

使用NAT配置ASA版本9埠轉發

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[允許內部主機通過PAT訪問外部網路](#)

[允許內部主機通過NAT訪問外部網路](#)

[允許不受信任的主機訪問受信任網路中的主機](#)

[靜態身份NAT](#)

[使用靜態的連線埠重新導向 \(轉送 \)](#)

[驗證](#)

[連線](#)

[系統日誌](#)

[Packet Tracer](#)

[CAPTURE](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何使用CLI或調適型安全裝置管理員(ASDM)，在調適型安全裝置(ASA)軟體版本9.x中設定連線埠重新導向 (轉送) 和外部網路位址轉譯(NAT)功能。

請參閱[Cisco ASA系列防火牆ASDM配置指南](#)瞭解更多資訊。

必要條件

需求

請參閱[配置管理訪問](#)以允許由ASDM配置裝置。

採用元件

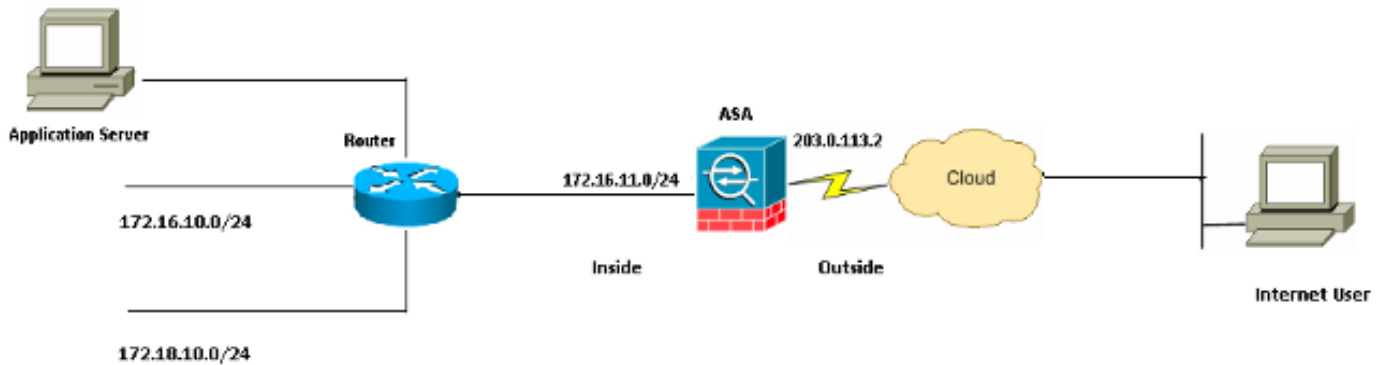
本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 5525系列安全裝置軟體版本9.x及更高版本
- ASDM 7.x及更高版本

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。"

設定

網路圖表



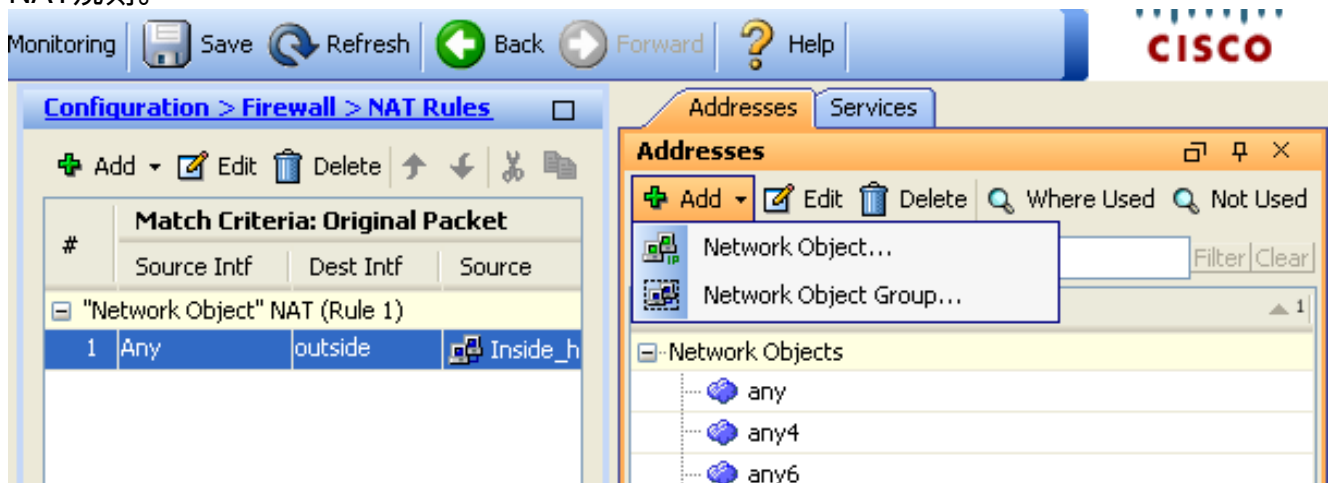
此配置中使用的IP地址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

允許內部主機通過PAT訪問外部網路

如果您希望內部主機共用一個公共地址進行轉換，請使用埠地址轉換(PAT)。最簡單的PAT配置之一涉及將所有內部主機轉換為類似於外部介面IP地址。當ISP提供的可路由IP地址的數量限制為少數幾個或只有一個時，通常使用這種PAT配置。

完成以下步驟，以允許內部主機使用PAT訪問外部網路：

1. 選擇Configuration > Firewall > NAT Rules。按一下Add，然後選擇Network Object以配置動態NAT規則。



2. 配置需要動態PAT的網路/主機/範圍。在此示例中，已選擇一個內部子網。對於要以此方式轉換的其他子網，可重複此過程。

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. 展開NAT。選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉選單中，選擇動態PAT (隱藏)。在Translated Addr欄位中，選擇反映外部介面的選項。按一下「Advanced」。

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

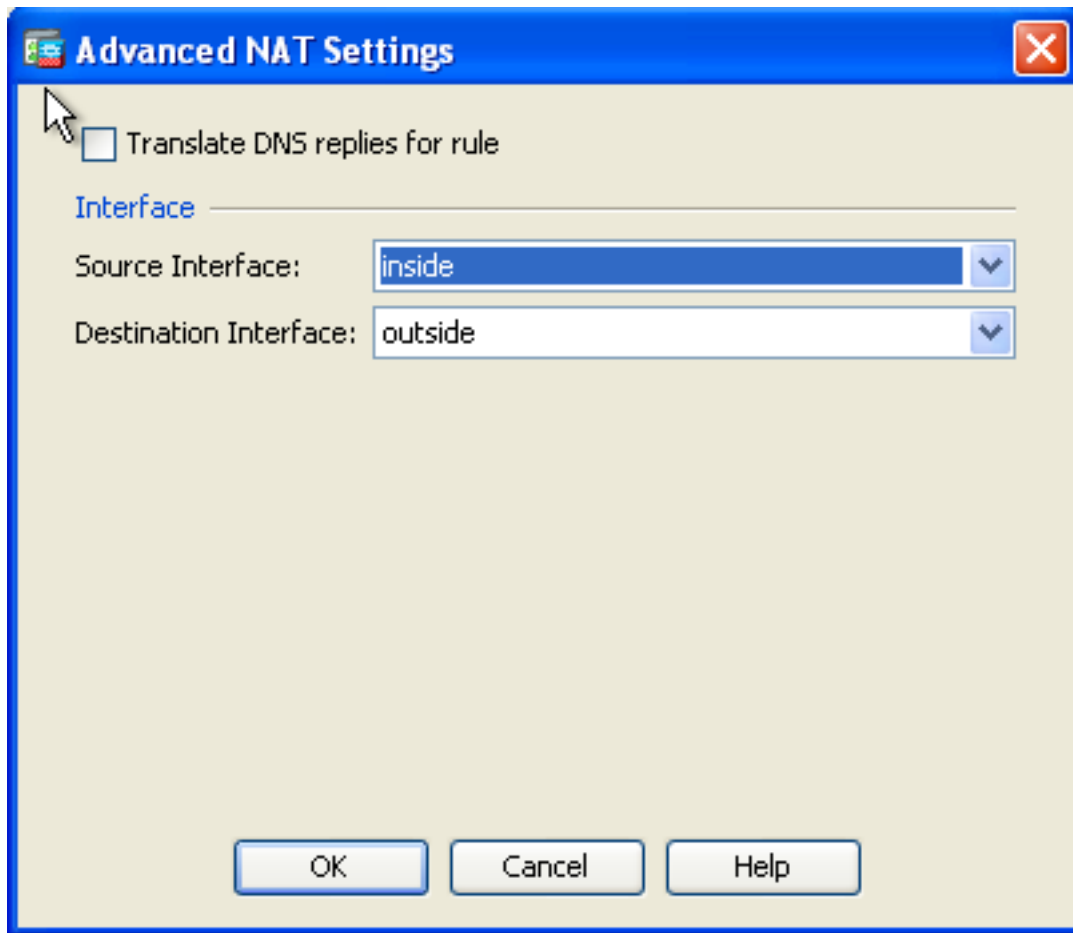
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。按一下OK，然後按一下Apply以使更改生效。



這是此PAT配置的等效的CLI輸出：

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

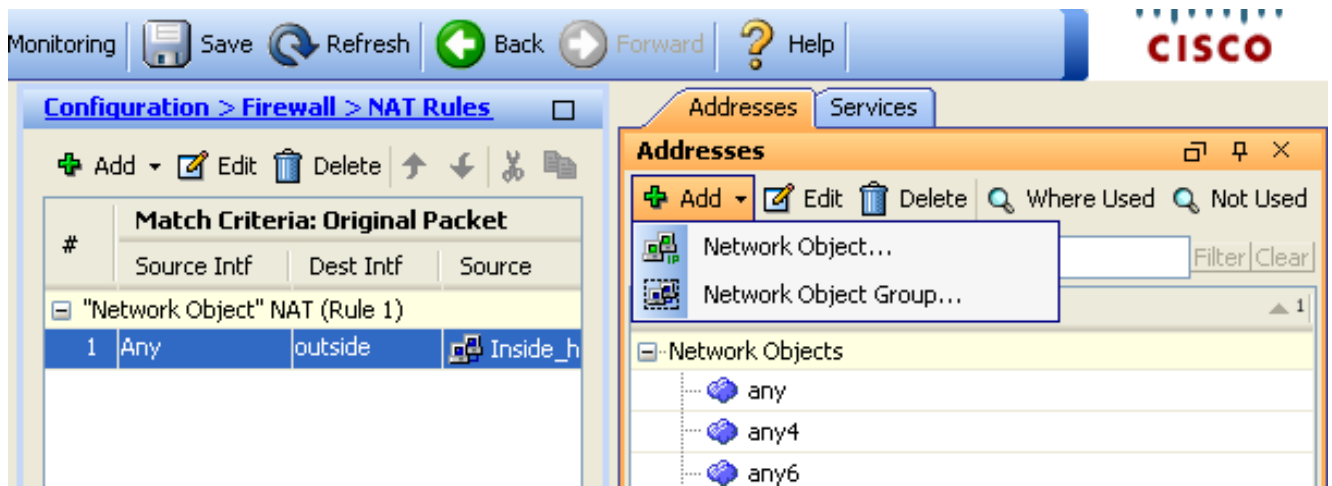
允許內部主機通過NAT訪問外部網路

您可以通過配置動態NAT規則，允許一組內部主機/網路訪問外部世界。與PAT不同，動態NAT從地址池分配轉換的地址。因此，一台主機對映到其自己的轉換IP地址，兩台主機不能共用同一個轉換IP地址。

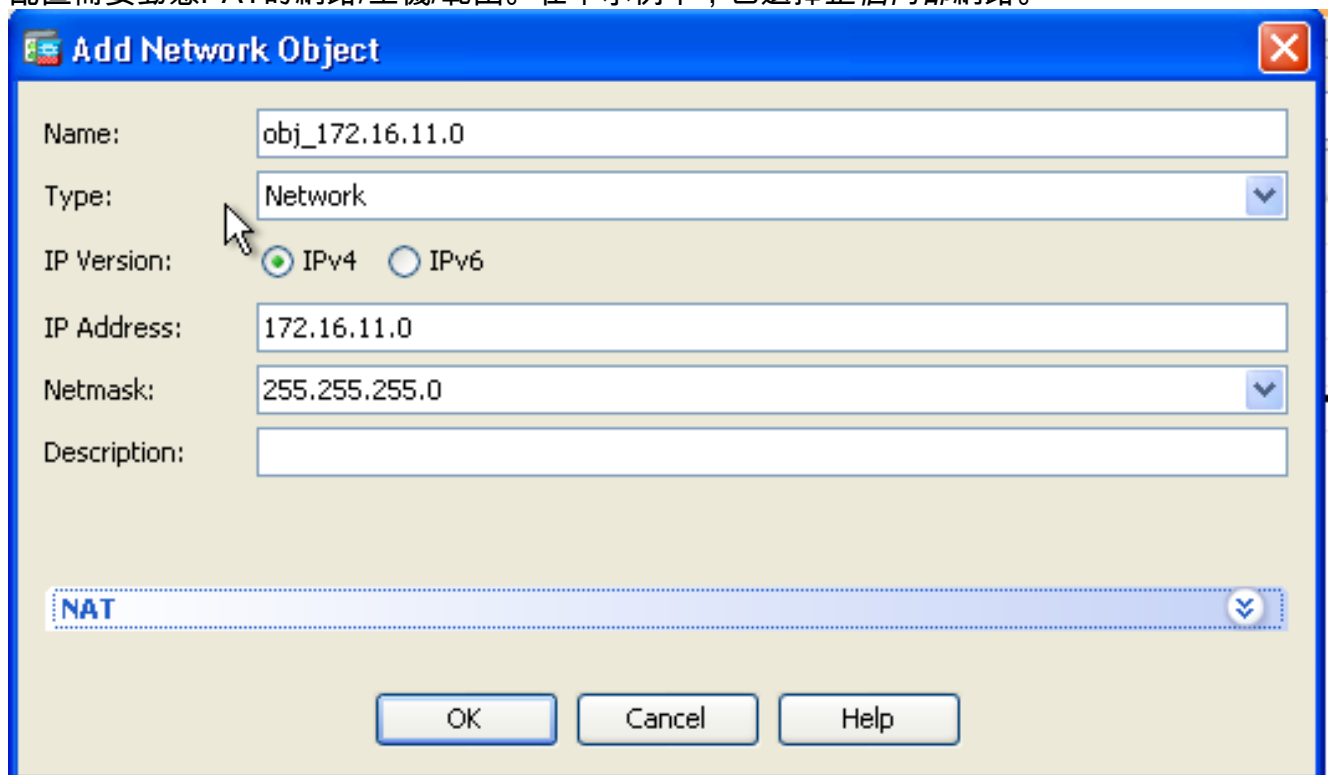
為此，您需要選擇要授予訪問許可權的主機/網路的實際地址，然後必須將其對映到已轉換的IP地址池。

完成以下步驟，以允許內部主機通過NAT訪問外部網路：

1. 選擇**Configuration > Firewall > NAT Rules**。按一下**Add**，然後選擇**Network Object**以配置動態NAT規則。



2. 配置需要動態PAT的網路/主機/範圍。在本示例中，已選擇整個內部網路。



3. 展開NAT。選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉式清單中選擇「動態」。在Translated Addr欄位中，選擇適當的選項。按一下「Advanced」。

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

- 按一下**Add**以新增網路對象。在「型別」下拉選單中，選擇「範圍」。在Start Address和End Address欄位中，輸入起始和結束PAT IP地址。按一下「OK」（確定）。

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. 在Translated Addr欄位中，選擇地址對象。按一下**Advanced**以選擇來源介面和目的地介面。

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: obj-my-range

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

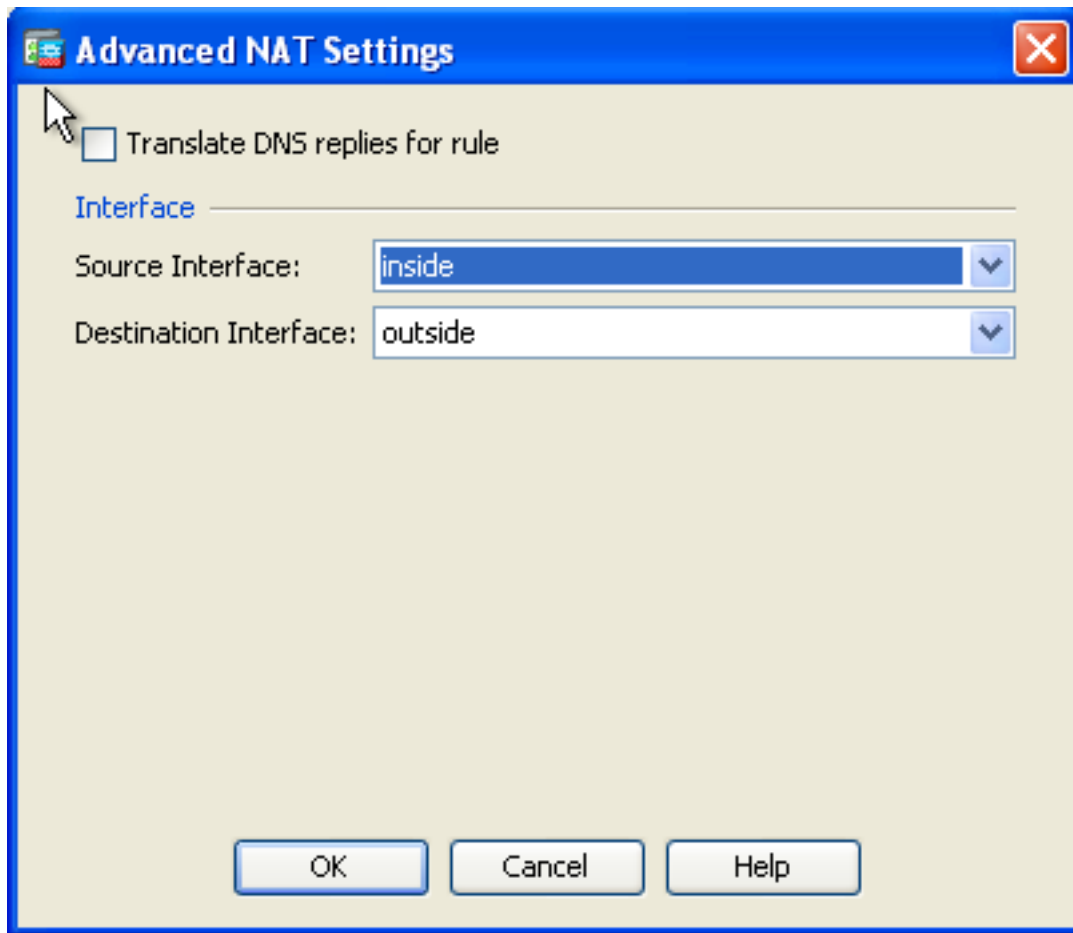
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

6. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。按一下**OK**，然後按一下**Apply**以使更改生效。



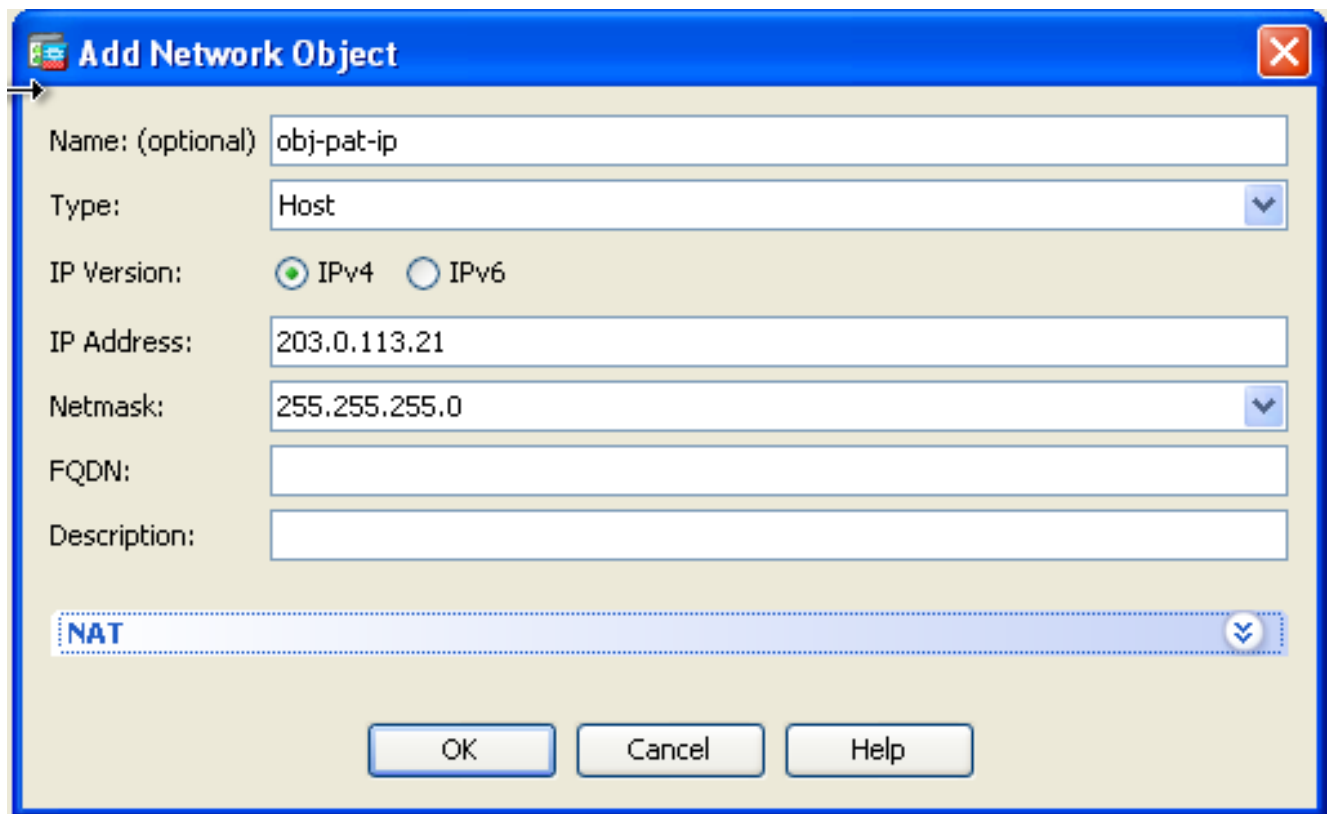
這是此ASDM配置的等效的CLI輸出：

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

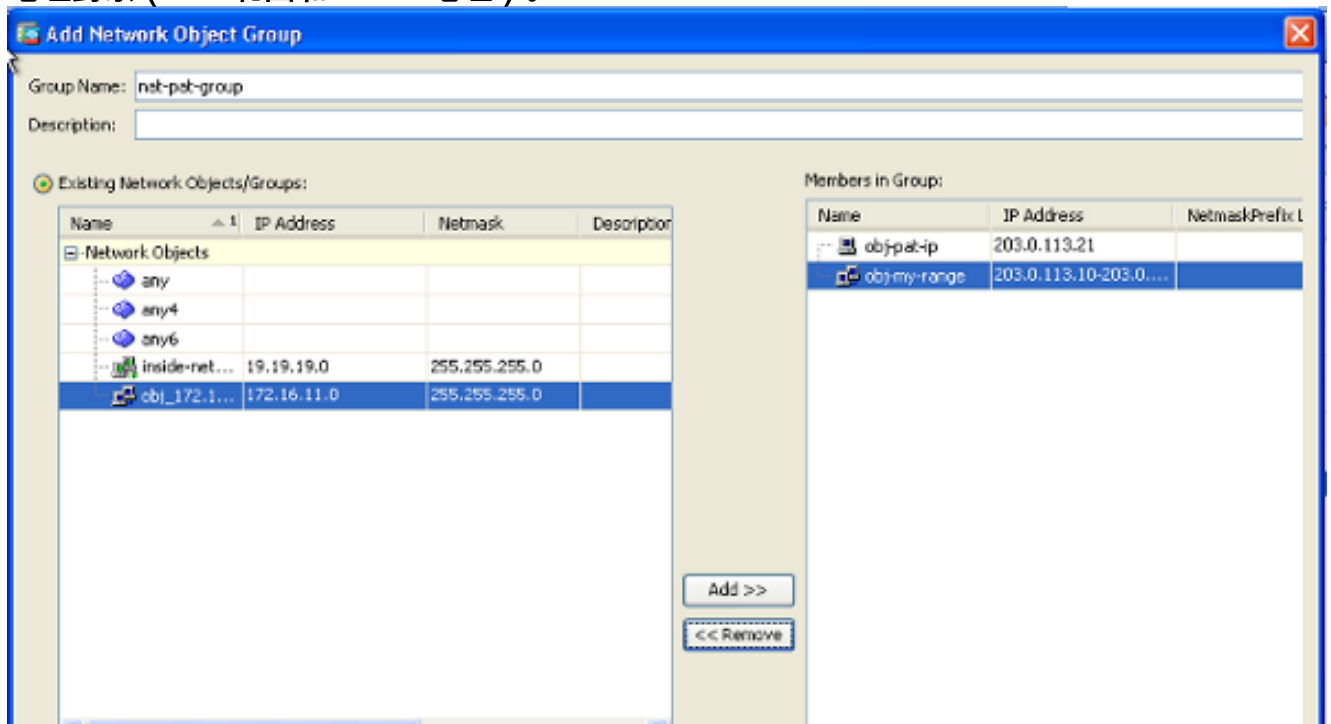
```
object network obj_172.16.11.0  
subnet 172.16.11.0 255.255.255.0  
nat(inside,outside) dynamic obj-my-range
```

根據此配置，172.16.11.0網路中的主機將轉換為NAT池(203.0.113.10 - 203.0.113.20)中的任何IP地址。如果對映池的地址少於實際組的地址，則地址可能會用盡。因此，您可以嘗試使用動態PAT備份實施動態NAT，也可以嘗試擴展當前池。

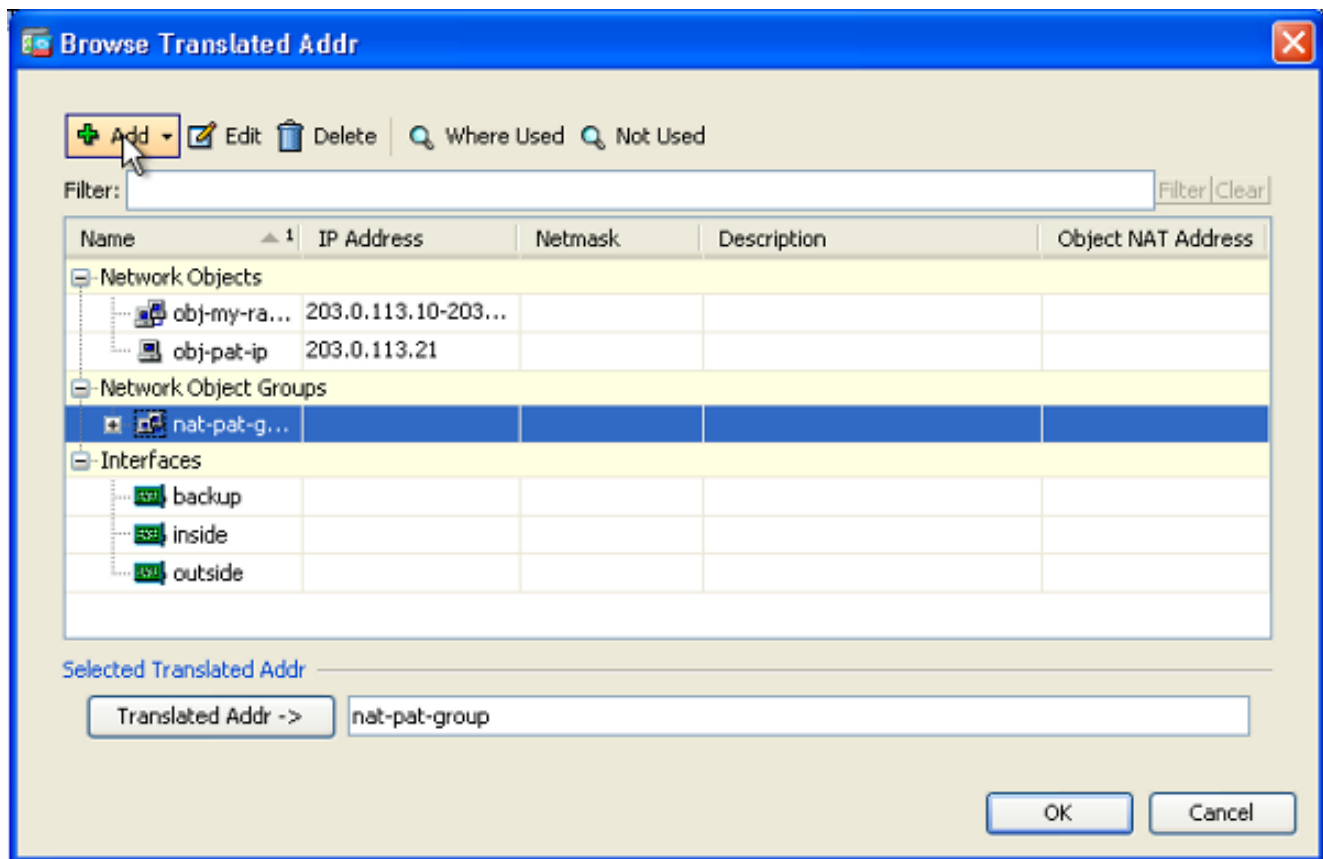
1. 在先前的配置中重複步驟1到3，然後再次按一下**Add**以新增網路對象。在「型別」下拉選單中，選擇**主機**。在IP Address欄位中，輸入PAT備份IP地址。按一下「**OK**」（確定）。



2. 按一下**Add**以新增網路對象組。在Group Name欄位中，輸入組名稱，並在組中同時新增兩個地址對象（NAT範圍和PAT IP地址）。



3. 選擇配置的NAT規則，並將Translated Addr更改為新配置的組「nat-pat-group」（以前為「obj-my-range」）。按一下「OK」（確定）。



4. 按一下**OK**以新增NAT規則。按一下**Advanced**以選擇來源介面和目的地介面。

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

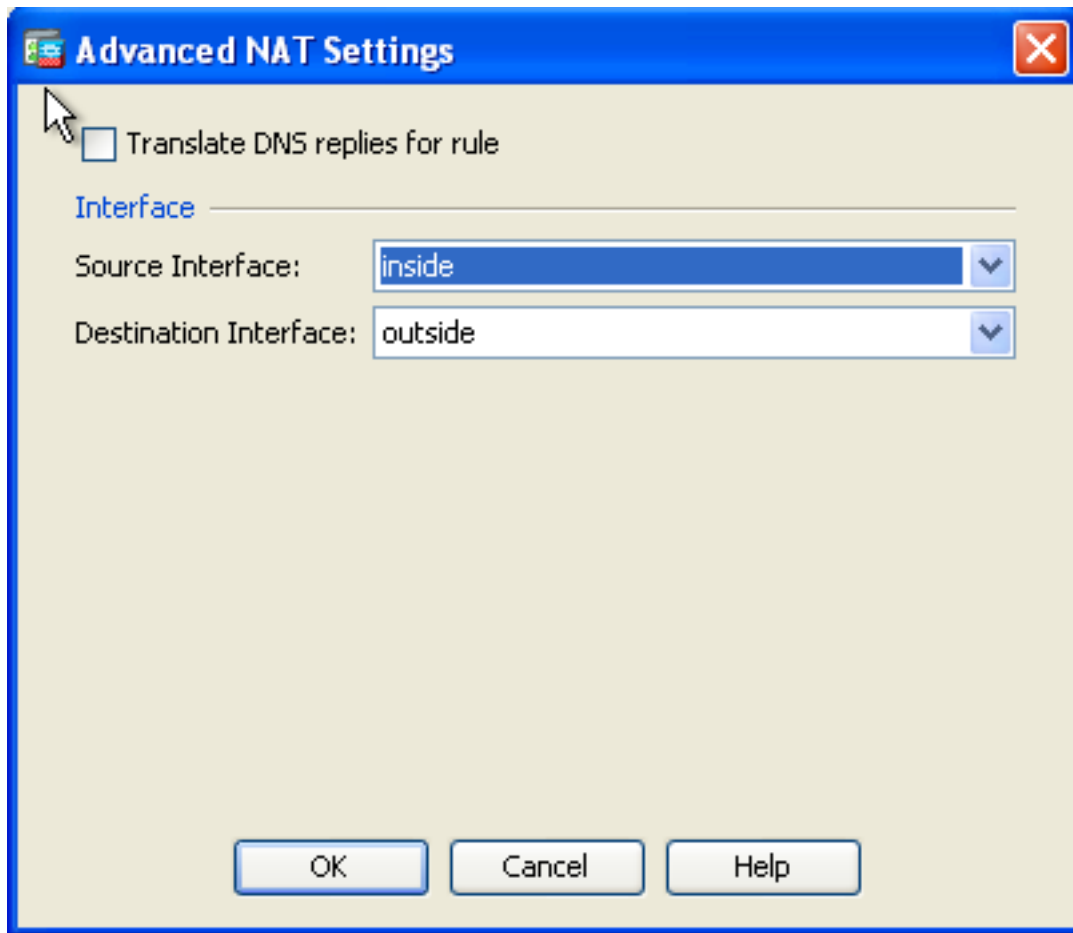
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

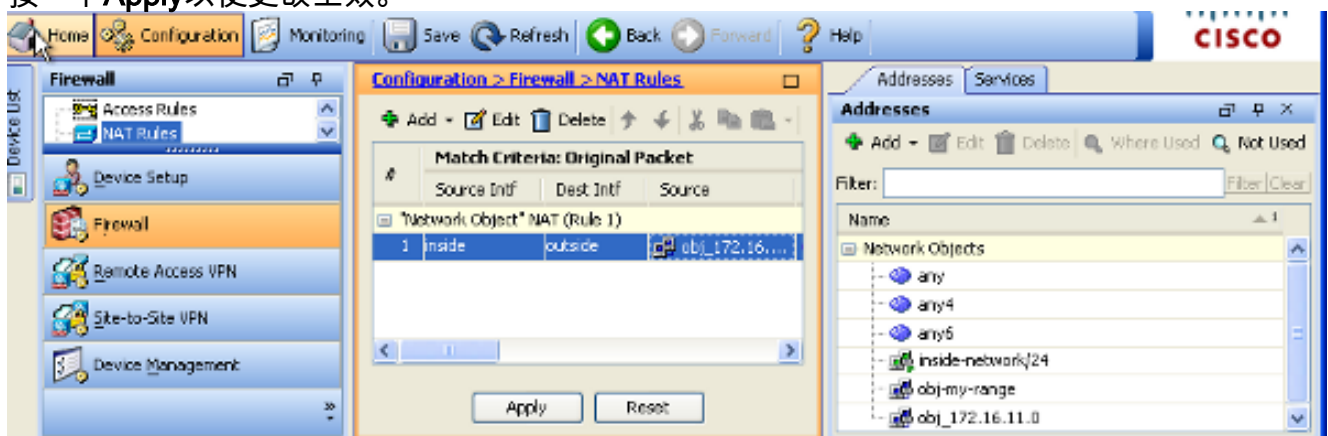
Advanced...

OK Cancel Help

5. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。按一下「OK」（確定）。



6. 按一下Apply以使更改生效。



這是此ASDM配置的等效的CLI輸出：

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

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

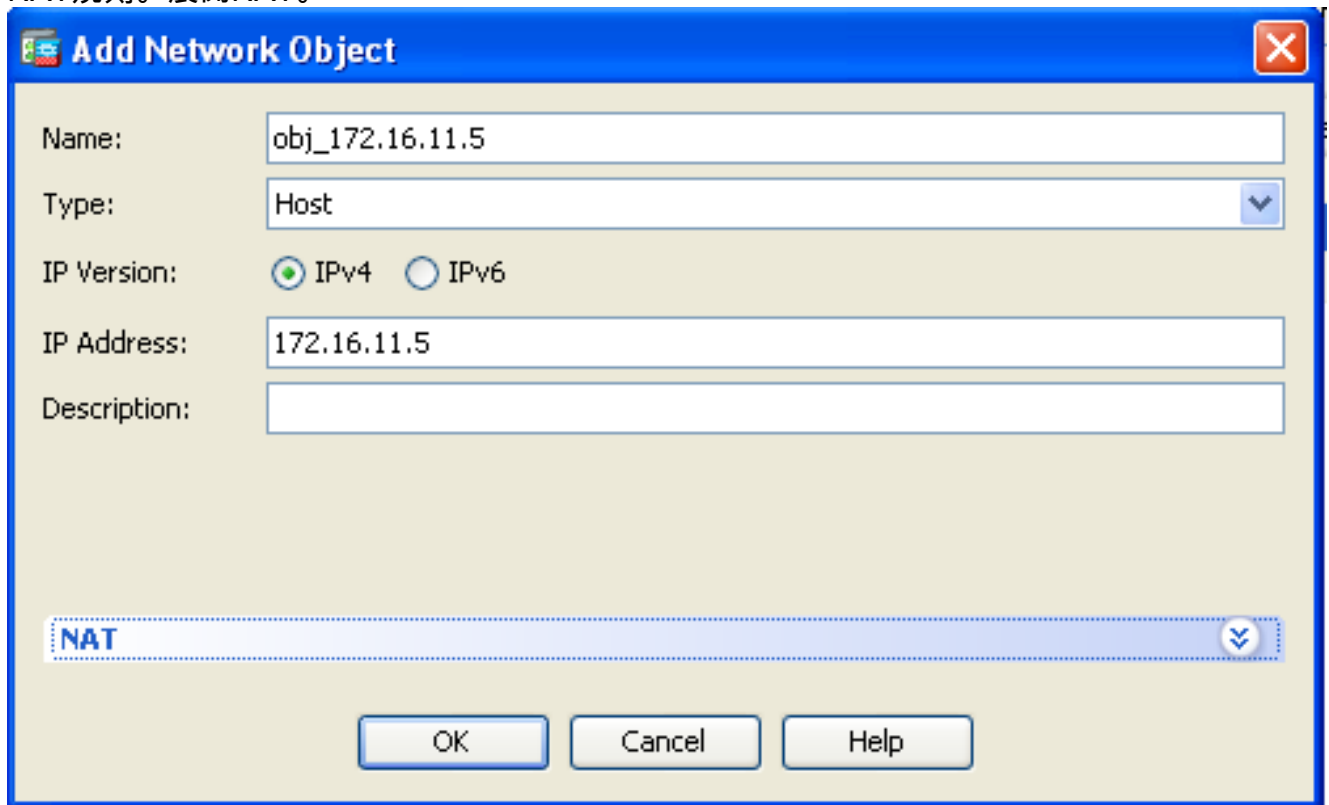
```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

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

允許不受信任的主機訪問受信任網路中的主機

這可以通過應用靜態NAT轉換和允許這些主機的訪問規則來實現。每當外部使用者想要訪問位於內部網路中的任何伺服器時，都需要進行此項配置。內部網路中的伺服器可以擁有不可在Internet上路由的專用IP地址。因此，您需要通過靜態NAT規則將該私有IP地址轉換為公有IP地址。假設您有一個內部伺服器(172.16.11.5)。為了讓此功能正常工作，您需要將此專用伺服器IP地址轉換為公共IP地址。本示例說明如何實施雙向靜態NAT以將172.16.11.5轉換為203.0.113.5。

1. 選擇**Configuration > Firewall > NAT Rules**。按一下**Add**，然後選擇**Network Object**以配置靜態NAT規則。展開NAT。



The screenshot shows the 'Add Network Object' dialog box. The fields are as follows:

- Name: obj_172.16.11.5
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 172.16.11.5
- Description: (empty)

At the bottom, there is a 'NAT' tab and three buttons: OK, Cancel, and Help.

2. 選中**Add Automatic Address Translation Rules**竅取方塊。在「型別」下拉選單中，選擇「靜態」。在Translated Addr欄位中，輸入IP地址。按一下**Advanced**以選擇來源介面和目的地介面。

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

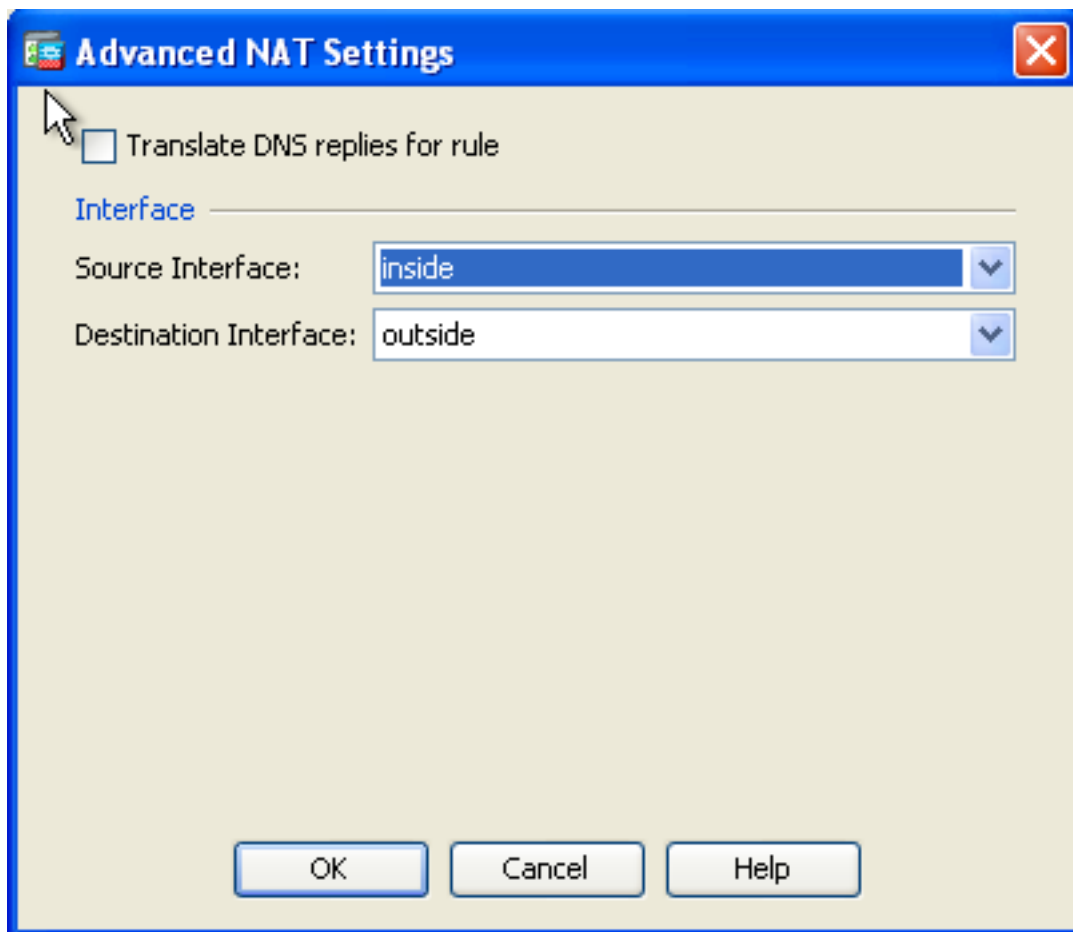
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

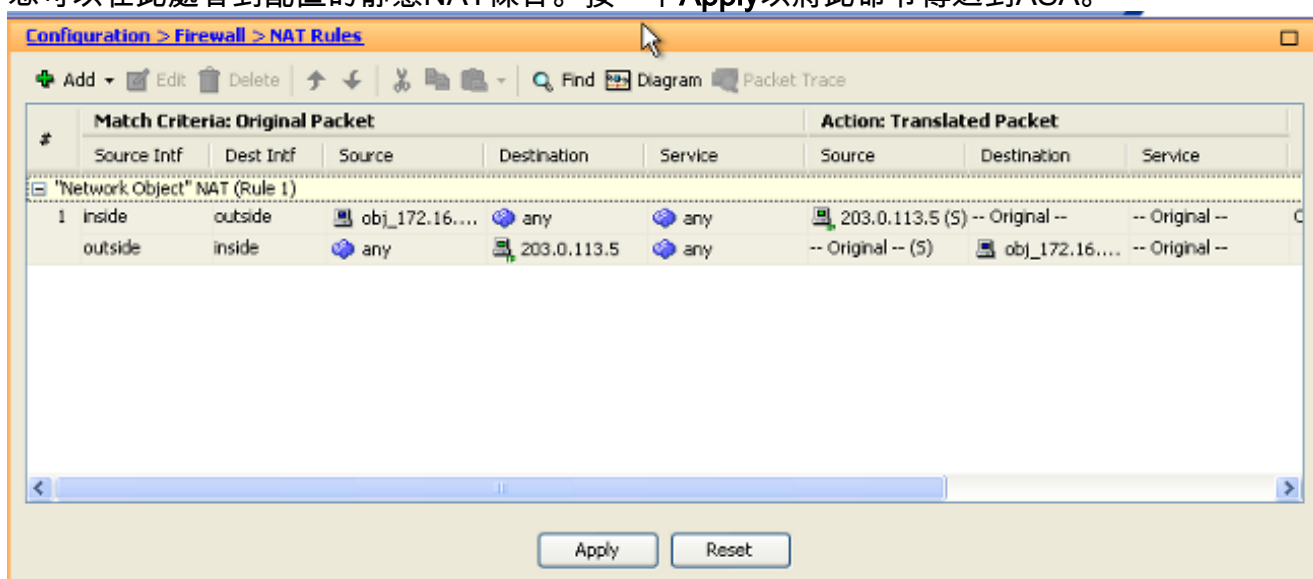
Advanced...

OK Cancel Help

3. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。按一下「OK」（確定）。



4. 您可以在此處看到配置的靜態NAT條目。按一下Apply以將此命令傳送到ASA。



以下是此NAT配置的等效的CLI輸出：

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

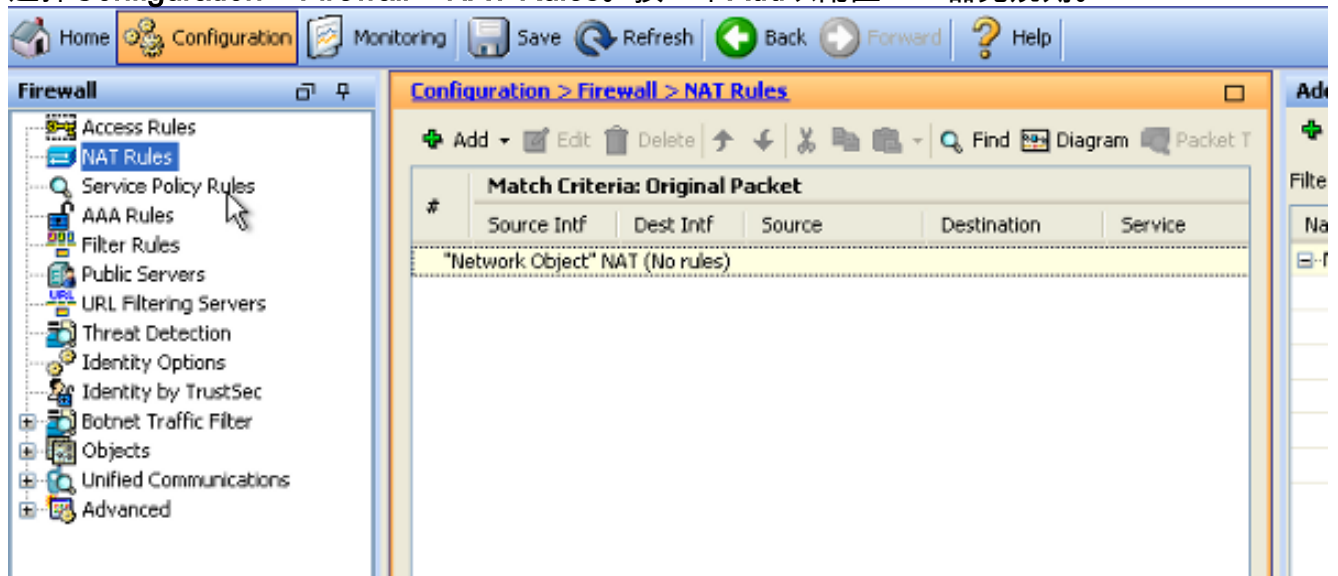
靜態身份NAT

NAT豁免是一個有用的功能，內部使用者可以在不完成NAT的情況下嘗試訪問遠端VPN主機/伺服器或ASA的任何其他介面後託管的一些主機/伺服器。為此，內部伺服器（具有私有IP地址）可以轉換為自己的身份，從而允許其訪問執行NAT的目標。

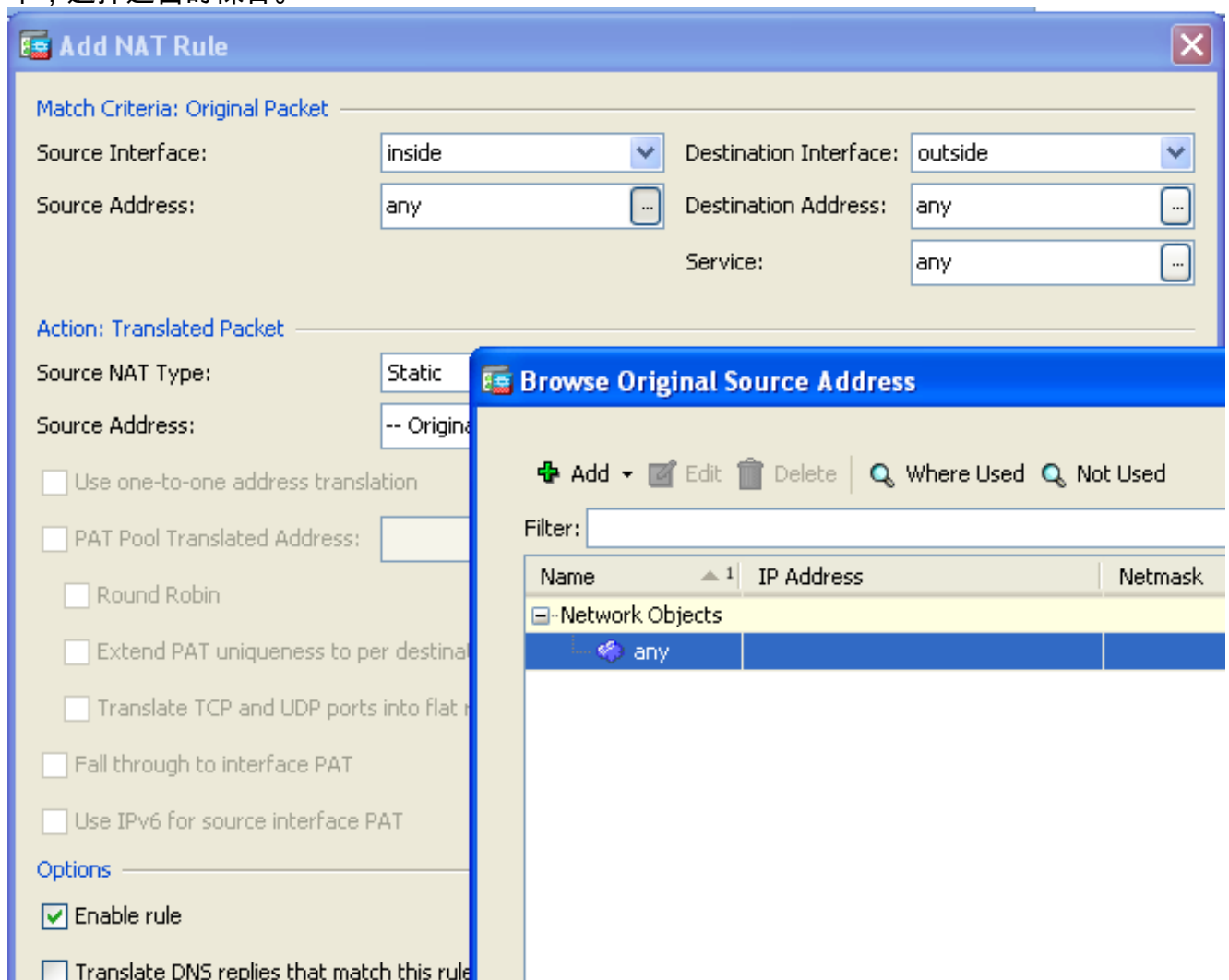
在本示例中，內部主機172.16.11.15需要訪問遠端VPN伺服器172.20.21.15。

完成以下步驟，在完成NAT後，允許內部主機訪問遠端VPN網路：

1. 選擇**Configuration > Firewall > NAT Rules**。按一下**Add**以配置NAT豁免規則。



2. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。在「源地址」欄位中，選擇適當的條目。



3. 按一下**Add**以新增網路對象。配置主機IP地址。

The screenshot shows the 'Add Network Object' dialog box with the following fields and values:

- Name: obj_172.16.11.15
- Type: Host
- IP Version: IPv4 IPv6
- IP Address: 172.16.11.15
- Description: (empty)

The NAT dropdown menu is expanded, showing 'NAT'. At the bottom, there are three buttons: OK, Cancel, and Help.

4. 同樣，瀏覽目的地地址。按一下**Add**以新增網路對象。配置主機IP地址。

The screenshot shows the 'Add Network Object' dialog box with the following fields and values:

- Name: obj_172.20.21.15
- Type: Host
- IP Version: IPv4 IPv6
- IP Address: 172.20.21.15
- Description: (empty)

The NAT dropdown menu is expanded, showing 'NAT'. At the bottom, there are three buttons: OK, Cancel, and Help.

5. 選擇已配置的源地址和目標地址對象。選中**Disable Proxy ARP on egress interface**和**Lookup route table to locate egress interface**覆取方塊。按一下「OK」（確定）。

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

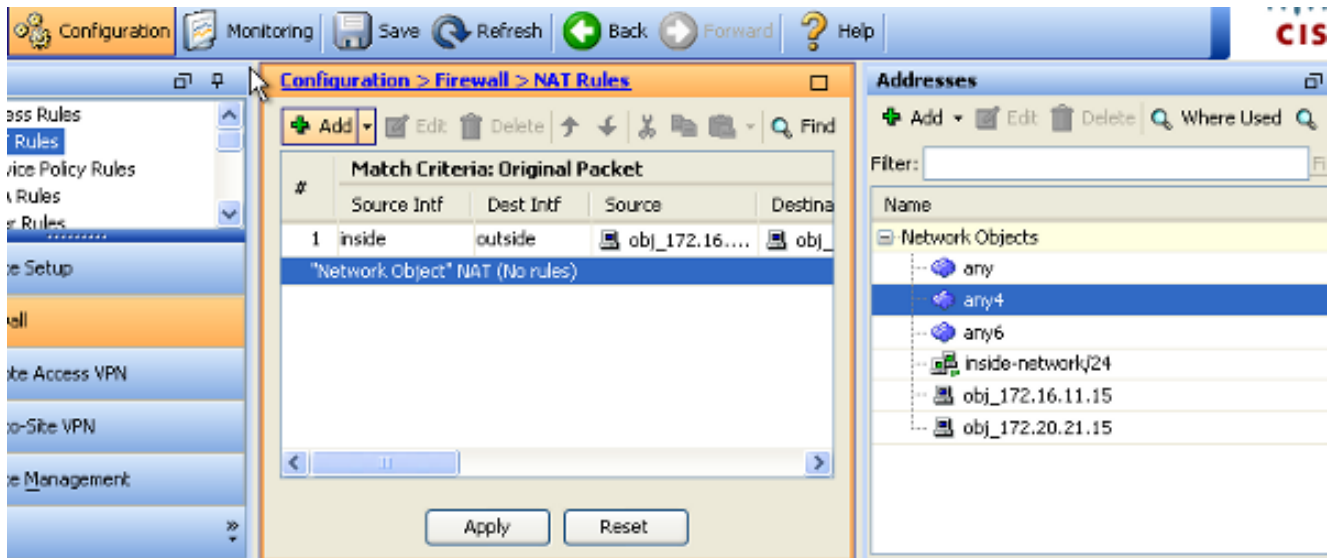
Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

6. 按一下**Apply**以使更改生效。



這是NAT豁免或身份NAT配置的等效的CLI輸出：

```
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
```

使用靜態的連線埠重新導向（轉送）

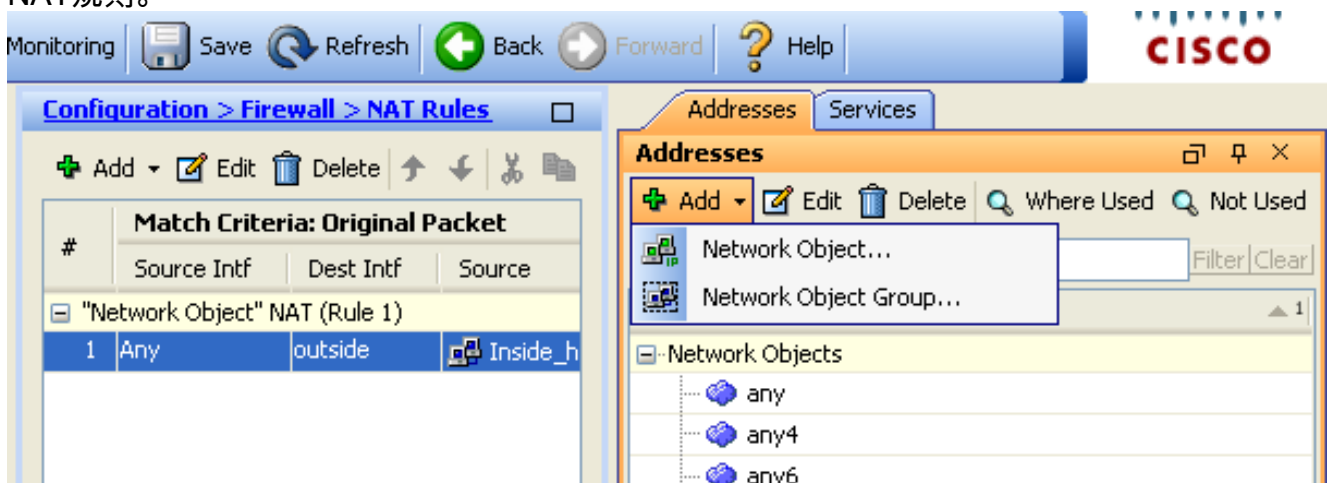
埠轉發或埠重定向是一項有用的功能，外部使用者可嘗試訪問特定埠上的內部伺服器。為此，內部伺服器（具有私有IP地址）可以轉換為公有IP地址，從而允許特定埠訪問。

在本例中，外部使用者想要訪問埠25上的SMTP伺服器203.0.113.15。這可通過兩個步驟完成：

1. 將埠25上的內部郵件伺服器172.16.11.15轉換為埠25上的公共IP地址203.0.113.15。
2. 允許訪問埠25上的公共郵件伺服器203.0.113.15。

當外部使用者嘗試訪問埠25上的伺服器203.0.113.15時，此流量將重定向到埠25上的內部郵件伺服器172.16.11.15。

1. 選擇Configuration > Firewall > NAT Rules。按一下Add，然後選擇Network Object以配置靜態NAT規則。



2. 配置需要埠轉發的主機。

Edit Network Object

Name: obj_172.16.11.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.16.11.15

Description:

NAT

OK Cancel Help

3. 展開NAT。選中**Add Automatic Address Translation Rules**覈取方塊。在「型別」下拉式清單中選擇「靜態」。在Translated Addr欄位中，輸入IP地址。按一下**Advanced**以選擇服務和來源及目的地介面。

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

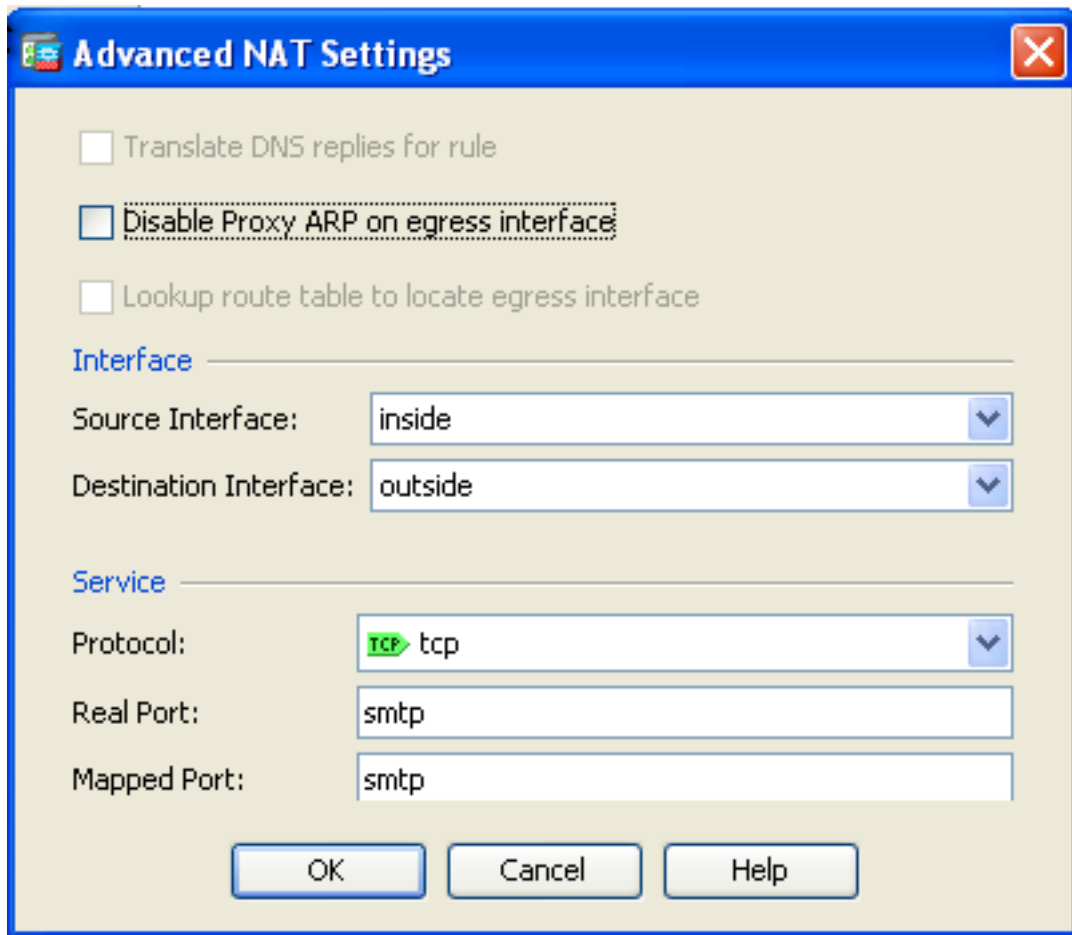
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

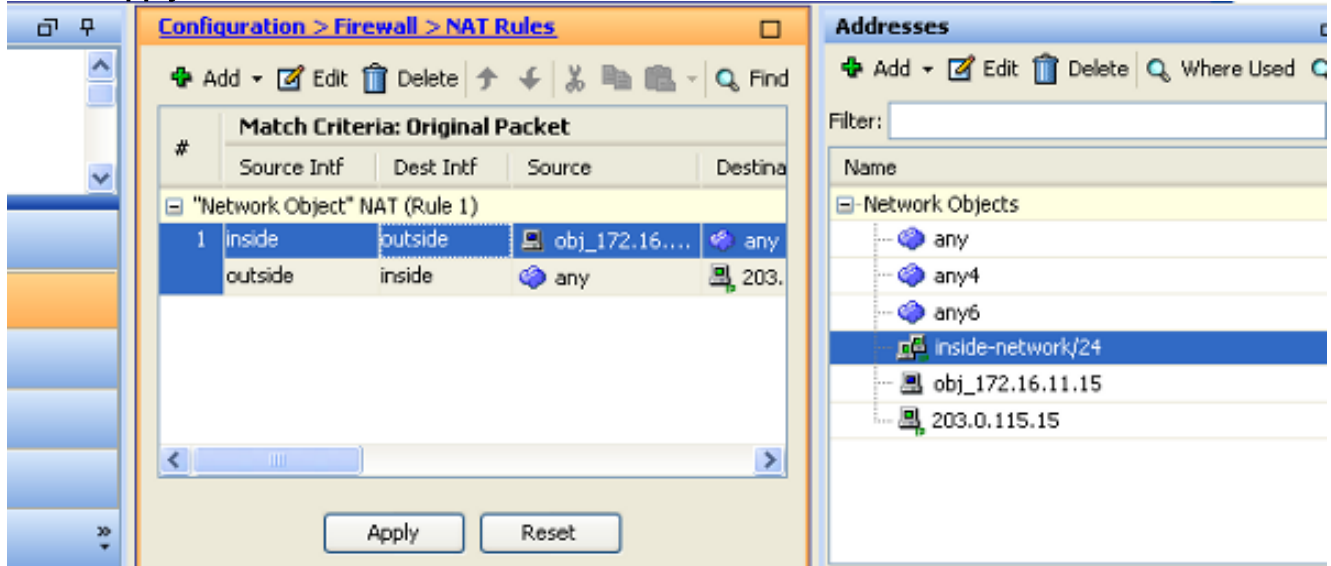
Advanced...

OK Cancel Help

4. 在Source Interface和Destination Interface下拉選單中，選擇適當的介面。配置服務。按一下「OK」（確定）。



5. 按一下Apply以使更改生效。



以下是此NAT配置的等效的CLI輸出：

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

驗證

使用本節內容，確認您的組態是否正常運作。

[Cisco CLI Analyzer \(僅供已註冊客戶使用 \)](#) 支援某些 show 指令。使用 Cisco CLI Analyzer 檢視

show 指令輸出的分析。

使用Web瀏覽器通過HTTP訪問網站。此示例使用託管在198.51.100.100的站點。如果連線成功，則可在ASA CLI上看到此輸出。

連線

```
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
```

ASA是有狀態防火牆，並且允許來自Web伺服器的返回流量通過防火牆，因為它與防火牆連線表中的**連接**。與預先存在的連線匹配的流量允許通過防火牆，不會被介面ACL阻止。

在前面的輸出中，內部介面上的客戶端已經從外部介面建立了到198.51.100.100主機的連線。此連線是使用TCP協定建立並且已空閒六秒。連線標誌指示此連線的當前狀態。有關連線標誌的詳細資訊，請參閱[ASA TCP連線標誌](#)。

系統日誌

```
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)
```

ASA防火牆在正常運行期間生成系統日誌。系統日誌的範圍取決於日誌記錄配置。輸出顯示在級別6或「資訊」級別上可見的兩個系統日誌。

在此示例中，生成了兩個系統日誌。第一個是指示防火牆已建立轉換（尤其是動態TCP轉換 [PAT]）的日誌消息。它表示流量從內部到外部介面傳輸時的源IP地址和埠以及轉換後的IP地址和埠。

第二個系統日誌表示防火牆在其連線表中為客戶端和伺服器之間的此特定流量建立了連線。如果防火牆配置為阻止此連線嘗試，或者某個其他因素阻止了此連線的建立（資源限制或可能的配置錯誤），則防火牆不會生成指示已建立連線的日誌。相反，它將記錄拒絕連線的原因，或有關禁止建立連線的因素的指示。

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
```

ASA上的Packet Tracer功能允許您指定模擬資料包，並檢視防火牆處理流量時執行的所有各種步驟、檢查和功能。使用此工具，識別您認為可以允許通過防火牆的流量范例，並使用該5元組來模擬流量會非常有用。在上一個示例中，使用Packet Tracer模擬符合以下條件的連線嘗試：

- 模擬資料包到達內部。
- 使用的協定是TCP。
- 模擬客戶端IP地址為172.16.11.5。
- 使用者端會傳送源自連線埠1234的流量。
- 流量將發往IP地址為198.51.100.100的伺服器。
- 流量將傳至連線埠80。

請注意，命令中沒有提到外部介面。這是通過Packet Tracer設計的。該工具將告訴您防火牆如何處理該型別的連線嘗試，包括它將如何路由它以及從哪個介面發出。有關Packet Tracer的詳細資訊，請參閱[使用Packet Tracer跟蹤資料包](#)。

CAPTURE

應用捕獲

```
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>
```

ASA防火牆可以捕獲進入或離開其介面的流量。此捕獲功能非常棒，因為它可以明確證明流量是到達防火牆還是離開防火牆。上例顯示了分別在內外部介面上配置兩個名為capin和capout的捕獲。capture命令使用match關鍵字，允許您具體說明要捕獲的流量。

對於捕獲，您指示想要匹配在與TCP主機172.16.11.5主機198.51.100.100匹配的內部介面（入口或出口）上看到的流量。換句話說，您要捕獲從主機172.16.11.5傳送到主機198.51.100.100的任何TCP流量，或者反之亦然。使用match關鍵字允許防火牆雙向捕獲該流量。為外部介面定義的capture命令不引用內部客戶端IP地址，因為防火牆在該客戶端IP地址上執行PAT。因此，您無法與該客戶端IP地址匹配。相反，此示例使用any來表示所有可能的IP地址都將與該條件匹配。

設定擷取後，您會嘗試再次建立連線，並繼續使用`show capture <capture_name>` 指令檢視擷取。在此範例中，您可以看到使用者端能夠連線到伺服器，從擷取中看到的TCP 3次交握可以清楚看到。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [ASA系統日誌配置示例](#)
- [使用CLI和ASDM的ASA資料包捕獲配置示例](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。