ASA 8.X及更高版本：通過ASDM GUI新增或修改訪問清單配置示例

目錄

簡介

本檔案將說明如何使用思科調適型資安裝置管理員(ASDM)來使用存取控制清單。這包括建立新訪問清單、如何編輯現有訪問清單以及使用訪問清單的其他功能。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 8.2.X版的Cisco自適應安全裝置(ASA)
- Cisco Adaptive Security Device Manager(ASDM)6.3.X版

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。

背景資訊

存取清單主要用於控制透過防火牆的流量。您可以使用存取清單允許或拒絕特定型別的流量。每個訪問清單包含許多控制從特定源到特定目標的流量的訪問清單條目(ACE)。通常，此訪問清單繫結到一個介面，以通知它應查詢到的流的方向。訪問清單主要分為兩大類。

1. 入站訪問清單
2. 出站訪問清單

入站訪問清單應用於進入該介面的流量，出站訪問清單應用於退出該介面的流量。入站/出站標籤表示流量在該介面的方向，但不表示流量在更高和更低安全介面之間的移動。

對於TCP和UDP連線，您不需要允許返回流量的訪問清單，因為安全裝置允許所有已建立的雙向連線的返回流量。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將訪問清單應用於源介面和目的介面，以便在兩個方向上允許ICMP，或者您需要啟用ICMP檢測引擎。ICMP檢測引擎將ICMP會話視為雙向連線。

從ASDM版本6.3.X中，可以配置兩種型別的訪問清單。

1. 介面訪問規則
2. 全域性訪問規則

注意：訪問規則是指單個訪問清單條目(ACE)。

介面訪問規則在建立時繫結到任何介面。如果不將它們繫結到介面，則無法建立它們。這與命令列示例不同。使用CLI，首先使用**access list**命令建立存取清單，然後使用**access-group**命令將此存取清單繫結到介面。在ASDM 6.3及更高版本中，訪問清單作為單個任務建立並繫結到介面。這僅適用於通過該特定介面的流量。

全域性訪問規則未繫結到任何介面。它們可以通過ASDM中的ACL Manager頁籤進行配置，並應用於全域性入口流量。當根據來源、目的地和通訊協定型別找到相符專案時，就會執行上述專案。這些規則不會在每個介面上複製，因此可以節省記憶體空間。

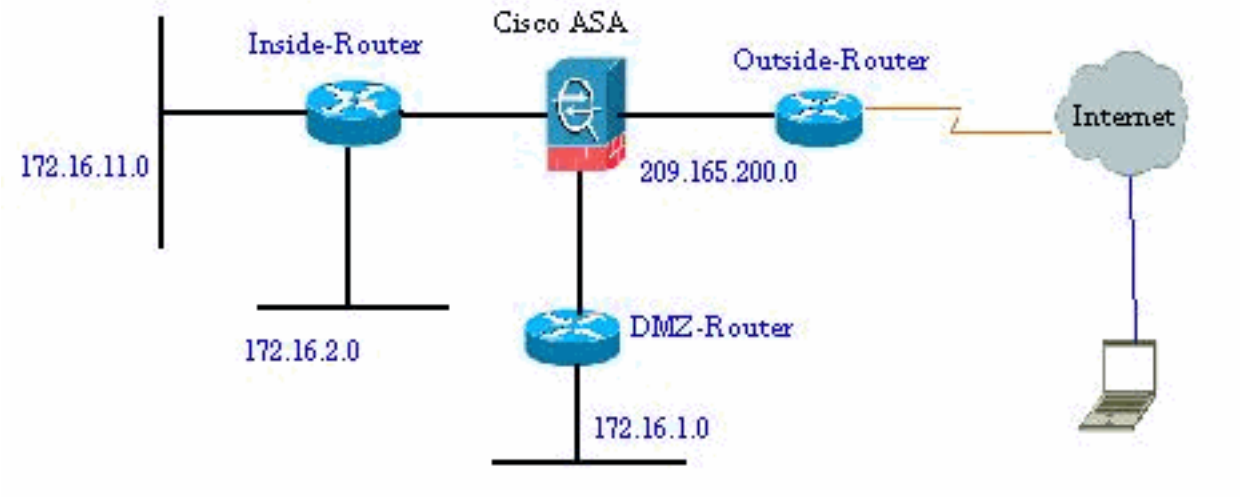
當要實施這兩個規則時，介面訪問規則通常優先於全域性訪問規則。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

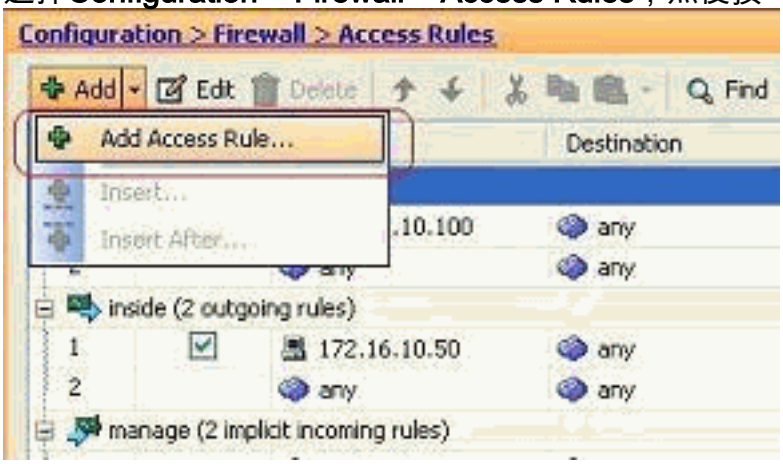
本檔案會使用以下網路設定：



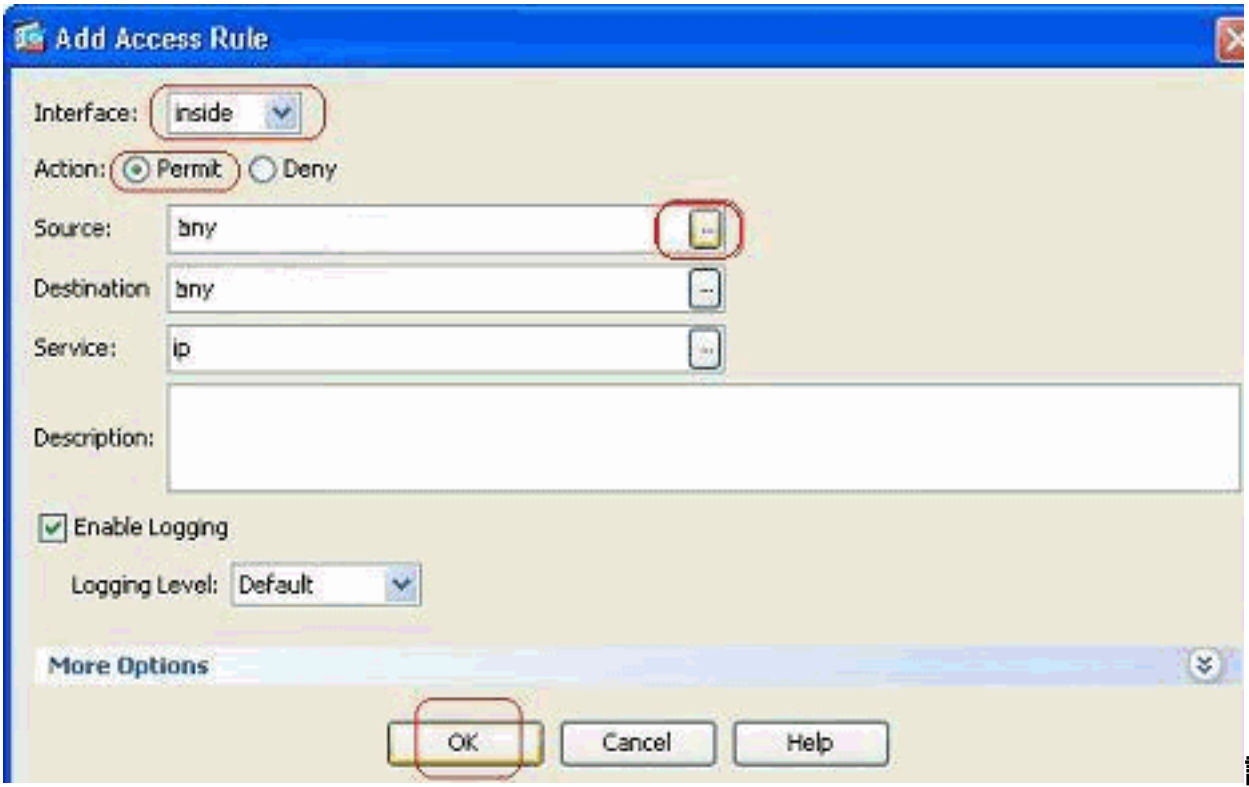
新增新訪問清單

完成以下步驟，以便使用ASDM建立新的訪問清單：

1. 選擇**Configuration > Firewall > Access Rules**，然後按一下**Add Access Rule**按鈕。

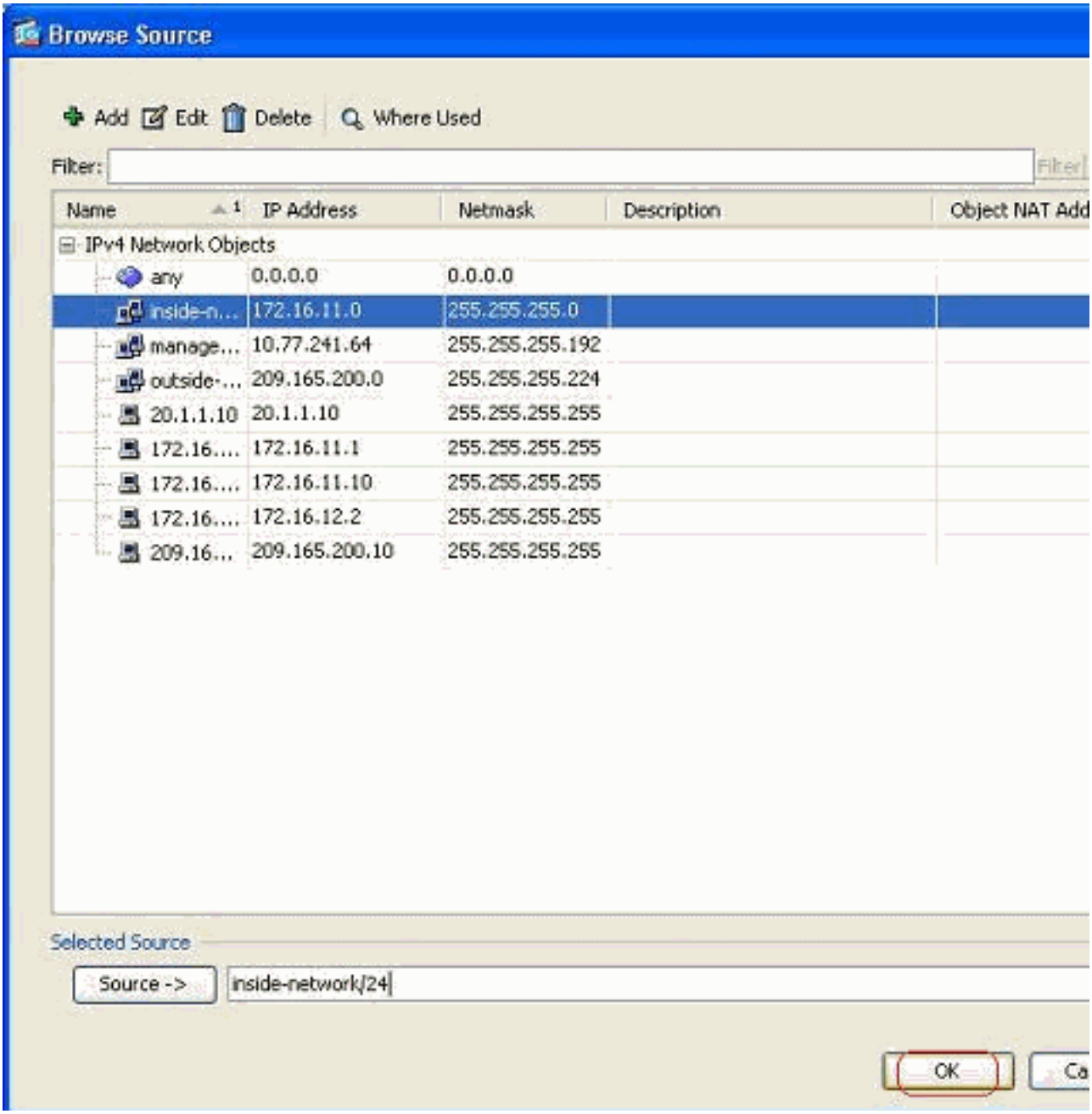


2. 選擇必須繫結此訪問清單的介面，以及要對流量執行的操作，例如permit/deny。然後按一下**Details**按鈕以選擇源網路。

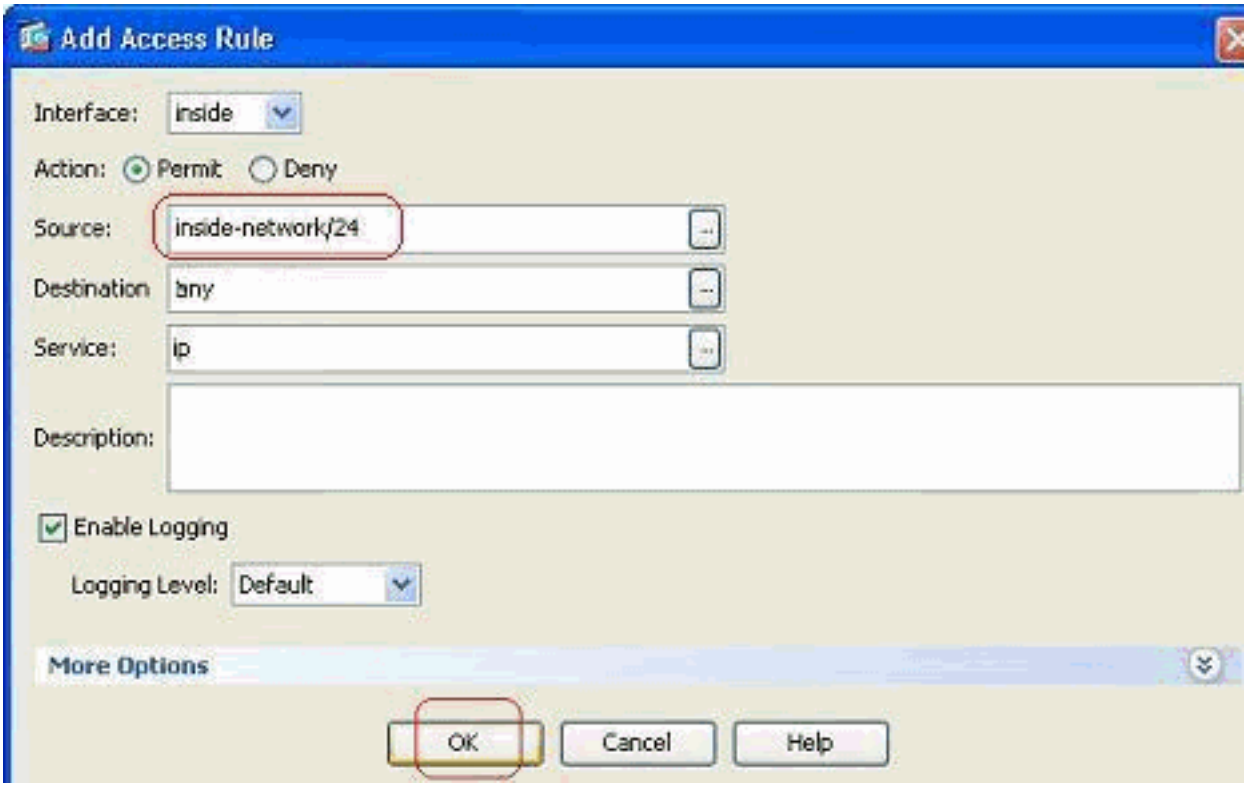


註：以下簡要說明了此視窗中顯示的不同欄位：**Interface** — 確定此訪問清單繫結到的介面。**Action** — 確定新規則的操作型別。有兩種可用選項。**Permit** allow all matching traffic和**Deny** blocks all matching traffic。**Source** — 此欄位指定流量的源。這可以是單個IP地址、網路、防火牆的介面IP地址或網路對象組中的任何一個。可以使用**Details**按鈕選擇這些選項。**Destination** — 此欄位指定流量的源。這可以是單個IP地址、網路、防火牆的介面IP地址或網路對象組中的任何一個。可以使用**Details**按鈕選擇這些選項。**Service** — 此欄位確定應用此訪問清單的流量的協定或服務。您還可以定義包含一組不同協定的服務組。

3. 按一下**Details**按鈕後，將顯示一個包含現有網路對象的新視窗。選擇**inside-network**，然後按一下**OK**。



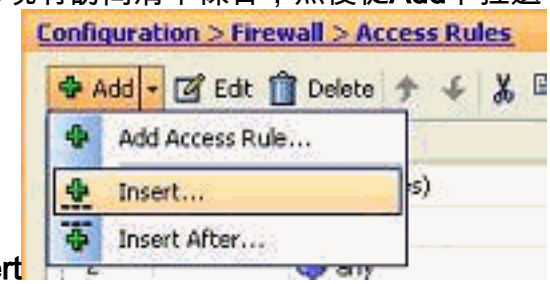
4. 您將返回到**Add Access Rule**窗口。在Destination欄位中鍵入**any**。並按一下**OK**以完成訪問規則的配置。



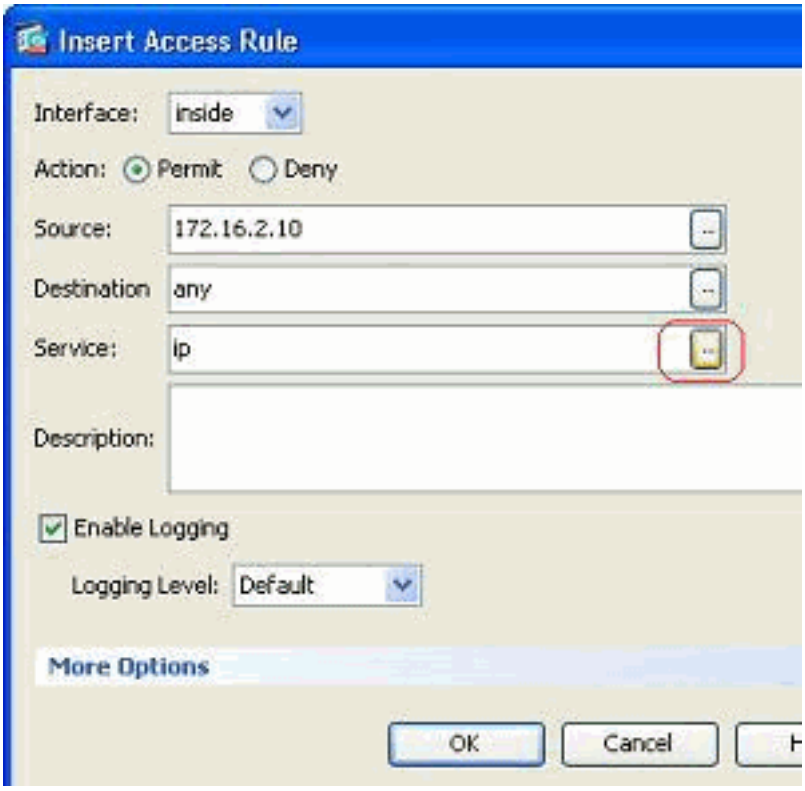
在現有訪問規則之前新增訪問規則：

完成以下步驟，以便在現有訪問規則之前新增訪問規則：

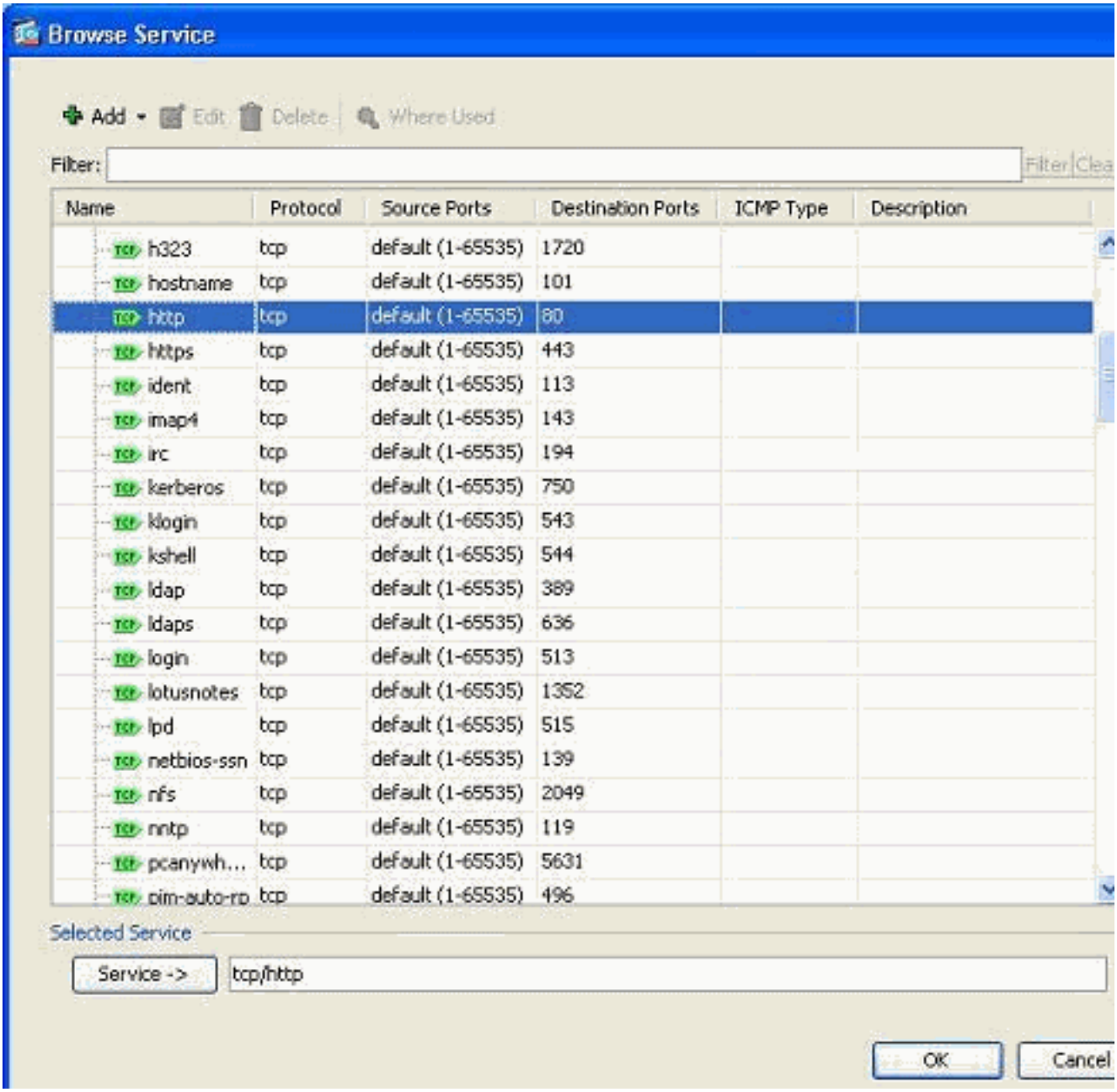
1. 選擇現有訪問清單條目，然後從**Add**下拉選單中按一下 **Insert**



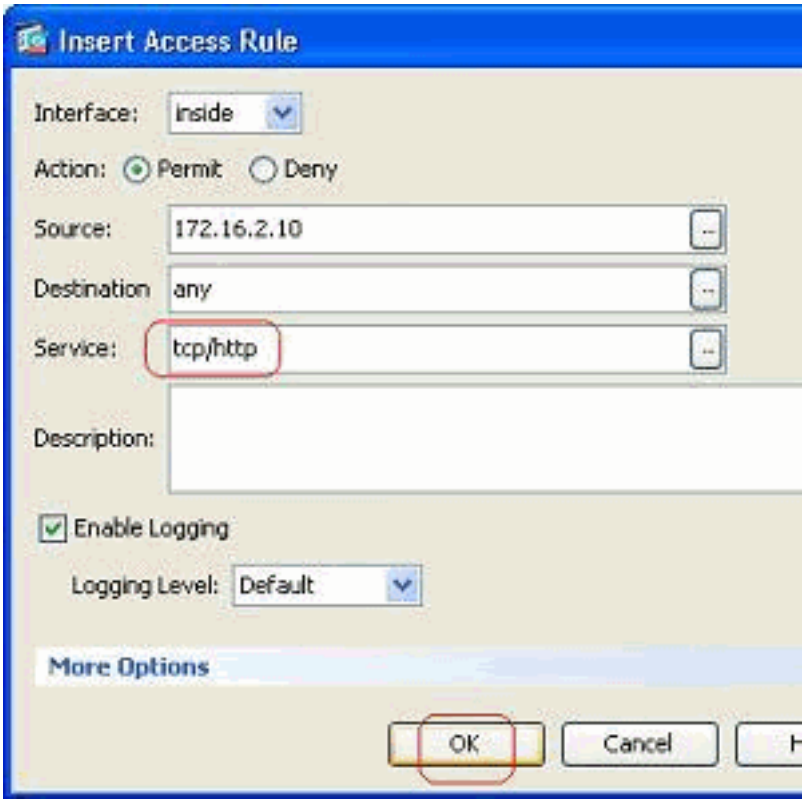
2. 選擇Source和Destination，然後按一下Service欄位的**Details**按鈕以選擇Protocol。



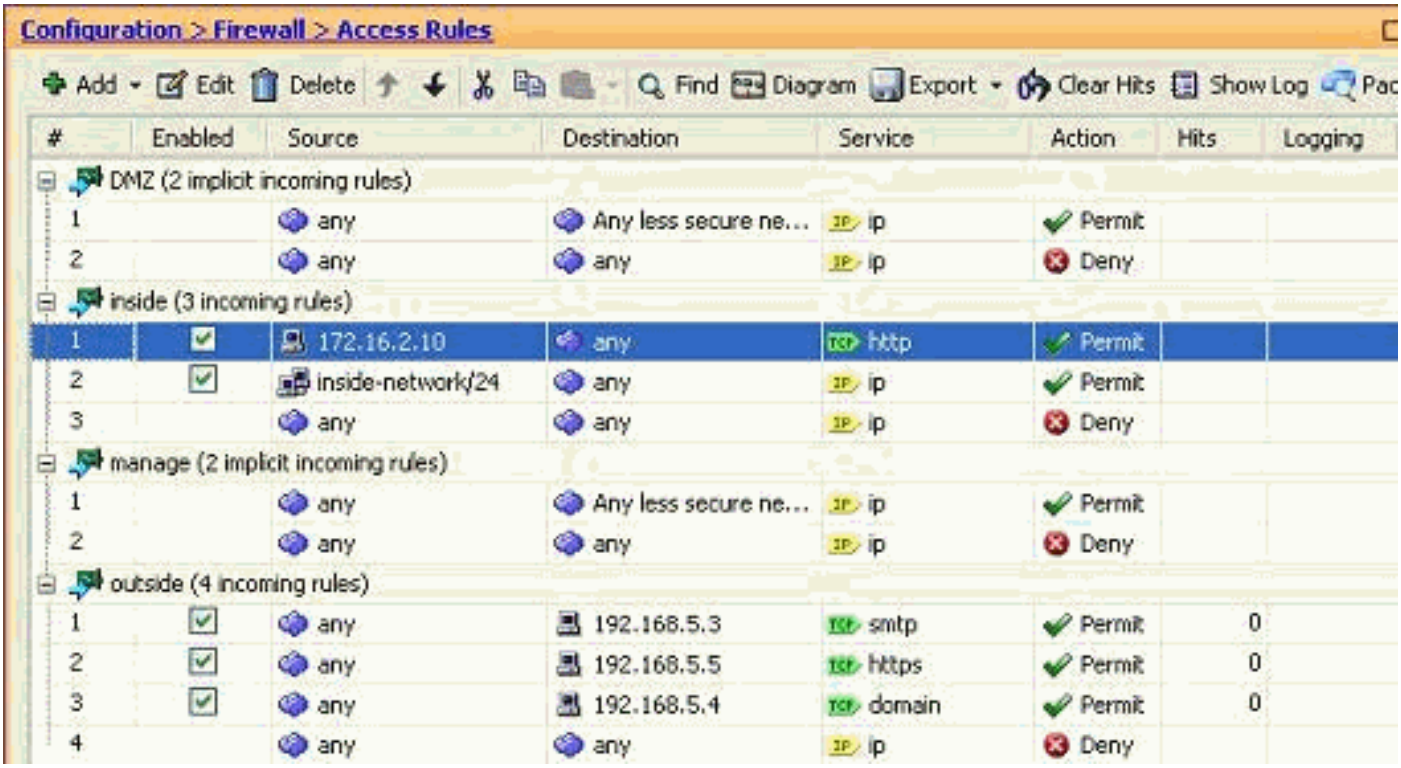
3. 選擇HTTP協定，然後按一下**OK**。



4. 您將返回到「插入訪問規則」視窗。「服務」(Service)欄位填充了**tcp/http**作為所選協定。按一下「**OK**」以完成新存取清單專案的組態。



現在，您可以觀察在Inside-Network的現有條目之前顯示的新訪問規則。



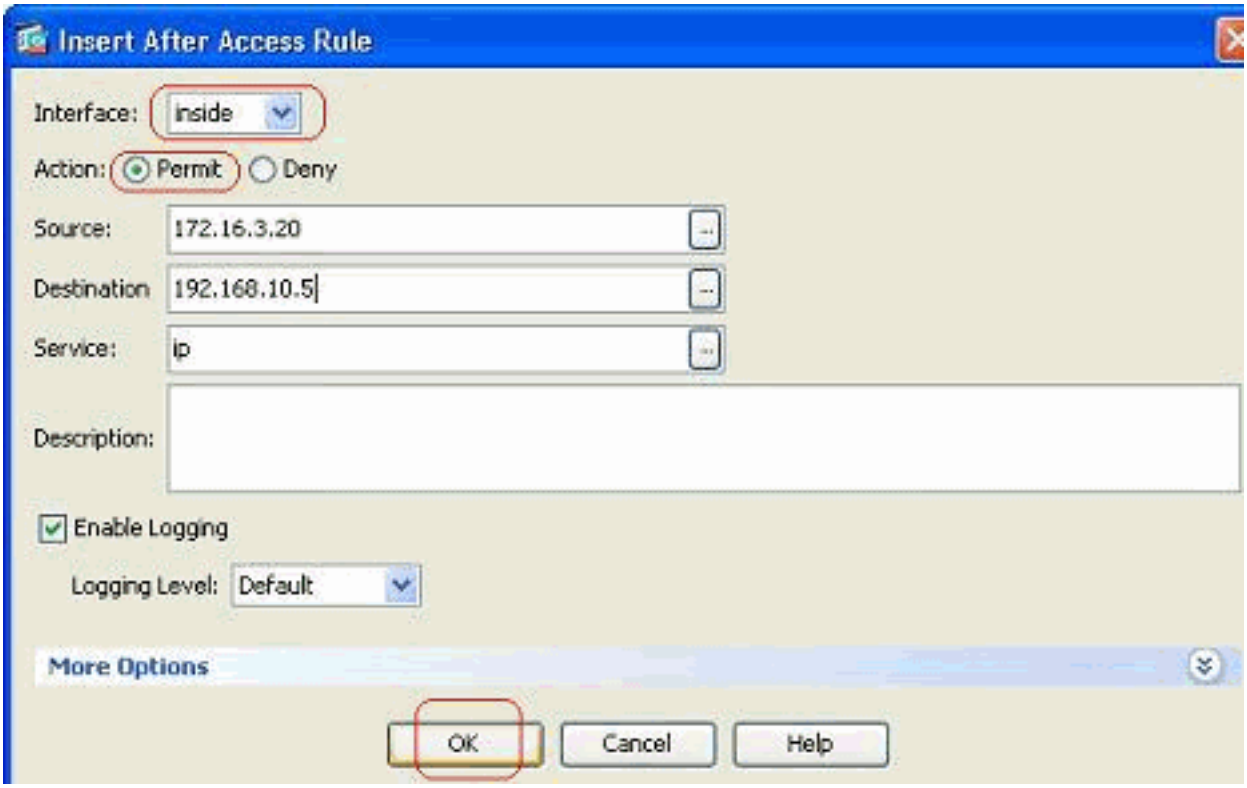
注意：訪問規則的順序非常重要。在處理要過濾的每個資料包時，ASA會檢查資料包是否按順序與任何訪問規則標準匹配，如果發生匹配，則會實施該訪問規則的操作。匹配訪問規則時，它不會繼續訪問規則並再次驗證它們。

在現有訪問規則後新增訪問規則：

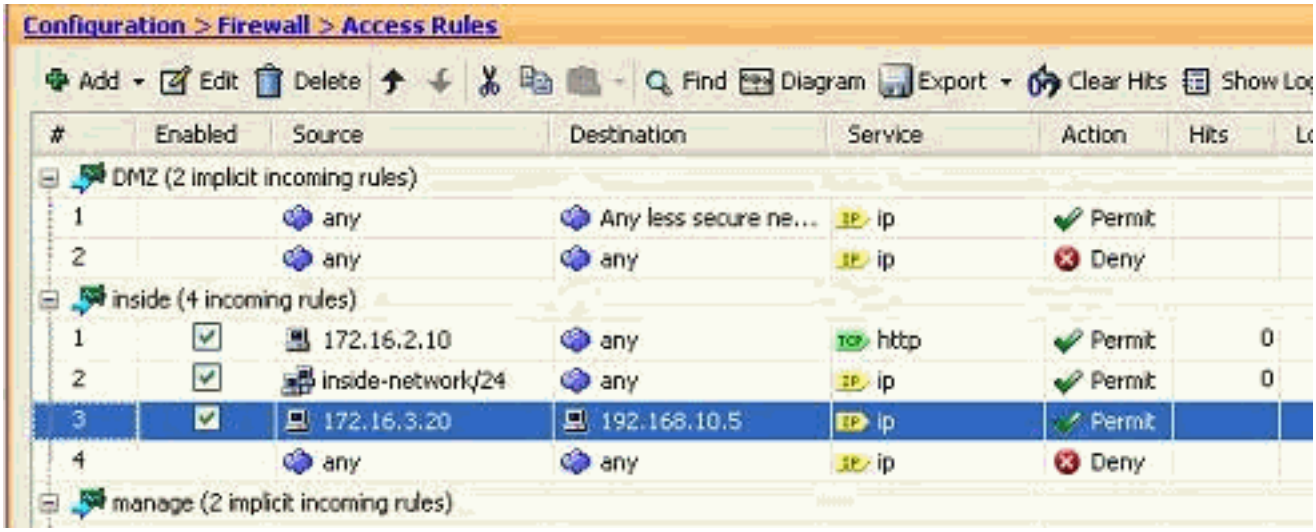
完成這些步驟，以便在現有訪問規則之後立即建立訪問規則。

1. 選擇需要在其後具有新訪問規則的訪問規則，然後從Add下拉選單中選擇**Insert After**。

2. 指定Interface、Action、Source、Destination和Service欄位，然後按一下**OK**完成此訪問規則的配置。



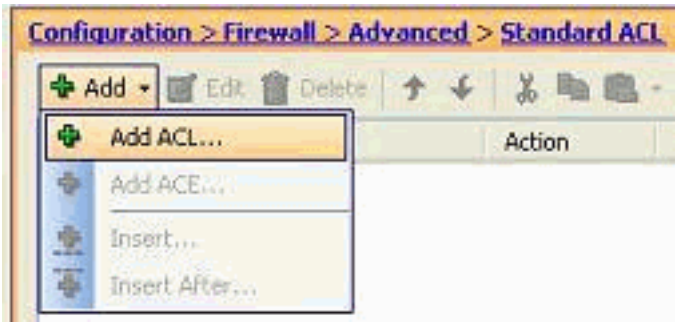
您可以看到新配置的訪問規則緊跟已配置的訪問規則。



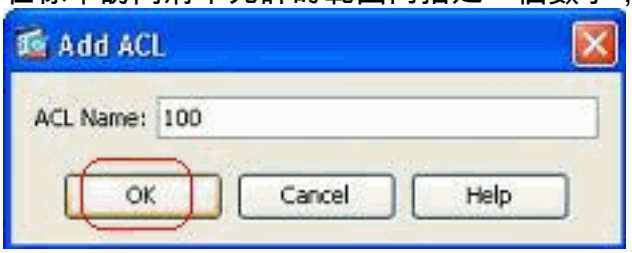
建立標準存取清單

完成這些步驟，以便使用ASDM GUI建立標準訪問清單。

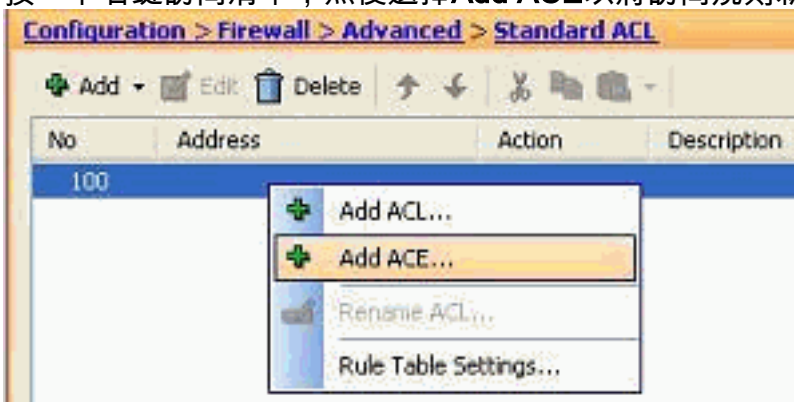
1. 選擇**Configuration > Firewall > Advanced > Standard ACL > Add**，然後點選**Add ACL**。



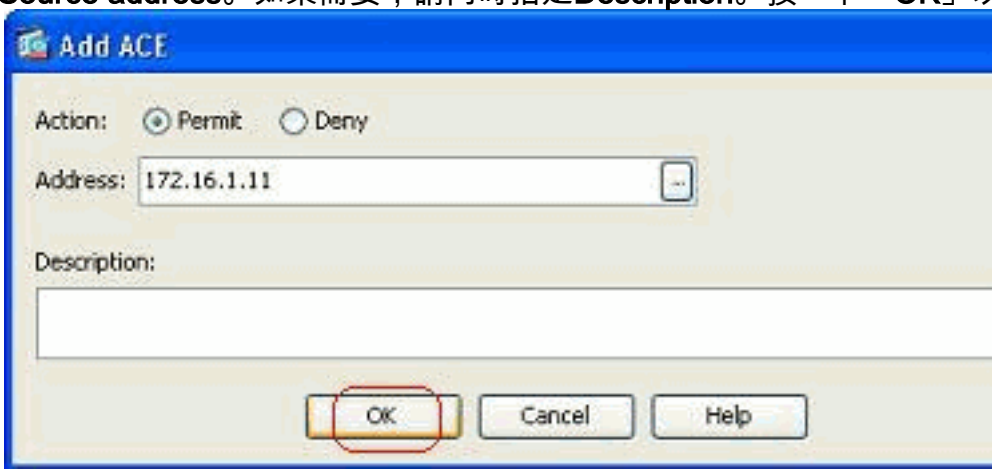
2. 在標準訪問清單允許的範圍內指定一個數字，然後按一下OK。



3. 按一下右鍵訪問清單，然後選擇Add ACE以將訪問規則新增到此訪問清單。



4. 選擇Action，並指定Source address。如果需要，請同時指定Description。按一下「OK」以完成存取規則的組態。

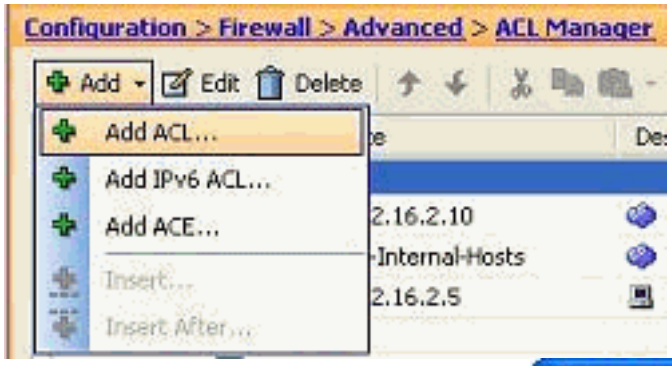


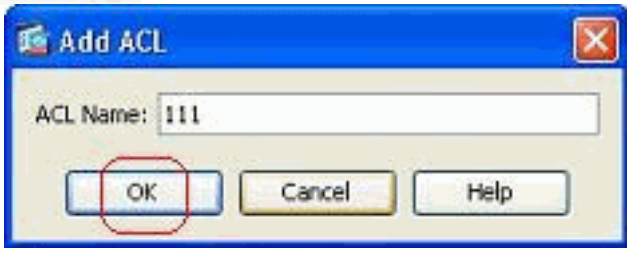
建立全域性訪問規則

完成這些步驟，建立包含全域性訪問規則的擴展訪問清單。

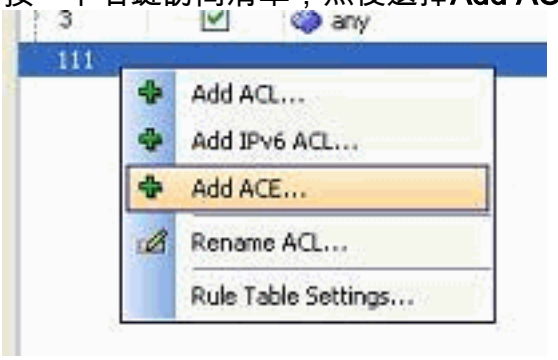
1. 選擇Configuration > Firewall > Advanced > ACL Manager > Add，然後按一下Add ACL按鈕

。

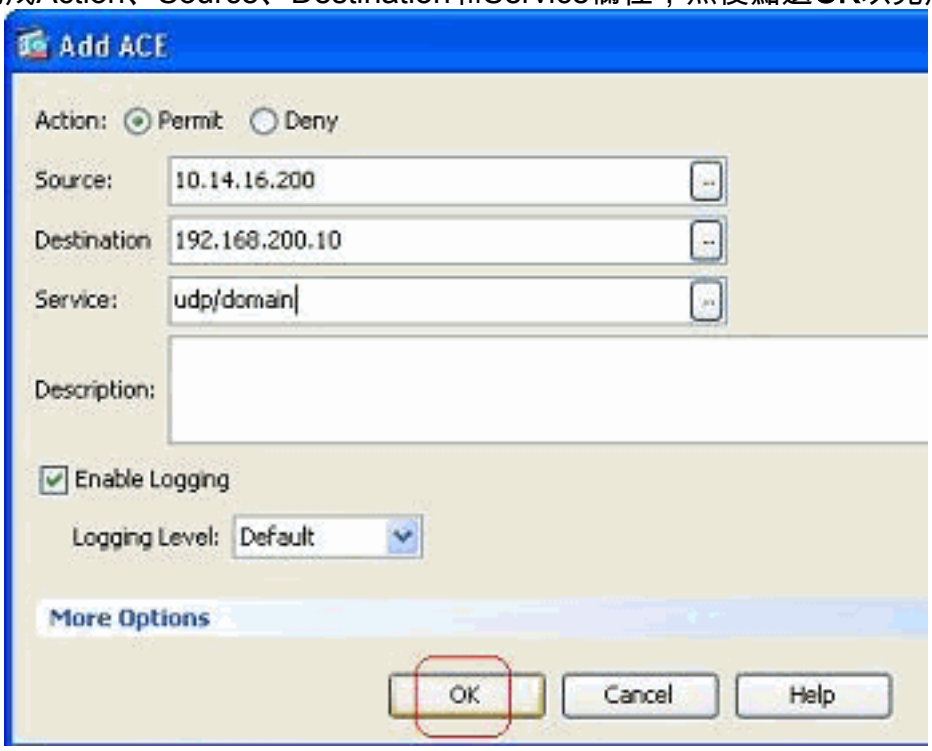




2. 指定訪問清單的名稱，然後按一下**OK**。
3. 按一下右鍵訪問清單，然後選擇**Add ACE**以將訪問規則新增到此訪問清單。



4. 完成Action、Source、Destination和Service欄位，然後點選**OK**以完成全域性訪問規則的配置



。

現在可以檢視全域性訪問規則，如圖所示。

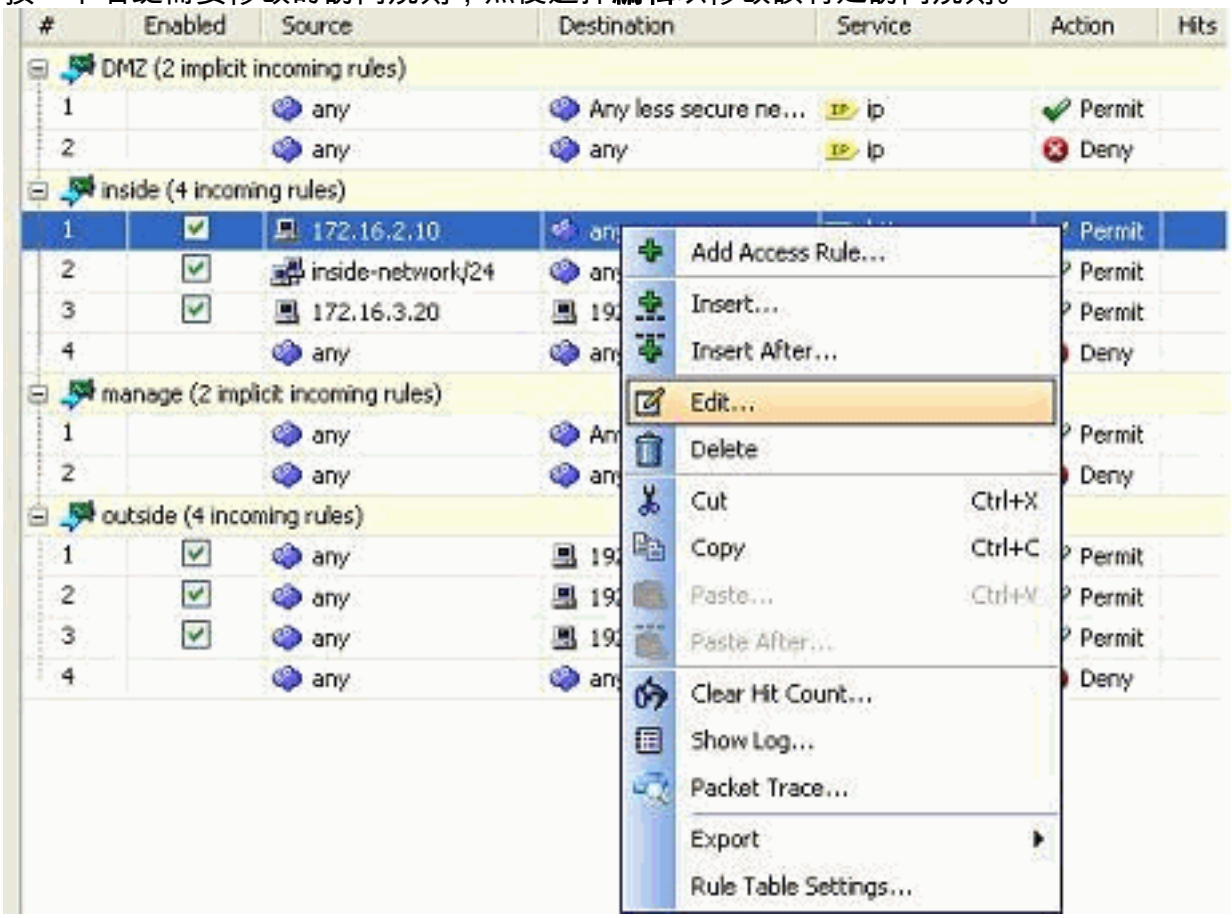
編輯現有訪問清單

本節討論如何編輯現有訪問。

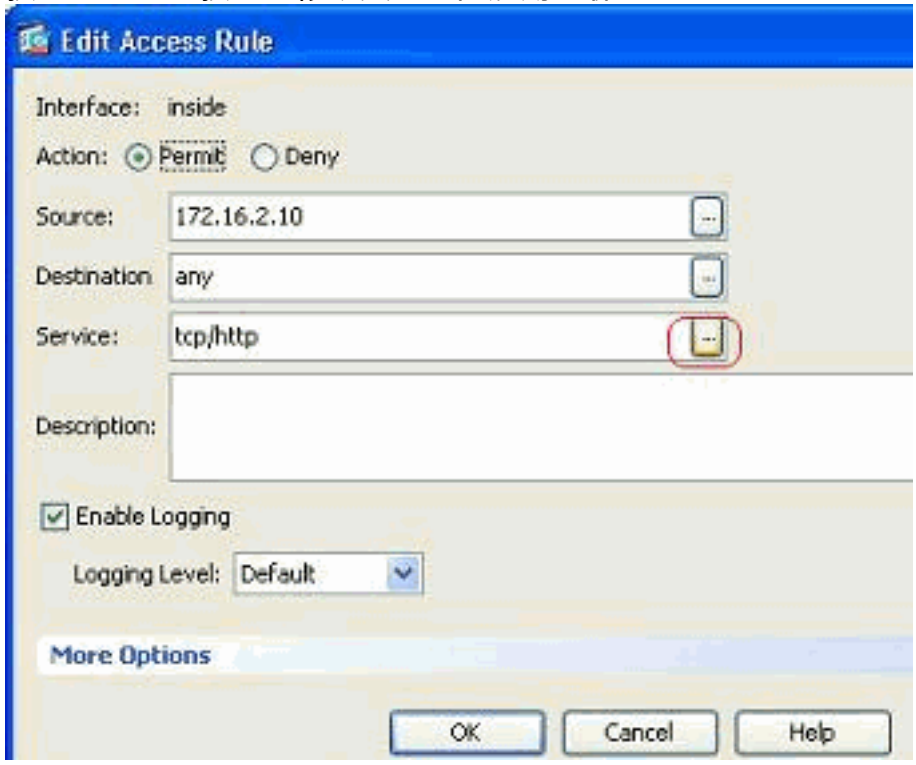
編輯Protocol欄位以建立服務組：

完成以下步驟以建立新的服務組。

1. 按一下右鍵需要修改的訪問規則，然後選擇**編輯**以修改該特定訪問規則。

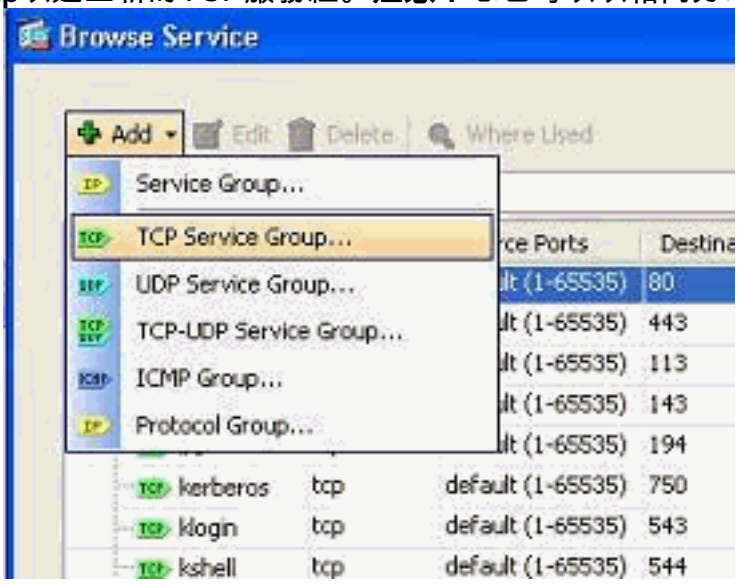


2. 按一下**Details**按鈕以修改與此訪問規則關聯的協定。

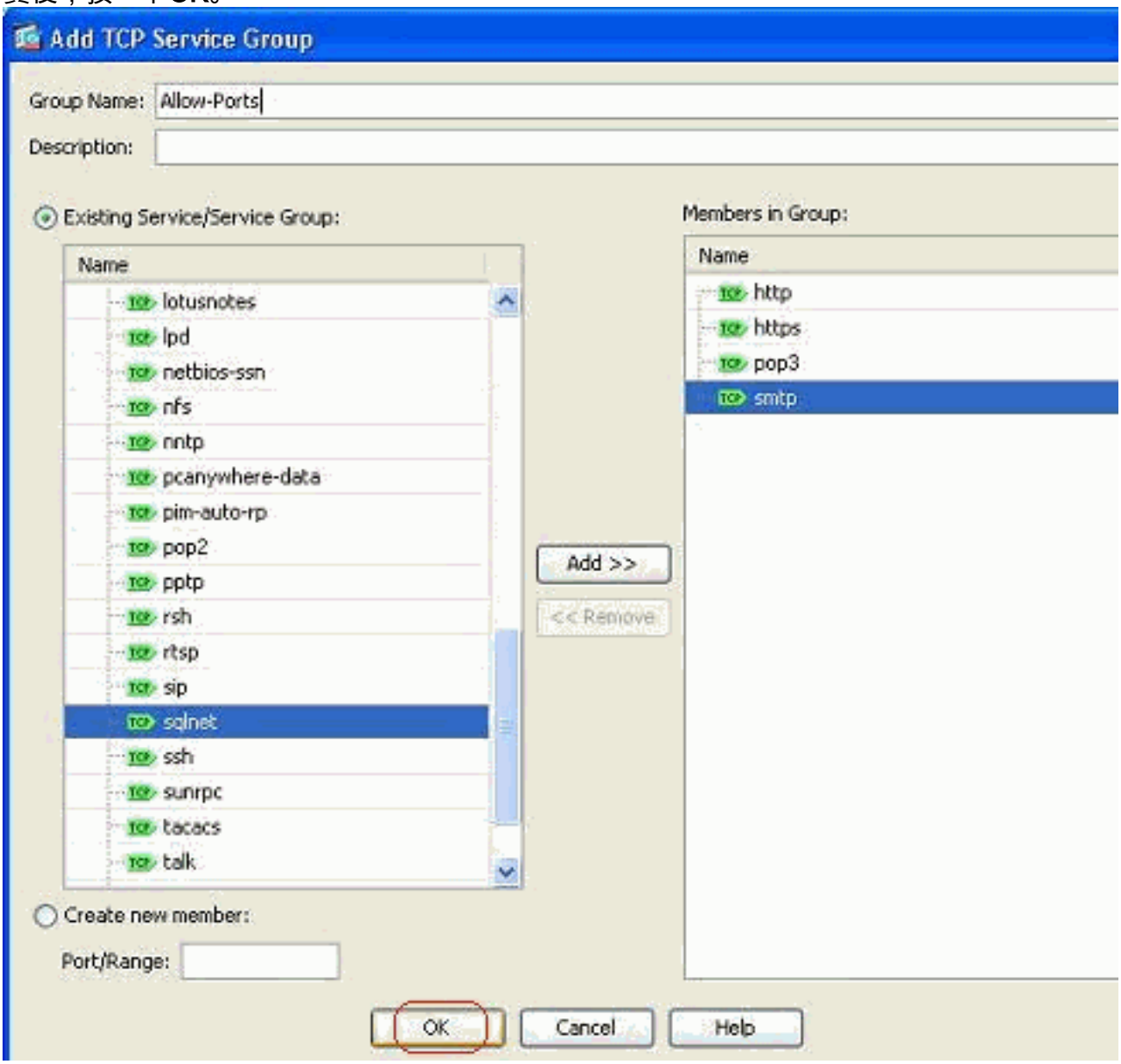


3. 如果需要，可以選擇除HTTP以外的任何協定。如果只選擇一個協定，則無需建立服務組。當

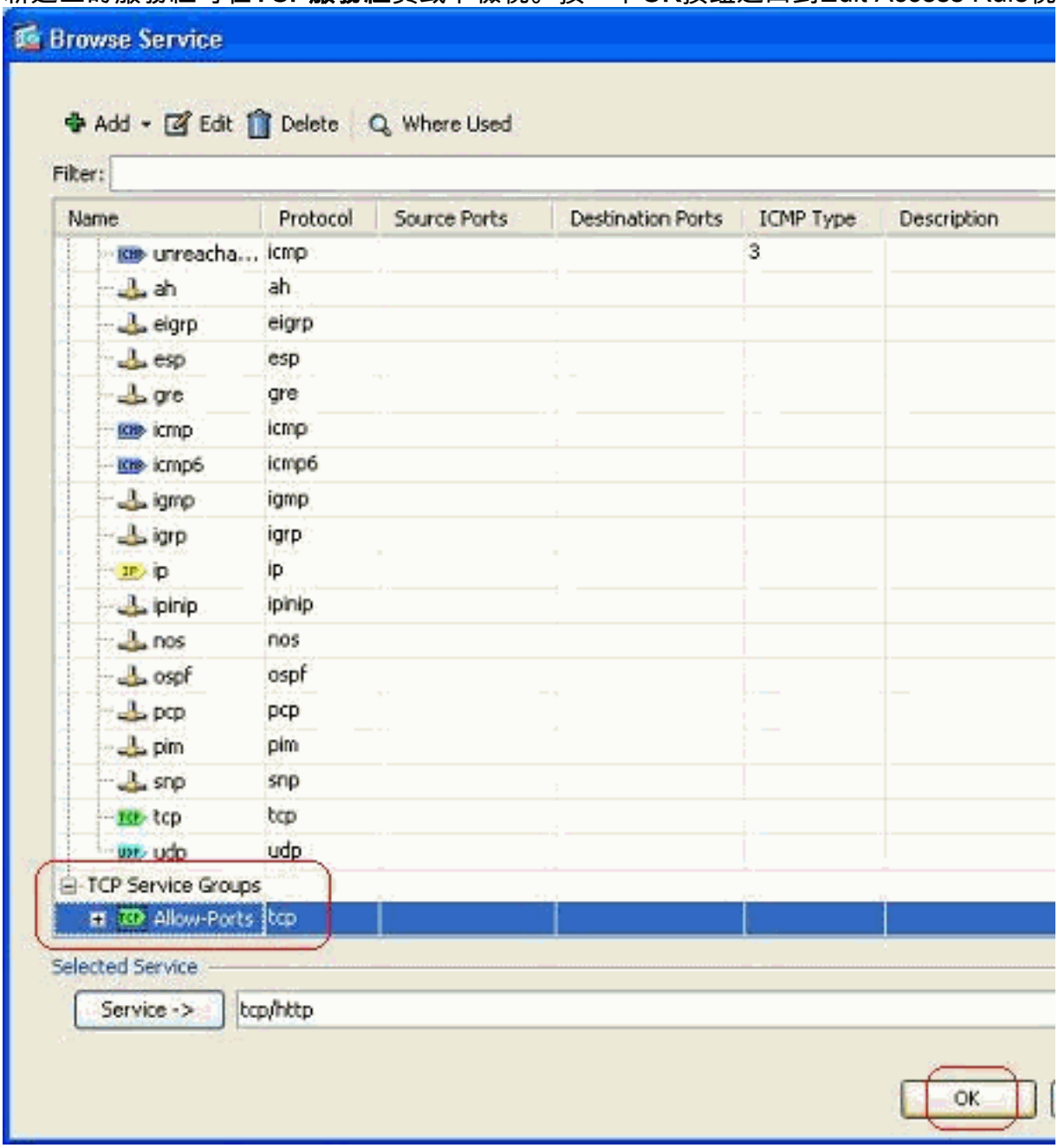
需要標識要與此訪問規則匹配的多個非相鄰協定時，建立服務組非常有用。選擇**Add > TCP service group**以建立新的TCP服務組。**注意**：您也可以以相同方式建立新的UDP服務組或ICMP組等。



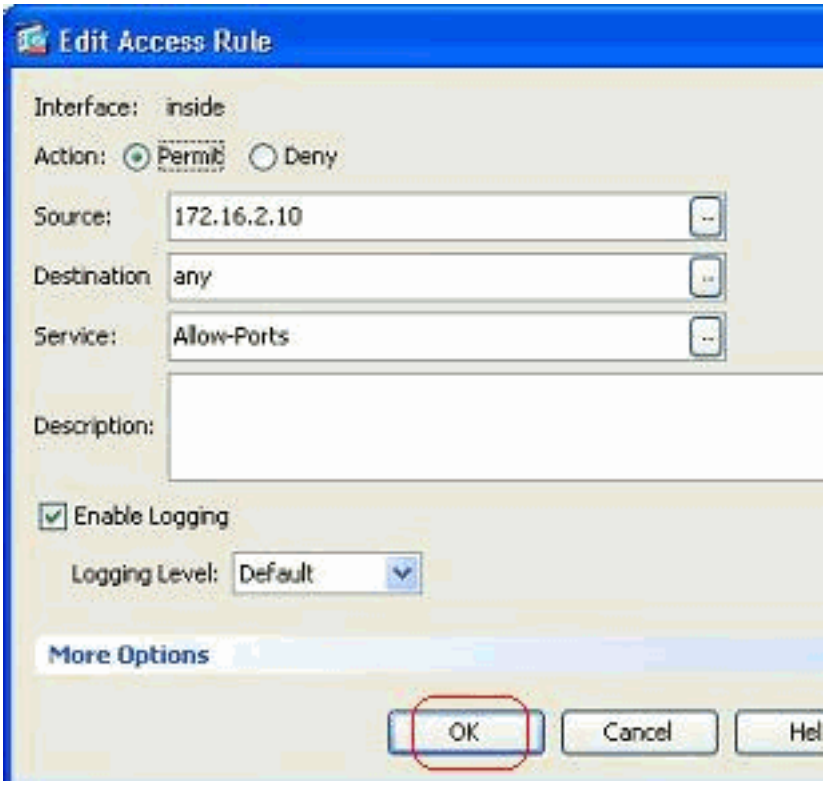
4. 指定此服務組的名稱，在左側選單中選擇協定，然後按一下**Add**以將其移動到右側的Members in Group選單中。可以根據要求新增多個協定作為服務組的成員。協定逐一新增。新增所有成員後，按一下**OK**。



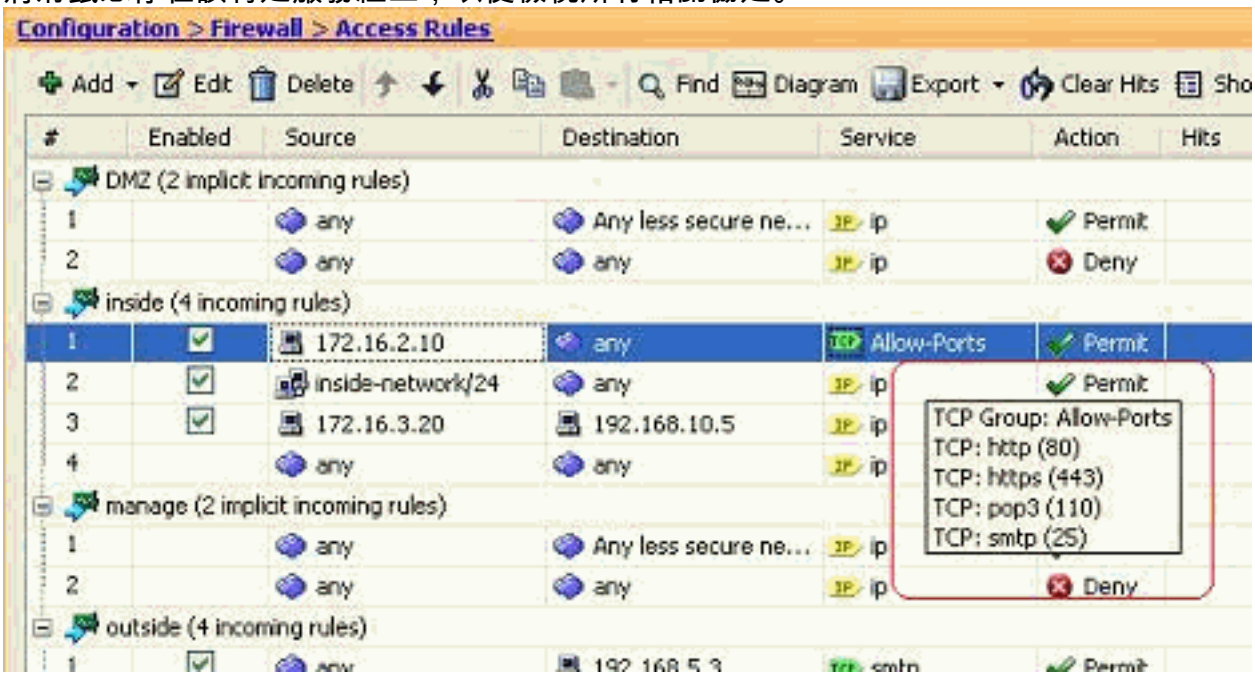
5. 新建立的服務組可在**TCP服務組**頁籤下檢視。按一下**OK**按鈕返回到Edit Access Rule視窗。



6. 您可以看到「服務」欄位填充有新建立的服務組。按一下「**OK**」以完成編輯。



7. 將滑鼠懸停在該特定服務組上，以便檢視所有相關協定。

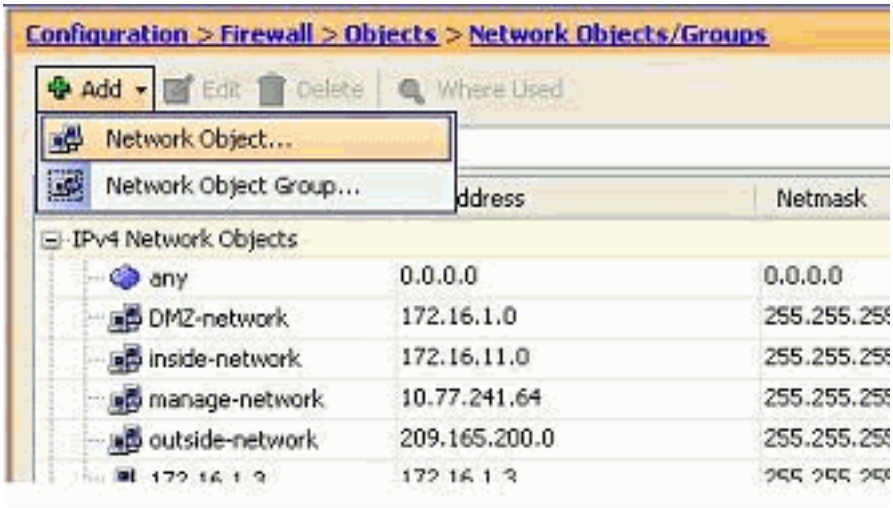


編輯Source/Destination欄位以建立Network對象組：

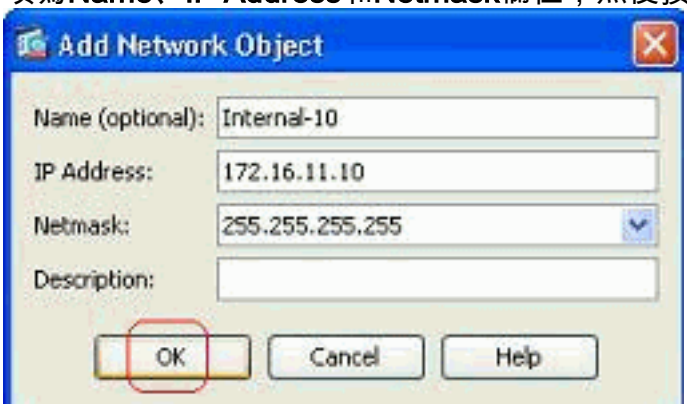
對象組用於簡化訪問清單的建立和維護。將類似的對象組合在一起時，可以在單個ACE中使用對象組，而不必分別為每個對象輸入ACE。建立對象組之前，需要建立對象。在ASDM術語中，對象稱為網路對象，對象組稱為網路對象組。

請完成以下步驟：

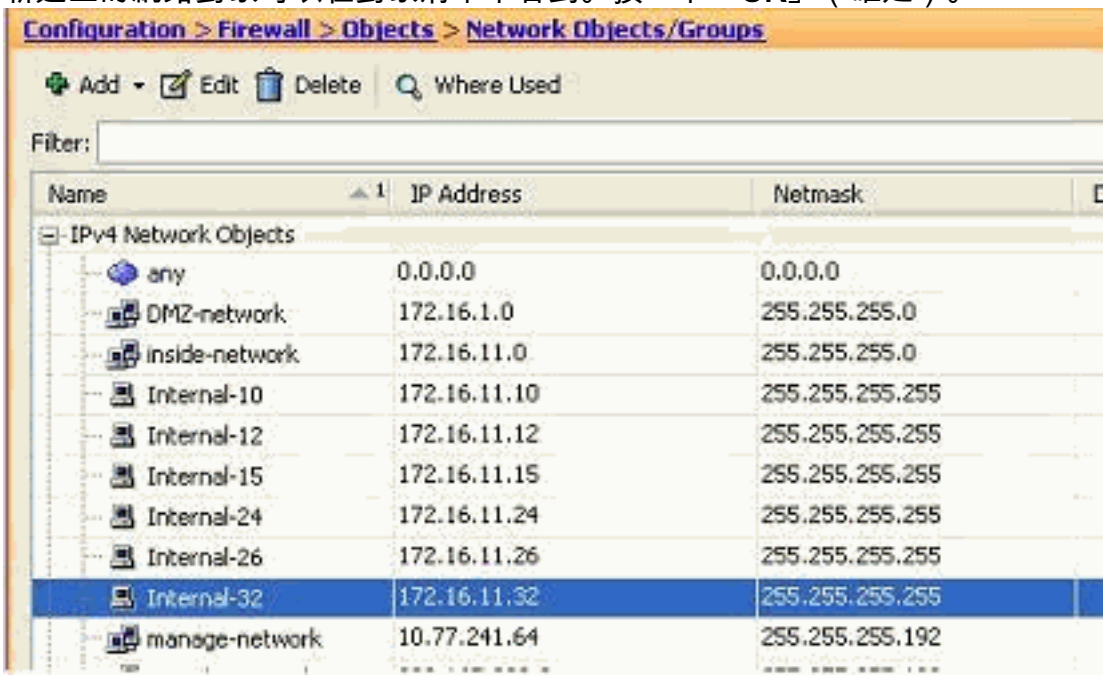
1. 選擇**Configuration > Firewall > Objects > Network Objects/Groups > Add**，然後按一下**Network Object**以建立新的網路對象。



2. 填寫Name、IP Address和Netmask欄位，然後按一下OK。

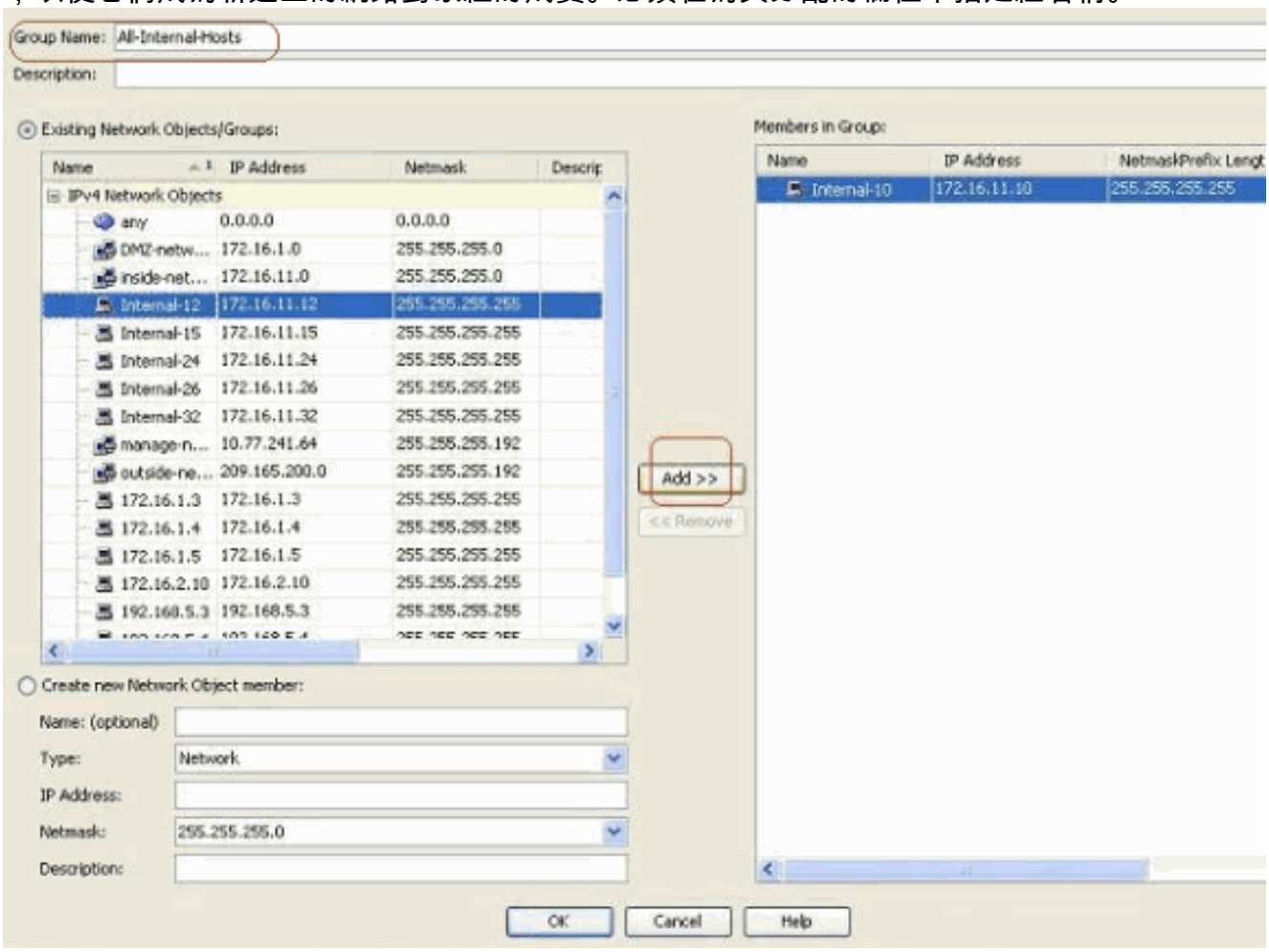


3. 新建立的網路對象可以在對象清單中看到。按一下「OK」（確定）。

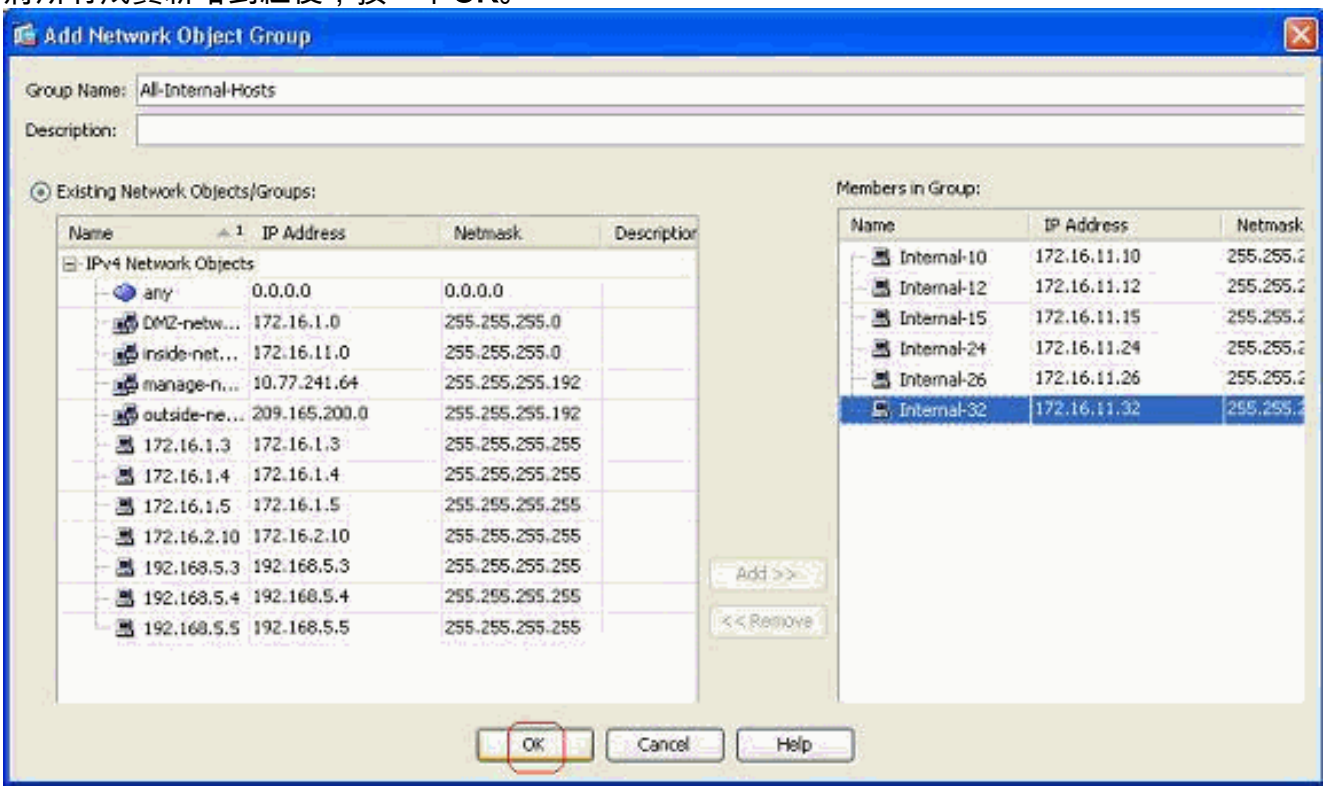


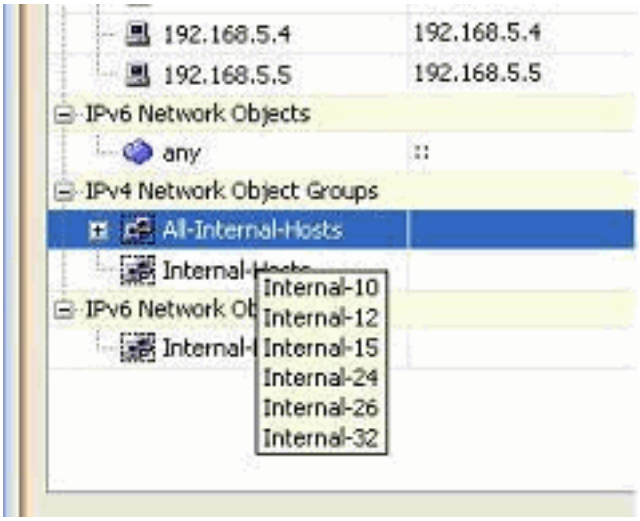
4. 選擇Configuration > Firewall > Objects > Network Objects/Groups > Add，然後按一下Network Object Group以建立新的網路對象組。

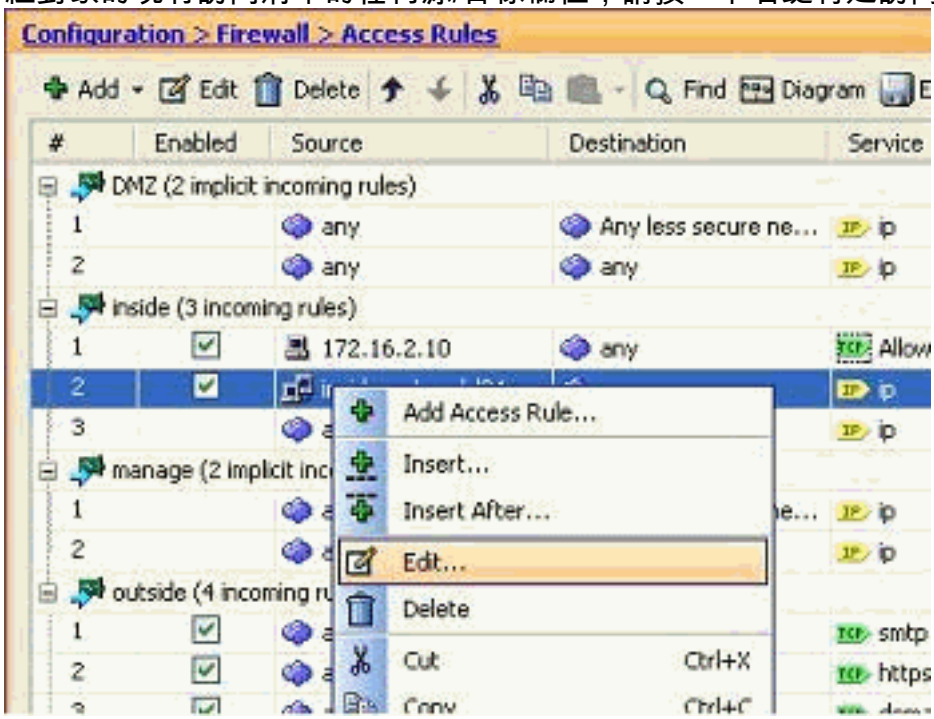
5. 所有網路對象的可用清單可在視窗的左窗格中找到。選擇單個網路對象，然後按一下**Add**按鈕，以使它們成為新建立的網路對象組的成員。必須在為其分配的欄位中指定組名稱。



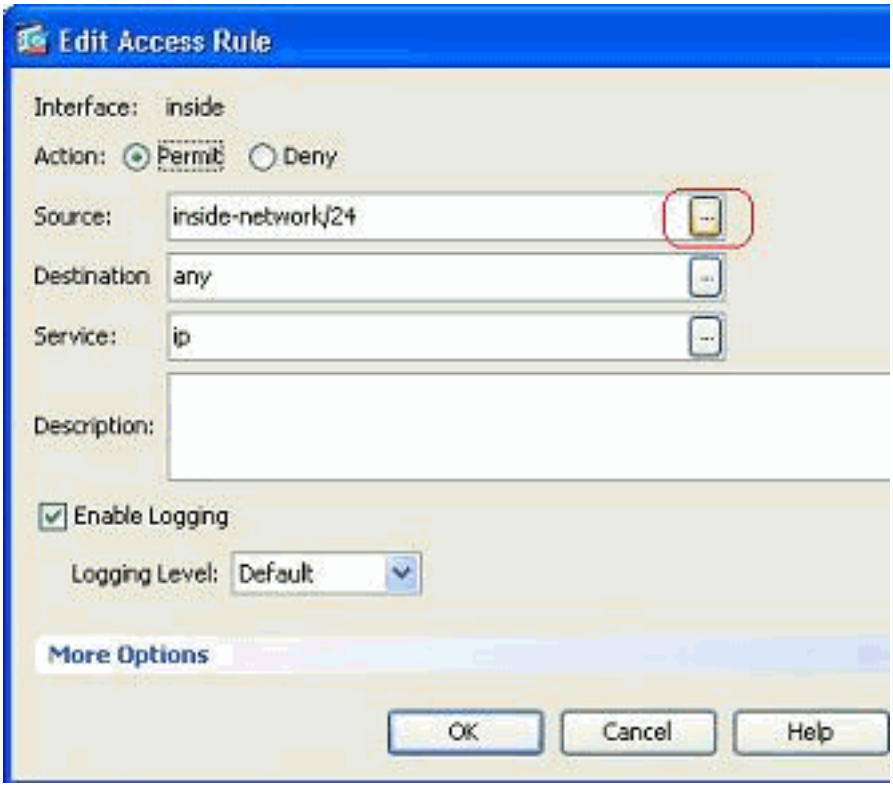
6. 將所有成員新增到組後，按一下**OK**。



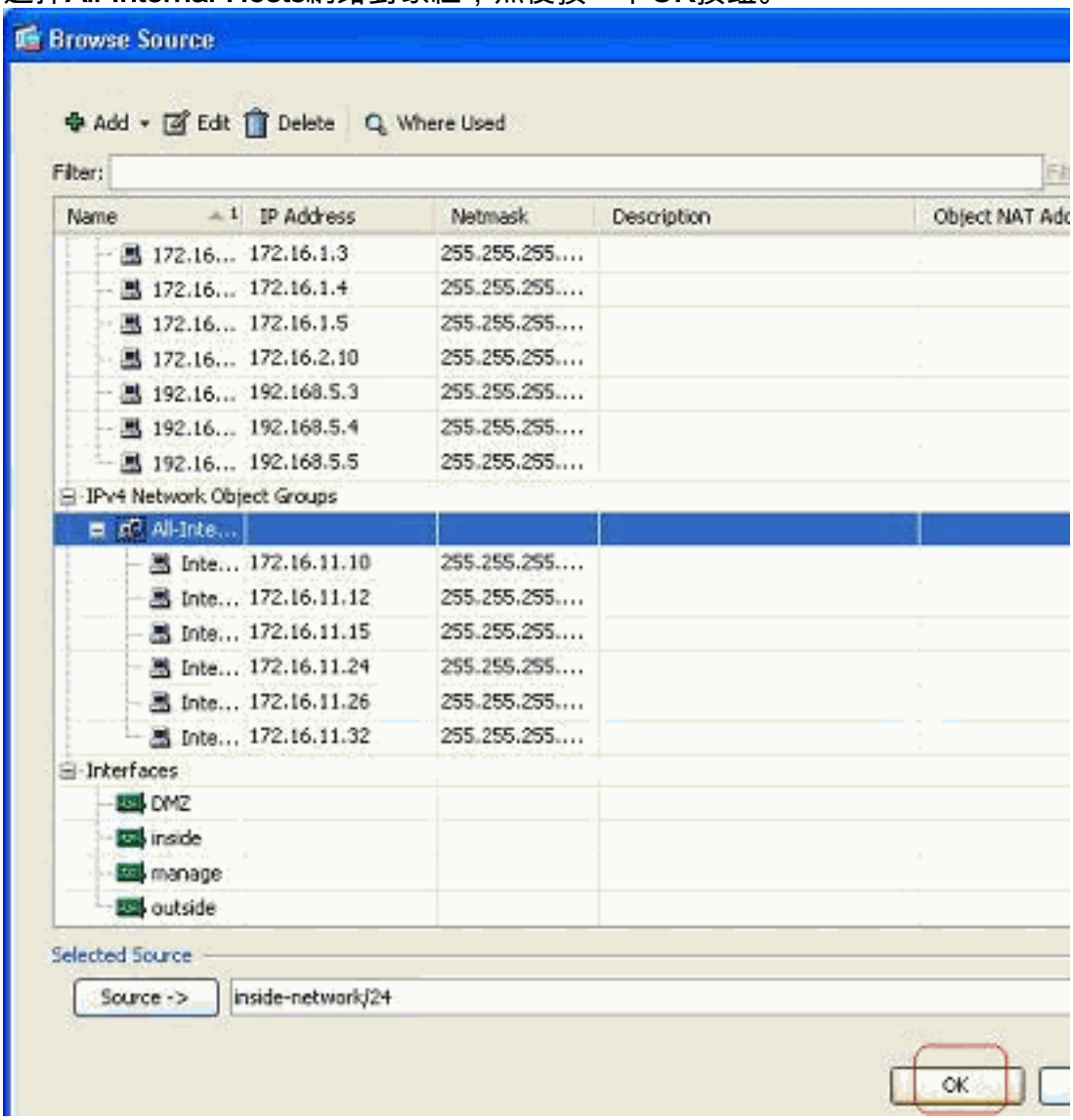
現在可以檢視網路對象組。 

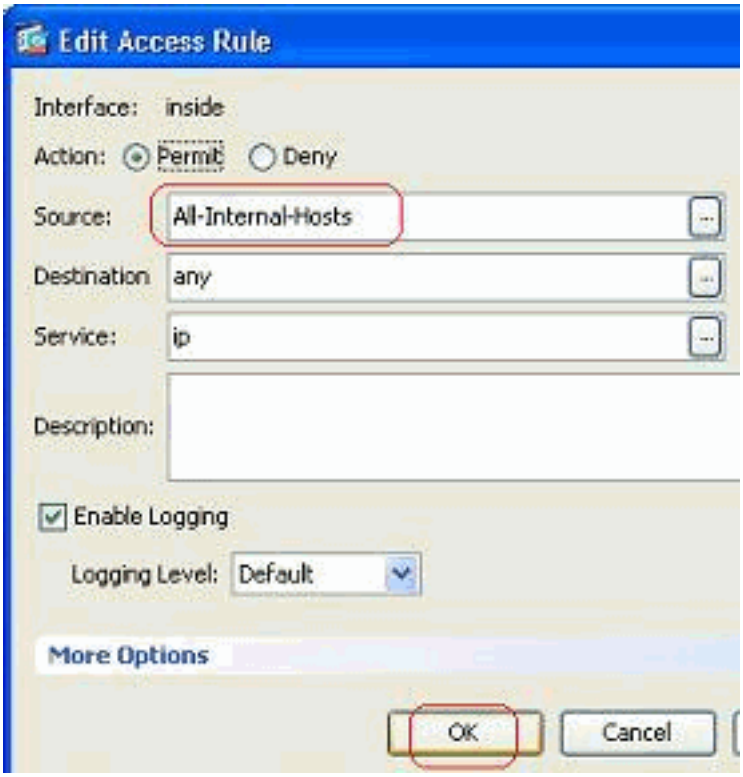
7. 若要修改具有網路組對象的現有訪問清單的任何源/目標欄位，請按一下右鍵特定訪問規則，然後選擇**編輯**。 

8. 系統將顯示Edit Access Rule視窗。按一下Source欄位的**Details**按鈕進行修改。

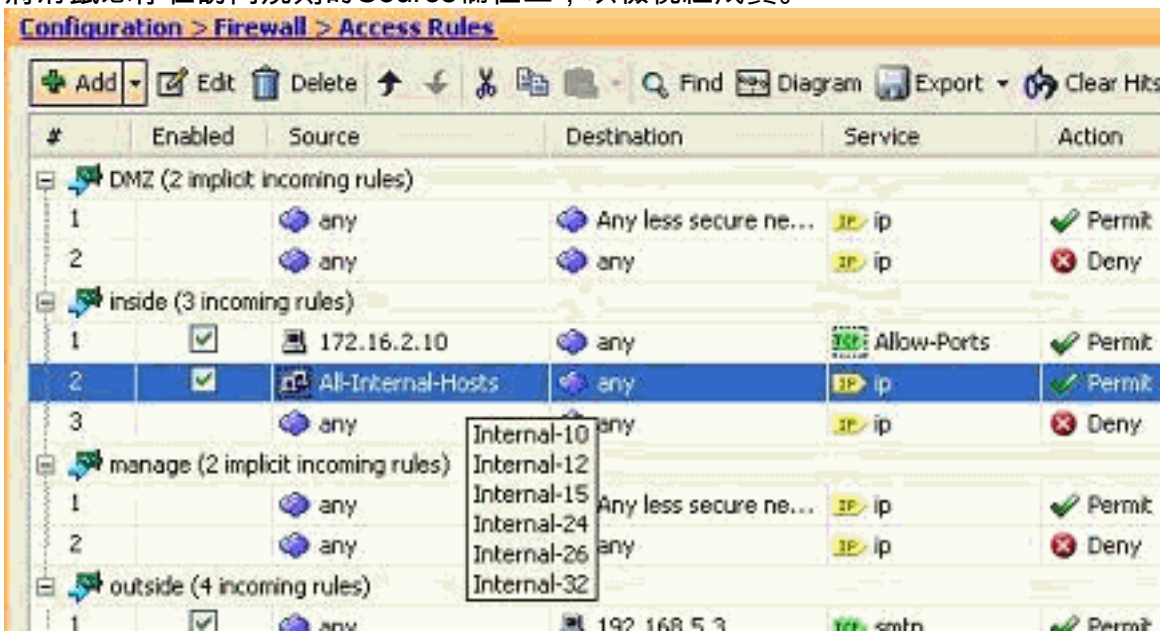


9. 選擇All-Internal-Hosts網路對象組，然後按一下OK按鈕。





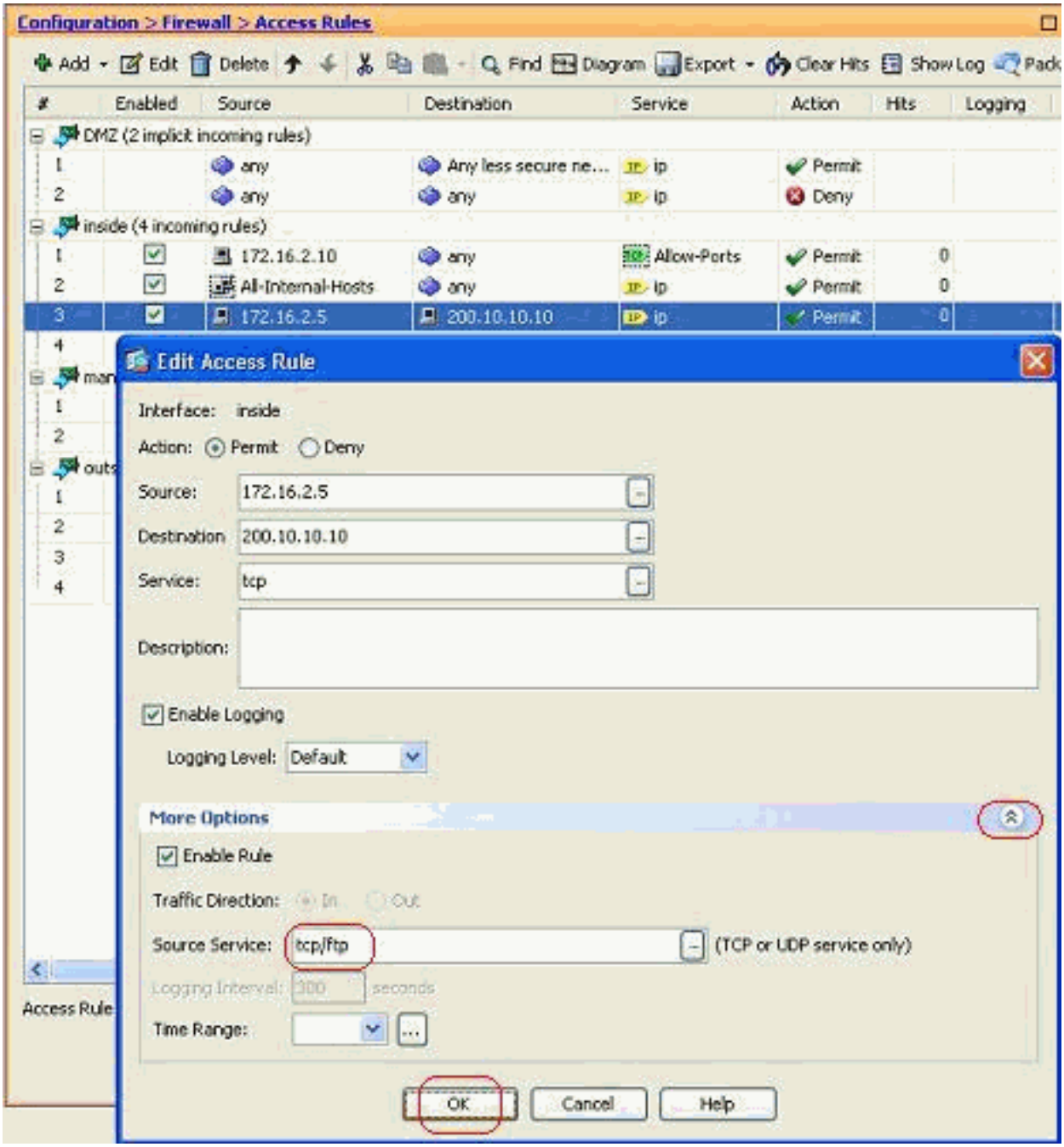
10. 按一下「**OK**」（確定）。
11. 將滑鼠懸停在訪問規則的Source欄位上，以檢視組成員。



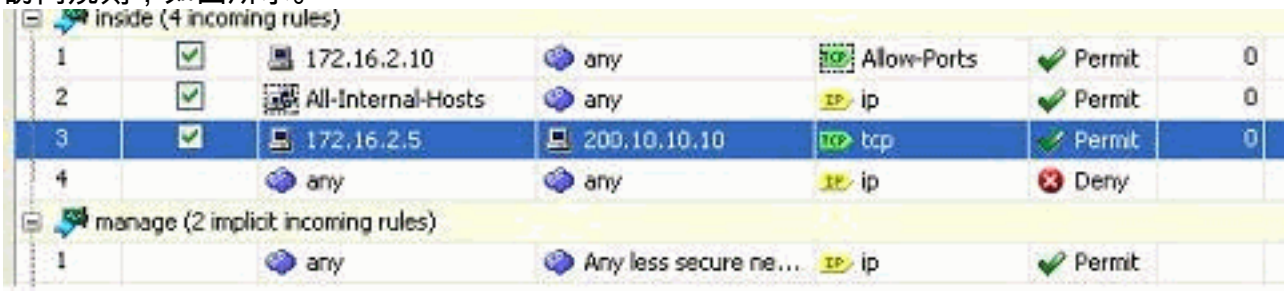
編輯源埠：

完成以下步驟即可修改存取規則的來源連線埠。

1. 若要修改現有訪問規則的源埠，請按一下右鍵該埠，然後選擇**Edit**。系統將顯示Edit Access Rule視窗。



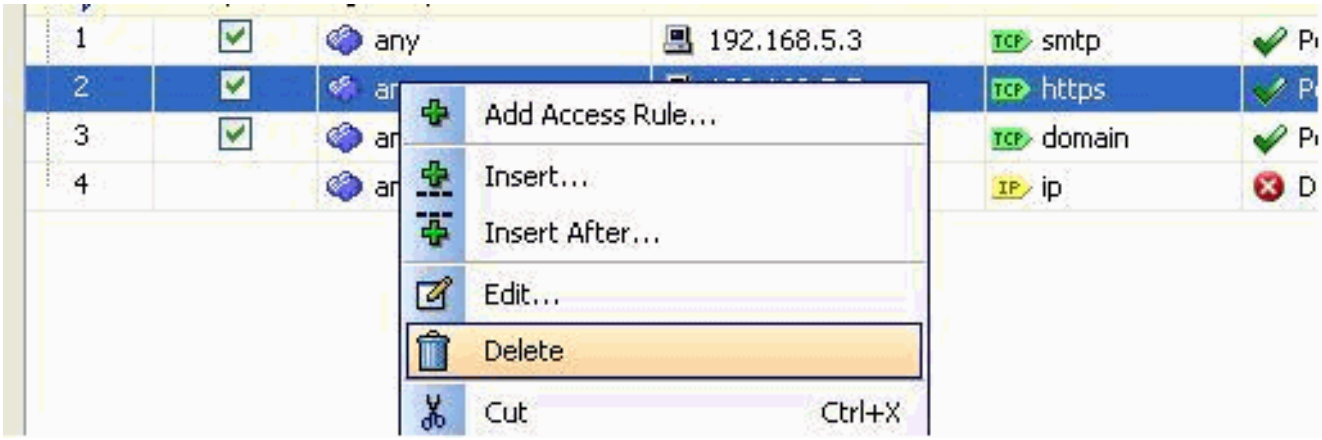
2. 按一下**More Options**下拉按鈕以修改Source Service欄位，然後按一下**OK**。您可以檢視修改的訪問規則，如圖所示。



刪除訪問清單

完成以下步驟即可刪除存取清單：

1. 刪除現有訪問清單之前，需要刪除訪問清單條目（訪問規則）。 除非首先刪除所有訪問規則，否則無法刪除訪問清單。按一下右鍵要刪除的訪問規則，然後選擇**刪除**。



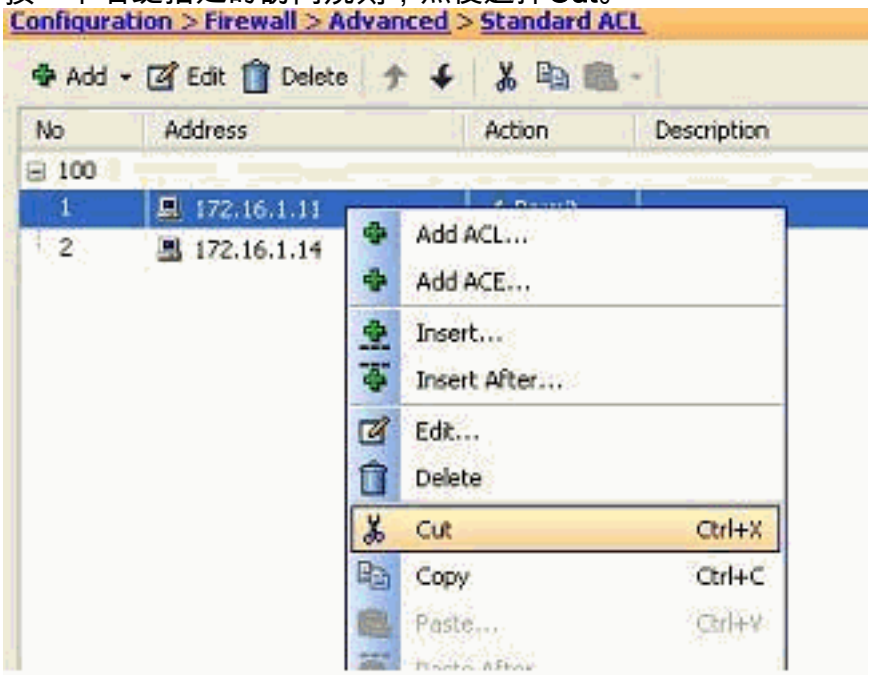
2. 對所有現有訪問規則完成相同的「刪除」操作，然後選擇訪問清單並選擇**刪除**以將其刪除。

匯出訪問規則

ASDM訪問規則將訪問清單與相應的介面繫結，而ACL Manager會跟蹤所有擴展訪問清單。使用ACL Manager建立的訪問規則不會繫結到任何介面。這些訪問清單通常用於NAT-Exempt、VPN-Filter以及沒有與介面關聯的其他類似功能。ACL Manager包含您在**Configuration > Firewall > Access Rules**部分具有的所有條目。此外，**ACL Manager**還包含未與任何介面關聯的全域性訪問規則。ASDM的組織方式可以讓您輕鬆地將訪問規則從任何訪問清單匯出到另一個訪問清單。

例如，如果您需要將已經是全域性訪問規則一部分的訪問規則與介面相關聯，則無需再次配置該規則。相反，您可以執行**剪下並貼上**操作來實現此目的。

1. 按一下右鍵指定的訪問規則，然後選擇**Cut**。



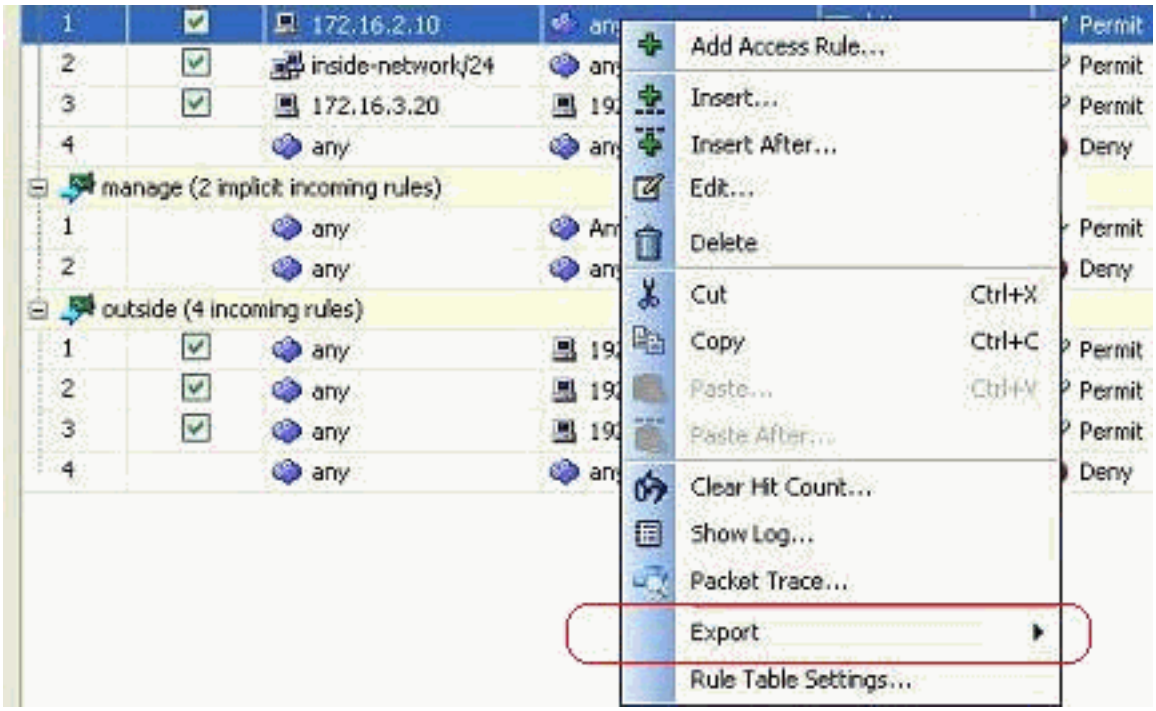
2. 選擇需要插入此訪問規則的所需訪問清單。您可以在工具欄中使用**貼上**來插入訪問規則。

匯出訪問清單資訊

您可以將訪問清單資訊匯出到另一個檔案。匯出此資訊支援兩種格式。

1. 逗號分隔值(CSV)格式
2. HTML格式

按一下右鍵任何訪問規則，然後選擇**匯出**以將訪問清單資訊傳送到檔案。



以下是以HTML格式顯示的訪問清單資訊。

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

驗證

目前沒有適用於此組態的驗證程序。

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

- ASDM配置示例和技術說明

- ASA配置示例和技術說明
- 技術支援與文件 - Cisco Systems