ASA 8.2: Reindirizzamento delle porte (inoltro) con comandi nat, globali, statici e access-list tramite ASDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Esempio di rete
Consenti accesso in uscita
Consenti agli host interni l'accesso alle reti esterne con NAT
Consenti agli host interni l'accesso alle reti esterne con PAT
Limita l'accesso degli host interni alle reti esterne
Consenti traffico tra interfacce con lo stesso livello di sicurezza
Consenti agli host non attendibili l'accesso agli host della rete attendibile
Disabilita NAT per host/reti specifiche
Reindirizzamento porte (inoltro) con statistiche
Limita sessione TCP/UDP tramite statico
Lista accessi temporizzati
Informazioni correlate

Introduzione

In questo documento viene descritto il funzionamento del reindirizzamento delle porte su Cisco Adaptive Security Appliance (ASA) con ASDM. Tratta del controllo di accesso del traffico attraverso l'ASA e del funzionamento delle regole di traduzione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Panoramica NAT
- PIX/ASA 7.X: Reindirizzamento porte

Componenti usati

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

- Cisco serie 5500 ASA versione 8.2
- Cisco ASDM versione 6.3

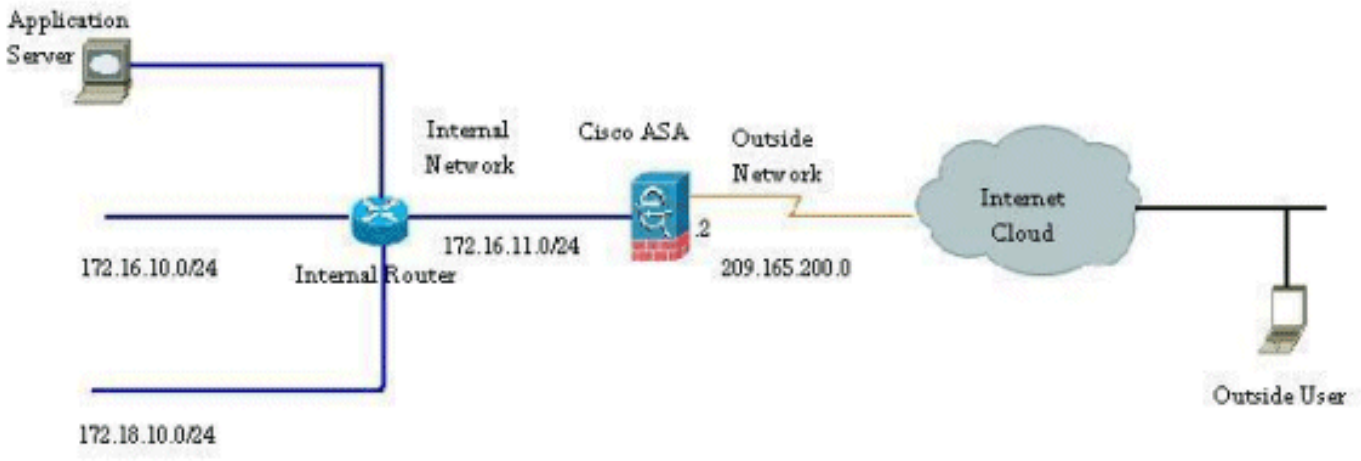
Nota: questa configurazione funziona correttamente solo dal software Cisco ASA versione 8.0 a 8.2, in quanto non ci sono modifiche importanti nella funzionalità NAT.

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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempio di rete

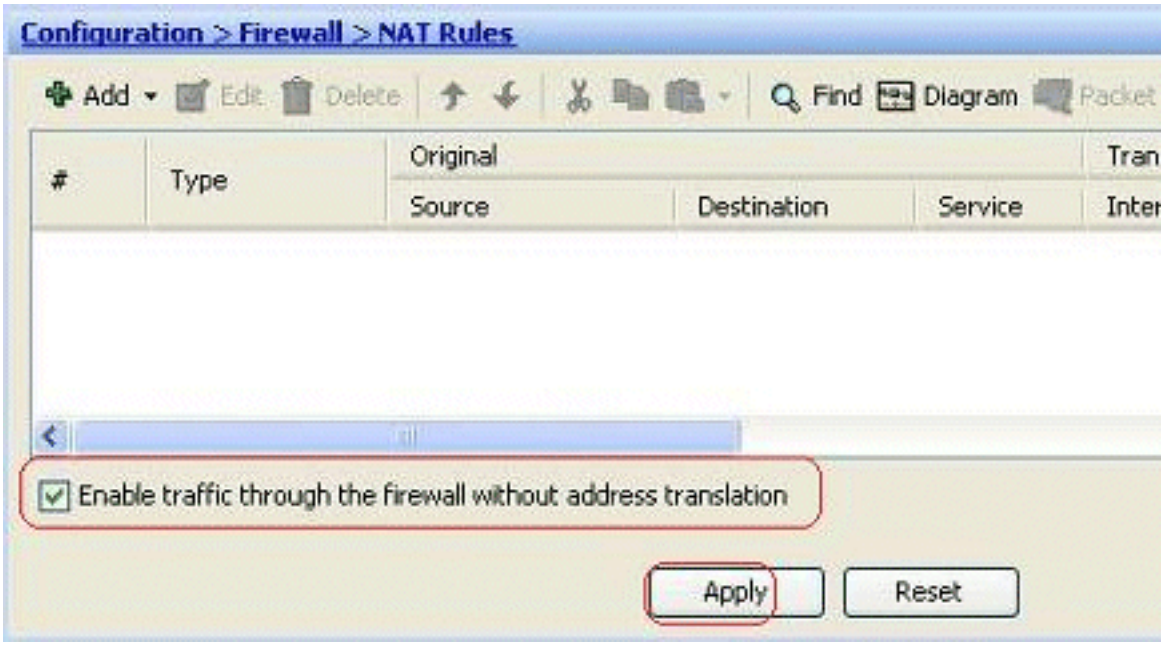


Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Consenti accesso in uscita

L'accesso in uscita descrive le connessioni da un'interfaccia con un livello di protezione più elevato a un'interfaccia con un livello di protezione più basso. Ciò include le connessioni dall'interno all'esterno, dall'interno alle zone demilitarizzate (DMZ) e le DMZ all'esterno. Questo può includere anche connessioni da una DMZ a un'altra, purché l'interfaccia dell'origine della connessione abbia un livello di protezione più alto rispetto alla destinazione.

Nessuna connessione può passare attraverso Appliance di sicurezza senza una regola di conversione configurata. Questa funzione è denominata nat-control. Nell'immagine mostrata di seguito viene mostrato come disabilitare questa funzionalità tramite ASDM per consentire le connessioni tramite ASA senza alcuna conversione degli indirizzi. Tuttavia, se è stata configurata una regola di conversione, la disattivazione di questa funzionalità non rimarrà valida per tutto il traffico e sarà necessario esentare esplicitamente le reti dalla conversione degli indirizzi.

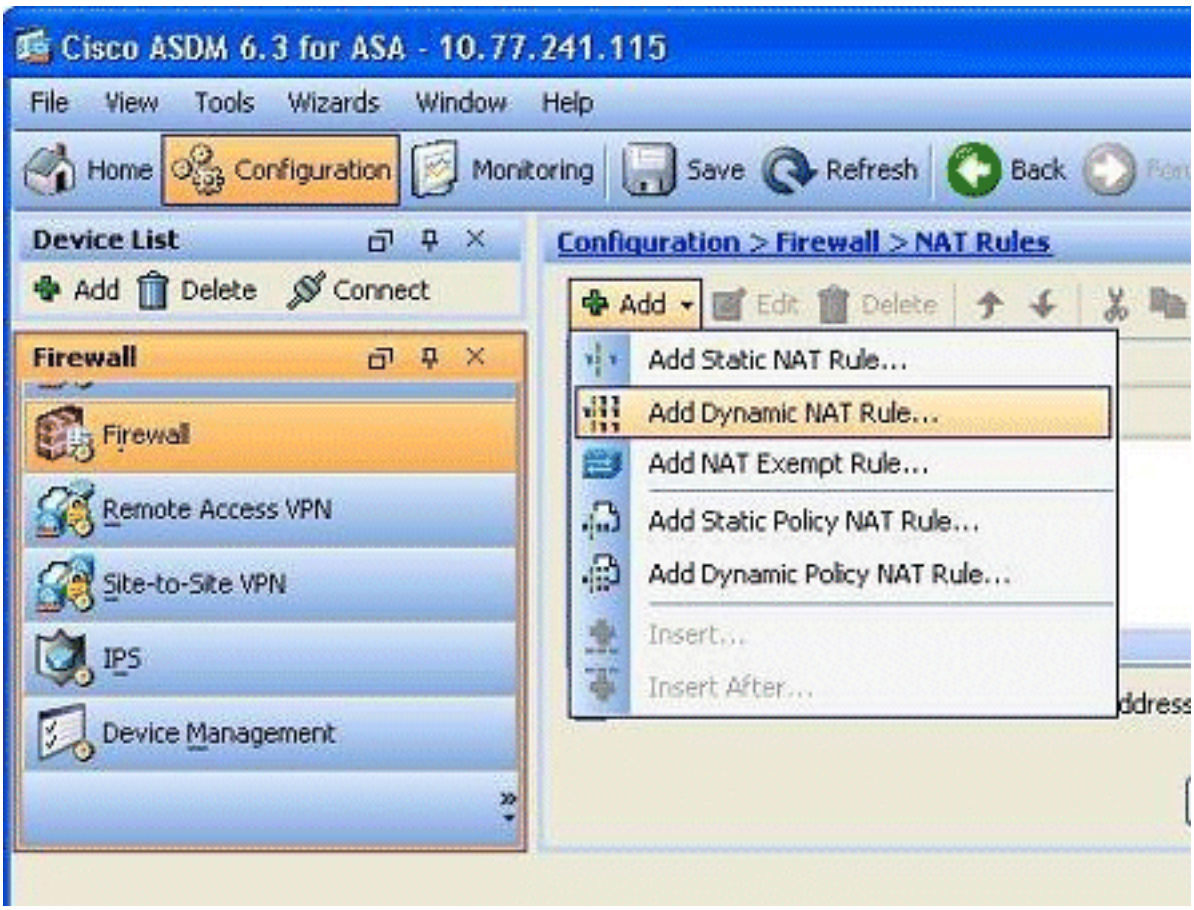


Consenti agli host interni l'accesso alle reti esterne con NAT

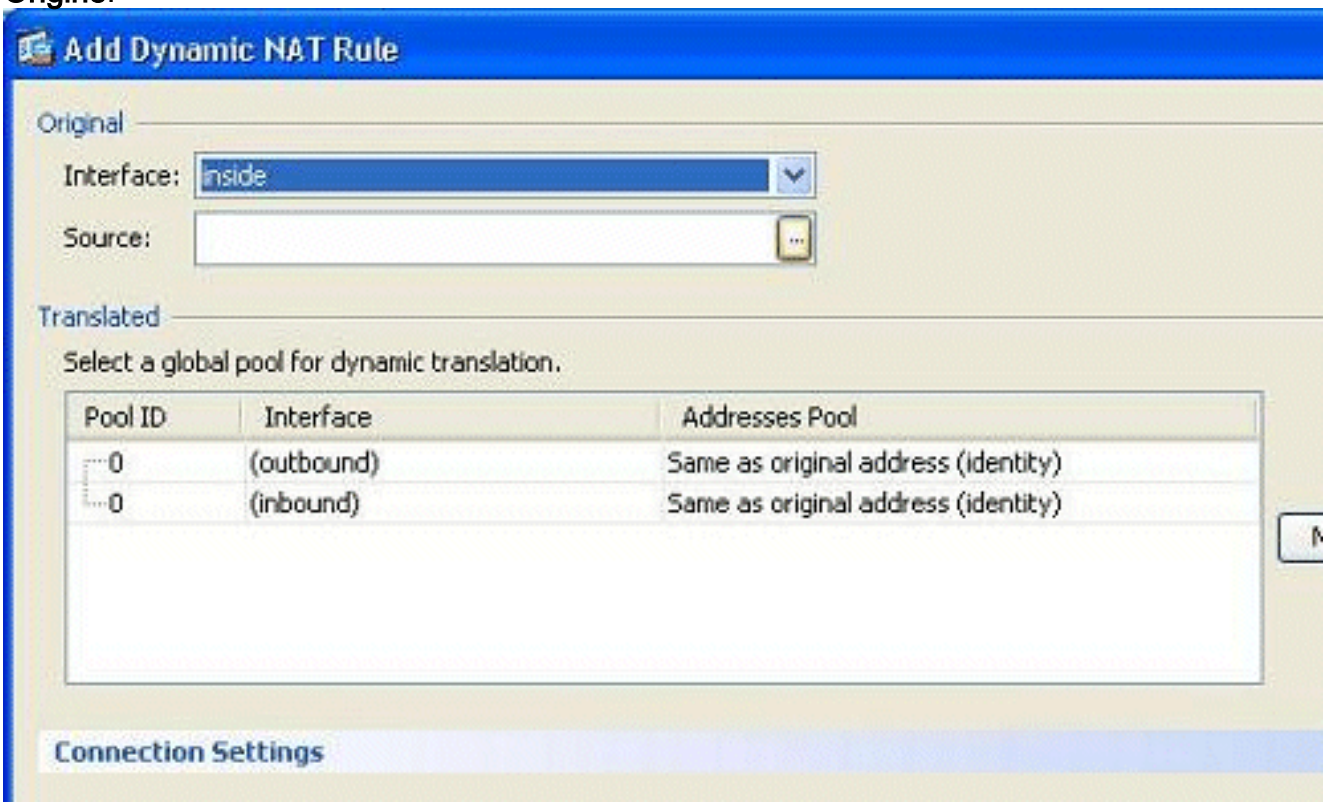
Èpossibile consentire a un gruppo di host/reti interni di accedere al mondo esterno configurando le regole NAT dinamiche. A tal fine, è necessario selezionare l'indirizzo reale degli host/reti a cui concedere l'accesso e associarli a un pool di indirizzi IP tradotti.

Completare questi passaggi per consentire agli host interni di accedere alle reti esterne con NAT:

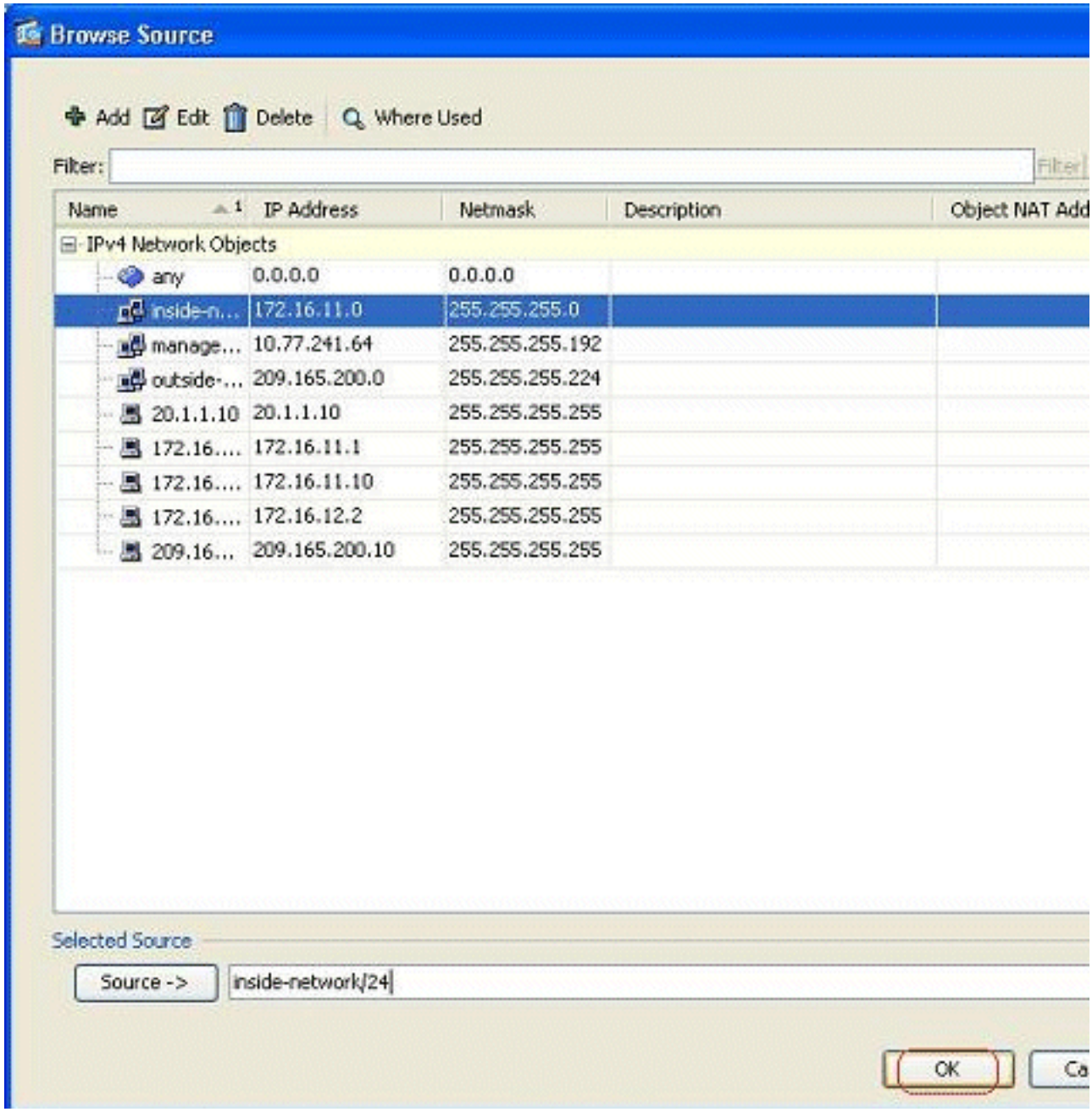
1. Andare a Configurazione > **Firewall** > **Regole NAT**, fare clic su **Aggiungi**, quindi scegliere l'opzione **Aggiungi regola NAT dinamica** per configurare una regola NAT dinamica.



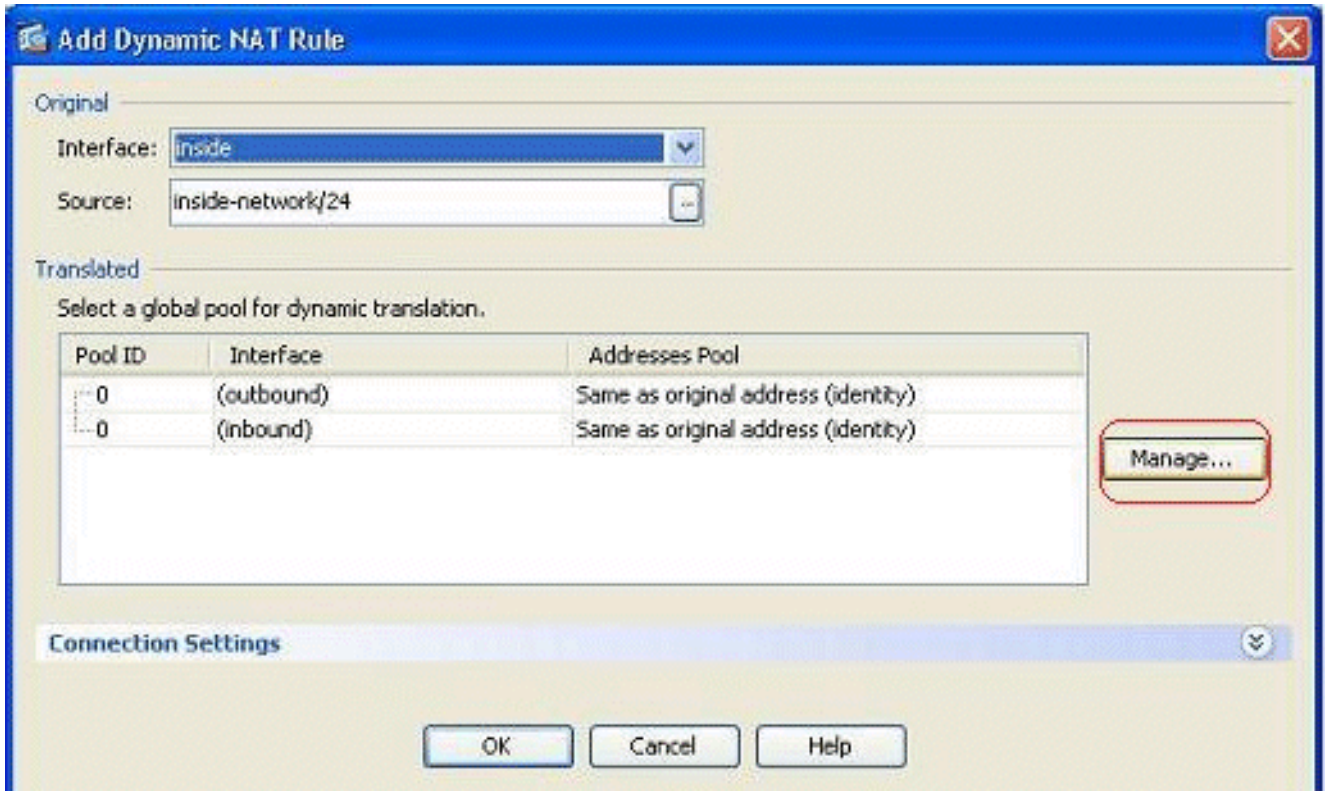
2. Scegliere il nome dell'interfaccia a cui sono connessi gli host reali. Scegliere l'indirizzo IP reale degli host/reti utilizzando il pulsante **Dettagli** nel campo **Origine**.



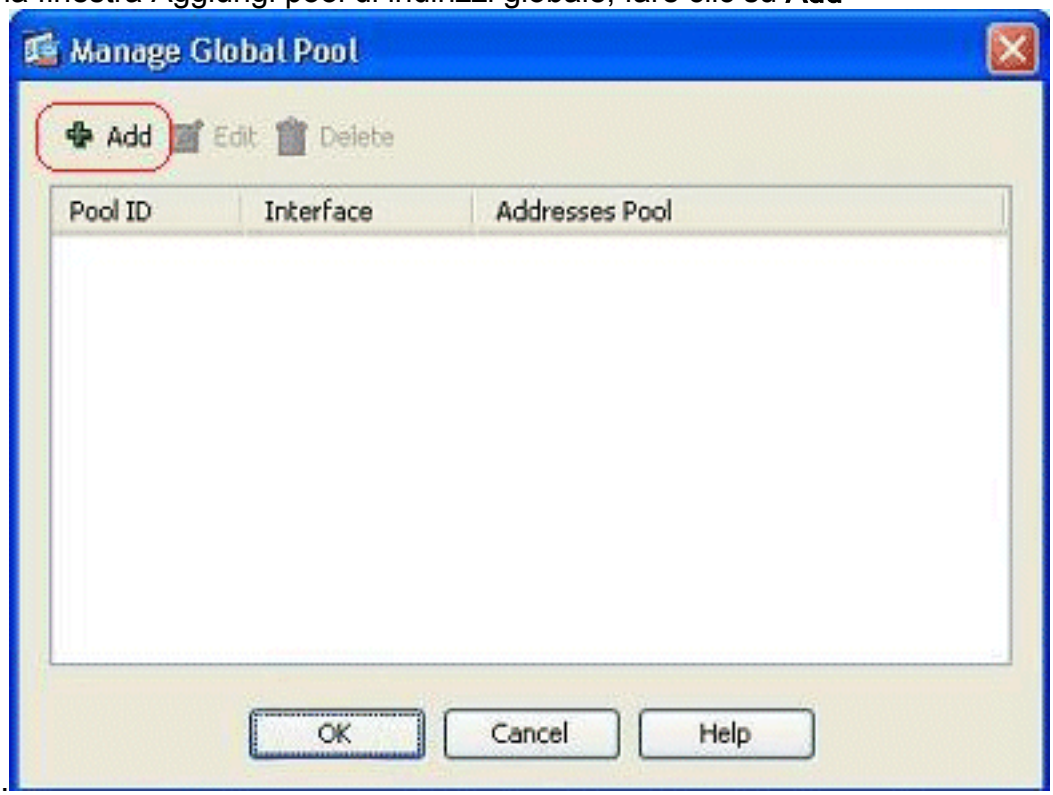
3. Nell'esempio è stata selezionata l'intera *rete interna*. Per completare la selezione, fare clic su **OK**.



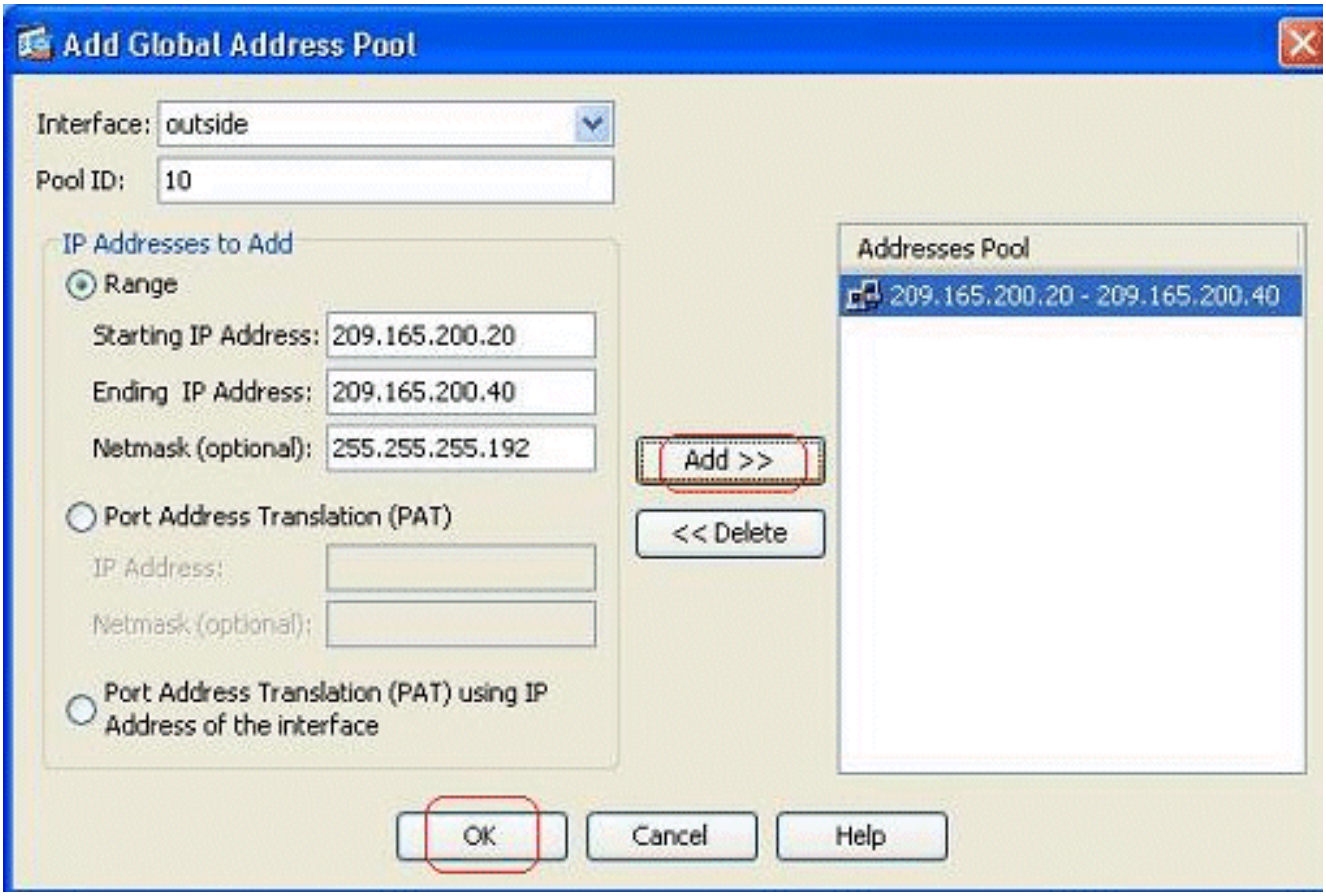
4. Per selezionare il pool di indirizzi IP a cui mappare la rete reale, fare clic su **Gestisci**.



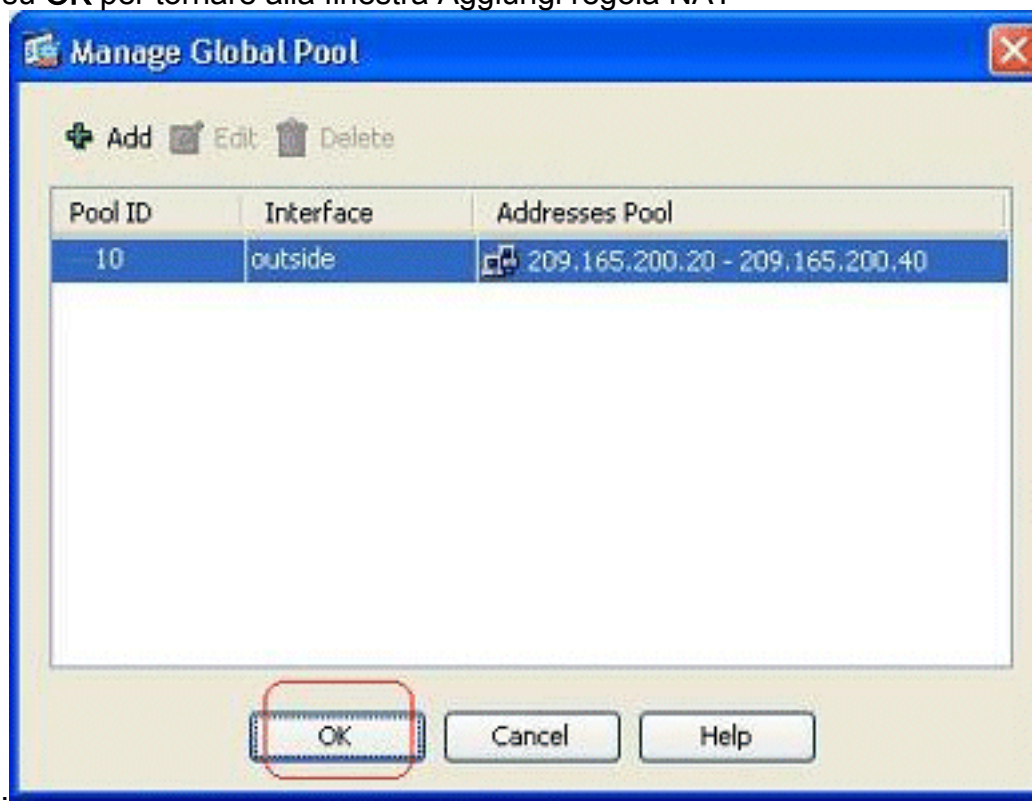
5. Per aprire la finestra Aggiungi pool di indirizzi globale, fare clic su **Add** (Aggiungi).



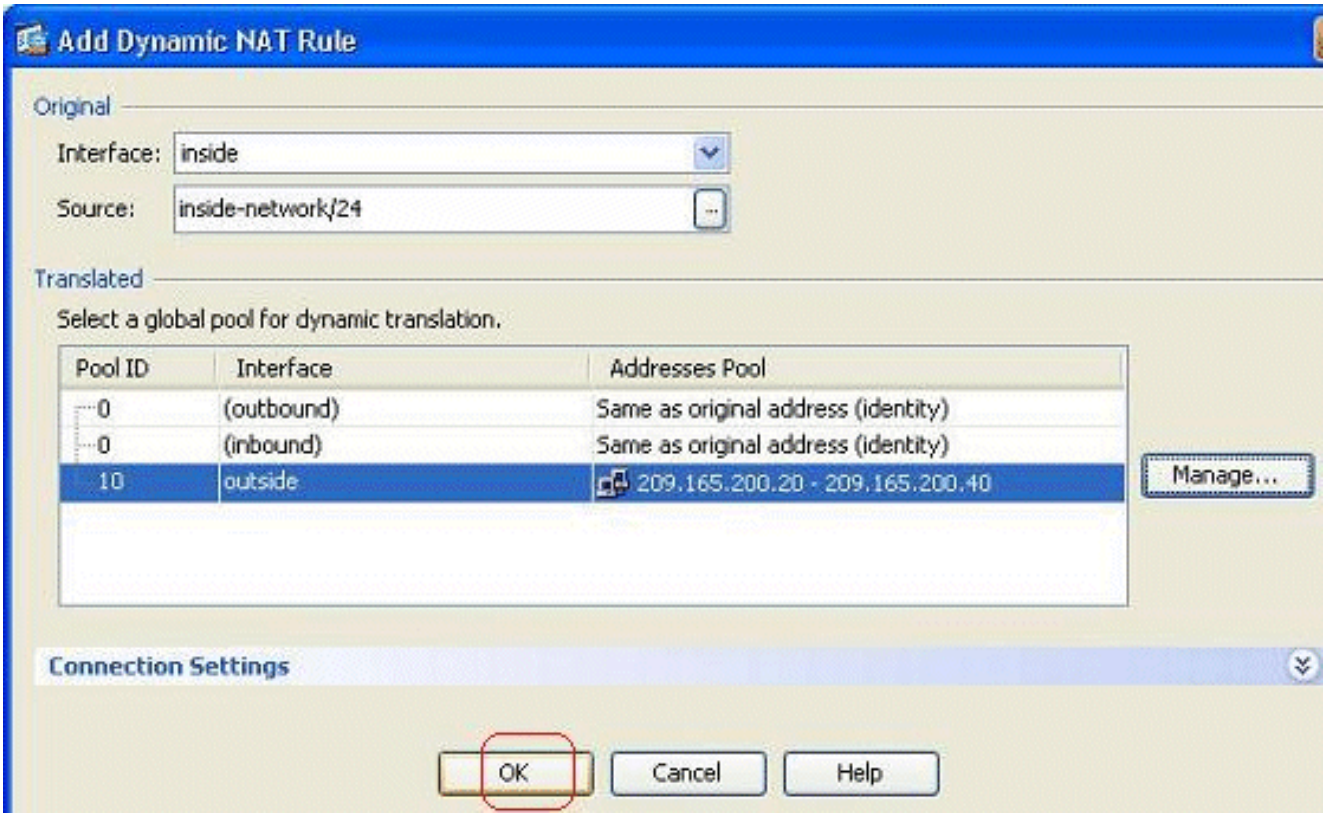
6. Selezionare l'opzione **Range** (Intervallo) e specificare gli indirizzi IP iniziale e finale insieme all'interfaccia di uscita. Inoltre, specificare un ID pool univoco e fare clic su **Add** per aggiungerli al pool di indirizzi. Fare clic su **OK** per tornare alla finestra Gestisci pool globale.



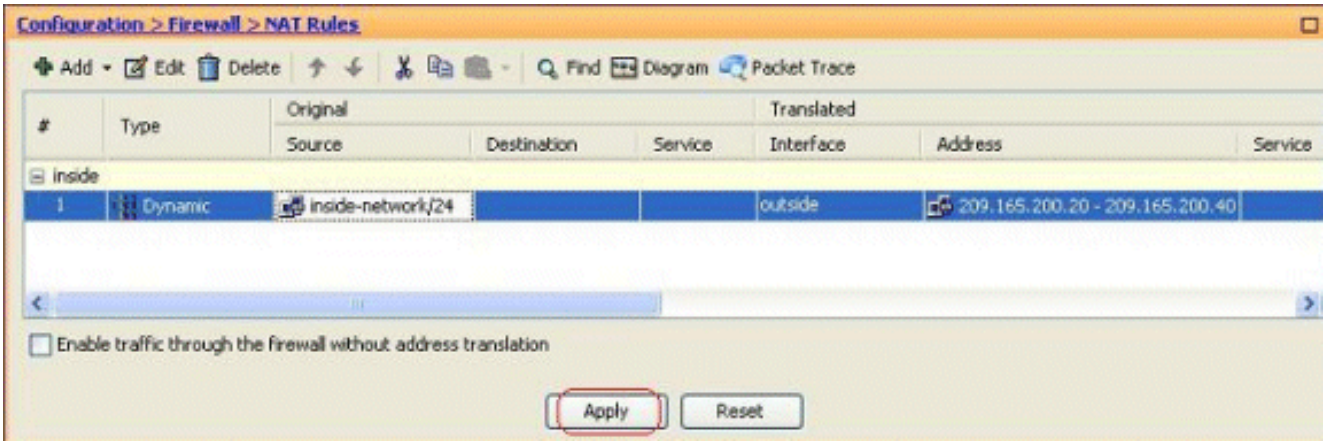
7. Fare clic su **OK** per tornare alla finestra Aggiungi regola NAT dinamica.



8. Per completare la configurazione della regola NAT dinamica, fare clic su **OK**.



9. Per rendere effettive le modifiche, fare clic su **Applica**.**Nota:** l'opzione **Abilita traffico attraverso il firewall senza conversione degli indirizzi** è deselezionata.



Questo è l'output CLI equivalente per questa configurazione ASDM:

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

In base a questa configurazione, gli host nella rete 172.16.11.0 verranno convertiti in qualsiasi indirizzo IP del pool NAT, 209.165.200.20-209.165.200.40. L'ID del pool NAT è molto importante. È possibile assegnare lo stesso pool NAT a un'altra rete interna/dmz. Se il pool mappato ha meno indirizzi del gruppo reale, è possibile esaurire gli indirizzi se la quantità di traffico è superiore al previsto. Di conseguenza, è possibile provare a implementare PAT o a modificare il pool di indirizzi esistente per estenderlo.

Nota: durante la modifica della regola di traduzione esistente, è necessario utilizzare il comando clear xlate per rendere effettive le modifiche. In caso contrario, la connessione esistente precedente rimarrà nella tabella di connessione fino al timeout. Prestare attenzione quando si

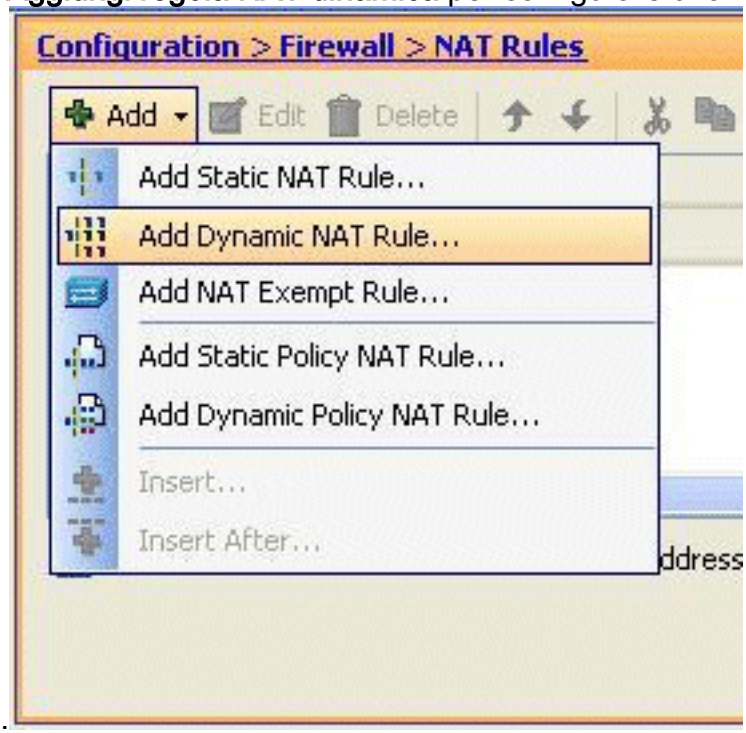
utilizza il comando **clear xlate**, in quanto interrompe immediatamente le connessioni esistenti.

Consenti agli host interni l'accesso alle reti esterne con PAT

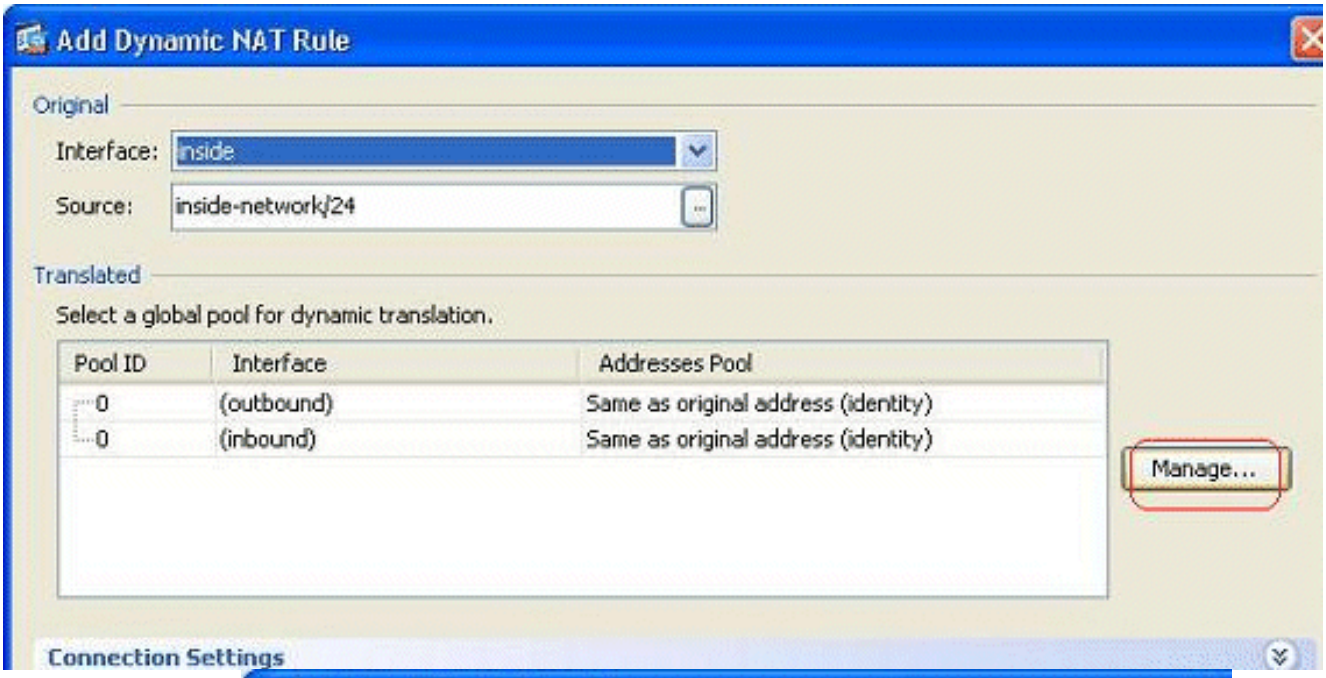
Se si desidera che gli host interni condividano un singolo indirizzo pubblico per la traduzione, utilizzare PAT. Se l'istruzione **globale** specifica un indirizzo, tale indirizzo viene convertito in porta. L'ASA consente la conversione di una porta per interfaccia e supporta fino a 65.535 oggetti **xlate** attivi su un unico indirizzo globale.

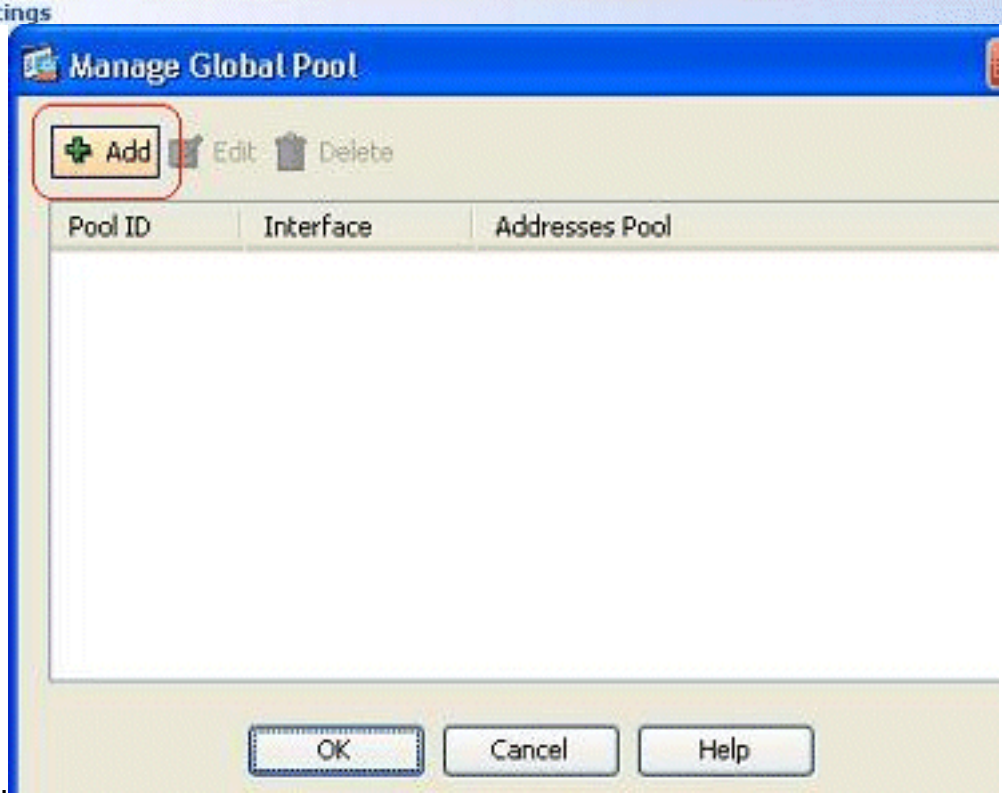
Completare questi passaggi per consentire agli host interni di accedere alle reti esterne con PAT:

1. Andare a Configurazione **> Firewall > Regole NAT**, fare clic su **Aggiungi**, quindi scegliere l'opzione **Aggiungi regola NAT dinamica** per configurare una regola NAT dinamica.

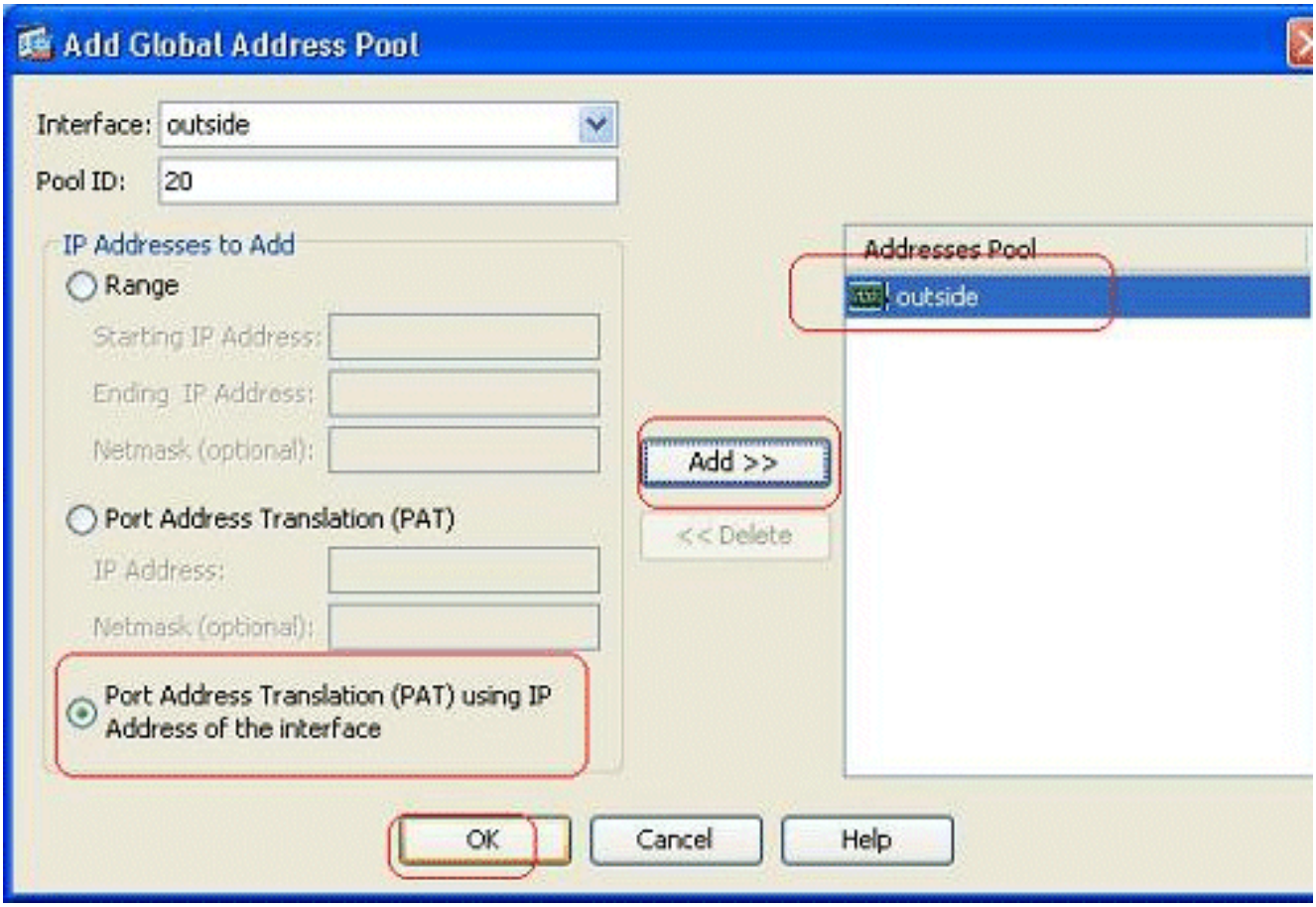


2. Scegliere il nome dell'interfaccia a cui sono connessi gli host reali. Selezionare l'indirizzo IP reale degli host/reti utilizzando il pulsante **Dettagli** nel campo **Source** (Origine), quindi scegliere **inside-network** (Rete interna). Per definire le informazioni sull'indirizzo tradotto, fare clic su **Gestisci**.

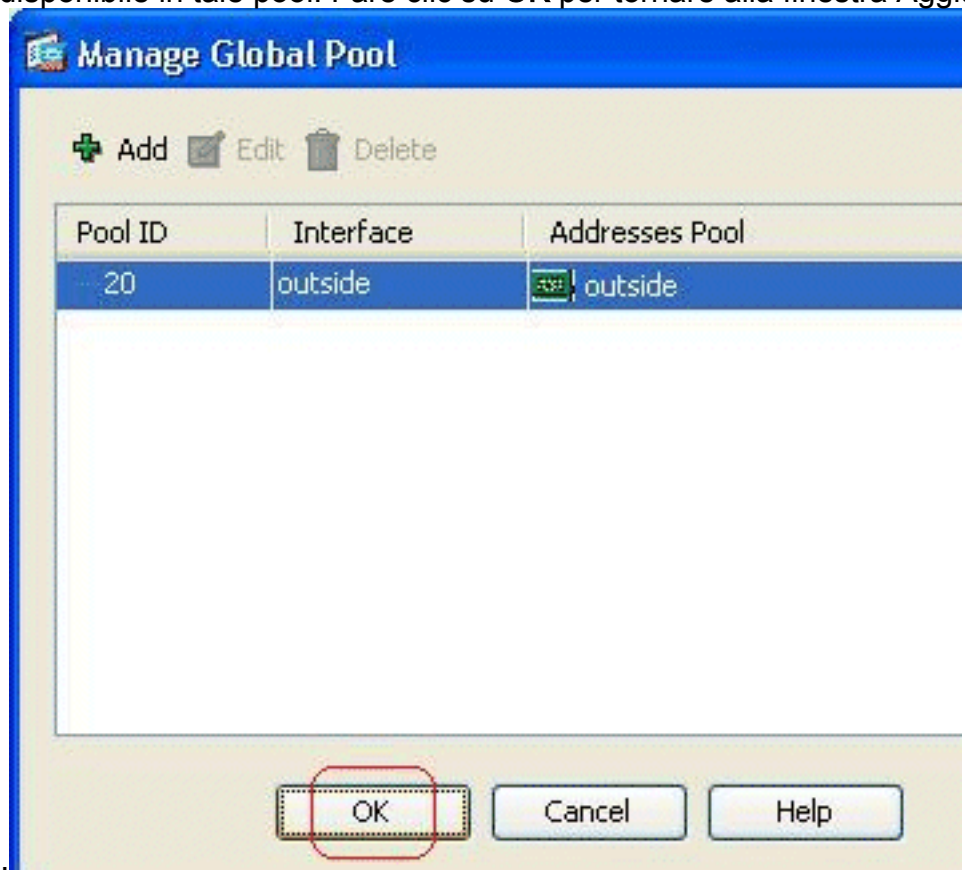




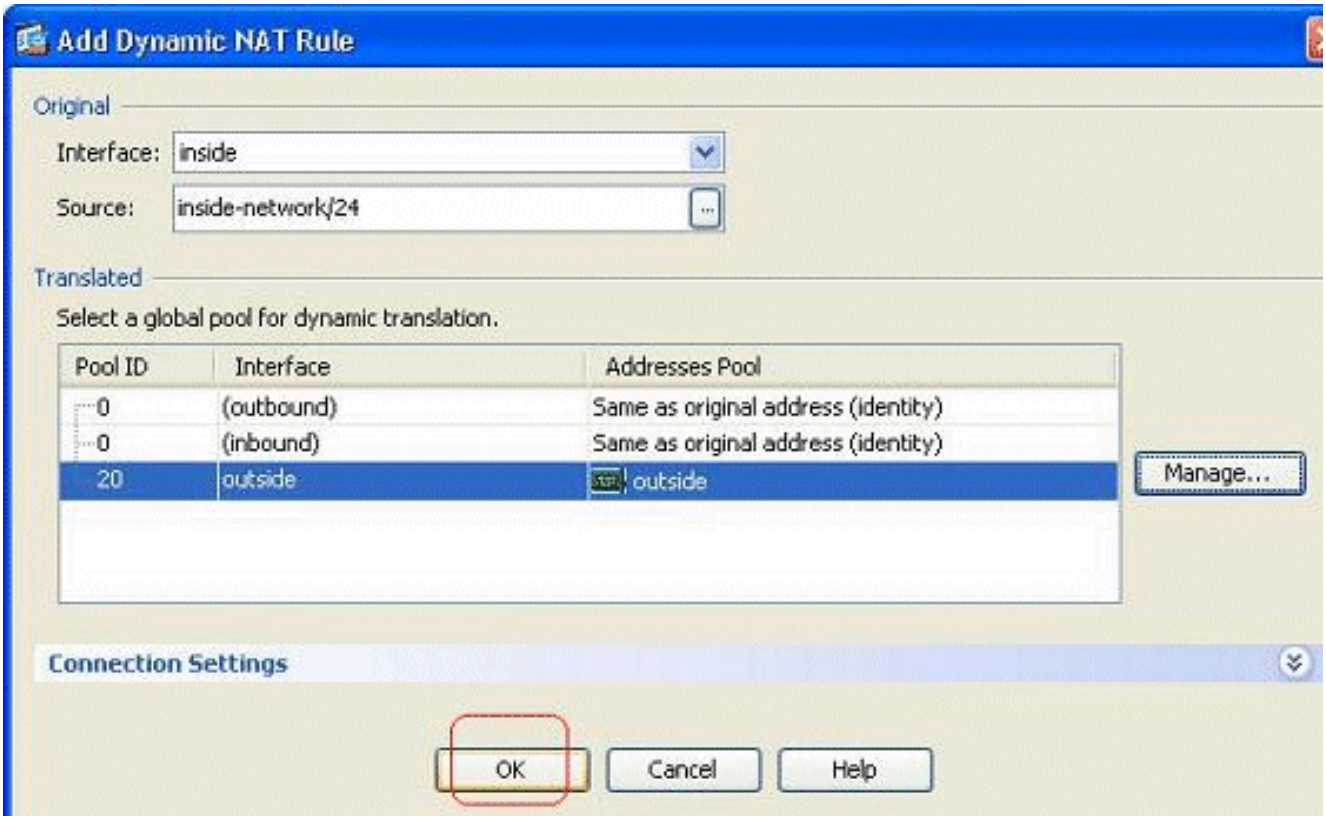
3. Fare clic su **Add**.
4. Selezionare l'opzione **Port Address Translation (PAT) utilizzando l'indirizzo IP dell'interfaccia**, quindi fare clic su **Add** (Aggiungi) per aggiungerlo al pool di indirizzi. Non dimenticare di assegnare un ID univoco per questo pool di indirizzi
NAT.



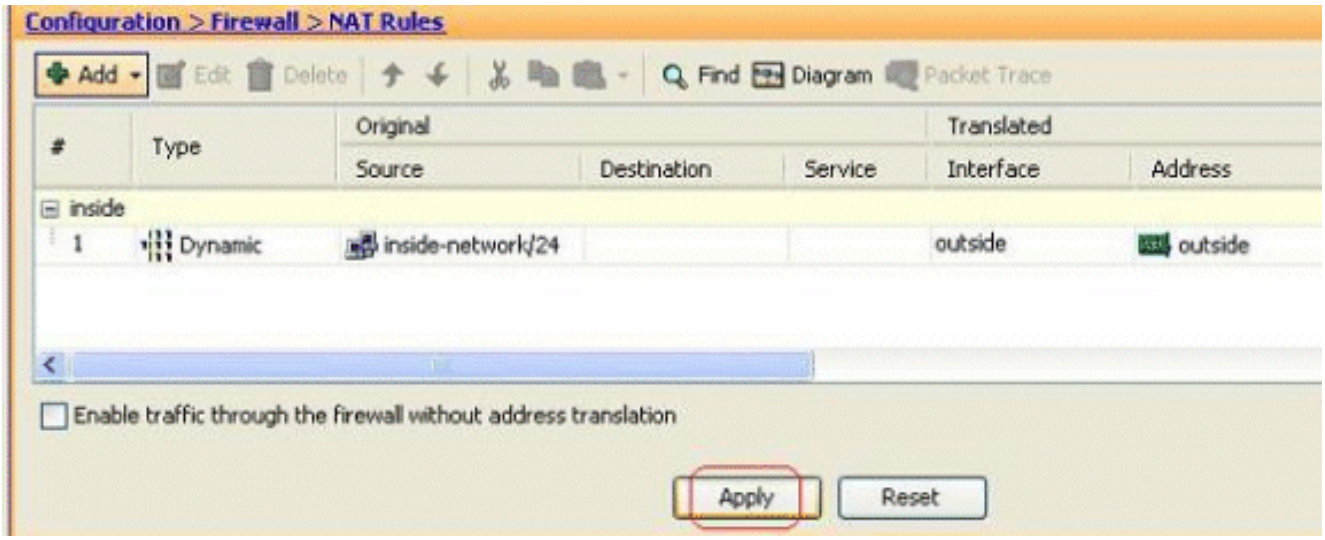
5. Di seguito è riportato il pool di indirizzi configurato con l'interfaccia esterna come unico indirizzo disponibile in tale pool. Fare clic su **OK** per tornare alla finestra Aggiungi regola NAT dinamica.



6. Fare clic su **OK**.



7. La regola NAT dinamica configurata viene visualizzata qui nel riquadro Configurazione > Firewall > Regole NAT.



Questo è l'output CLI equivalente per questa configurazione PAT:

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

Limita l'accesso degli host interni alle reti esterne

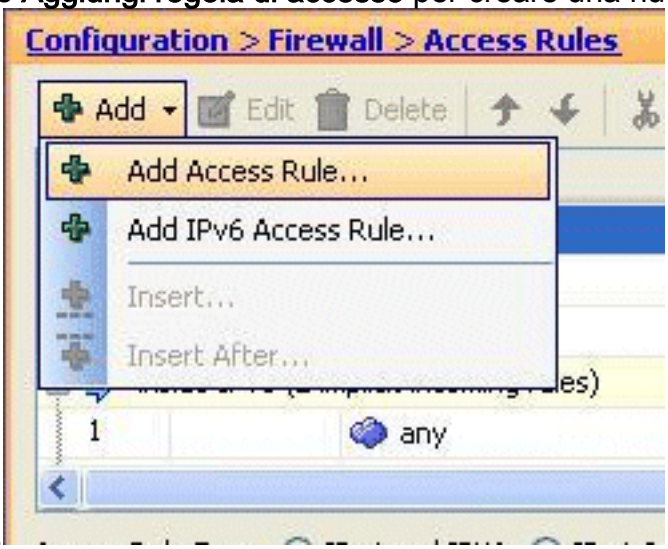
Quando non vengono definite regole di accesso, gli utenti di un'interfaccia con protezione più elevata possono accedere a qualsiasi risorsa associata a un'interfaccia con protezione più bassa. Per impedire a determinati utenti di accedere a determinate risorse, utilizzare le regole di accesso in ASDM. In questo esempio viene descritto come consentire a un singolo utente di accedere a risorse esterne (con FTP, SMTP, POP3, HTTPS e WWW) e impedire a tutti gli altri utenti di

accedere alle risorse esterne.

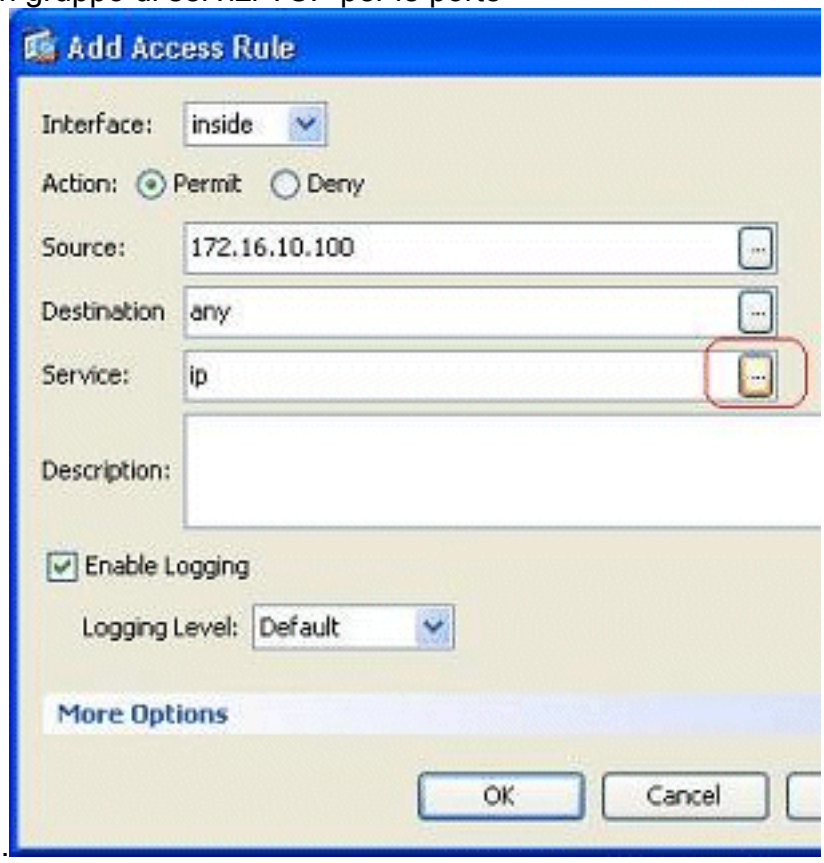
Nota: alla fine di ogni elenco degli accessi sarà presente una regola di "rifiuto implicito".

Attenersi alla seguente procedura:

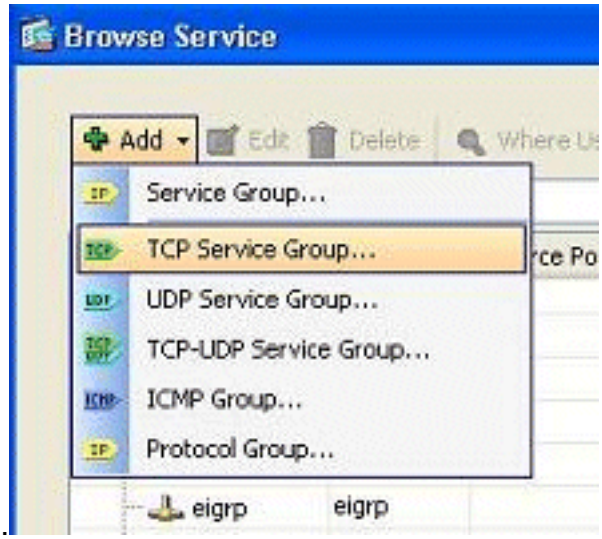
1. Andare a Configurazione > **Firewall** > **Regole di accesso**, fare clic su **Aggiungi** e scegliere l'opzione **Aggiungi regola di accesso** per creare una nuova voce dell'elenco degli accessi.



2. Scegliere l'indirizzo IP di origine da autorizzare nel campo **Origine**. Selezionate **any** come Destinazione (Destination), **inside** come Interfaccia (Interface) e **Permit** come Azione (**Permit**). Infine, fare clic sul pulsante **Details** (Dettagli) nel campo Service (Servizio) per creare un gruppo di servizi TCP per le porte richieste.

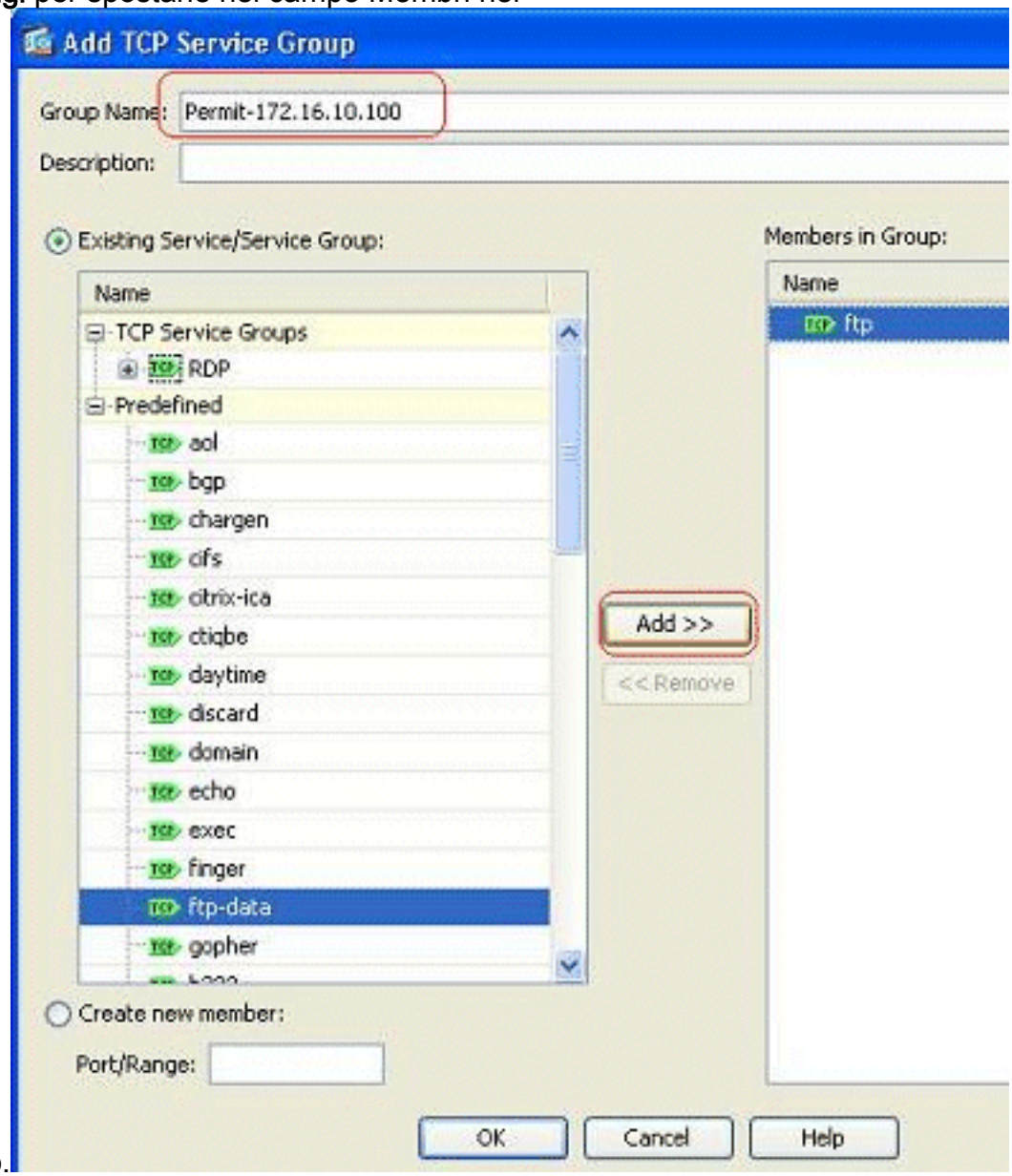


3. Fare clic su **Add**, quindi scegliere l'opzione **TCP Service**



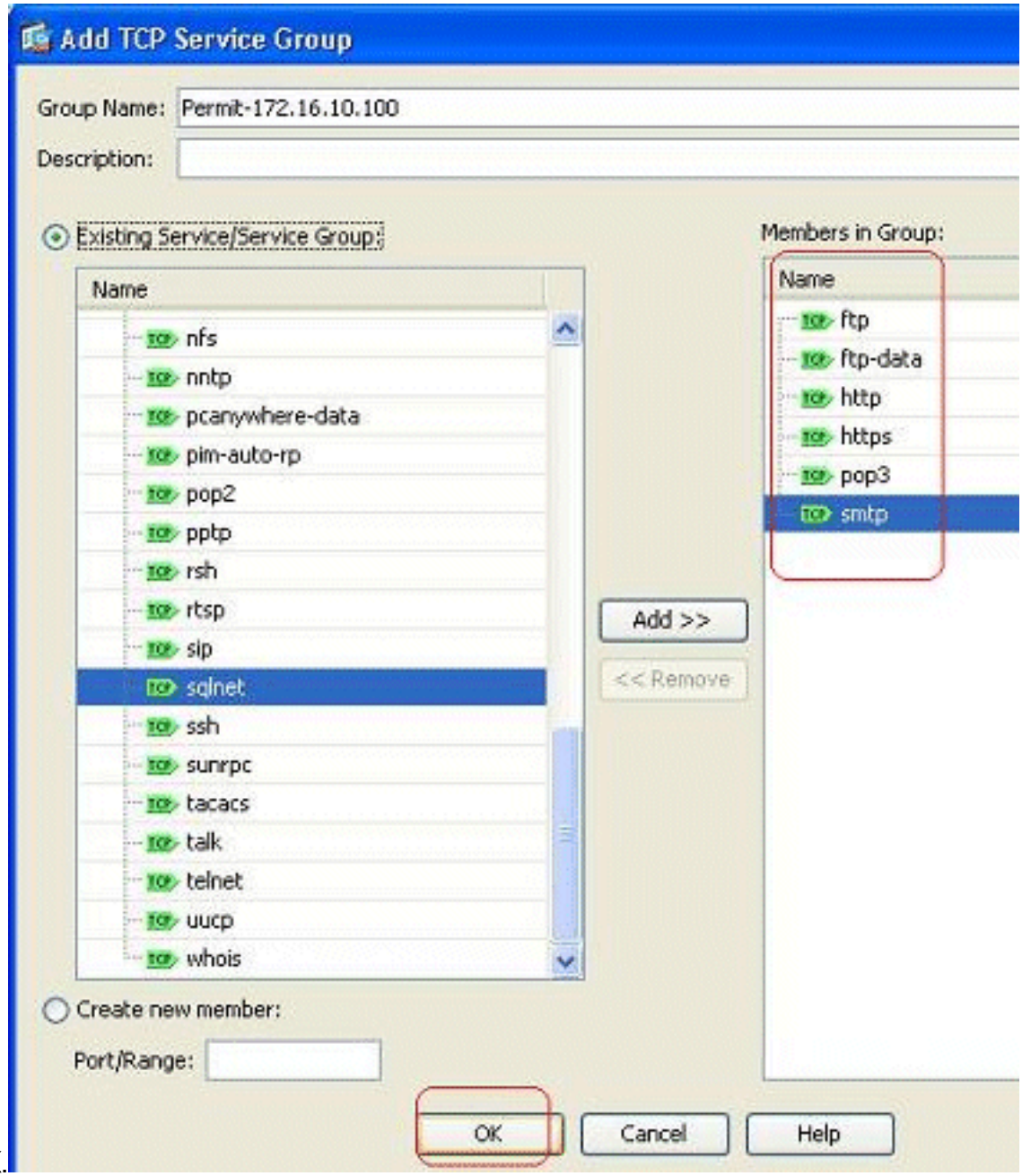
Group.

4. Immettere un nome per il gruppo. Scegliere ciascuna delle porte richieste e fare clic su **Aggiungi** per spostarle nel campo Membri nel



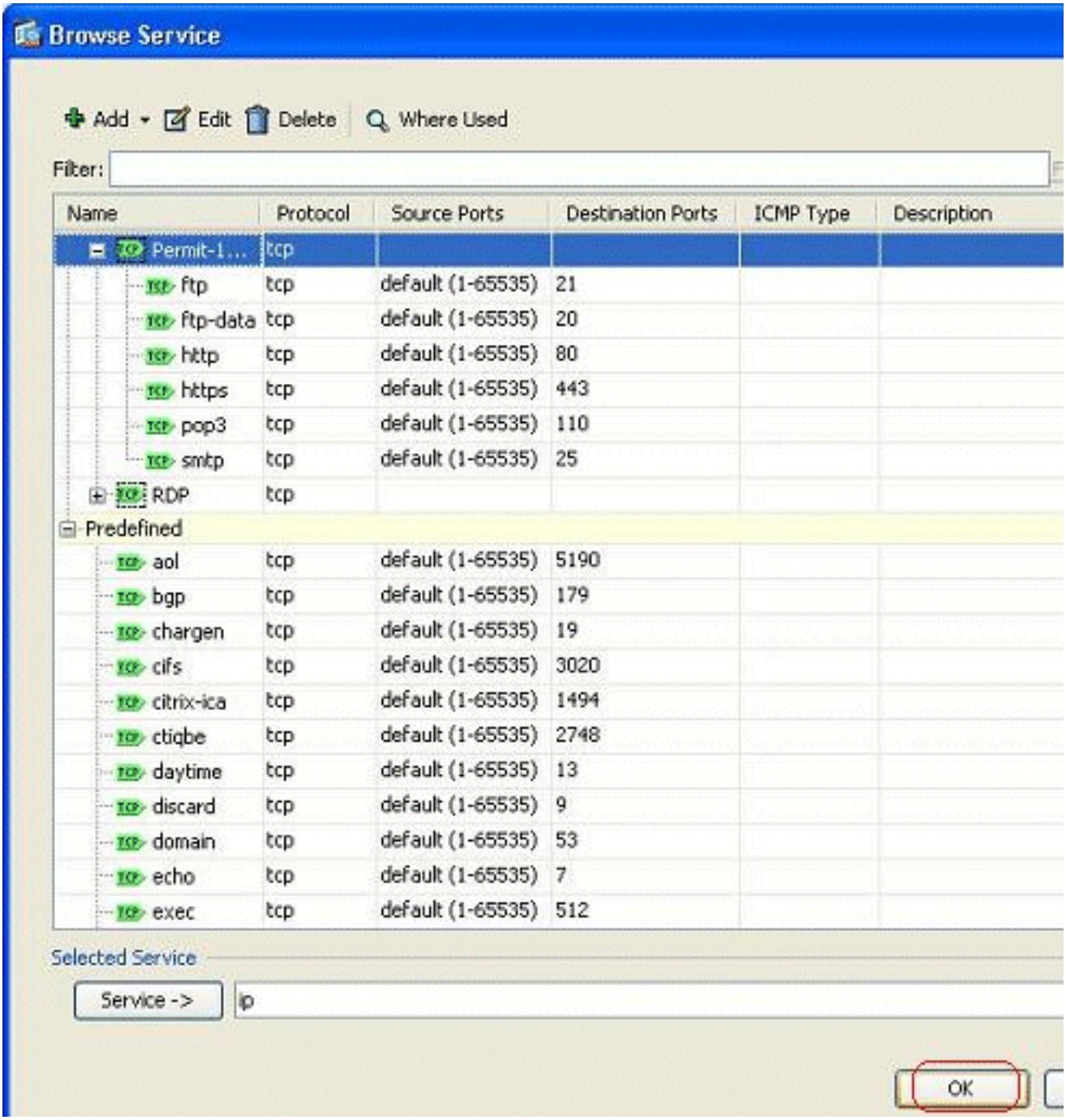
gruppo.

5. Tutte le porte selezionate dovrebbero essere visualizzate nel campo a destra. Per completare il processo di selezione delle porte di accesso, fare clic su



OK.

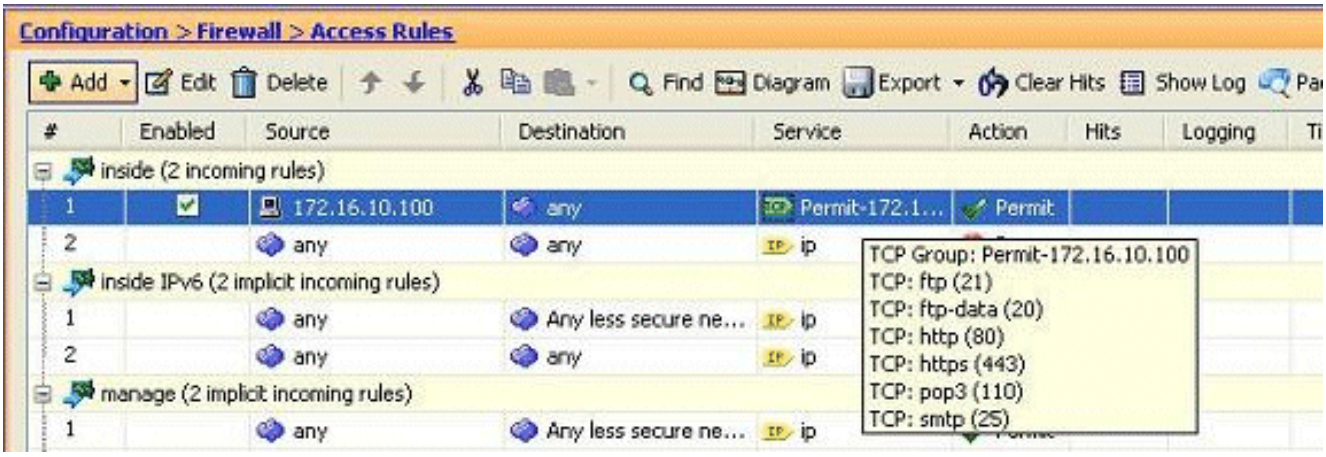
6. Èpossibile visualizzare qui il gruppo di servizi TCP configurato. Fare clic su **OK**.



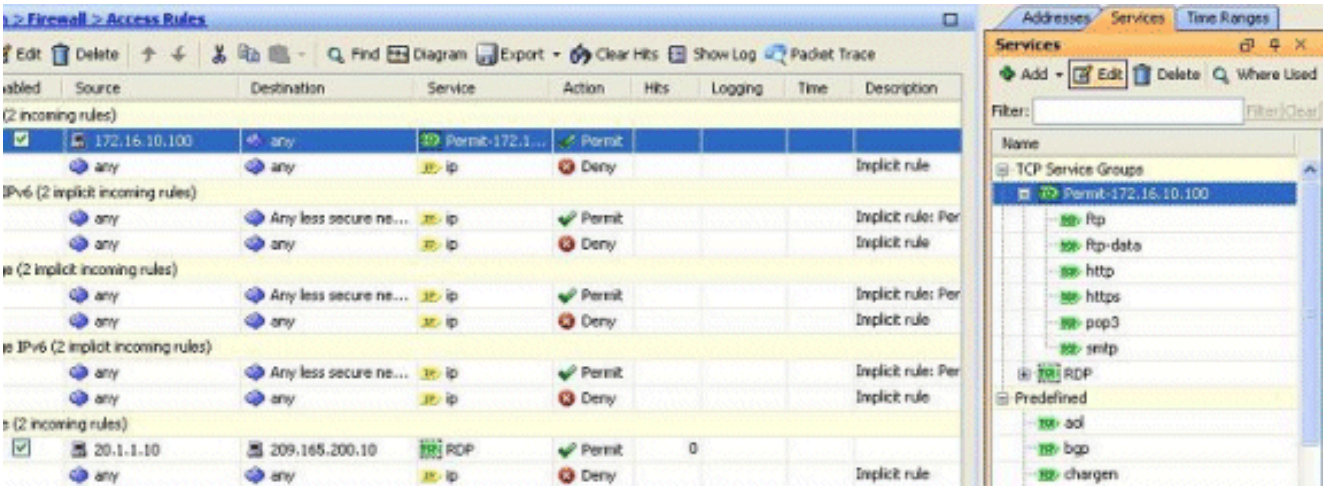
7. Per completare la configurazione, fare clic su

OK.

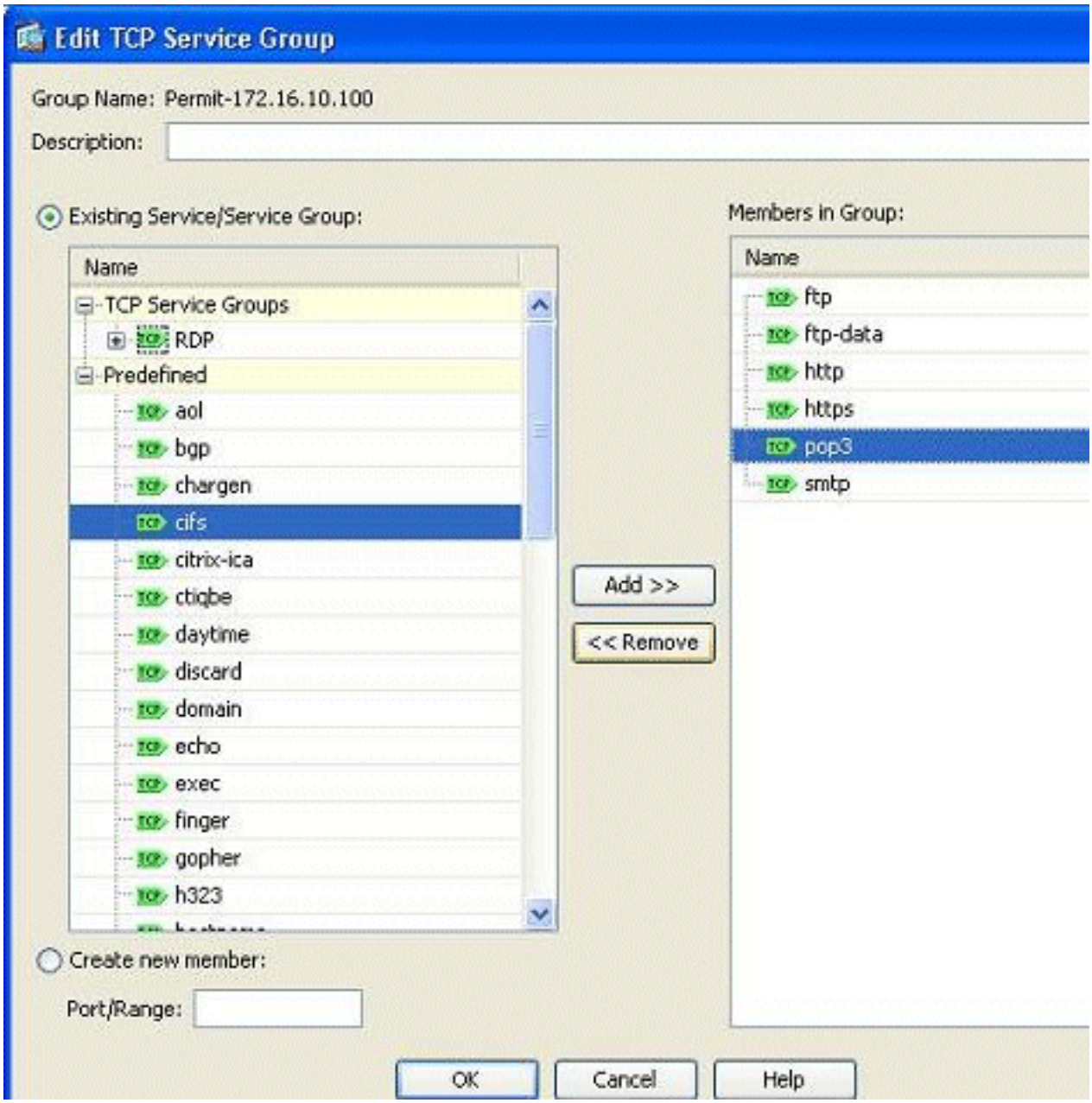
8. La regola di accesso configurata può essere visualizzata nell'interfaccia **interna** nel riquadro Configurazione > Firewall > Regole di accesso.



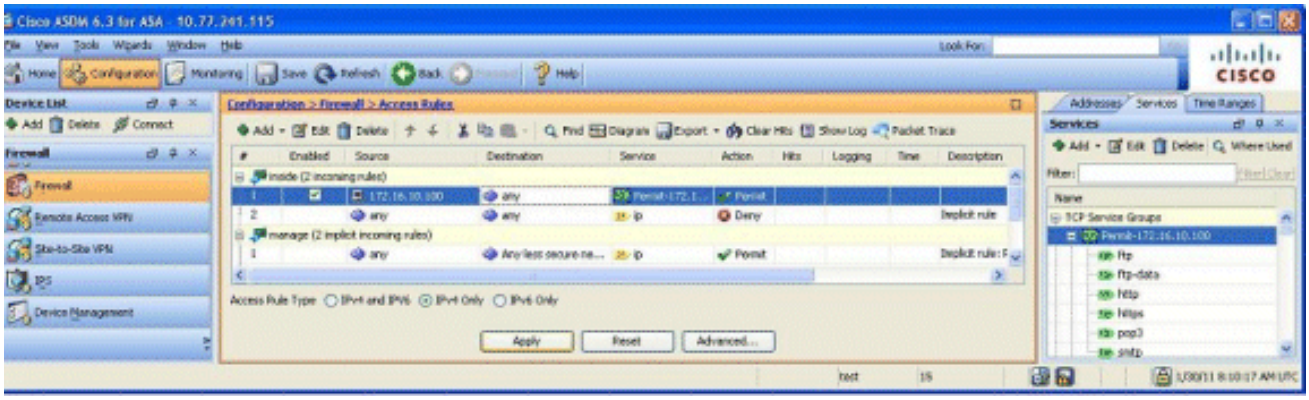
9. Per semplicità di utilizzo, è possibile modificare il gruppo di servizi TCP direttamente nel riquadro di destra della scheda **Servizi**. Per modificare direttamente questo gruppo di servizi, fare clic su **Modifica**.



10. Viene nuovamente reindirizzato alla finestra Modifica gruppo di servizi TCP. Apportare le modifiche desiderate e fare clic su **OK** per salvarle.



11. Di seguito è riportata una vista completa di ASDM:



Questa è la configurazione CLI equivalente:

```
object-group service Permit-172.16.10.100 TCP
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

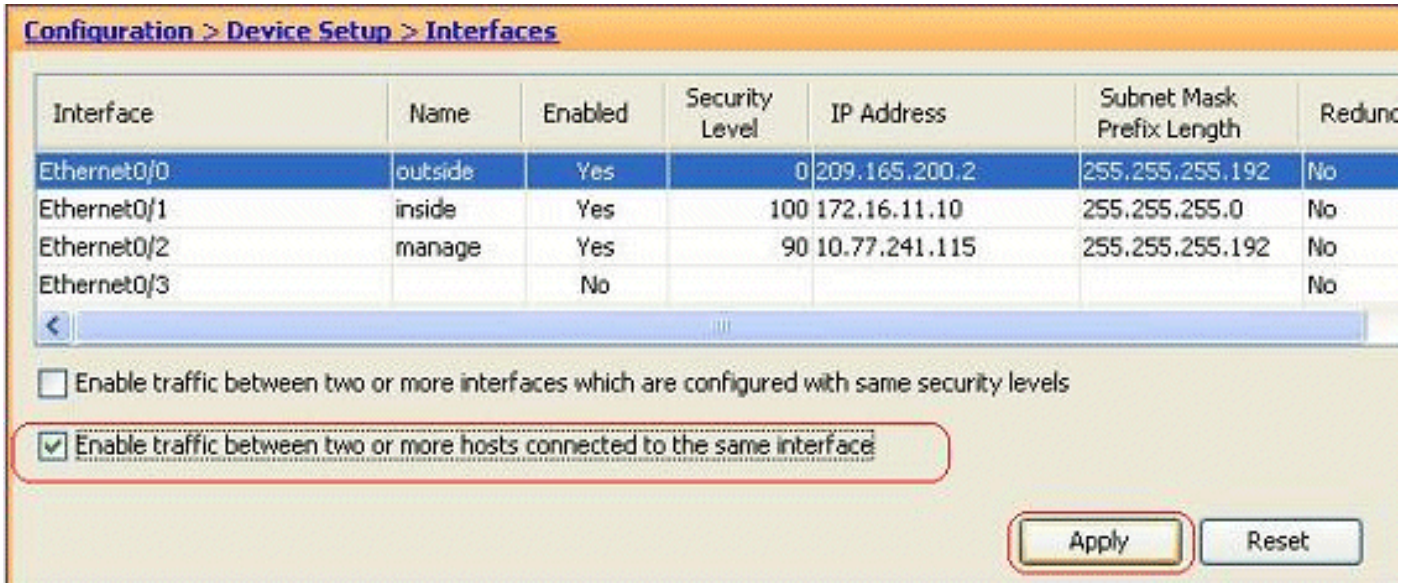
Per informazioni complete sull'implementazione del controllo di accesso, consultare il documento sull'aggiunta o la modifica di un elenco degli accessi dall'interfaccia utente di ASDM.

Consenti traffico tra interfacce con lo stesso livello di sicurezza

In questa sezione viene descritto come abilitare il traffico all'interno di interfacce con gli stessi livelli di sicurezza.

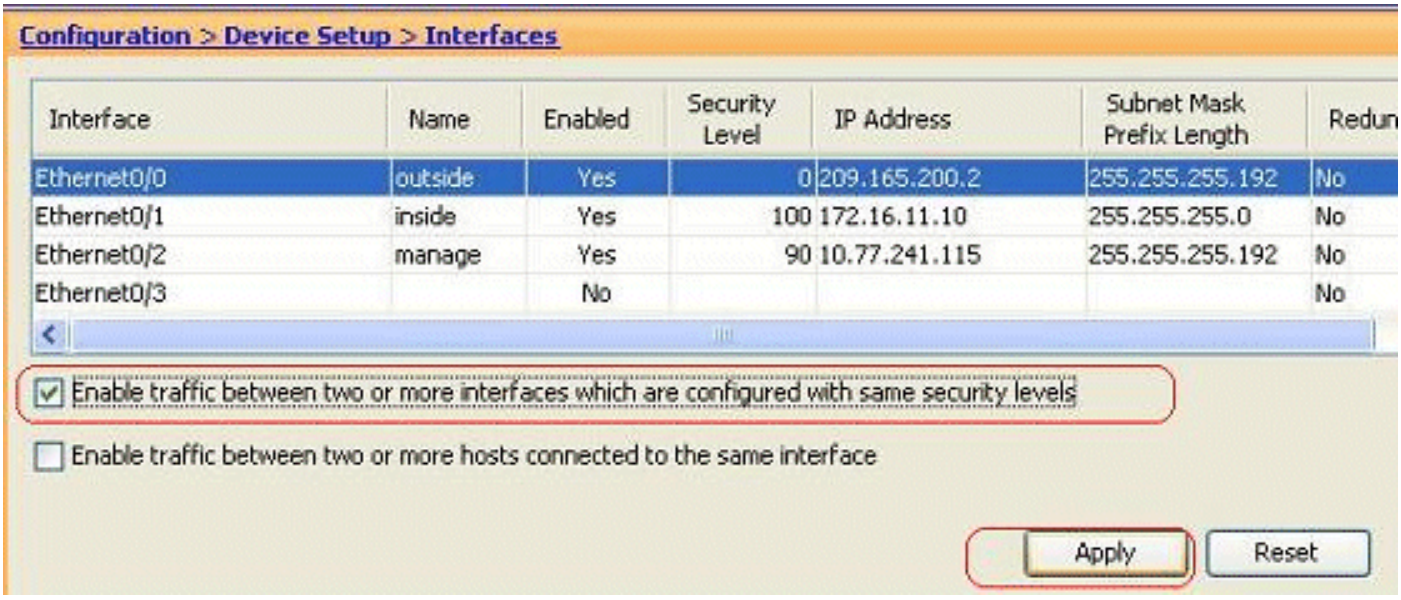
Queste istruzioni descrivono come abilitare la comunicazione intra-interfaccia.

Ciò sarà utile per il traffico VPN che entra in un'interfaccia, ma che viene quindi indirizzato alla stessa interfaccia. In questo caso, il traffico VPN potrebbe non essere crittografato o potrebbe essere crittografato nuovamente per un'altra connessione VPN. Selezionare **Configuration > Device Setup > Interfaces**, quindi selezionare l'opzione **Enable traffic between two or more hosts connected to the same interface** (Abilita traffico tra due o più host connessi alla stessa interfaccia).



Queste istruzioni descrivono come abilitare la comunicazione tra interfacce.

Questa opzione permette la comunicazione tra interfacce con pari livelli di sicurezza. Selezionare **Configuration > Device Setup > Interfaces**, quindi selezionare l'opzione **Enable traffic between two or more interfaces that are configure with same security level** (Abilita traffico tra due o più interfacce configurate con gli stessi livelli di sicurezza).



Questa è la CLI equivalente per entrambe le impostazioni:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

Consenti agli host non attendibili l'accesso agli host della rete attendibile

A tale scopo, è possibile applicare una traduzione NAT statica e una regola di accesso per consentire tali host. È necessario configurare questa opzione ogni volta che un utente esterno desidera accedere a un server della rete interna. Il server nella rete interna avrà un indirizzo IP privato che non è instradabile su Internet. Di conseguenza, è necessario convertire l'indirizzo IP privato in un indirizzo IP pubblico tramite una regola NAT statica. Si supponga di disporre di un

server interno (172.16.11.5). Per far funzionare questo, è necessario convertire questo IP del server privato in un IP pubblico. Nell'esempio viene descritto come implementare l'NAT statico bidirezionale per convertire da 172.16.11.5 a 209.165.200.5.

In questa sezione non è illustrata la sezione relativa all'autorizzazione all'utente esterno di accedere al server Web implementando una regola di accesso. Di seguito è riportato un breve frammento della CLI per la comprensione dell'utente:

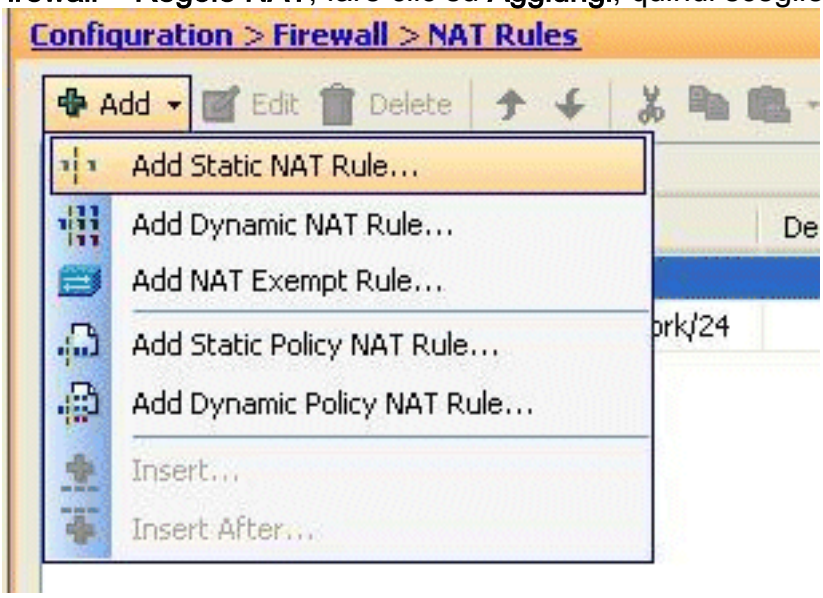
```
access-list 101 permit TCP any host 209.165.200.5
```

Per ulteriori informazioni, consultare il documento sull'aggiunta o la modifica di un elenco degli accessi dall'interfaccia utente di ASDM.

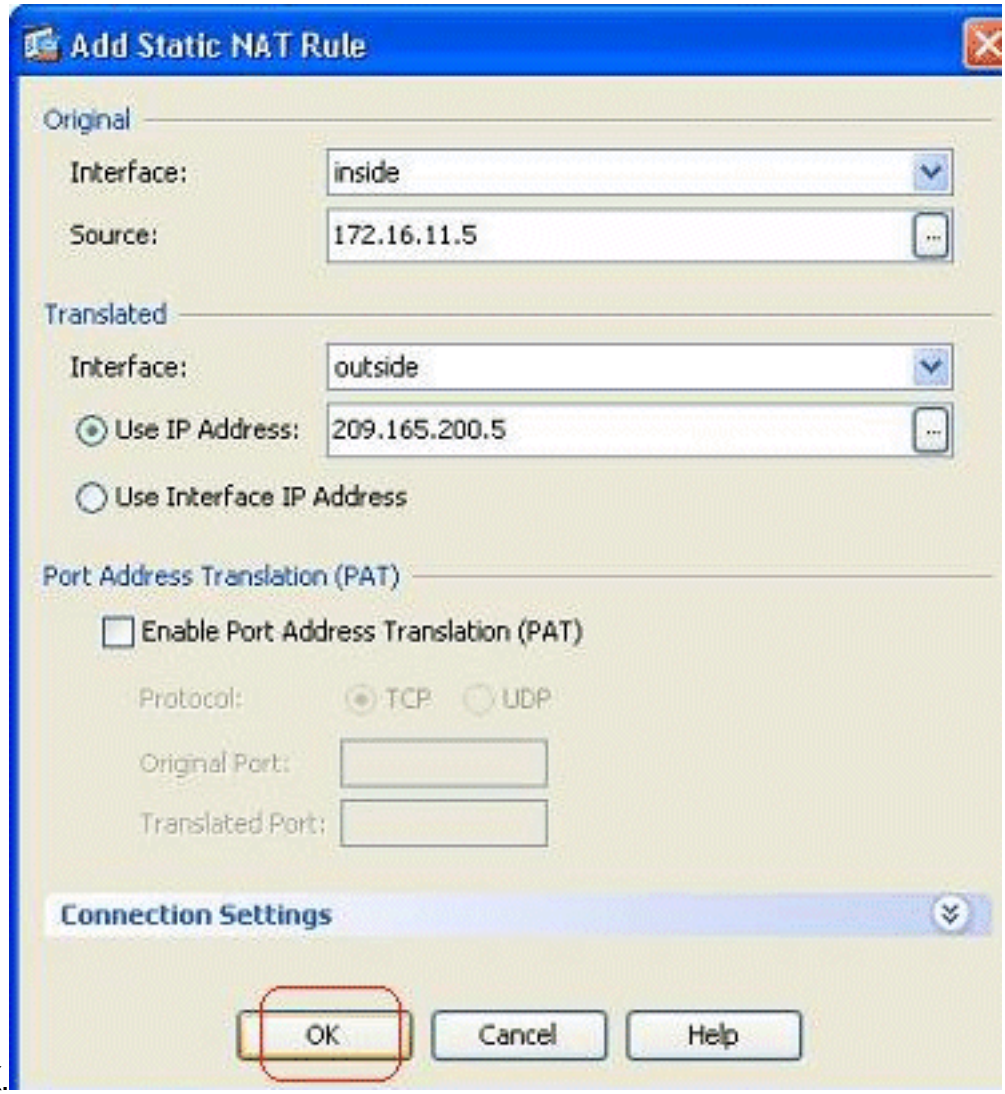
Nota: specificando la parola chiave "any" (qualsiasi), qualsiasi utente del mondo esterno può accedere a questo server. Inoltre, se non viene specificato per nessuna porta di servizio, è possibile accedere al server da qualsiasi porta di servizio mentre queste rimangono aperte. Prestare attenzione quando si implementa e si consiglia di limitare l'autorizzazione al singolo utente esterno e anche alla porta richiesta sul server.

Completare questa procedura per configurare il NAT statico:

1. Andare a Configurazione > **Firewall** > **Regole NAT**, fare clic su **Aggiungi**, quindi scegliere **Aggiungi regola NAT statica**.

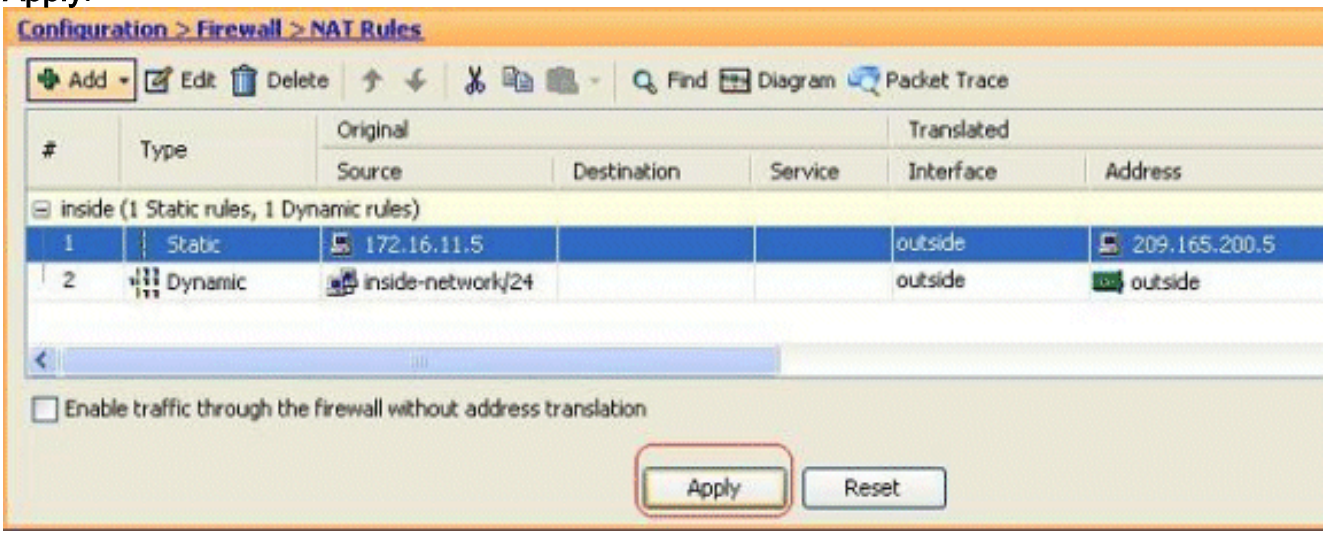


2. Specificare l'indirizzo IP originale e l'indirizzo IP tradotto insieme alle interfacce associate,



quindi fare clic su **OK**.

3. Qui è possibile vedere la voce NAT statica configurata. Per inviare il messaggio all'appliance ASA, fare clic su **Apply**.



Questo è un breve esempio di CLI per questa configurazione ASDM:

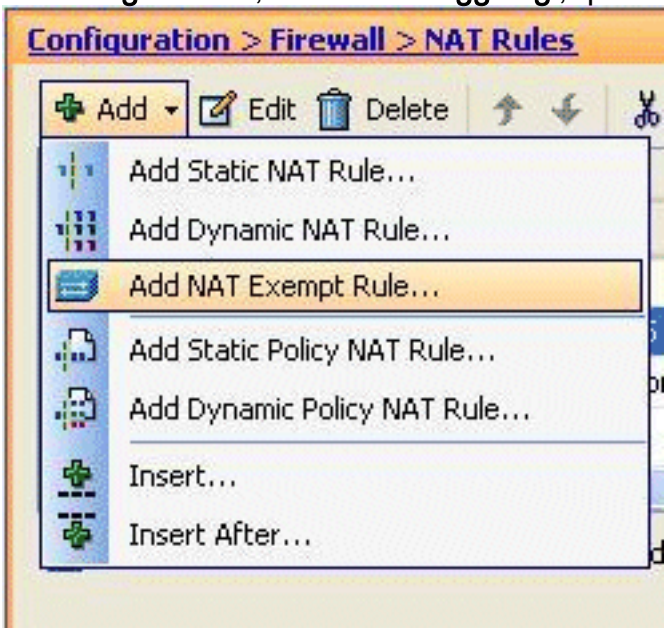
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

Disabilita NAT per host/reti specifiche

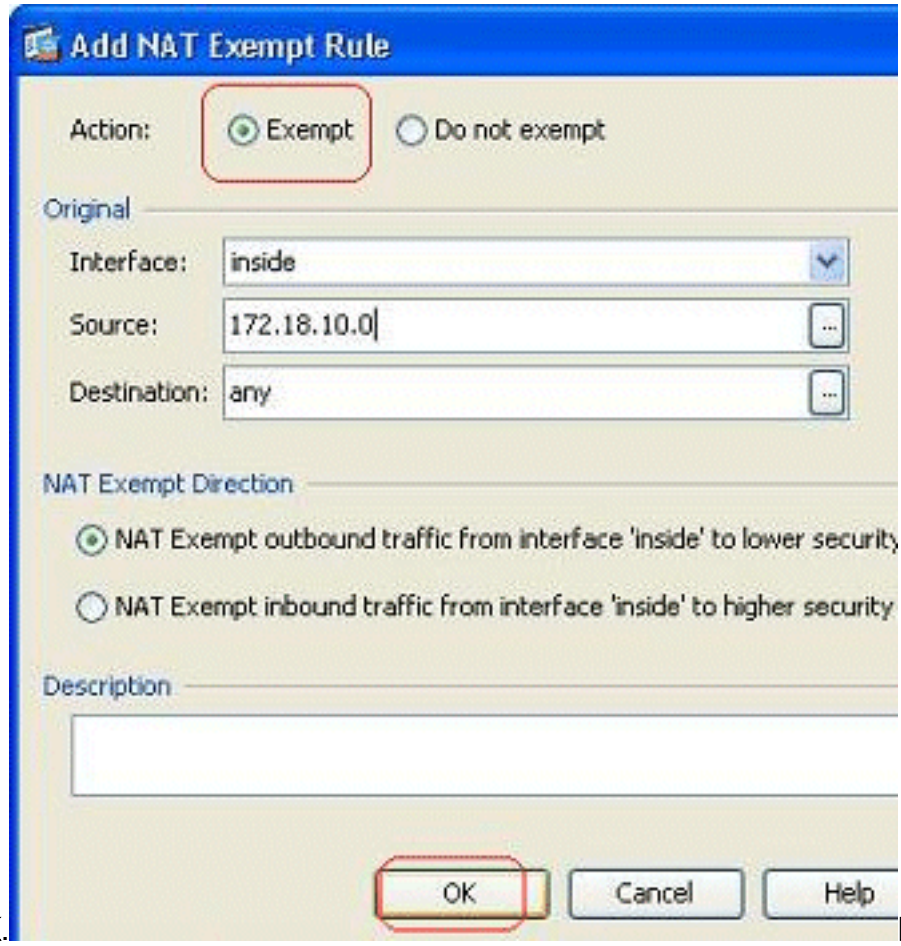
Per esentare host o reti specifici da NAT, aggiungere una regola di esenzione NAT per disabilitare la conversione degli indirizzi. Ciò consente agli host tradotti e remoti di avviare le connessioni.

Attenersi alla seguente procedura:

1. Andare a Configurazione > **Firewall** > **Regole NAT**, fare clic su **Aggiungi**, quindi scegliere **Aggiungi regola esenzione NAT**.

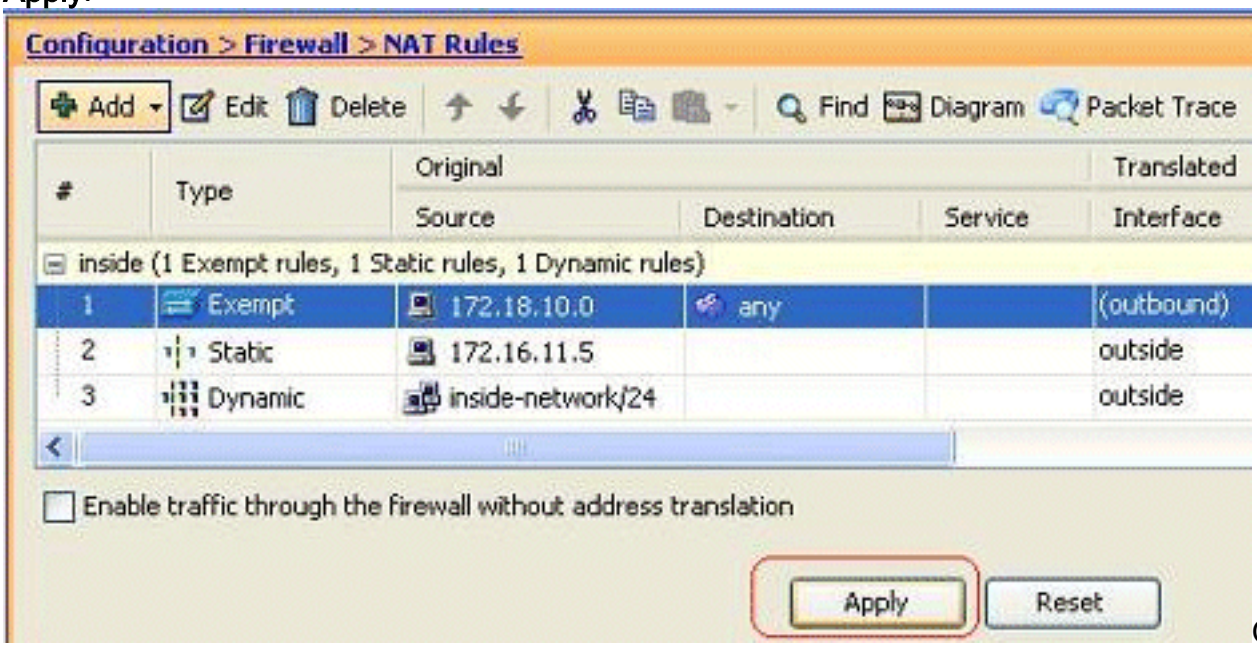


2. Qui, la rete interna 172.18.10.0 è stata esentata dalla traduzione dell'indirizzo. Assicurarsi che l'opzione **Esente** sia stata selezionata. La direzione di esenzione NAT prevede due opzioni:Traffico in uscita verso interfacce di sicurezza inferioriTraffico in entrata verso interfacce di sicurezza più elevateL'opzione predefinita è per il traffico in uscita. Per completare il passo, fare clic su



OK.**Nota:** quando si sceglie l'opzione **Non esentare**, l'host specificato non sarà esentato da NAT e verrà aggiunta una regola di accesso separata con la parola chiave "nega". Ciò è utile per evitare host specifici esenti da NAT in quanto la subnet completa, esclusi questi host, sarà esente da NAT.

3. Èpossibile vedere la regola di esenzione NAT per la direzione in uscita qui. Per inviare la configurazione all'appliance ASA, fare clic su **Apply**.

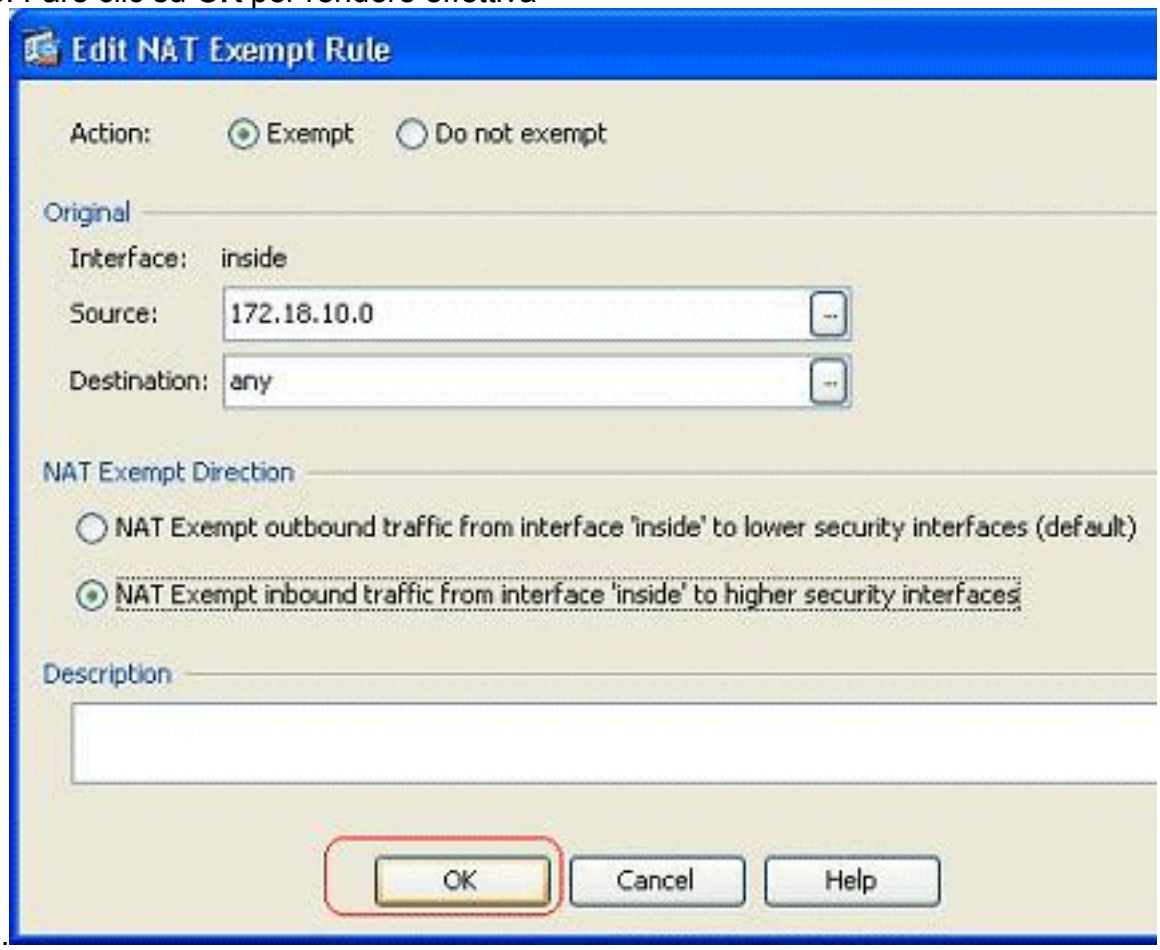


Que sto è l'output CLI equivalente per il riferimento:

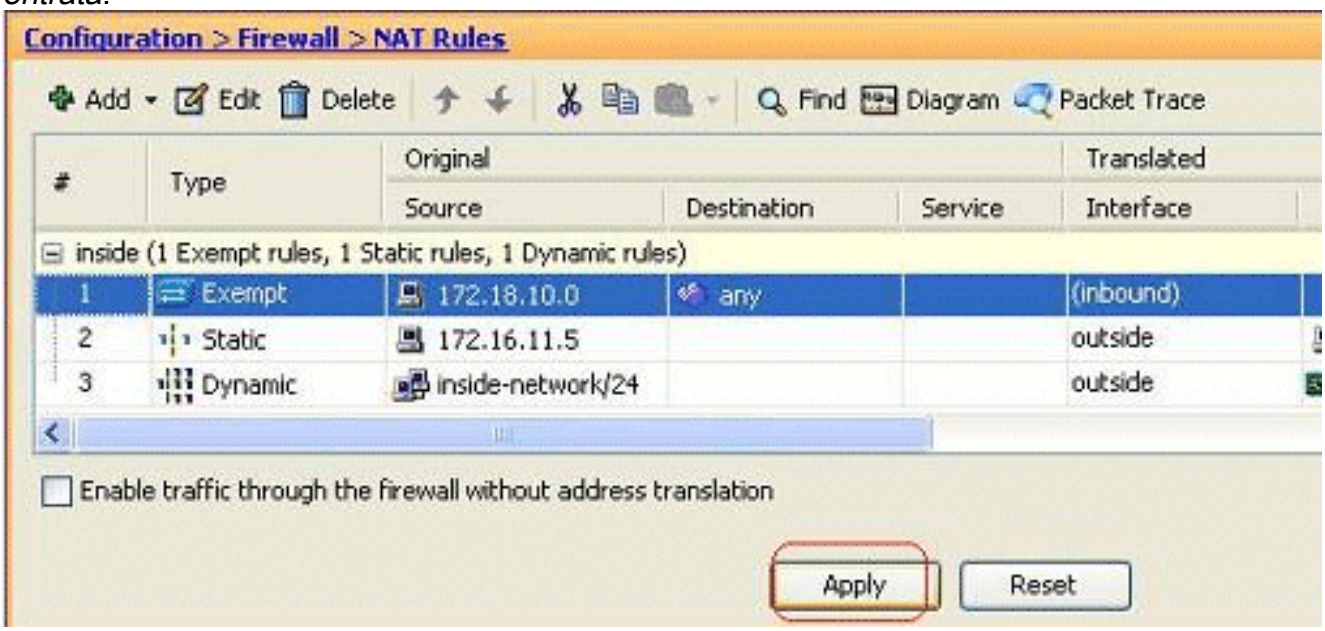
```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. In questa sezione viene illustrato come modificare la regola di esenzione NAT per la relativa

direzione. Fare clic su **OK** per rendere effettiva l'opzione.



5. Ora potete vedere che la direzione è stata cambiata in *entrata*.



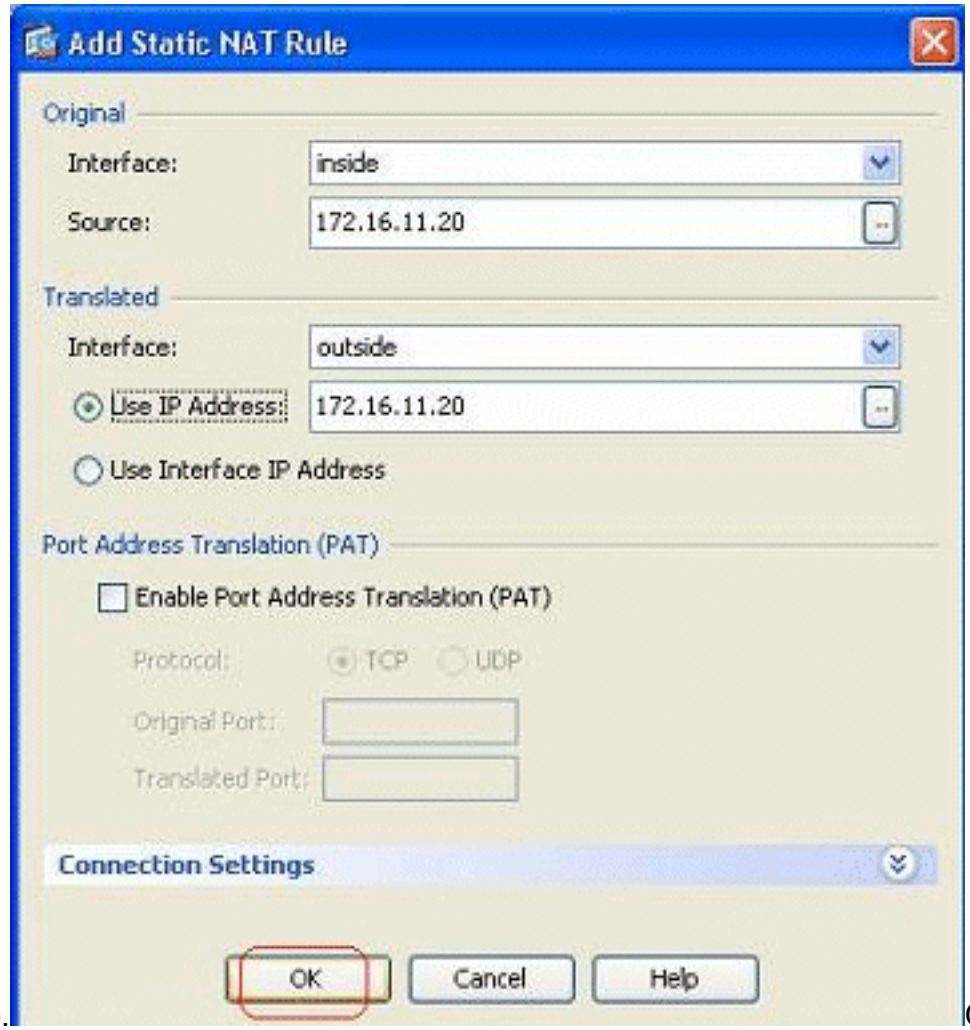
Per inviare l'output CLI all'appliance ASA, fare clic su **Apply**:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

Nota: da questo si può vedere che una nuova parola chiave (esterna) è stata aggiunta alla fine del comando **nat 0**. Questa funzionalità è denominata **NAT esterno**.

6. Un altro modo per disabilitare NAT è tramite l'implementazione di Identity NAT. Identity NAT converte un host nello stesso indirizzo IP. Di seguito è riportato un esempio di NAT con

identità statica regolare, in cui l'host (172.16.11.20) viene convertito nello stesso indirizzo IP quando vi si accede



dall'esterno. Questo è l'output CLI equivalente:

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

Reindirizzamento porte (inoltro) con statistiche

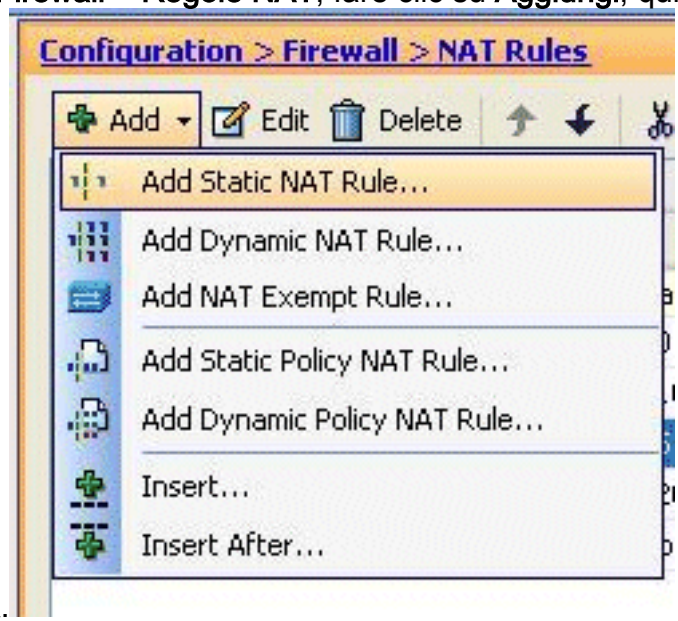
L'inoltro o il reindirizzamento delle porte è una funzionalità utile quando gli utenti esterni tentano di accedere a un server interno su una porta specifica. A tale scopo, il server interno, che dispone di un indirizzo IP privato, verrà convertito in un indirizzo IP pubblico che a sua volta potrà accedere alla porta specifica.

In questo esempio, l'utente esterno desidera accedere al server SMTP, 209.165.200.15 sulla porta 25. A tale scopo, è necessario eseguire due passaggi:

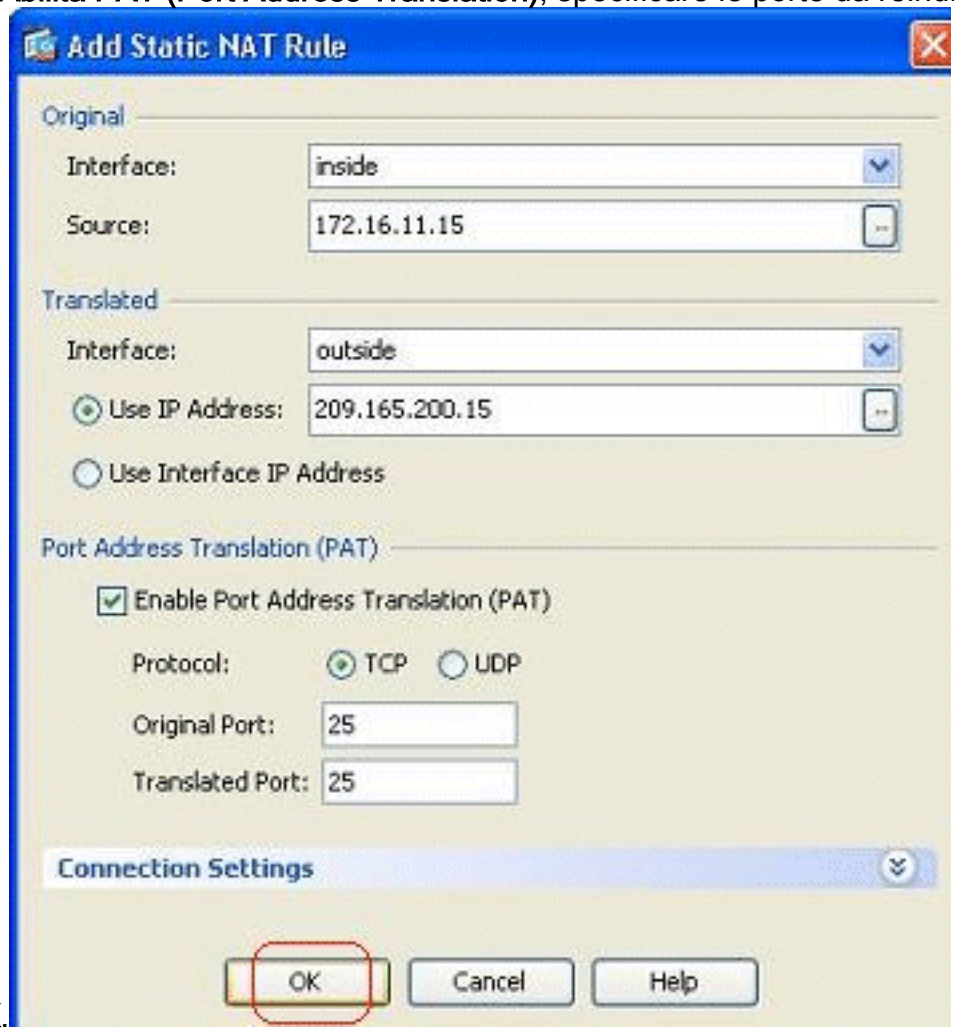
1. Tradurre il server di posta interno, 172.16.11.15 sulla porta 25, nell'indirizzo IP pubblico, 209.165.200.15 sulla porta 25.
2. Consentire l'accesso al server di posta pubblica, 209.165.200.15 sulla porta 25.

Quando l'utente esterno tenta di accedere al server, 209.165.200.15 alla porta 25, il traffico verrà reindirizzato al server di posta interno, 172.16.11.15 alla porta 25.

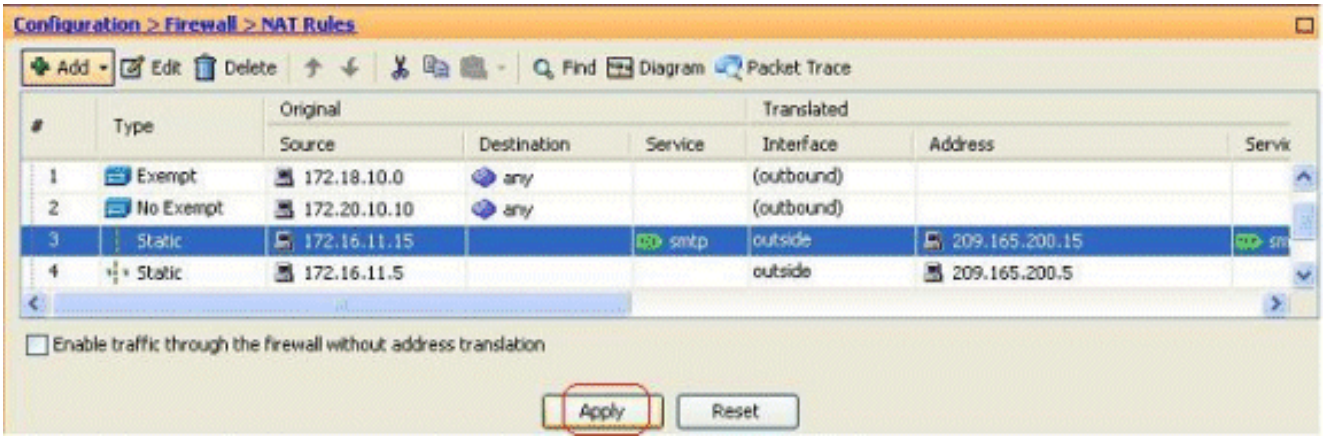
1. Andare a Configurazione **> Firewall > Regole NAT**, fare clic su **Aggiungi**, quindi scegliere **Aggiungi regola NAT statica**.



2. Specificare l'origine originale e l'indirizzo IP tradotto insieme alle relative interfacce associate. Scegliere **Abilita PAT (Port Address Translation)**, specificare le porte da reindirizzare e fare clic su **OK**.



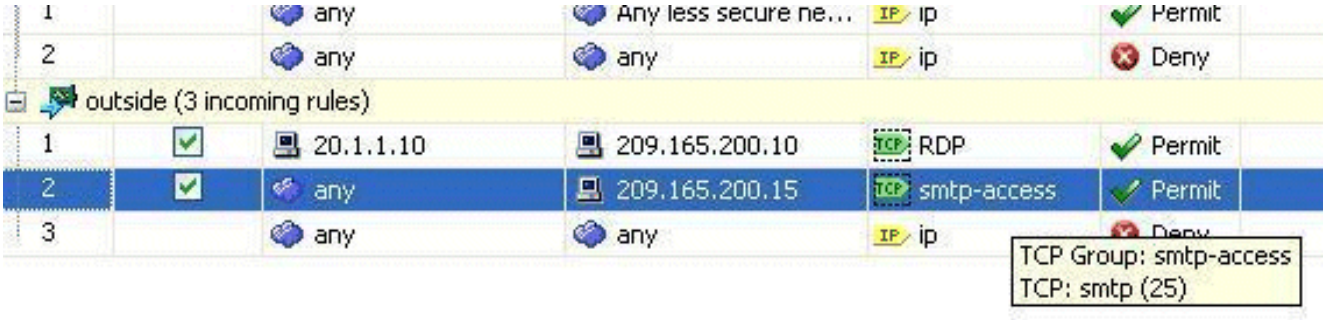
3. La regola PAT statica configurata è visualizzata di seguito:



Questo è l'output CLI equivalente:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. Questa è la regola di accesso che consente all'utente esterno di accedere al server smtp pubblico al numero 209.165.200.15:



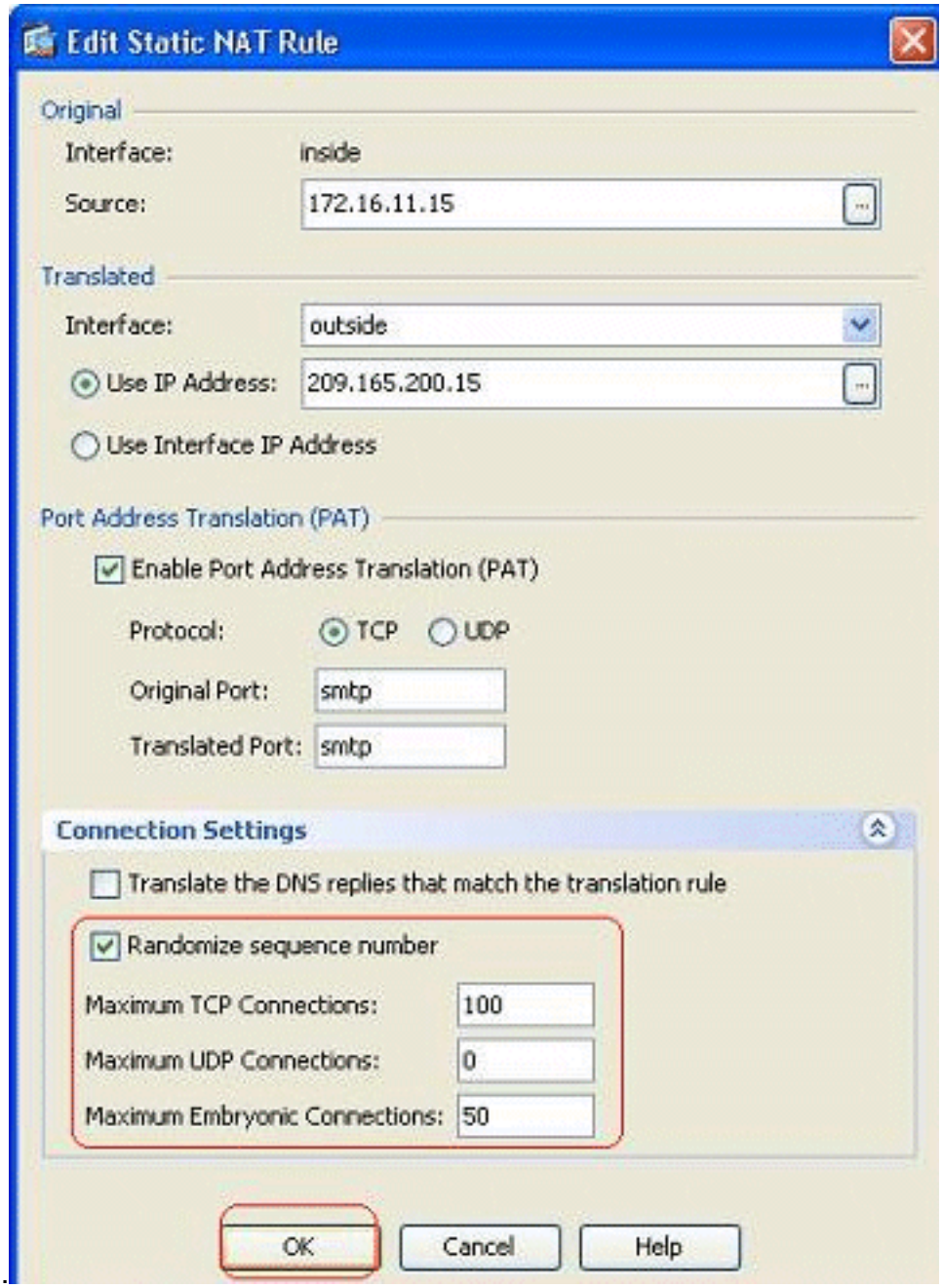
Nota: assicurarsi di utilizzare host specifici anziché la parola chiave **any** nell'origine della regola di accesso.

Limita sessione TCP/UDP tramite statico

Èpossibile specificare il numero massimo di connessioni TCP/UDP utilizzando la regola statica. Potete anche specificare il numero massimo di connessioni embrionali. Una connessione embrionale è una connessione che è uno stato mezzo aperto. Un numero maggiore di questi problemi influirà sulle prestazioni dell'appliance ASA. Limitando queste connessioni si eviteranno certi attacchi come DoS e SYN in una certa misura. Per una mitigazione completa, è necessario definire il criterio nel framework MPF, che esula dall'ambito di questo documento. Per ulteriori informazioni su questo argomento, consultare il documento sulla mitigazione degli attacchi di rete.

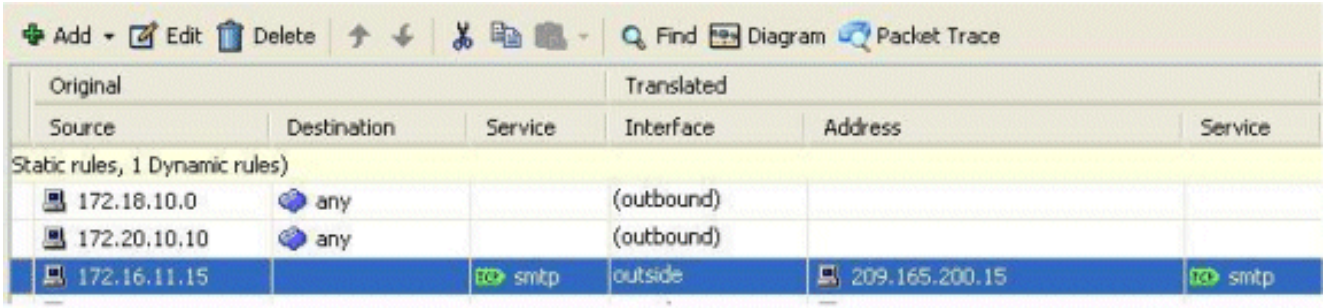
Attenersi alla seguente procedura:

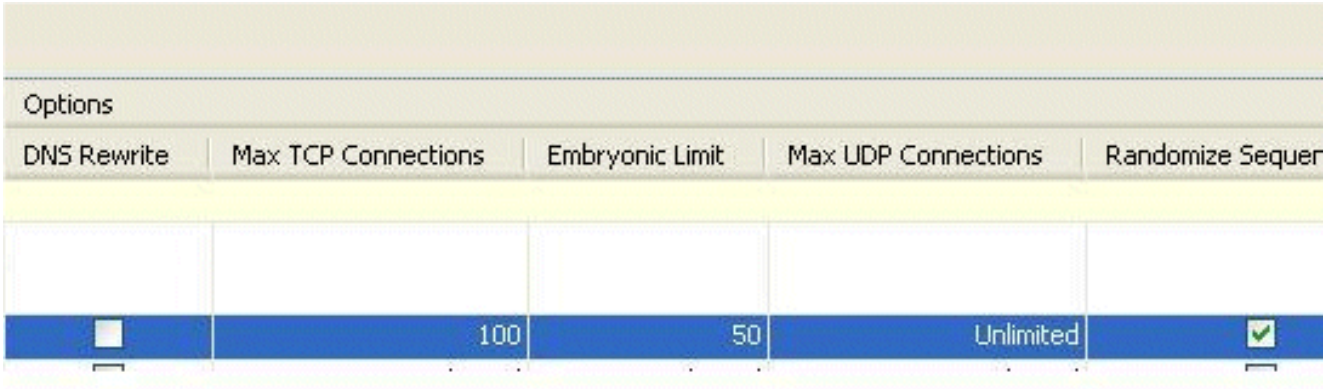
1. Fare clic sulla scheda **Impostazioni di connessione** e specificare i valori per il numero massimo di connessioni per la traduzione



statica.

2. Le immagini seguenti mostrano i limiti di connessione per questa specifica traduzione statica:





Questo è l'output CLI equivalente:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

Lista accessi temporizzati

In questa sezione viene illustrata l'implementazione di elenchi degli accessi a tempo con ASDM. Le regole di accesso possono essere applicate in base al tempo. Per implementare questa funzionalità, è necessario definire un intervallo di tempo che specifichi gli intervalli in base al giorno/settimana/mese/anno. Quindi, è necessario associare questo intervallo di tempo alla regola di accesso richiesta. L'intervallo di tempo può essere definito in due modi:

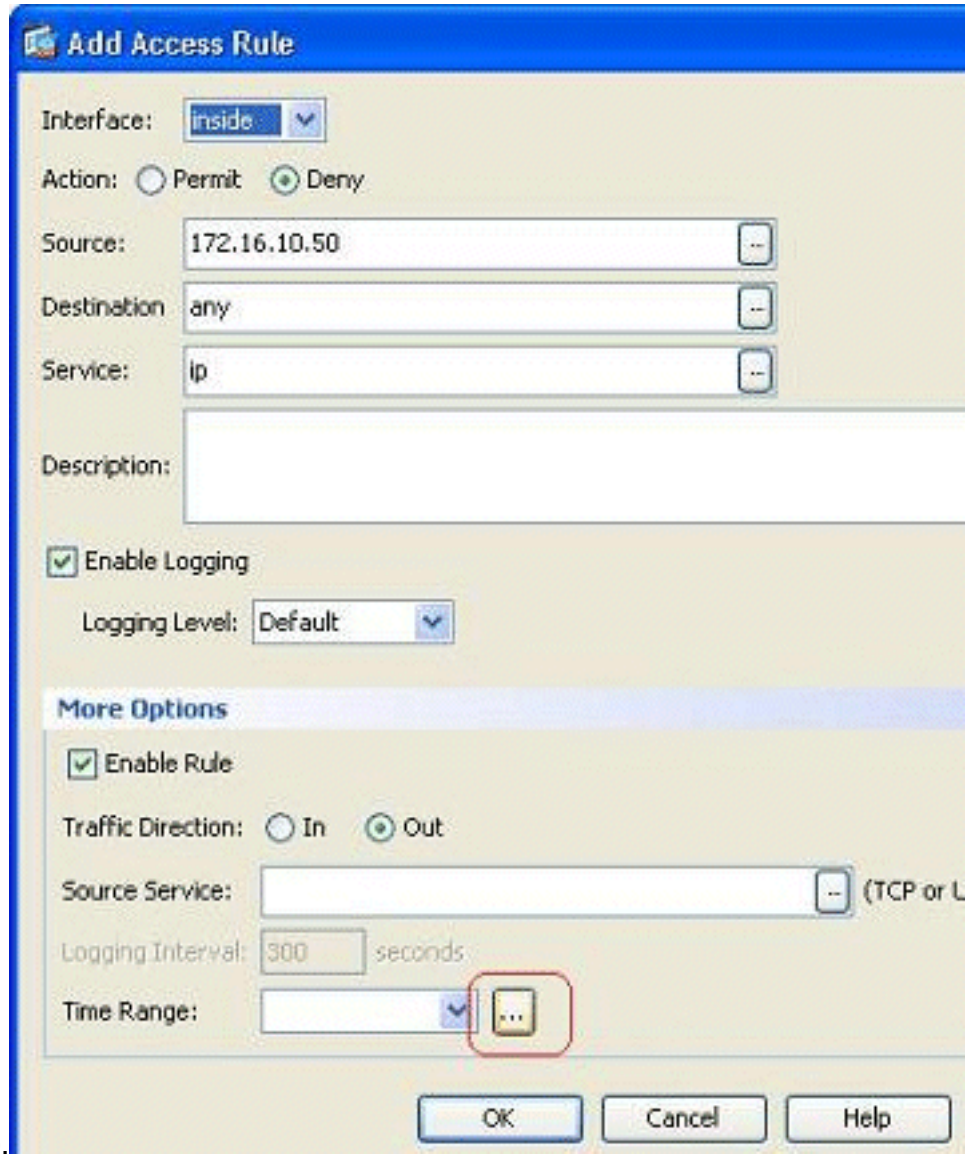
1. Assoluto: definisce un periodo di tempo con ora di inizio e ora di fine.
2. Periodico - Denominato anche ricorrente. Definisce un periodo di tempo che si verifica a intervalli specificati.

Nota: prima di configurare l'intervallo di tempo, verificare che l'ASA sia stata configurata con le impostazioni di data e ora corrette, in quanto questa funzione utilizza le impostazioni dell'orologio di sistema per implementare. La sincronizzazione dell'ASA con il server NTP darà risultati migliori.

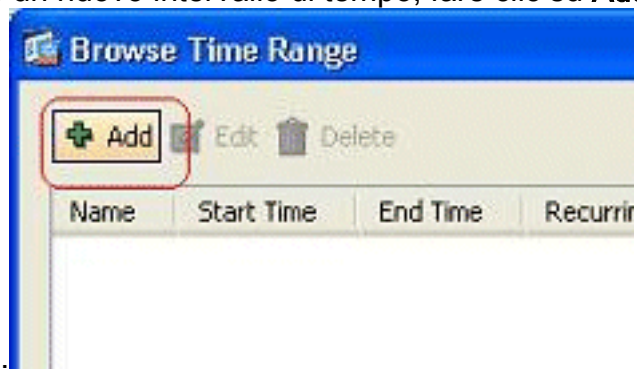
Per configurare questa funzione tramite ASDM, completare la procedura seguente:

1. Durante la definizione della regola di accesso, fare clic sul pulsante **Dettagli** nel campo

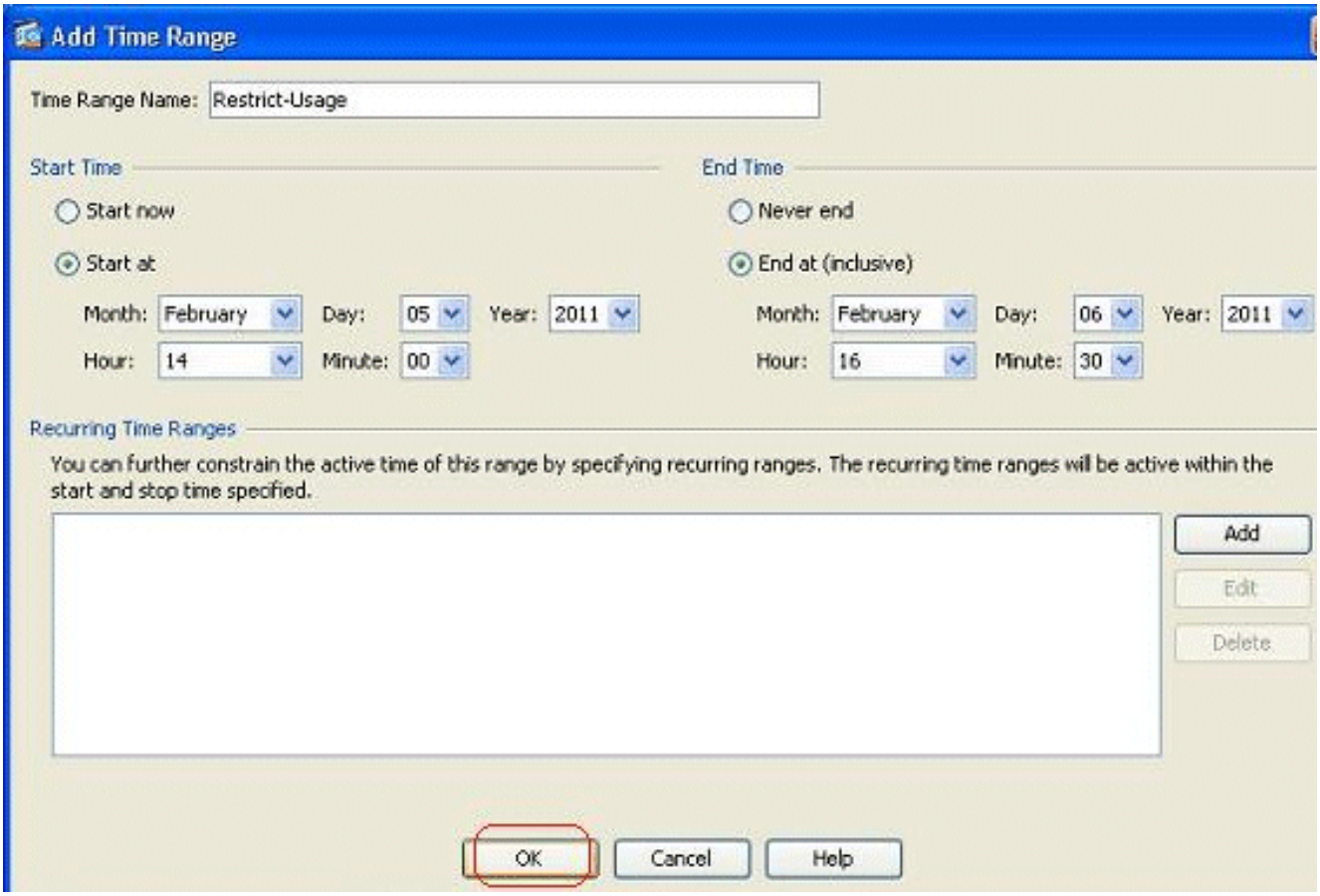
Intervallo di tempo.



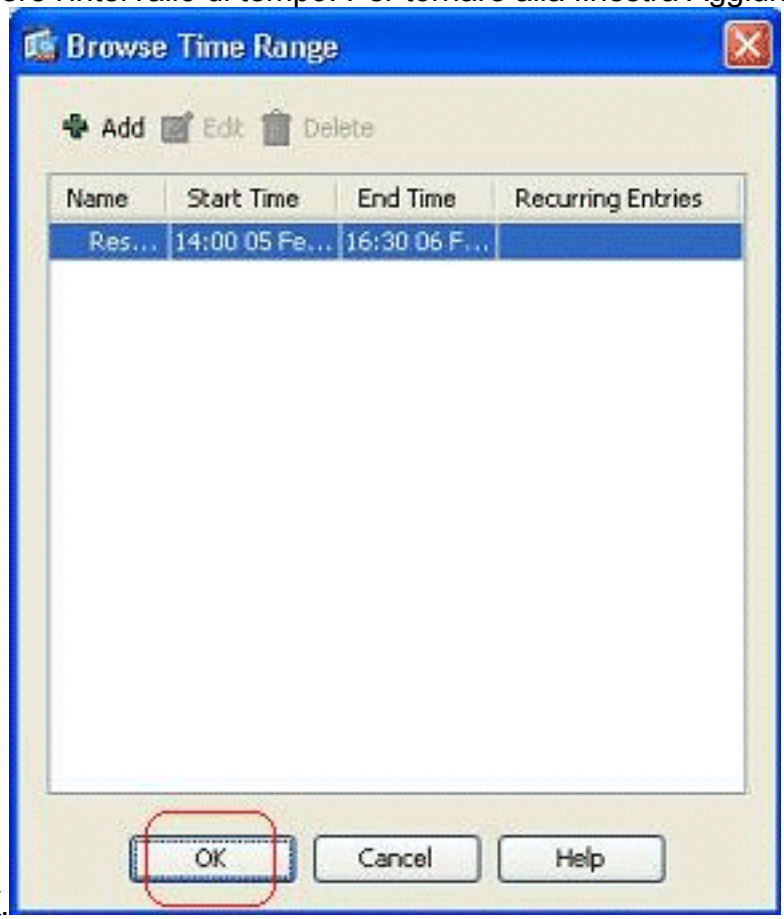
2. Per creare un nuovo intervallo di tempo, fare clic su **Add** (Aggiungi).



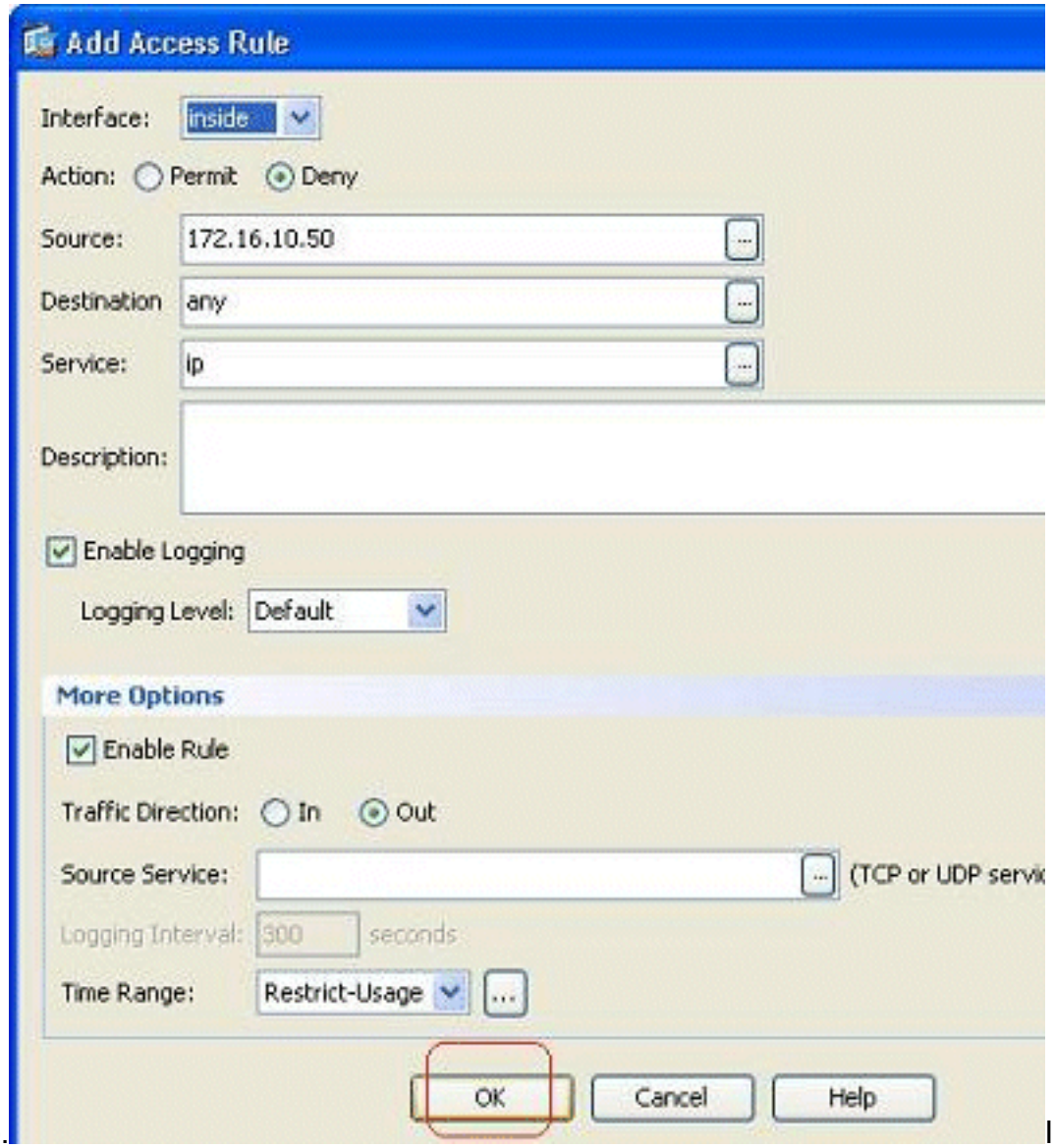
3. Definire il nome dell'intervallo di tempo e specificare l'ora di inizio e di fine. Fare clic su **OK**.



4. Qui potete vedere l'intervallo di tempo. Per tornare alla finestra Aggiungi regola di accesso, fare clic su **OK**.



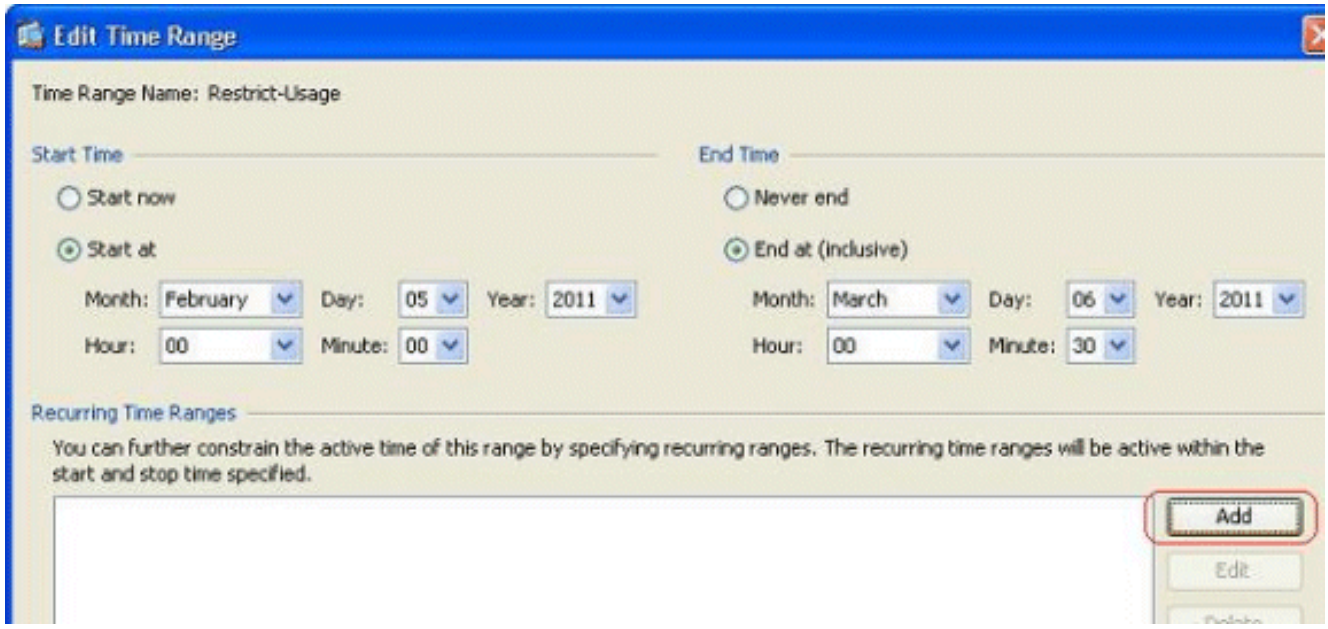
5. Èora possibile verificare che l'intervallo di tempo Restrict-Usage è stato associato a questa regola di



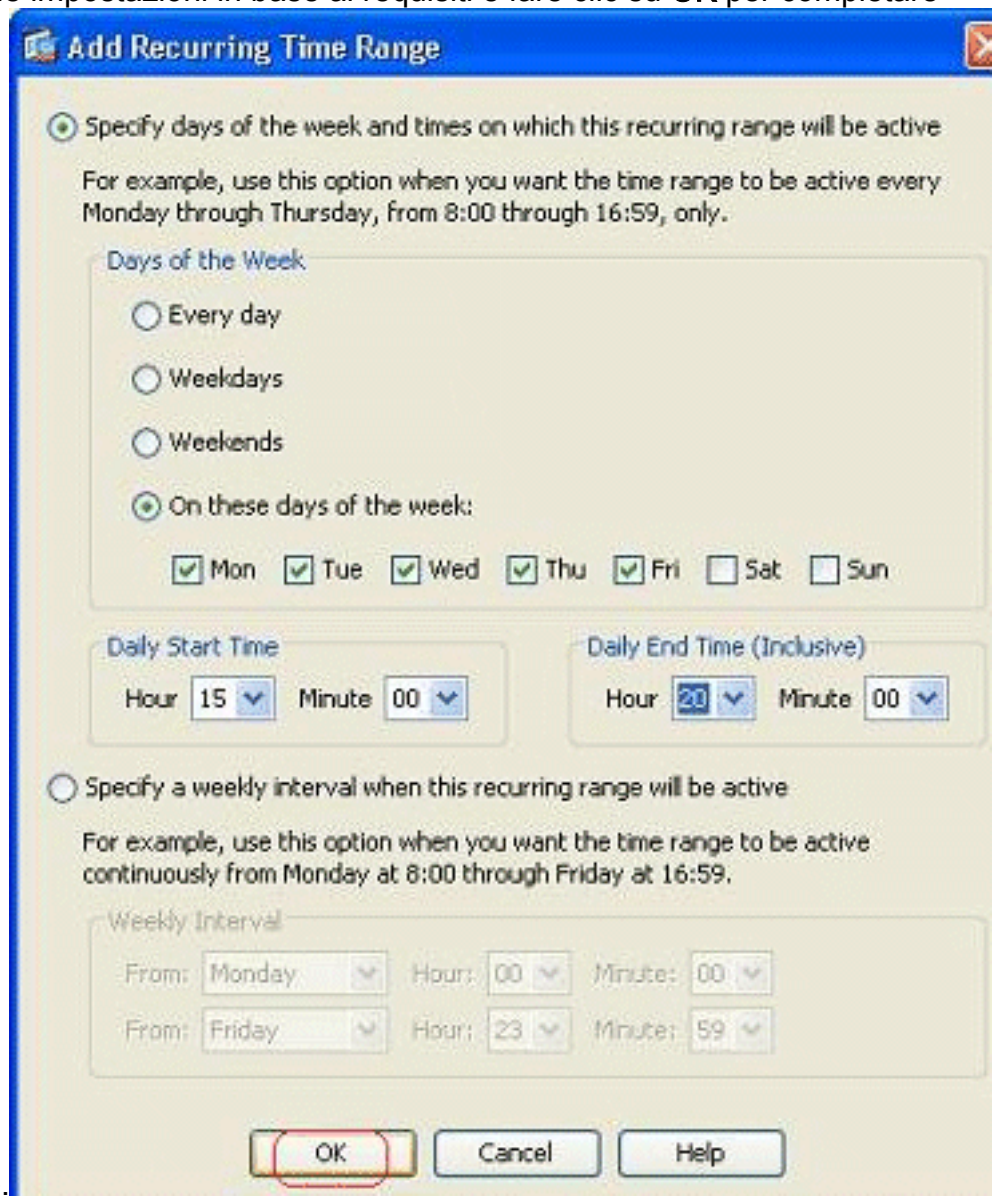
accesso. In base a questa configurazione della regola di accesso, all'utente alla 172.16.10.50 è stato limitato l'utilizzo di risorse dal 05/Feb/2011 2 PM al 06/Feb/2011 4.30 PM. Questo è l'output CLI equivalente:

```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

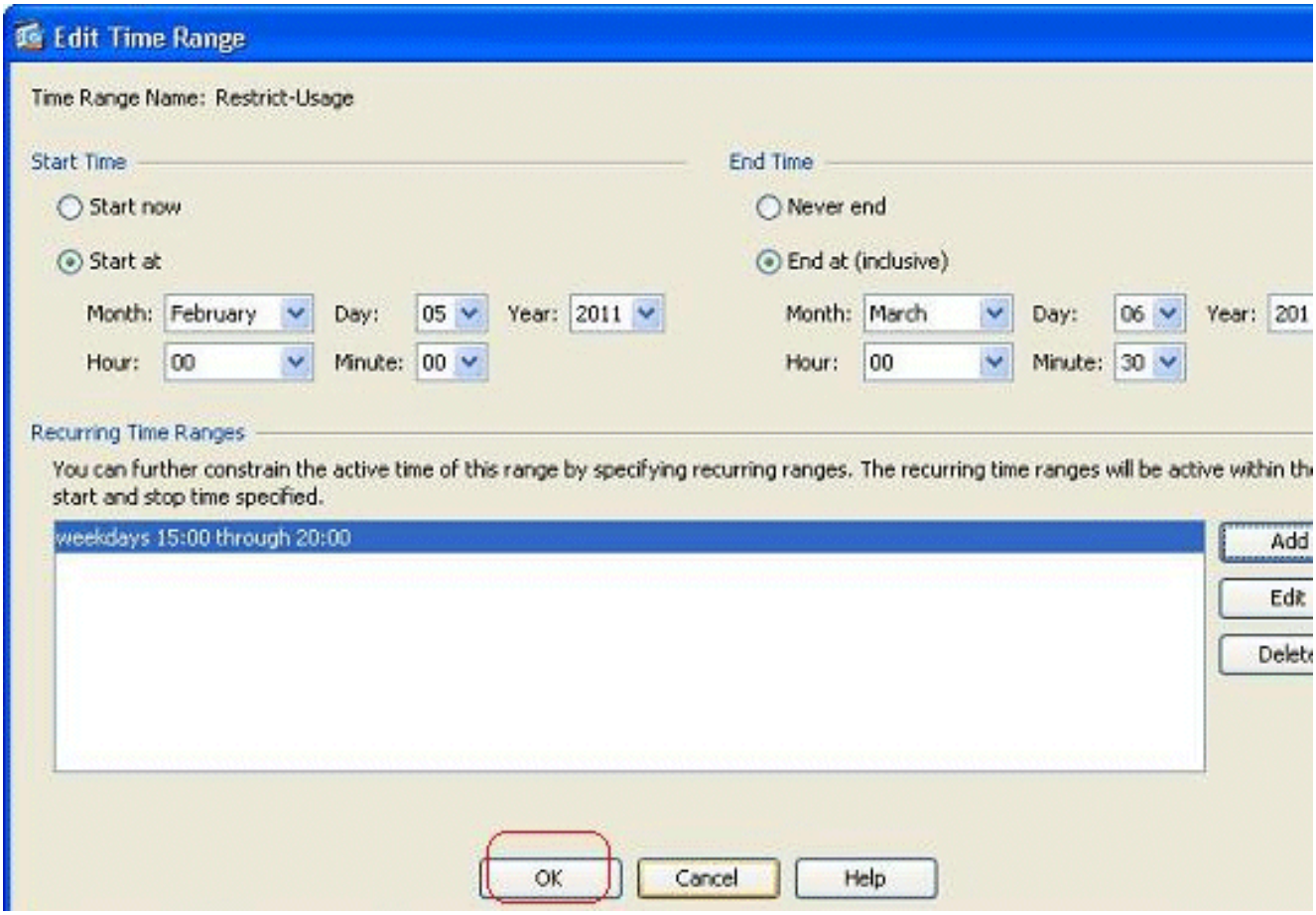
6. Di seguito è riportato un esempio su come specificare un intervallo di tempo ricorrente. Per definire un intervallo di tempo ricorrente, fare clic su **Add** (Aggiungi).



7. Specificare le impostazioni in base ai requisiti e fare clic su **OK** per completare l'operazione.



8. Fare clic su **OK** per tornare alla finestra Intervallo di tempo.



In base a questa configurazione, all'utente alle 172.16.10.50 è stato negato l'accesso a qualsiasi risorsa dalle 15 alle 20 in tutti i giorni feriali tranne sabato e domenica.

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

Nota: se per un comando di **intervallo di tempo** sono specificati sia valori assoluti che periodici, i comandi **periodici** vengono valutati solo dopo il raggiungimento dell'ora di inizio assoluta e non vengono valutati ulteriormente dopo il raggiungimento dell'ora di fine assoluta.

Informazioni correlate

- Pagina documentazione di Cisco ASA
- Documentazione e supporto tecnico – Cisco Systems