

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

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[VPN 3000配置](#)

[LAN到LAN VPN隧道的過濾器](#)

[VPN 3000配置 — RADIUS過濾器分配](#)

[CSNT伺服器配置 — RADIUS過濾器分配](#)

[調試 — RADIUS過濾器分配](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

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。

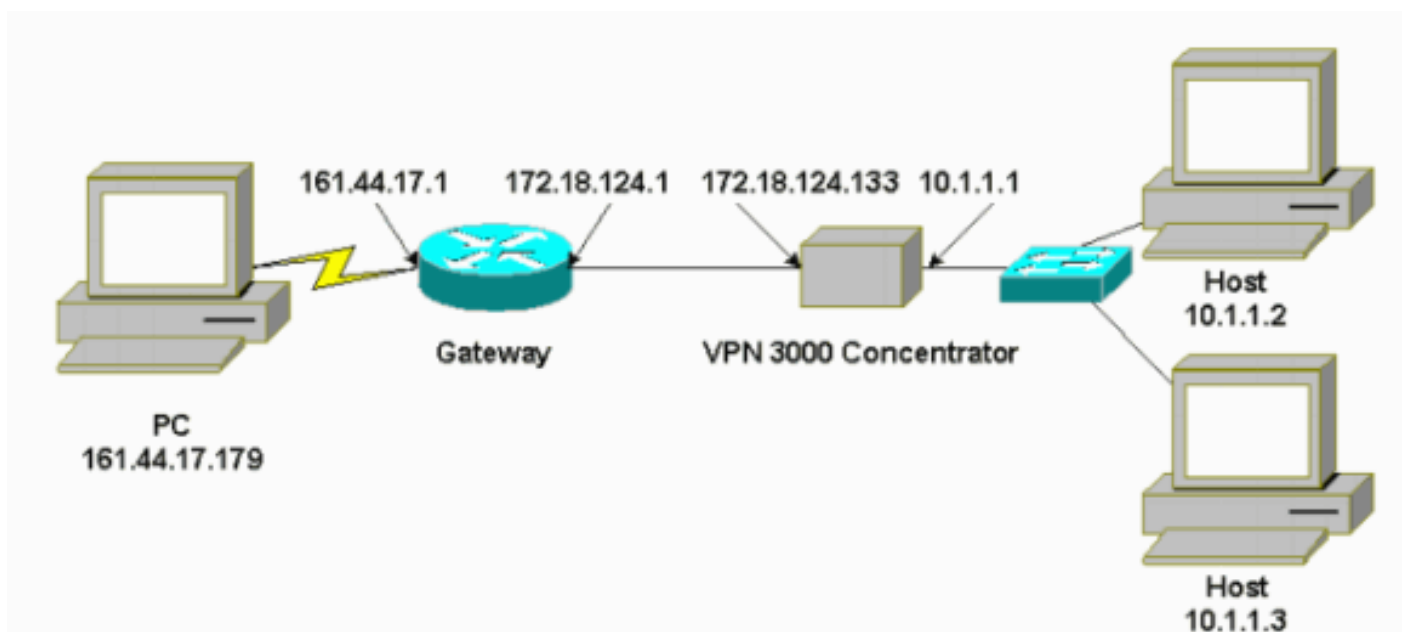
採用元件

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

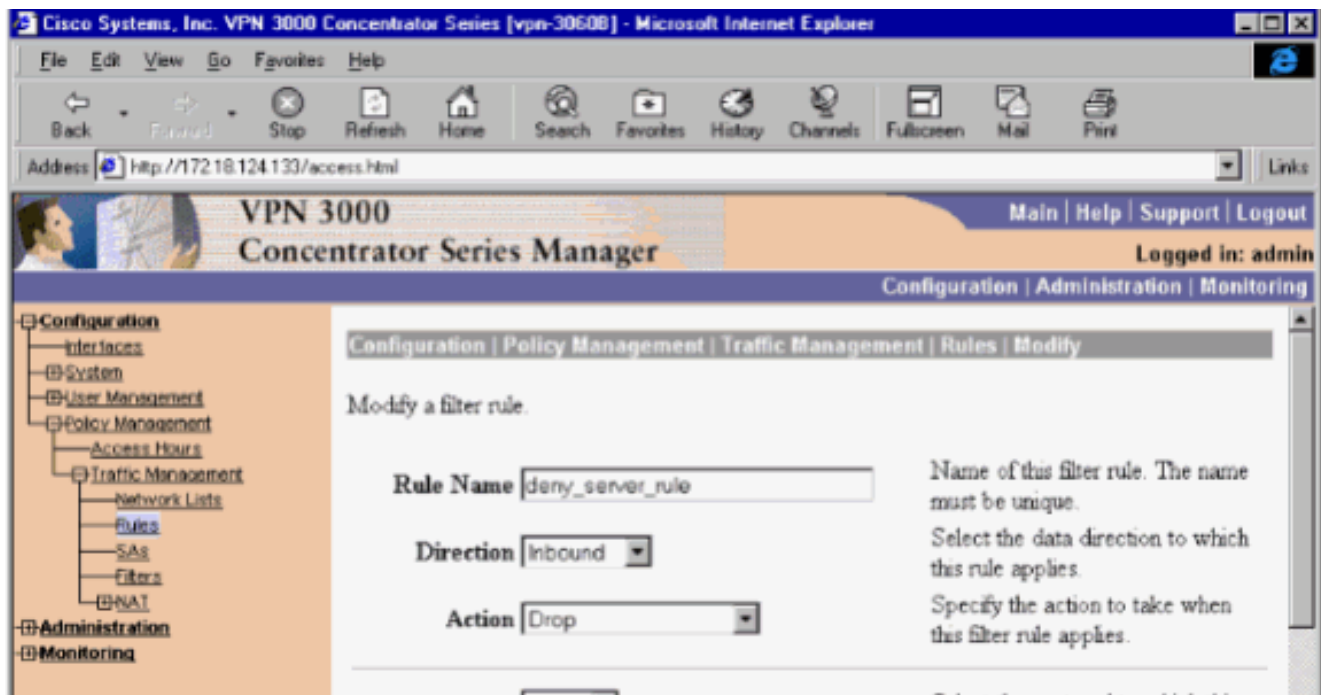
The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer". The address bar shows "http://172.16.124.133/access.html". The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes "Configuration", "Administration", and "Monitoring".

The main content area is titled "Configuration | Policy Management | Traffic Management | Rules | Add". It contains the following fields and instructions:

- Rule Name:** Name of this filter rule. The name must be unique.
- Direction:** Select the data direction to which this rule applies.
- Action:** Specify the action to take when this filter rule applies.
- Protocol:** Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
- or Other:** Enter the protocol number.
- TCP Connection:** Select whether this rule should apply to an established TCP connection.
- Source Address:**
 - Network List:** Specify the source network address list or the IP address and wildcard mask that this rule checks.
 - IP Address:**
 - Wildcard-mask:** **Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**
- Destination Address:**
 - Network List:** Specify the destination network address list or the IP address and wildcard mask that this rule checks.
 - IP Address:** **Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**
 - Wildcard-mask:**
- TCP/UDP Source Port:**
 - Port:** For TCP/UDP, specify the source port ranges that this rule checks.
 - or Range:** to For a single port number, use the same number for the start and end.

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。

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html

VPN 3000 Concentrator Series Manager Main | Help | Support | Log

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name Name of the filter you are adding. The name must be unique.

Default Action Select the default action to take when no rules on this filter apply.

Source Routing Check to have this filter allow IP source routed packets to pass.

Fragments Check to have this filter allow fragmented IP packets to pass.

Description

Add Cancel

CISCO SYSTEMS

Internet zone

4. 將兩個規則新增到 filter_with_2_rules:

Address: http://172.18.124.133/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Save Needed

Configuration

- Interfaces
- System
- User Management
- Policy Management
 - Access Hours
 - Traffic Management
 - Network Lists
 - Rules
 - SAs
 - Filters
 - NAT
- Administration
- Monitoring

Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: filter_with_2_rules

Select an **Available Rule** and click **Add** to apply it to this filter.

Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.

Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

| Current Rules in Filter | Actions | Available Rules |
|---|---|--|
| permit_server_rule (forward/in) deny_server_rule (drop/in) | << Add << Insert Above Remove >> Move Up Move Down Assign SA to Rule Done | GRE In (forward/in) GRE Out (forward/out) IPSEC-ESP In (forward/in) IKE In (forward/in) IKE Out (forward/out) PPTP In (forward/in) PPTP Out (forward/out) L2TP In (forward/in) L2TP Out (forward/out) ICMP In (forward/in) ICMP Out (forward/out) RIP In (forward/in) |

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

:

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer

Address: http://172.16.124.133/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify servergroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

| General Parameters | | | |
|---------------------------------|-------------------------------------|-------------------------------------|--|
| Attribute | Value | Inherit? | Description |
| Access Hours | -No Restrictions- | <input checked="" type="checkbox"/> | Select the access hours assigned to this group. |
| Simultaneous Logins | 3 | <input checked="" type="checkbox"/> | Enter the number of simultaneous logins for this group. |
| Minimum Password Length | 8 | <input checked="" type="checkbox"/> | Enter the minimum password length for users in this group. |
| Allow Alphabetic-Only Passwords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Enter whether to allow alphabetic-only passwords. |
| Idle Timeout | 30 | <input checked="" type="checkbox"/> | (minutes) Enter the idle timeout for this group. |
| Maximum Connect Time | 0 | <input checked="" type="checkbox"/> | (minutes) Enter the maximum connect time for this group. |
| Filter | filter_with_2_rules | <input type="checkbox"/> | Enter the filter assigned to this group. |
| Primary DNS | | <input checked="" type="checkbox"/> | Enter the IP address of the primary DNS server. |
| Secondary DNS | | <input type="checkbox"/> | Enter the IP address of the |

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 Concentrator Series Manager

- Configuration
 - Interfaces
 - System
 - Servers
 - Address Management
 - Tunneling Protocols
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - IP Routing
 - Management Protocols
 - Events
 - General
 - Client Update
 - Load Balancing
 - User Management
 - Policy Management
- Administration
- Monitoring

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name

Interface

Peer

Digital Certificate

Certificate Entire certificate chain

Transmission Identity certificate only

Preshared Key

Authentication

Encryption

IKE Proposal

Filter

IPSec NAT-T

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：

Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name

Name of the filter to be modified. The name must be unique.

Default Action

Select the default action to be applied to traffic when no rules are found.

Source Routing

Check to allow the filter to apply to source-routed packets.

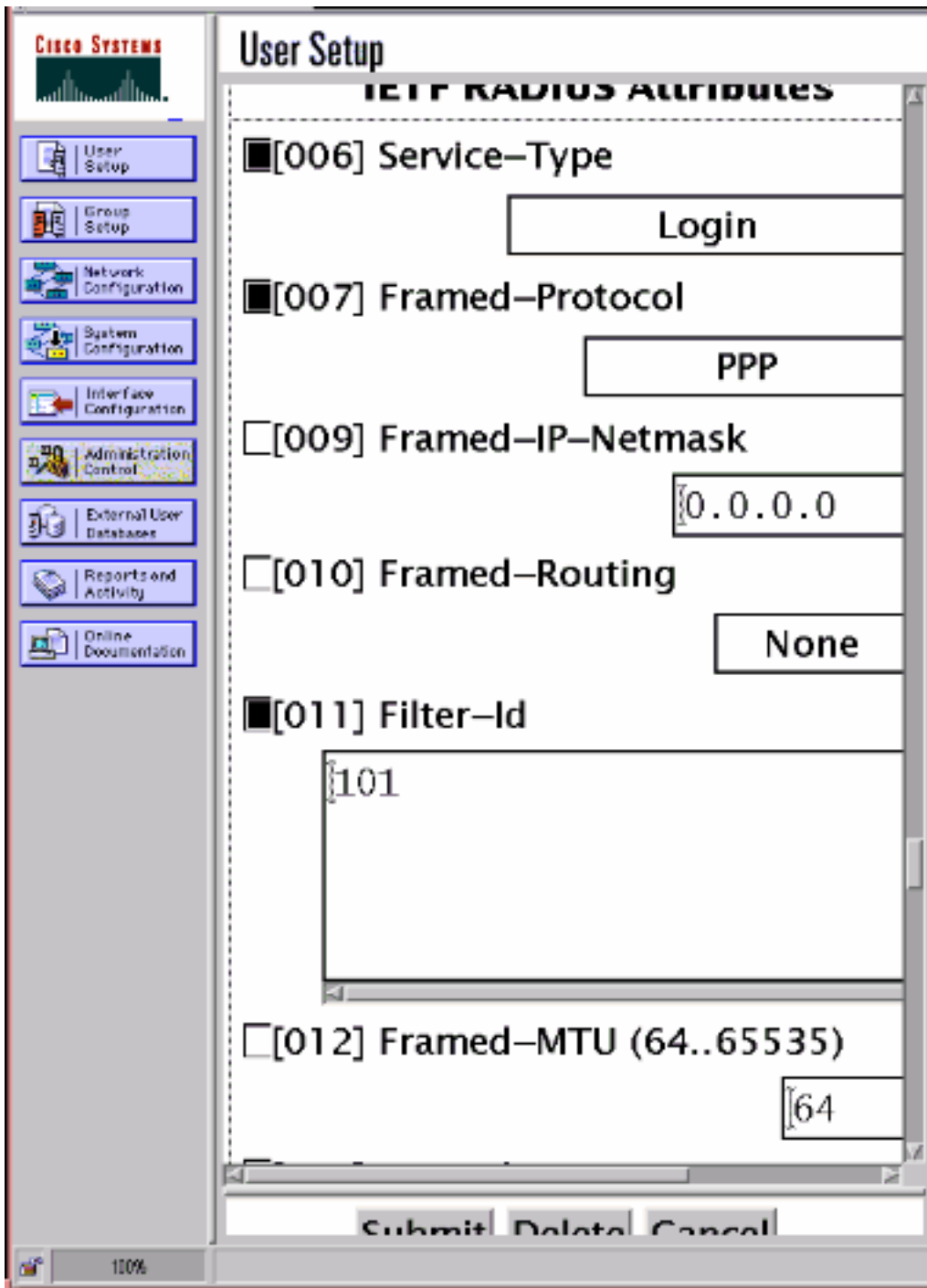
Fragments

Check to allow the filter to apply to fragmented IP packets.

Description

[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 FFFFFFFF ..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](#)