ASA 7.x/PIX 6.x e versioni successive: Esempio di configurazione delle porte Open/Block

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per aprire o bloccare le porte per i diversi tipi di traffico, ad esempio http o ftp, nell'appliance di sicurezza.

Nota: i termini "apertura della porta" e "autorizzazione della porta" hanno lo stesso significato. Analogamente, le parole "bloccare la porta" e "limitare la porta" hanno lo stesso significato.

Prerequisiti

Requisiti

Per le successive spiegazioni, si presume che il protocollo PIX/ASA sia configurato e funzioni correttamente.

Componenti usati

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

- Cisco serie 5500 Adaptive Security Appliance (ASA) con versione 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM) versione 6.3(5)

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco serie 500 PIX Firewall Appliance versione software 6.x e successive.

Convenzioni

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

Configurazione

Ogni interfaccia deve avere un livello di protezione da 0 (minimo) a 100 (massimo). È ad esempio necessario assegnare la rete più sicura, ad esempio la rete host interna, al livello 100. Mentre la rete esterna connessa a Internet può essere al livello 0, altre reti, ad esempio le DMZ, possono essere posizionate nel mezzo. È possibile assegnare più interfacce allo stesso livello di protezione.

Per impostazione predefinita, tutte le porte sono bloccate sull'interfaccia esterna (livello di sicurezza 0) e tutte le porte sono aperte sull'interfaccia interna (livello di sicurezza 100) dell'accessorio di sicurezza. In questo modo, tutto il traffico in uscita può passare attraverso l'appliance di sicurezza senza alcuna configurazione, ma il traffico in entrata può essere autorizzato dalla configurazione dell'elenco degli accessi e dei comandi statici nell'appliance di sicurezza.

Nota: in generale, tutte le porte sono bloccate dall'area di sicurezza inferiore all'area di sicurezza superiore e tutte le porte sono aperte dall'area di sicurezza superiore all'area di sicurezza inferiore purché l'ispezione con conservazione dello stato sia abilitata per il traffico in entrata e in uscita.

Questa sezione comprende le sottosezioni riportate di seguito.

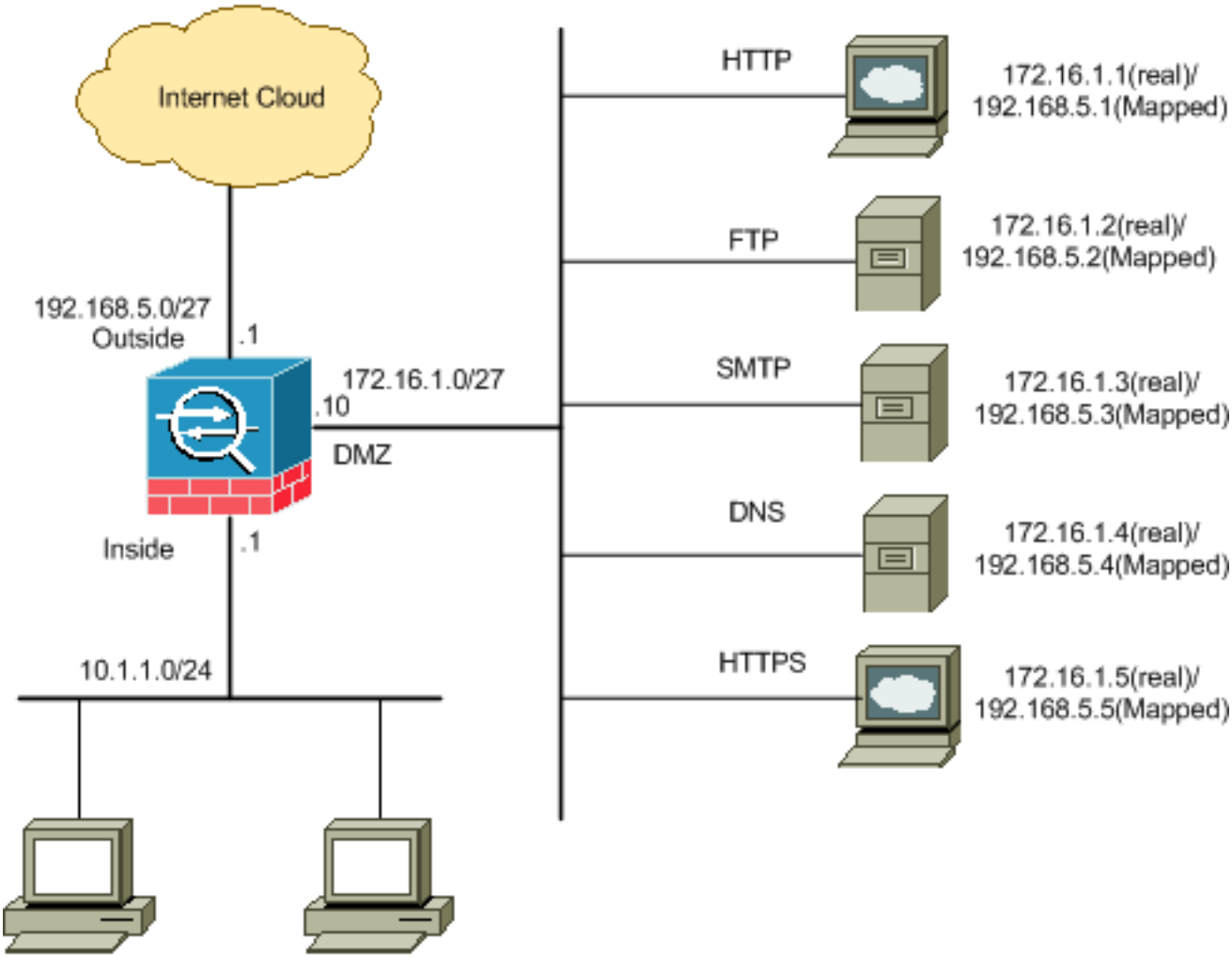
- Esempio di rete
- Blocco della configurazione delle porte
- Apertura della configurazione delle porte

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

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Blocco della configurazione delle porte

L'appliance di sicurezza consente tutto il traffico in uscita a meno che non venga esplicitamente bloccato da un elenco degli accessi esteso.

Un elenco degli accessi è costituito da una o più voci di controllo dell'accesso. A seconda del tipo di elenco degli accessi, è possibile specificare gli indirizzi di origine e di destinazione, il protocollo, le porte (per TCP o UDP), il tipo ICMP (per ICMP) o EtherType.

Nota: per i protocolli senza connessione, ad esempio ICMP, l'appliance di sicurezza stabilisce sessioni unidirezionali, quindi è necessario disporre di elenchi degli accessi per consentire l'accesso ICMP in entrambe le direzioni (applicando gli elenchi degli accessi alle interfacce di origine e di destinazione) oppure abilitare il motore di ispezione ICMP. Il motore di ispezione ICMP tratta le sessioni ICMP come connessioni bidirezionali.

Completare questa procedura per bloccare le porte, in genere applicate al traffico proveniente dall'interno (area di sicurezza superiore) verso la DMZ (area di sicurezza inferiore) o verso l'esterno della DMZ.

1. Creare un elenco di controllo di accesso in modo da bloccare il traffico sulla porta specificata.

```
access-list
```

2. Quindi, associare l'elenco degli accessi al comando **access-group** per essere attivo.

```
access-group
```

Esempi:

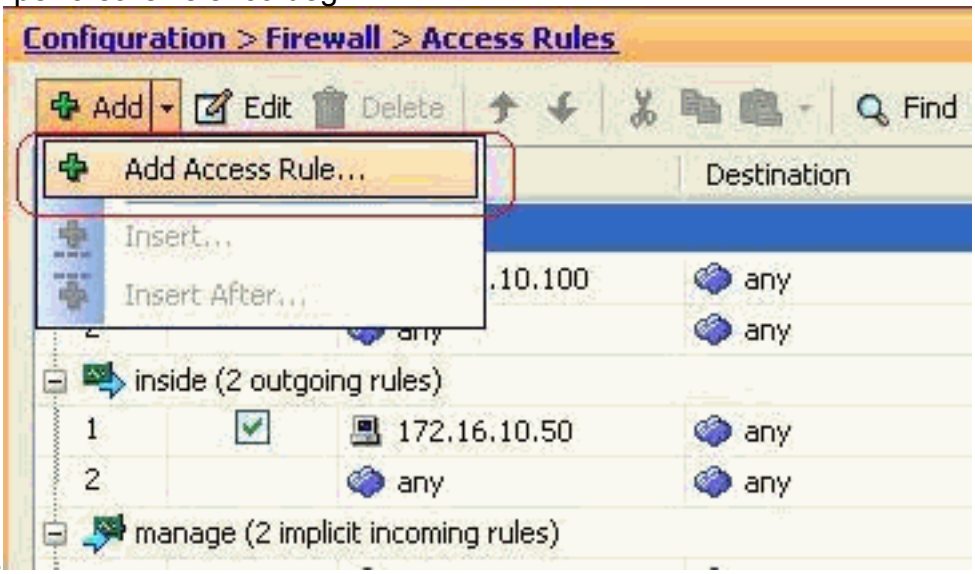
1. **Bloccare il traffico della porta HTTP:** Per bloccare l'accesso alla rete interna 10.1.1.0 al server Web http con IP 172.16.1.1 inserito nella rete DMZ, creare un ACL come mostrato:
```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

   Nota: per rimuovere il blocco della porta, usare **no** seguito dai comandi dell'elenco degli accessi.
2. **Blocca il traffico sulla porta FTP:** Per bloccare la rete interna 10.1.1.0 dall'accesso al file server FTP con IP 172.16.1.2 inserito nella rete DMZ, creare un ACL come mostrato:
```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

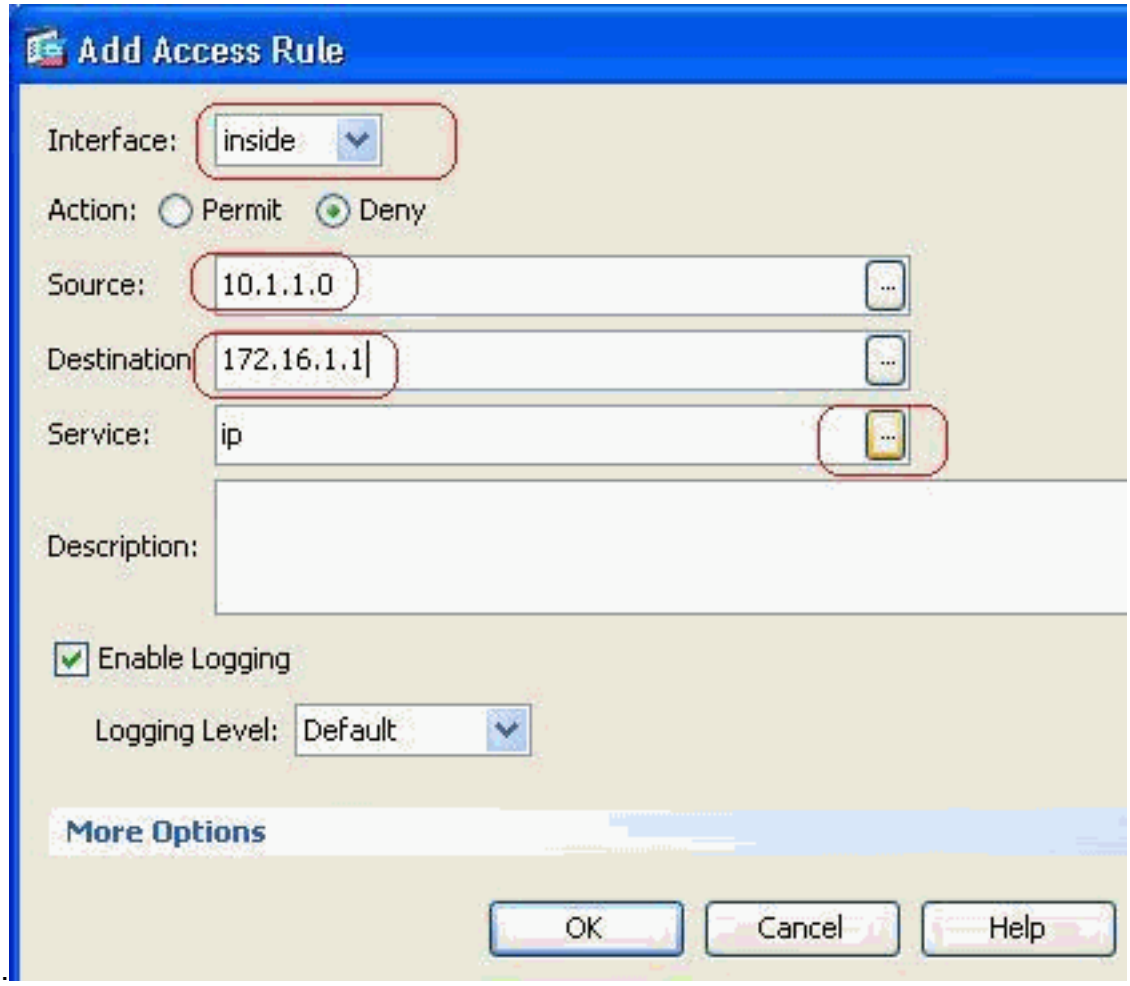
Nota: per ulteriori informazioni sull'assegnazione delle porte, consultare il documento sulle porte IANA.

In questa sezione viene illustrata la configurazione dettagliata per eseguire questa operazione tramite ASDM.

1. Selezionare **Configurazione > Firewall > Regole di accesso**. Fare clic su **Aggiungi regola di accesso** per creare l'elenco degli accessi.

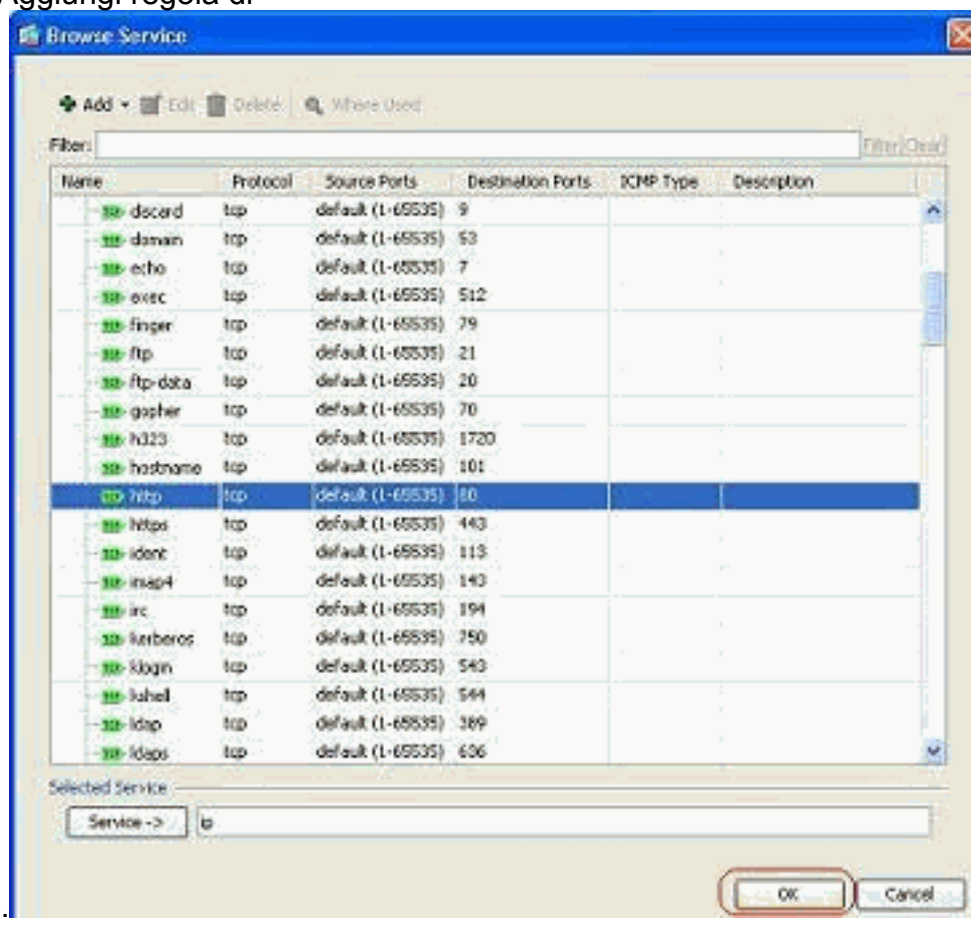


2. Definire l'origine e la destinazione, nonché l'azione della regola di accesso e l'interfaccia a cui verrà associata. Selezionare i dettagli per scegliere la porta specifica da



bloccare.

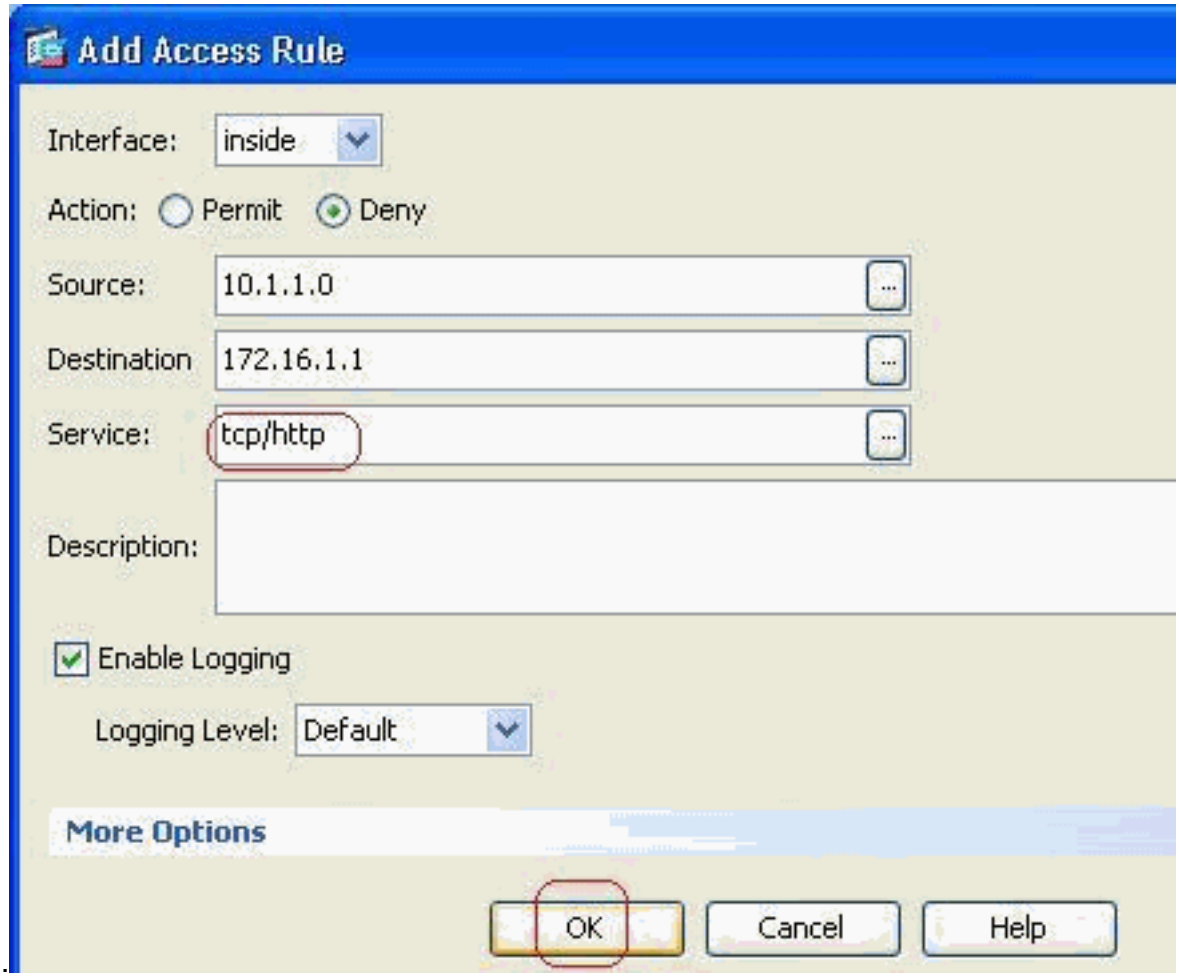
3. Scegliere **http** dall'elenco delle porte disponibili, quindi fare clic su **OK** per tornare alla finestra Aggiungi regola di



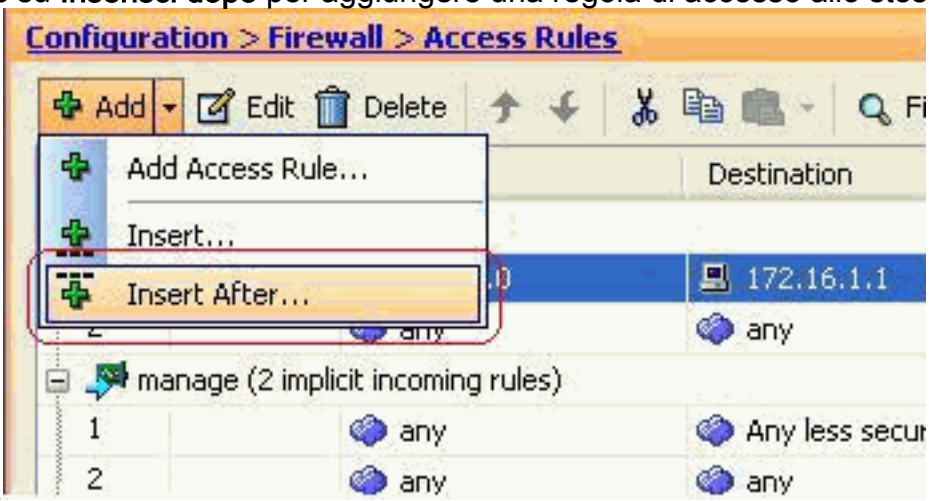
accesso.

4. Fare clic su **OK** per completare la configurazione della regola di

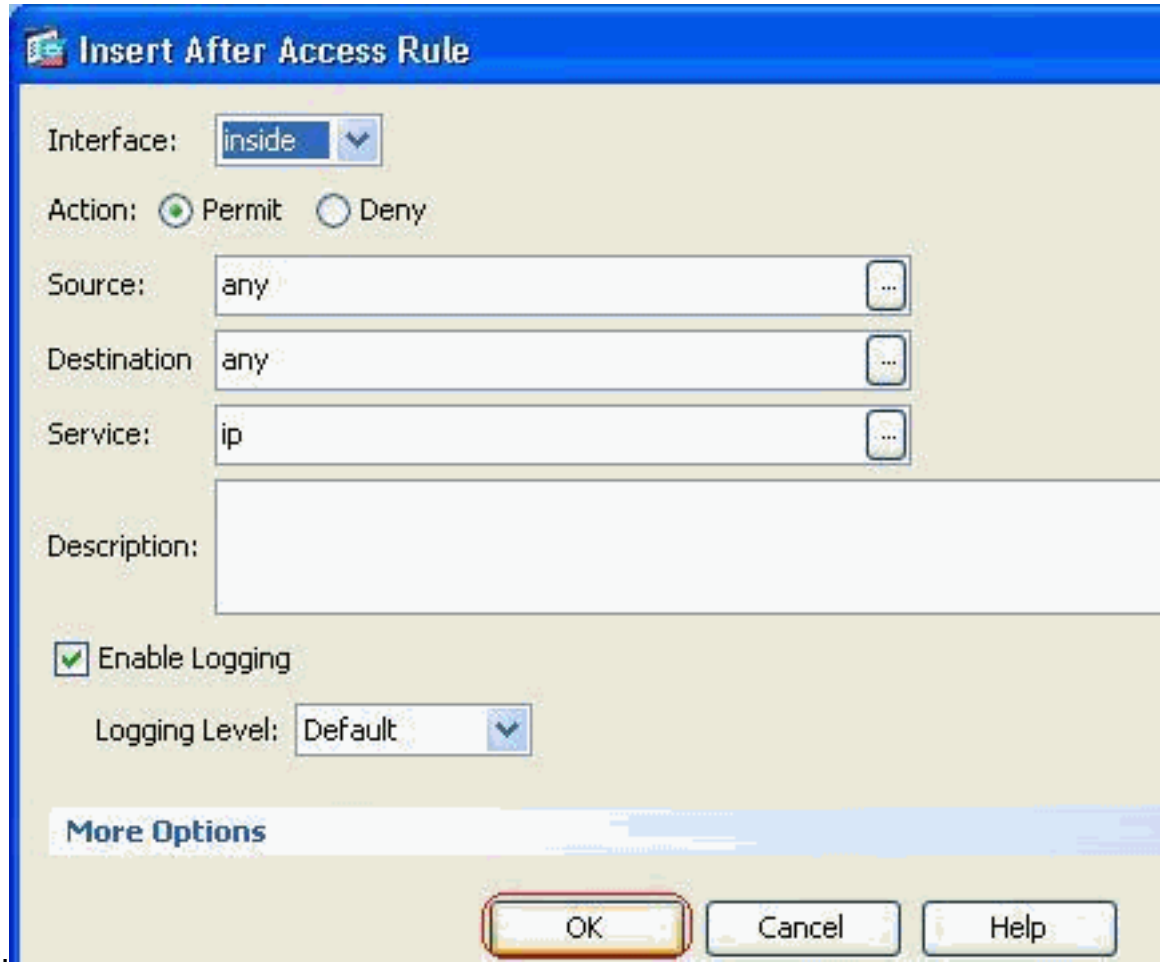
accesso.



5. Fare clic su **Inserisci dopo** per aggiungere una regola di accesso allo stesso elenco degli accessi.

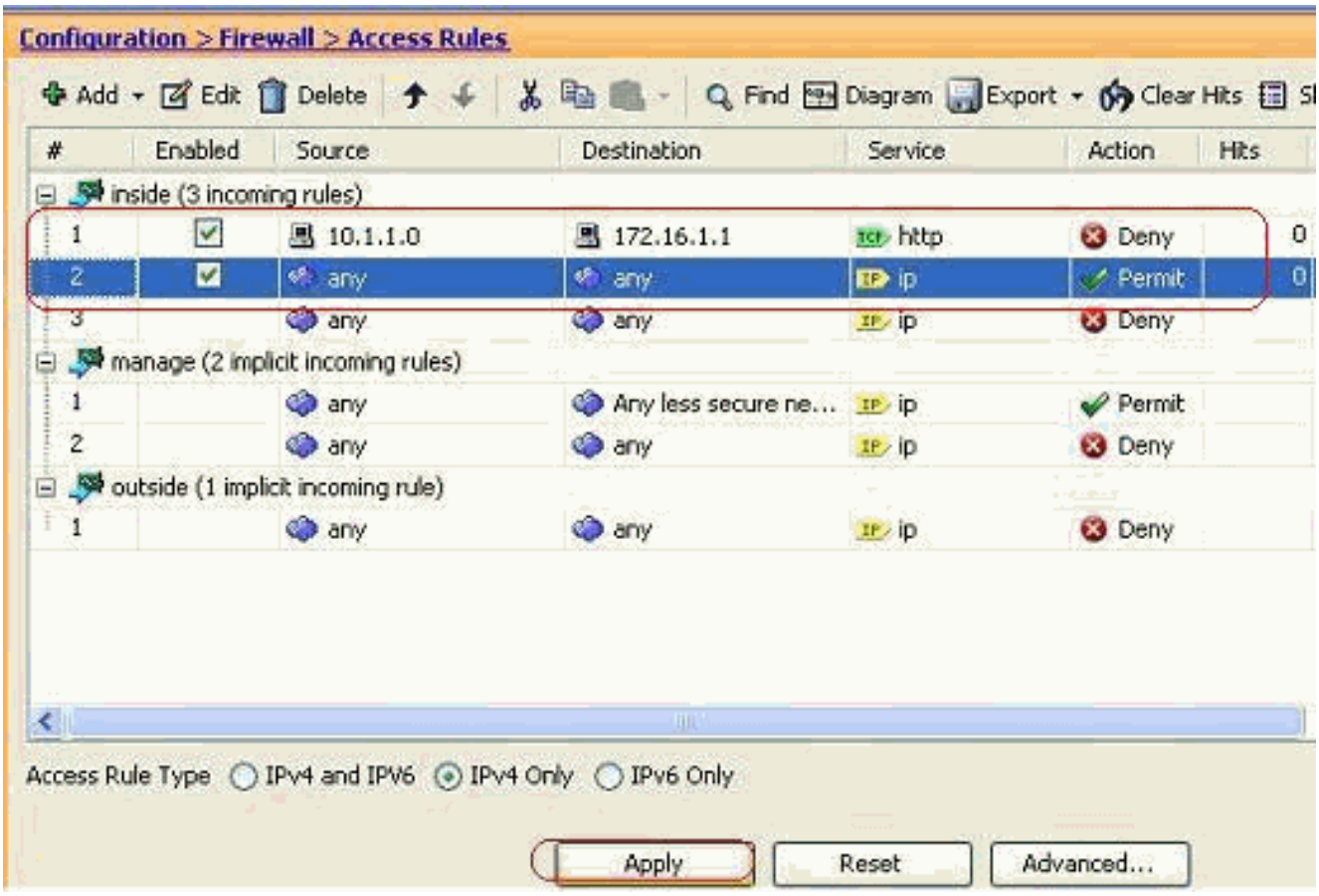


6. Consentire il traffico da "qualsiasi" a "qualsiasi" per impedire il "rifiuto implicito". Fare quindi clic su **OK** per completare l'aggiunta della regola di



accesso.

7. L'elenco degli accessi configurato può essere visualizzato nella scheda Regole di accesso. Fare clic su **Applica** per inviare la configurazione all'appliance di sicurezza.



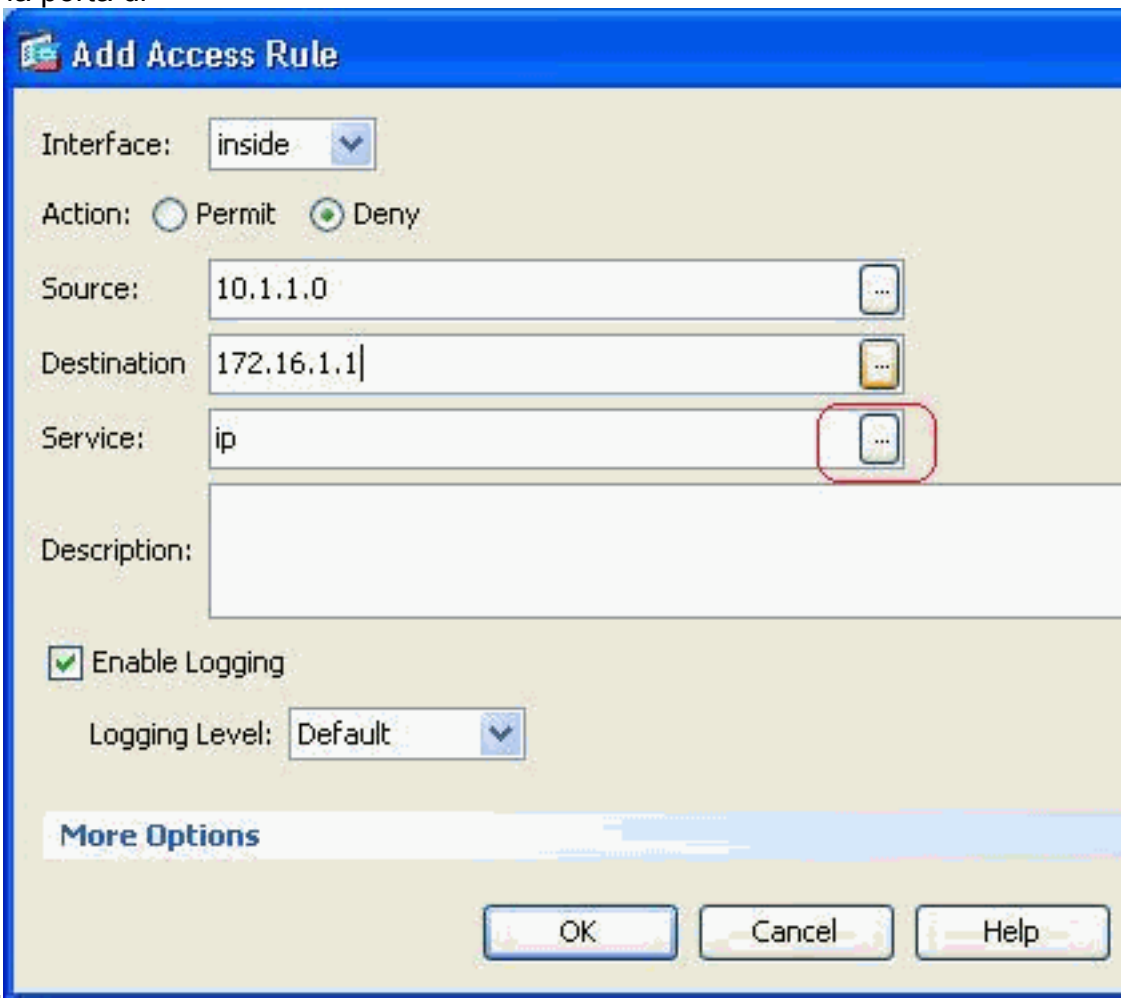
La configurazione inviata dall'ASDM restituisce questo gruppo di comandi sull'interfaccia

della riga di comando (CLI) dell'ASA.

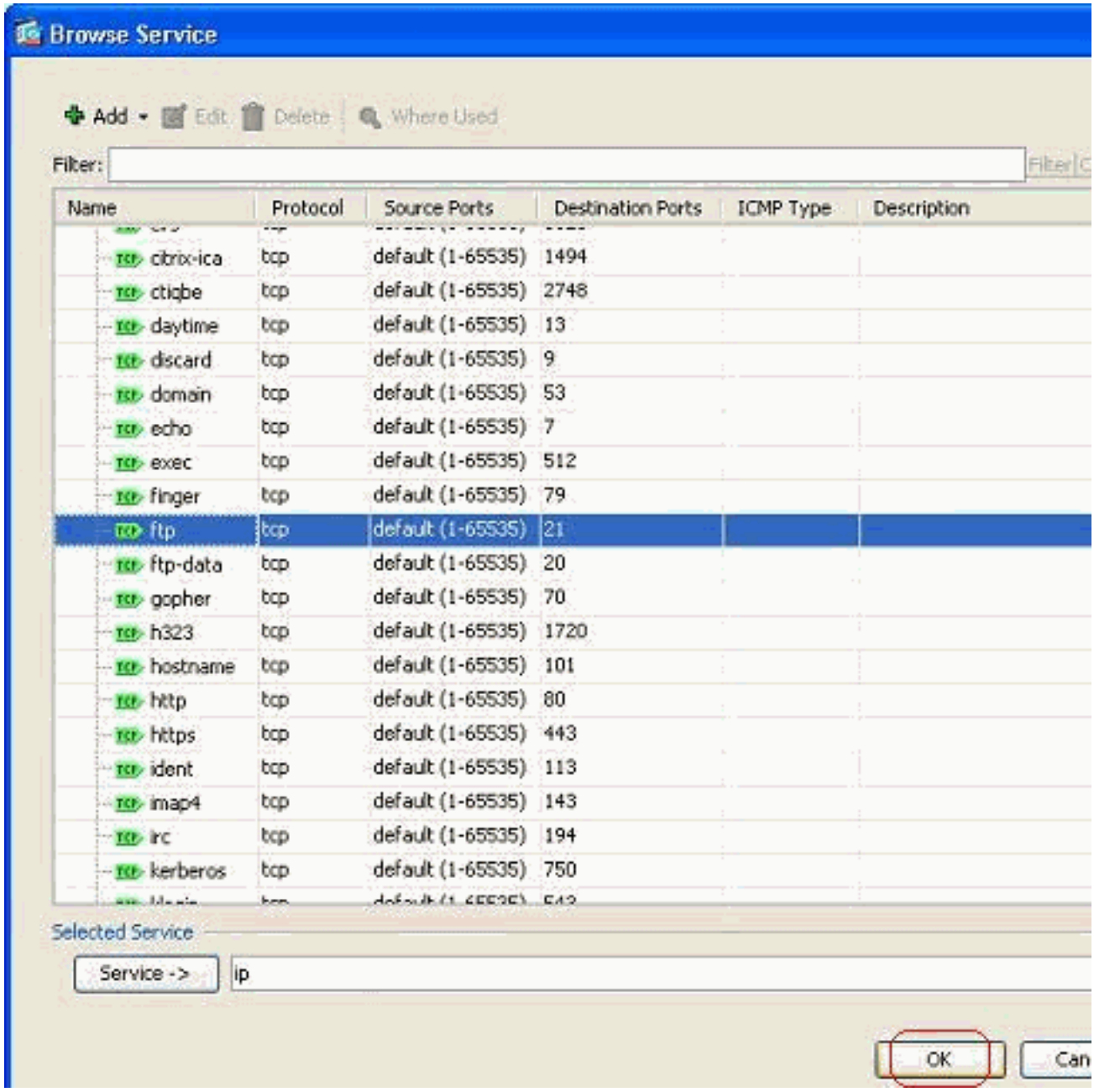
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Mediante questi passaggi, l'esempio 1 è stato eseguito tramite ASDM per impedire alla rete 10.1.1.0 di accedere al server Web, 172.16.1.1. L'esempio 2 può essere ottenuto anche nello stesso modo per impedire all'intera rete 10.1.1.0 di accedere al server FTP, 172.16.1.2. L'unica differenza consiste nel momento in cui si sceglie la porta.**Nota:** si presume che la configurazione della regola di accesso per l'esempio 2 sia nuova.

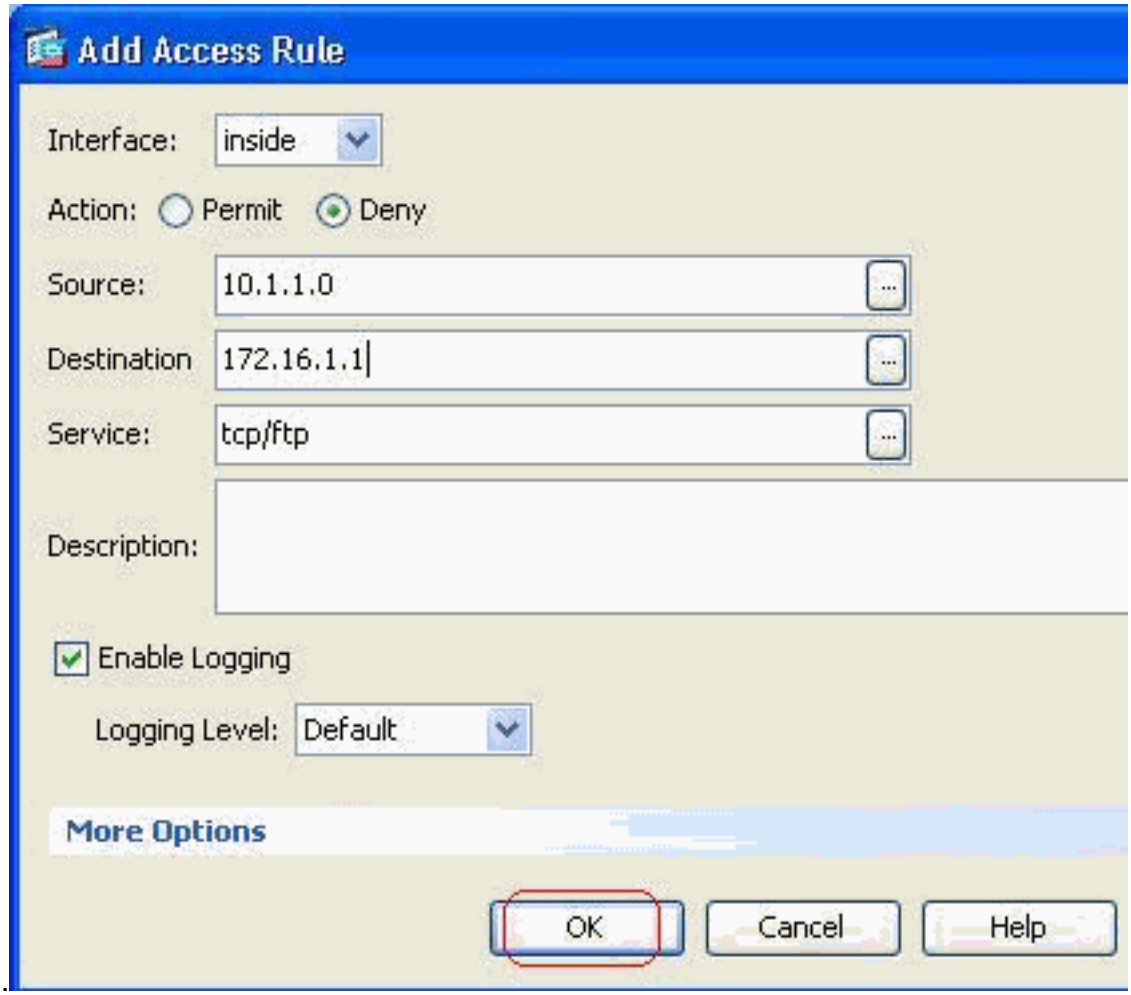
8. Definire la regola di accesso per bloccare il traffico FTP, quindi fare clic sulla scheda **Dettagli** per scegliere la porta di destinazione.



9. Scegliere la porta **ftp** e fare clic su **OK** per tornare alla finestra Aggiungi regola di accesso.

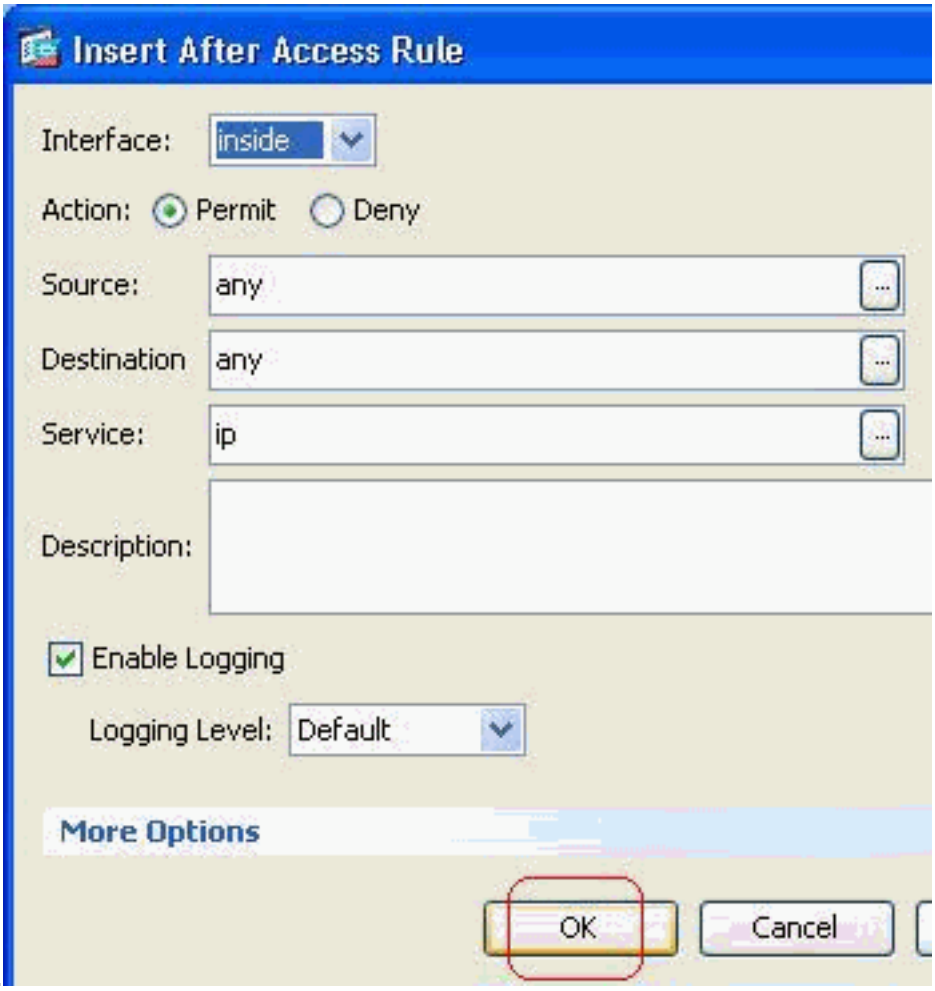


10. Fare clic su **OK** per completare la configurazione della regola di



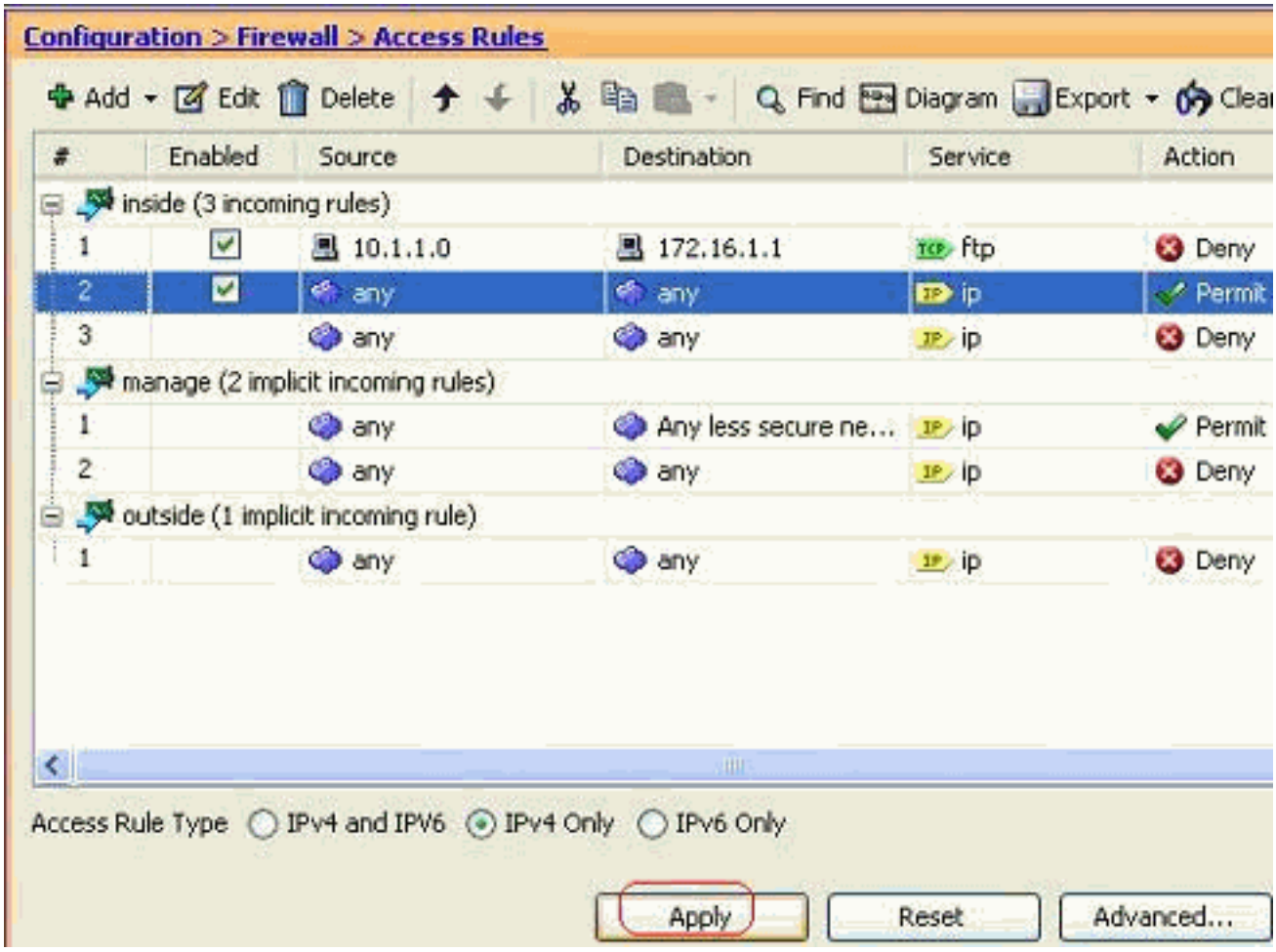
accesso.

11. Aggiungere un'altra regola di accesso per autorizzare qualsiasi altro tipo di traffico. In caso contrario, la regola di rifiuto implicito bloccherà tutto il traffico su questa



interfaccia.

12. L'aspetto della configurazione completa dell'elenco degli accessi è simile a quello della scheda Regole di
accesso.



13. Fare clic su **Apply** per inviare la configurazione all'appliance ASA. La configurazione CLI equivalente è simile alla seguente:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Apertura della configurazione delle porte

L'appliance di sicurezza non consente il traffico in entrata a meno che non sia esplicitamente autorizzato da un elenco degli accessi esteso.

Se si desidera consentire a un host esterno di accedere a un host interno, è possibile applicare un elenco degli accessi in entrata sull'interfaccia esterna. È necessario specificare l'indirizzo tradotto dell'host interno nell'elenco degli accessi perché l'indirizzo tradotto è quello che può essere utilizzato nella rete esterna. Completare questa procedura per aprire le porte dall'area di sicurezza inferiore a quella di sicurezza superiore. Ad esempio, consentire il traffico dall'esterno (area di sicurezza inferiore) all'interfaccia interna (area di sicurezza superiore) o alla DMZ all'interfaccia interna.

1. NAT statico crea una traduzione fissa di un indirizzo reale in un indirizzo mappato. Questo indirizzo mappato è un indirizzo host su Internet che può essere utilizzato per accedere al server applicazioni sulla DMZ senza la necessità di conoscere l'indirizzo reale del server.

```
static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
   access-list access_list_name | interface}
```

   Per ulteriori informazioni, consultare la sezione Static NAT della guida di riferimento dei comandi per PIX/ASA.

2. Per autorizzare il traffico sulla porta, creare un ACL.

```
access-list
```

3. Per essere attivo, associare l'elenco degli accessi con il comando **access-group**.

```
access-group
```

Esempi:

1. **Aprire il traffico della porta SMTP:** Aprire la porta **tcp 25** per consentire agli host esterni (Internet) di accedere al server di posta situato nella rete DMZ.Il comando **Static** mappa l'indirizzo esterno 192.168.5.3 all'indirizzo DMZ reale 172.16.1.3.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **Aprire il traffico della porta HTTPS:** Aprire la porta **tcp 443** per consentire agli host esterni (Internet) di accedere al server Web (protetto) situato nella rete DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **Consenti traffico DNS:** Aprire la porta **udp 53** per consentire agli host esterni (Internet) di accedere al server DNS (protetto) situato nella rete DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

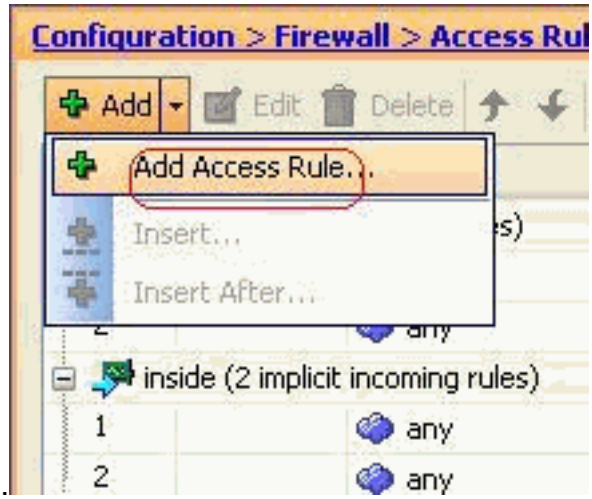
Nota: per ulteriori informazioni sull'assegnazione delle porte, consultare il documento sulle porte IANA.

Configurazione tramite ASDM

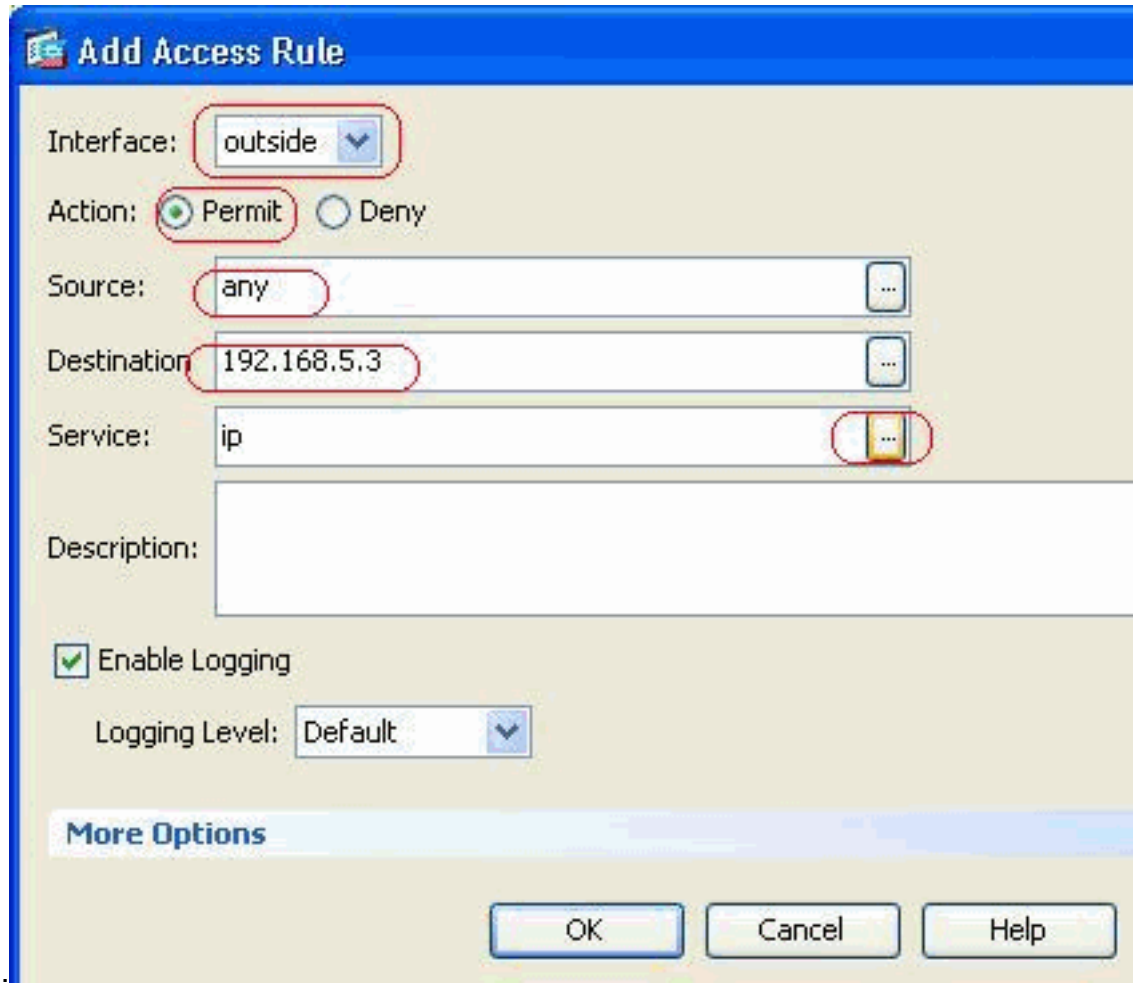
In questa sezione viene illustrato un approccio graduale per eseguire le attività sopra descritte tramite ASDM.

1. Creare la regola di accesso per autorizzare il traffico smtp sul server

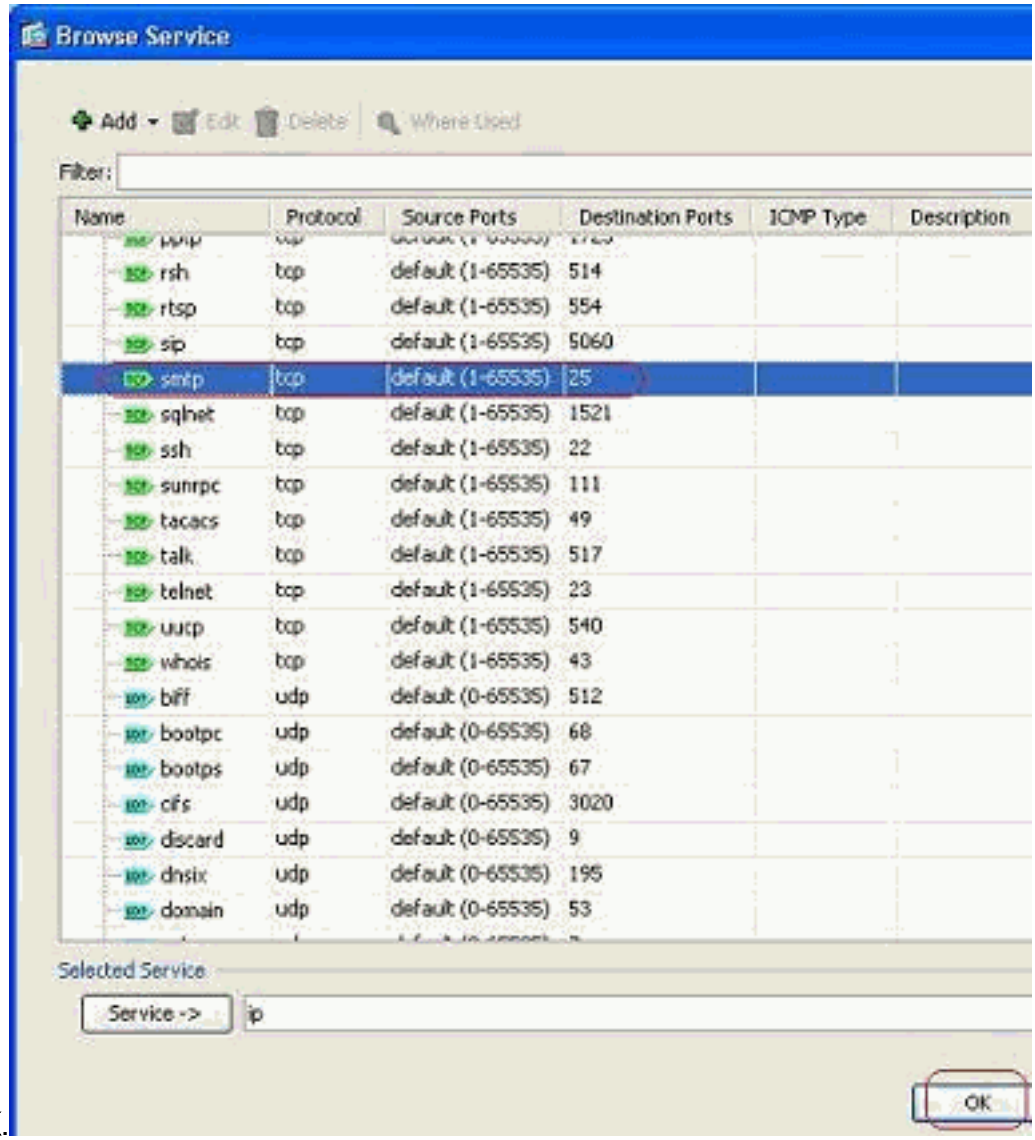
192.168.5.3.



2. Definire l'origine e la destinazione della regola di accesso e l'interfaccia a cui la regola è associata. Definire inoltre l'azione come **Consenti**.

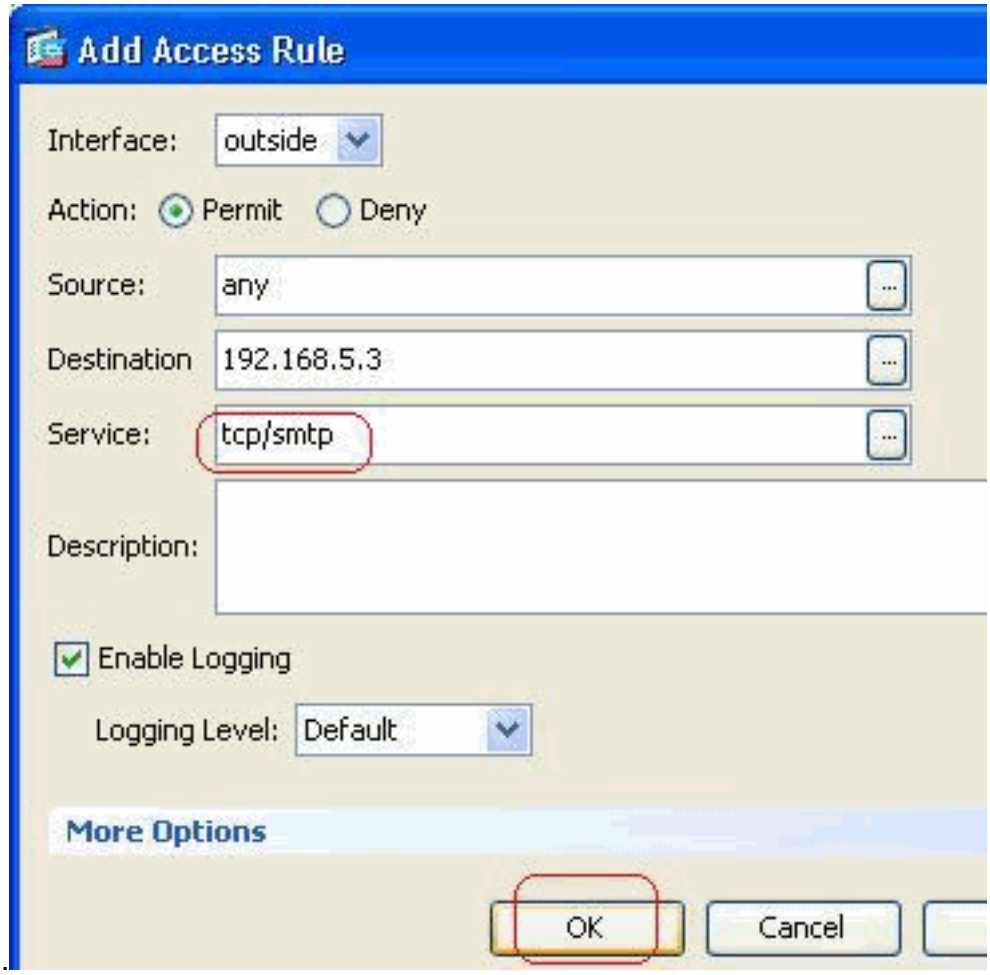


3. Selezionare **SMTP** come porta, quindi fare clic su



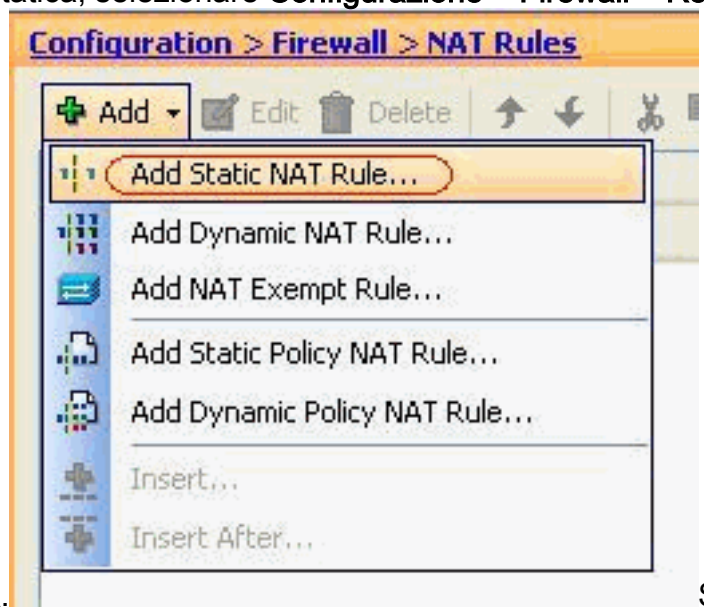
OK.

4. Fare clic su **OK** per completare la configurazione della regola di

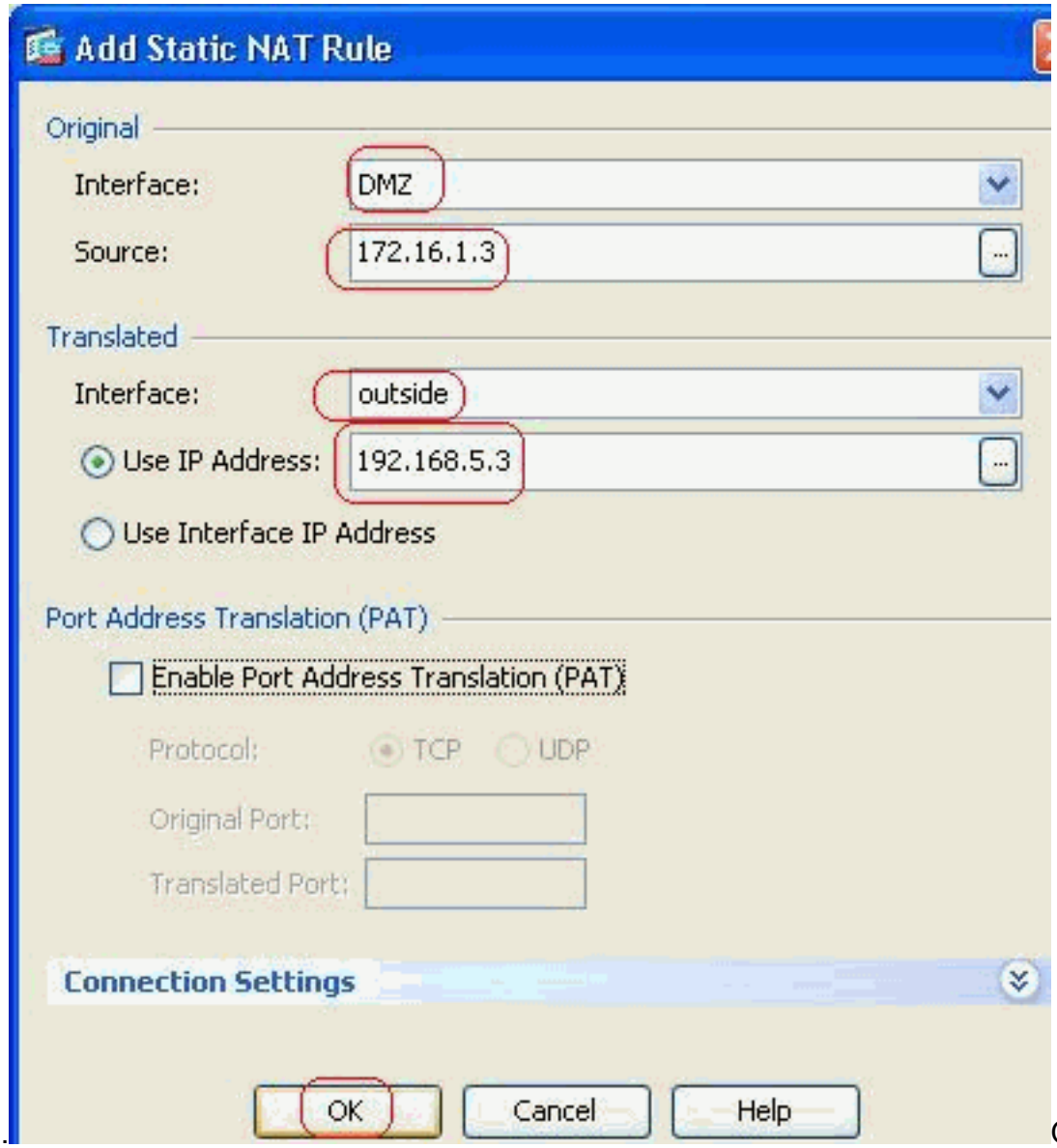


accesso.

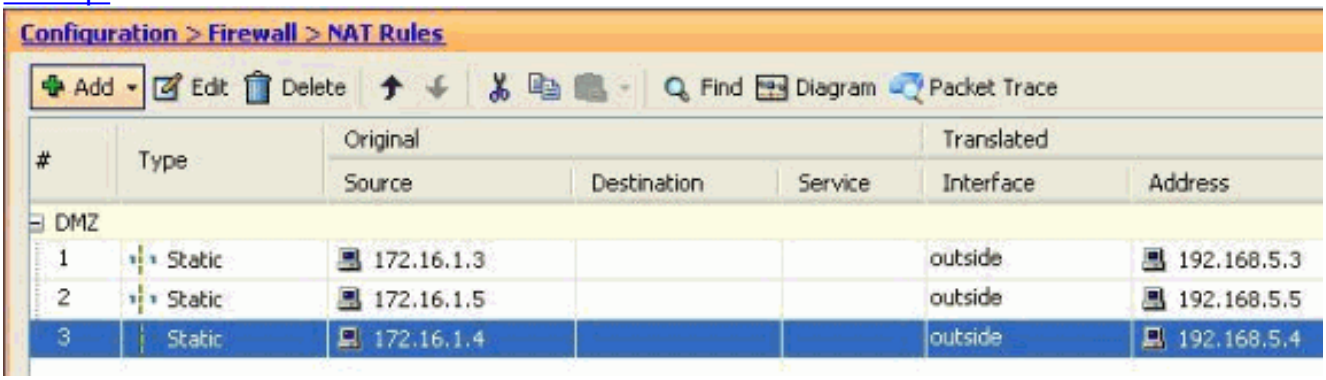
5. Configurare il NAT statico per convertire le versioni da 172.16.1.3 a 192.168.5.3Per aggiungere una voce NAT statica, selezionare **Configurazione > Firewall > Regole NAT >**



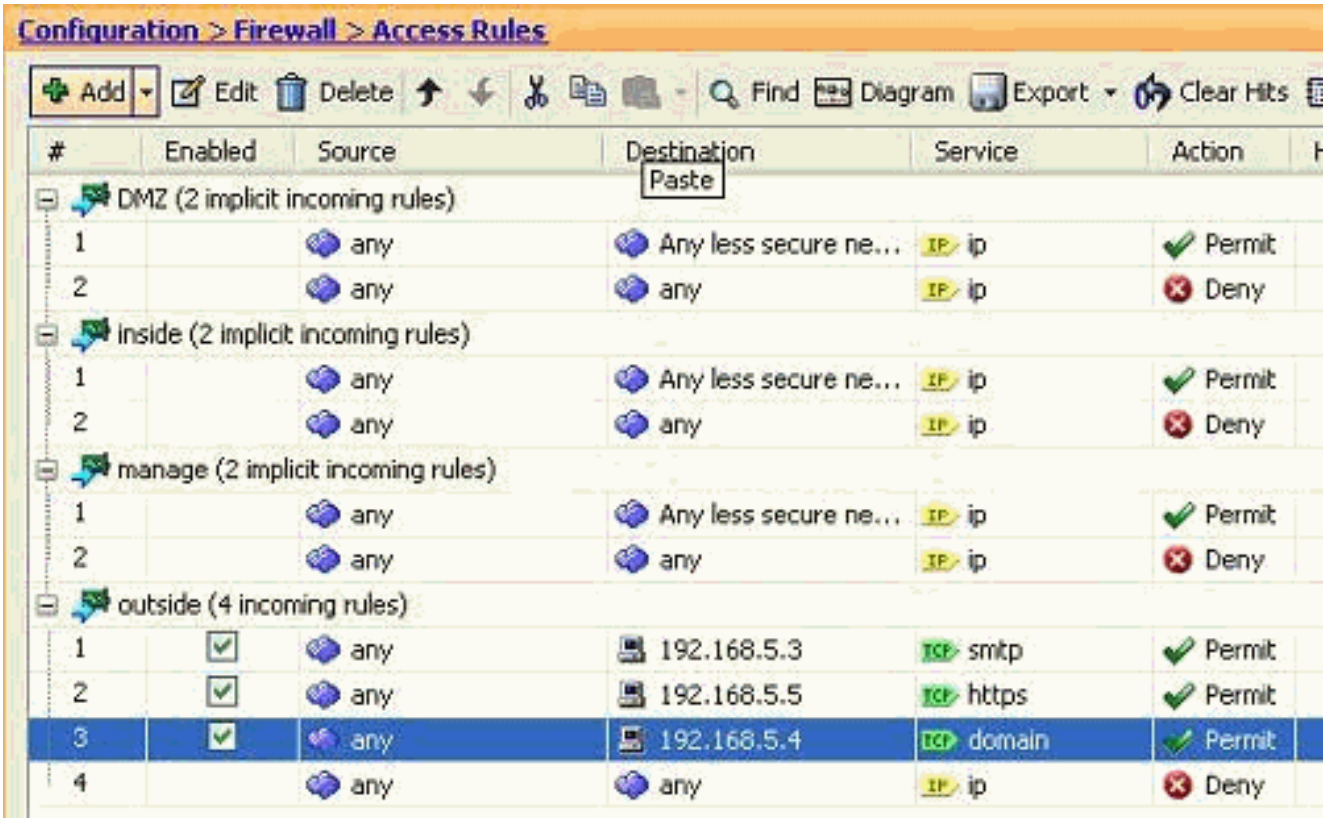
Aggiungi regola NAT statica. Selezionare l'origine originale e l'indirizzo IP tradotto insieme alle interfacce associate, quindi fare clic su **OK** per completare la configurazione della regola NAT



statica. Questa immagine mostra tutte e tre le regole statiche elencate nella sezione Esempi:



Questa immagine mostra tutte e tre le regole di accesso elencate nella sezione Esempi:



Verifica

Èpossibile eseguire la verifica con alcuni comandi **show**, come mostrato di seguito:

- **show xlate -** visualizza le informazioni correnti sulla traduzione
- **show access-list**: visualizza i contatori visite per i criteri di accesso
- **show logging**: visualizza i log nel buffer.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

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

Informazioni correlate

- PIX/ASA 7.x: Abilita/Disabilita la comunicazione tra le interfacce
- PIX 7.0 e Adaptive Security Appliance Port Redirection(Forwarding) con comandi nat, global, static, conduit e access-list
- Uso dei comandi nat, global, static, conduit e access-list e del reindirizzamento delle porte (inoltro) su PIX
- PIX/ASA 7.x: Esempio di configurazione dell'abilitazione dei servizi FTP/TFTP
- PIX/ASA 7.x: Esempio di configurazione dell'abilitazione dei servizi VoIP (SIP,MGCP,H323,SCCP)
- PIX/ASA 7.x: Esempio di accesso al server di posta nella DMZ

- Documentazione e supporto tecnico – Cisco Systems