

Configurazione dell'inoltro porte ASA versione 9 con NAT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Consenti agli host interni l'accesso alle reti esterne con PAT](#)

[Consenti agli host interni l'accesso alle reti esterne con NAT](#)

[Consenti agli host non attendibili l'accesso agli host della rete attendibile](#)

[NAT identità statica](#)

[Reindirizzamento delle porte \(inoltro\) con](#)

[Verifica](#)

[Connessione](#)

[Syslog](#)

[Packet Tracer](#)

[Acquisisci](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare le funzionalità di reindirizzamento delle porte (inoltro) e NAT (Network Address Translation) esterno nel software Adaptive Security Appliance (ASA) versione 9.x, con l'uso della CLI o di Adaptive Security Device Manager (ASDM).

Per ulteriori informazioni, consultare la [guida alla configurazione di Cisco ASA Series Firewall ASDM](#).

Prerequisiti

Requisiti

Per consentire la configurazione del dispositivo da parte dell'ASDM, consultare il documento sulla [configurazione dell'accesso alla gestione](#).

Componenti usati

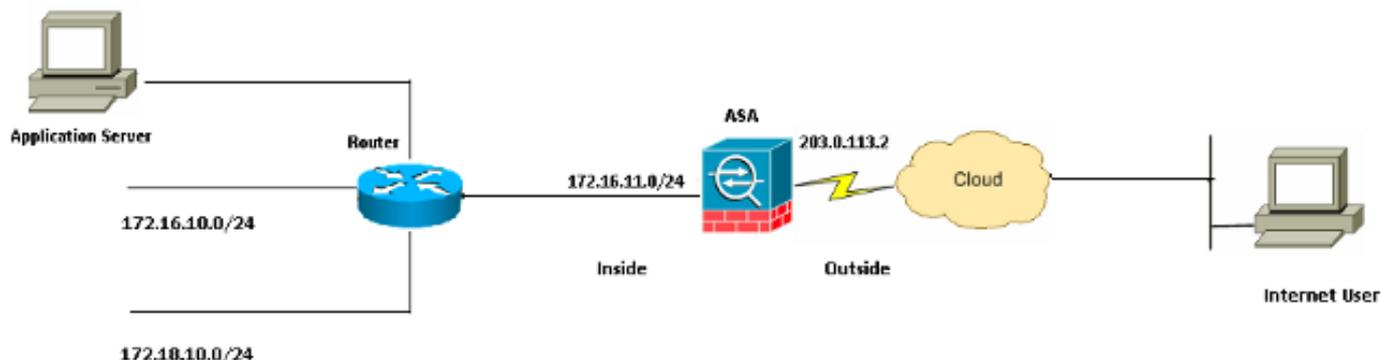
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5525 Security Appliance Software versione 9.x e successive
- ASDM versione 7.x e successive

"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".

Configurazione

Esempio di rete



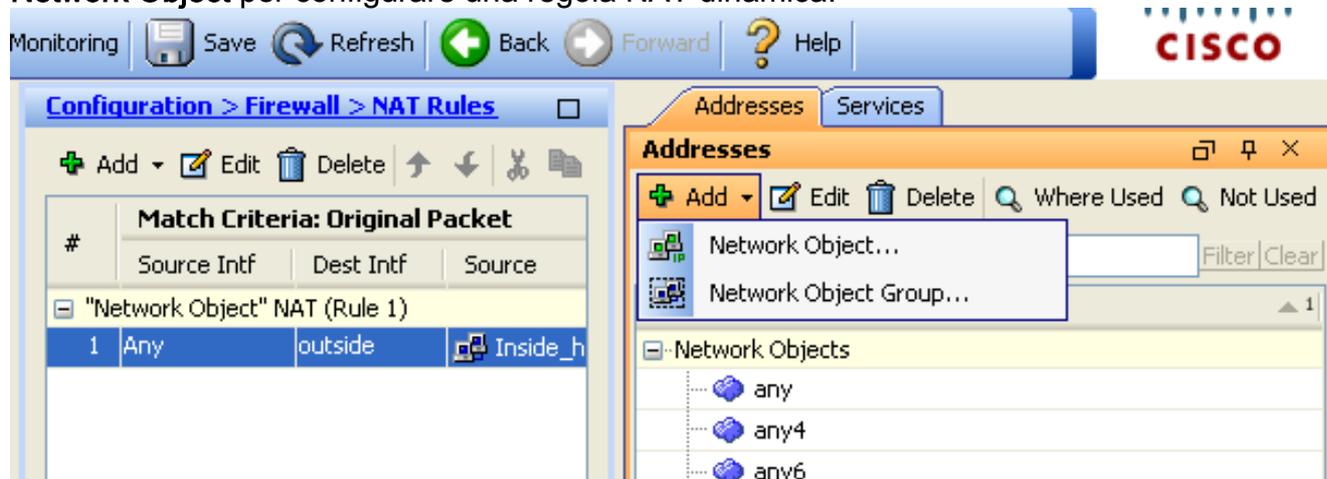
Gli schemi di indirizzi IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

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

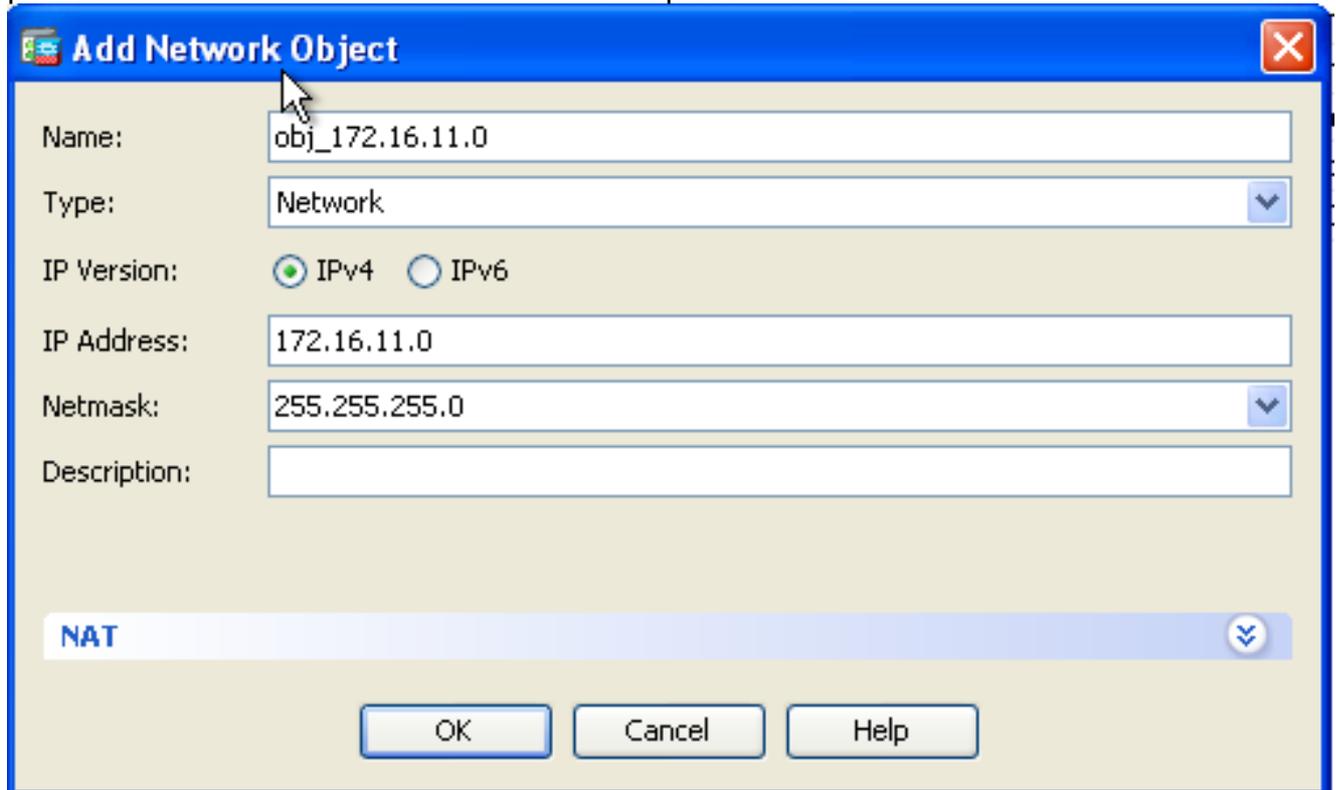
Se si desidera che gli host interni condividano un singolo indirizzo pubblico per la traduzione, utilizzare Port Address Translation (PAT). Una delle configurazioni PAT più semplici prevede la conversione di tutti gli host interni in modo che assomiglino all'indirizzo IP dell'interfaccia esterna. Si tratta della configurazione tipica utilizzata quando il numero di indirizzi IP instradabili disponibili presso l'ISP è limitato a pochi o forse a uno solo.

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

1. Scegliere **Configurazione > Firewall > Regole NAT**. Fare clic su **Add**, quindi selezionare **Network Object** per configurare una regola NAT dinamica.



2. Configurare la rete/l'host/l'intervallo per cui è richiesto il **percorso dinamico**. In questo esempio è stata selezionata una delle subnet interne. Questo processo può essere ripetuto per le altre subnet che si desidera tradurre in questo modo.



Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

OK Cancel Help

3. Espandere NAT. Selezionare la casella di controllo **Aggiungi regole di conversione automatica indirizzi**. Nell'elenco a discesa Tipo (Type), selezionate **PAT dinamico (Dynamic PAT) (Nascondi (Hide))**. Nel campo **Indirizzi tradotti**, scegliere l'opzione che riflette l'interfaccia esterna. Fare clic su **Avanzate**.

Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

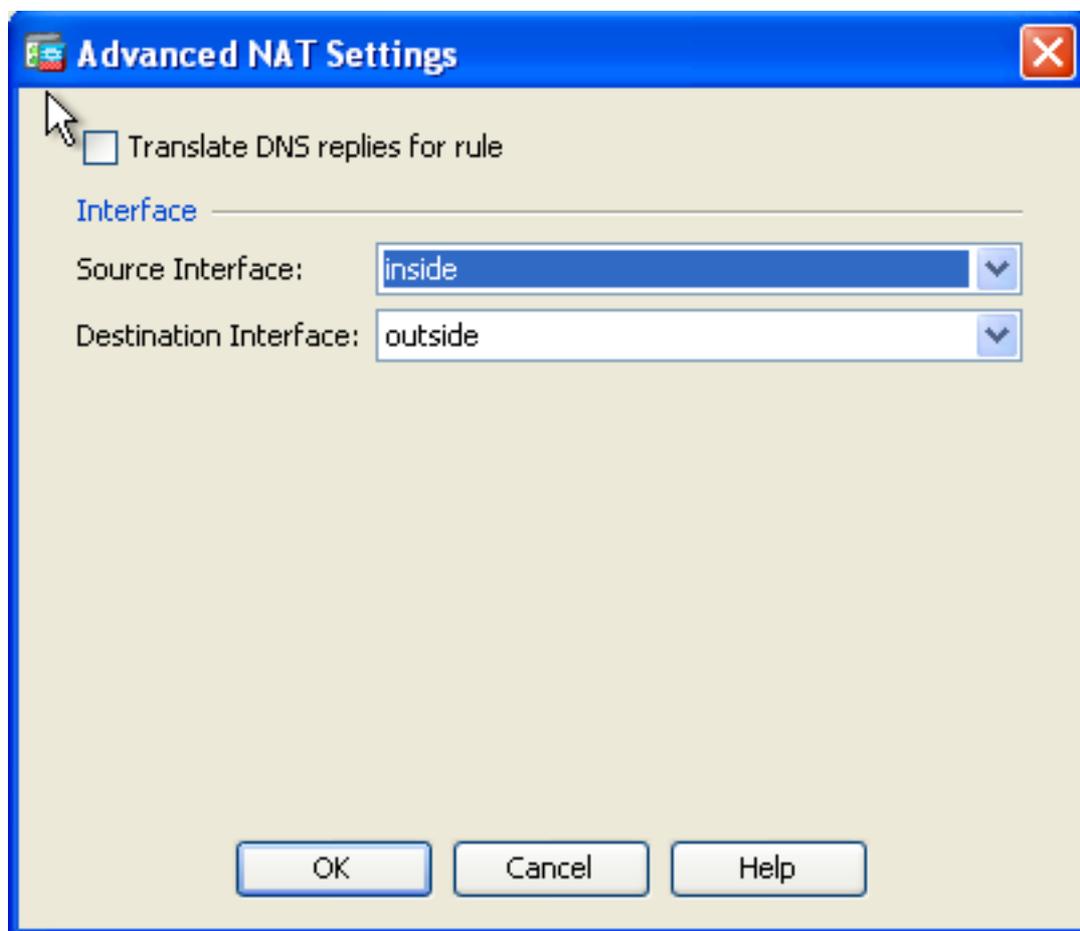
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Per rendere effettive le modifiche, fare clic su **OK** e su **Applica**.



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

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

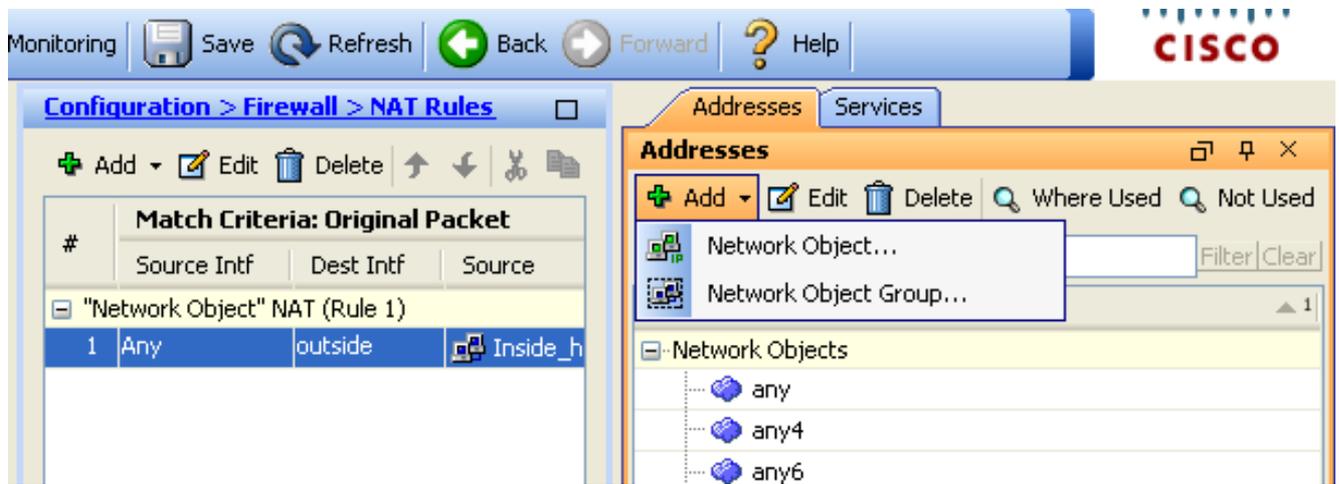
Consenti agli host interni l'accesso alle reti esterne con NAT

È possibile consentire a un gruppo di host/reti interni di accedere al mondo esterno con la configurazione delle regole NAT dinamiche. A differenza di PAT, NAT dinamico alloca gli indirizzi tradotti da un pool di indirizzi. Di conseguenza, un host viene mappato al proprio indirizzo IP tradotto e due host non possono condividere lo stesso indirizzo IP tradotto.

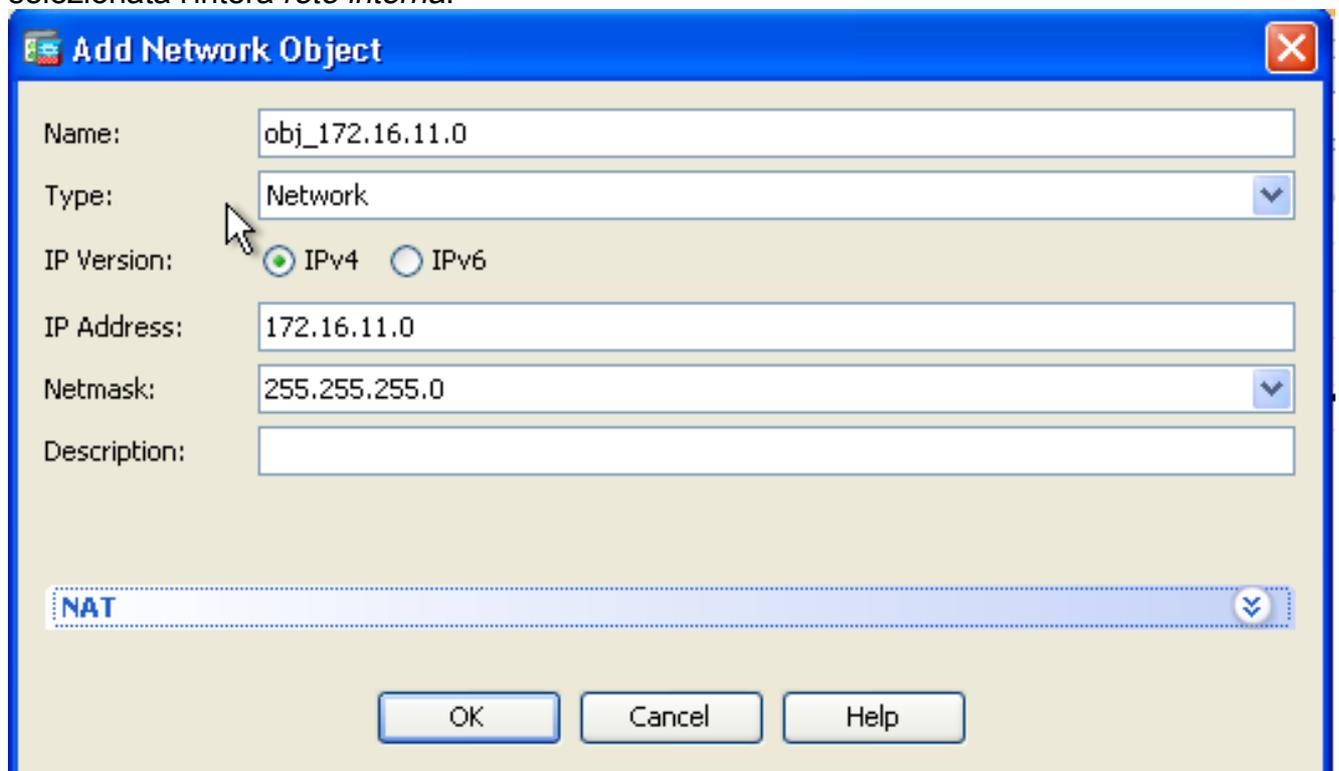
A tal fine, è necessario selezionare l'indirizzo reale degli host/reti a cui concedere l'accesso e associarli a un pool di indirizzi IP tradotti.

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

1. Scegliere **Configurazione > Firewall > Regole NAT**. Fare clic su **Add**, quindi selezionare **Network Object** per configurare una regola NAT dinamica.



2. Configurare la rete/l'host/l'intervallo per cui è richiesto Dynamic PAT. Nell'esempio è stata selezionata l'intera *rete interna*.



3. Espandere NAT. Selezionare la casella di controllo **Aggiungi regole di conversione automatica indirizzi**. Nell'elenco a discesa Tipo (Type), selezionate **Dinamico (Dynamic)**. Nel campo Indirizzo tradotto, scegliere la selezione appropriata. Fare clic su **Avanzate**.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. Fare clic su **Add** (Aggiungi) per aggiungere l'oggetto di rete. Nell'elenco a discesa Tipo, scegliere **Intervallo**. Nei campi Indirizzo iniziale e Indirizzo finale immettere gli indirizzi IP iniziale e finale. Fare clic su **OK**.

Add Network Object

Name: obj-my-range

Type: Range

IP Version: IPv4 IPv6

Start Address: 203.0.113.10

End Address: 203.0.113.20

Description:

NAT

OK Cancel Help

5. Nel campo Indirizzo tradotto, scegliere l'oggetto indirizzo. Per selezionare le interfacce di origine e di destinazione, fare clic su **Advanced** (Avanzate).

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

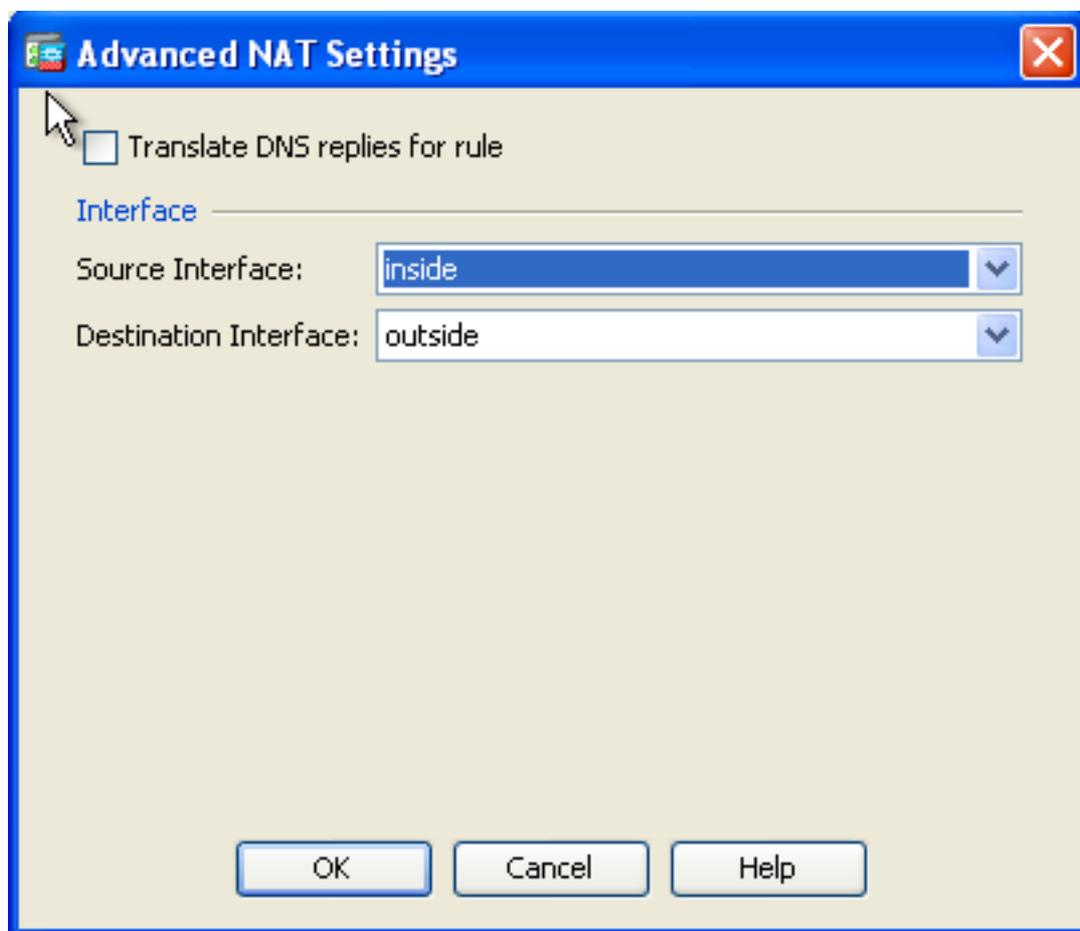
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

6. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Per rendere effettive le modifiche, fare clic su **OK** e su **Applica**.



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

```
object network obj-my-range  
range 203.0.113.10 203.0.113.20
```

```
object network obj_172.16.11.0  
subnet 172.16.11.0 255.255.255.0  
nat(inside,outside) dynamic obj-my-range
```

In base a questa configurazione, gli host nella rete 172.16.11.0 vengono convertiti in qualsiasi indirizzo IP del pool NAT, 203.0.113.10 - 203.0.113.20. Se il pool mappato ha meno indirizzi del gruppo reale, si potrebbe esaurire il numero di indirizzi. Di conseguenza, è possibile provare a implementare un NAT dinamico con il backup PAT dinamico oppure espandere il pool corrente.

1. Ripetere i passaggi da 1 a 3 nella configurazione precedente e fare di nuovo clic su **Add** (Aggiungi) per aggiungere un oggetto di rete. Nell'elenco a discesa Tipo, scegliere **Host**. Nel campo IP Address (Indirizzo IP), immettere l'indirizzo IP di backup del PAT. Fare clic su **OK**.

Add Network Object

Name: (optional)

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

FQDN:

Description:

NAT

OK Cancel Help

2. Fare clic su **Add** (Aggiungi) per aggiungere un gruppo di oggetti di rete. Nel campo Nome gruppo, immettere un nome di gruppo e **aggiungere** entrambi gli oggetti indirizzo (intervallo NAT e indirizzo IP PAT) nel gruppo.

Add Network Object Group

Group Name:

Description:

Existing Network Objects/Groups:

Name	IP Address	Netmask	Description
- Network Objects			
any			
any4			
any6			
inside-net...	19.19.19.0	255.255.255.0	
obj_172.1...	172.16.11.0	255.255.255.0	

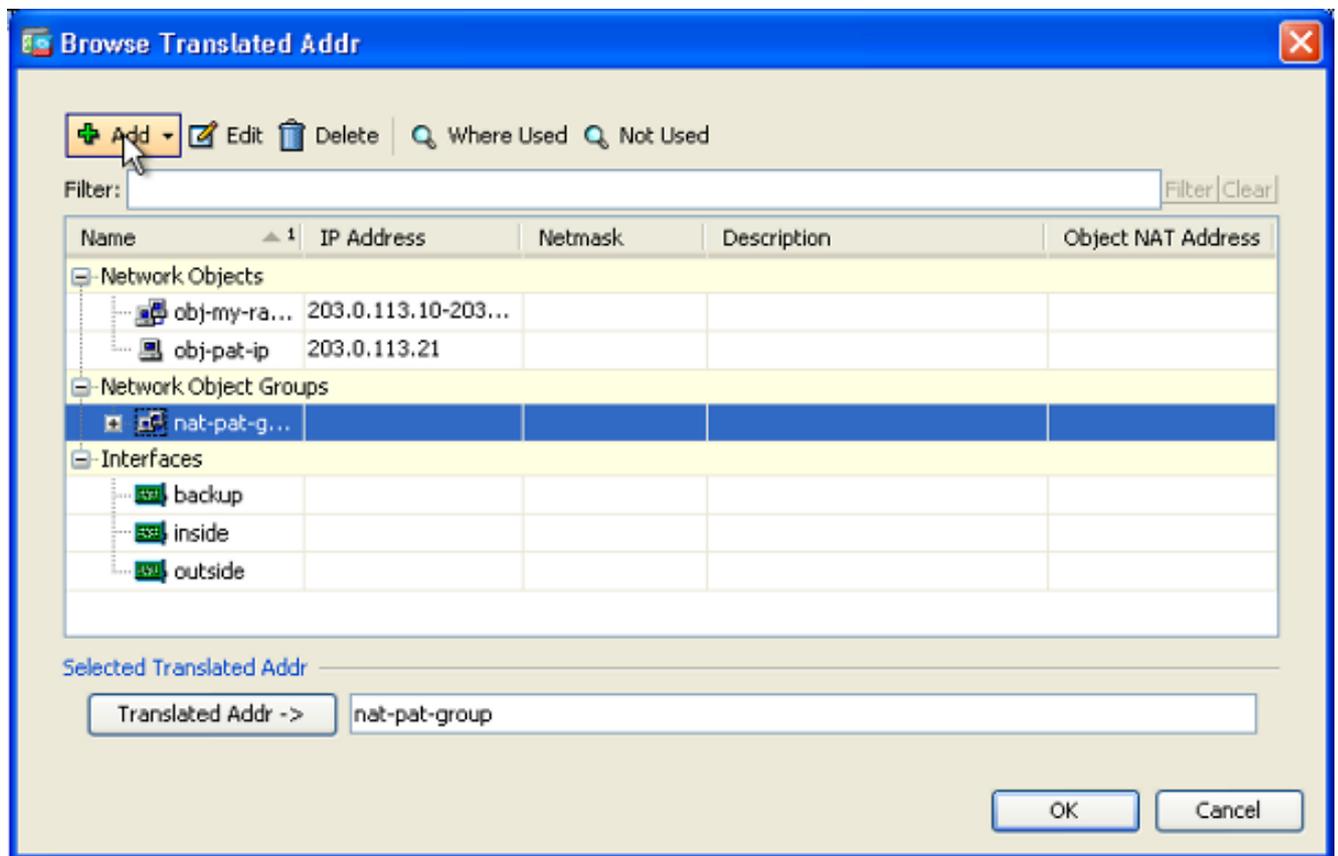
Members in Group:

Name	IP Address	Netmask/Prefix L
obj-pat-ip	203.0.113.21	
obj-my-range	203.0.113.10-203.0.113.21	

Add >>

<< Remove

3. Scegliere la regola NAT configurata e modificare l'indirizzo tradotto in modo che diventi il gruppo appena configurato 'nat-pat-group' (in precedenza 'obj-my-range'). Fare clic su **OK**.



4. Fare clic su **OK** per aggiungere la regola NAT. Per selezionare le interfacce di origine e di destinazione, fare clic su **Advanced** (Avanzate).

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: nat-pat-group

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

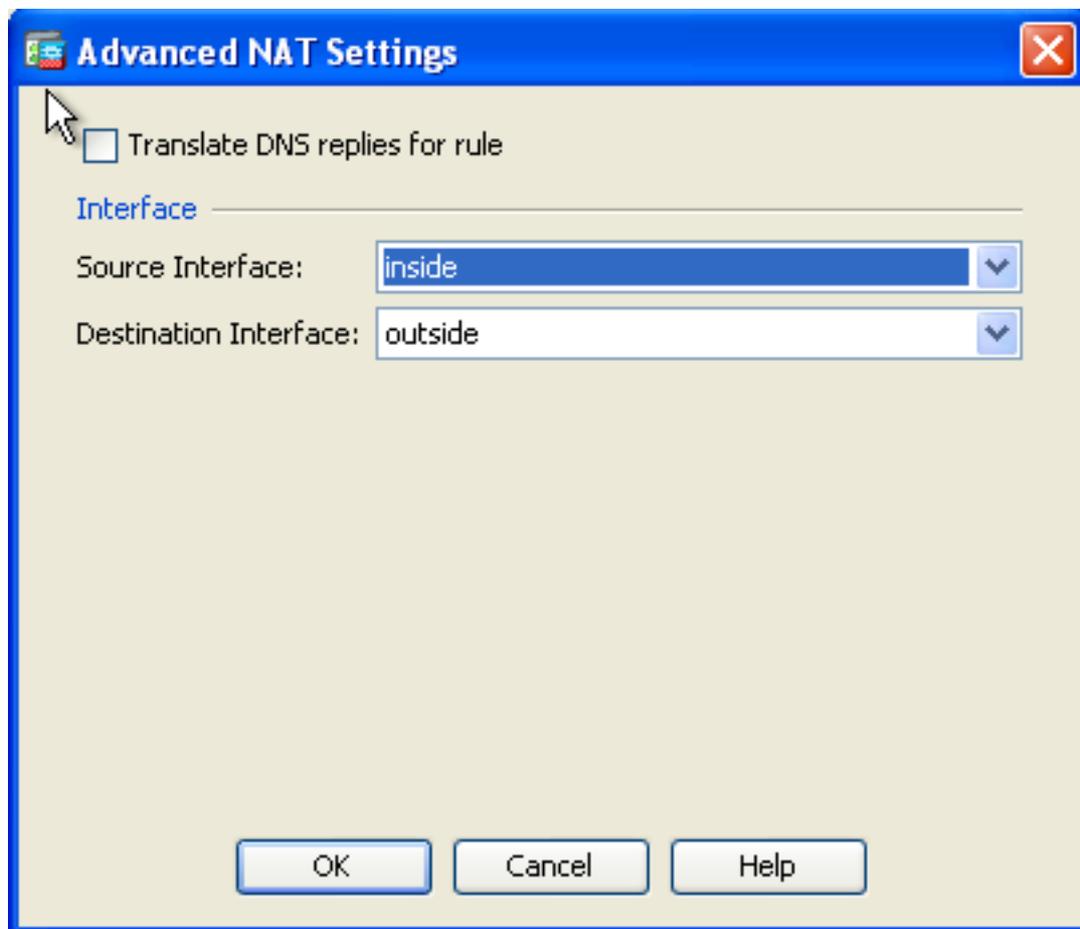
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

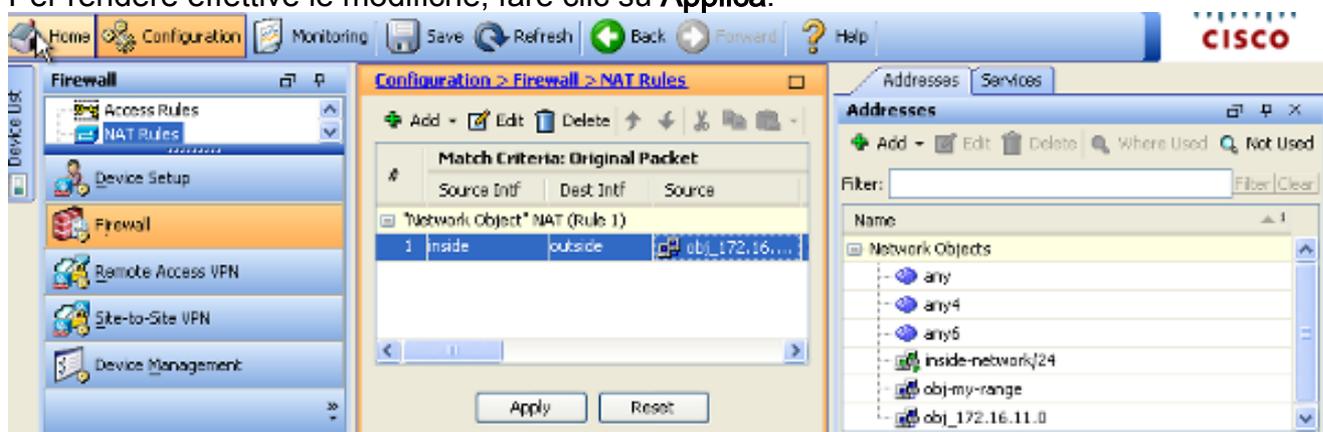
Advanced...

OK Cancel Help

5. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Fare clic su **OK**.



6. Per rendere effettive le modifiche, fare clic su **Applica**.



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

```
object network obj-my-range
range 203.0.113.10 203.0.113.20
```

```
object network obj-pat-ip
host 203.0.113.21
```

```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

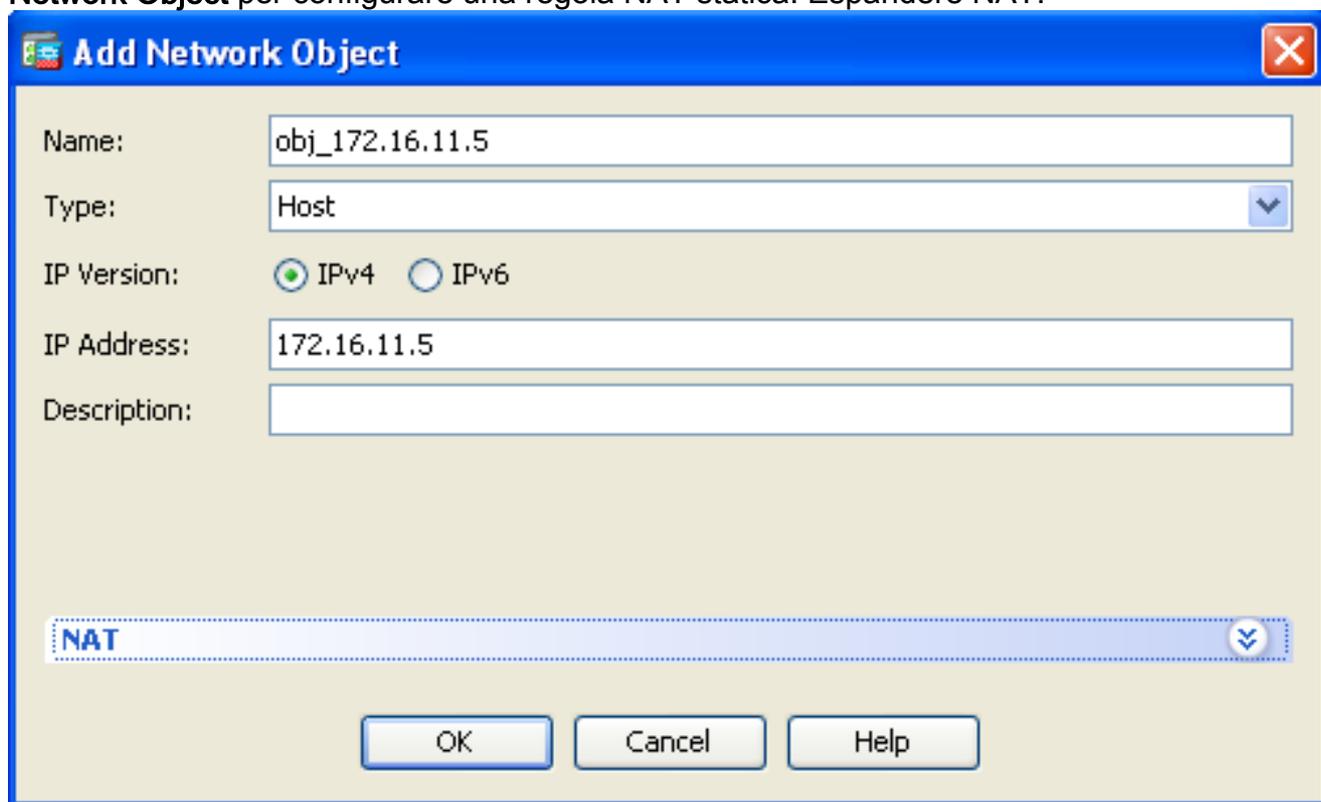
```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

nat (inside,outside) dynamic nat-pat-group

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 può avere un indirizzo IP privato che non può essere instradato 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 eseguire questa operazione, è necessario convertire l'indirizzo IP del server privato in un indirizzo IP pubblico. Nell'esempio viene descritto come implementare il protocollo NAT statico bidirezionale per convertire da 172.16.11.5 a 203.0.113.5.

1. Scegliere **Configurazione > Firewall > Regole NAT**. Fare clic su **Add**, quindi selezionare **Network Object** per configurare una regola NAT statica. Espandere NAT.



2. Selezionare la casella di controllo **Aggiungi regole di conversione automatica indirizzi**. Nell'elenco a discesa Tipo (Type), selezionate **Statico (Static)**. Nel campo Indirizzo tradotto, immettere l'indirizzo IP. Per selezionare le interfacce di origine e di destinazione, fare clic su **Advanced (Avanzate)**.

Add Network Object

Name: obj_172.16.11.5

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.16.11.5

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.113.5

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

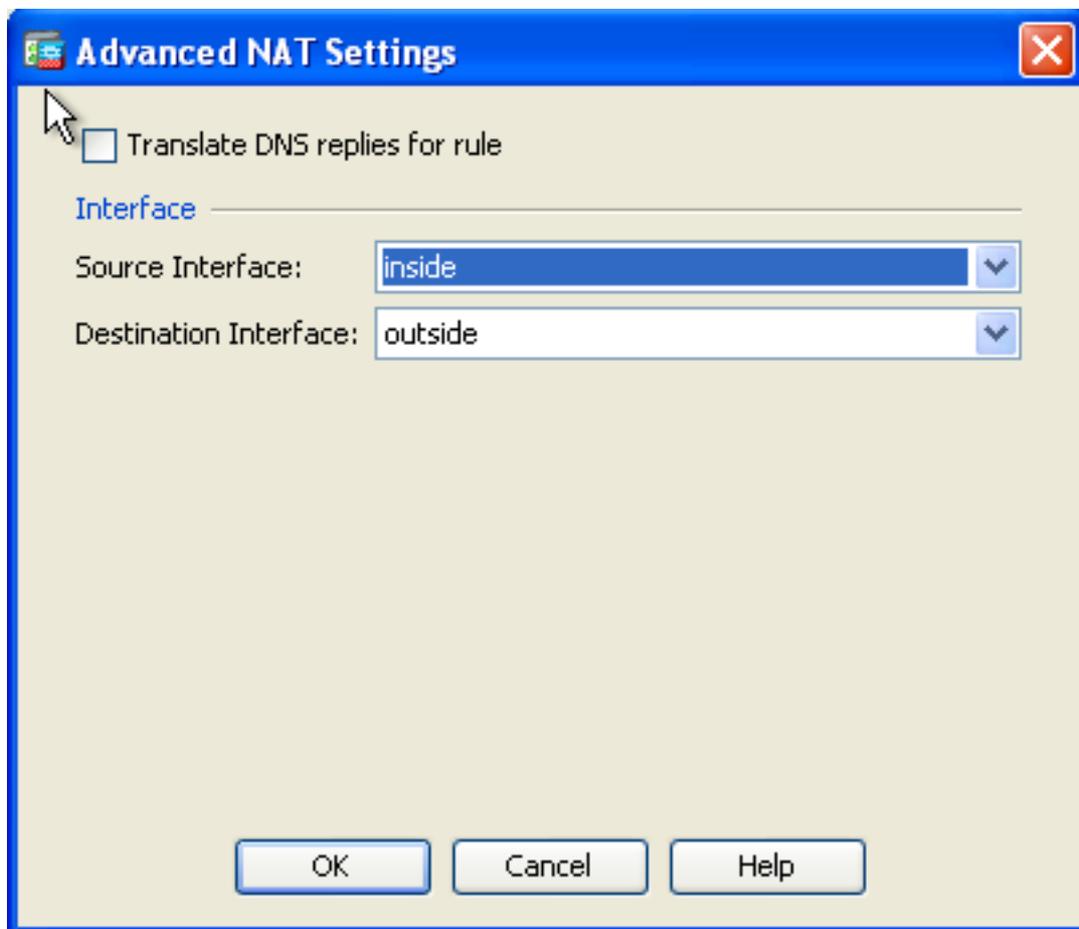
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

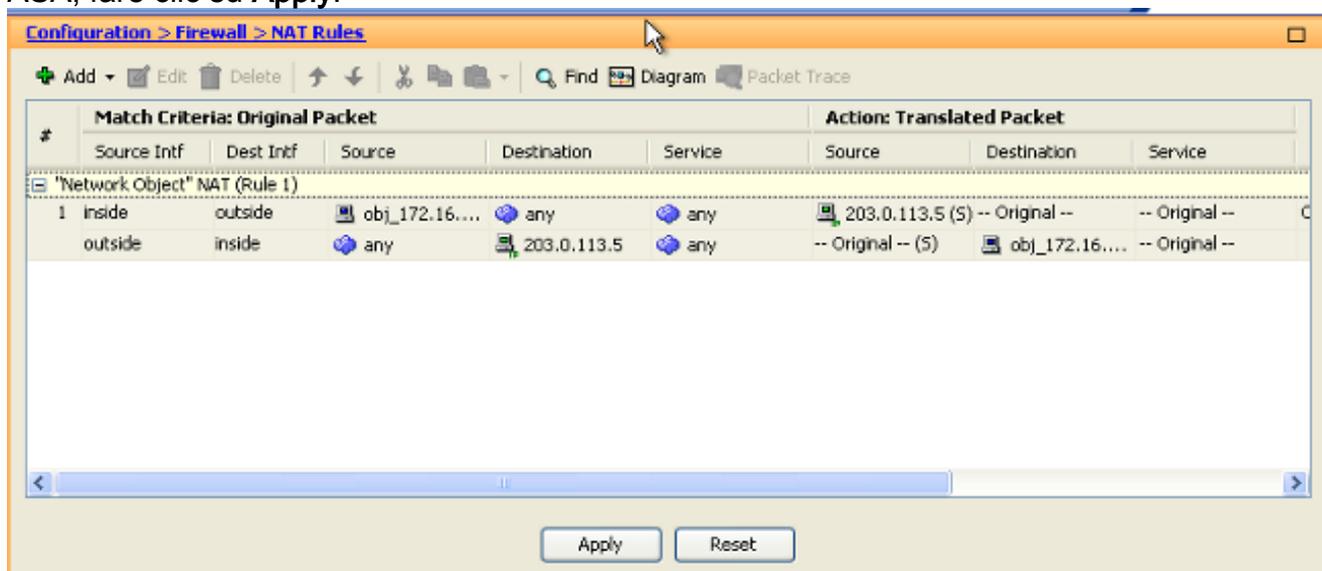
Advanced...

OK Cancel Help

3. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Fare clic su **OK**.



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



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

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

NAT identità statica

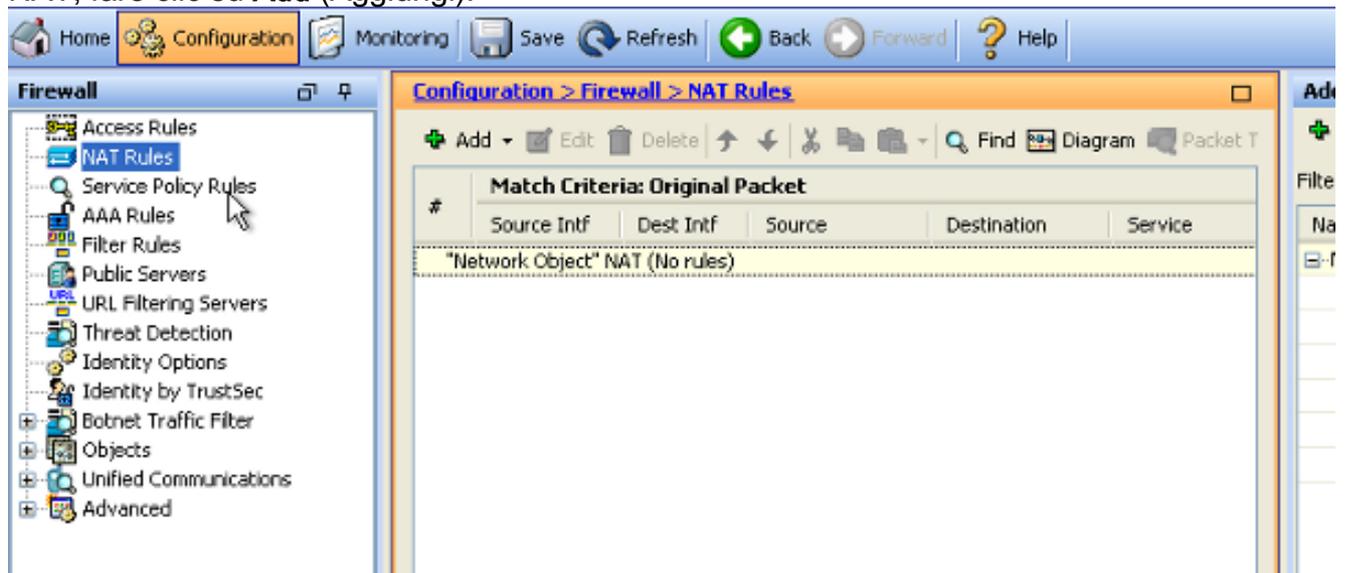
L'esenzione NAT è una funzionalità utile quando gli utenti interni tentano di accedere a un host/server VPN remoto o a un host/server ospitato dietro un'altra interfaccia dell'ASA senza

completare un'esenzione NAT. A tal fine, il server interno, che dispone di un indirizzo IP privato, può essere tradotto a se stesso e che a sua volta può accedere alla destinazione che esegue un NAT.

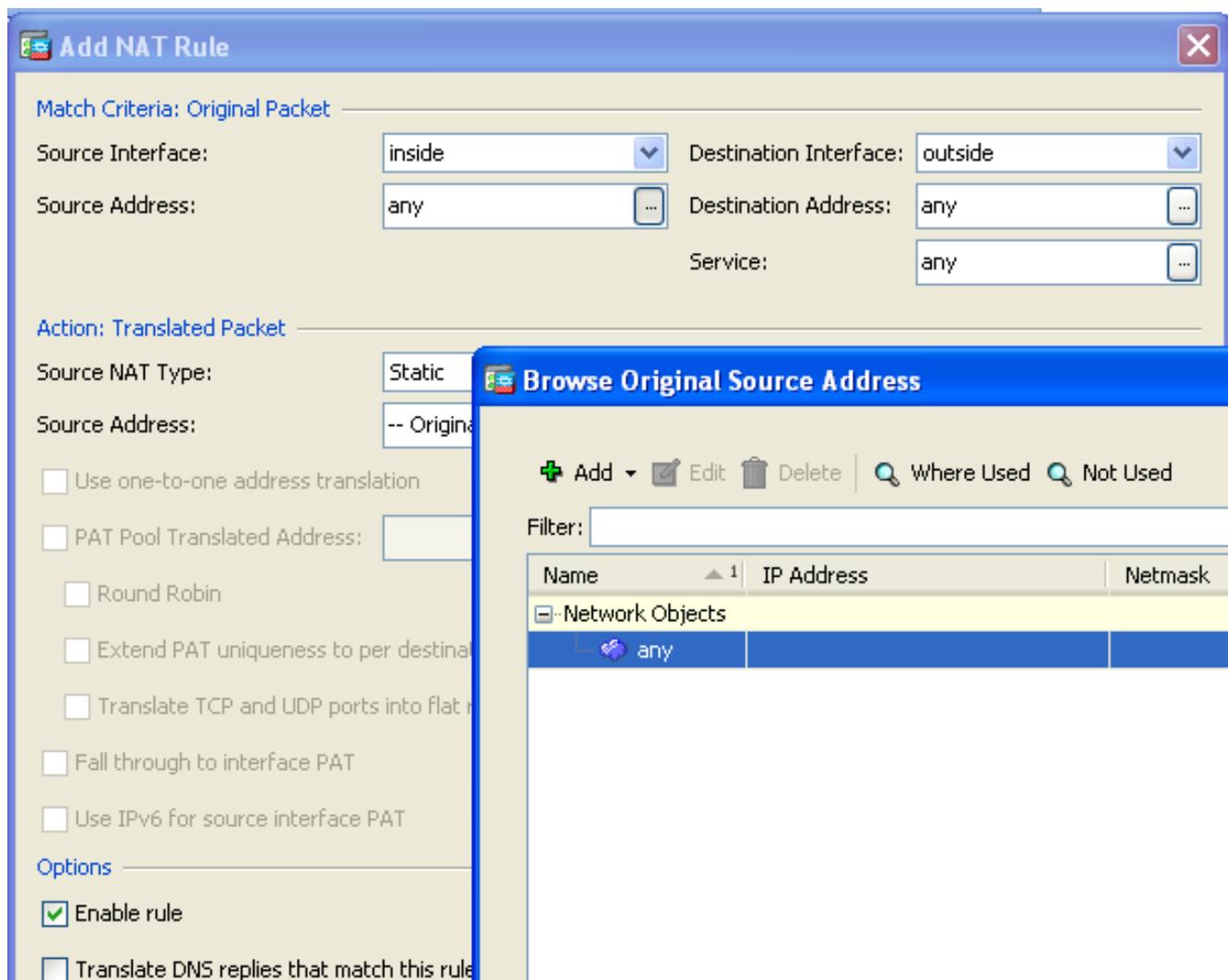
Nell'esempio, l'host interno 172.16.11.15 deve accedere al server VPN remoto 172.20.21.15.

Completare questi passaggi per consentire agli host interni di accedere alla rete VPN remota con il completamento di un NAT:

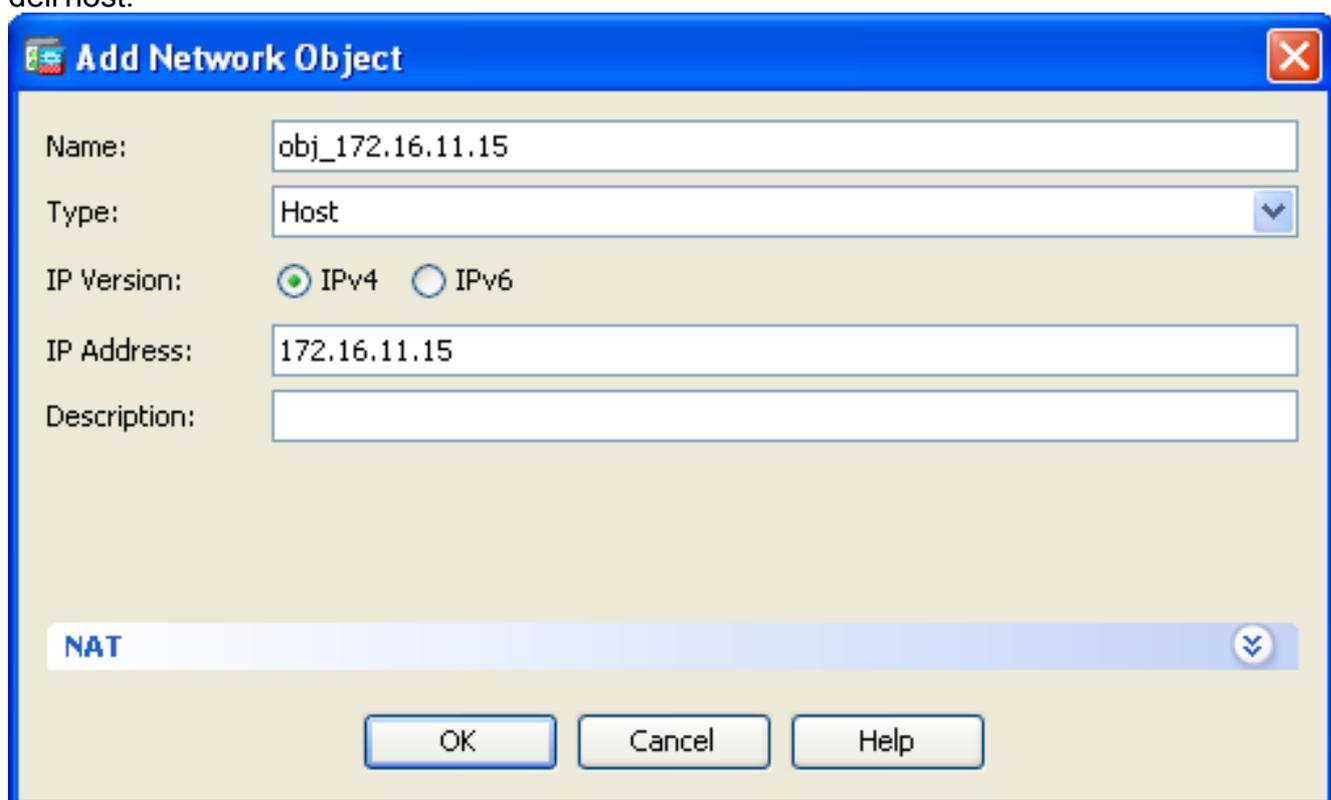
1. Scegliere **Configurazione > Firewall > Regole NAT**. Per configurare una regola di esenzione NAT, fare clic su **Add (Aggiungi)**.



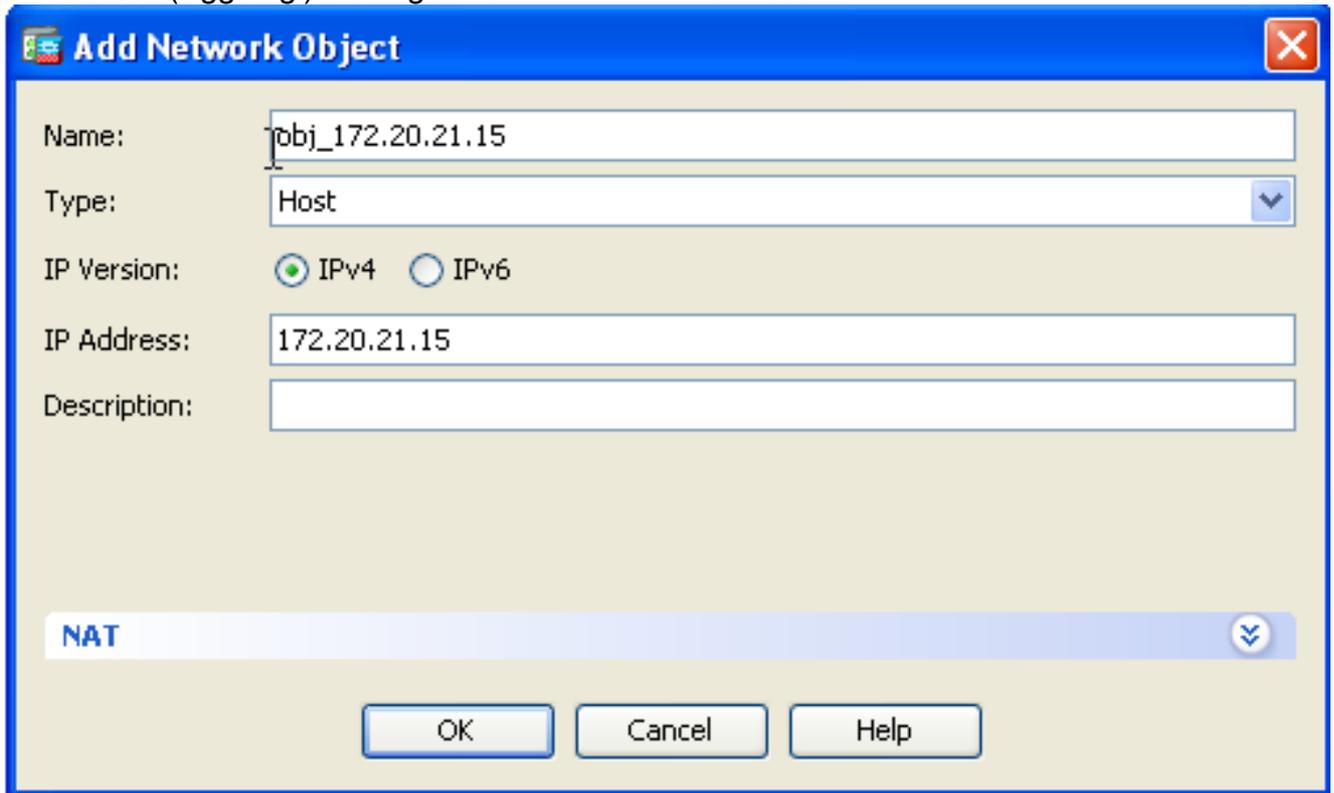
2. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Nel campo Source Address (Indirizzo di origine), scegliere la voce appropriata.



3. Per aggiungere un oggetto di rete, fare clic su **Add** (Aggiungi). Configurare l'indirizzo IP dell'host.



4. Analogamente, sfogliare l'**indirizzo di destinazione**. Per aggiungere un oggetto di rete, fare clic su **Add** (Aggiungi). Configurare l'indirizzo IP dell'host.



Add Network Object

Name: obj_172.20.21.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.20.21.15

Description:

NAT

OK Cancel Help

5. Scegliere gli oggetti Source Address e Destination Address configurati. Selezionare le caselle di controllo **Disabilita ARP proxy** sull'interfaccia di uscita e **Ricerca tabella route** per individuare l'interfaccia di uscita. Fare clic su **OK**.

Add NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address: Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

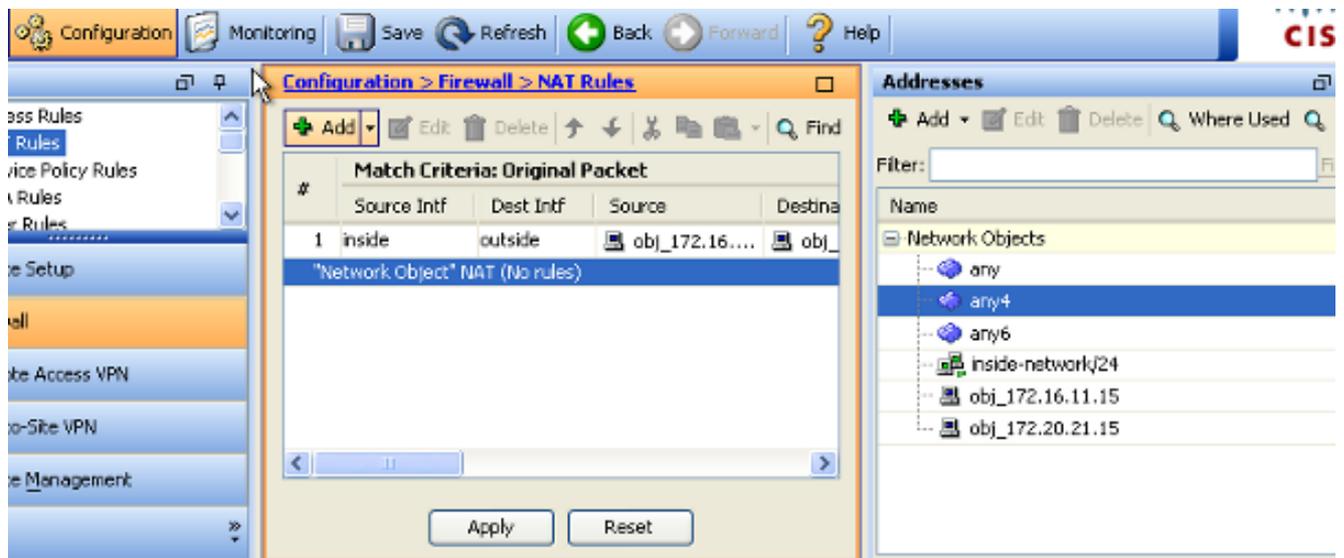
Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

6. Per rendere effettive le modifiche, fare clic su **Applica**.



Questo è l'output CLI equivalente per la configurazione NAT Exempt o Identity NAT:

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15
```

```
nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

Reindirizzamento delle porte (inoltro) con

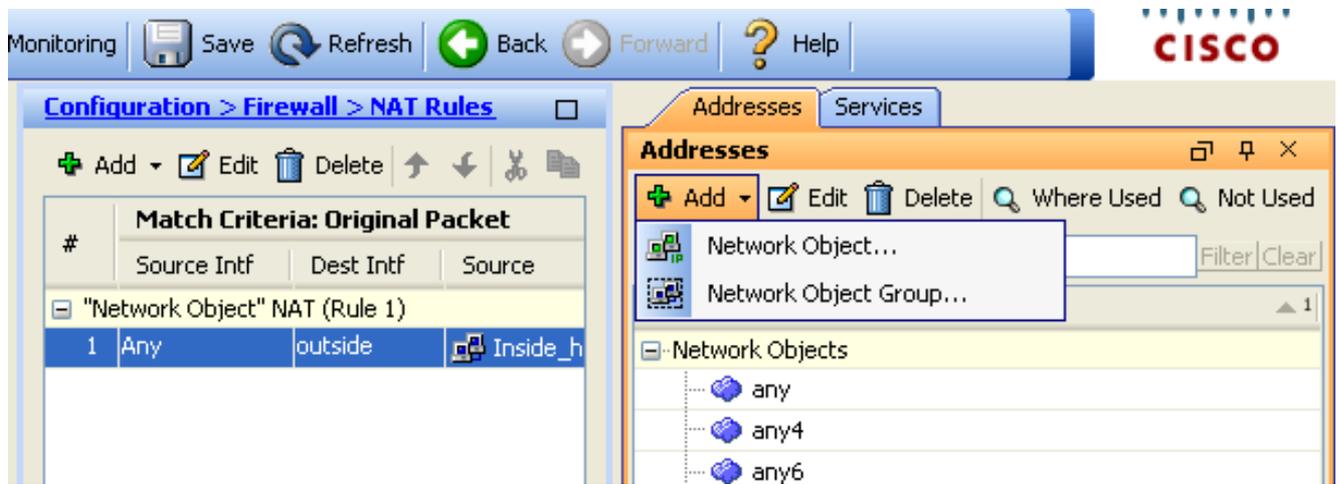
L'inoltro o il reindirizzamento delle porte è una funzionalità utile quando gli utenti esterni tentano di accedere a un server interno su una porta specifica. A tale scopo, il server interno, che dispone di un indirizzo IP privato, può essere convertito in un indirizzo IP pubblico che a sua volta può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

In questo esempio, l'utente esterno desidera accedere al server SMTP, 203.0.113.15 sulla porta 25. Questa operazione viene eseguita in due passaggi:

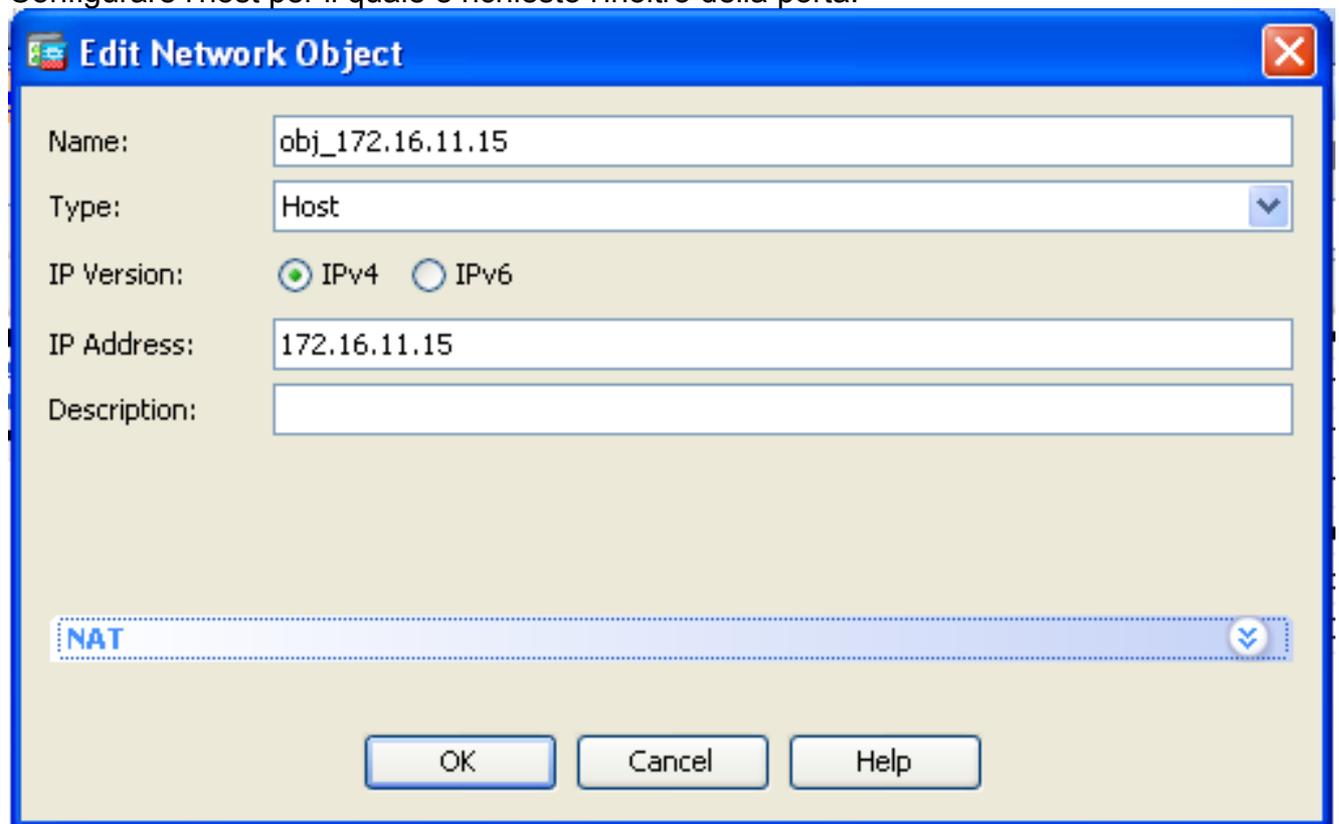
1. Tradurre il server di posta interno, 172.16.11.15 sulla porta 25, nell'indirizzo IP pubblico, 203.0.113.15 sulla porta 25.
2. Consentire l'accesso al server di posta pubblica, 203.0.113.15 sulla porta 25.

Quando l'utente esterno tenta di accedere al server, 203.0.113.15 alla porta 25, il traffico viene reindirizzato al server di posta interno, 172.16.11.15 alla porta 25.

1. Scegliere **Configurazione > Firewall > Regole NAT**. Fare clic su **Add**, quindi selezionare **Network Object** per configurare una regola NAT statica.



2. Configurare l'host per il quale è richiesto l'inoltro della porta.



3. Espandere NAT. Selezionare la casella di controllo **Aggiungi regole di conversione automatica degli indirizzi**. Nell'elenco a discesa Tipo (Type), selezionate **Statico (Static)**. Nel campo Indirizzo tradotto, immettere l'indirizzo IP. Per selezionare le interfacce di servizio, origine e destinazione, fare clic su **Advanced (Avanzate)**.

Edit Network Object

Name: obj_172.16.11.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.16.11.15

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.115.15

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

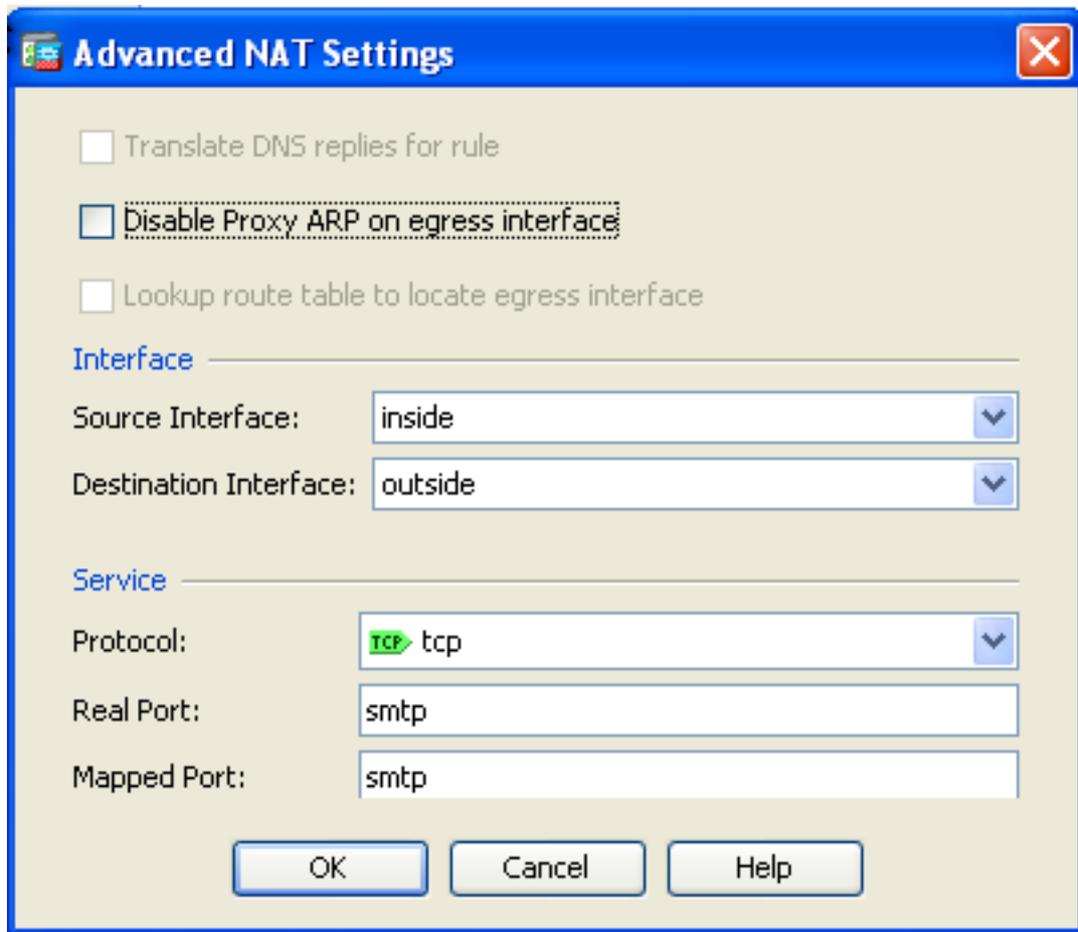
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

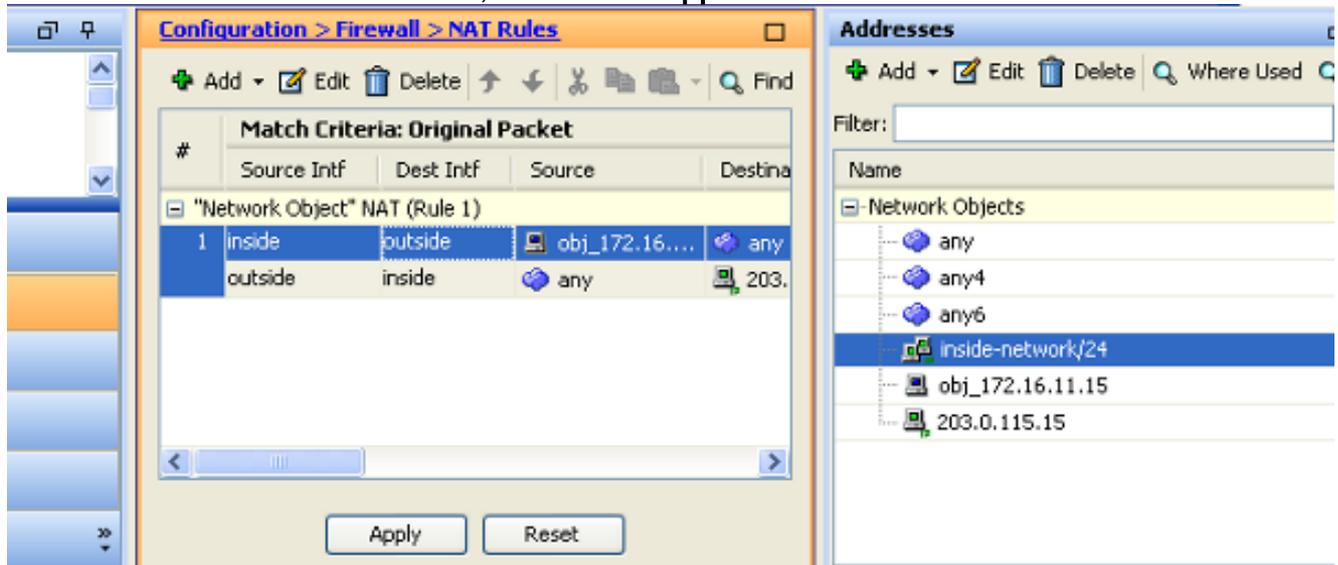
Advanced...

OK Cancel Help

4. Negli elenchi a discesa Interfaccia di origine e Interfaccia di destinazione, scegliere le interfacce appropriate. Configurare il servizio. Fare clic su **OK**.



5. Per rendere effettive le modifiche, fare clic su **Applica**.



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

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

[Cisco CLI Analyzer \(solo utenti registrati\) supporta alcuni comandi show](#). Usare Cisco CLI

Analyzer per visualizzare un'analisi dell'output del comando **show**.

Accedere a un sito Web tramite HTTP tramite un browser. In questo esempio viene usato un sito ospitato all'indirizzo 198.51.100.100. Se la connessione ha esito positivo, questo output può essere visualizzato sulla CLI di ASA.

Connessione

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

L'ASA è un firewall con stato e il traffico di ritorno dal server Web può attraversare nuovamente il firewall perché corrisponde a una **connessione** nella tabella delle connessioni del firewall. Il traffico che corrisponde a una connessione preesistente può passare attraverso il firewall senza essere bloccato da un ACL di interfaccia.

Nell'output precedente, il client sull'interfaccia interna ha stabilito una connessione con l'host 198.51.100.100 dall'interfaccia esterna. Questa connessione viene effettuata con il protocollo TCP ed è rimasta inattiva per sei secondi. I flag di connessione indicano lo stato corrente della connessione. Per ulteriori informazioni sui flag di connessione, consultare [Flag di connessione TCP ASA](#).

Syslog

```
ASA(config)# show log | in 172.16.11.5
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

Il firewall ASA genera syslog durante il normale funzionamento. L'intervallo dei syslog è espresso in dettaglio in base alla configurazione di registrazione. L'output mostra due syslog visualizzati al livello sei o al livello "informativo".

In questo esempio vengono generati due syslog. Il primo è un messaggio di registro che indica che il firewall ha creato una traduzione, in particolare una traduzione TCP dinamica (PAT). Indica l'indirizzo IP e la porta di origine, nonché l'indirizzo IP e la porta convertiti, quando il traffico attraversa le interfacce interna ed esterna.

Il secondo syslog indica che il firewall ha creato una connessione nella relativa tabella di connessione per il traffico specifico tra il client e il server. Se il firewall è stato configurato per bloccare questo tentativo di connessione o altri fattori hanno impedito la creazione della connessione (vincoli di risorse o una possibile configurazione errata), il firewall non genererà un registro che indichi che la connessione è stata creata. Viene invece registrato un motivo per cui la connessione viene negata o un'indicazione relativa al fattore che ha impedito la creazione della connessione.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80
```

```
--Omitted--
```

```
Result:
```

```
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La funzionalità di tracciamento dei pacchetti sull'appliance ASA consente di specificare un pacchetto *simulato* e di visualizzare tutte le fasi, i controlli e le funzioni attraversati dal firewall quando elabora il traffico. Con questo strumento, è utile identificare un esempio di traffico che si ritiene *possa* essere autorizzato a passare attraverso il firewall e utilizzare quel 5-tuple per simulare il traffico. Nell'esempio precedente, il packet tracer viene usato per simulare un tentativo di connessione che soddisfa i seguenti criteri:

- Il pacchetto simulato arriva all'interno.
- Il protocollo utilizzato è TCP.
- L'indirizzo IP del client simulato è 172.16.11.5.
- Il client invia il traffico proveniente dalla porta 1234.
- Il traffico è destinato a un server all'indirizzo IP 198.51.100.100.
- Il traffico è destinato al porto 80.

Nel comando non è stata menzionata alcuna interfaccia esterna. Questo è dovuto al design del tracer dei pacchetti. Lo strumento indica il modo in cui il firewall elabora il tipo di tentativo di connessione, incluse le modalità di instradamento e di uscita dall'interfaccia. Per ulteriori informazioni su packet tracer, vedere [Analisi dei pacchetti con Packet Tracer](#).

Acquisisci

Applica acquisizione

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA#show capture capin
```

```
3 packets captured
```

```
1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA#show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
```

```
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Il firewall ASA può acquisire il traffico in entrata o in uscita dalle interfacce. Questa funzionalità di acquisizione è fantastica perché può dimostrare in modo definitivo se il traffico arriva a un firewall o se ne esce. L'esempio precedente mostrava la configurazione di due clip chiamate capin e cappuccio rispettivamente sulle interfacce interna ed esterna. I comandi di acquisizione hanno utilizzato la parola chiave match, che consente di specificare il traffico da acquisire.

Per il capin di acquisizione, è stato indicato che si desidera far corrispondere il traffico visualizzato sull'interfaccia interna (in entrata o in uscita) che corrisponde all'host TCP 172.16.11.5 host 198.51.100.100. In altre parole, si desidera acquisire il traffico TCP inviato dall'host 172.16.11.5 all'host 198.51.100.100 o viceversa. L'utilizzo della parola chiave match consente al firewall di acquisire il traffico in modo bidirezionale. Il comando capture definito per l'interfaccia esterna non fa riferimento all'indirizzo IP del client interno perché il firewall esegue PAT su tale indirizzo IP del client. Di conseguenza, non è possibile stabilire una corrispondenza con l'indirizzo IP del client. Nell'esempio viene invece utilizzato any (qualsiasi) per indicare che tutti gli indirizzi IP possibili soddisferanno la condizione.

Dopo aver configurato le clip, tentare di stabilire nuovamente la connessione e continuare a visualizzarle con il comando **show capture <nome_acquisizione>**. In questo esempio, è possibile notare che il client è stato in grado di connettersi al server come evidenziato dall'handshake TCP a 3 vie rilevato nelle acquisizioni.

Risoluzione dei problemi

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

Informazioni correlate

- [Esempio di configurazione del syslog ASA](#)
- [Esempio di acquisizione di pacchetti ASA con CLI e configurazione ASDM](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

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