PIX/ASA 7.x和FWSM:NAT和PAT語句

目錄

簡介

本文檔提供思科PIX/ASA安全裝置上的基本網路地址轉換(NAT)和埠地址轉換(PAT)配置示例。提供了簡化的網路圖。有關詳細資訊，請參閱PIX/ASA軟體版本的PIX/ASA文檔。

請參閱在PIX上使用nat、global、static、conduit和access-list命令以及埠重定向（轉發），以瞭解有關PIX 5.x及更高版本上的nat、global、**static**、conduit和**access-list**命令以及埠重定向（轉發）的詳細資訊。

請參閱在Cisco安全PIX防火牆上使用NAT和PAT語句，以瞭解有關Cisco安全PIX防火牆上的基本NAT和PAT配置示例的詳細資訊。

有關ASA 8.3及更高版本中NAT配置的詳細資訊，請參閱有關NAT的資訊。

注意：PIX/ASA 8.x版支援透明模式中的NAT。有關詳細資訊，請參閱透明模式中的NAT。

必要條件

需求

本文檔的讀者應瞭解Cisco PIX/ASA安全裝置。

採用元件

本文檔中的資訊基於Cisco PIX 500系列安全裝置軟體版本7.0及更高版本。

附註： 本文檔已通過PIX/ASA 8.x版重新認證。

注意：本文檔中使用的命令適用於防火牆服務模組(FWSM)。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

nat-control命令

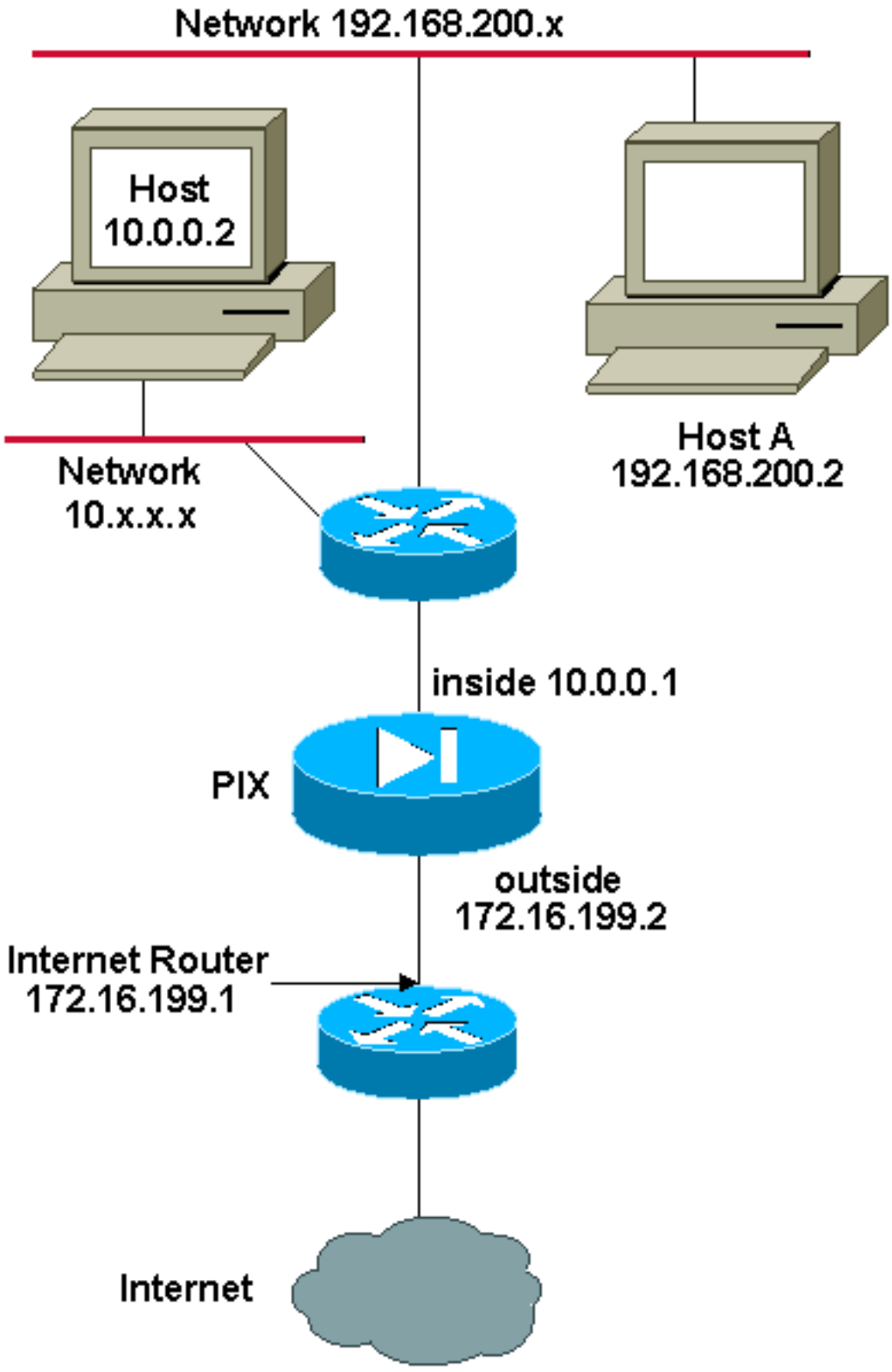
PIX/ASA上的**nat-control**命令指定所有通過防火牆的流量都必須具有特定的轉換條目(具有匹配的**global**或**static**語句的**nat**語句)才能通過該防火牆。**nat-control**命令可確保轉換行為與低於7.0的PIX防火牆版本相同。PIX/ASA 7.0及更高版本的預設配置是**no nat-control**命令的規範。在PIX/ASA 7.0及更高版本中，可以在發出**nat-control**命令時更改此行為。

禁用**nat-control**後，PIX/ASA將資料包從較高安全性的介面轉發到較低的安全性介面，而無需配置中的特定轉換條目。若要將流量從安全性較低的介面傳遞到安全性較高的介面，請使用存取清單來允許流量。然後PIX/ASA轉發流量。本文檔重點介紹啟用了**nat**-control的PIX/ASA安**全裝置的**行為。

注意：如果要刪除或禁用PIX/ASA中的nat-control語句，則需要從安全裝置中刪除所有NAT語句。通常，在關閉NAT控制之前需要刪除NAT。您必須在PIX/ASA中重新配置NAT語句才能按預期工作。

使用NAT 0的多個NAT語句

網路圖表



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

在本示例中，ISP為網路管理員提供從172.16.199.1到172.16.199.63的地址範圍。網路管理員決定將172.16.199.1分配給Internet路由器上的內部介面，將172.16.199.2分配給PIX/ASA的外部介面。

網路管理員已經將一個C類地址分配給網路192.168.200.0/24，並且有一些工作站使用這些地址來訪問Internet。這些工作站不會被地址轉換。但是，在10.0.0.0/8網路中為新工作站分配了地址，這些地址需要轉換。

為了適應此網路設計，網路管理員必須在PIX/ASA配置中使用兩個NAT語句和一個全域性池，如以下輸出所示：

```
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
```

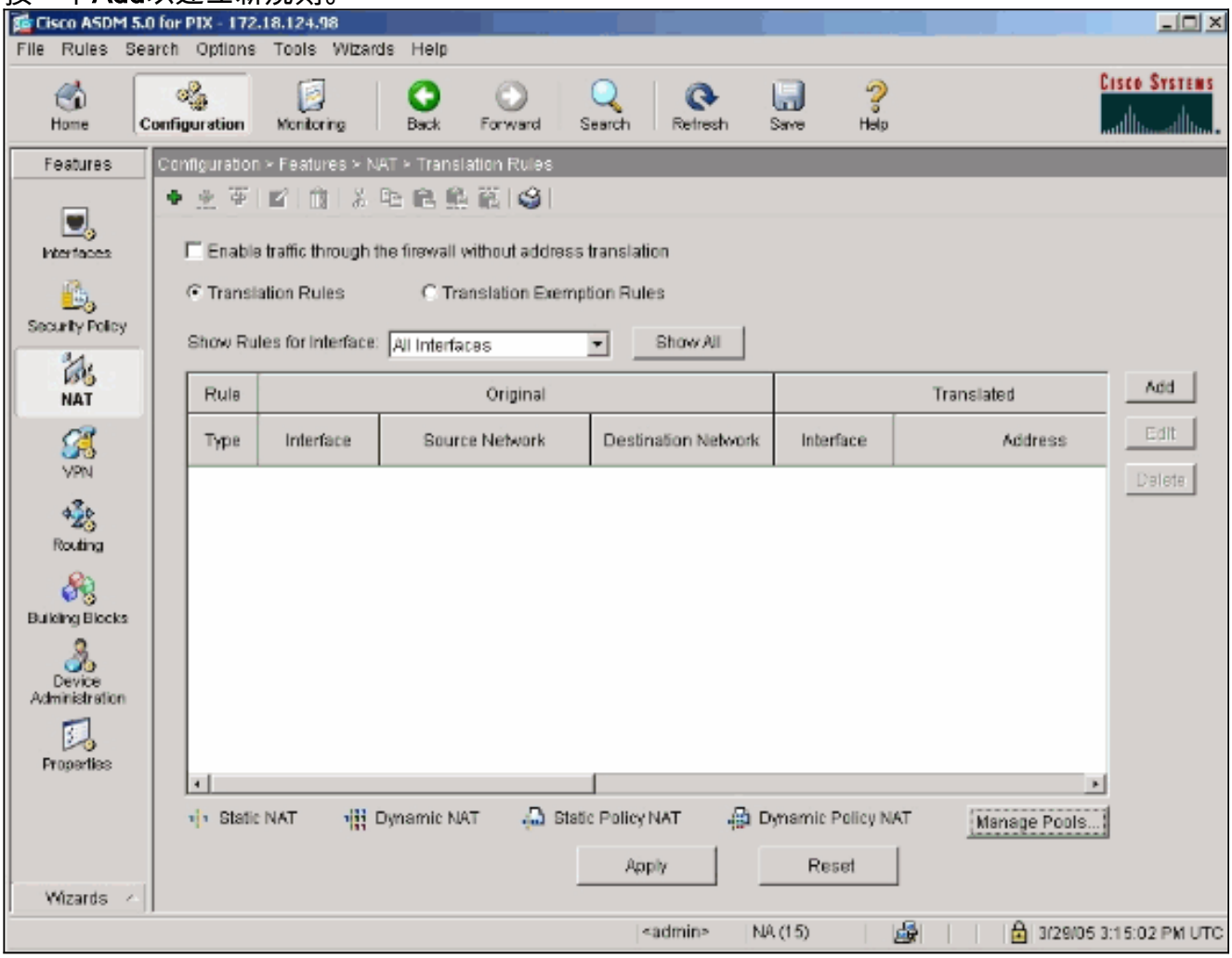
此配置不會轉換來自192.168.200.0/24網路的任何出站流量的源地址。它將10.0.0.0/8網路中的源地址轉換為從172.16.199.3到172.16.199.62範圍內的地址。

以下步驟說明如何使用調適型安全裝置管理員(ASDM)套用此相同組態。

注意：通過CLI或ASDM執行所有配置更改。使用CLI和ASDM進行配置更改會導致在ASDM應用內容方面出現非常不穩定的行為。這不是錯誤，而是因為ASDM的工作方式。

注意：當您開啟ASDM時，它將從PIX/ASA匯入當前配置，並在您進行和應用更改時從該配置運行。如果在ASDM會話處於開啟狀態時對PIX/ASA進行了更改，則ASDM不再使用它認為PIX/ASA的當前配置。如果通過CLI進行配置更改，請確保關閉所有ASDM會話。當您需要通過GUI工作時，再次開啟ASDM。

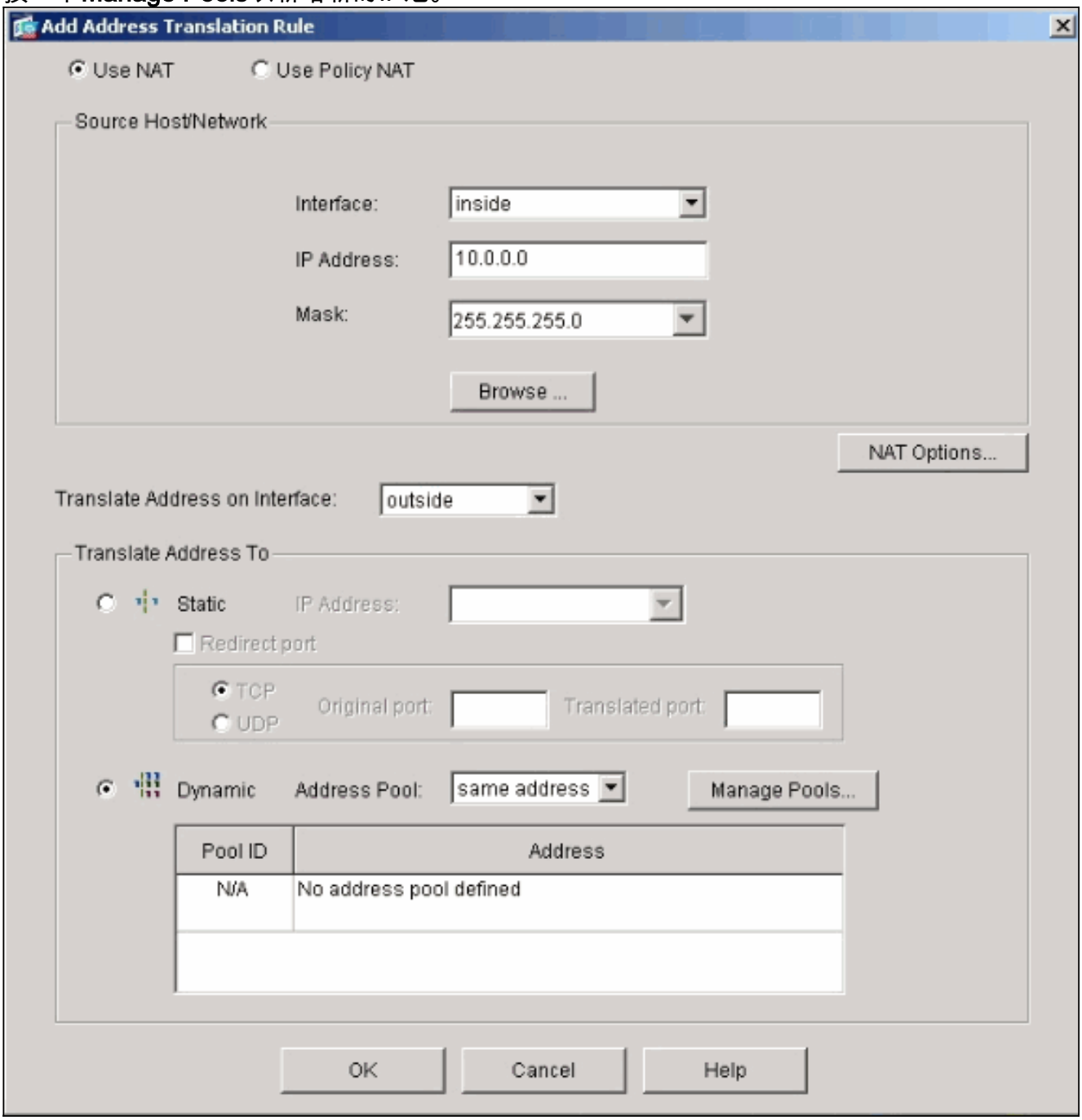
1. 啟動ASDM，瀏覽到Configuration頁籤，然後點選**NAT**。
2. 按一下**Add**以建立新規則。



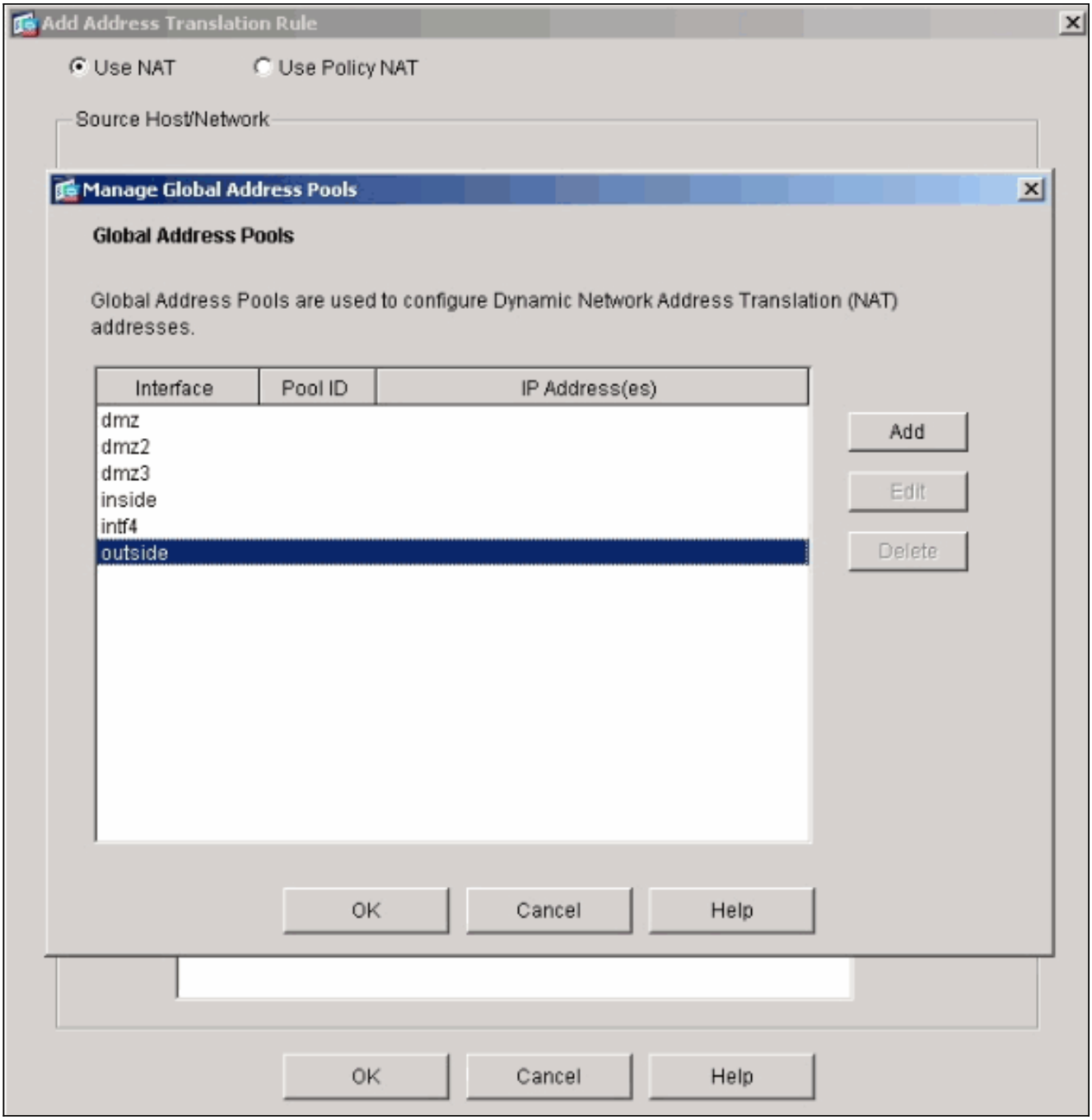
將出現一個新視窗，允許使用者更改此NAT條目的NAT選項。在本示例中，對到達內部介面且來自特定10.0.0.0/24網路的資料包執行NAT。PIX/ASA將這些資料包轉換為外部介面上的動態

IP池。輸入描述哪些流量到NAT的資訊後，請為轉換後的流量定義IP地址池。

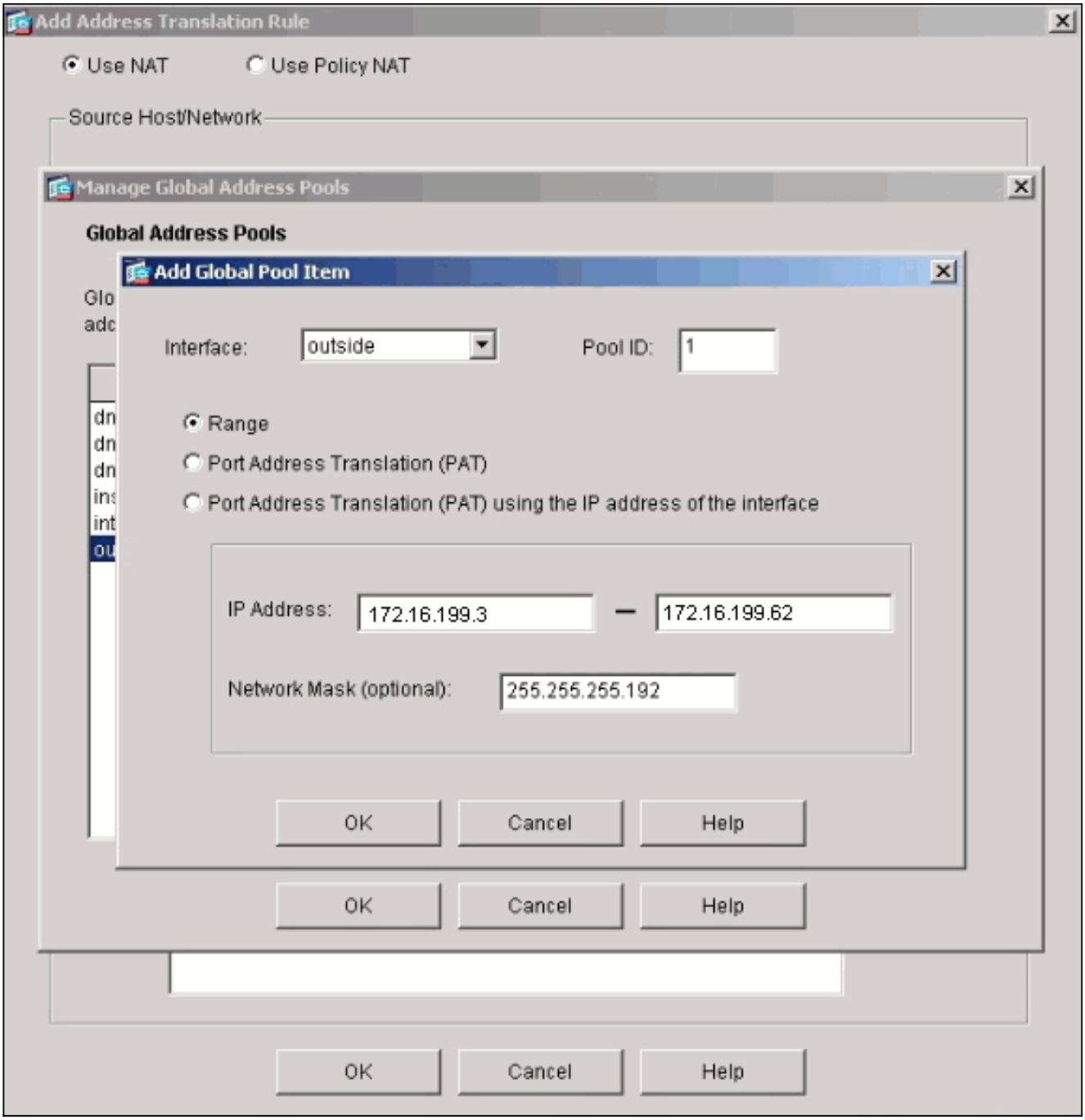
3. 按一下**Manage Pools**以新增新的IP池。



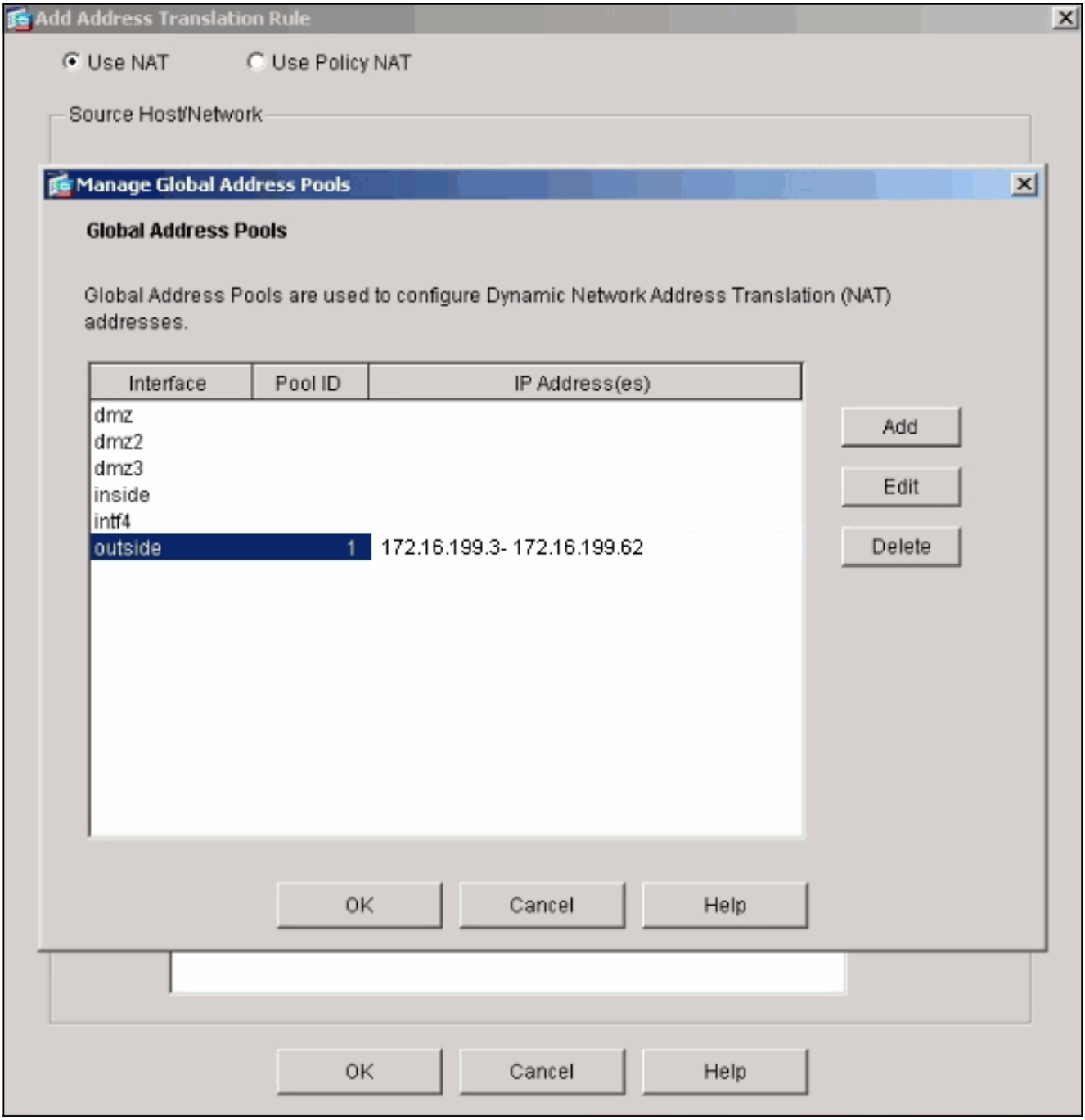
4. 選擇**outside**，然後按一下**Add**。



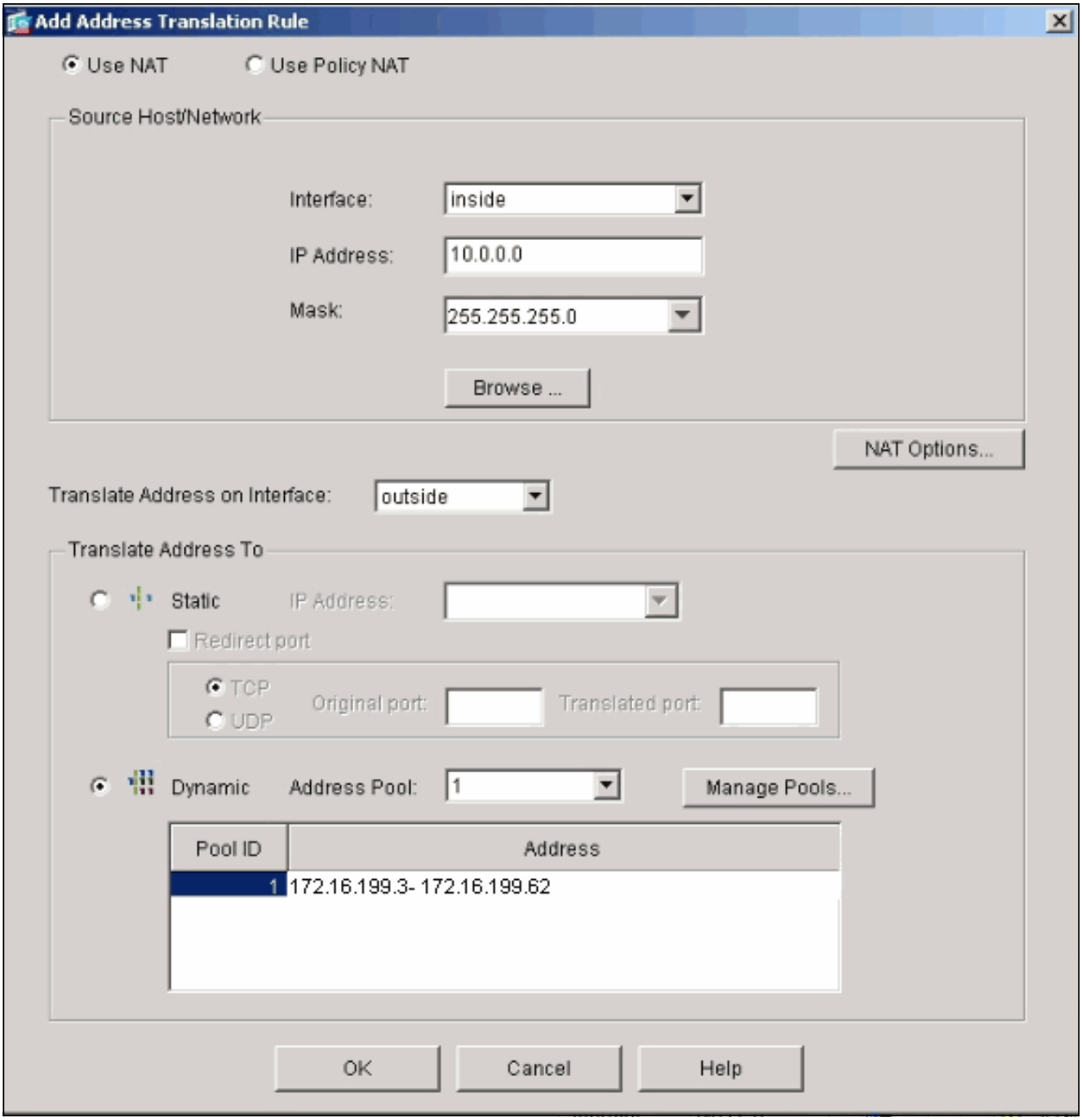
5. 指定池的IP範圍，並為池指定一個唯一的整數ID號。



6. 輸入適當的值，然後按一下**確定**。為外部介面定義新池。

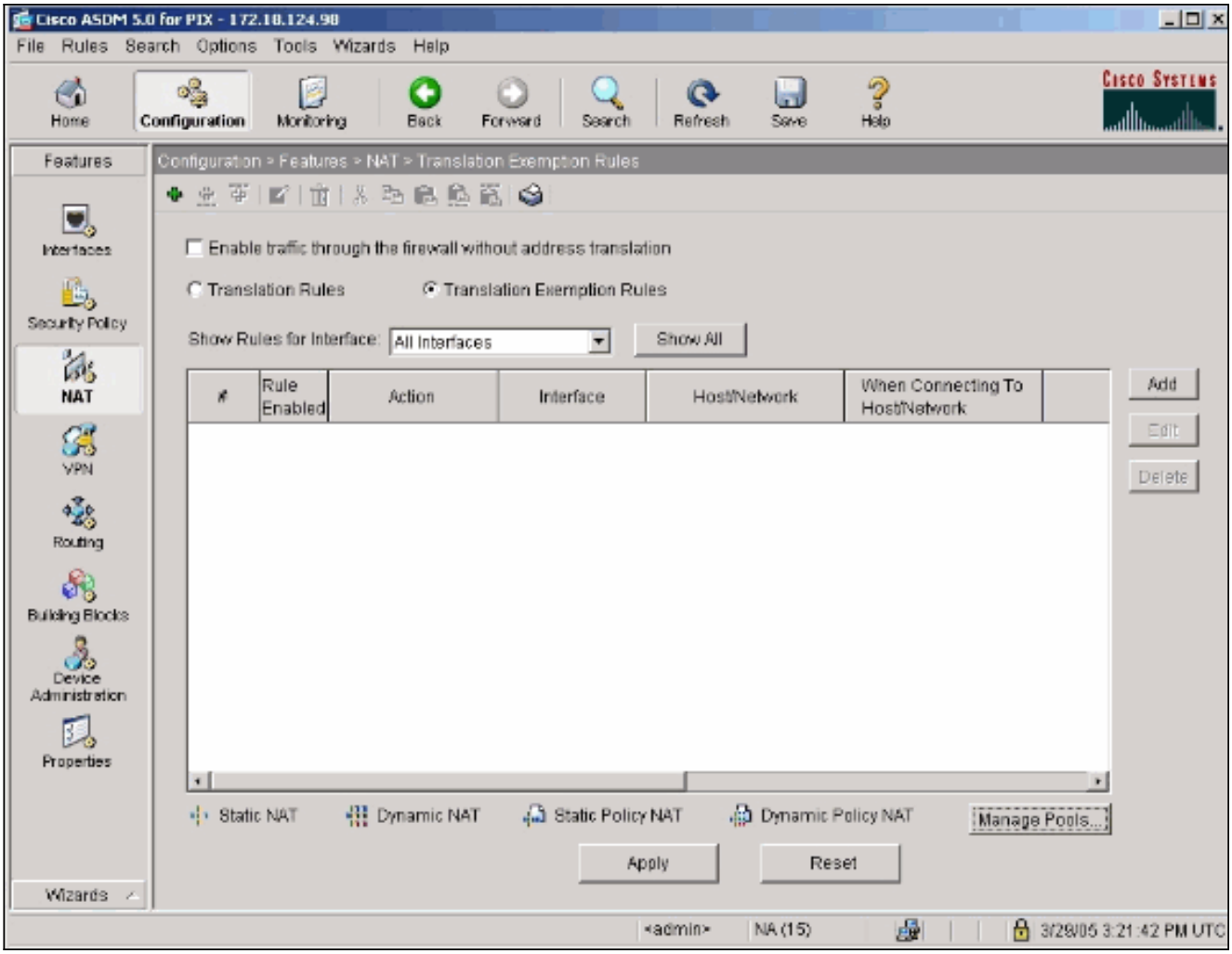


7. 定義池後，按一下**OK**以返回NAT規則配置視窗。確保選擇您剛剛在Address Pool下拉選單下建立的正確池。

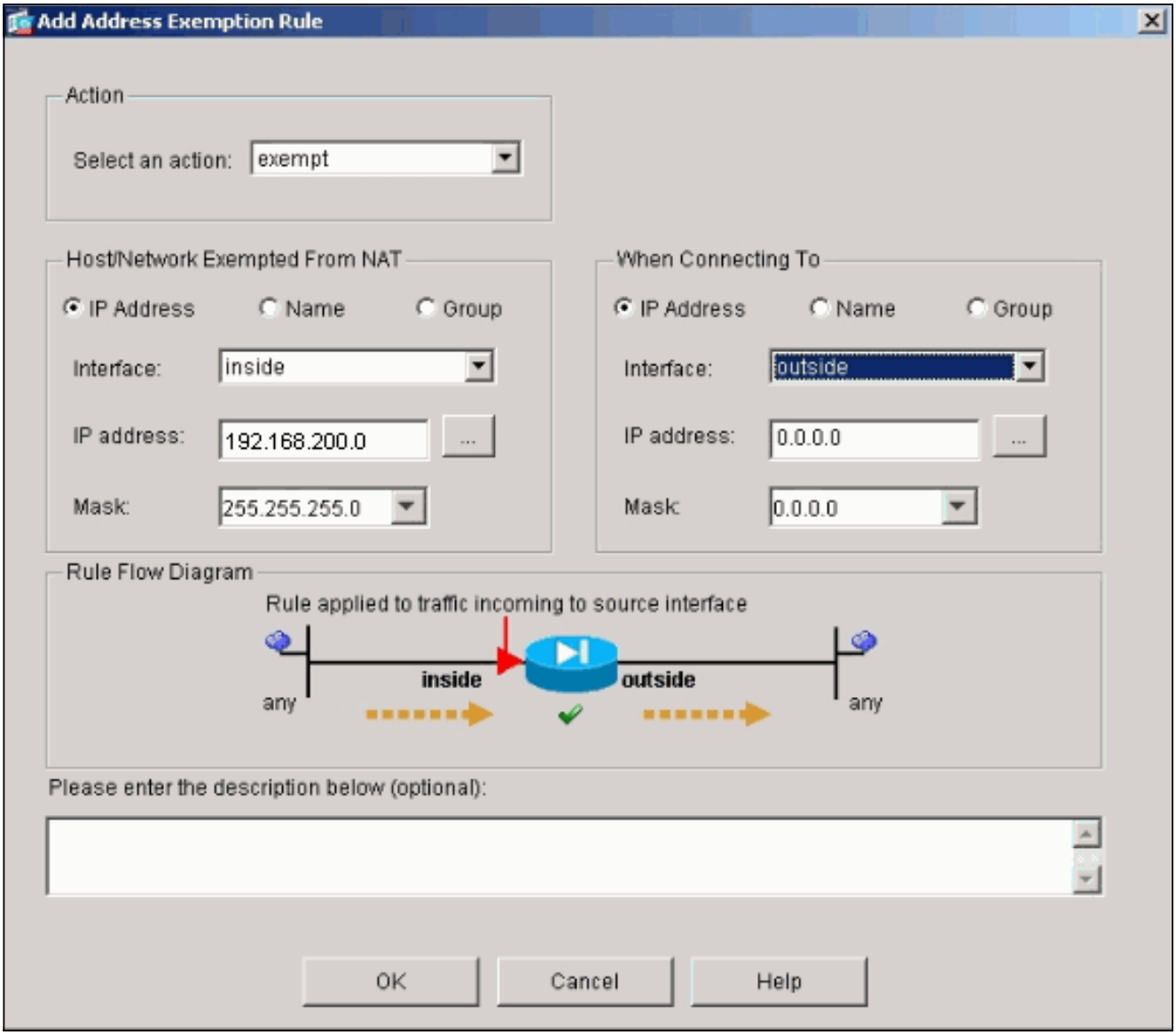


現在，您已建立通過安全裝置的NAT轉換。但是，您仍需要建立指定哪些流量不屬於NAT的NAT條目。

8. 按一下位於視窗頂部的**Translation Exemption Rules**，然後按一下**Add**以建立新規則。



9. 選擇*inside*介面作為源，並指定192.168.200.0/24子網。保留「連線時」值為預設值。



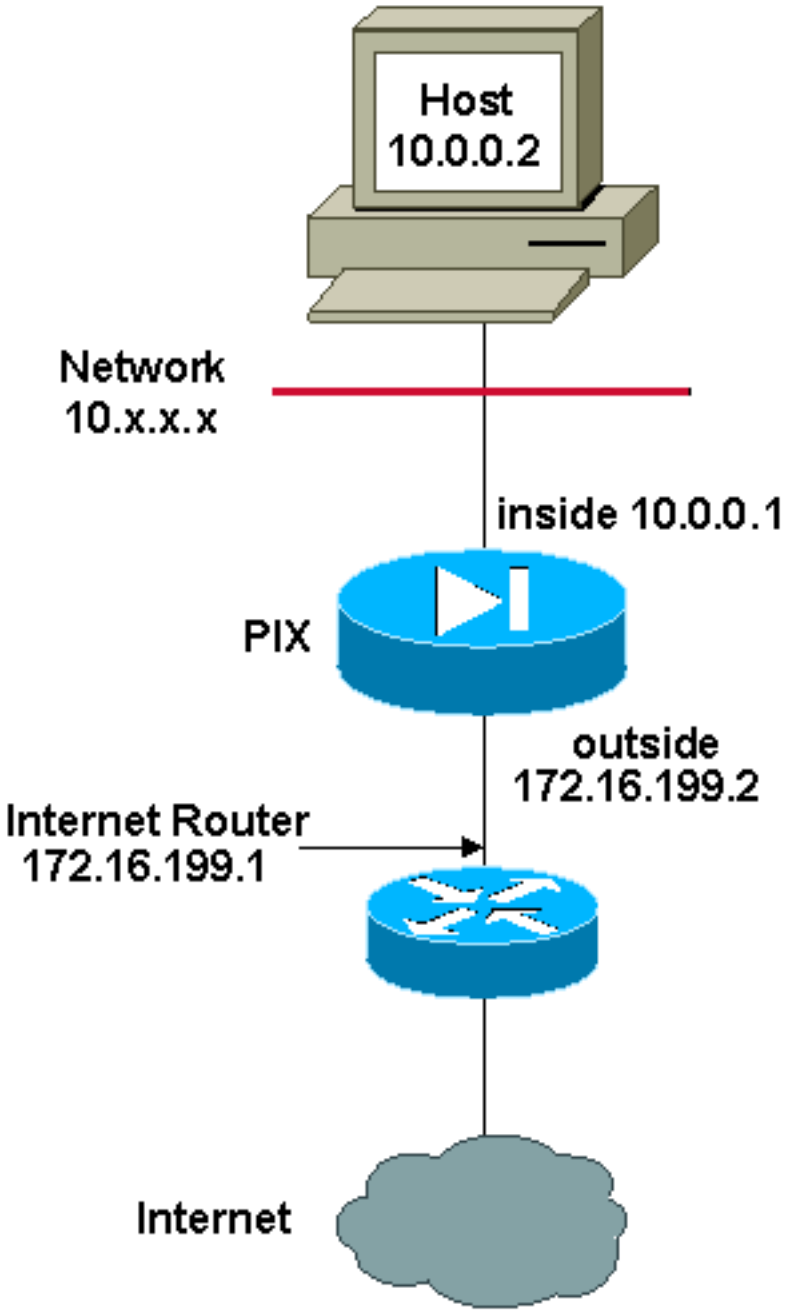
現在定義了NAT規則。

10. 按一下**Apply**以將更改應用於安全裝置的當前運行配置。此輸出顯示了應用於PIX/ASA配置的實際增加內容。它們與從手動方法輸入的命令略有不同，但它們是相同的。

```
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
```

多個全域性池

網路圖表



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

在本例中，網路管理器有兩個範圍的IP地址在Internet上註冊。網路管理員必須將10.0.0.0/8範圍內的所有內部地址轉換為註冊地址。網路管理員必須使用的IP位址範圍是172.16.199.1到172.16.199.62和192.168.150.1到192.168.150.254。網路管理員可以執行以下操作：

```
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
```

在動態NAT中，更具體的語句是在全域性上使用同一介面時優先使用的語句。

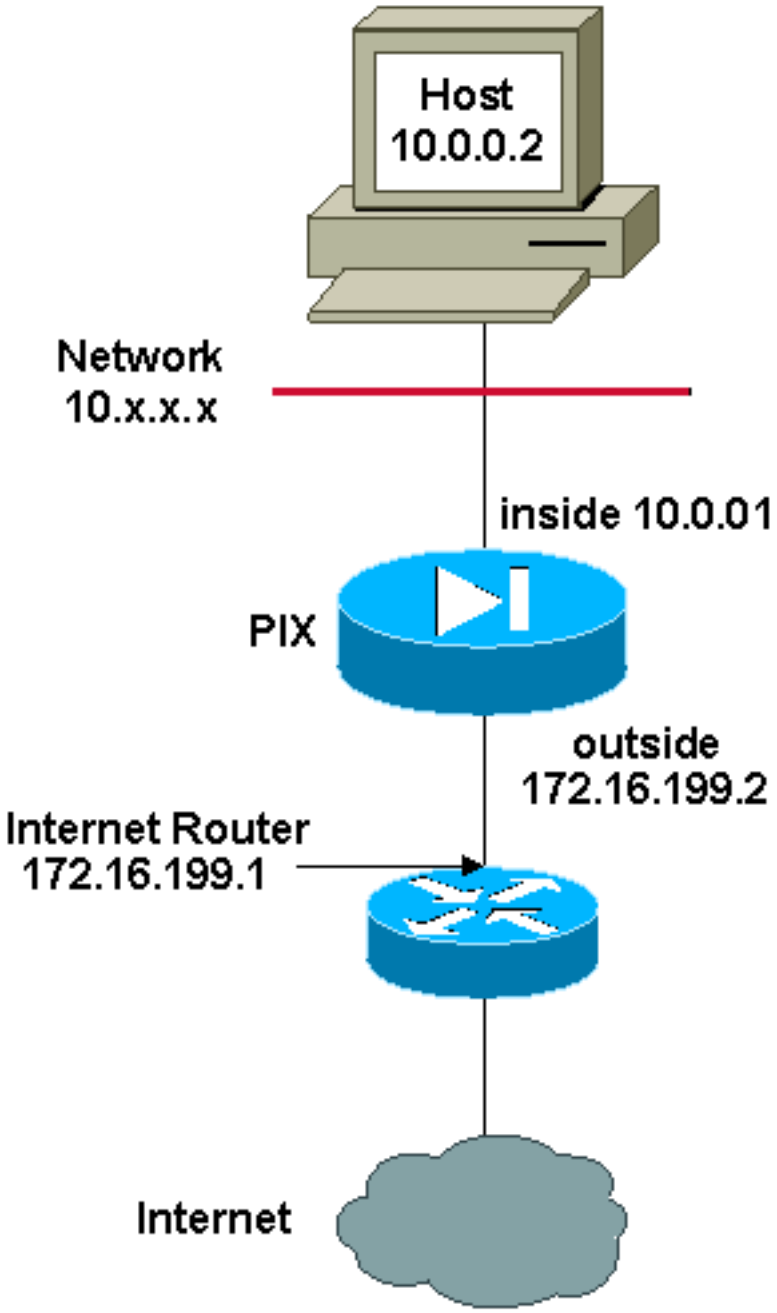
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
```

```
global (outside) 2 192.168.1.1
```
如果內部網路為10.1.0.0，則NAT global 2優先於1，因為它更專門用於轉換。

注意：NAT語句中使用了萬用字元定址方案。此語句通知PIX/ASA在內部源地址傳出到Internet時對其進行轉換。如果需要，此命令中的地址可以更具體一些。

混合NAT和PAT全域性語句

網路圖表



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

在本例中，ISP為網路管理員提供從172.16.199.1到172.16.199.63的地址範圍以供公司使用。網路管理員決定將172.16.199.1用於Internet路由器上的內部介面，將172.16.199.2用於PIX/ASA上的外部介面。您將剩下172.16.199.3到172.16.199.62以用於NAT池。但是，網路經理知道，在任何時候

，都可能有60多人嘗試離開PIX/ASA。因此，網路管理員決定採用172.16.199.62並將其設定為PAT地址，以便多個使用者可以同時共用一個地址。

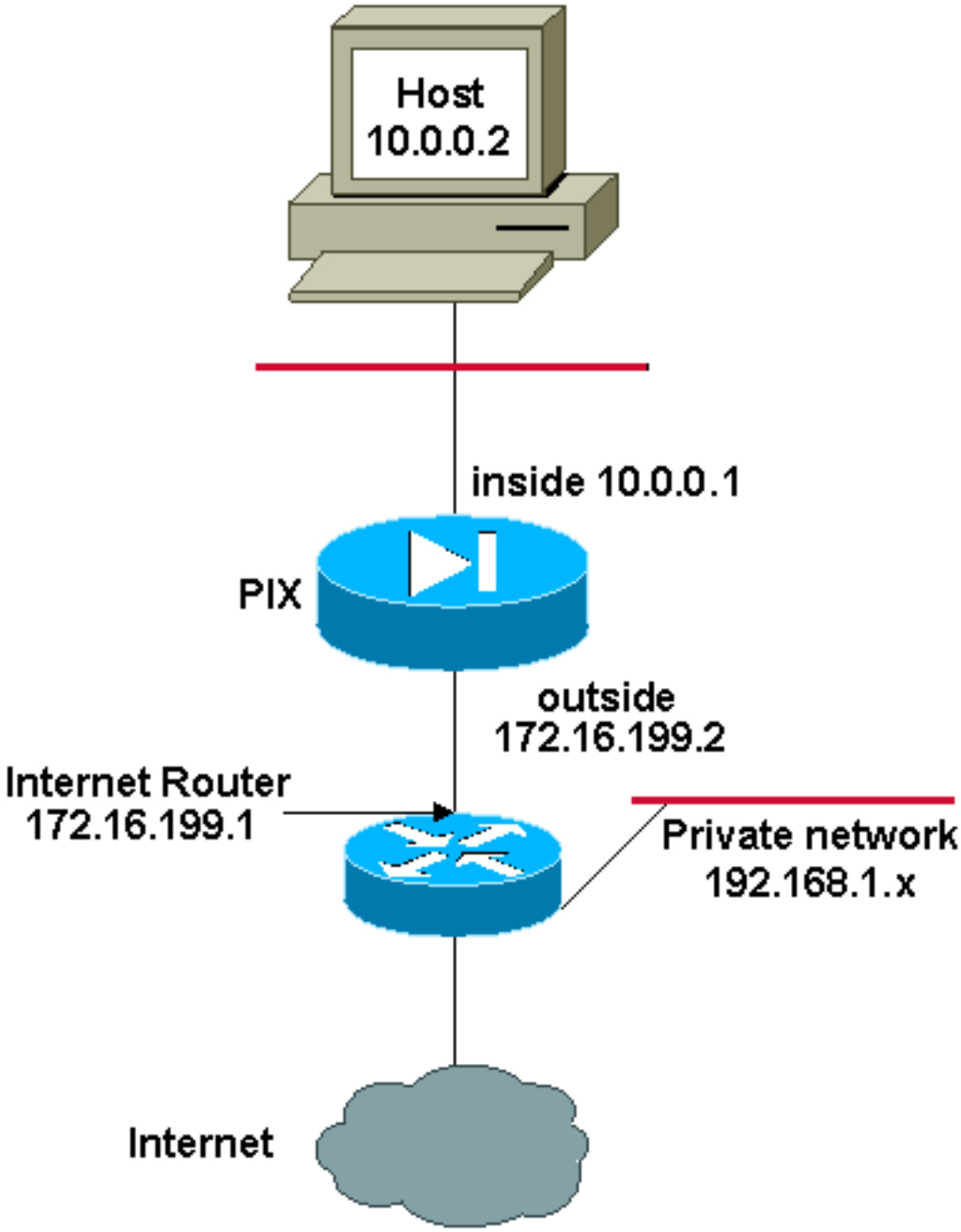
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

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
```

這些命令指示PIX/ASA將源地址轉換為172.16.199.3到172.16.199.61，以便前59個內部使用者通過PIX/ASA。在這些地址耗盡後，PIX會將所有後續源地址轉換為172.16.199.62，直到NAT池中的某個地址變為空閒地址。

注意：NAT語句中使用了萬用字元定址方案。此語句通知PIX/ASA在內部源地址傳出到Internet時對其進行轉換。如果您願意，此命令中的地址可以更具體一些。

具有NAT 0訪問清單的多個NAT語句

網路圖表



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

在本例中，ISP為網路管理員提供從172.16.199.1到172.16.199.63的地址範圍。網路管理員決定將172.16.199.1分配給Internet路由器上的內部介面，將172.16.199.2分配給PIX/ASA的外部介面。

但是在此案例中，另一個私有LAN網段被放置在Internet路由器之外。當這兩個網路中的主機相互通訊時，網路管理員不希望浪費全域性池中的地址。當所有內部使用者(10.0.0.0/8)連線到Internet時，網路管理員仍需要轉換其源地址。

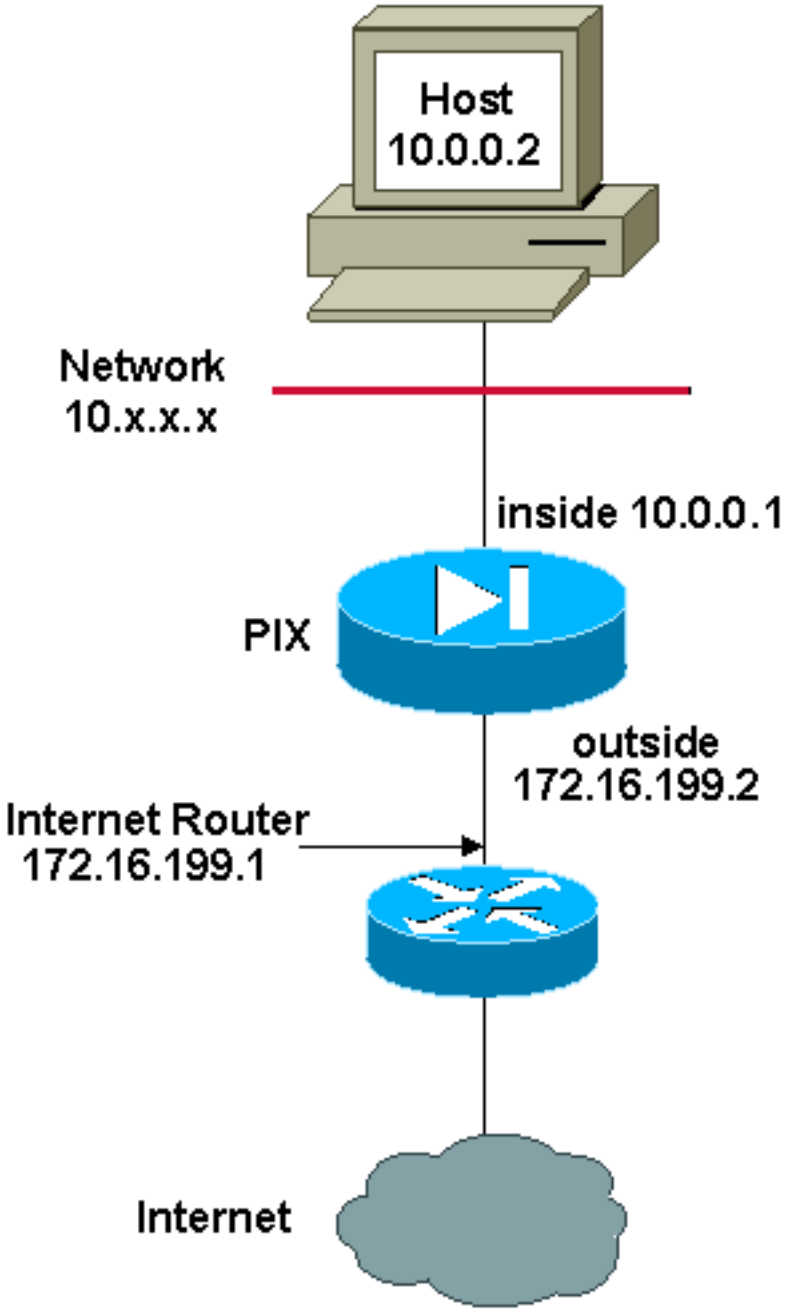
```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

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
```

此組態不會將來源位址為10.0.0.0/8、目的地位址為192.168.1.0/24的位址轉譯。它會將來源位址從從10.0.0.0/8網路中起始且目的地為192.168.1.0/24以外的任何流量的來源位址轉譯成從172.16.199.3到172.16.199.62範圍內的位址。

如果您有來自Cisco裝置的**write terminal**命令輸出，可以使用Output Interpreter Tool(僅限註冊客戶)。

使用策略NAT

網路圖表



注意：此配置中使用的IP編址方案在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 。

將訪問清單與**nat**命令一起用於除0以外的任何NAT ID時，將啟用策略NAT。

注意：策略NAT是在6.3.2版中引入的。

在訪問清單中指定源地址和目標地址（或埠）時，策略NAT允許您標識本地流量以進行地址轉換。常規NAT僅使用源地址/埠，而策略NAT同時使用源地址和目標地址/埠。

注意：除NAT免除(**nat 0 access**-list)外，所有型別的**NAT都支援策略**NAT。NAT免除使用訪問控制清單來標識本地地址，但與策略NAT的不同之處在於不考慮埠。

使用策略NAT，可以建立多個NAT或靜態語句，只要源/埠和目標/埠組合對於每條語句是唯一的，這些語句就標識同一個本地地址。然後，您可以將不同的全域性地址與每個源/埠和目標/埠對匹配。

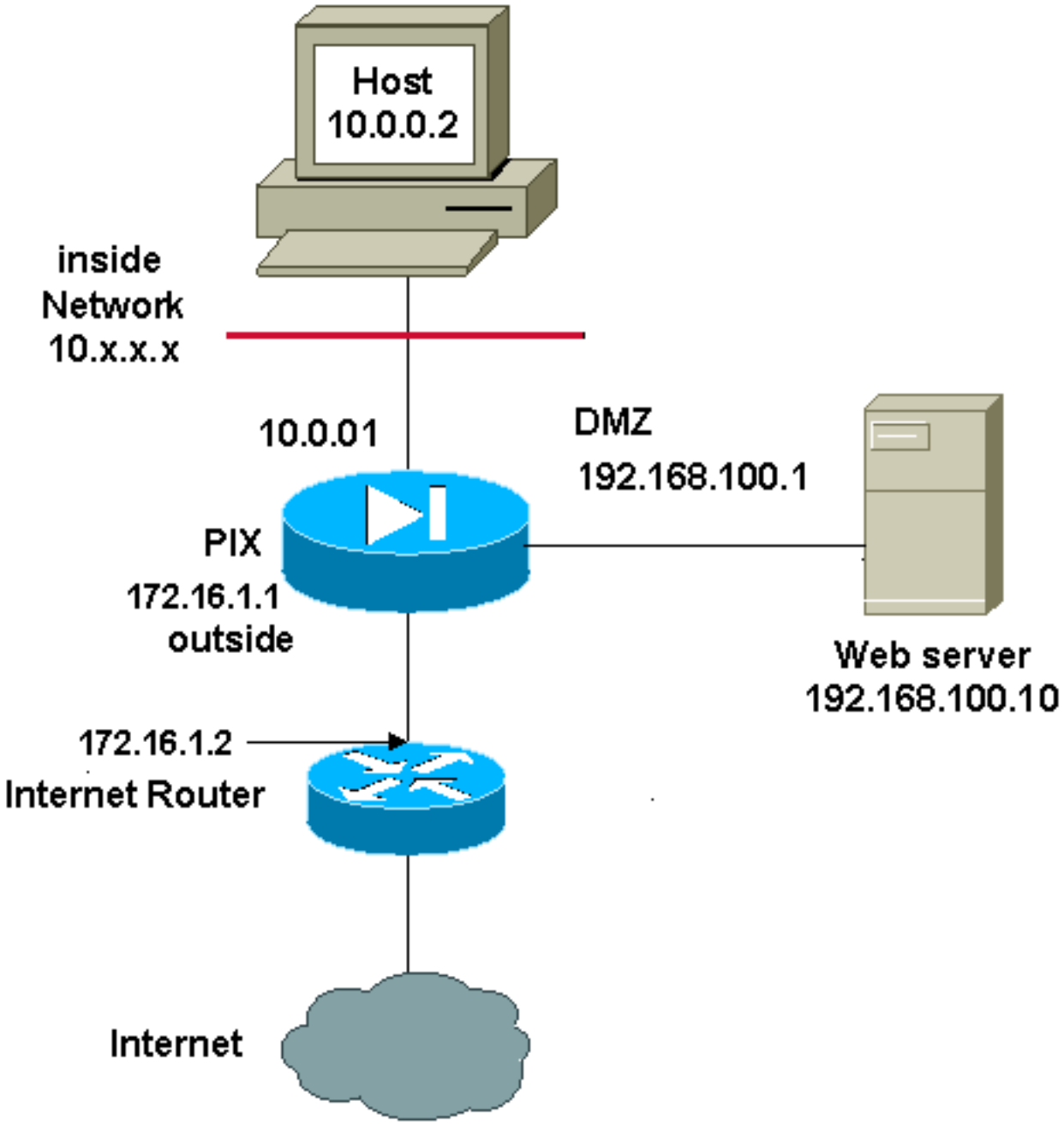
在本例中，網路管理器為埠80(Web)和埠23(Telnet)提供對目標IP地址192.168.201.11的訪問，但必須使用兩個不同的IP地址作為源地址。IP地址172.16.199.3用作Web的源地址。IP地址172.16.199.4用於Telnet，必須轉換10.0.0.0/8範圍內的所有內部地址。網路管理員可以執行以下操作：

```
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
```

您可以使用輸出直譯器工具(僅供註冊客戶使用)顯示潛在問題和修正程式。

靜態NAT

網路圖表



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

靜態NAT配置建立一對一對映，並將特定地址轉換為另一個地址。這種型別的配置在NAT表中建立永久條目（只要該配置存在），並使內部主機和外部主機都能啟動連線。這對於提供應用服務（如郵件、Web、FTP等）的主機最有用。在本示例中，靜態NAT語句配置為允許內部使用者和外部使用者訪問DMZ上的Web伺服器。

此輸出顯示了如何構造靜態語句。記下對映和實際IP地址的順序。

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

以下是已建立的靜態轉譯，用於讓內部介面上的使用者存取非軍事區上的伺服器。它建立內部地址與DMZ上伺服器的地址之間的對映。然後，內部使用者可以通過內部地址訪問DMZ上的伺服器。

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

以下是已建立的靜態轉譯，用於讓外部介面上的使用者訪問DMZ上的伺服器。它建立外部地址與DMZ上伺服器的地址之間的對映。然後，外部使用者可以通過外部地址訪問DMZ上的伺服器。

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

注意：由於外部介面的安全級別低於DMZ，因此還必須建立訪問清單，以允許外部使用者訪問DMZ上的伺服器。訪問清單必須授予使用者對靜態轉換中**對映地**址的訪問許可權。建議將此訪問清單設定得儘可能具體。在這種情況下，任何主機都只能訪問Web伺服器上的埠80(www/http)和443(https)。

```
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
```

然後，必須將訪問清單應用到外部介面。

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

如需**access-list**和access-group命令的詳細資訊，請參閱access-list extended和access-group。

如何繞過NAT

本節介紹如何繞過NAT。啟用NAT控制時，您可能希望繞過NAT。可以使用身份NAT、靜態身份NAT或NAT豁免來繞過NAT。

配置身份NAT

身份NAT將實際IP地址轉換為同一個IP地址。只有「已轉換」的主機可以建立NAT轉換，並且允許回發響應流量。

附註：如果更改NAT配置，並且不希望等待現有轉換超時，然後才使用新的NAT資訊，則使用**clear xlate**命令清除轉換表。但是，清除轉換表時，所有使用轉換的當前連線都將斷開。

要配置身份NAT，請輸入以下命令：

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

例如，要對內部10.1.1.0/24網路使用身份NAT，請輸入以下命令：

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

有關**nat**命令的詳細資訊，請參閱思科安全裝置命令參考7.2版。

配置靜態標識NAT

靜態身份NAT將實際IP地址轉換為同一個IP地址。轉換始終處於活動狀態，「已轉換」主機和遠端主機都可以發起連線。靜態身份NAT允許您使用常規NAT或策略NAT。在確定要轉換的實際地址時，通過策略NAT可以識別實際地址和目標地址(有關策略NAT的詳細資訊，請參閱使用策略NAT部分

)。 例如，當一個內部地址訪問外部介面並且目標為伺服器A時，可以對該內部地址使用策略靜態身份NAT，但在訪問外部伺服器B時使用普通轉換。

附註：如果刪除靜態命令，則使用轉換的當前連線不會受到影響。若要移除這些連線，請輸入clear local-host 指令。不能使用**clear xlate**命令從轉換表中清除靜態轉換；您必須改為移除static命令。使用clear xlate 命令只能刪除nat和全域性命令建立的動態轉換。

要配置策略靜態標識NAT，請輸入以下命令：

```
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]
```

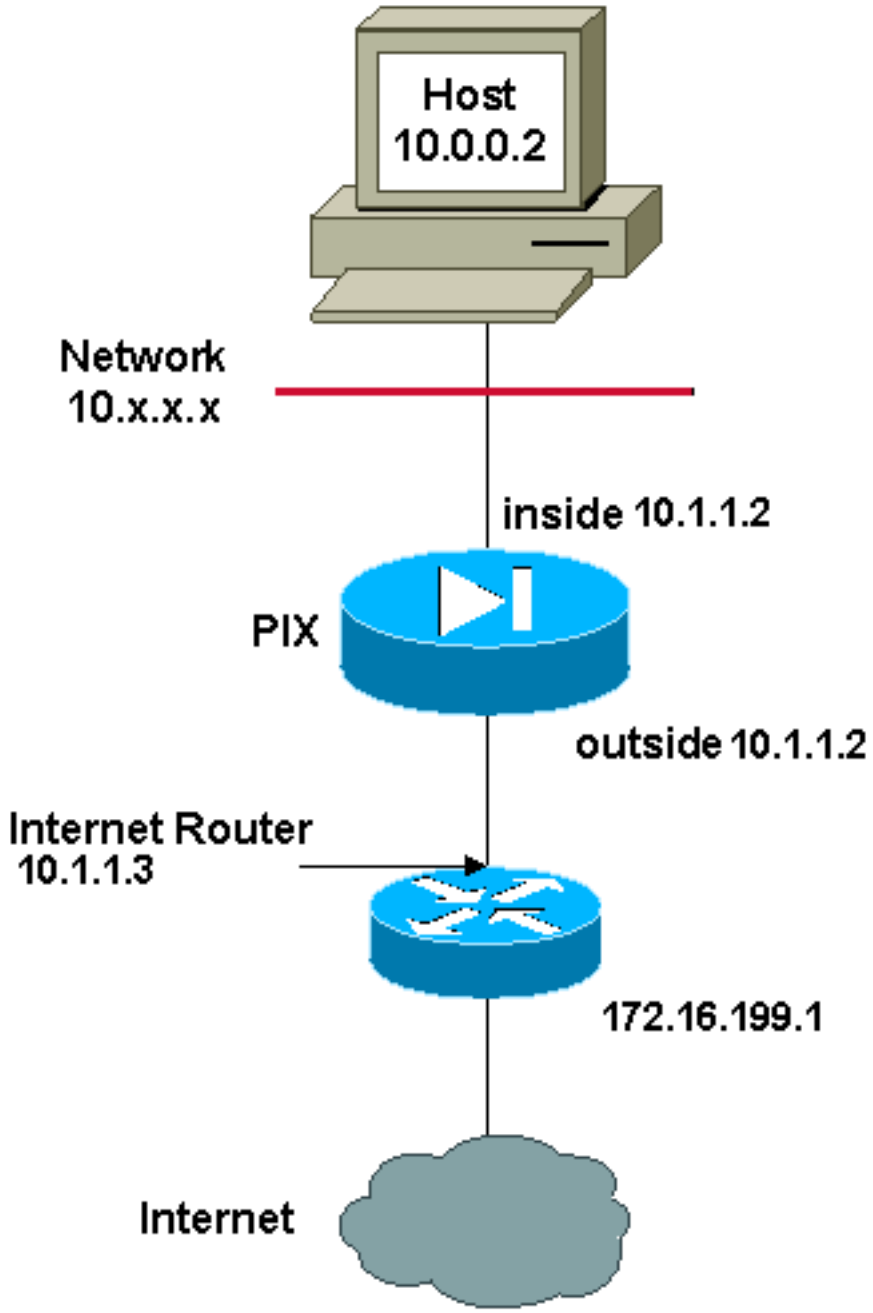
使用**access-list extended**命令以建立擴展訪問清單。此訪問清單應僅包含允許ACE。確儲存取清單中的來源位址與此指令中的real_ip相符。策略NAT不考慮inactive或time-range關鍵字；對於策略NAT配置，所有ACE都被視為處於活動狀態。如需詳細資訊，請參閱使用原則NAT一節。

要配置常規靜態身份NAT，請輸入以下命令：

```
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]
```

為兩個real_ip引數指定相同的IP地址。

網路圖表



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

例如，當外部訪問時，此命令對內部IP地址(10.1.1.2)使用靜態身份NAT:

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

有關static命令的詳細資訊，請參閱思科安全裝置命令參考7.2版。

當內部訪問外部地址(172.16.199.1)時，此命令使用靜態身份NAT:

```
hostname(config)#static (outside,inside) 172.16.199.1
 172.16.199.1 netmask 255.255.255.255
```

此命令靜態對映整個子網：

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

此靜態身份策略NAT示例顯示訪問一個目標地址時使用身份NAT的單個實際地址，訪問另一個目標地址時使用轉換：

```
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
```

附註： 有關**static**命令的詳細資訊，請參閱Cisco ASA 5580自適應安全裝置命令參考8.1版。

附註： 有關訪問清單的詳細資訊，請參閱Cisco ASA 5580自適應安全裝置命令列配置指南8.1版。

配置NAT免除

NAT免除將地址排除在轉換之外，並允許實際主機和遠端主機發起連線。NAT免除允許您在確定要免除的實際流量時指定實際地址和目標地址（類似於策略NAT），因此使用NAT免除比身份NAT具有更大的控制能力。但是，與策略NAT不同的是，NAT免除不考慮訪問清單中的埠。使用靜態身份NAT來考慮訪問清單中的埠。

附註：如果刪除NAT免除配置，使用NAT免除的現有連線不會受到影響。要刪除這些連線，請輸入clear local-host命令。

要配置NAT免除，請輸入以下命令：

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

使用access-list extended命令建立擴展訪問清單。此訪問清單可同時包含允許ACE和拒絕ACE。請勿在存取清單中指定實際連線埠和目的地連線埠；NAT免除不考慮埠。NAT免除也不考慮inactive或time-range關鍵字；對於NAT免除配置，所有ACE都被視為處於活動狀態。

預設情況下，此命令豁免從內部到外部的流量。如果您希望從外部到內部的流量繞過NAT，則新增一個額外的**nat**命令並輸入outside以將NAT例項標識為外部NAT。如果為外部介面配置動態NAT並要免除其他流量，則可能需要使用外部NAT免除。

例如，要在訪問任何目標地址時排除內部網路，請輸入以下命令：

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


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

若要對DMZ網路使用動態外部NAT，並豁免另一個DMZ網路，請輸入以下命令：

```
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
```

要在訪問兩個不同的目標地址時排除內部地址，請輸入以下命令：

```
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
```

驗證

流經安全裝置的流量最有可能通過NAT。請參閱PIX/ASA:監控和解決效能問題，以驗證安全裝置上正在使用的轉換。

show xlate count命令顯示通過PIX的當前和最大轉換數。轉換是內部地址到外部地址的對映，可以是一對一對映（如NAT）或多對一對映（如PAT）。此命令是**show xlate**命令的子集，它通過PIX輸出每個轉換。命令輸出顯示「使用中」轉換，這是指發出命令時PIX中的活動轉換數；「最常用」是指自PIX通電以來在PIX上見過的最大轉換數。

疑難排解

為埠443新增靜態PAT時收到錯誤消息

問題

當您為埠443新增靜態PAT時，會收到以下錯誤消息：

```
[] static(INSIDEOUTSIDE)tcp interface 443 192.168.1.87 443 netmask 255.255.255 tcp 0 udp 0

PAT443
```

解決方案

當ASDM或WEBVPN在443埠上運行時，會出現此錯誤消息。為了解決此問題，請登入防火牆，然後完成以下步驟之一：

- 若要將ASDM埠更改為443以外的任何埠，請運行以下命令：
  ```
  ASA(config)#no http server enable
  ASA(config)#http server enable 8080
  ```

- 若要將WEBVPN埠更改為443以外的任何埠，請運行以下命令：
  ```
  ASA(config)#webvpn
  ASA(config-webvpn)#enable outside
  ASA(config-webvpn)#port 65010
  ```

運行這些命令後，您應該能夠將埠443上的NAT/PAT新增到另一台伺服器。以後嘗試使用ASDM管理ASA時，請將新埠指定為8080。

錯誤：對映地址與現有靜態地址衝突

問題

在ASA上新增靜態語句時收到此錯誤：

解決方案

驗證要新增的靜態源項是否已經存在。

相關資訊

- PIX支援頁
- PIX命令參考
- ASA支援頁
- ASA命令參考
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems