PIX/ASA 7.x e FWSM: Dichiarazioni NAT e PAT

Sommario

Introduzione

Questo documento fornisce esempi di configurazioni di base NAT (Network Address Translation) e PAT (Port Address Translation) sulle appliance di sicurezza Cisco PIX/ASA. Sono forniti diagrammi di rete semplificati. Per informazioni dettagliate, consultare la documentazione della versione software di PIX/ASA in uso.

Fare riferimento a Utilizzo dei comandi nat, global, static, conduit e access-list e del reindirizzamento delle porte (inoltro) sui PIX per ulteriori informazioni sui comandi nat, global, **static**, **conduit**, e **access-list** e sul reindirizzamento delle porte (inoltro) sui PIX 5.x e versioni successive.

Per ulteriori informazioni sugli esempi di configurazioni NAT e PAT di base sul firewall Cisco Secure PIX, consultare il documento sull'uso delle istruzioni NAT e PAT sul firewall Cisco Secure PIX.

Per ulteriori informazioni sulla configurazione NAT in ASA versione 8.3 e successive, consultare il documento sulle informazioni sulla configurazione NAT.

Nota: il protocollo NAT in modalità trasparente è supportato da PIX/ASA versione 8.x. Per ulteriori informazioni, fare riferimento a NAT in modalità trasparente.

Prerequisiti

Requisiti

I lettori di questo documento devono essere a conoscenza delle appliance di sicurezza Cisco PIX/ASA.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco PIX serie 500 Security Appliance versione 7.0 e successive.

Nota: Questo documento è stato ricertificato con PIX/ASA versione 8.x.

Nota: i comandi utilizzati in questo documento sono applicabili al modulo FWSM (Firewall Service Module).

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.

Il comando nat-control

Il comando **nat-control** sull'appliance PIX/ASA specifica che per consentire il passaggio del traffico attraverso il firewall, tutto il traffico che attraversa il firewall deve avere una voce di traduzione specifica (istruzione **nat** con un'istruzione **globale** o **statica** corrispondente). Il comando **nat-control** garantisce che il comportamento della traduzione sia lo stesso delle versioni di PIX Firewall precedenti alla 7.0. La configurazione predefinita di PIX/ASA versione 7.0 e successive è la specifica del comando **no nat-control**. Con PIX/ASA versione 7.0 e successive, è possibile modificare questo comportamento quando si usa il comando **nat-control**.

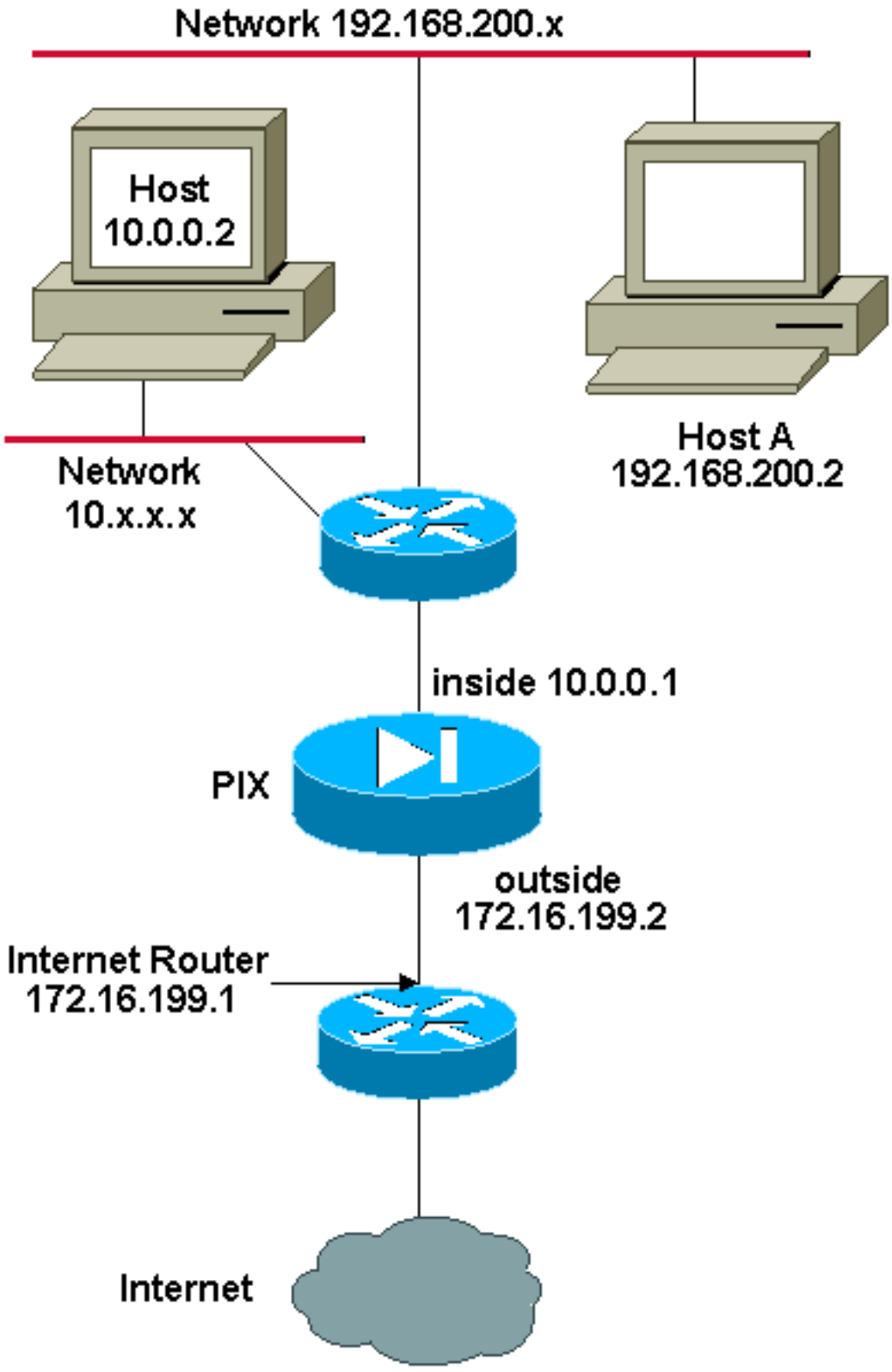
Se **nat-control** è disabilitato, il PIX/ASA inoltra i pacchetti da un'interfaccia di sicurezza superiore a una inferiore senza una voce di conversione specifica nella configurazione. Per passare il traffico da un'interfaccia di sicurezza inferiore a una più alta, usare gli elenchi degli accessi per

autorizzare il traffico. Infine, il PIX/ASA inoltra il traffico. Nel documento si fa riferimento al comportamento di un'appliance di sicurezza PIX/ASA con **controllo nat** abilitato.

Nota: se si desidera rimuovere o disabilitare l'istruzione nat-control in PIX/ASA, è necessario rimuovere tutte le istruzioni NAT dall'appliance di sicurezza. In generale, è necessario rimuovere il NAT prima di disattivare il controllo NAT. È necessario riconfigurare l'istruzione NAT in PIX/ASA in modo che funzioni come previsto.

Istruzioni NAT multiple con NAT 0

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Nell'esempio, l'ISP fornisce al gestore della rete un intervallo di indirizzi compreso tra 172.16.199.1 e 172.16.199.63. Il gestore della rete decide di assegnare 172.16.199.1 all'interfaccia interna del router Internet e 172.16.199.2 all'interfaccia esterna del PIX/ASA.

All'amministratore di rete era già stato assegnato un indirizzo di classe C, 192.168.200.0/24, e sono disponibili alcune workstation che utilizzano tali indirizzi per accedere a Internet. Queste workstation non devono essere tradotte tramite indirizzi. Tuttavia, alle nuove workstation vengono

assegnati indirizzi nella rete 10.0.0.0/8 e devono essere tradotti.

Per supportare questo progetto di rete, l'amministratore di rete deve utilizzare due istruzioni NAT e un pool globale nella configurazione PIX/ASA, come mostrato nell'output:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

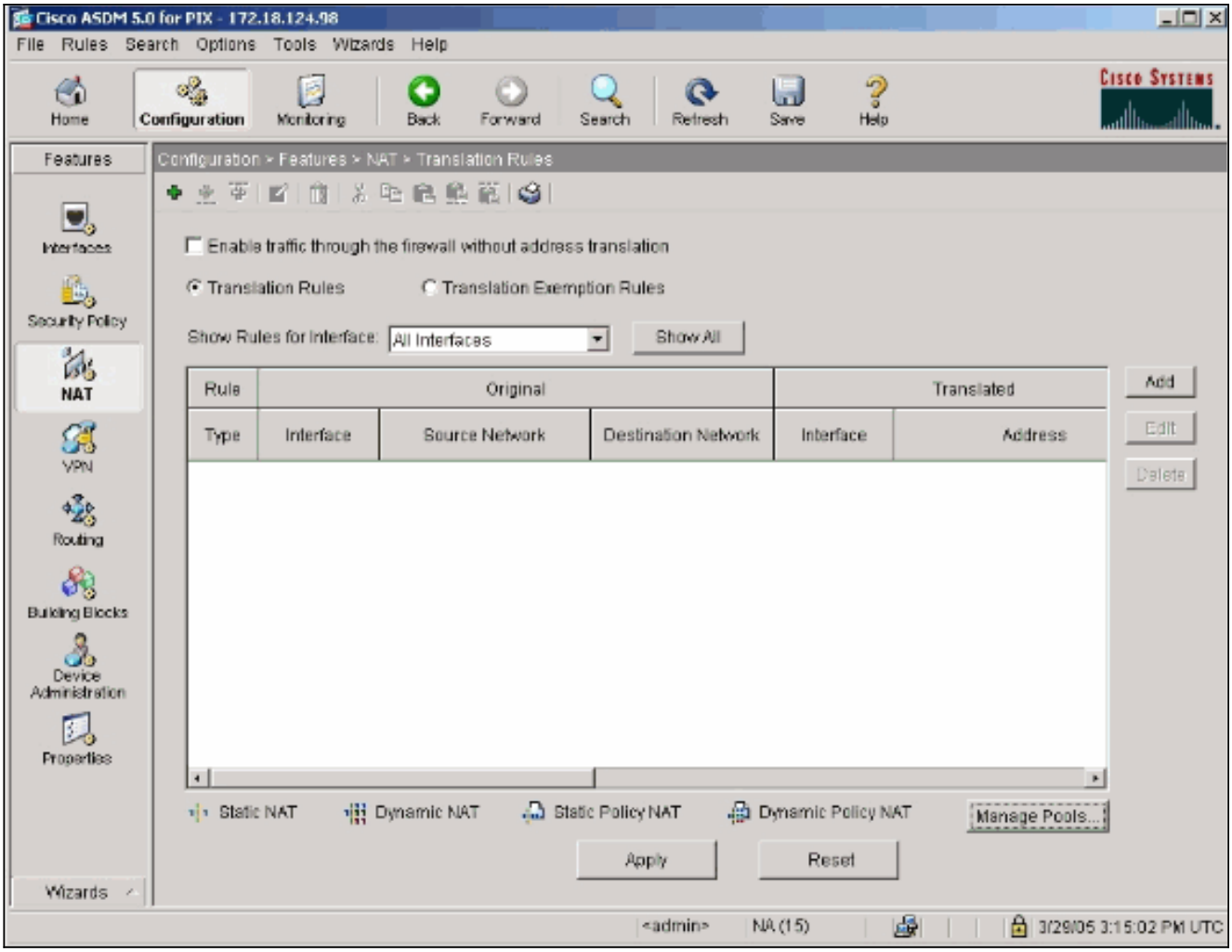
Questa configurazione non converte l'indirizzo di origine di alcun traffico in uscita dalla rete 192.168.200.0/24. Converte un indirizzo di origine nella rete 10.0.0.0/8 in un indirizzo compreso nell'intervallo da 172.16.199.3 a 172.16.199.62.

La procedura descritta di seguito spiega come applicare la stessa configurazione con Adaptive Security Device Manager (ASDM).

Nota: eseguire tutte le modifiche alla configurazione tramite CLI o ASDM. L'uso di CLI e ASDM per le modifiche alla configurazione causa un comportamento molto errato in termini di ciò che viene applicato da ASDM. Questo non è un bug, ma si verifica a causa del funzionamento di ASDM.

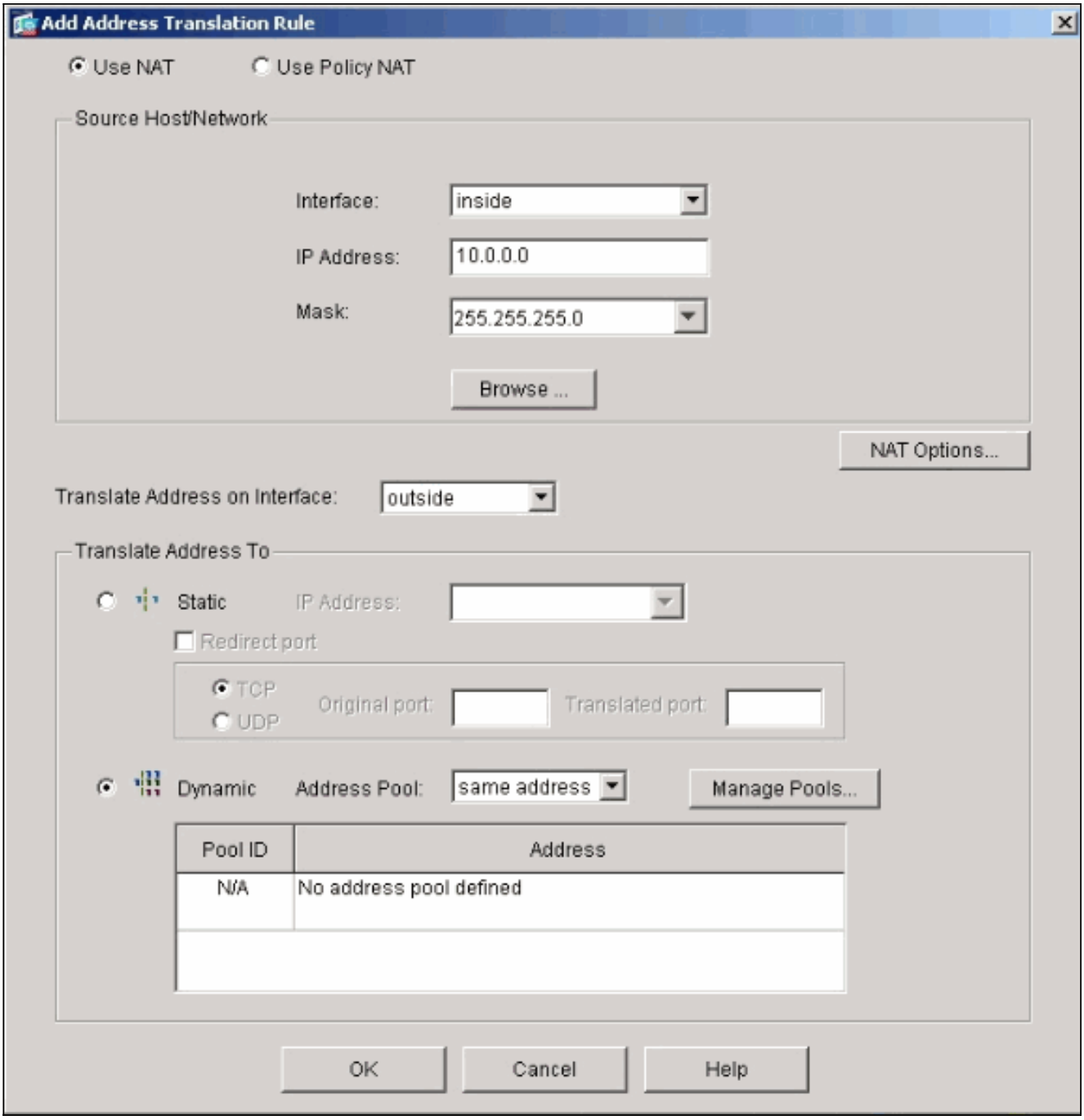
Nota: quando si apre ASDM, la configurazione corrente viene importata dal PIX/ASA e funziona da tale configurazione quando si apportano e si applicano le modifiche. Se si apporta una modifica su PIX/ASA mentre la sessione ASDM è aperta, ASDM non funziona più con la configurazione corrente di PIX/ASA. Assicurarsi di chiudere tutte le sessioni ASDM se si apportano modifiche alla configurazione tramite la CLI. Aprire nuovamente l'ASDM quando si desidera lavorare tramite la GUI.

1. Avviare ASDM, selezionare la scheda Configurazione e fare clic su **NAT**.
2. Per creare una nuova regola, fare clic su **Add**
   (Aggiungi).

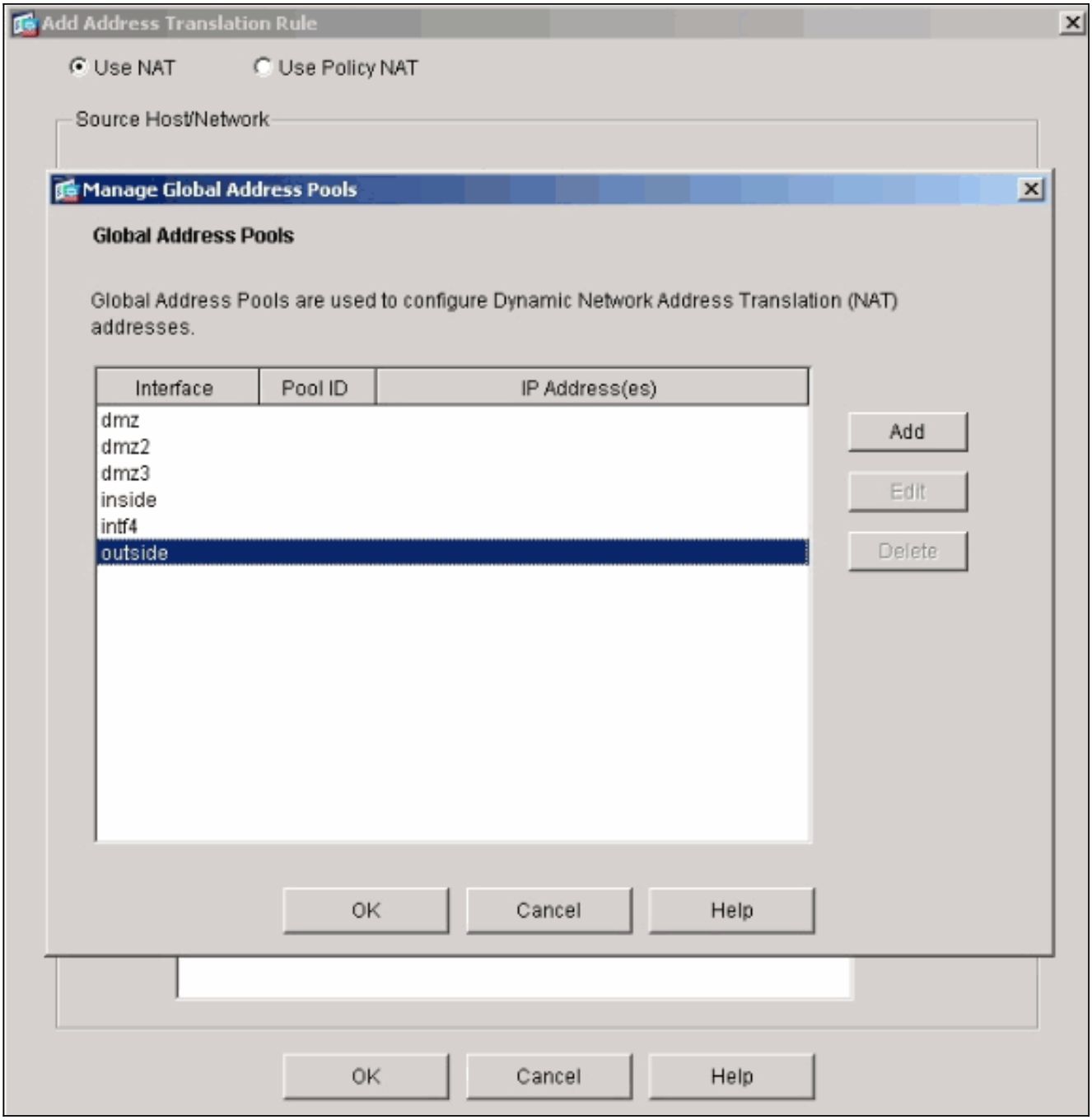


Viene visualizzata una nuova finestra che consente all'utente di modificare le opzioni NAT per questa voce NAT. Per questo esempio, eseguire NAT sui pacchetti in arrivo sull'interfaccia interna provenienti dalla rete 10.0.0.0/24 specifica.Il PIX/ASA converte questi pacchetti in un pool IP dinamico sull'interfaccia esterna. Dopo aver immesso le informazioni che descrivono il traffico diretto a NAT, definire un pool di indirizzi IP per il traffico convertito.

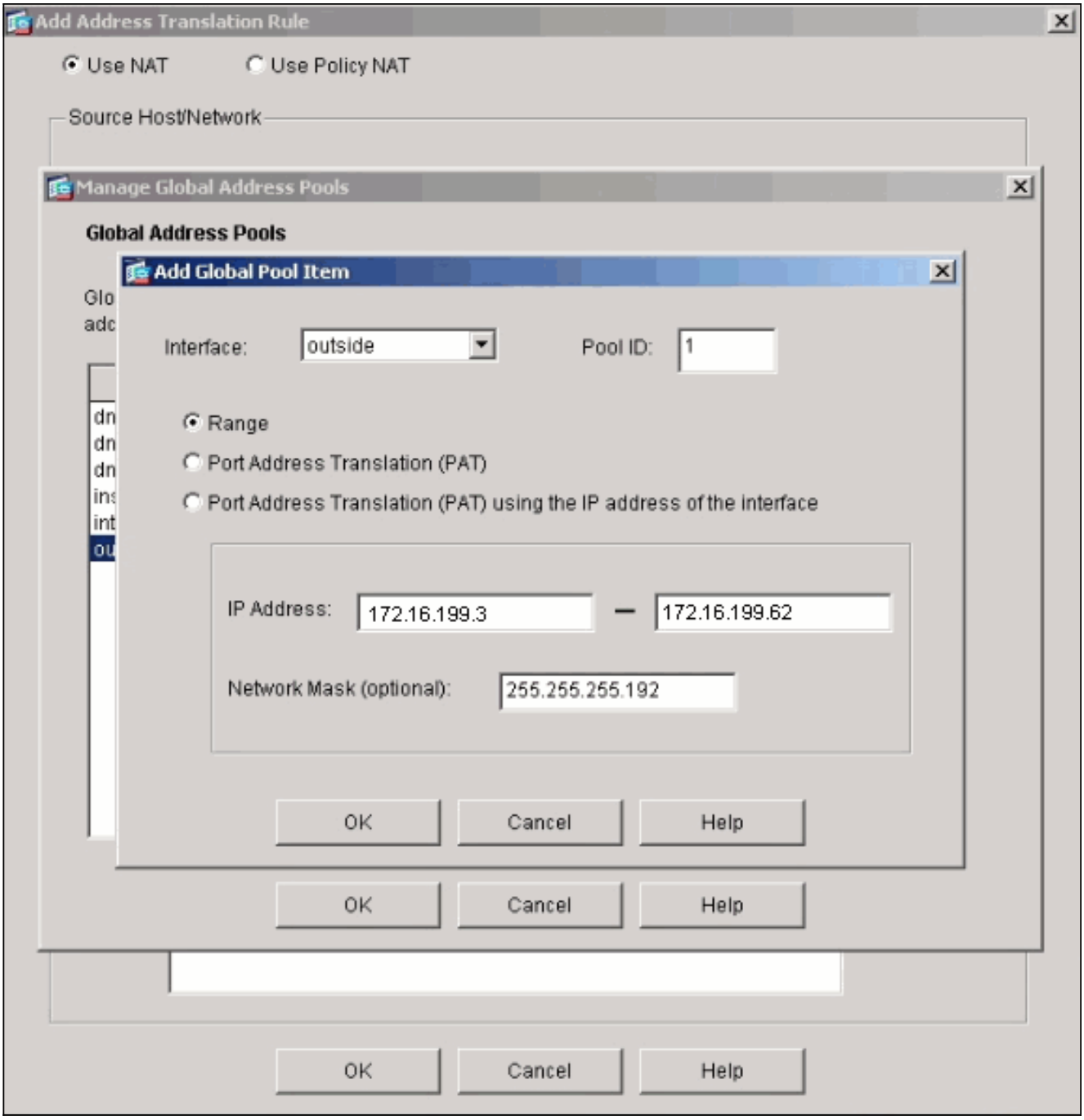
3. Per aggiungere un nuovo pool IP, fare clic su **Gestisci pool**.



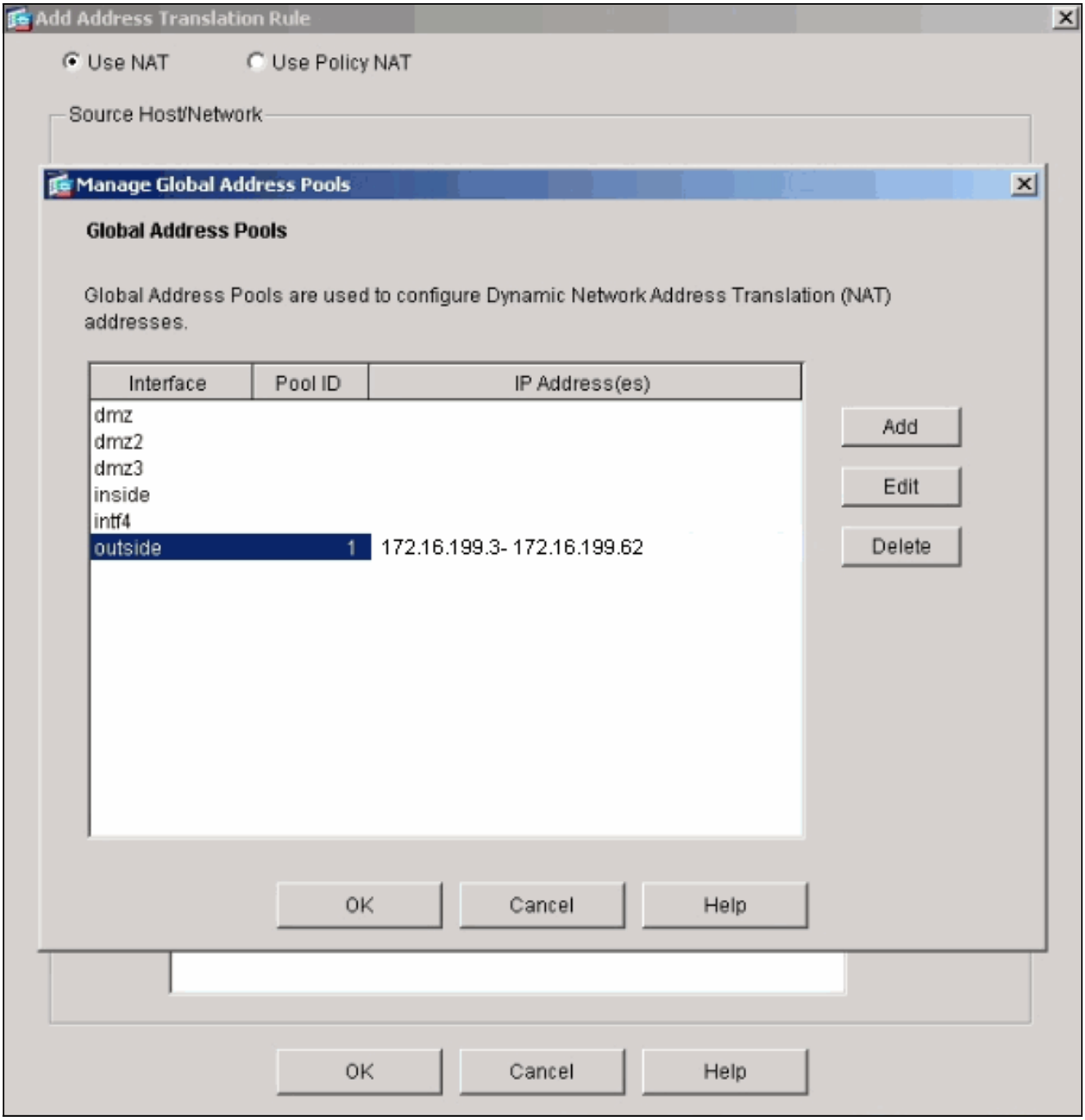
4. Scegliere **all'esterno** e fare clic su **Aggiungi**.



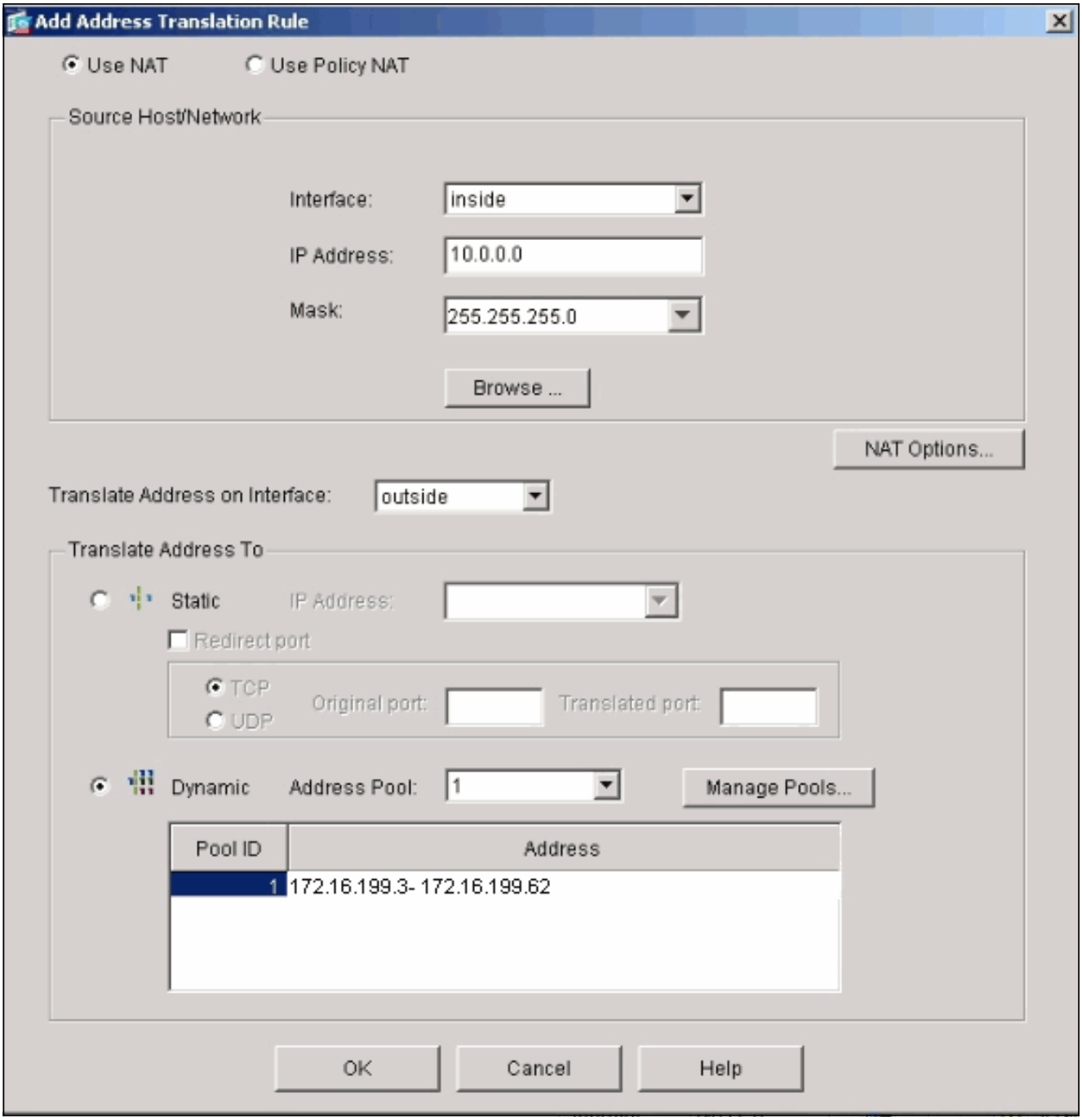
5. Specificare l'intervallo IP per il pool e assegnare al pool un numero ID intero univoco.



6. Immettere i valori appropriati e fare clic su **OK**.Il nuovo pool è definito per l'interfaccia esterna.

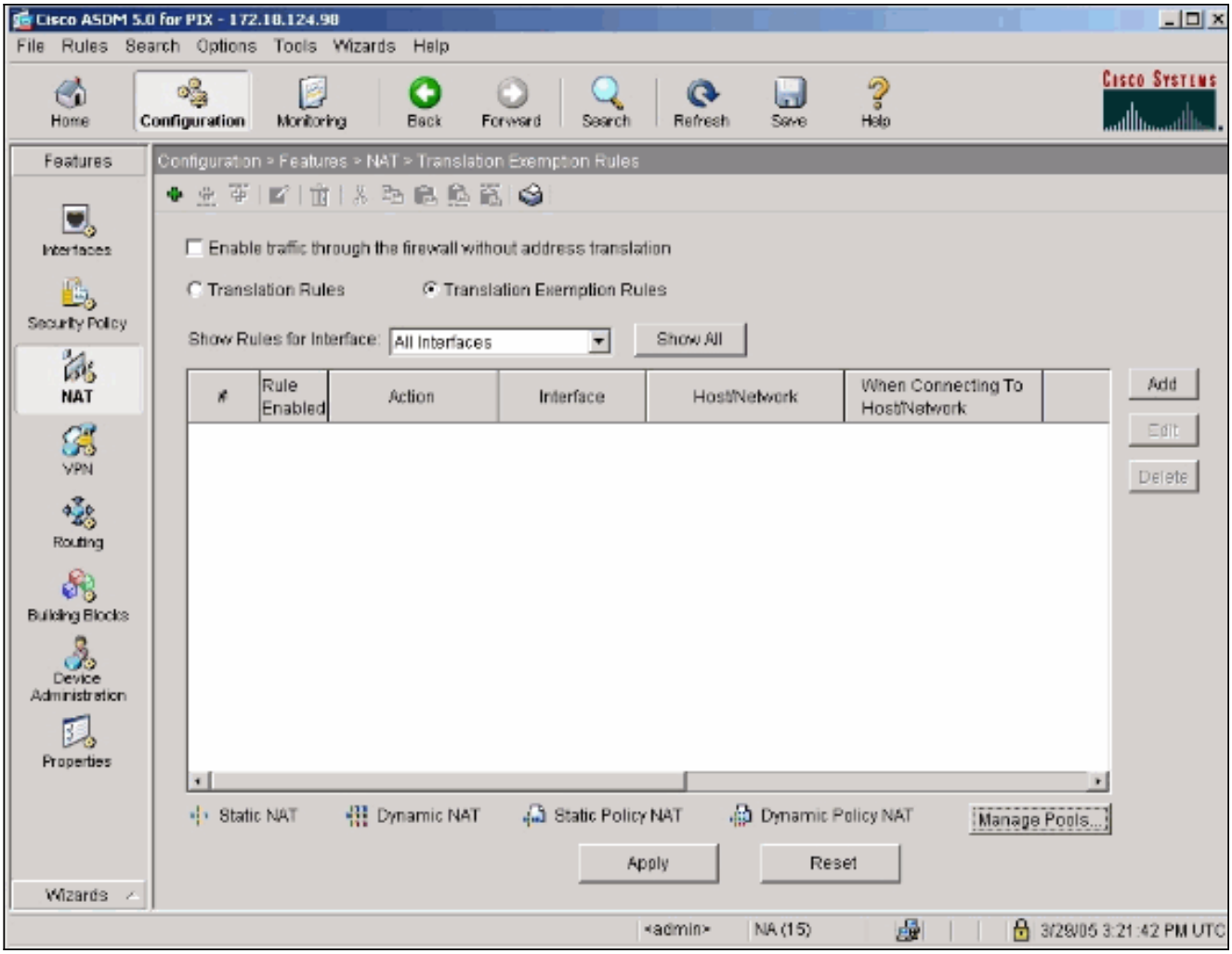


7. Dopo aver definito il pool, fare clic su **OK** per tornare alla finestra di configurazione della regola NAT.Assicurarsi di scegliere il pool appena creato dall'elenco a discesa Pool di indirizzi.

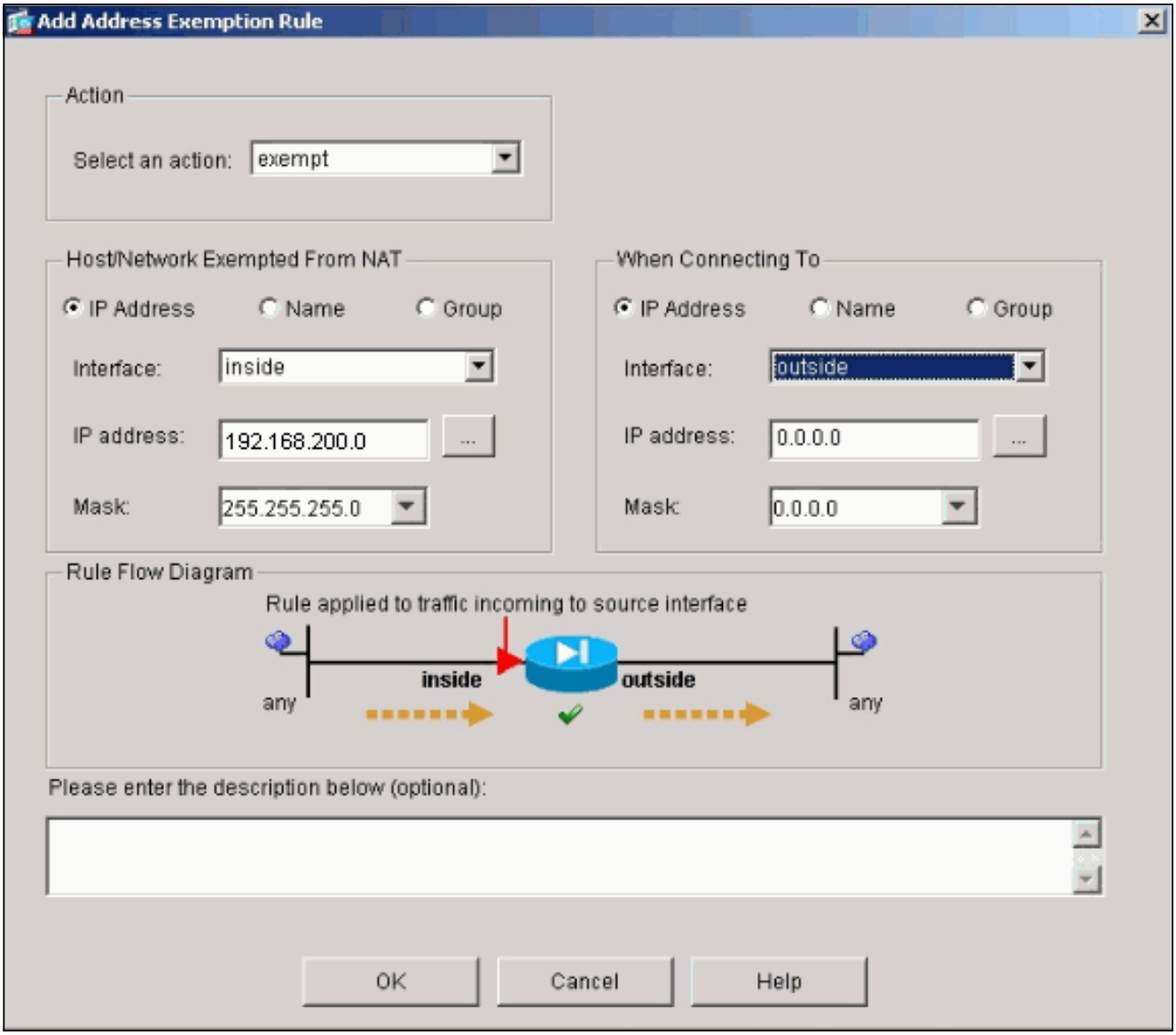


Èstata creata una traduzione NAT tramite l'appliance di sicurezza. Tuttavia, è ancora necessario creare la voce NAT che specifica quale traffico non diretto a NAT.

8. Per creare una nuova regola, fare clic su **Regole esenzione conversione** nella parte superiore della finestra e quindi su **Aggiungi**.



9. Scegliere l'interfaccia *interna* come origine e specificare la subnet **192.168.200.0/24**. Accettate i valori di default "Durante la connessione".



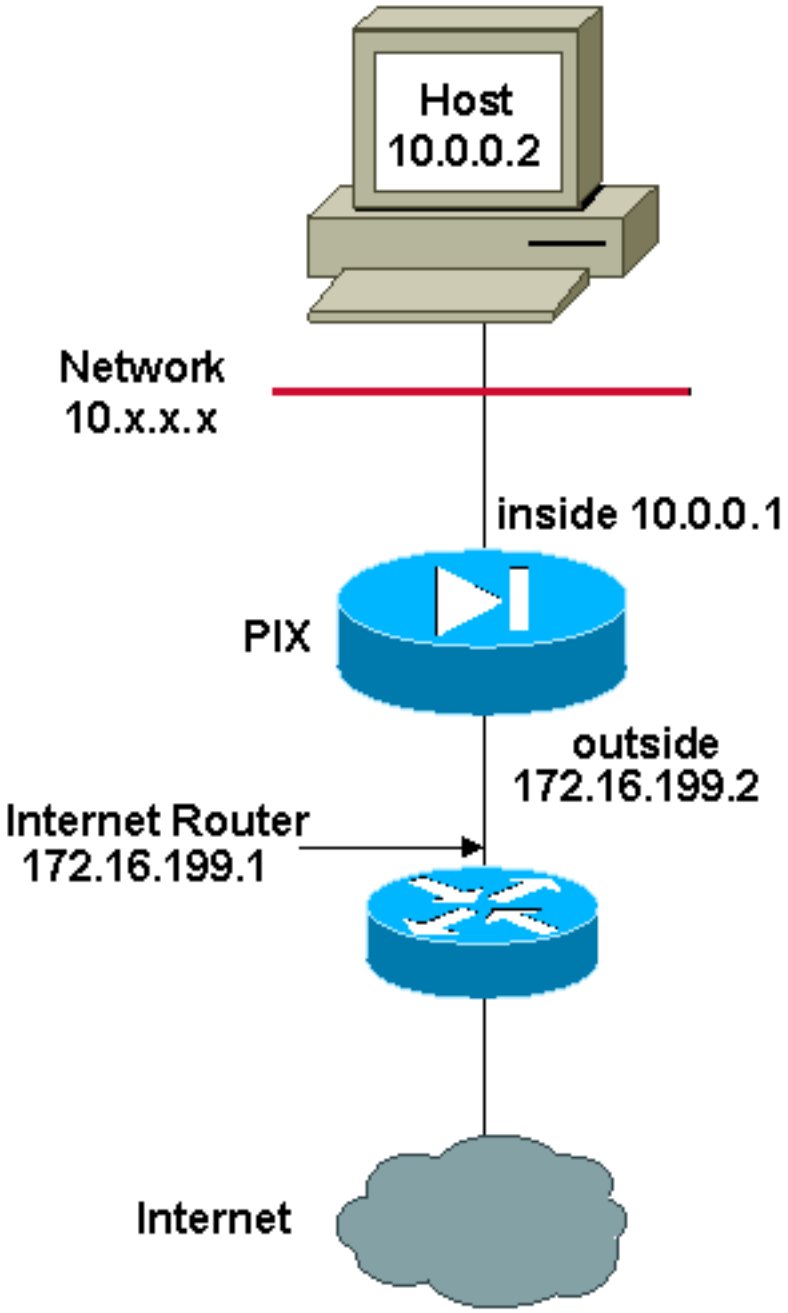
Le regole NAT sono ora definite.

10. Per applicare le modifiche alla configurazione corrente dell'appliance di sicurezza, fare clic su **Applica**.Questo output mostra le aggiunte effettive applicate alla configurazione PIX/ASA. Sono leggermente diversi dai comandi immessi dal metodo manuale, ma sono uguali.

```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

Più pool globali

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

In questo esempio, il gestore della rete dispone di due intervalli di indirizzi IP che vengono registrati su Internet. Il gestore della rete deve convertire tutti gli indirizzi interni compresi nell'intervallo 10.0.0.0/8 in indirizzi registrati. Gli intervalli di indirizzi IP che il gestore della rete deve utilizzare sono da 172.16.199.1 a 172.16.199.62 e da 192.168.150.1 a 192.168.150.254. Il gestore della rete può eseguire questa operazione con:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

In NAT dinamico, l'istruzione più specifica ha la precedenza quando si utilizza la stessa interfaccia su Global.

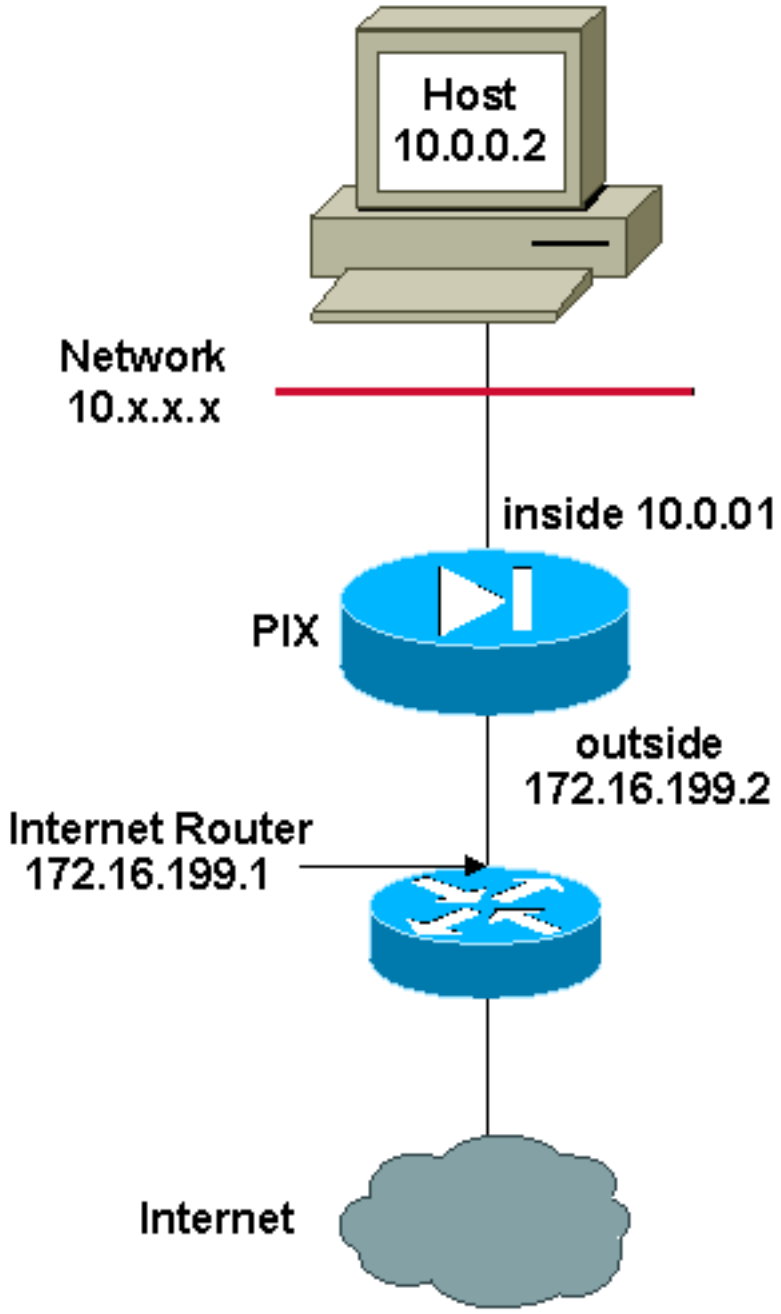
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Se la rete interna è impostata su 10.1.0.0, il NAT global 2 ha la precedenza su 1 in quanto più specifico per la traduzione.

Nota: nell'istruzione NAT viene utilizzato uno schema di indirizzamento con caratteri jolly. Questa istruzione indica al PIX/ASA di tradurre qualsiasi indirizzo di origine interno quando va su Internet. Se lo si desidera, l'indirizzo specificato in questo comando può essere più specifico.

Combinazione di dichiarazioni globali NAT e PAT

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente

instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Nell'esempio, l'ISP fornisce al gestore della rete un intervallo di indirizzi compreso tra 172.16.199.1 e 172.16.199.63, ad uso della società. Il gestore della rete decide di utilizzare 172.16.199.1 per l'interfaccia interna sul router Internet e 172.16.199.2 per l'interfaccia esterna sull'appliance PIX/ASA. Viene lasciato un numero compreso tra 172.16.199.3 e 172.16.199.62 da utilizzare per il pool NAT. Tuttavia, il gestore della rete sa che, in un dato momento, possono esserci più di sessanta persone che tentano di uscire dall'appliance PIX/ASA. Pertanto, il gestore della rete decide di prendere 172.16.199.62 e di impostarlo come indirizzo PAT in modo che più utenti possano condividere un indirizzo contemporaneamente.

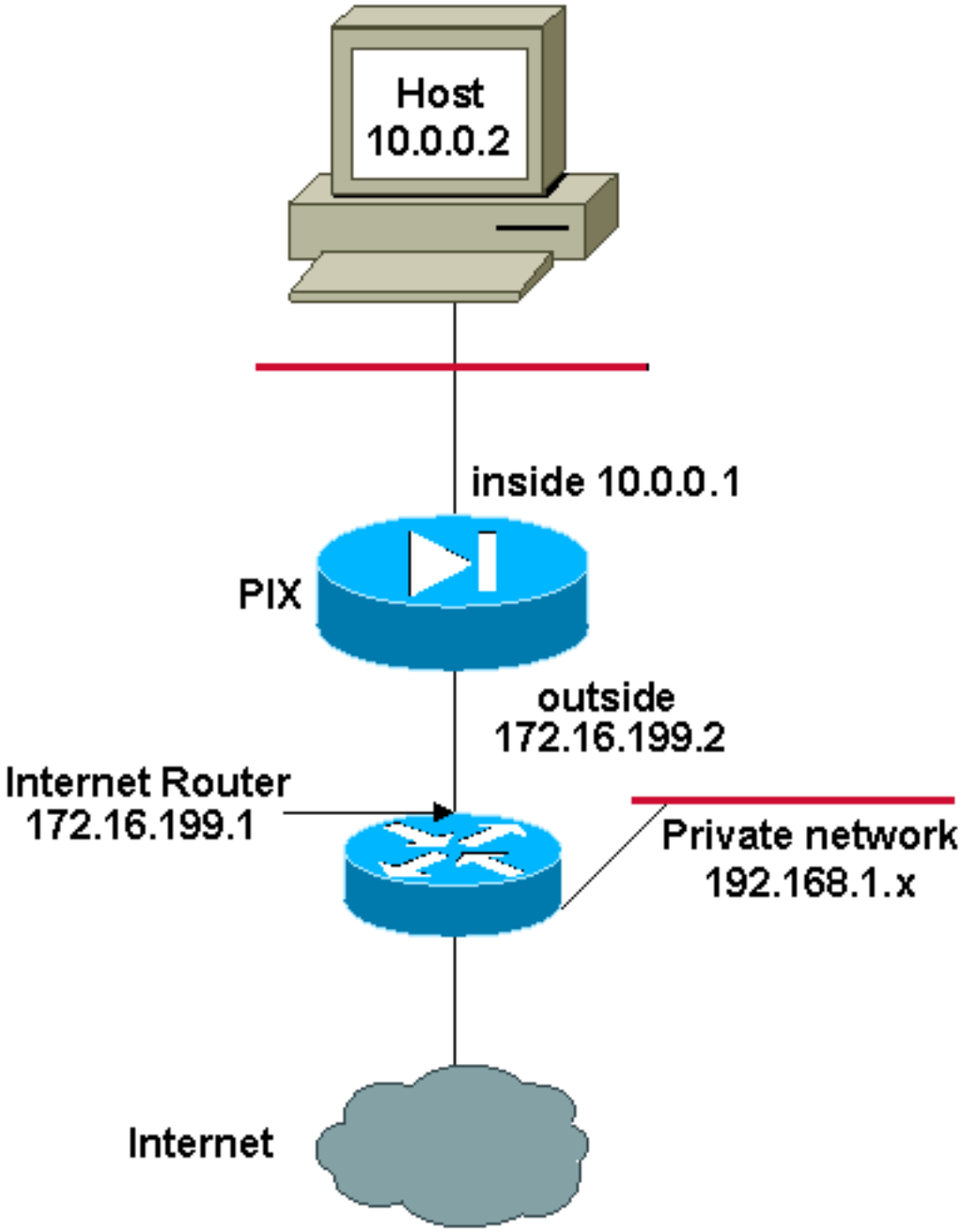
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Questi comandi istruiscono PIX/ASA a convertire l'indirizzo di origine in 172.16.199.3 a 172.16.199.61 per consentire ai primi 59 utenti interni di passare attraverso PIX/ASA. Una volta esauriti questi indirizzi, il PIX converte tutti gli indirizzi di origine successivi in 172.16.199.62 finché uno degli indirizzi nel pool NAT non diventa libero.

Nota: nell'istruzione NAT viene utilizzato uno schema di indirizzamento con caratteri jolly. Questa istruzione indica al PIX/ASA di tradurre qualsiasi indirizzo di origine interno quando va su Internet. L'indirizzo specificato in questo comando può essere più specifico.

Istruzioni NAT multiple con Access-List NAT 0

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Nell'esempio, l'ISP fornisce al gestore della rete un intervallo di indirizzi compreso tra 172.16.199.1 e 172.16.199.63. Il gestore della rete decide di assegnare 172.16.199.1 all'interfaccia interna del router Internet e 172.16.199.2 all'interfaccia esterna del PIX/ASA.

Tuttavia, in questo scenario, un altro segmento della LAN privata viene posizionato fuori dal router Internet. Il gestore della rete preferisce non sprecare gli indirizzi dal pool globale quando gli host di queste due reti comunicano tra loro. Il gestore della rete deve ancora tradurre l'indirizzo di origine di tutti gli utenti interni (10.0.0.0/8) quando si collegano a Internet.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list 101
```

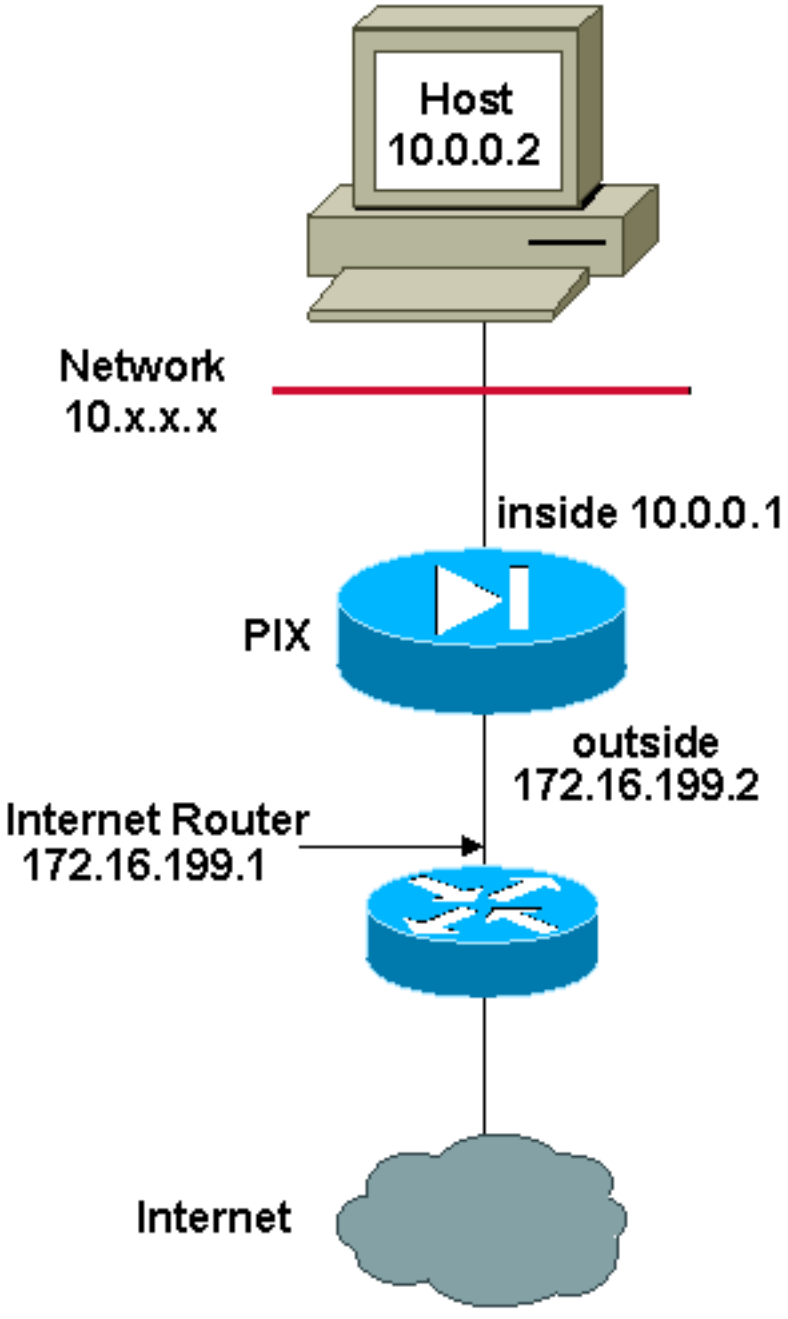
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Questa configurazione non converte gli indirizzi con indirizzo di origine 10.0.0.0/8 e indirizzo di destinazione 192.168.1.0/24. Converte l'indirizzo di origine da qualsiasi traffico avviato dalla rete 10.0.0.0/8 e destinato a un percorso diverso da 192.168.1.0/24 in un indirizzo compreso nell'intervallo da 172.16.199.3 a 172.16.199.62.

se il dispositivo Cisco restituisce i risultati di un comando **write terminal**, è possibile usare lo strumento Output Interpreter (solo utenti registrati).

Usa criterio NAT

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Quando si utilizza un elenco degli accessi con il comando **nat** per qualsiasi ID NAT diverso da 0, si abilita il criterio NAT.

Nota: la policy NAT è stata introdotta nella versione 6.3.2.

Il criterio NAT consente di identificare il traffico locale per la traduzione degli indirizzi quando si specificano gli indirizzi di origine e di destinazione (o le porte) in un elenco degli accessi. Il protocollo NAT normale utilizza solo indirizzi/porte di origine, mentre il criterio NAT utilizza sia indirizzi/porte di origine che di destinazione.

Nota: tutti i tipi di NAT supportano i criteri NAT ad eccezione dell'esenzione NAT (**elenco degli accessi nat 0**). L'esenzione NAT utilizza un elenco di controllo di accesso per identificare gli indirizzi locali, ma differisce dal criterio NAT in quanto le porte non vengono considerate.

Con il criterio NAT, è possibile creare più istruzioni NAT o statiche che identificano lo stesso indirizzo locale purché la combinazione di origine/porta e destinazione/porta sia univoca per ogni istruzione. È quindi possibile far corrispondere diversi indirizzi globali a ciascuna coppia origine/porta e destinazione/porta.

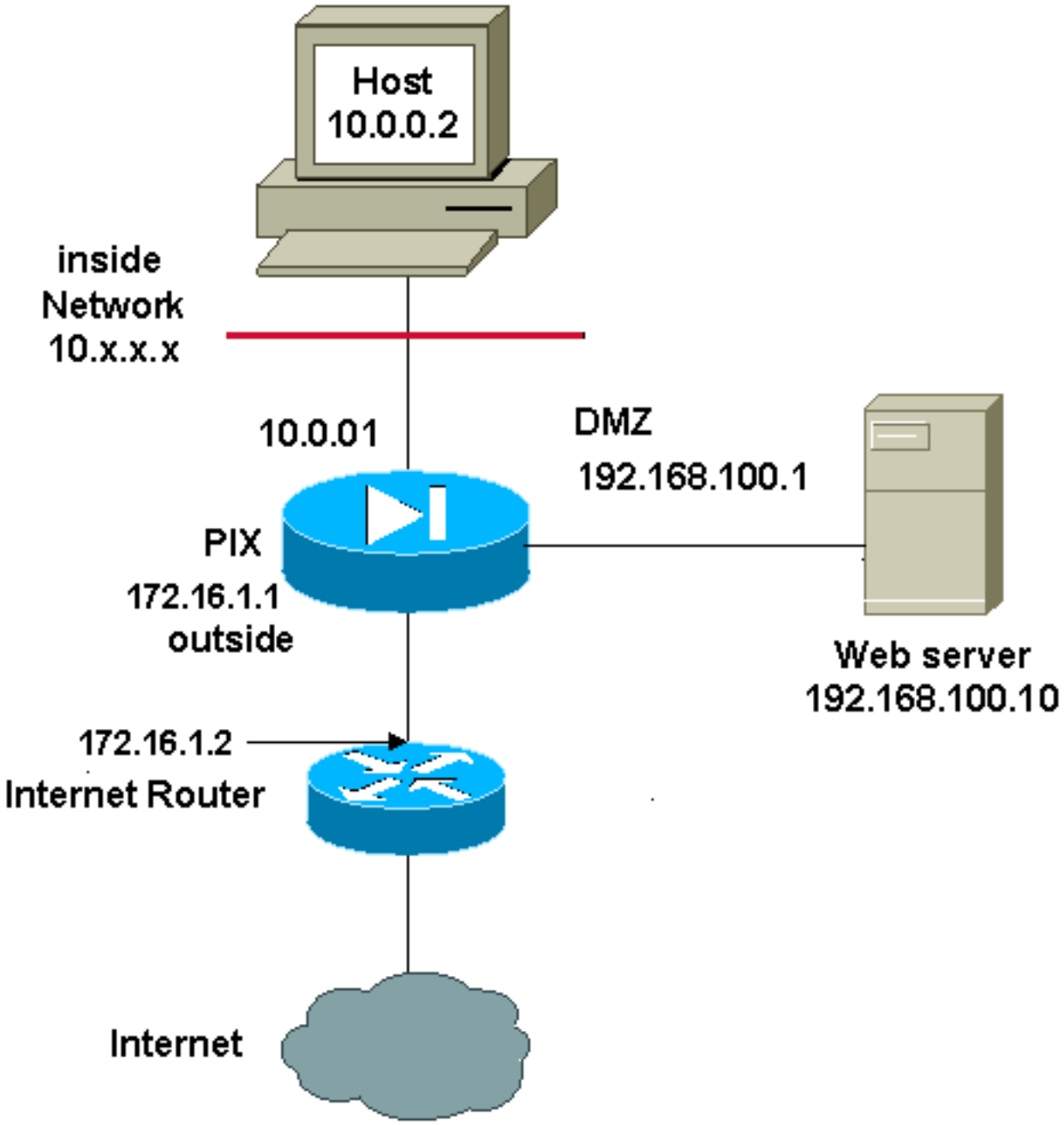
Nell'esempio, il gestore della rete fornisce l'accesso per l'indirizzo IP di destinazione 192.168.201.11 per la porta 80 (Web) e la porta 23 (Telnet), ma deve utilizzare due indirizzi IP diversi come indirizzo di origine. L'indirizzo IP 172.16.199.3 viene usato come indirizzo di origine per il Web. L'indirizzo IP 172.16.199.4 viene utilizzato per Telnet e deve convertire tutti gli indirizzi interni compresi nell'intervallo 10.0.0.0/8. Il gestore della rete può eseguire questa operazione con:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Èpossibile usare lo strumento Output Interpreter (solo utenti registrati) per visualizzare i potenziali errori e correggerli.

NAT statico

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Una configurazione NAT statica crea una mappatura uno-a-uno e converte un indirizzo specifico in un altro indirizzo. Questo tipo di configurazione crea una voce nella tabella NAT finché la configurazione è presente e consente agli host interni ed esterni di avviare una connessione. Ciò è utile soprattutto per gli host che forniscono servizi applicativi quali posta, Web, FTP e altri. Nell'esempio, le istruzioni NAT statiche sono configurate per consentire agli utenti interni e agli utenti esterni di accedere al server Web nella DMZ.

Questo output mostra come viene costruita un'istruzione statica. Prendere nota dell'ordine degli indirizzi IP reali e mappati.

`static (`*`real_interface`*`,`*`mapped_interface`*`)` *`mapped_ip real_ip`* `netmask` *`mask`*

Ecco la traduzione statica creata per fornire agli utenti dell'interfaccia interna l'accesso al server sulla DMZ. Viene creata una mappatura tra un indirizzo all'interno e l'indirizzo del server sulla

DMZ. Gli utenti all'interno possono quindi accedere al server sulla DMZ tramite l'indirizzo interno.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

Ecco la traduzione statica creata per fornire agli utenti dell'interfaccia esterna l'accesso al server sulla DMZ. Viene creata una mappatura tra un indirizzo esterno e l'indirizzo del server nella DMZ. Gli utenti esterni possono quindi accedere al server sulla DMZ tramite l'indirizzo esterno.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Nota: poiché l'interfaccia esterna ha un livello di protezione inferiore rispetto alla DMZ, è necessario creare anche un elenco degli accessi per consentire agli utenti esterni di accedere al server sulla DMZ. L'elenco degli accessi deve concedere agli utenti l'accesso all'**indirizzo mappato** nella traduzione statica. Si consiglia di rendere questo elenco degli accessi il più specifico possibile. In questo caso, a qualsiasi host è consentito l'accesso solo alle porte 80 (www/http) e 443 (https) sul server Web.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

L'elenco degli accessi deve quindi essere applicato all'interfaccia esterna.

```
access-group OUTSIDE in interface outside
```

Per ulteriori informazioni sui comandi access-list-extended e **access-group**, consultare il documento.

Come ignorare NAT

Questa sezione illustra come ignorare NAT. Quando si abilita il controllo NAT, potrebbe essere necessario ignorare NAT. È possibile utilizzare l'esenzione Identity NAT, Static Identity NAT o NAT per ignorare NAT.

Configura NAT identità

Identity NAT converte l'indirizzo IP reale nello stesso indirizzo IP. Solo gli host "tradotti" possono creare traduzioni NAT e il traffico di risposta può essere restituito.

Nota: Se si modifica la configurazione NAT e non si desidera attendere il timeout delle traduzioni esistenti prima di utilizzare le nuove informazioni NAT, utilizzare il comando **clear xlate** per cancellare la tabella di traduzione. Tuttavia, tutte le connessioni correnti che utilizzano le traduzioni vengono disconnesse quando si cancella la tabella di conversione.

Per configurare l'identità NAT, immettere questo comando:

```
hostname(config)#nat (real_interface) 0 real_ip
 [mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
 udp_max_conns]
```

Ad esempio, per utilizzare Identity NAT per la rete interna 10.1.1.0/24, immettere questo comando:

```
hostname(config)#nat (inside) 0 10.1.1.0
 255.255.255.0
```

Per ulteriori informazioni sul comando **nat**, consultare la guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2.

Configura NAT identità statica

L'identità statica NAT converte l'indirizzo IP reale nello stesso indirizzo IP. La traduzione è sempre attiva e sia gli host "tradotti" che quelli remoti possono creare connessioni. Il protocollo NAT per l'identità statica consente di utilizzare un NAT standard o un NAT basato su criteri. Policy NAT consente di identificare gli indirizzi reali e di destinazione quando si determinano gli indirizzi reali da tradurre (vedere la sezione Utilizzare Policy NAT per ulteriori informazioni sui criteri NAT). Ad esempio, è possibile utilizzare l'identità statica dei criteri NAT per un indirizzo interno quando accede all'interfaccia esterna e la destinazione è il server A, ma utilizzare una traduzione normale quando si accede al server esterno B.

Nota: Se si rimuove un comando statico, le connessioni correnti che utilizzano la traslazione non vengono interessate. Per rimuovere queste connessioni, immettere il comando **clear local-host**. Non è possibile cancellare le traduzioni statiche dalla tabella di traduzione con il comando **clear xlate**; è necessario rimuovere il comando statico. Con il comando clear xlate è possibile rimuovere solo le traduzioni dinamiche create dai comandi nat e globali.

Per configurare l'identità statica dei criteri NAT, immettere questo comando:

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip access-list acl_id [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

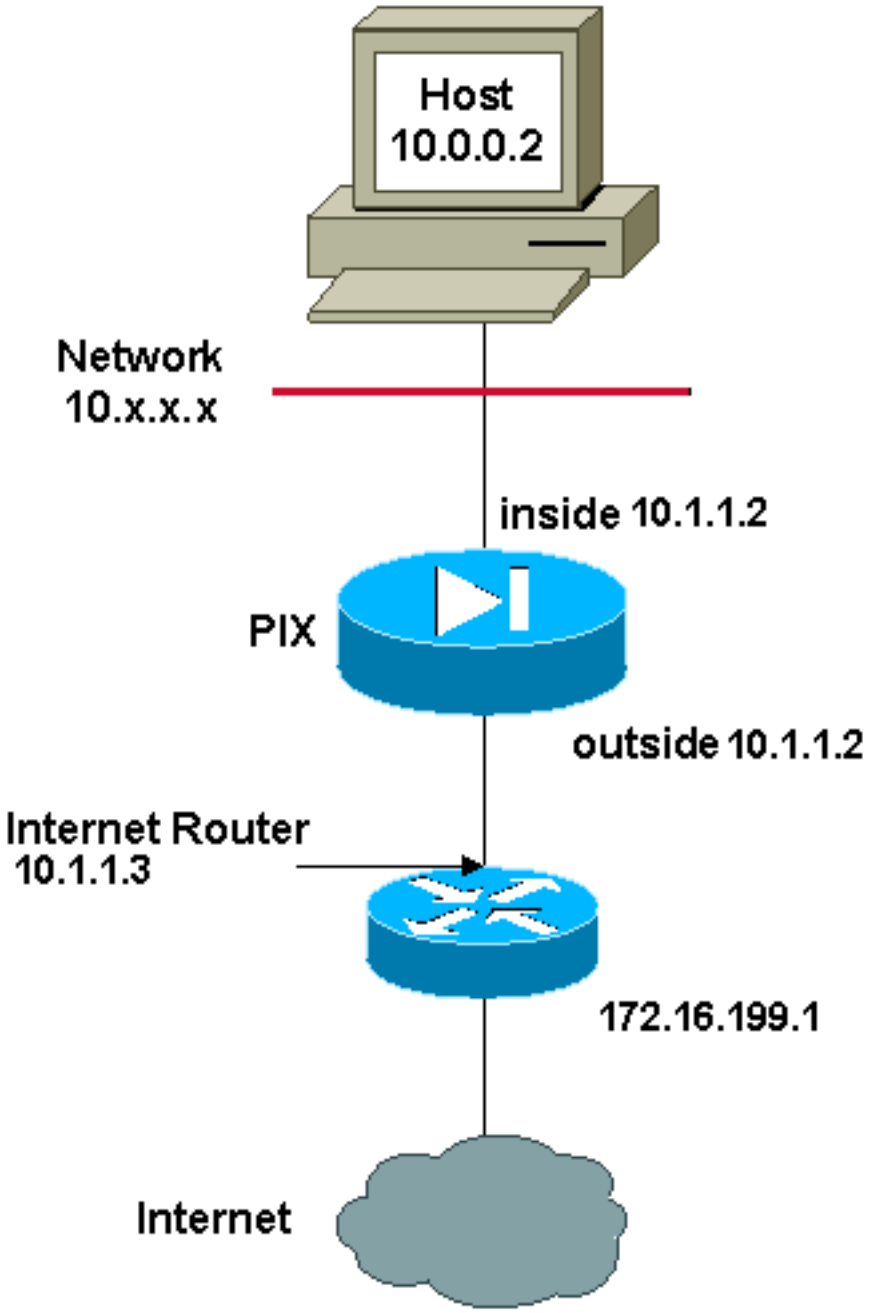
Usare il comando **access-list extended** per creare l'elenco degli accessi esteso. L'elenco degli accessi deve includere solo le voci ACE consentite. Verificare che l'indirizzo di origine nell'elenco degli accessi corrisponda a real_ip in questo comando. La policy NAT non considera le parole chiave inattive o basate sull'intervallo di tempo; tutte le ACE sono considerate attive per la configurazione NAT dei criteri. Per ulteriori informazioni, vedere la sezione Usa criterio NAT.

Per configurare un NAT di identità statica regolare, immettere questo comando:

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
 udp_max_conns]
```

Specificare lo stesso indirizzo IP per entrambi gli argomenti real_ip.

Esempio di rete



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Ad esempio, questo comando utilizza l'identità statica NAT per un indirizzo IP interno (10.1.1.2) quando vi si accede dall'esterno:

```
hostname(config)#static (inside,outside) 10.1.1.2
 10.1.1.2 netmask 255.255.255.255
```

Per ulteriori informazioni sul comando **statico**, consultare la guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2.

Questo comando utilizza l'identità statica NAT per un indirizzo esterno (172.16.199.1) quando vi si accede dall'interno:

```
hostname(config)#static (outside,inside) 172.16.199.1
```

```
 172.16.199.1 netmask 255.255.255.255
```

Questo comando esegue il mapping statico di un'intera subnet:

```
 hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
 netmask 255.255.255.0
```

Nell'esempio di NAT dei criteri di identità statici viene mostrato un singolo indirizzo reale che utilizza un NAT di identità quando si accede a un indirizzo di destinazione e una traduzione quando si accede a un altro indirizzo:

```
hostname(config)#access-list NET1 permit ip host
 10.1.1.3 172.16.199.0 255.255.255.224


hostname(config)#access-list NET2 permit ip host
 10.1.1.3 172.16.199.224 255.255.255.224


hostname(config)#static (inside,outside) 10.1.1.3
 access-list NET1


hostname(config)#static (inside,outside) 172.16.199.1
 access-list NET2
```

Nota: Per ulteriori informazioni sul comando **statico**, consultare la guida di riferimento dei comandi di Cisco ASA 5580 Adaptive Security Appliance, versione 8.1.

Nota: Per ulteriori informazioni sugli elenchi degli accessi, consultare la guida alla configurazione della riga di comando di Cisco ASA 5580 Adaptive Security Appliance, versione 8.1.

Configurazione dell'esenzione NAT

L'esenzione NAT esenta gli indirizzi dalla traduzione e consente agli host reali e remoti di creare connessioni. L'esenzione NAT consente di specificare gli indirizzi reali e di destinazione quando si determina il traffico reale da esentare (in modo simile alla policy NAT), in modo da avere un maggiore controllo utilizzando l'esenzione NAT rispetto all'identità NAT. Tuttavia, a differenza della policy NAT, l'esenzione NAT non considera le porte nell'elenco degli accessi. Utilizzare il protocollo NAT con identità statica per prendere in considerazione le porte nell'elenco degli accessi.

Nota: La rimozione di una configurazione di esenzione NAT non ha effetto sulle connessioni esistenti che utilizzano l'esenzione NAT. Per rimuovere queste connessioni, immettere il comando clear local-host.

Per configurare l'esenzione NAT, immettere questo comando:

```
hostname(config)#nat (real_interface) 0 access-list
 acl_name [outside]
```

Creare l'elenco degli accessi estesi con il comando **access-list extended**. L'elenco degli accessi può includere sia le voci di controllo di accesso consentite che quelle non consentite. Non specificare le porte reali e di destinazione nell'elenco degli accessi; L'esenzione NAT non considera i porti. L'esenzione NAT non prende inoltre in considerazione le parole chiave inattive o basate sull'intervallo di tempo; tutte le ACE sono considerate attive per la configurazione dell'esenzione NAT.

Per impostazione predefinita, questo comando esenta il traffico dall'interno all'esterno. Se si desidera che il traffico dall'esterno all'interno ignori NAT, aggiungere un altro comando **nat** e immettere all'esterno per identificare l'istanza NAT come esterna a NAT. È possibile utilizzare un'esenzione NAT esterna se si configura un NAT dinamico per l'interfaccia esterna e si desidera esentare il traffico di altro tipo.

Ad esempio, per esentare una rete interna quando si accede a un indirizzo di destinazione, immettere questo comando:

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0
 255.255.255.0 any


hostname(config)# nat (inside) 0 access-list
 EXEMPT
```

Per utilizzare il comando dinamico all'esterno di NAT per una rete DMZ ed esentare un'altra rete DMZ, immettere questo comando:

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0
 outside dns


hostname(config)#global (inside) 1
 10.1.1.2


hostname(config)#access-list EXEMPT permit ip 10.1.1.0
 255.255.255.0 any


hostname(config)#nat (dmz) 0 access-list
 EXEMPT
```

Per esentare un indirizzo interno quando si accede a due indirizzi di destinazione diversi, immettere questo comando:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
 255.255.255.0 172.16.199.0 255.255.255.224


hostname(config)#access-list NET1 permit ip 10.1.1.0
 255.255.255.0 172.16.199.224 255.255.255.224
```

```
hostname(config)#nat (inside) 0 access-list NET1
```

Verifica

Il traffico che attraversa l'appliance di sicurezza passa molto probabilmente a NAT. Per ulteriori informazioni, fare riferimento al documento PIX/ASA: Monitoraggio e risoluzione dei problemi di prestazioni per verificare le traduzioni in uso sull'appliance di sicurezza.

Il comando **show xlate count** visualizza il numero massimo e corrente di conversioni attraverso il PIX. Una traduzione è un mapping di un indirizzo interno a un indirizzo esterno e può essere un mapping uno-a-uno, ad esempio NAT, o un mapping molti-a-uno, ad esempio PAT. Questo comando è un sottoinsieme del comando **show xlate** , che invia ciascuna traslazione attraverso il PIX. L'output del comando mostra le traduzioni "in uso", che si riferiscono al numero di traduzioni attive nel PIX quando il comando viene emesso; "most used" (più usato) si riferisce alle massime conversioni che siano mai state viste sul PIX da quando è stato acceso.

Risoluzione dei problemi

Messaggio di errore ricevuto durante l'aggiunta di una porta statica per la porta 443

Problema

quando si aggiunge una porta statica per la porta 443 viene visualizzato questo messaggio:

```
[ERRORE] interfaccia tcp statica (INTERNA, ESTERNA) 443 192.168.1.87 443 netmask 255.255.255.255
tcp 0 0 udp 0

impossibile riservare la porta 443 per il percorso statico

ERRORE: impossibile scaricare i criteri
```

Soluzione

Questo messaggio di errore viene visualizzato quando ASDM o WEBVPN è in esecuzione sulla porta 443. Per risolvere il problema, accedere al firewall e completare una delle seguenti operazioni:

- Per modificare la porta ASDM a un valore diverso da 443, eseguire questi comandi:
  ```
  ASA(config)#no http server enable
  ASA(config)#http server enable 8080
  ```

- Per modificare la porta WEBVPN in un valore diverso da 443, eseguire questi comandi:
  ```
  ASA(config)#webvpn
  ASA(config-webvpn)#enable outside
  ASA(config-webvpn)#port 65010
  ```

Dopo aver eseguito questi comandi, dovrebbe essere possibile aggiungere un NAT/PAT sulla porta 443 a un altro server. Se si tenta di utilizzare ASDM per gestire l'appliance ASA in futuro, specificare la nuova porta come 8080.

ERRORE: conflitto di indirizzi mappati con indirizzi statici esistenti

Problema

Quando si aggiunge un'istruzione statica sull'appliance ASA, viene visualizzato questo messaggio:

```
ERRORE: conflitto di indirizzi mappati con indirizzi statici esistenti
```

Soluzione

Verificare che non esista già una voce per l'origine statica che si desidera aggiungere.

Informazioni correlate

- Pagina di supporto PIX
- Riferimenti per i comandi PIX
- Pagina di supporto ASA
- Riferimenti per i comandi ASA
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems