ASA 7.x/PIX 6.x及更高版本：開啟/封鎖連線埠組態範例

目錄

簡介

本文提供一個範例組態，說明如何為安全裝置中各種型別的流量（例如http或ftp）開啟或封鎖連線埠。

注意：「開啟埠」和「允許埠」這兩個術語具有相同的含義。同樣，「阻塞埠」和「限制埠」也具有相同的含義。

必要條件

需求

本文檔假設PIX/ASA已配置且工作正常。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行8.2(1)版的Cisco 5500系列調適型安全裝置(ASA)
- 思科調適型安全裝置管理員(ASDM)版本6.3(5)

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。

相關產品

此配置還可以與軟體版本6.x及更高版本的Cisco 500系列PIX防火牆裝置配合使用。

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。

設定

每個介面的安全級別必須介於0（最低）到100（最高）之間。 例如，您必須將最安全的網路（例如內部主機網路）分配到第100級。雖然連線到Internet的外部網路可以是0級，但其他網路（例如DMZ）可以位於兩者之間。您可以將多個介面分配給相同的安全級別。

預設情況下，在外部介面（安全級別0）上阻止所有埠，並且在安全裝置的內部介面（安全級別100）上開啟所有埠。通過這種方式，所有出站流量都可以通過安全裝置，而無需進行任何配置，但可以通過安全裝置中的訪問清單和靜態命令配置來允許入站流量。

注意：一般情況下，從較低安全區域到較高安全區域的所有埠都會被阻止，並且從較高安全區域到較低安全區域的所有埠都會開啟，前提是對入站和出站流量啟用狀態檢查。

本節包括以下小節：

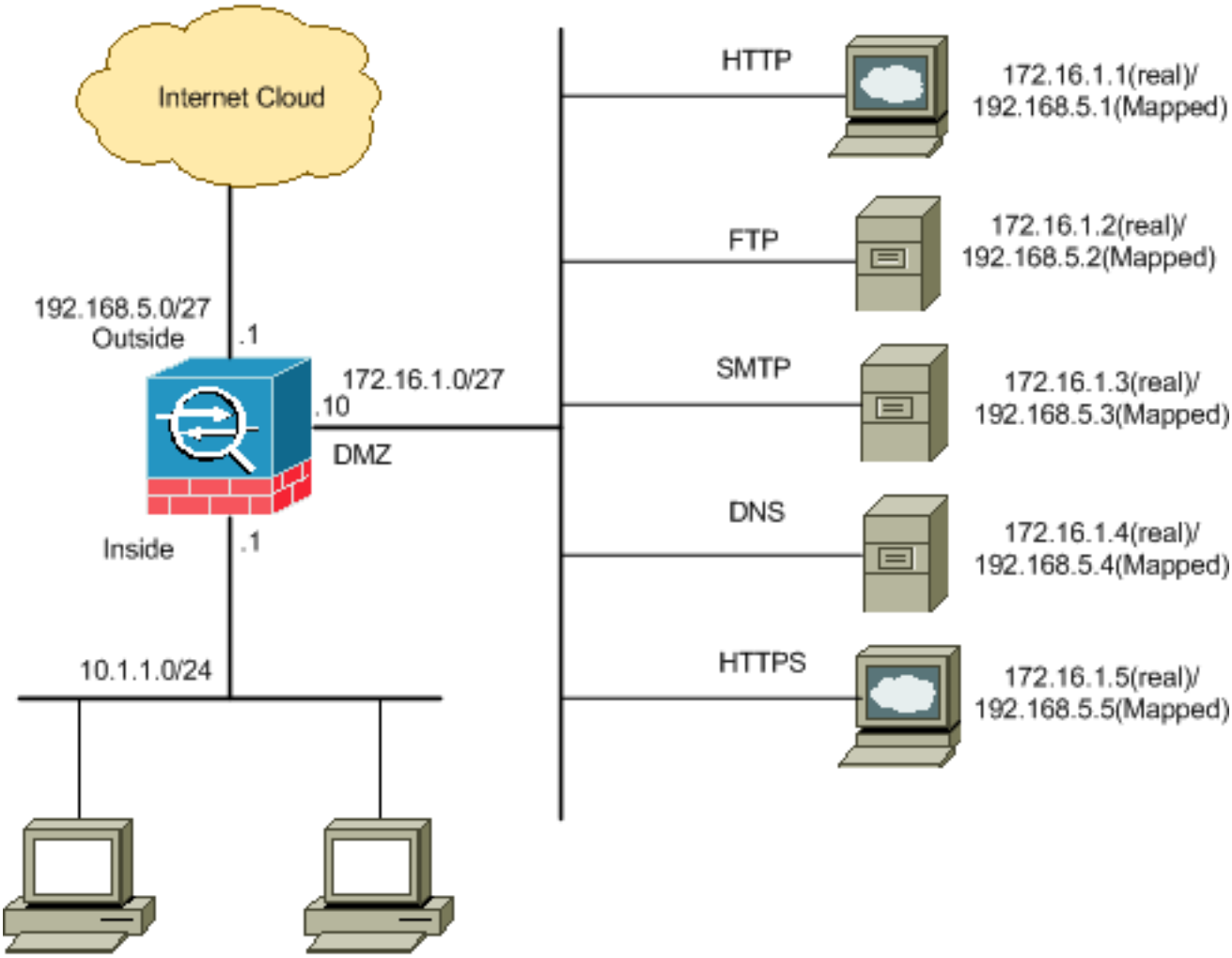
- 網路圖表
- 阻塞埠配置
- 開啟埠配置

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



阻塞埠配置

除非擴展訪問清單明確阻止任何出站流量，否則安全裝置允許任何出站流量。

訪問清單由一個或多個訪問控制條目組成。視存取清單型別而定，您可以指定來源和目的地位址、通訊協定、連線埠（適用於TCP或UDP）、ICMP型別（適用於ICMP）或EtherType。

注意：對於無連線協定（如ICMP），安全裝置會建立單向會話，因此您需要訪問清單來允許兩個方向的ICMP（通過將訪問清單應用到源和目標介面），或者需要啟用ICMP檢測引擎。ICMP檢測引擎將ICMP會話視為雙向連線。

完成這些步驟即可封鎖連線埠，這些連線埠通常適用於從內部（較高安全區域）到DMZ（較低安全區域）或DMZ到外部的流量。

1. 以阻止指定埠流量的方式建立訪問控制清單。

```
access-list
```

2. 然後使用access-group命令繫結訪問清單以便處於活動狀態。

```
access-group
```

示例：

1. **阻止HTTP埠流量：**若要阻止內部網路10.1.1.0存取IP為172.16.1.1且位於DMZ網路中的http（Web伺服器），請建立一個ACL，如下所示：

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

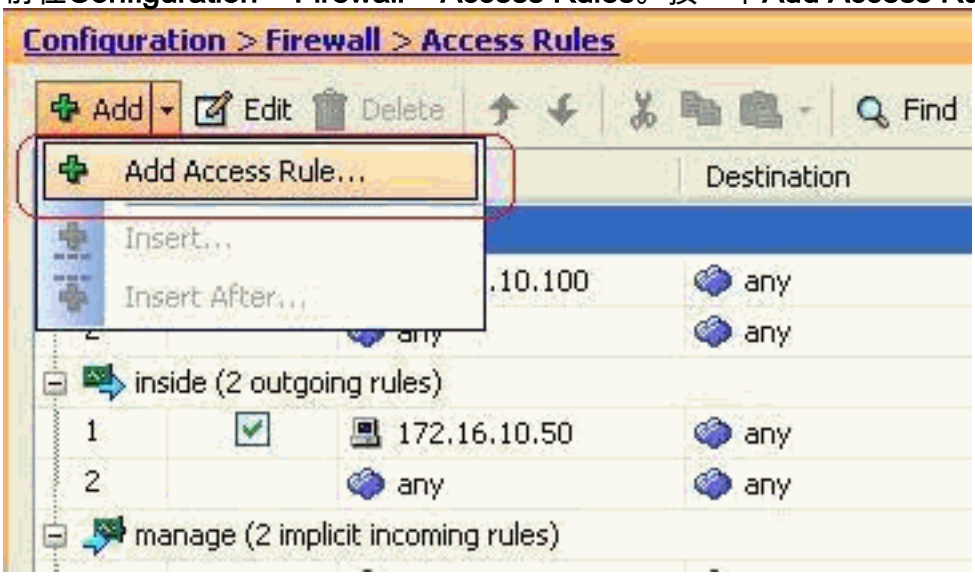
   注意：使用no，然後使用access list命令以刪除埠阻塞。
2. **封鎖FTP連線埠流量：**若要阻止內部網路10.1.1.0存取FTP（檔案伺服器）（IP為172.16.1.2）且放在DMZ網路中，請建立一個ACL，如下所示：

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

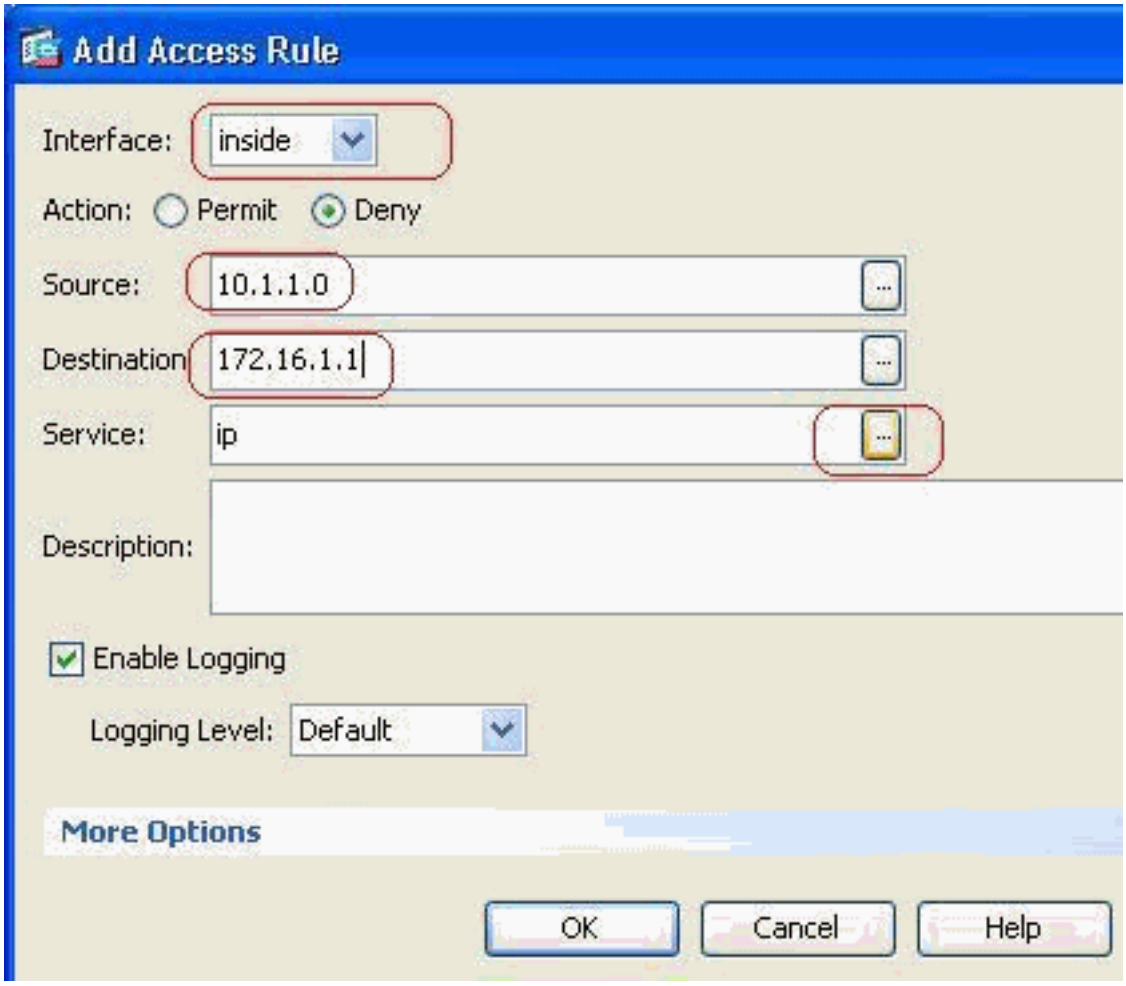
注意：請參閱IANA埠以瞭解有關埠分配的更多資訊。

本節顯示了通過ASDM執行此操作的逐步配置。

1. 前往**Configuration > Firewall > Access Rules**。按一下**Add Access Rule**以建立訪問清單。

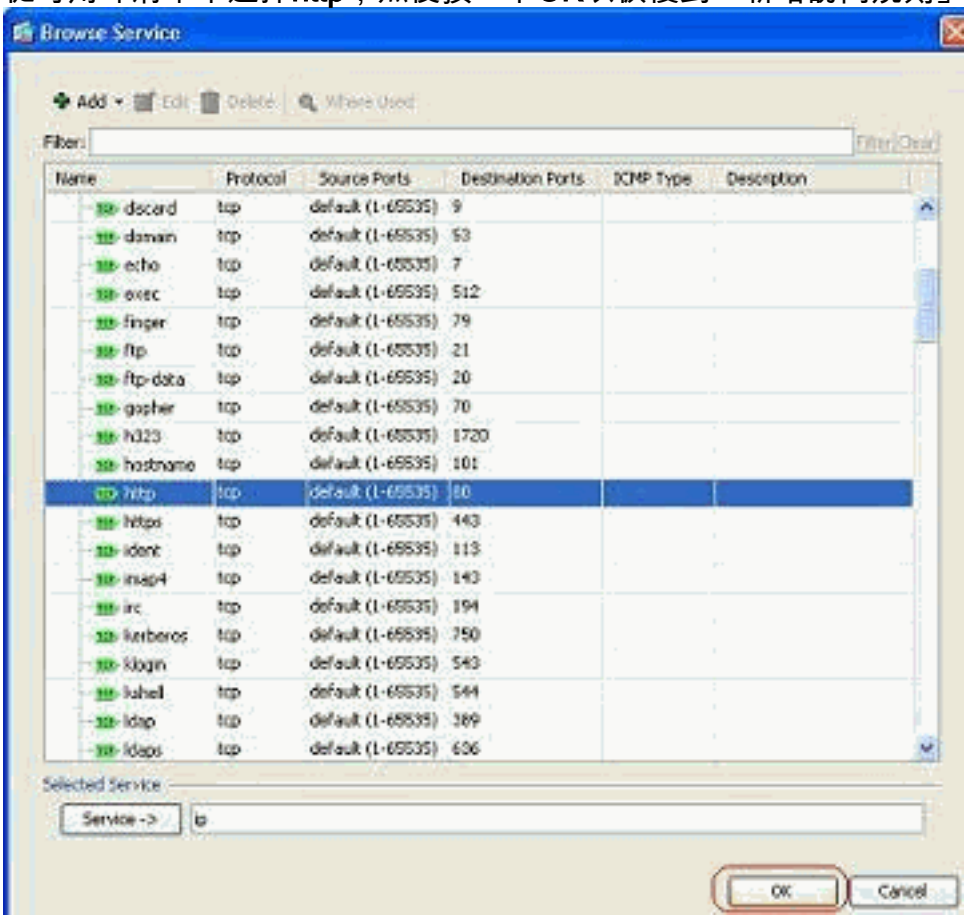


2. 定義訪問規則的源、目標和操作以及與此訪問規則關聯的介面。選擇詳細資訊以選擇要阻止的

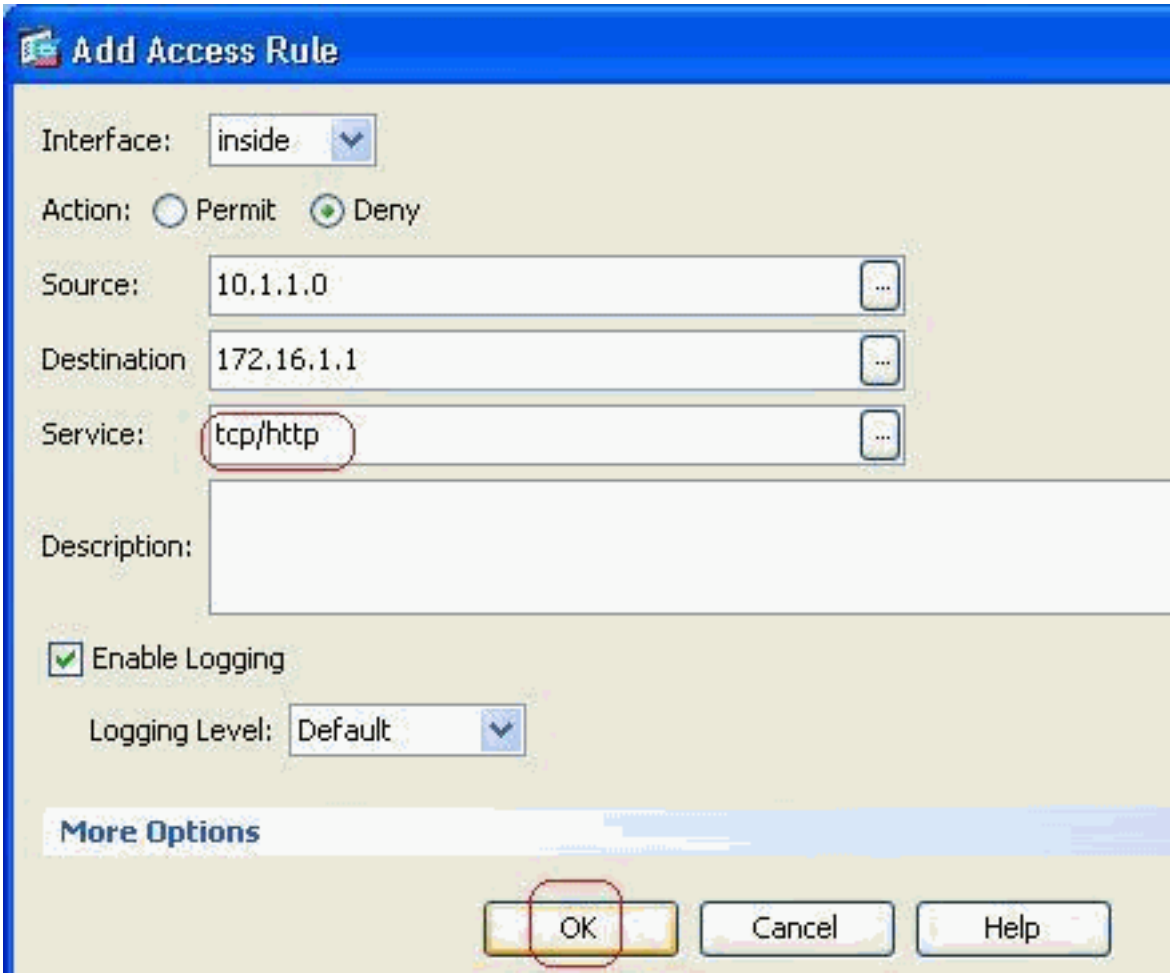


特定埠。

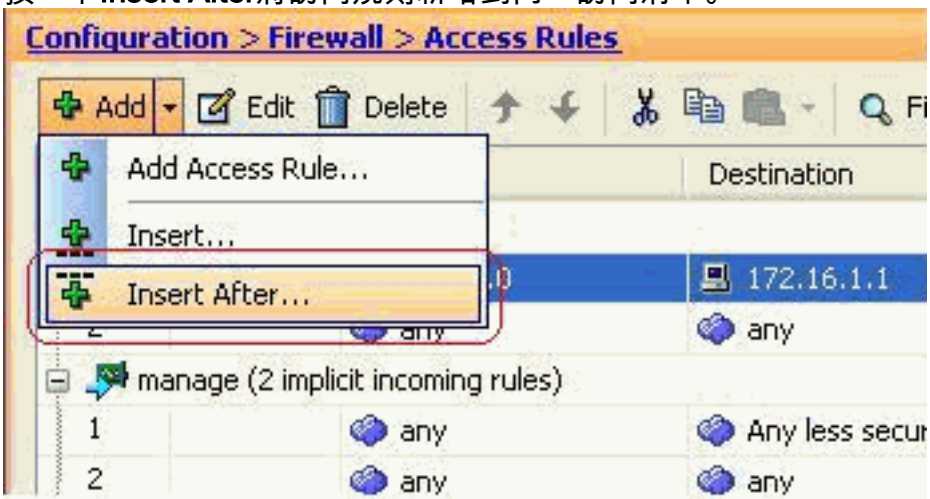
3. 從可用埠清單中選擇**http**，然後按一下**OK**以恢復到「新增訪問規則」視窗。



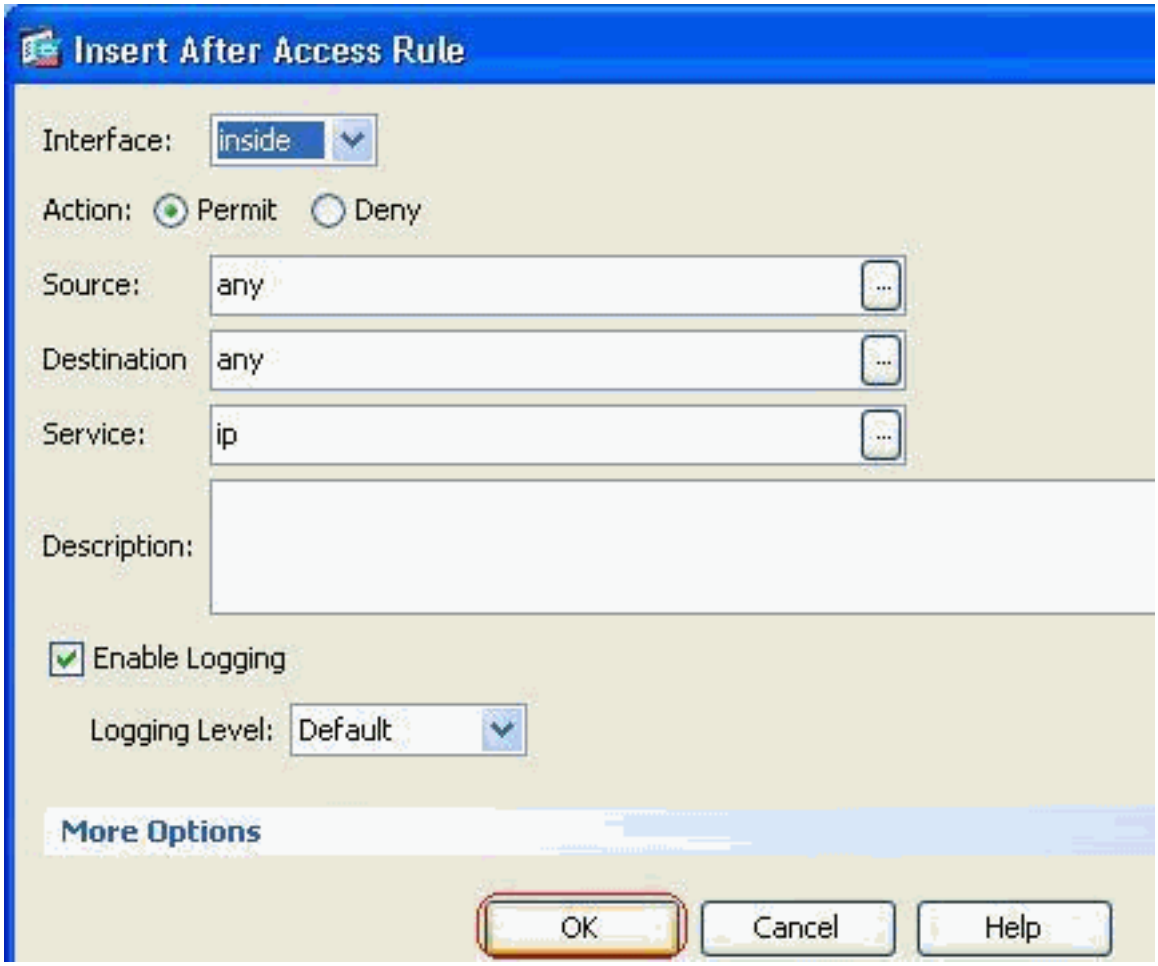
4. 按一下**OK**完成訪問規則的配置。



5. 按一下**Insert After**將訪問規則新增到同一訪問清單。

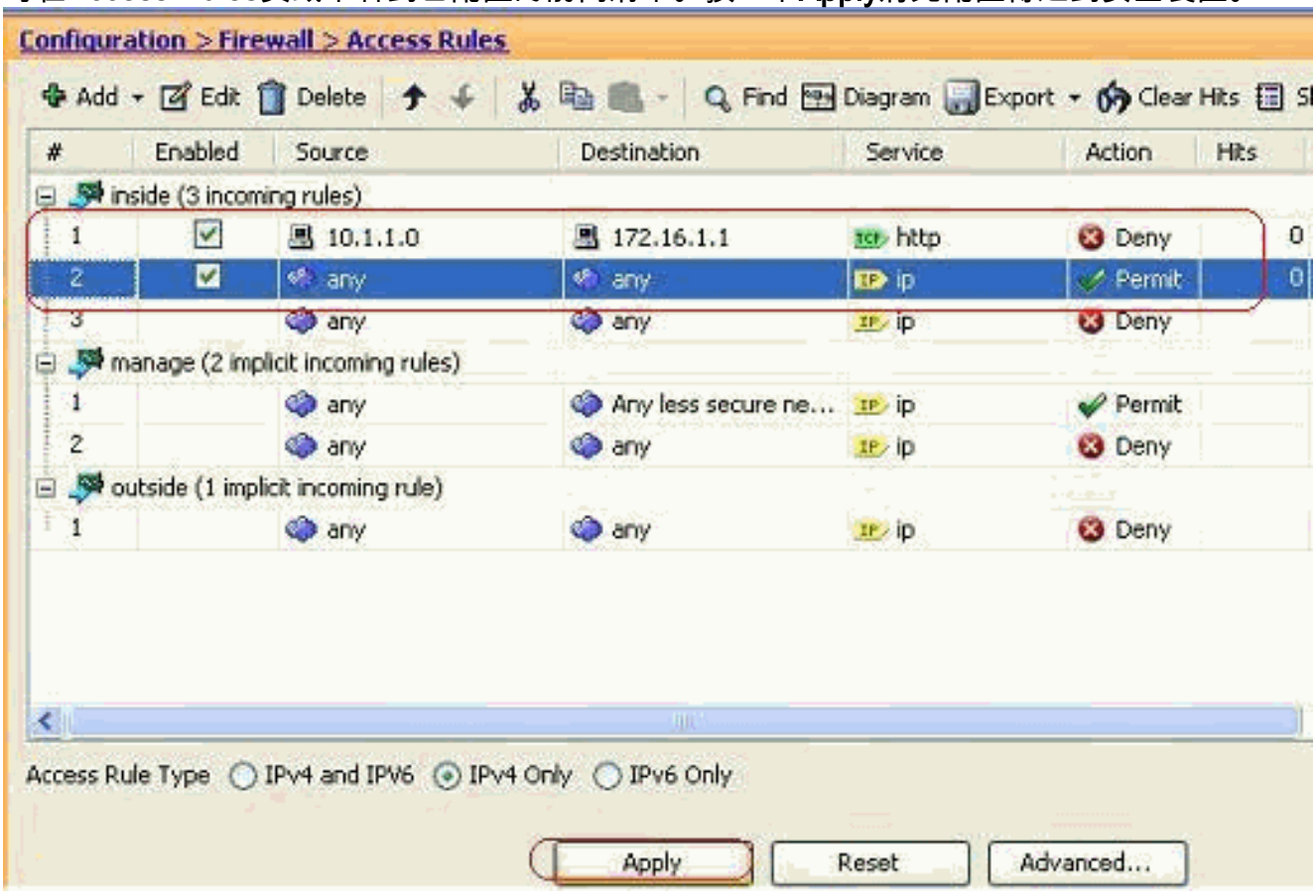


6. 允許從「any」到「any」的流量防止「Implicit deny」。 然後，按一下**OK**完成新增此訪問規



則。

7. 可在Access Rules頁籤中看到已配置的訪問清單。按一下**Apply**將此配置傳送到安全裝置。

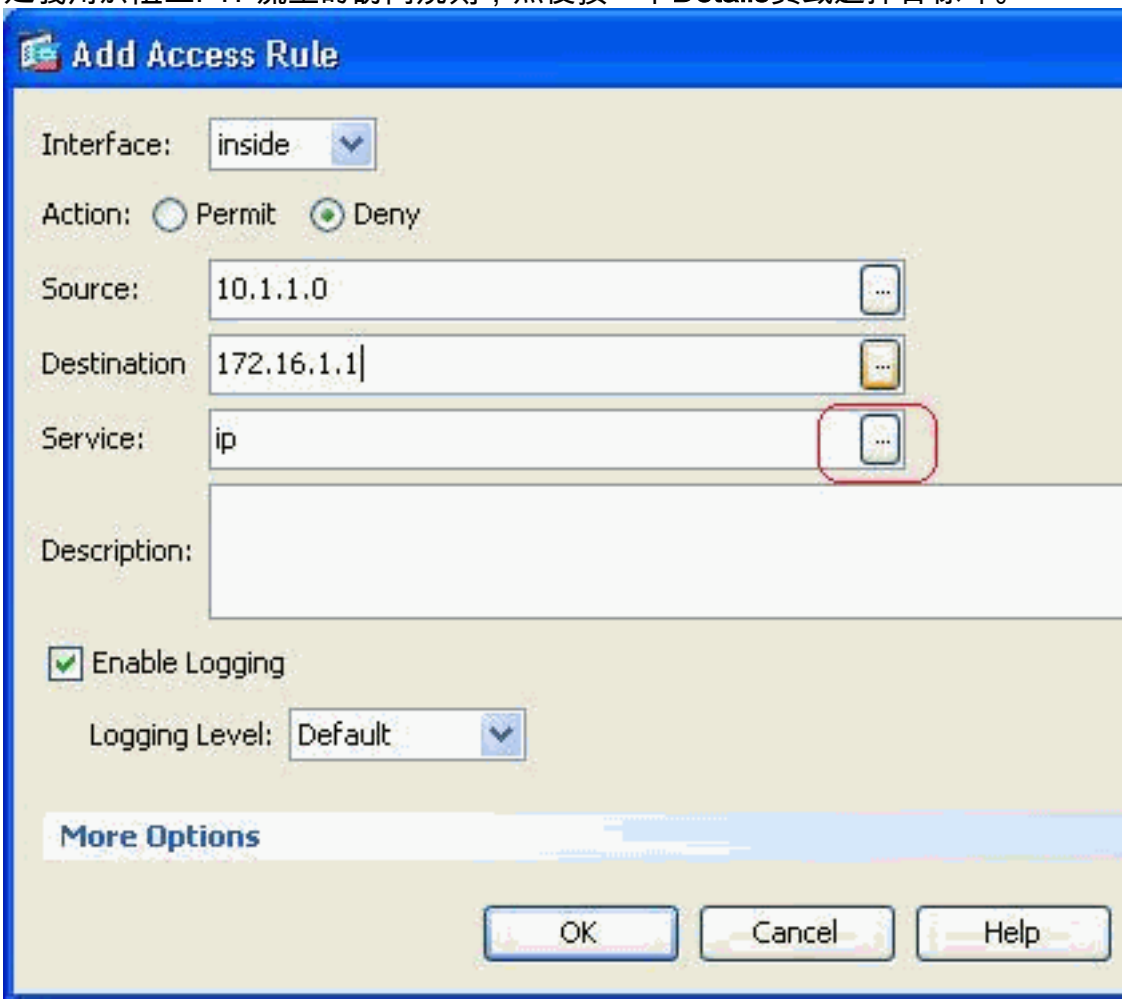


從ASDM傳送的配置將在ASA的命令列介面(CLI)上生成這組命令。

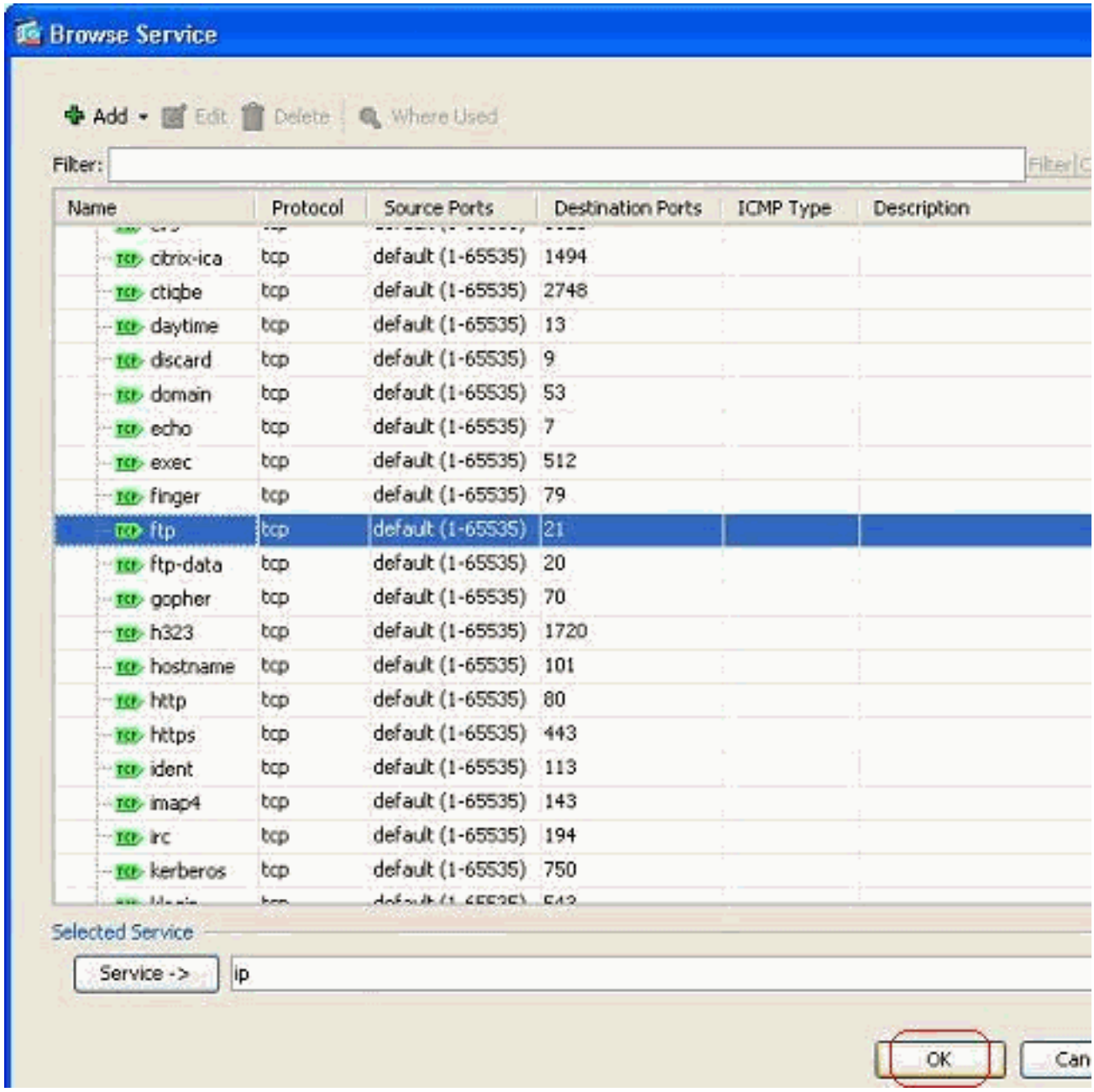
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

通過這些步驟，已通過ASDM執行示例1以阻止10.1.1.0網路訪問Web伺服器172.16.1.1。示例2還可以以相同的方式阻止整個10.1.1.0網路訪問FTP伺服器172.16.1.2。唯一的區別是在選擇埠時。**注意：**例如2的此訪問規則配置假定為全新配置。

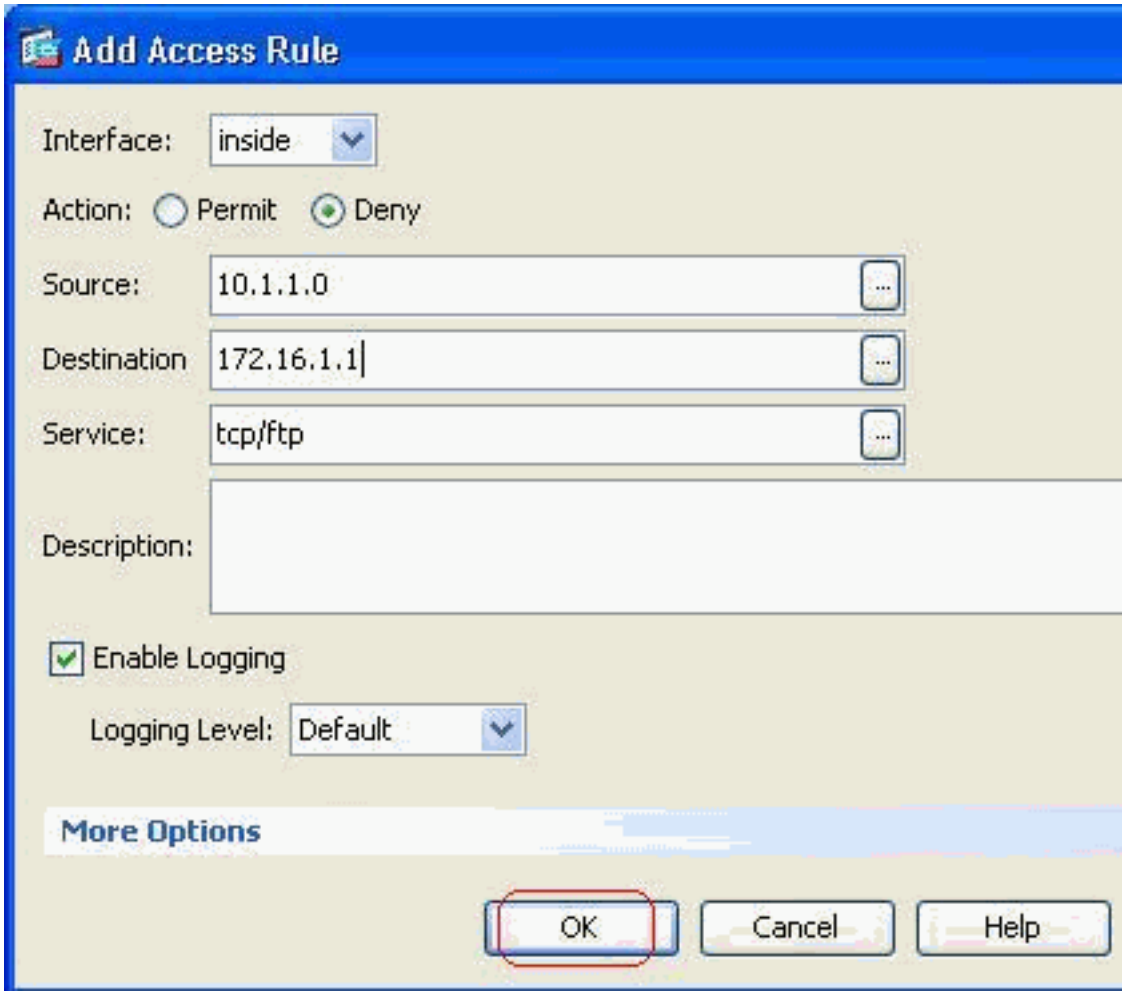
8. 定義用於阻止FTP流量的訪問規則，然後按一下**Details**頁籤選擇目標埠。



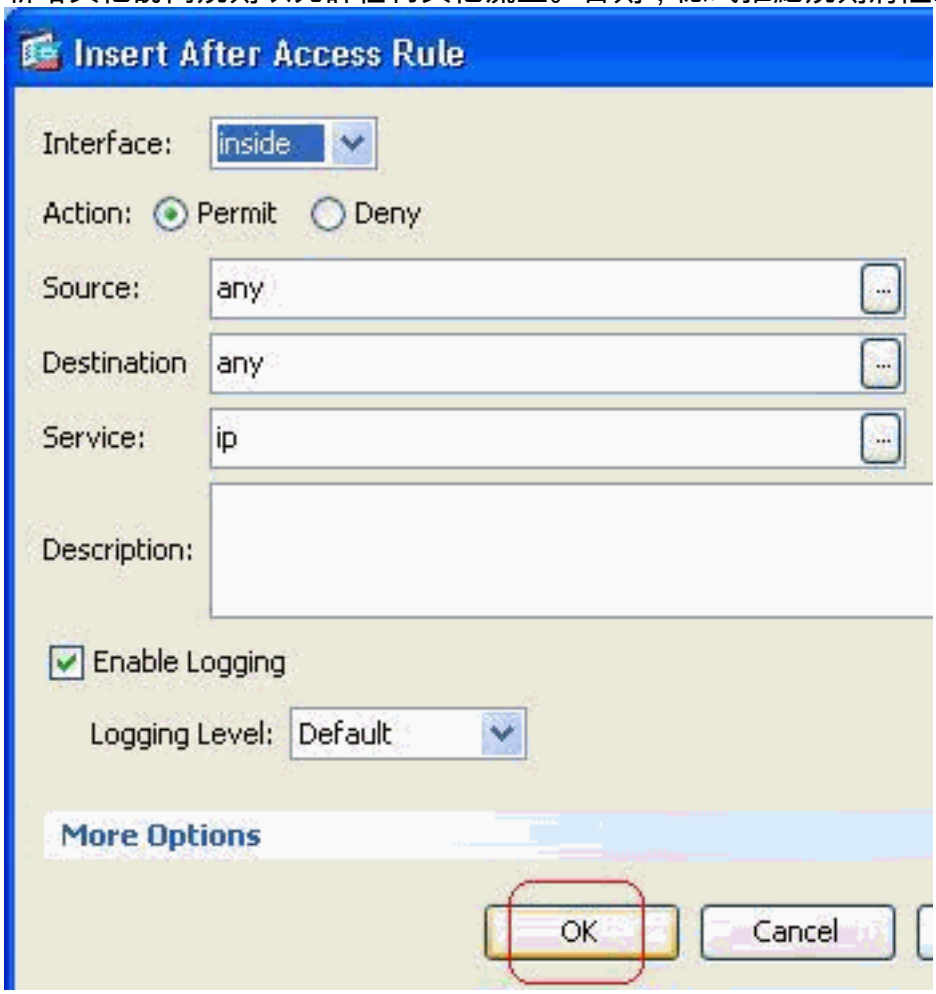
9. 選擇**ftp**埠，然後按一下**OK**以恢復到Add Access Rule視窗。



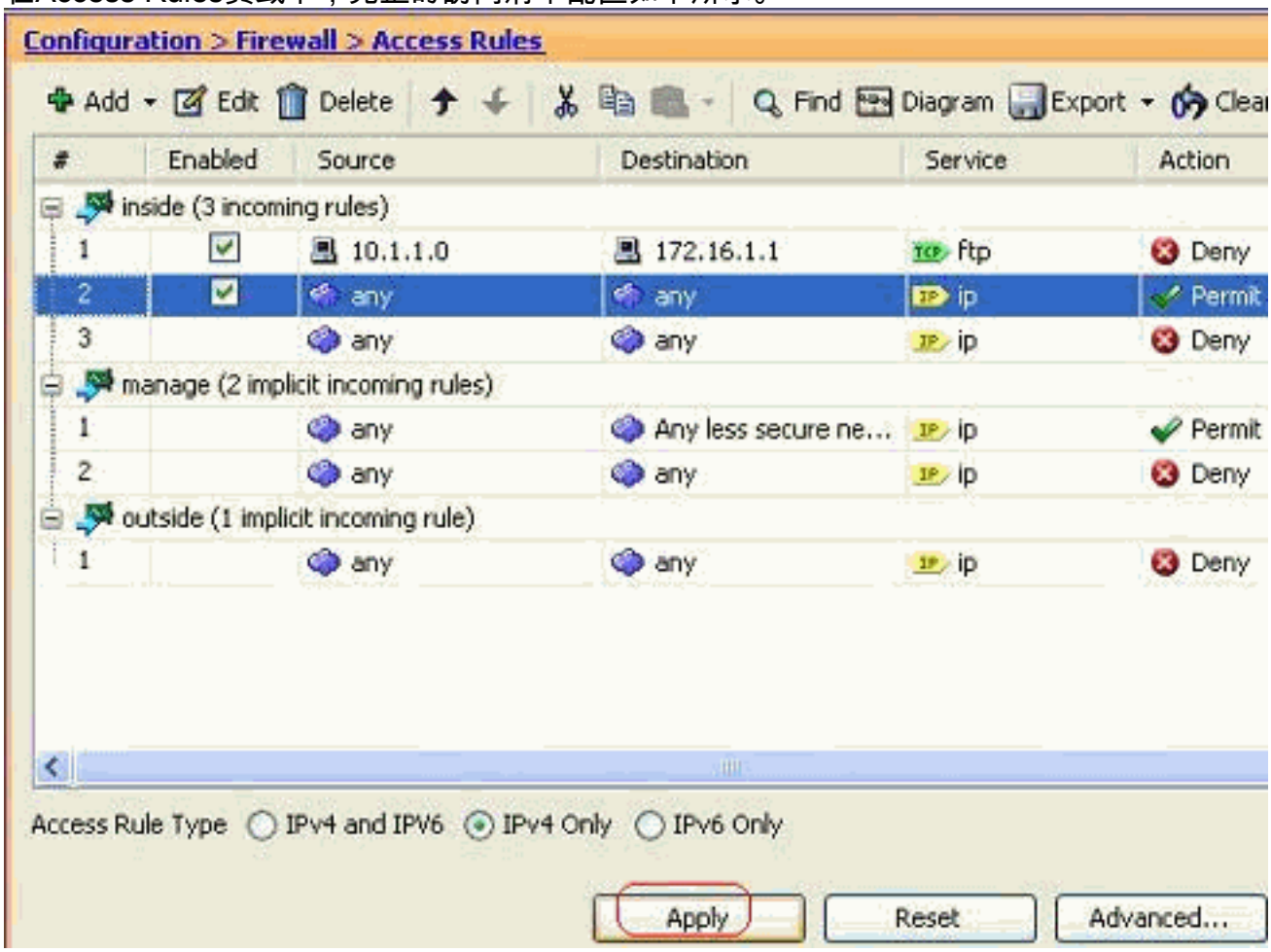
10. 按一下**OK**完成訪問規則的配置。



11. 新增其他訪問規則以允許任何其他流量。否則，隱式拒絕規則將阻止此介面上的所有流量。



12. 在Access Rules頁籤下，完整的訪問清單配置如下所示。



13. 按一下**Apply**將配置傳送到ASA。等效的CLI配置如下所示：

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

開啟埠配置

除非擴展訪問清單明確允許，否則安全裝置不允許任何入站流量。

如果要允許外部主機訪問內部主機，可以在外部介面上應用入站訪問清單。您需要指定訪問清單中內部主機的轉換地址，因為轉換後的地址是可用於外部網路的地址。完成以下步驟，即可開啟從較低安全區域到較高安全區域的連線埠。例如，允許從外部（較低安全區域）到內部介面（較高安全區域）或DMZ到內部介面的流量。

1. 靜態NAT將實際地址轉換為對映地址。此對映地址是託管在Internet上的地址，可用於訪問DMZ上的應用伺服器，而無需知道伺服器的實際地址。

```
static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
   access-list access_list_name | interface}
```

   請參閱PIX/ASA命令參考的靜態NAT部分以瞭解詳細資訊。
2. 建立ACL以允許特定連線埠流量。

```
access-list
```

3. 使用**access-group**命令繫結訪問清單以便處於活動狀態。

```
access-group
```

示例：

1. **開啟SMTP埠流量：**開啟埠**tcp 25**，以允許來自外部(Internet)的主機訪問位於DMZ網路中的郵件伺服器。**Static**命令將外部地址192.168.5.3對映到實際DMZ地址172.16.1.3。

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **開啟HTTPS連線埠流量：**開啟埠**tcp 443**，以允許來自外部(Internet)的主機訪問放置在DMZ網路中的Web伺服器（安全）。

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **允許DNS流量：**開啟埠**udp 53**，以允許來自外部(Internet)的主機訪問位於DMZ網路中的DNS伺服器（安全）。

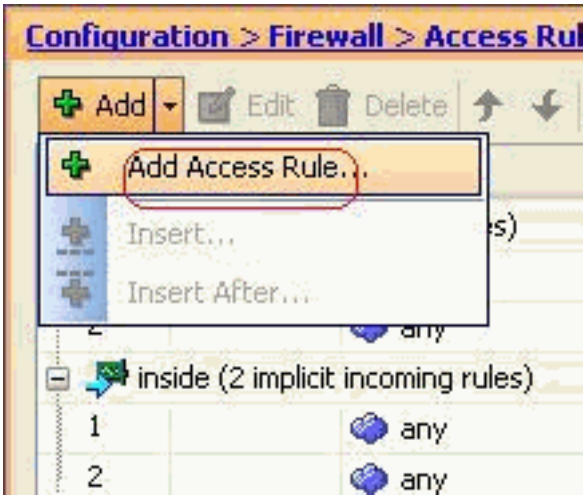
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

注意：請參閱IANA埠以瞭解有關埠分配的更多資訊。

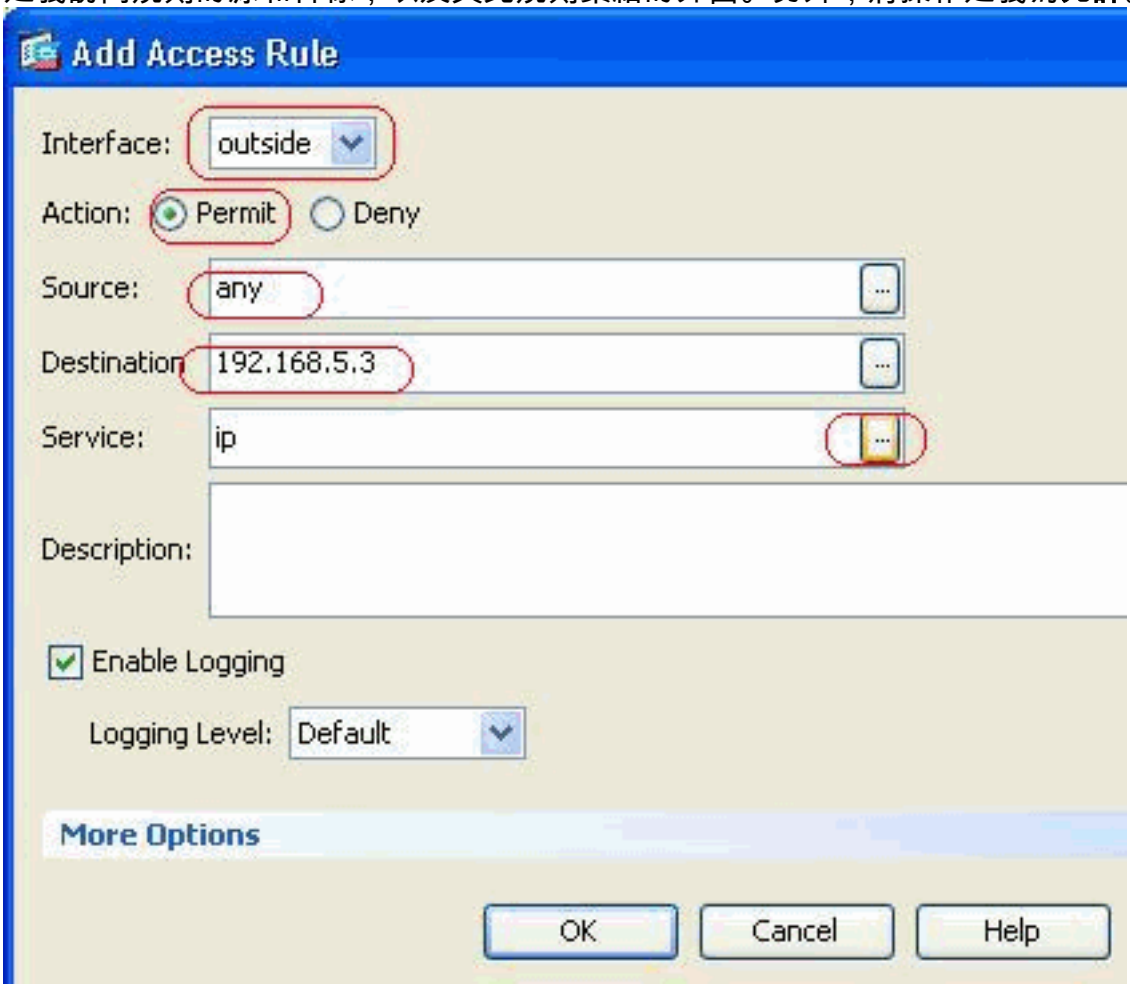
通過ASDM配置

本節顯示了通過ASDM執行上述任務的逐步方法。

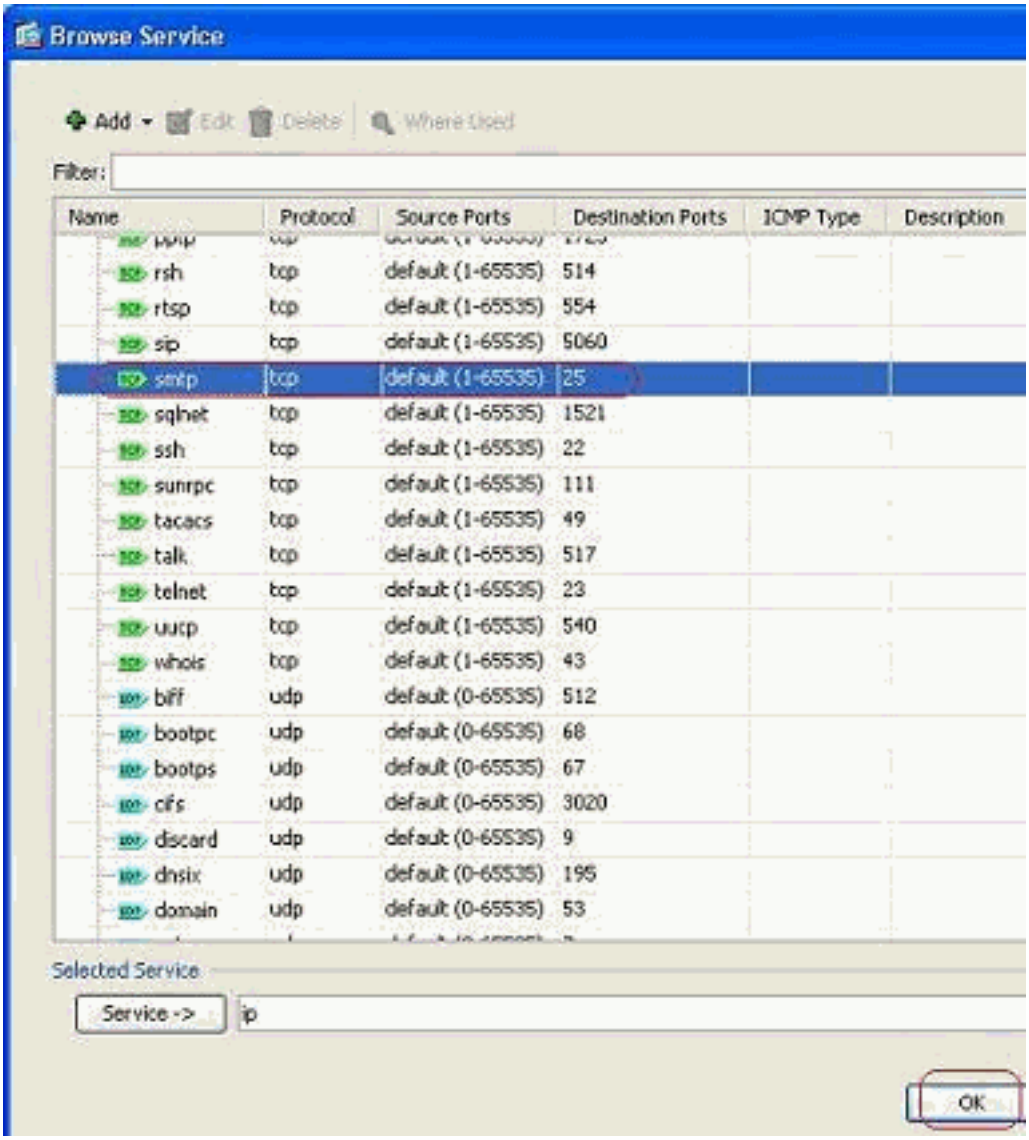
1. 建立允許到192.168.5.3伺服器的smtp流量的訪問規則。



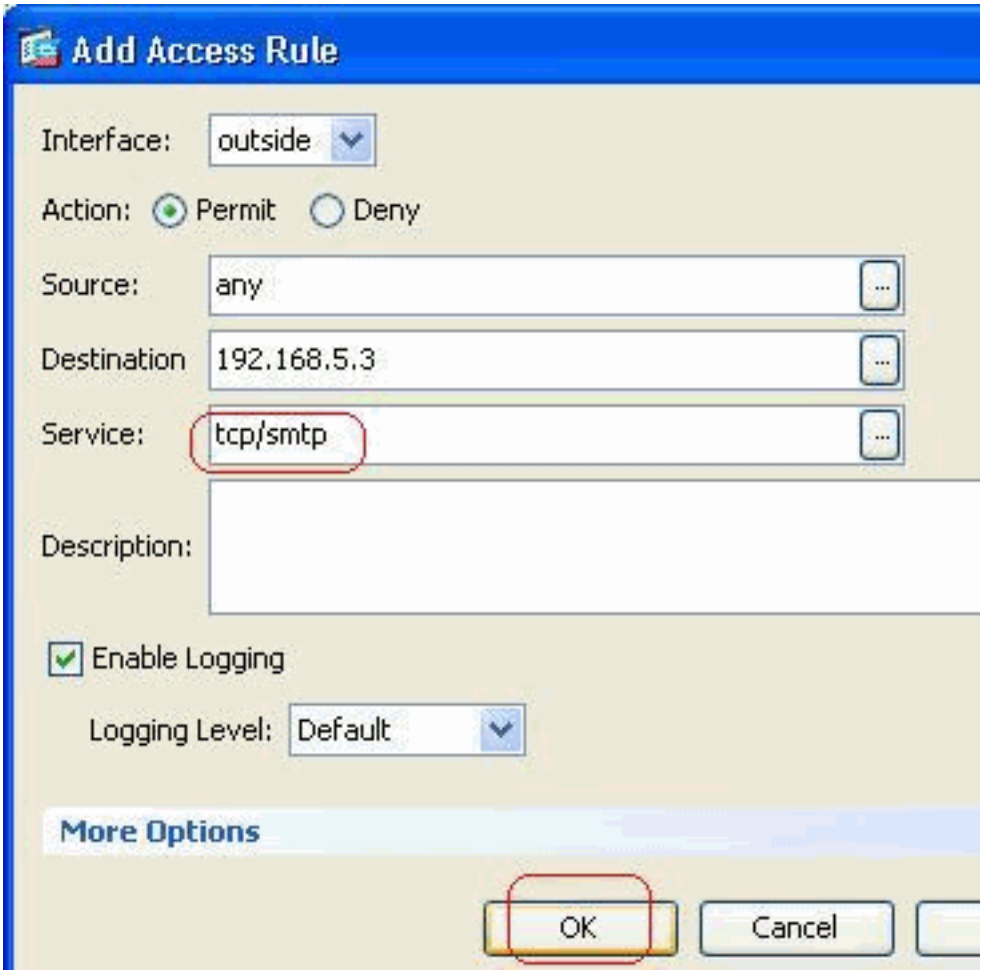
2. 定義訪問規則的源和目標，以及與此規則繫結的介面。另外，將操作定義為**允許**。



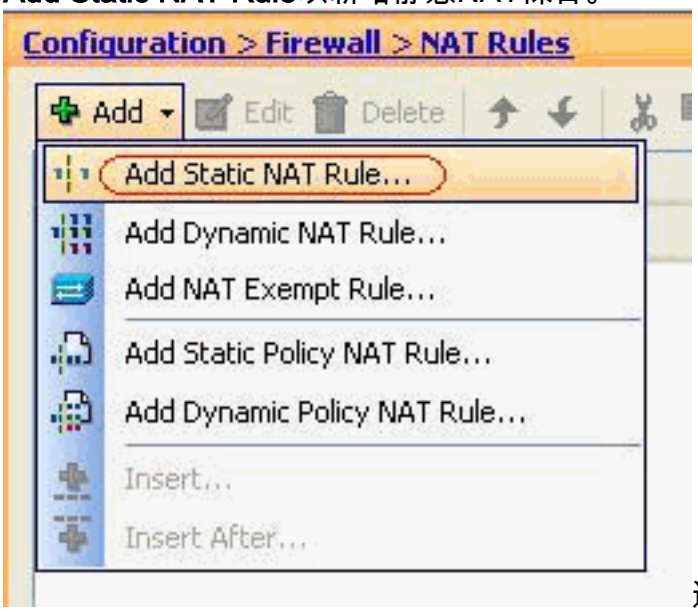
3. 選擇**SMTP**作為埠，然後按一下**OK**。



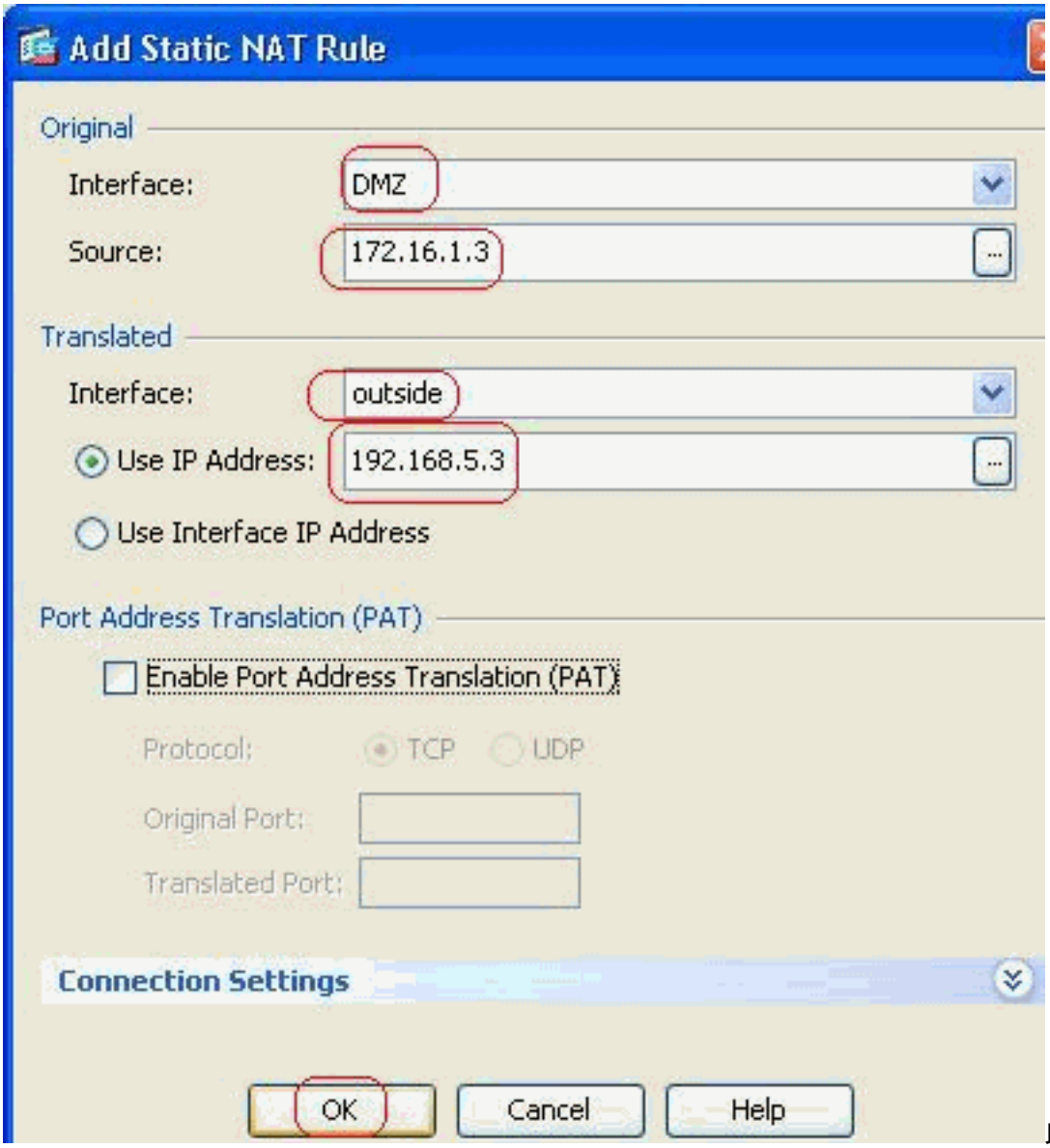
4. 按一下**OK**完成訪問規則的配置。



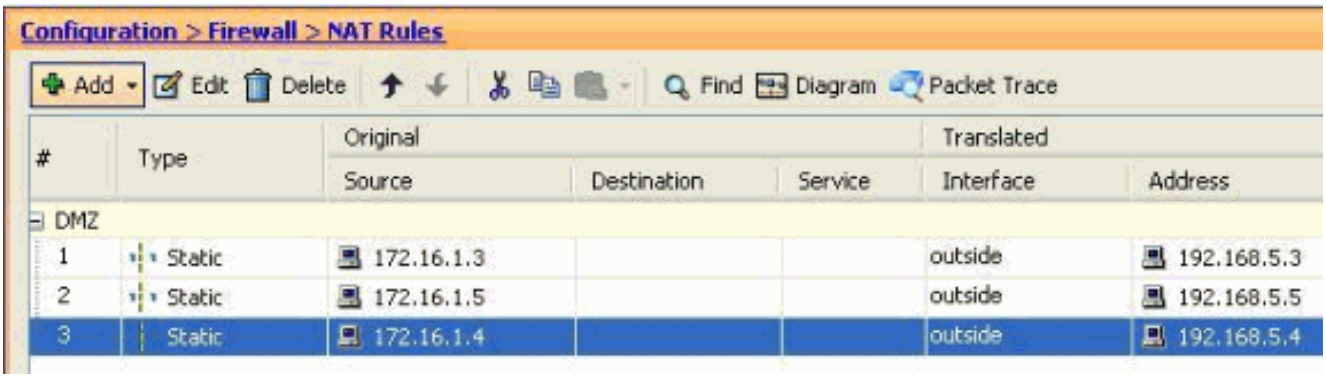
5. 配置靜態NAT以將172.16.1.3轉換為192.168.5.3轉到**Configuration > Firewall > NAT Rules > Add Static NAT Rule**以新增靜態NAT條目。



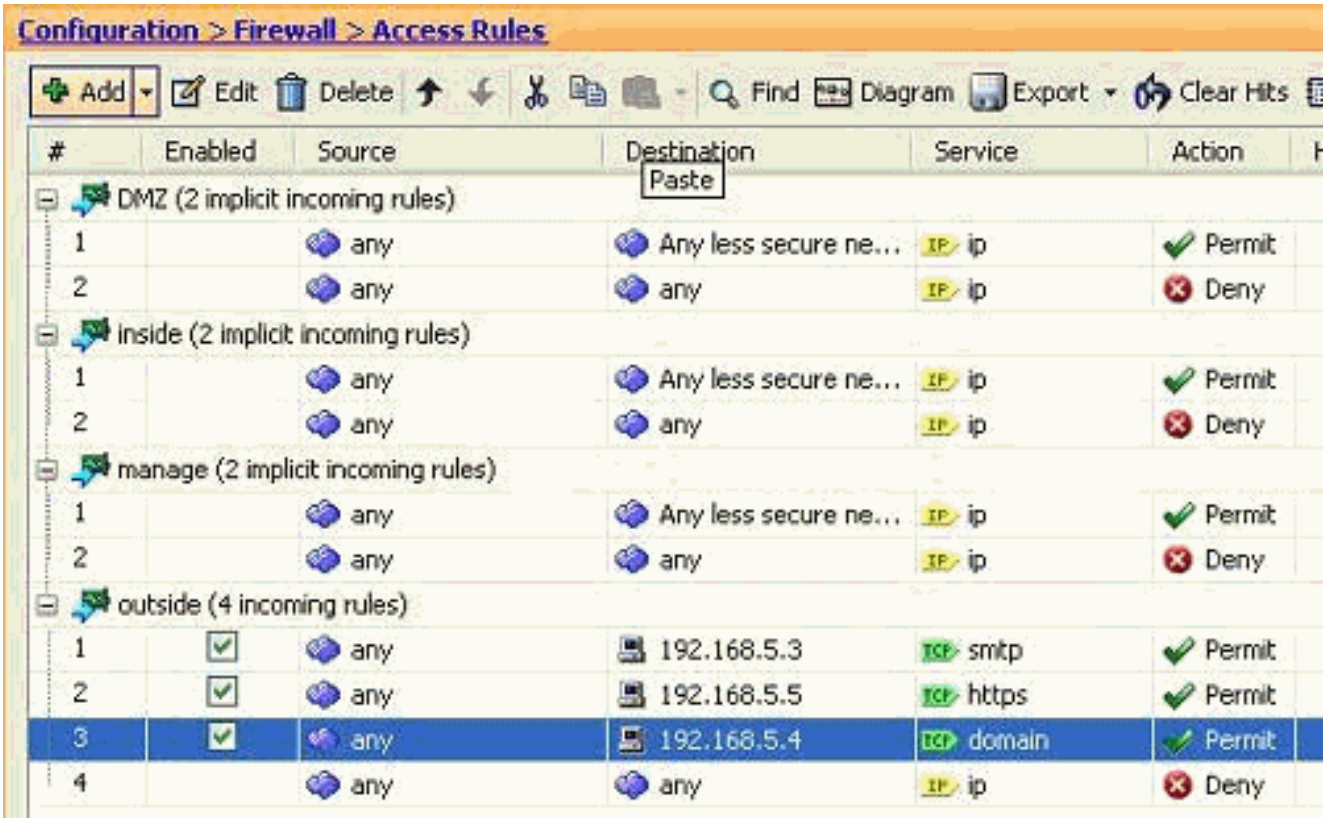
選擇Original Source和Translated IP address及其關聯的介面，然後按一下**OK**完成靜態NAT規則的配置。



此圖說明[範例](#)一節中列出的所有三個靜態規則：



此圖說明[範例](#)一節中列出的所有三個存取規則：



驗證

您可以使用某些**show**命令進行驗證，如下所示：

- **show xlate — 顯示**當前轉換資訊
- **show access-list** — 顯示訪問策略的命中計數器
- **show logging** — 顯示緩衝區中的日誌。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

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

- PIX/ASA 7.x:啟用/禁用介面之間的通訊
- 使用nat、global、static、conduit和access-list命令的PIX 7.0和自適應安全裝置埠重定向（轉發）
- 在PIX上使用nat、global、static、conduit和access-list命令和埠重定向（轉發）
- PIX/ASA 7.x:啟用FTP/TFTP服務配置示例
- PIX/ASA 7.x:啟用VoIP(SIP、MGCP、H323、SCCP)服務配置示例
- PIX/ASA 7.x:DMZ上的郵件伺服器訪問配置示例
- 技術支援與文件 - Cisco Systems