配置Cisco VPN 3000集中器以使用過濾器和RADIUS過濾器分配進行阻止

目錄

簡介

在此示例配置中，我們希望使用過濾器僅允許使用者訪問網路中的一個伺服器(10.1.1.2)，並阻止訪問所有其他資源。Cisco VPN 3000 Concentrator可以設定為通過過濾器控制IPsec、點對點隧道協定(PPTP)和L2TP客戶端對網路資源的訪問。過濾器由規則組成，類似於路由器上的訪問清單。如果路由器配置用於：

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

與VPN集中器等效的是設定一個包含規則的過濾器。

我們的第一個VPN集中器規則是**permit_server_rule**，它等效於路由器的**permit ip any host 10.1.1.2**命令。我們的第二條VPN集中器規則是**deny_server_rule**，它相當於路由器的**deny ip any any**命令。

我們的VPN集中器過濾器是**filter_with_2_rules**，它相當於路由器的101訪問清單；它使用**permit_server_rule**和**deny_server_rule**（按此順序）。 假設使用者端可以在新增過濾器之前正確連線；它們從VPN集中器上的池接收IP地址。

請參閱PIX/ASA 7.x ASDM:限制遠端訪問VPN使用者的網路訪問，以瞭解有關PIX/ASA 7.x阻止VPN使用者訪問的方案的詳細資訊。

必要條件

需求

本文件沒有特定需求。

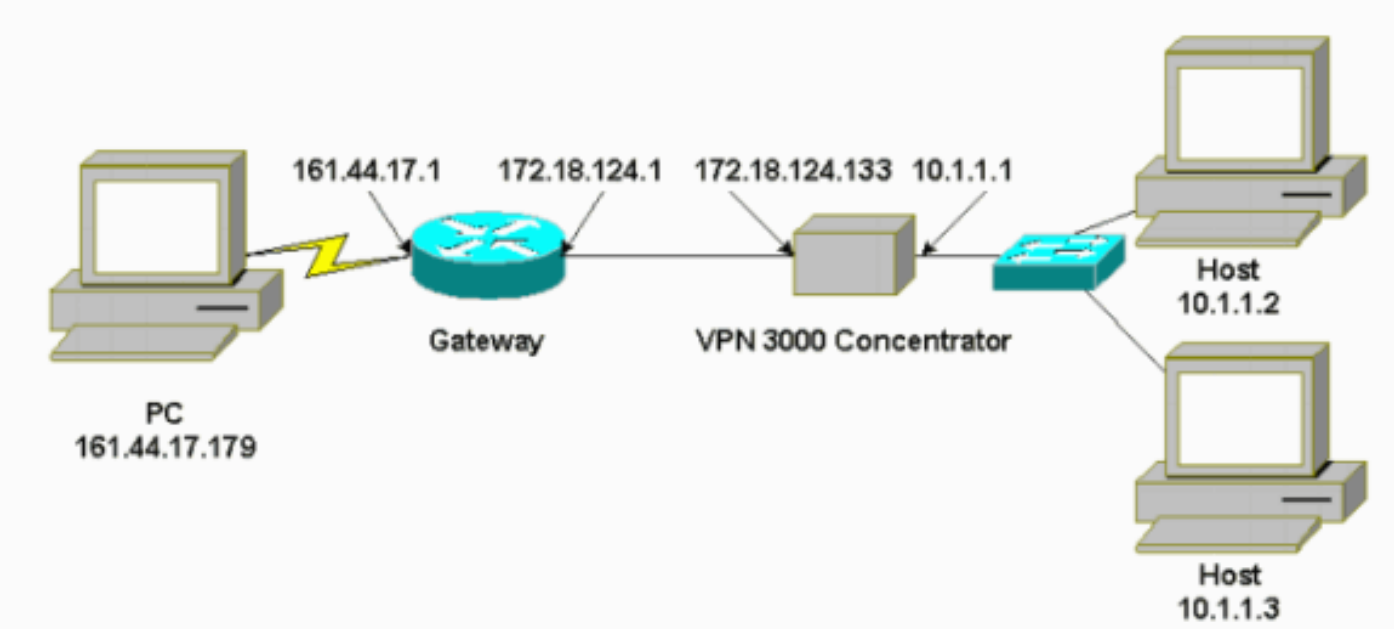
採用元件

本文檔中的資訊基於Cisco VPN 3000集中器版本2.5.2.D。

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。

網路圖表

本檔案會使用以下網路設定：



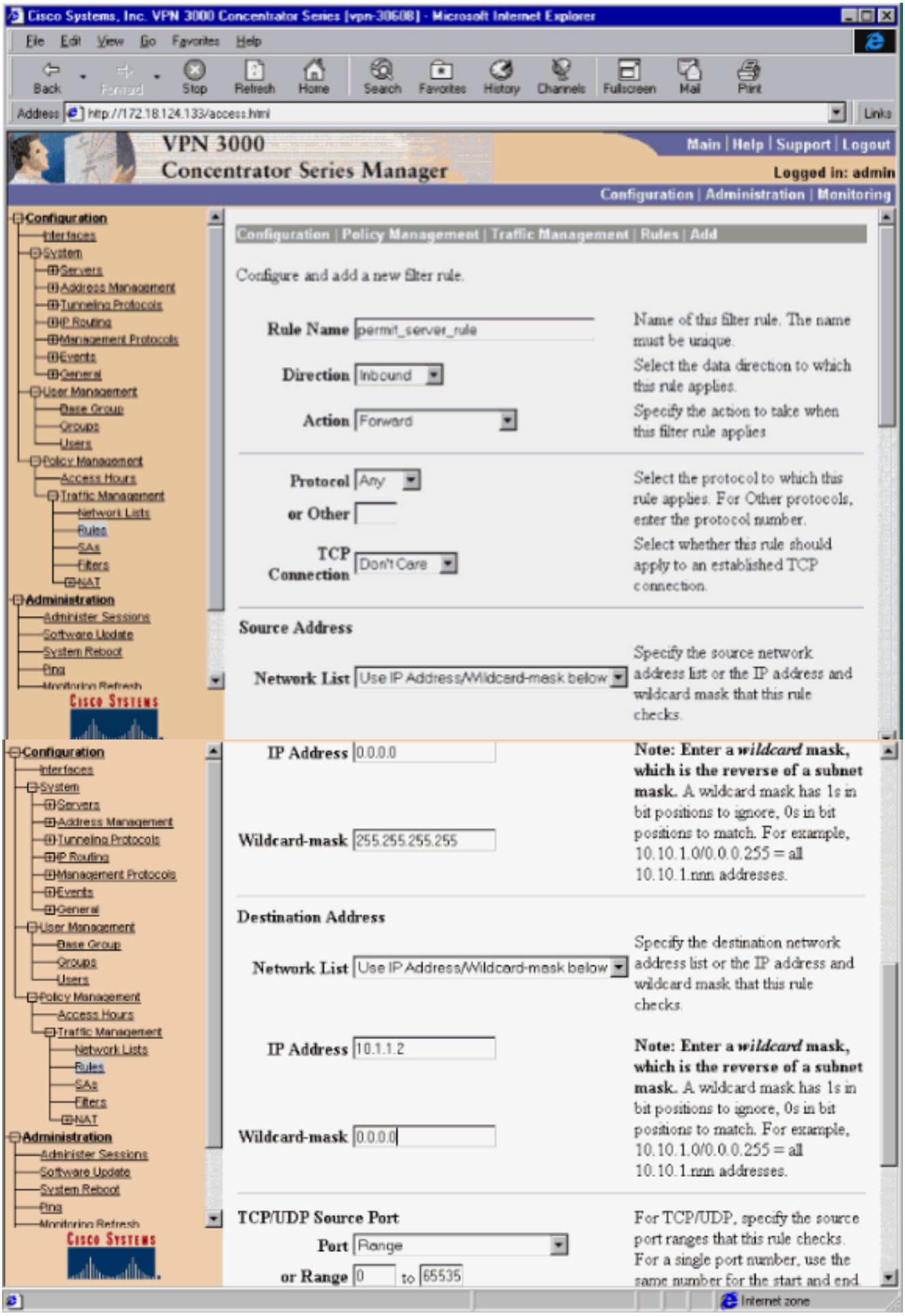
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

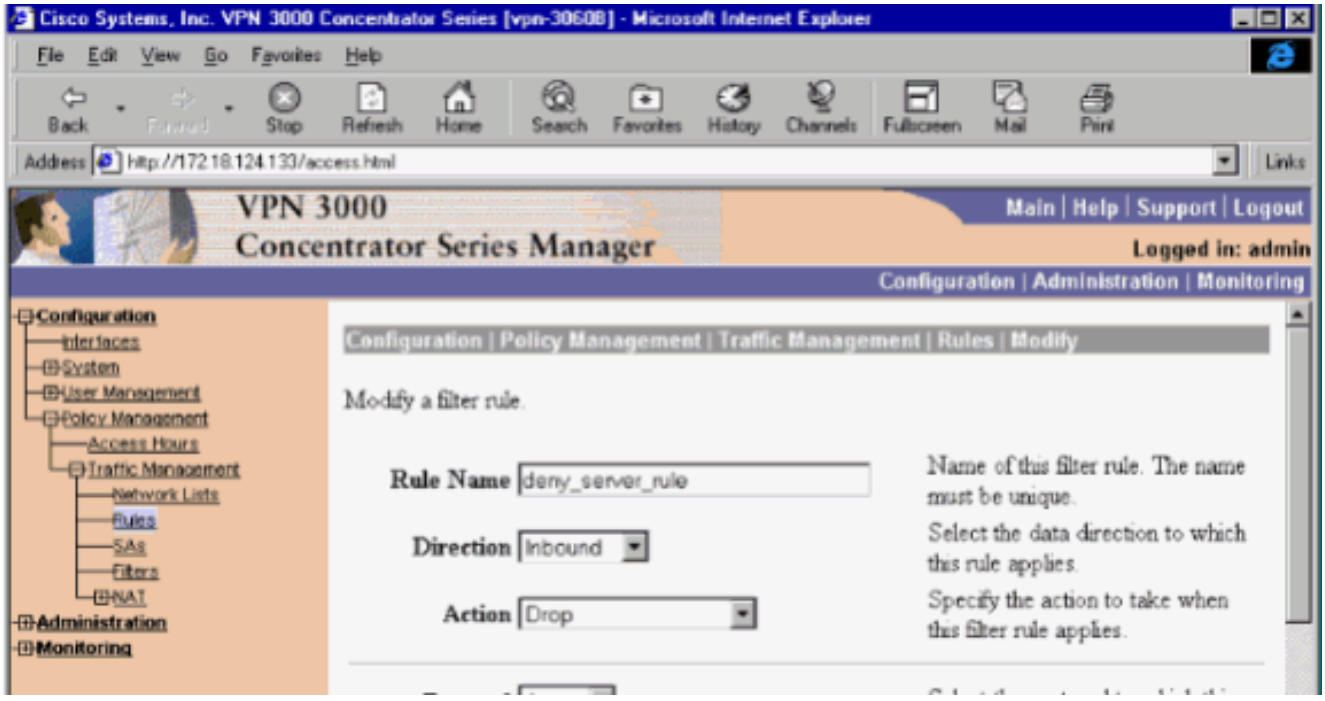
VPN 3000配置

完成以下步驟即可配置VPN 3000集中器。

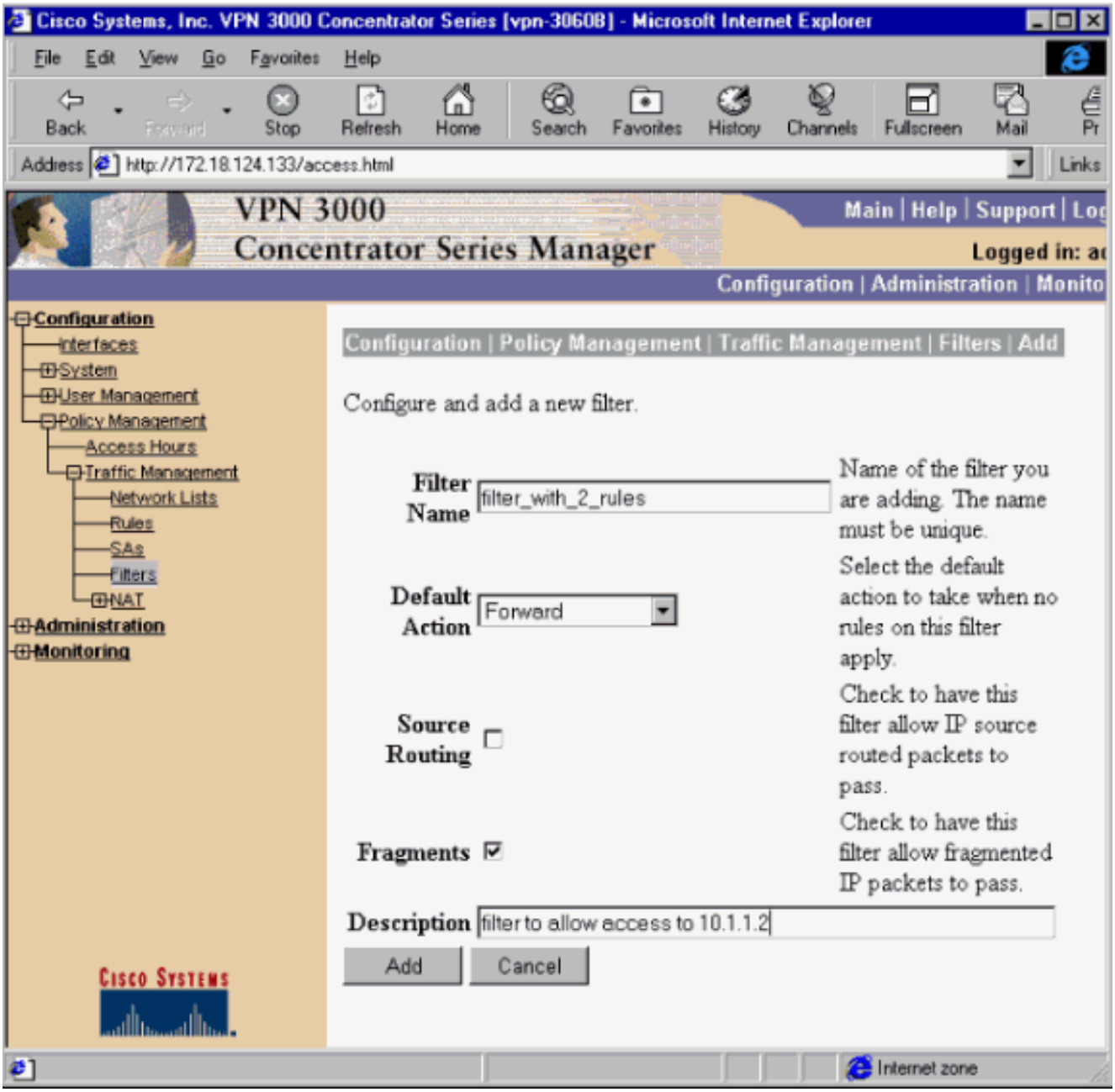
1. 選擇**Configuration > Policy Management > Traffic Management > Rules > Add**，然後使用以下設定定義第一個名為**permit_server_rule**的VPN集中器規則：Direction — 入**站**Action — 轉**向**源地址— **255.255.255.255**目標地址- **10.1.1.2**萬用字元掩碼- **0.0.0.0**



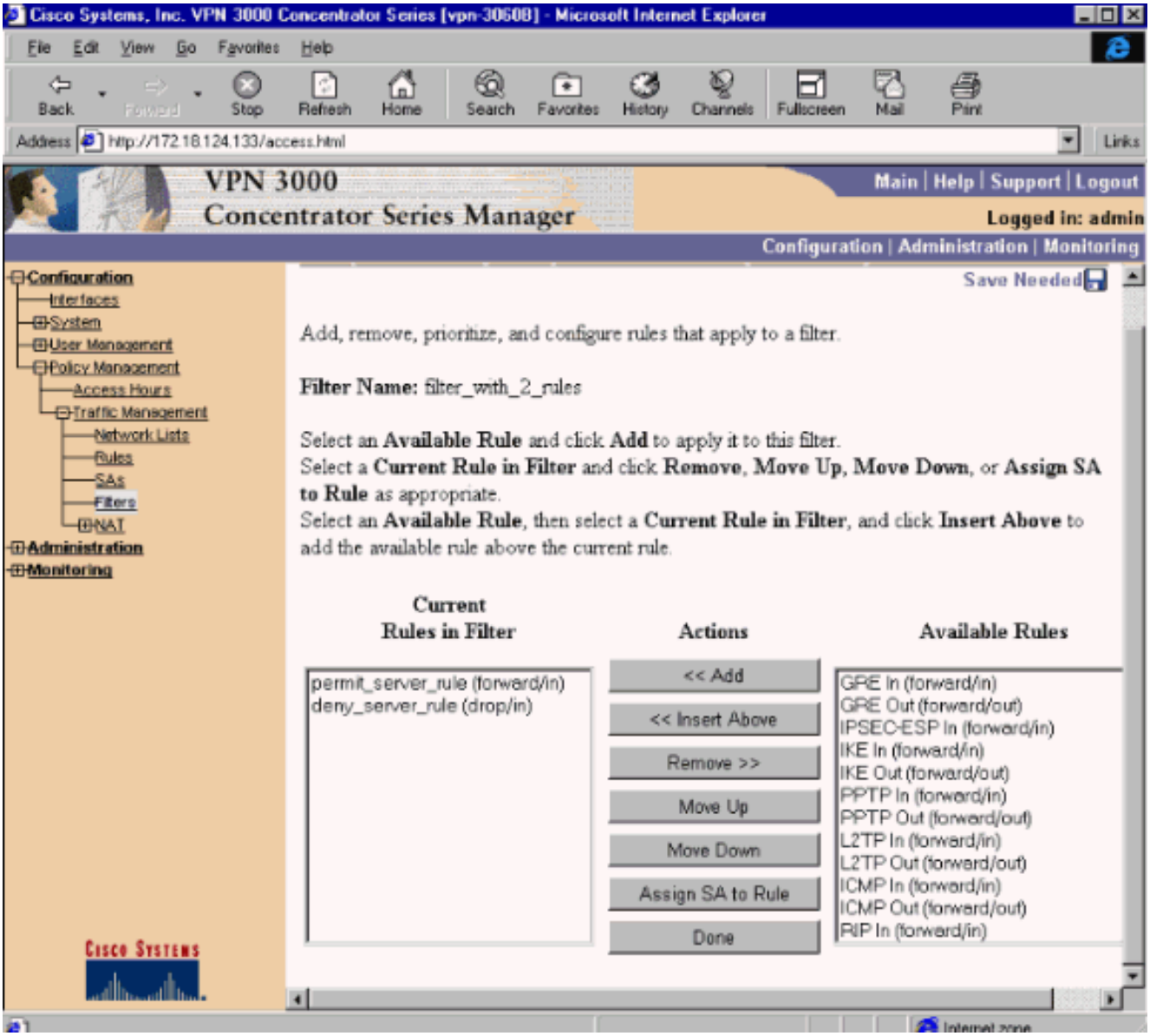
2. 在同一區域，定義名為**deny_server_rule**的第二個VPN集中器規則，預設值為：Direction — 入站Action -**Drop**任何地址(255.255.255.255)的源地址和目的地址
：



3. 選擇Configuration > Policy Management > Traffic Management > Filters，然後新增filter_with_2_rules過濾器。



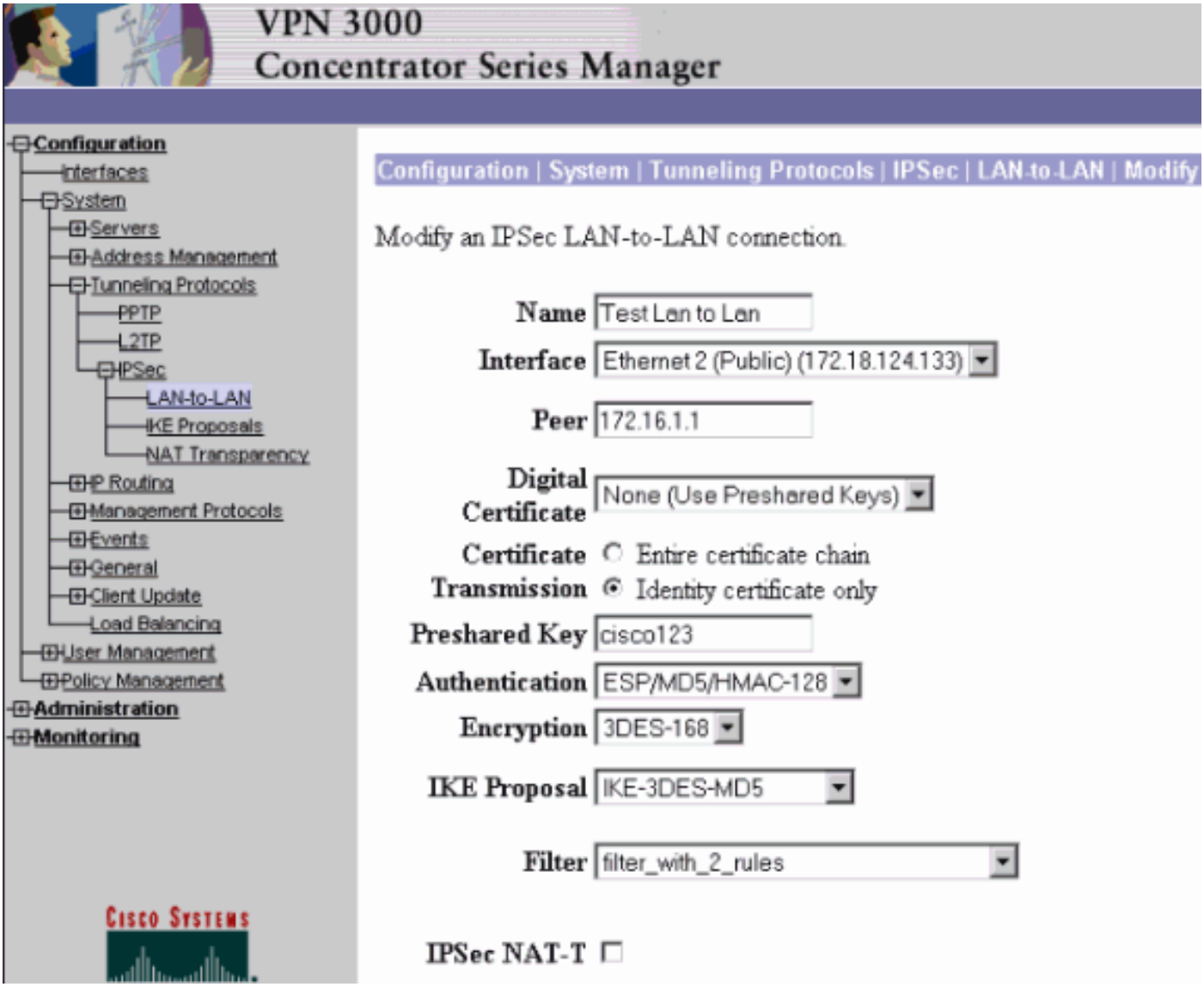
4. 將兩個規則新增到 filter_with_2_rules:



5. 選擇**Configuration > User Management > Groups**，然後將過濾器應用到組：

LAN到LAN VPN隧道的過濾器

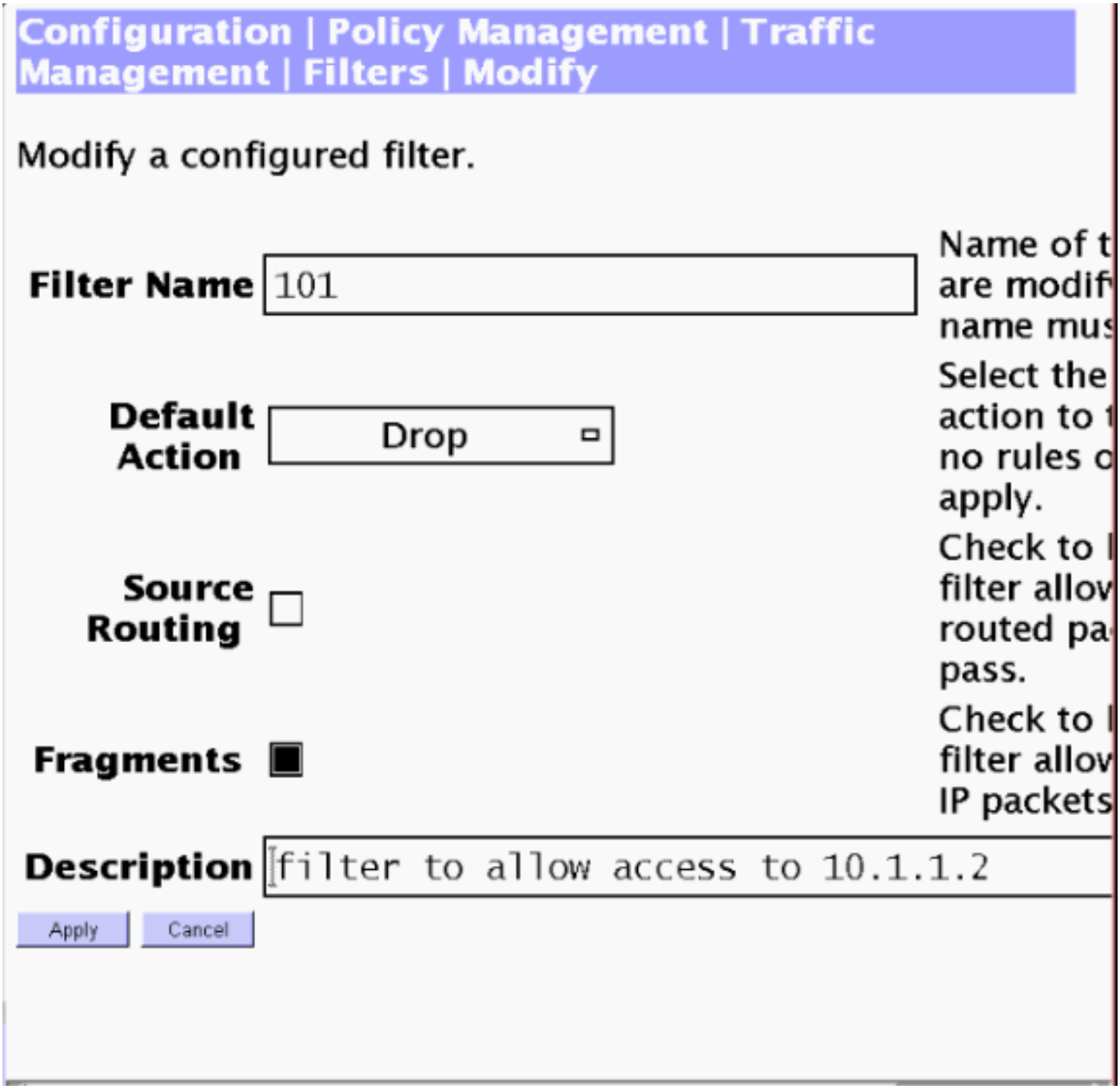
從VPN集中器代碼3.6及更高版本中，可以過濾每個LAN到LAN IPsec VPN隧道的流量。例如，如果建立到另一個地址為172.16.1.1的VPN集中器的LAN到LAN隧道，並希望在拒絕所有其他流量時允許主機10.1.1.2訪問該隧道，則可以在選擇**Configuration > System > Tunneling Protocols > IPSec > LAN到LAN > Modify**時應用**filter_with_2_rules**，然後在**Filter**下選擇**filter_with_2_rules**。



VPN 3000配置 — RADIUS過濾器分配

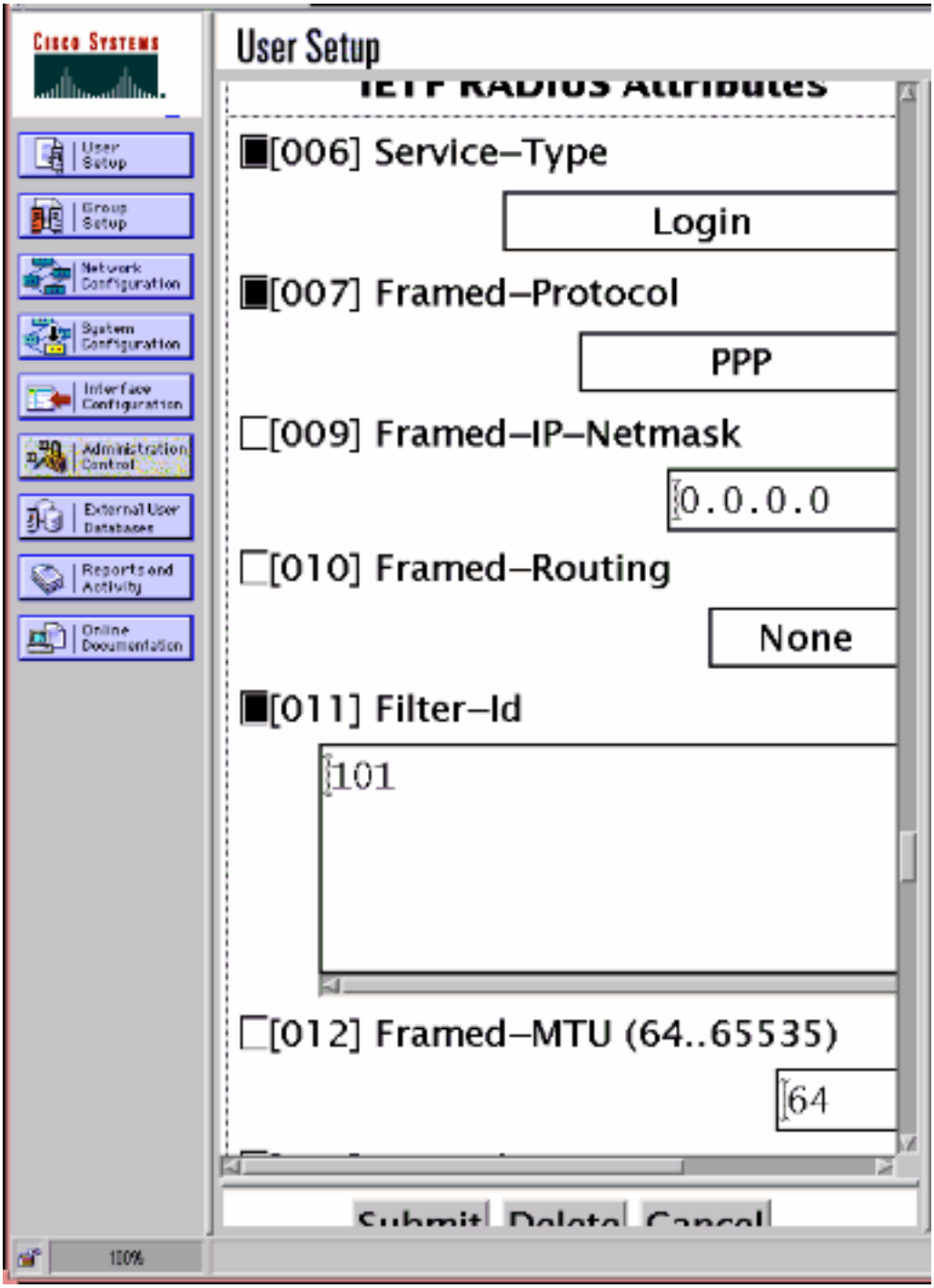
也可以在VPN集中器中定義過濾器，然後從RADIUS伺服器傳遞過濾器編號（在RADIUS術語中，屬性11為Filter-id），以便當使用者在RADIUS伺服器上進行身份驗證時，Filter-id與該連線相關聯。在本示例中，假設針對VPN集中器使用者的RADIUS身份驗證已正常運行，且僅新增Filter-id。

在VPN集中器上定義過濾器，如上一個示例所示：



CSNT伺服器配置 — RADIUS過濾器分配

將Cisco Secure NT伺服器上的屬性11, Filter-id配置為**101**:



調試 — RADIUS過濾器分配

如果VPN集中器中的AUTHDECODE（1-13嚴重性）處於開啟狀態，則日誌顯示Cisco Secure NT伺服器向下傳送屬性11(0x0B)中的訪問清單101:

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

僅出於故障排除目的，您可以在選擇**Configuration > System > Events > Classes**並新增**FILTERDBG**類(嚴重性為**Log = 13**)時啟用過濾器調試。在規則中，將Default操作從Forward（或Drop）更改為**Forward and Log**（或Drop and Log）。 在**Monitoring > Event Log**中檢索事件日誌時，它應顯示如下條目：

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

相關資訊

- IPSec 協商/IKE 通訊協定
- VPN 3000 Concentrator常見問題
- RADIUS支援
- Cisco VPN 3000 Concentrator支援
- Cisco VPN 3000使用者端支援
- Cisco Secure ACS for Windows支援
- 要求建議(RFC)
- 技術支援與文件 - Cisco Systems