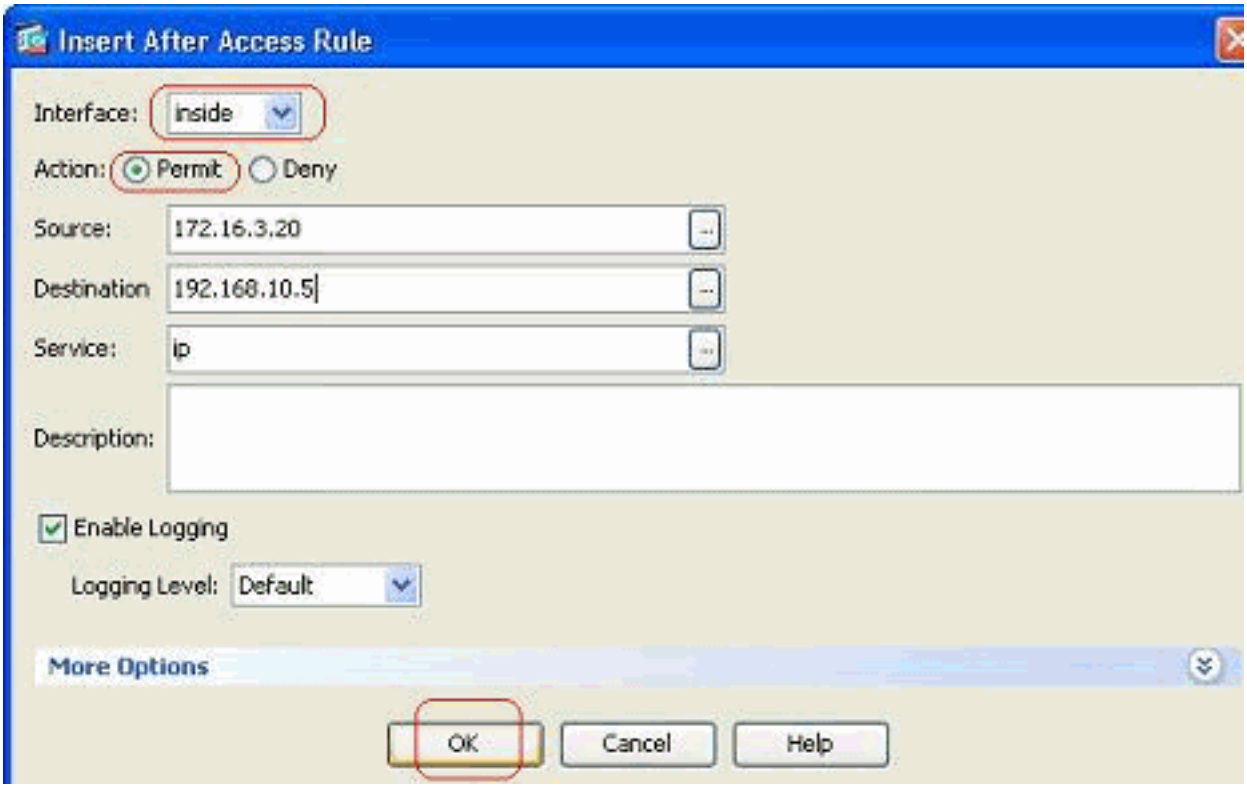
Aggiungere una regola di accesso dopo una regola esistente:

Completare questi passaggi per creare una regola di accesso subito dopo una regola di accesso già esistente.

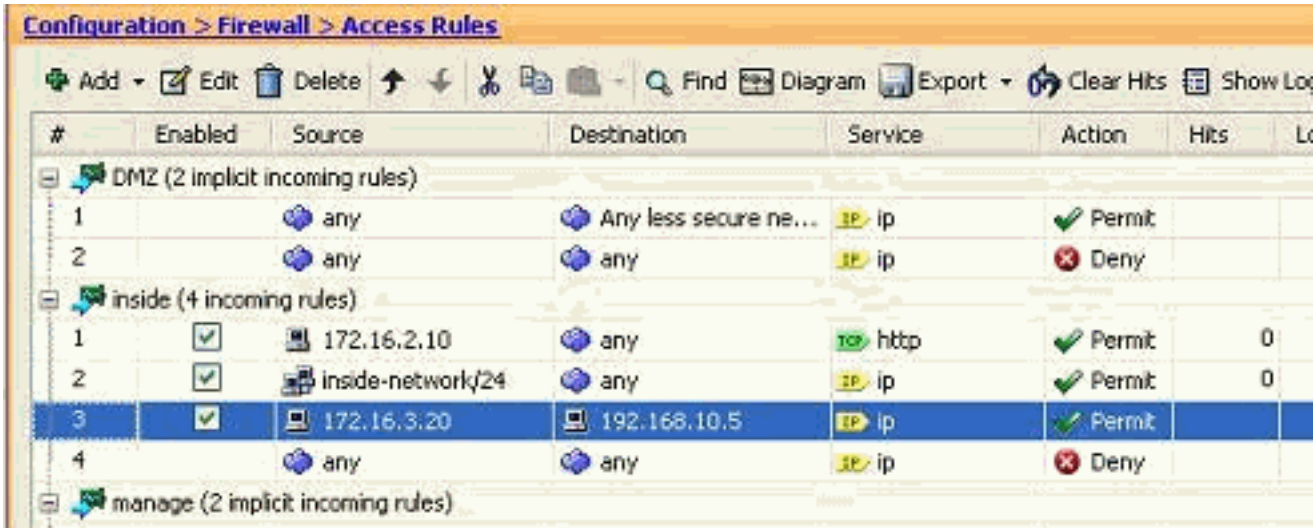
1. Selezionare la regola di accesso dopo la quale è necessario disporre di una nuova regola di accesso e scegliere **Inserisci dopo** dal menu a discesa Aggiungi.



2. Specificare i campi Interfaccia, Azione, Origine, Destinazione e Servizio e fare clic su **OK** per completare la configurazione della regola di accesso.

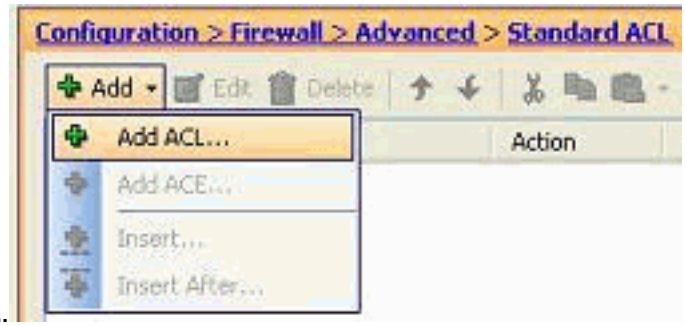


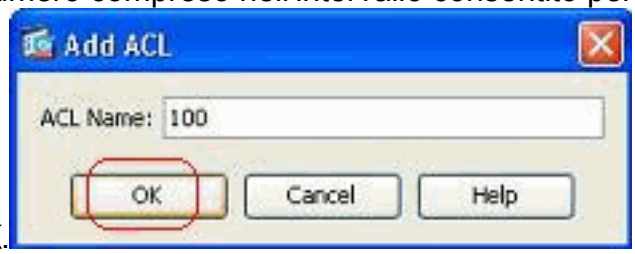
Èpossibile visualizzare che la regola di accesso appena configurata viene applicata subito dopo quella già configurata.

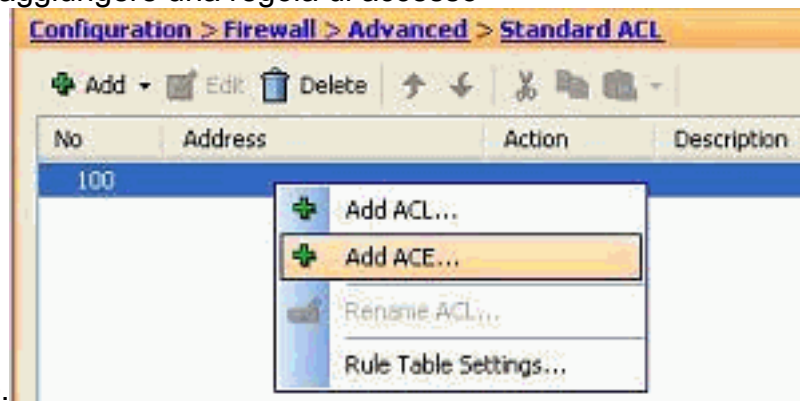


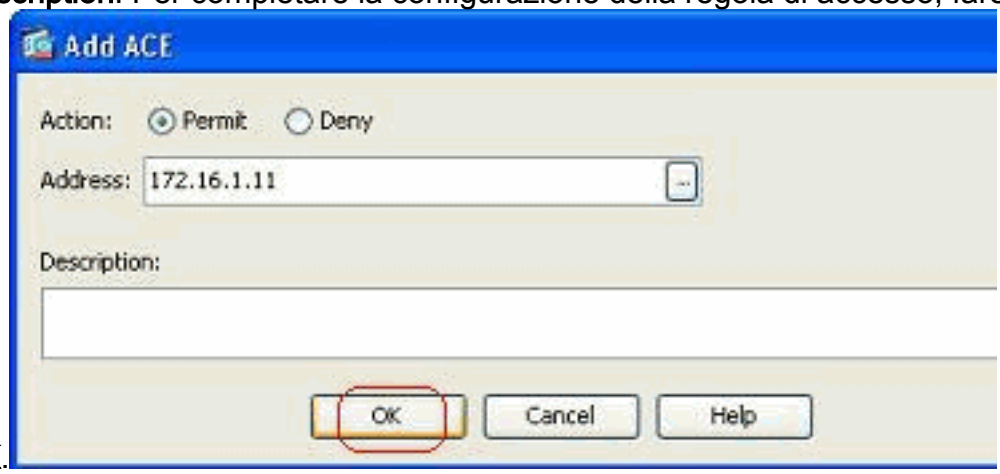
Creazione di un elenco degli accessi standard

Completare questa procedura per creare un elenco degli accessi standard con l'interfaccia utente di ASDM.

1. Scegliere **Configurazione > Firewall > Avanzate > ACL standard > Aggiungi**, quindi fare clic su **Aggiungi ACL**.


2. Assegnare un numero compreso nell'intervallo consentito per l'elenco degli accessi standard e fare clic su **OK**.


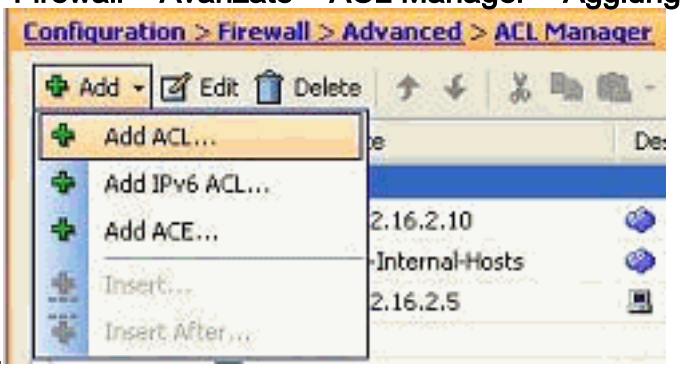
3. Fare clic con il pulsante destro del mouse sull'elenco degli accessi e scegliere **Aggiungi voce ACE** per aggiungere una regola di accesso all'elenco.


4. Selezionare l'**azione** e specificare l'**indirizzo di origine**. Se necessario, specificare anche **Description**. Per completare la configurazione della regola di accesso, fare clic su **OK**.


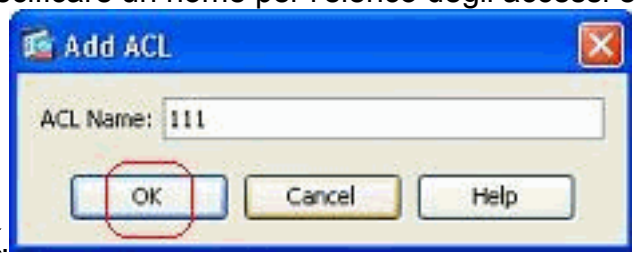
Creare una regola di accesso globale

Completare questa procedura per creare un elenco degli accessi estesi contenente le regole di accesso globali.

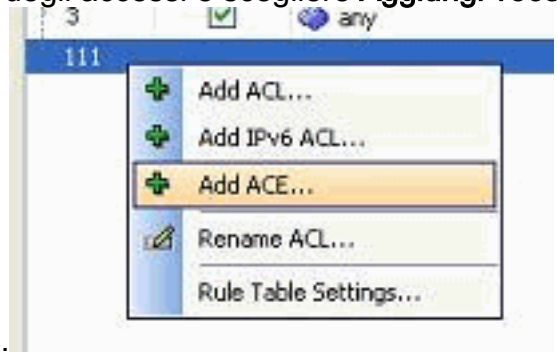
1. Scegliere **Configurazione > Firewall > Avanzate > ACL Manager > Aggiungi**, quindi fare clic sul pulsante **Aggiungi ACL**.



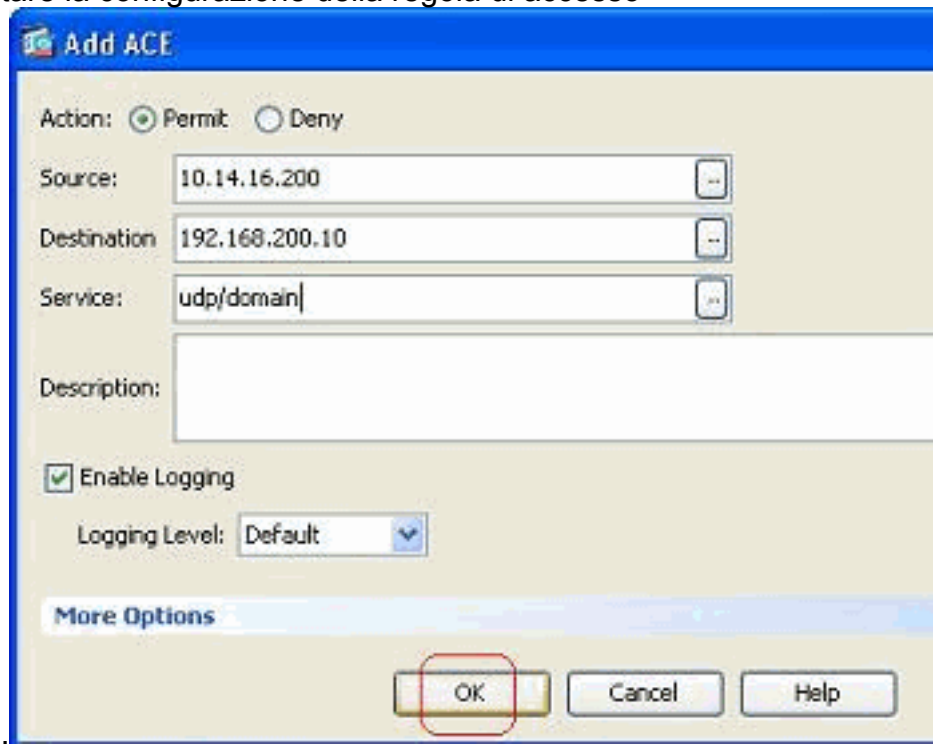
2. Specificare un nome per l'elenco degli accessi e fare clic su **OK**.



3. Fare clic con il pulsante destro del mouse sull'elenco degli accessi e scegliere **Aggiungi voce ACE** per aggiungere una regola di accesso all'elenco.



4. Completare i campi Azione, Origine, Destinazione e Servizio e fare clic su **OK** per completare la configurazione della regola di accesso globale.



Èora possibile visualizzare la regola di accesso globale, come illustrato.

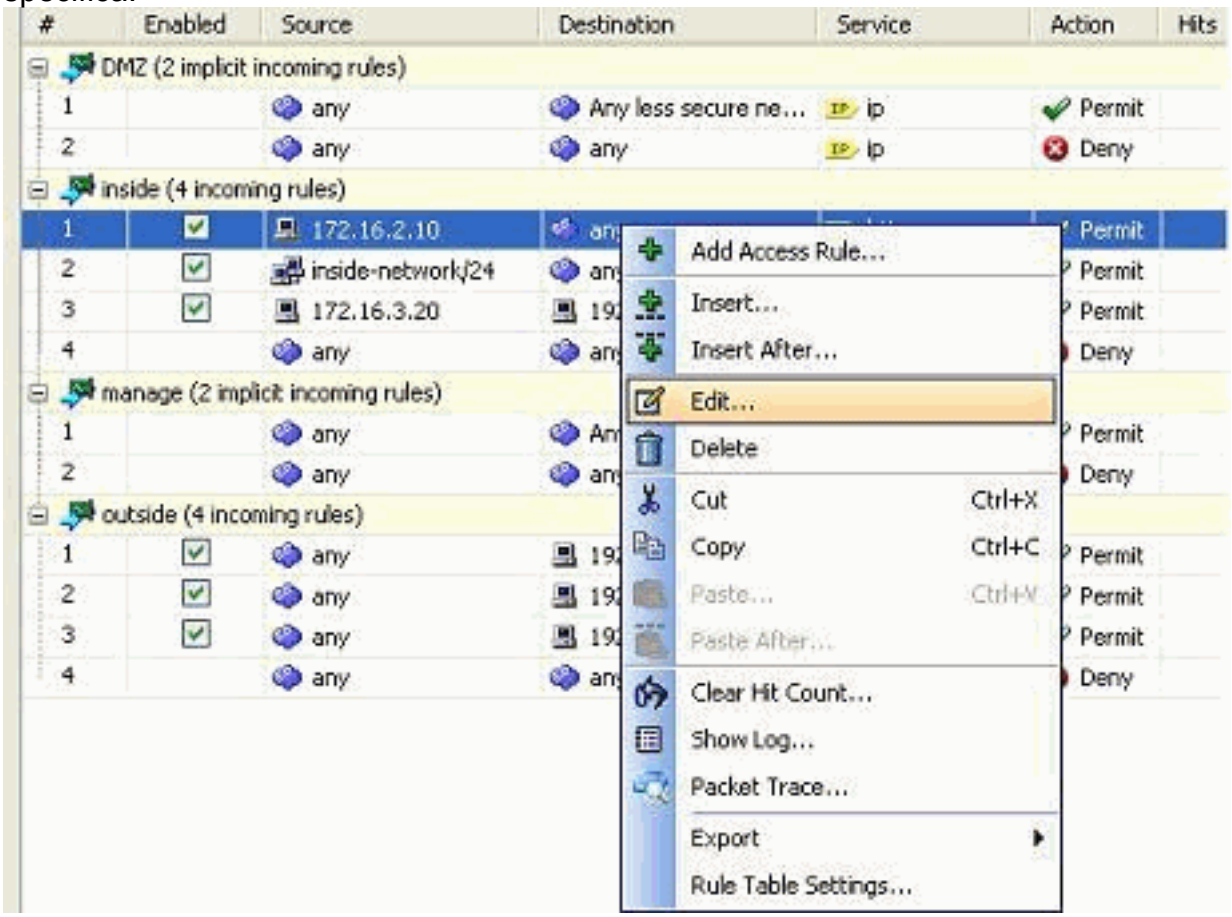
Modifica elenco accessi esistente

In questa sezione viene descritto come modificare un accesso esistente.

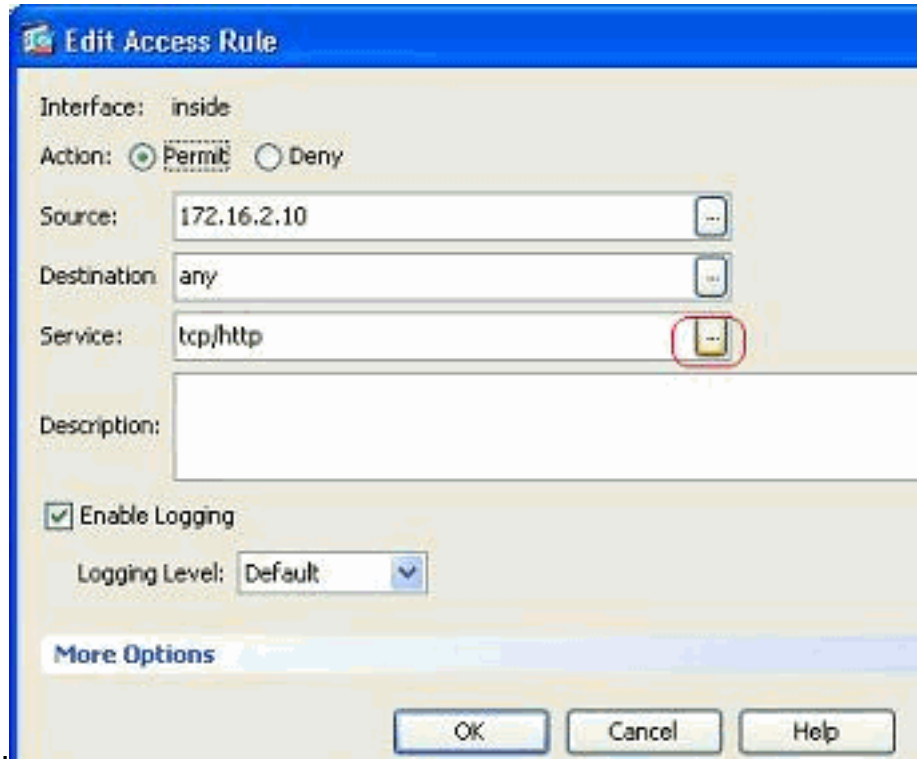
Modificare il campo Protocollo per creare un gruppo di servizi:

Completare questa procedura per creare un nuovo gruppo di servizi.

1. Fare clic con il pulsante destro del mouse sulla regola di accesso da modificare e scegliere **Modifica** per modificare la regola di accesso specifica.

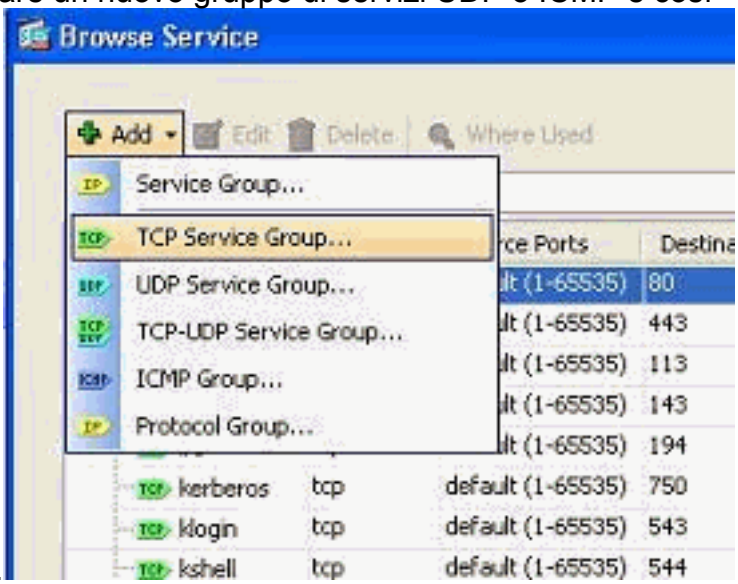


2. Fare clic sul pulsante **Dettagli** per modificare il protocollo associato a questa regola di



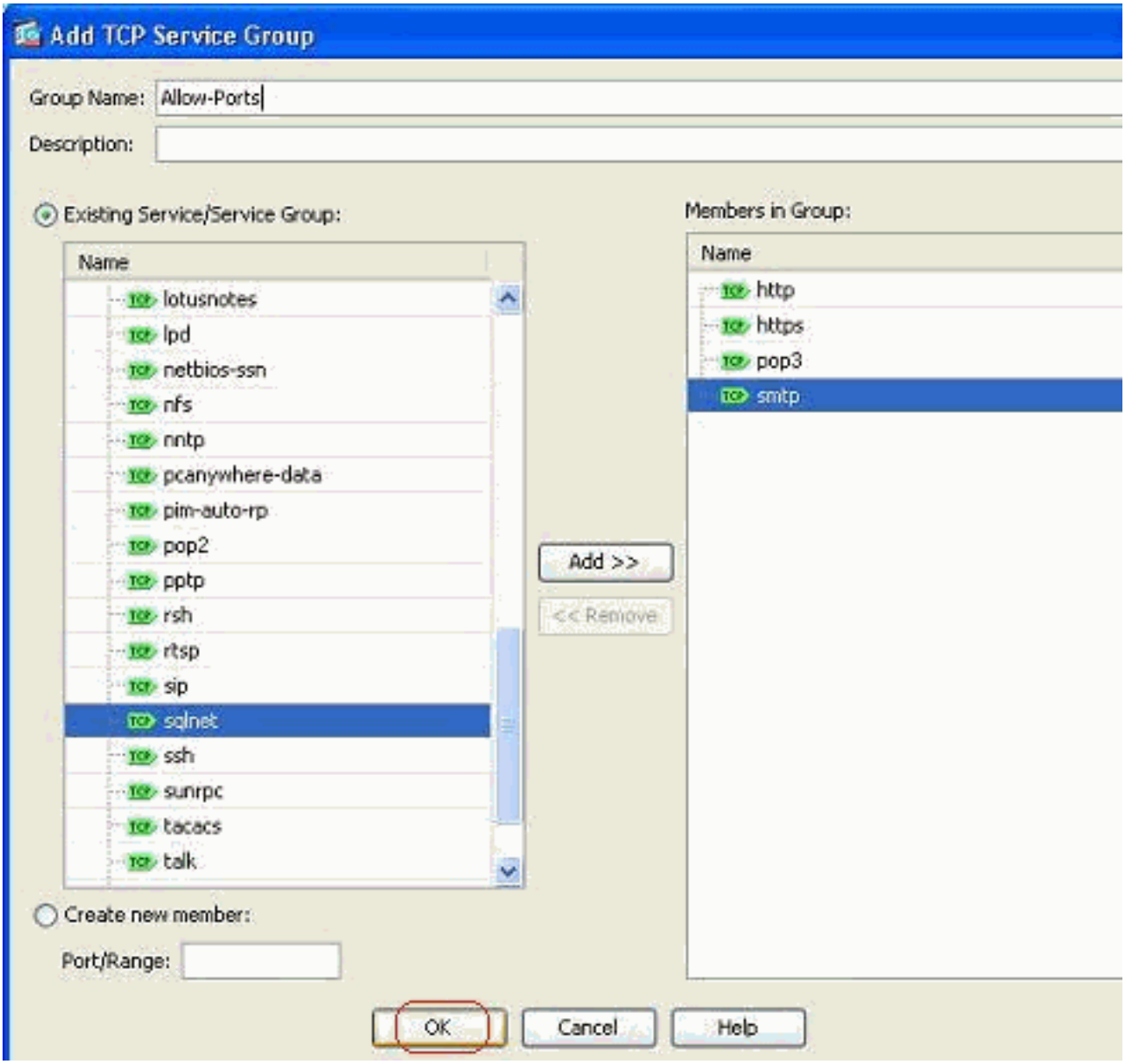
accesso.

3. Se necessario, è possibile selezionare qualsiasi protocollo diverso da HTTP. Se è necessario selezionare un solo protocollo, non è necessario creare il gruppo di servizi. È utile creare un gruppo di servizi quando è necessario identificare numerosi protocolli non adiacenti a cui deve corrispondere questa regola di accesso.Per creare un nuovo gruppo di servizi TCP, scegliere **Aggiungi > Gruppo** di servizi TCP.**Nota:** allo stesso modo, è possibile creare un nuovo gruppo di servizi UDP o ICMP e così

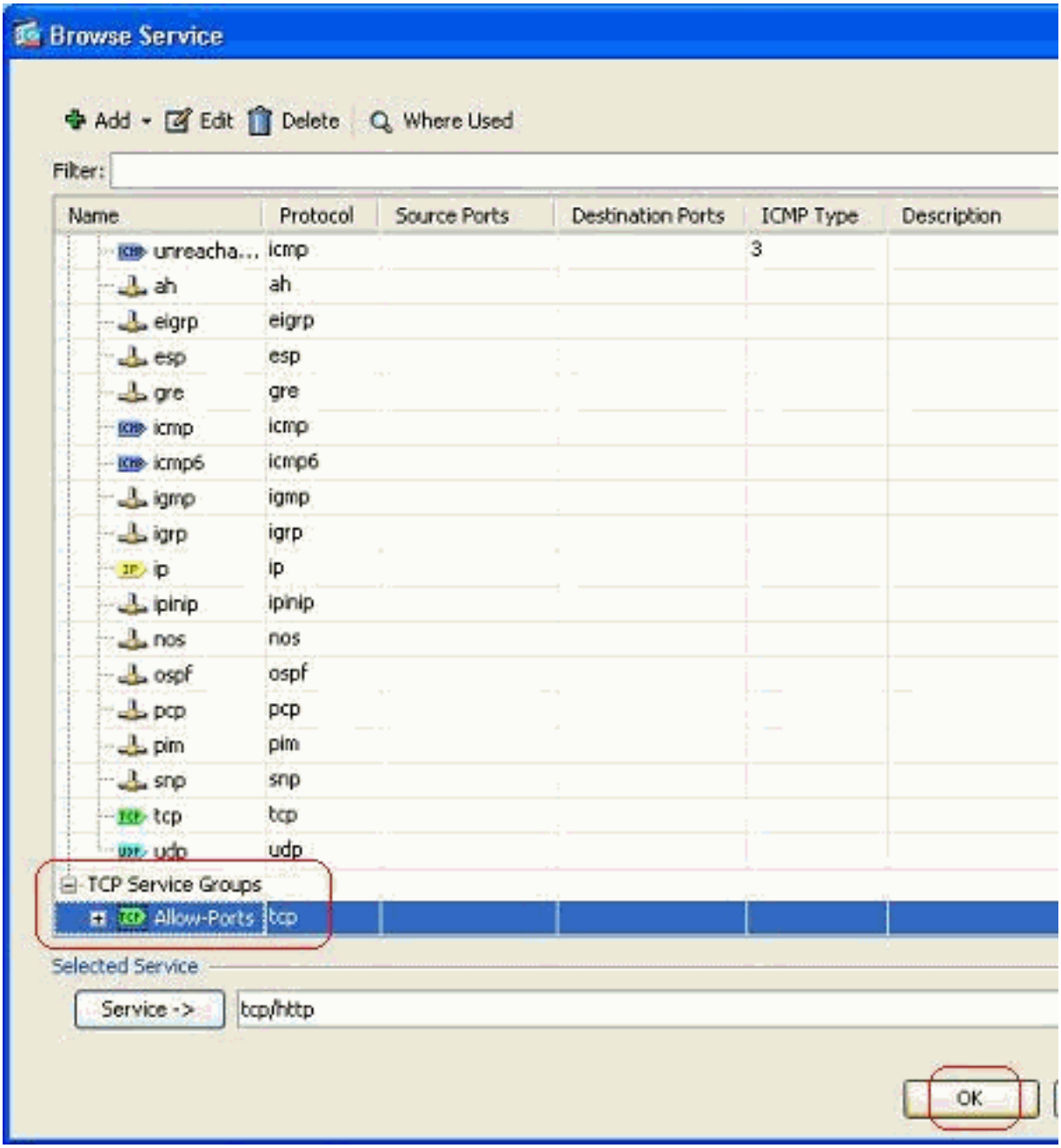


via.

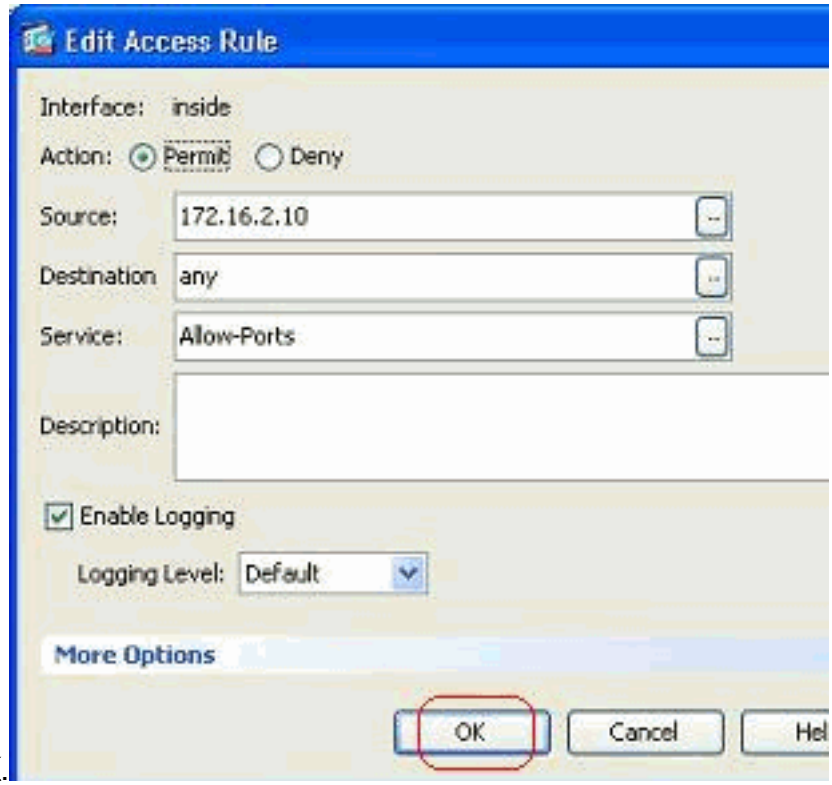
4. Specificare un nome per il gruppo di servizi, selezionare il protocollo nel menu a sinistra e fare clic su **Aggiungi** per spostarli nel menu Membri nel gruppo a destra. È possibile aggiungere numerosi protocolli come membri di un gruppo di servizi in base ai requisiti. I protocolli vengono aggiunti uno alla volta. Dopo aver aggiunto tutti i membri, fare clic su **OK**.



5. Il gruppo di servizi appena creato può essere visualizzato nella scheda **Gruppi di servizi TCP**. Fare clic su **OK** per tornare alla finestra Modifica regola di accesso.

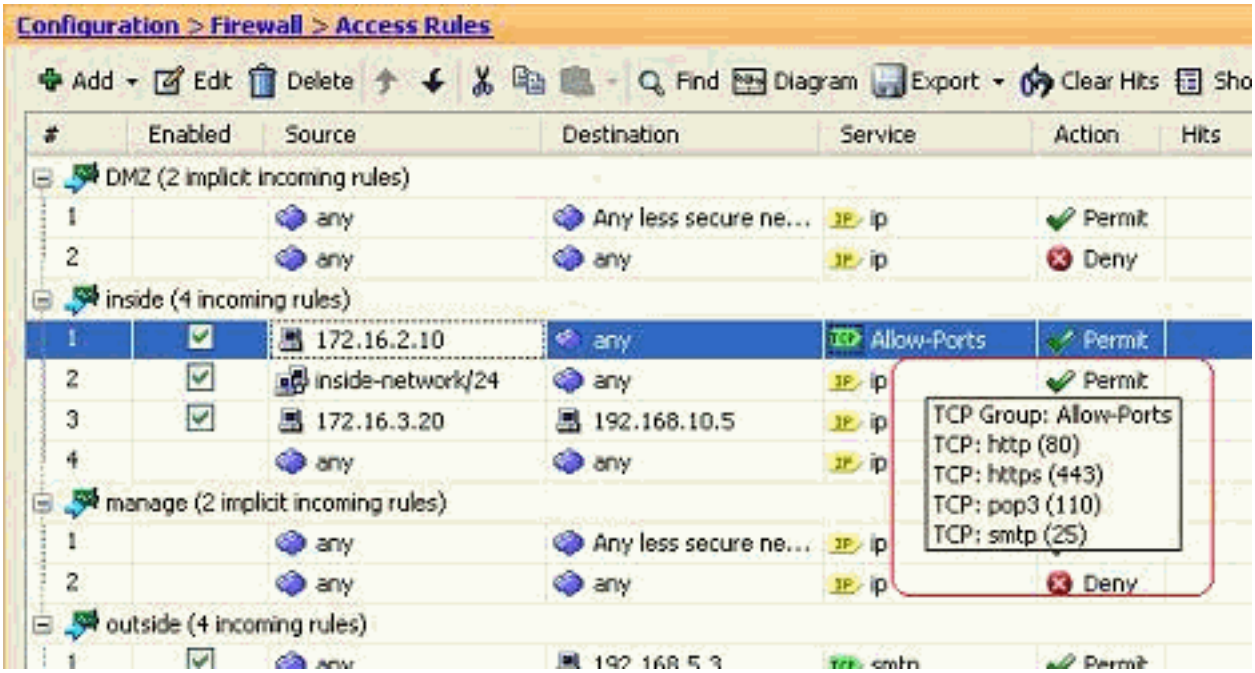


6. Nel campo Servizio è indicato il gruppo di servizi appena creato. Per completare la modifica,



fare clic su **OK**.

7. Passare il mouse su quello specifico gruppo di servizi per visualizzare tutti i protocolli associati.

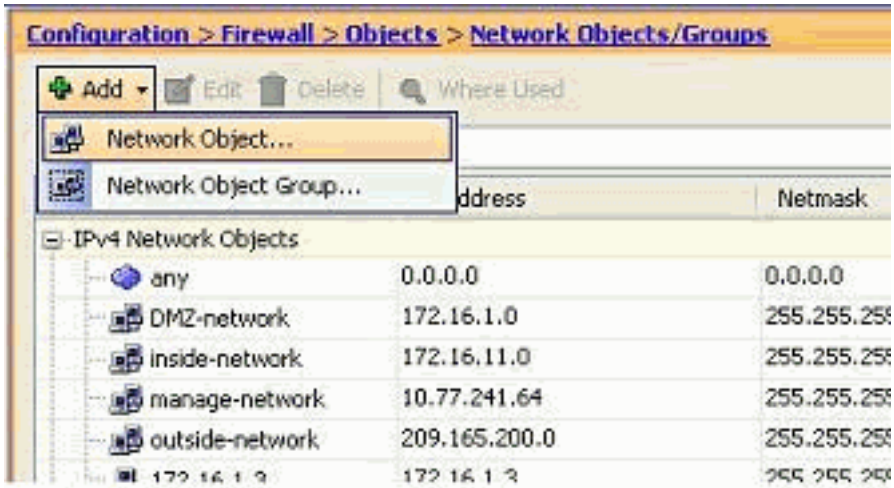


Modificare i campi Origine/Destinazione per creare un gruppo di oggetti di rete:

I gruppi di oggetti vengono utilizzati per semplificare la creazione e la gestione degli elenchi di accesso. Quando si raggruppano oggetti simili, è possibile utilizzare il gruppo di oggetti in una singola voce ACE anziché immettere una voce ACE per ogni oggetto separatamente. Prima di creare il gruppo di oggetti, è necessario creare gli oggetti. Nella terminologia ASDM, l'oggetto è denominato oggetto di rete e il gruppo di oggetti è denominato gruppo di oggetti di rete.

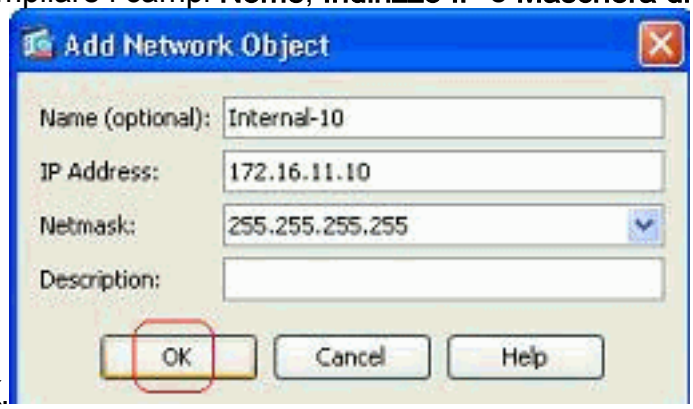
Attenersi alla seguente procedura:

1. Scegliere **Configurazione > Firewall > Oggetti > Oggetti/gruppi di rete > Aggiungi**, quindi fare clic su **Oggetto di rete** per creare un nuovo oggetto di



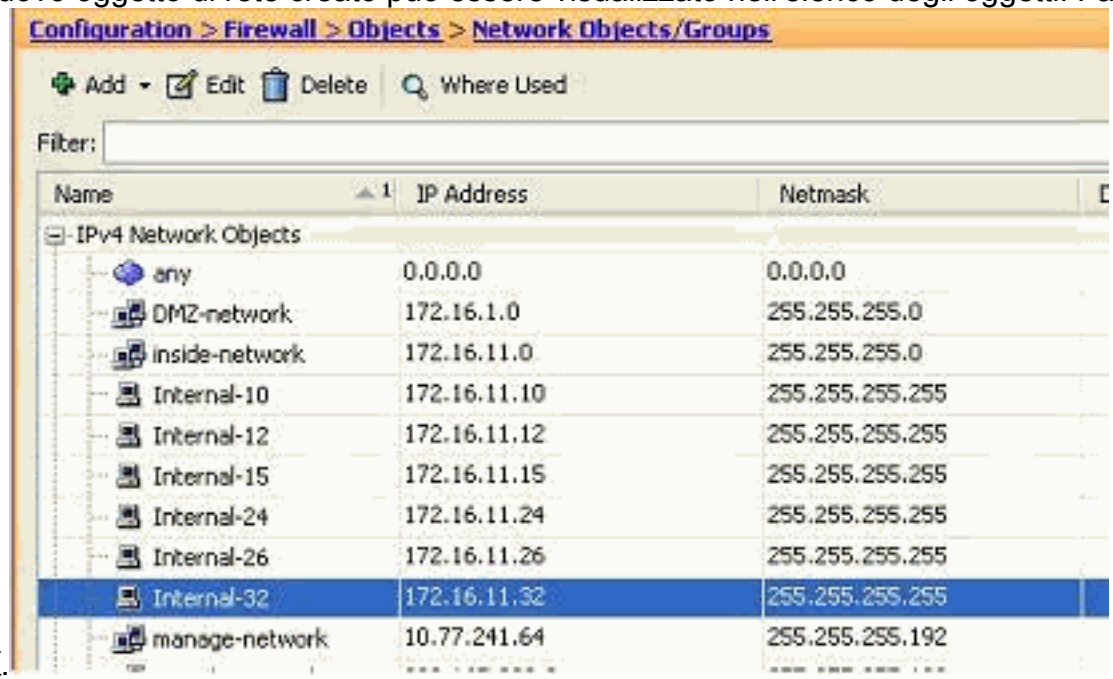
rete.

2. Compilare i campi **Nome**, **Indirizzo IP** e **Maschera di rete** e fare clic su



OK.

3. Il nuovo oggetto di rete creato può essere visualizzato nell'elenco degli oggetti. Fare clic su

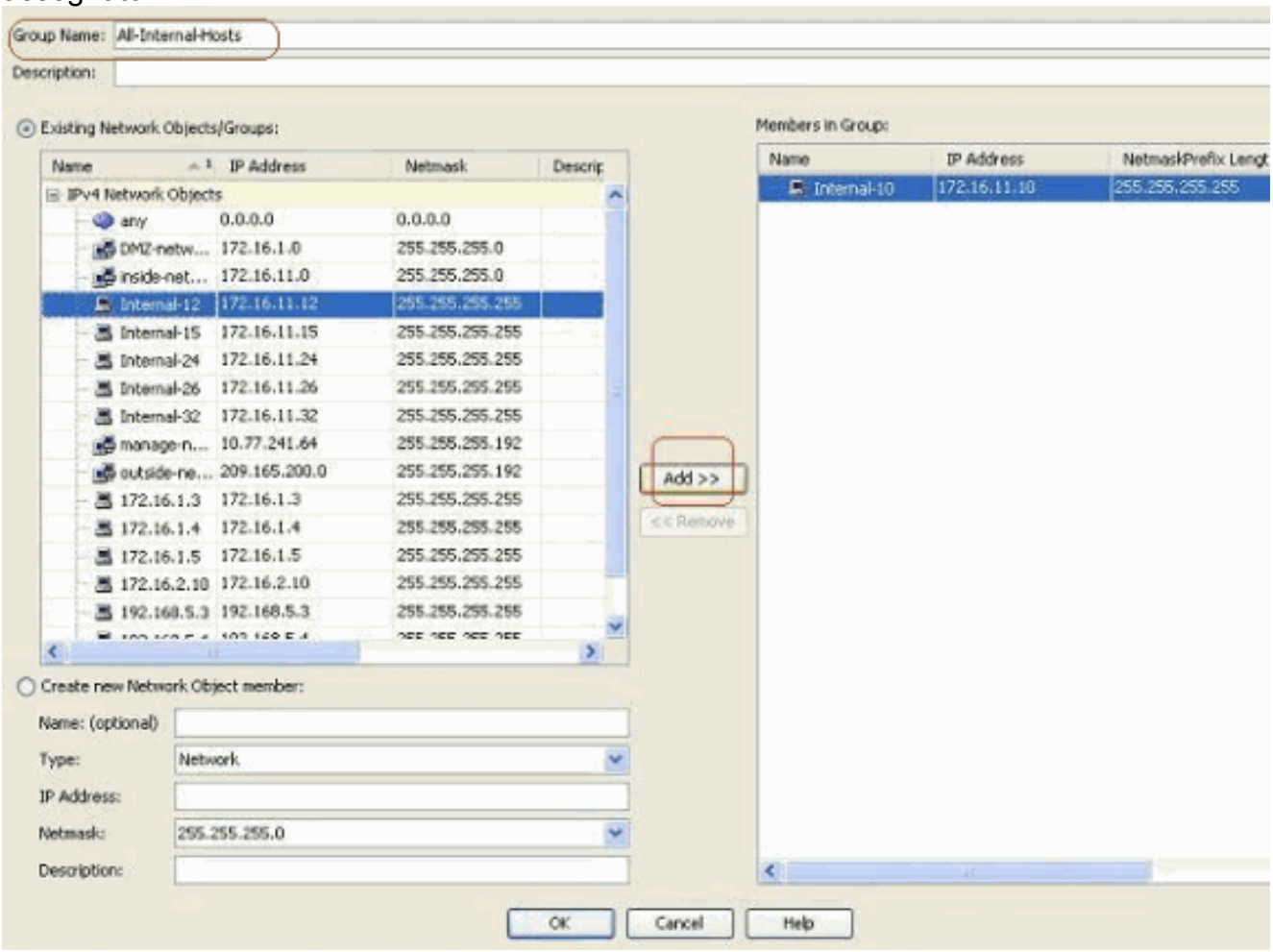


OK.

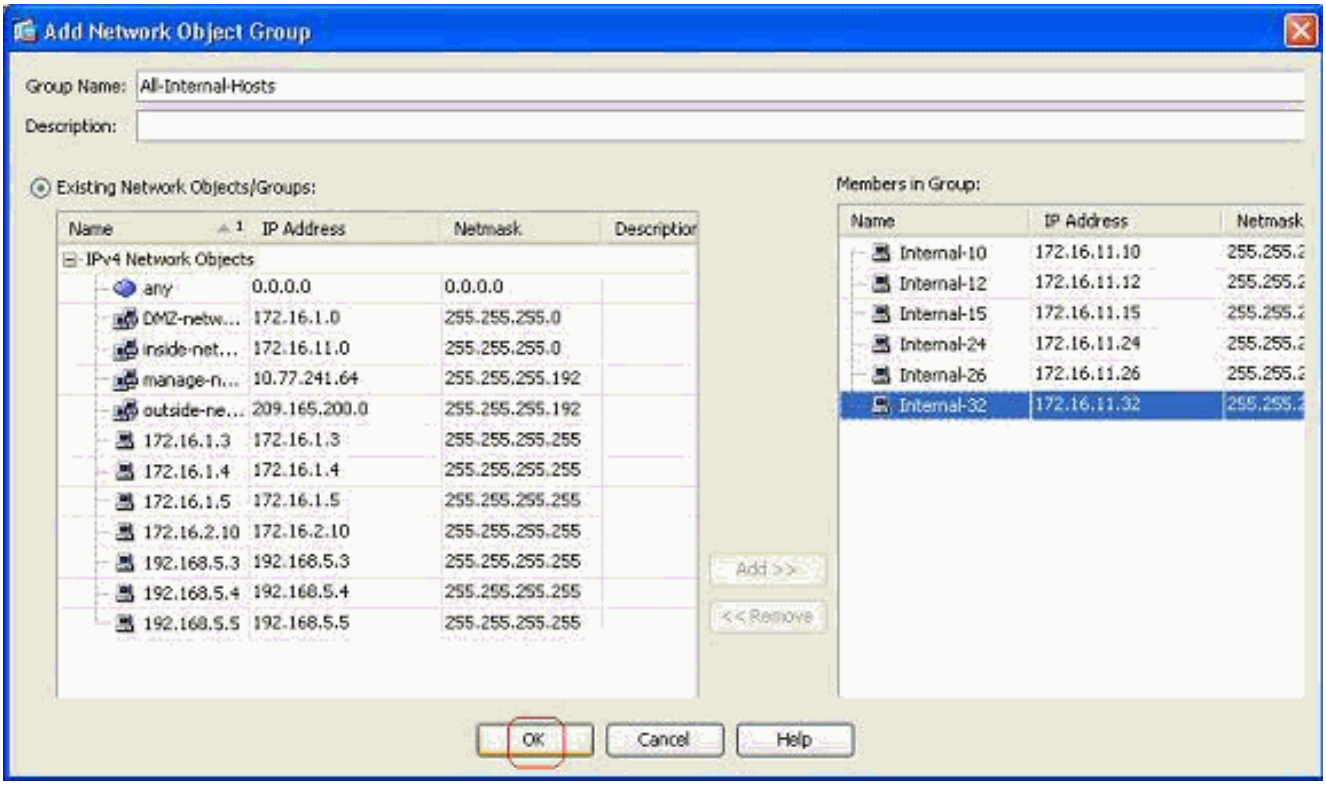
4. Scegliere **Configurazione > Firewall > Oggetti > Oggetti/gruppi di rete > Aggiungi**, quindi fare clic su **Gruppo di oggetti di rete** per creare un nuovo gruppo di oggetti di

rete.

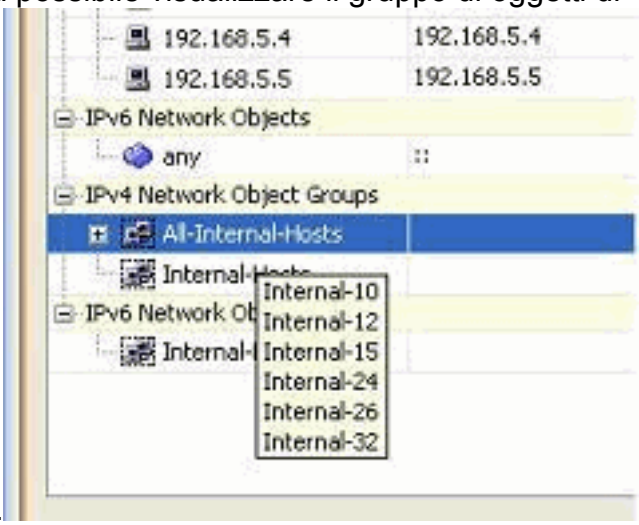
5. L'elenco disponibile di tutti gli oggetti di rete è disponibile nel riquadro sinistro della finestra. Selezionare singoli oggetti di rete e fare clic sul pulsante **Aggiungi** per renderli membri del gruppo di oggetti di rete appena creato. È necessario specificare il nome del gruppo nel campo ad esso
assegnato.



6. Fare clic su **OK** dopo aver aggiunto tutti i membri al
gruppo.

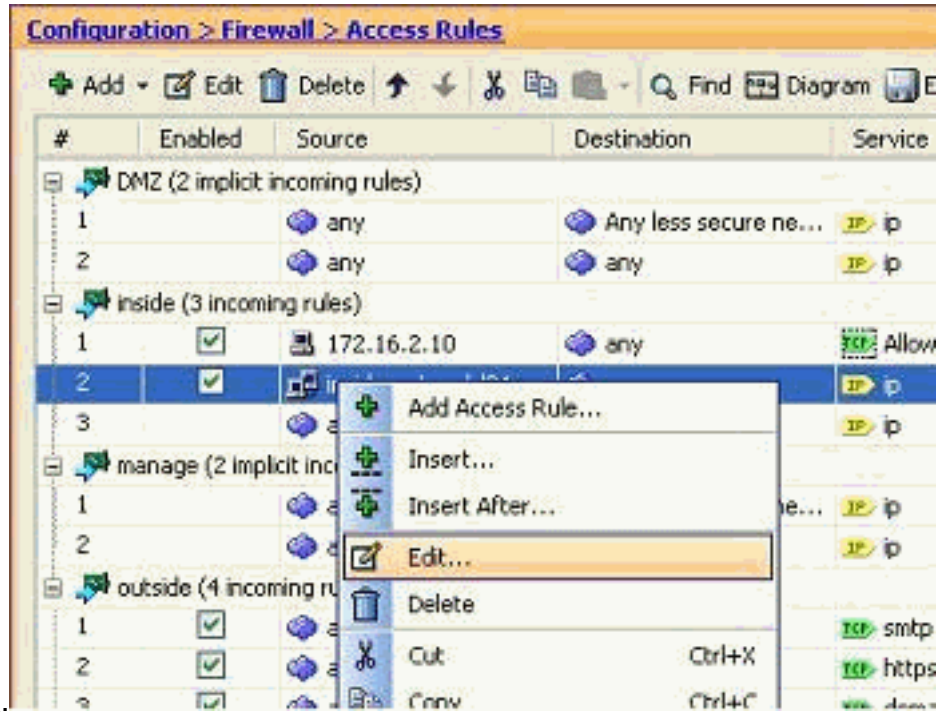


Èora possibile visualizzare il gruppo di oggetti di



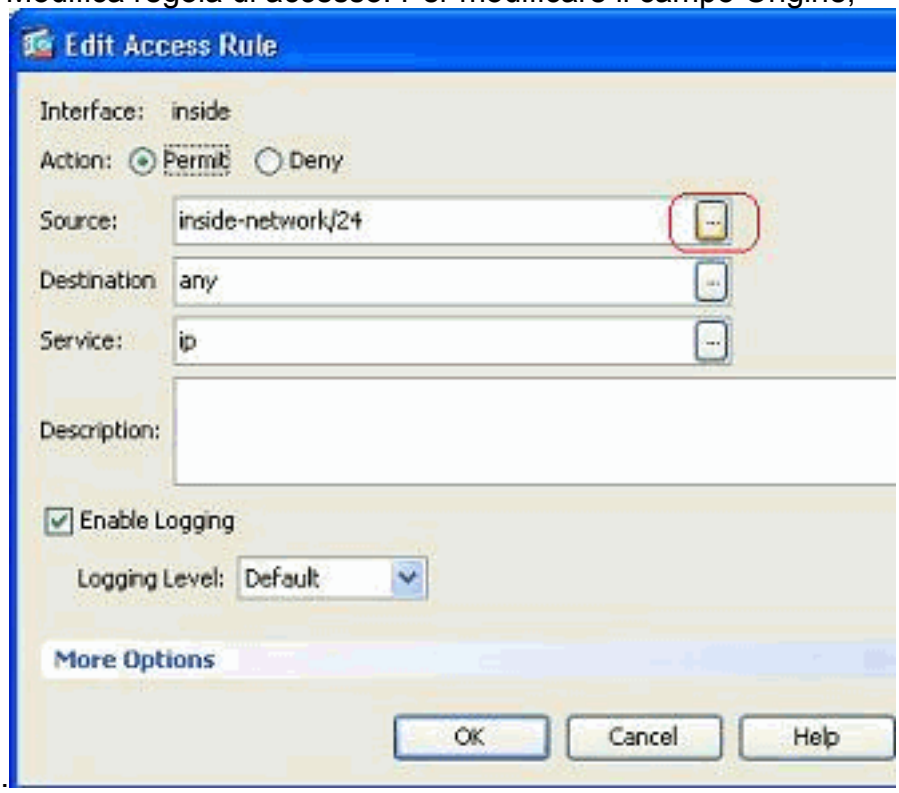
rete.

7. Per modificare qualsiasi campo di origine/destinazione di un elenco degli accessi esistente con un oggetto gruppo di rete, fare clic con il pulsante destro del mouse sulla regola di accesso specifica e scegliere



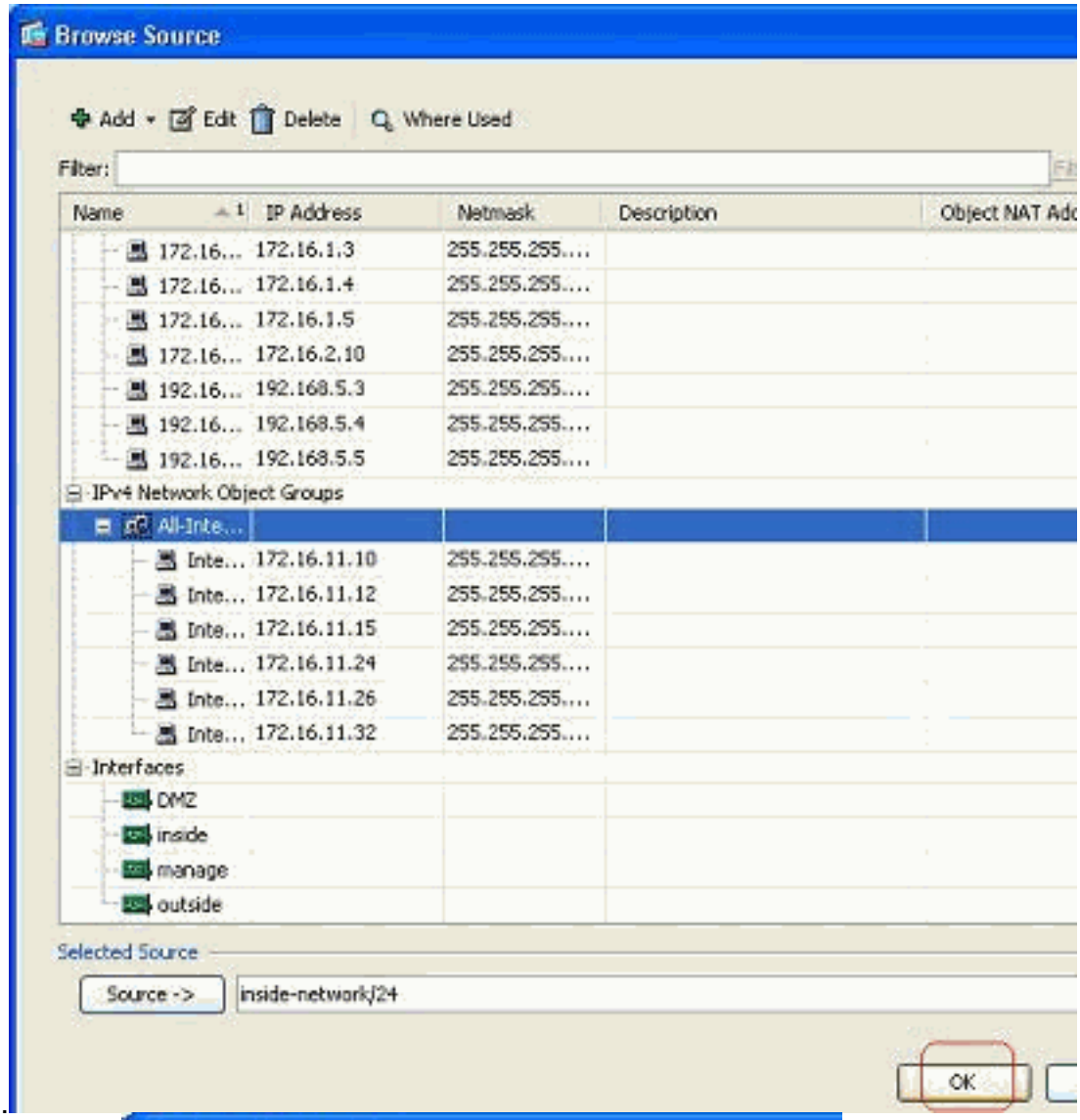
Modifica.

8. Viene visualizzata la finestra Modifica regola di accesso. Per modificare il campo Origine, fare clic sul pulsante **Dettagli**.

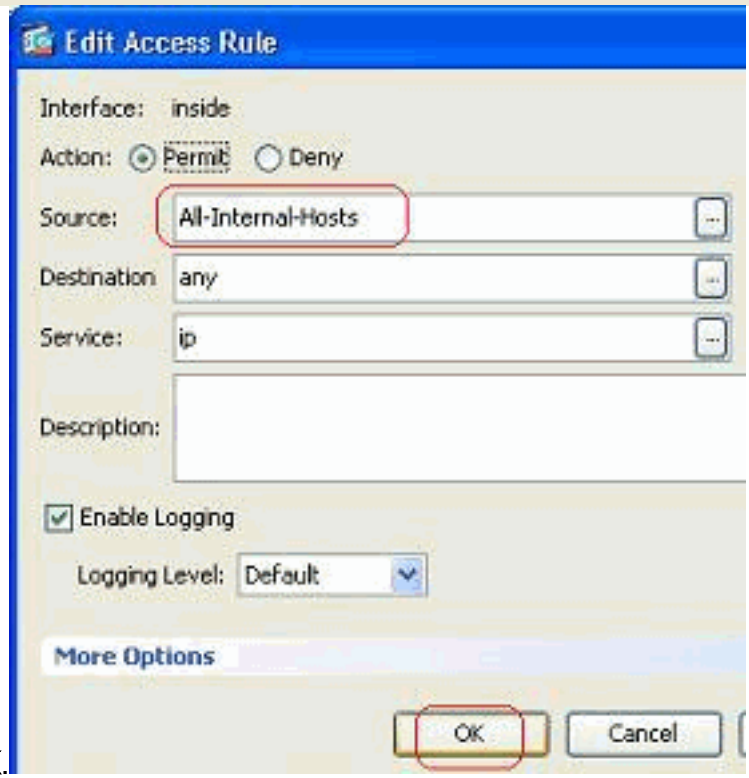


9. Selezionare il gruppo di oggetti di rete **Tutti gli host interni** e fare clic su **OK**

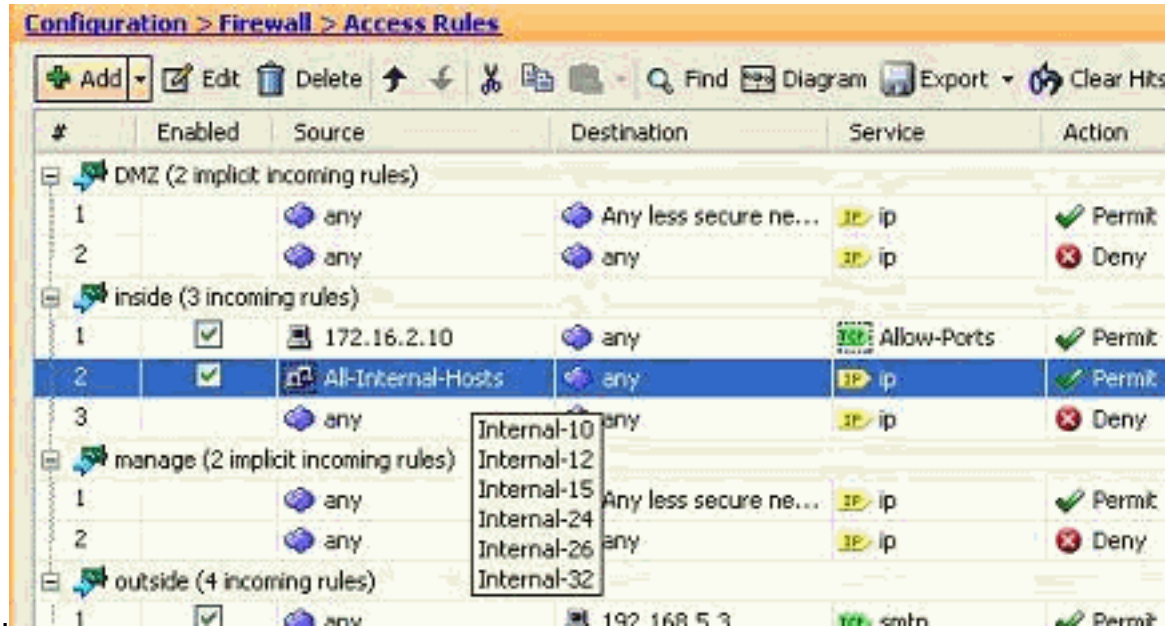
pulsante.



10. Fare clic su **OK**.



11. Passare il mouse sul campo Origine della regola di accesso per visualizzare i membri del

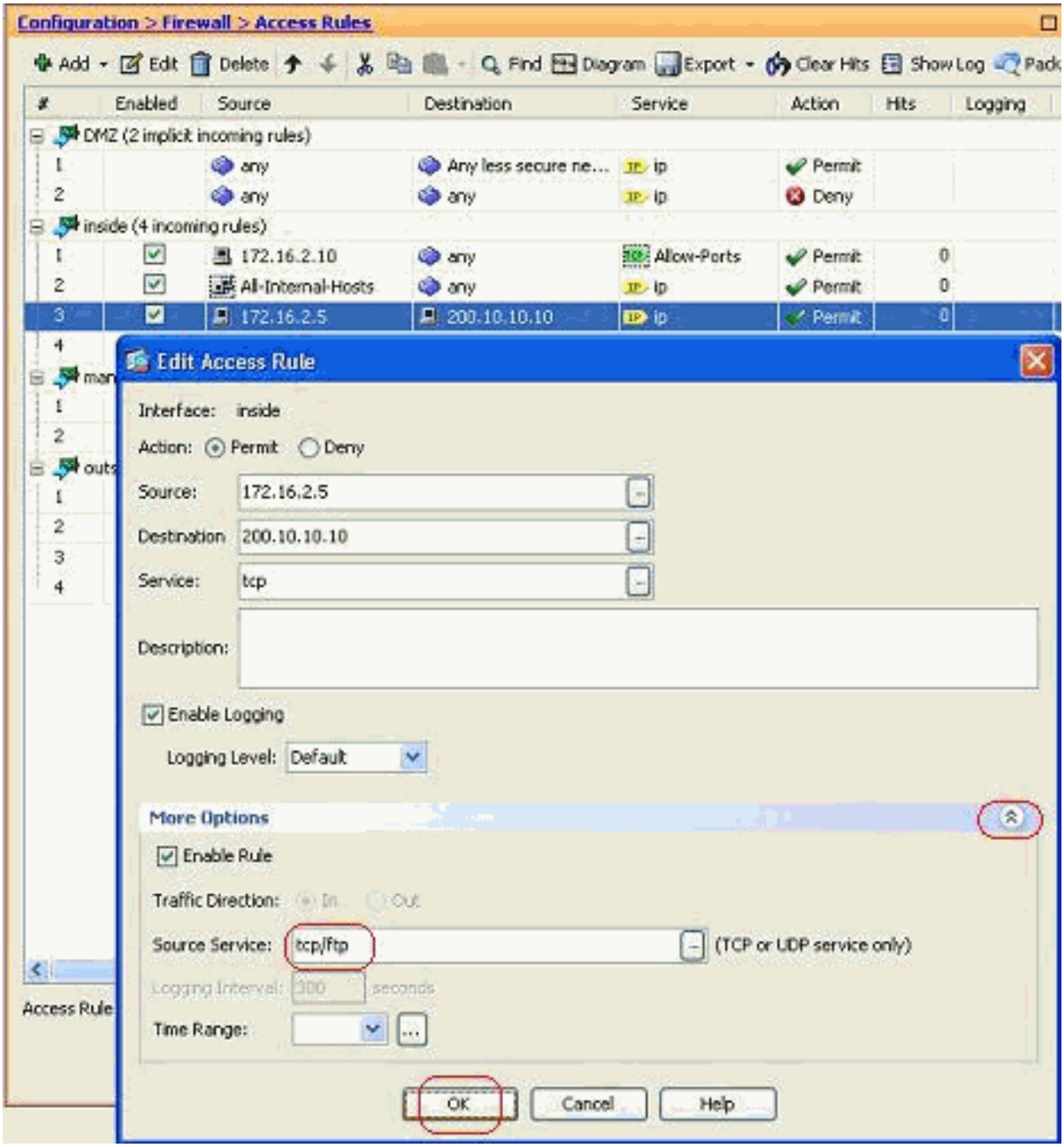


gruppo.

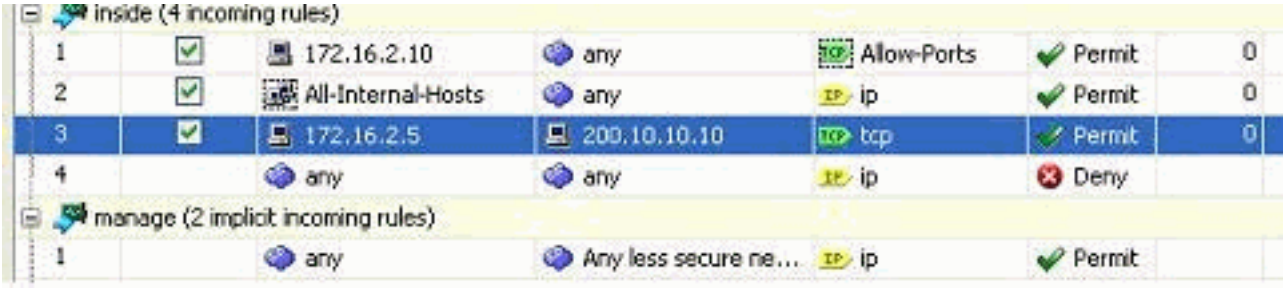
Modificare la porta di origine:

Completare questi passaggi per modificare la porta di origine di una regola di accesso.

1. Per modificare la porta di origine di una regola di accesso esistente, fare clic con il pulsante destro del mouse su di essa e scegliere **Modifica**.Viene visualizzata la finestra Modifica regola di
accesso.



2. Fare clic sul pulsante a discesa **Altre opzioni** per modificare il campo Servizio di origine, quindi fare clic su **OK**.Èpossibile visualizzare la regola di accesso modificata, come illustrato.

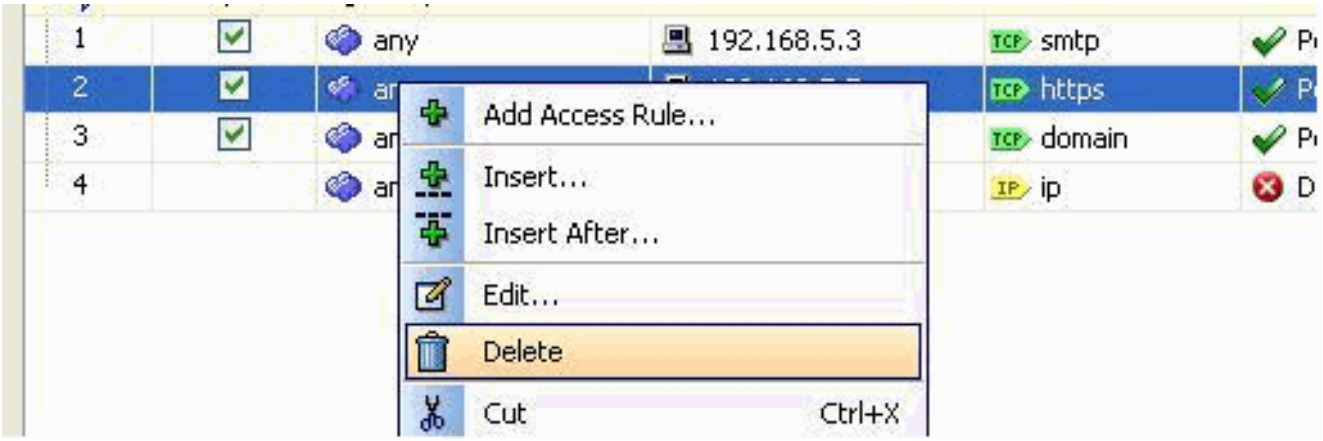


Eliminare un elenco degli accessi

Per eliminare un elenco degli accessi, completare la procedura seguente:

1. Prima di eliminare un elenco degli accessi esistente, è necessario eliminare le voci dell'elenco degli accessi (le regole di accesso). Non è possibile eliminare l'elenco degli

accessi a meno che non si eliminino prima tutte le regole di accesso.Fare clic con il pulsante destro del mouse sulla regola di accesso da eliminare e scegliere **Elimina**.



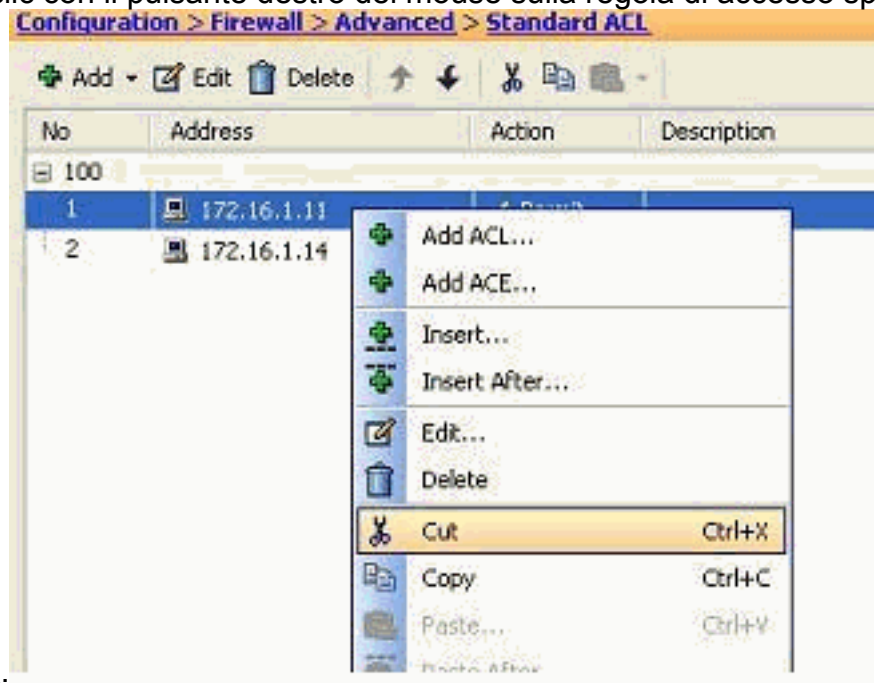
2. Completare la stessa operazione di eliminazione per tutte le regole di accesso esistenti, quindi selezionare l'elenco degli accessi e scegliere **Elimina** per eliminarlo.

Esporta la regola di accesso

Le regole di accesso ASDM associano l'elenco degli accessi all'interfaccia corrispondente, mentre ACL Manager tiene traccia di tutti gli elenchi degli accessi estesi. Le regole di accesso create con ACL Manager non si associano ad alcuna interfaccia. Questi elenchi degli accessi sono in genere utilizzati per le funzioni NAT-Exempt, VPN-Filter e altre funzioni simili a cui non è possibile associare l'interfaccia. ACL Manager contiene tutte le voci presenti nella sezione **Configurazione > Firewall > Regole di accesso**. **ACL Manager**, inoltre, contiene anche le regole di accesso globale non associate ad alcuna interfaccia. ASDM è organizzato in modo che sia possibile esportare facilmente una regola di accesso da qualsiasi elenco di accesso a un altro.

Ad esempio, se è necessario associare a un'interfaccia una regola di accesso che fa già parte di una regola di accesso globale, non è necessario configurarla nuovamente. Per ottenere questo risultato, potete invece eseguire un'operazione **Taglia e incolla** (**Cut & Paste**).

1. Fare clic con il pulsante destro del mouse sulla regola di accesso specificata e scegliere **Taglia**.



2. Selezionare l'elenco accessi richiesto in cui inserire la regola di accesso. È possibile

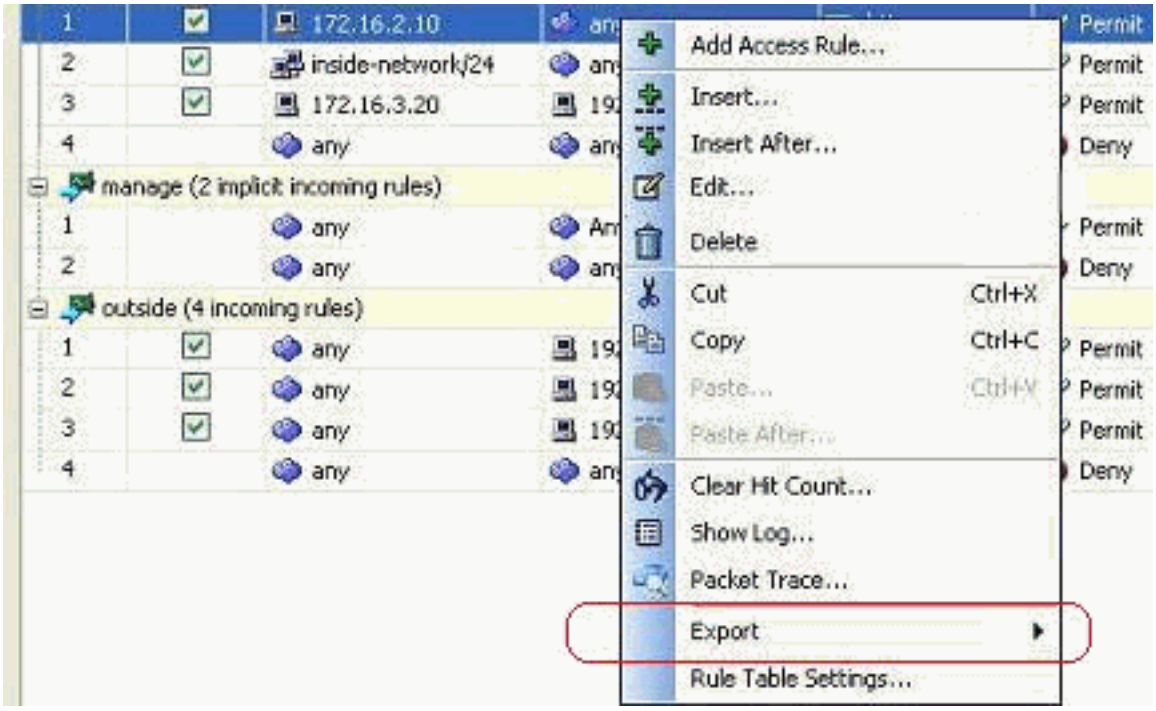
utilizzare l'opzione **Incolla** nella barra degli strumenti per inserire la regola di accesso.

Esportare le informazioni dell'elenco accessi

Èpossibile esportare le informazioni dell'elenco degli accessi in un altro file. Per esportare queste informazioni sono supportati due formati.

1. Formato CSV (Comma Separated Value)
2. Formato HTML

Fare clic con il pulsante destro del mouse su una delle regole di accesso e scegliere **Esporta** per inviare le informazioni dell'elenco degli accessi a un file.



Di seguito sono riportate le informazioni dell'elenco degli accessi in formato HTML.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Esempi di configurazione di ASDM e note tecniche
- Esempi di configurazione delle appliance ASA e note tecniche
- Documentazione e supporto tecnico – Cisco Systems