配置 Cisco VPN 3000 集中器以阻断过滤器与 RADIUS 过滤器分配

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[网络图](#)
[规则](#)
[VPN 3000 配置](#)
[LAN到LAN VPN隧道的过滤器](#)
[VPN 3000 配置 - RADIUS 过滤器分配](#)
[CSNT 服务器配置 - RADIUS 过滤器分配](#)
[调试 - RADIUS 过滤器分配](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

在此配置示例中，我们只要使用过滤器允许用户访问一个服务器(10.1.1.2)在网络里面和阻止对其他资源的访问。Cisco VPN 3000集中器可以设置用过滤器控制IPsec、点对点隧道协议(PPTP)和L2TP访客接入对网络资源。过滤器包括规则，类似于在路由器的访问列表。如果路由器配置为：

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

VPN集中器等同是设置有规则的一个过滤器。

我们的第一个VPN集中器规则是**permit_server_rule**，与路由器的**permit ip**是等同的**所有主机10.1.1.2**命令。与**deny ip any any命令的**路由器的是等同的我们的第二个VPN集中器规则是**deny_server_rule**。

我们的VPN集中器过滤器是**filter_with_2_rules**，与路由器的101访问列表是等同的;它使用**permit_server_rule**和**deny_server_rule** (按该顺序)。假设，客户端能在添加过滤器之前正确连接;他们收到他们的从一个池的IP地址VPN集中器的。

有关如何配置远程访问服务器以及限制访问的更多信息，请参阅 [PIX/ASA 7.x ASDM：限制远程访问VPN用户网络访问](#)为了得知更多PIX/ASA 7.x块从VPN用户的访问的方案。

先决条件

要求

本文档没有任何特定的要求。

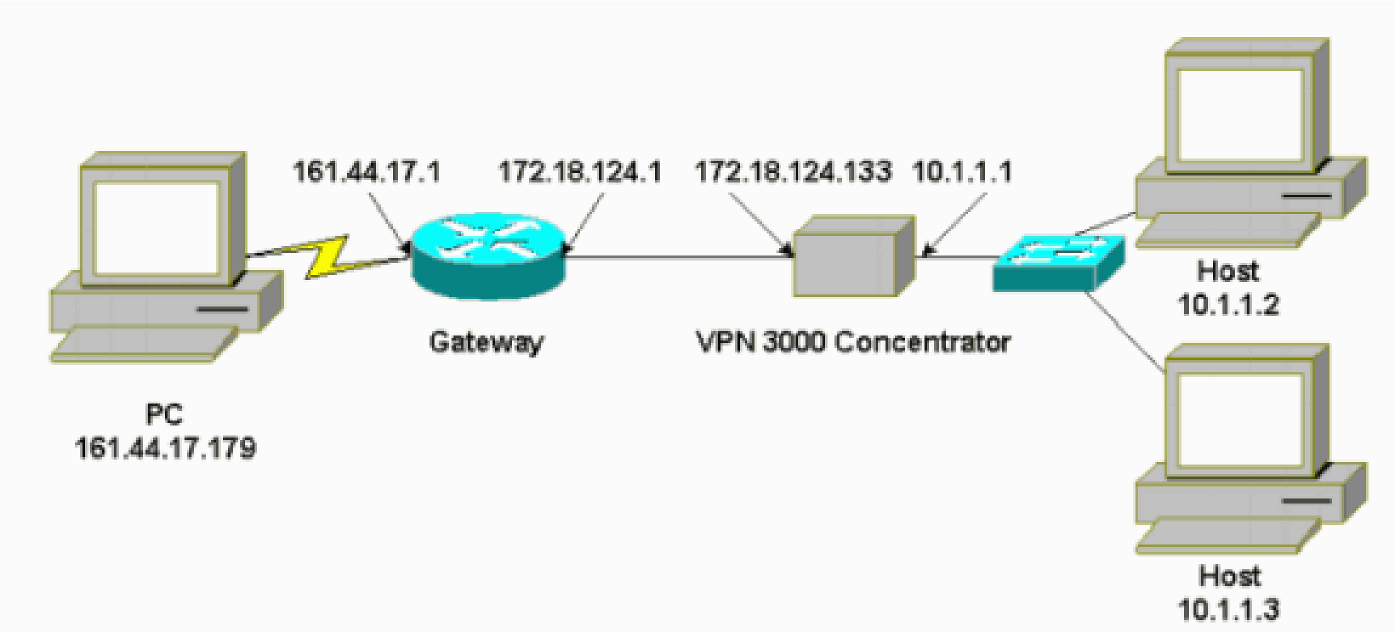
使用的组件

本文档中的信息根据Cisco VPN 3000集中器版本2.5.2.D。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



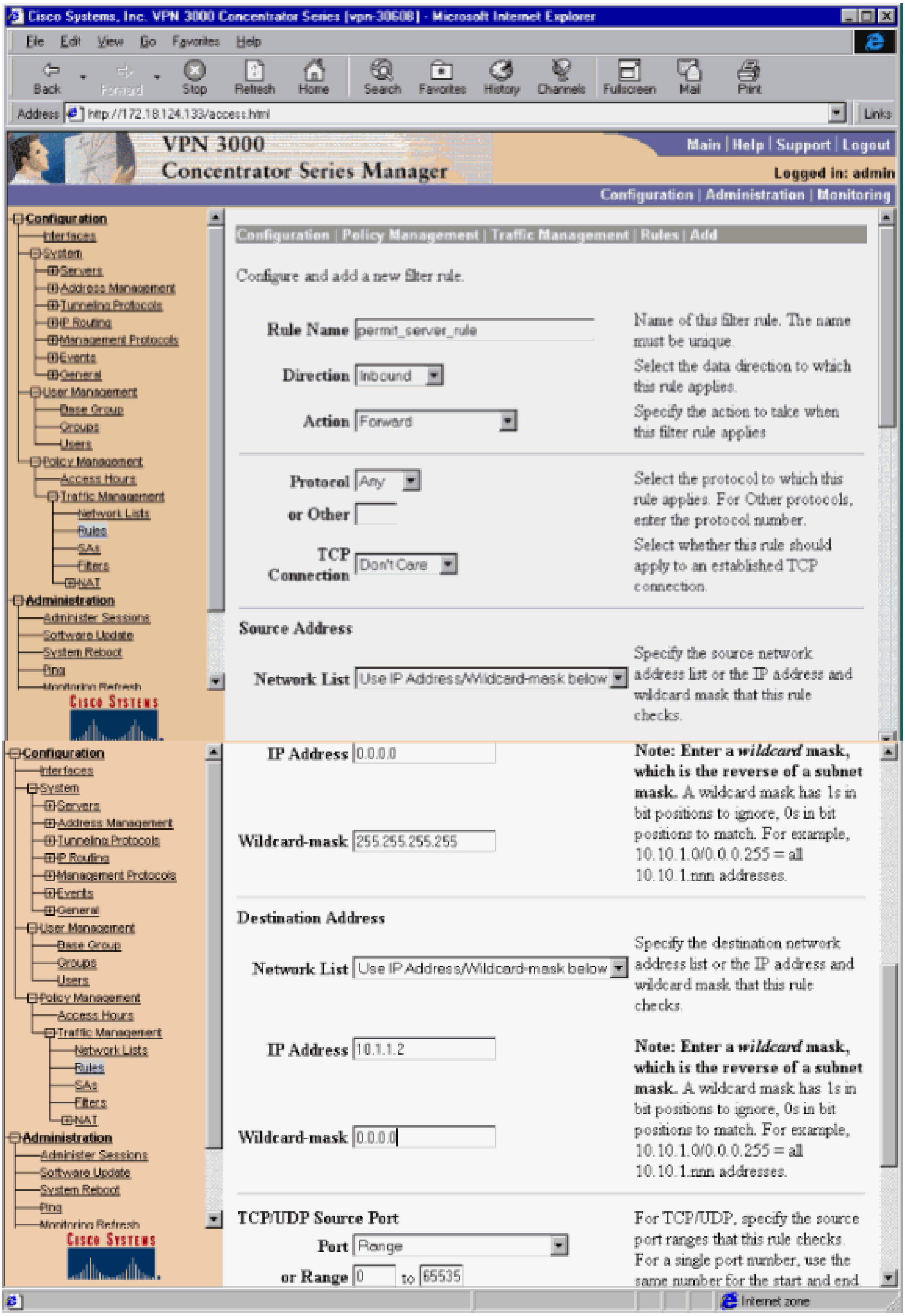
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

VPN 3000 配置

完成这些步骤为了配置VPN 3000集中器。

1. 选择**配置>Policy Management>流量管理>规则>Add**并且定义与这些设置的第一个VPN集中器规则呼叫的**permit_server_rule** ：方向**—入站**操作**—前言**源地址**— 255.255.255.255**目的地址**— 10.1.1.2**通配符掩码**—**
   0.0.0.0



Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name: permit_server_rule — Name of this filter rule. The name must be unique.

Direction: Inbound — Select the data direction to which this rule applies.

Action: Forward — Specify the action to take when this filter rule applies.

Protocol: Any — or Other: — Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

TCP Connection: Don't Care — Select whether this rule should apply to an established TCP connection.

Source Address

Network List: Use IP Address/Wildcard-mask below — Specify the source network address list or the IP address and wildcard mask that this rule checks.

IP Address: 0.0.0.0

Wildcard-mask: 255.255.255.255

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: Use IP Address/Wildcard-mask below — Specify the destination network address list or the IP address and wildcard mask that this rule checks.

IP Address: 10.1.1.2

Wildcard-mask: 0.0.0.0

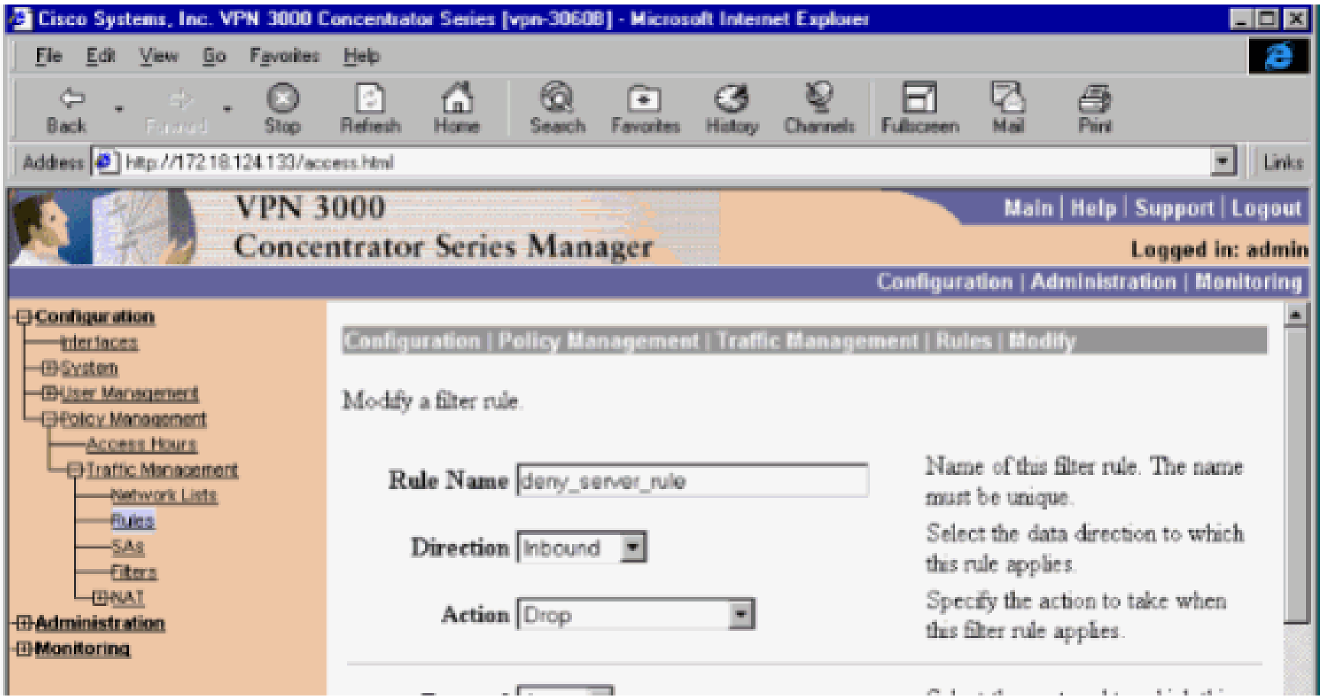
Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

TCP/UDP Source Port

Port: Range — For TCP/UDP, specify the source port ranges that this rule checks.

or Range: 0 to 65535 — For a single port number, use the same number for the start and end

2. 在同一个区域中，请定义呼叫的第二个VPN集中器规则**deny_server_rule**以这些默认：方向**—入站**操作**—丢弃**任何东西的源地址和目的地址(255.255.255.255)：

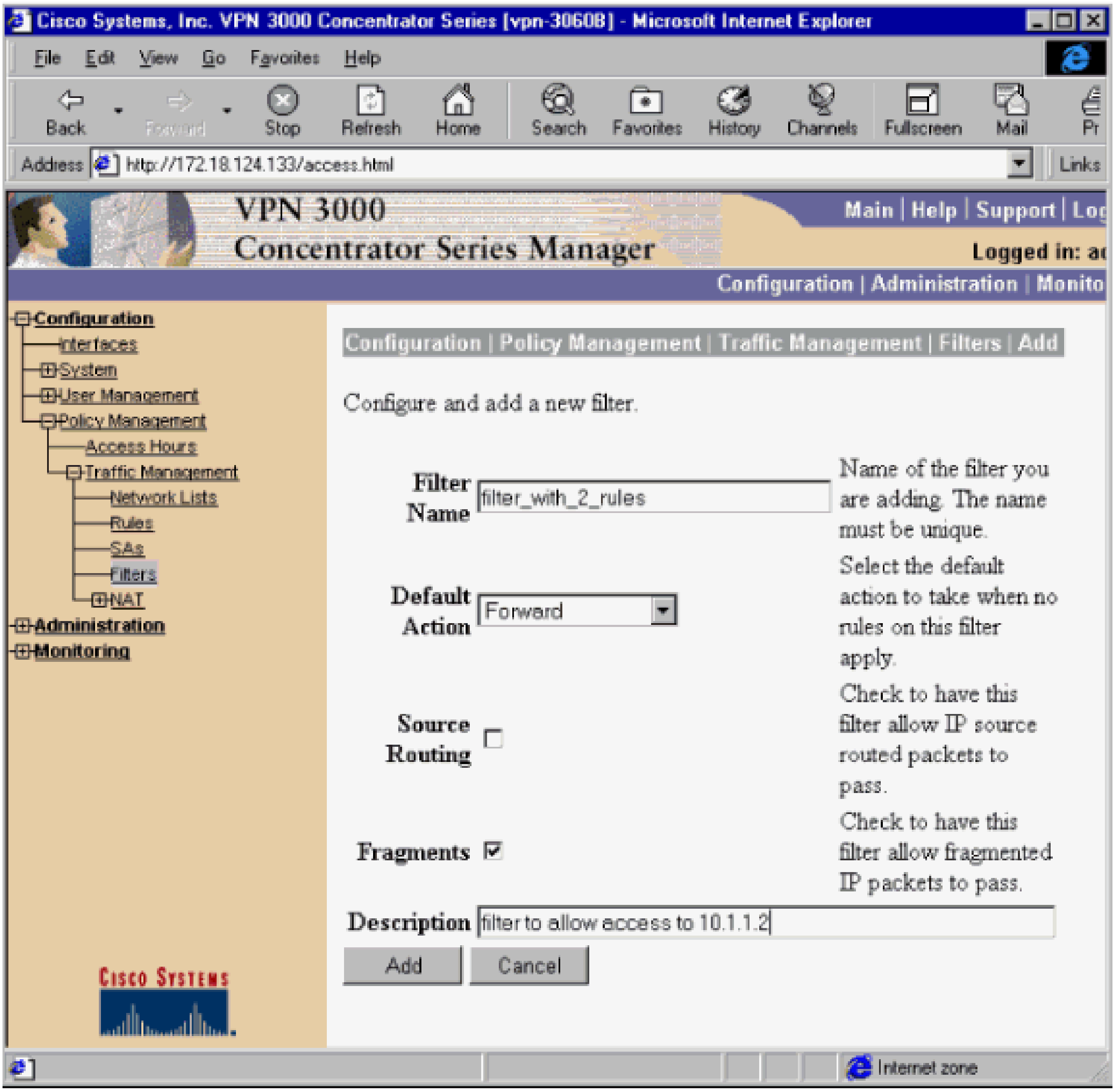

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring

Configuration | Policy Management | Traffic Management | Rules | Modify

Modify a filter rule.

Rule Name	deny_server_rule	Name of this filter rule. The name must be unique.
Direction	Inbound	Select the data direction to which this rule applies.
Action	Drop	Specify the action to take when this filter rule applies.

3. 选择Configuration > Policy Management > Traffic Management > Filters并且添加您的filter_with_2_rules过滤器。


Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Pr
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Log
Logged in: ac
Configuration | Administration | Monito
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Internet zone

Configuration | Policy Management | Traffic Management | Filters | Add

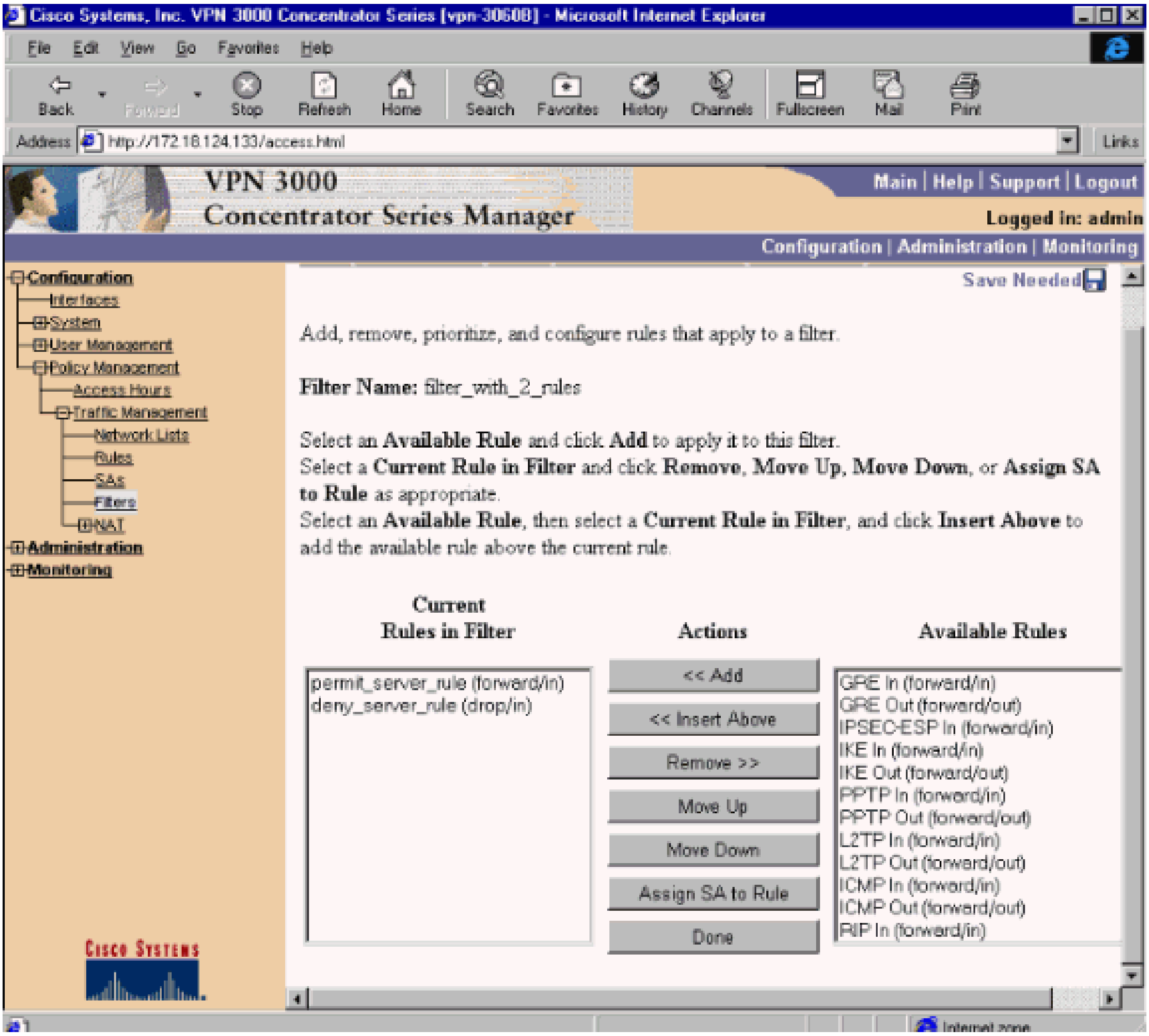
Configure and add a new filter.

Filter Name	filter_with_2_rules	Name of the filter you are adding. The name must be unique.
Default Action	Forward ▾	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	filter to allow access to 10.1.1.2	

Add   Cancel

4. 增加两个规则到filter_with_2_rules

：


Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30600] - 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
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Save Needed
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Assign SA to Rule
Done
Internet zone

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

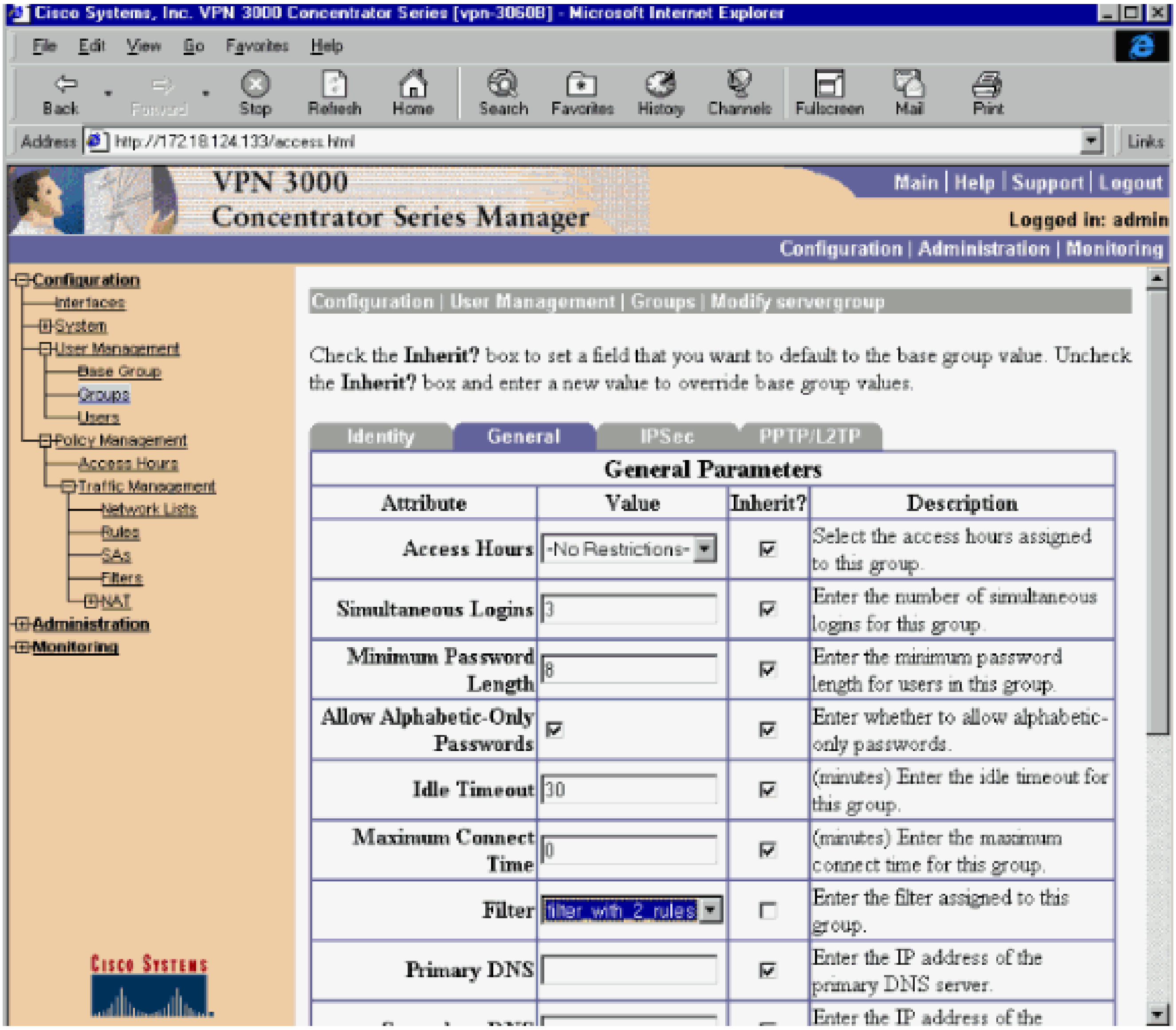
permit_server_rule (forward/in)
deny_server_rule (drop/in)

Actions

Available Rules

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. 选择**Configuration > User Management > Groups**并且应用过滤器给组
:


Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - 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
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Identity
General
IPSec
PPTP/L2TP

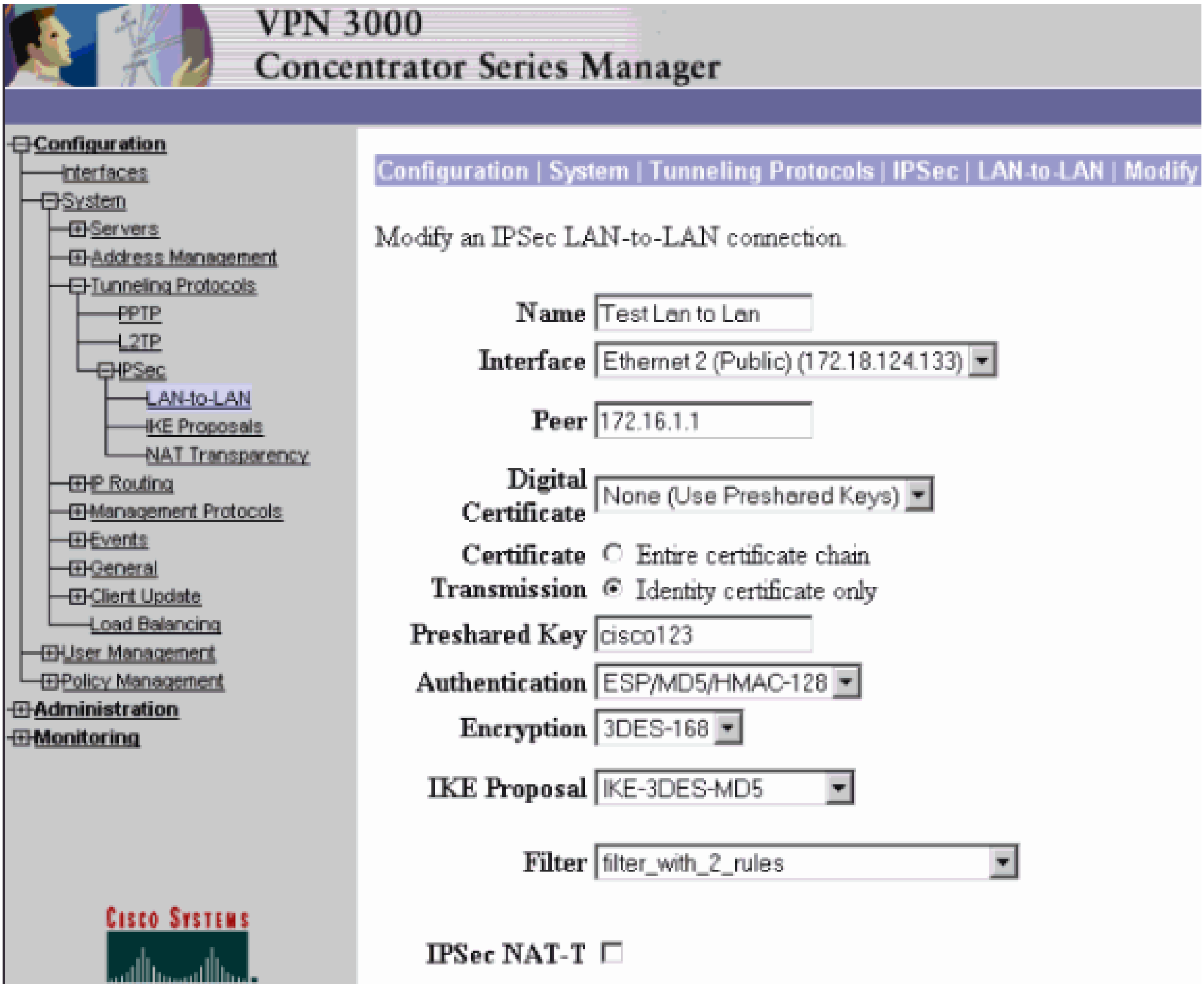
Configuration | User Management | Groups | Modify servergroup

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-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	filter_with_2_rules	☐	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
Secondary DNS		☐	Enter the IP address of the

LAN到LAN VPN隧道的过滤器

从VPN集中器代码3.6及以上版本，您能每个LAN对LAN IPSec VPN通道的过滤数据流。例如，如果构建LAN-to-LAN隧道到有地址的172.16.1.1另一个VPN集中器，和要允许主机对通道的10.1.1.2访问，当您否决其他流量时，您能应用**filter_with_2_rules，**当您选择**Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify**并且选择**filter_with_2_rules**在**过滤器**下时。



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

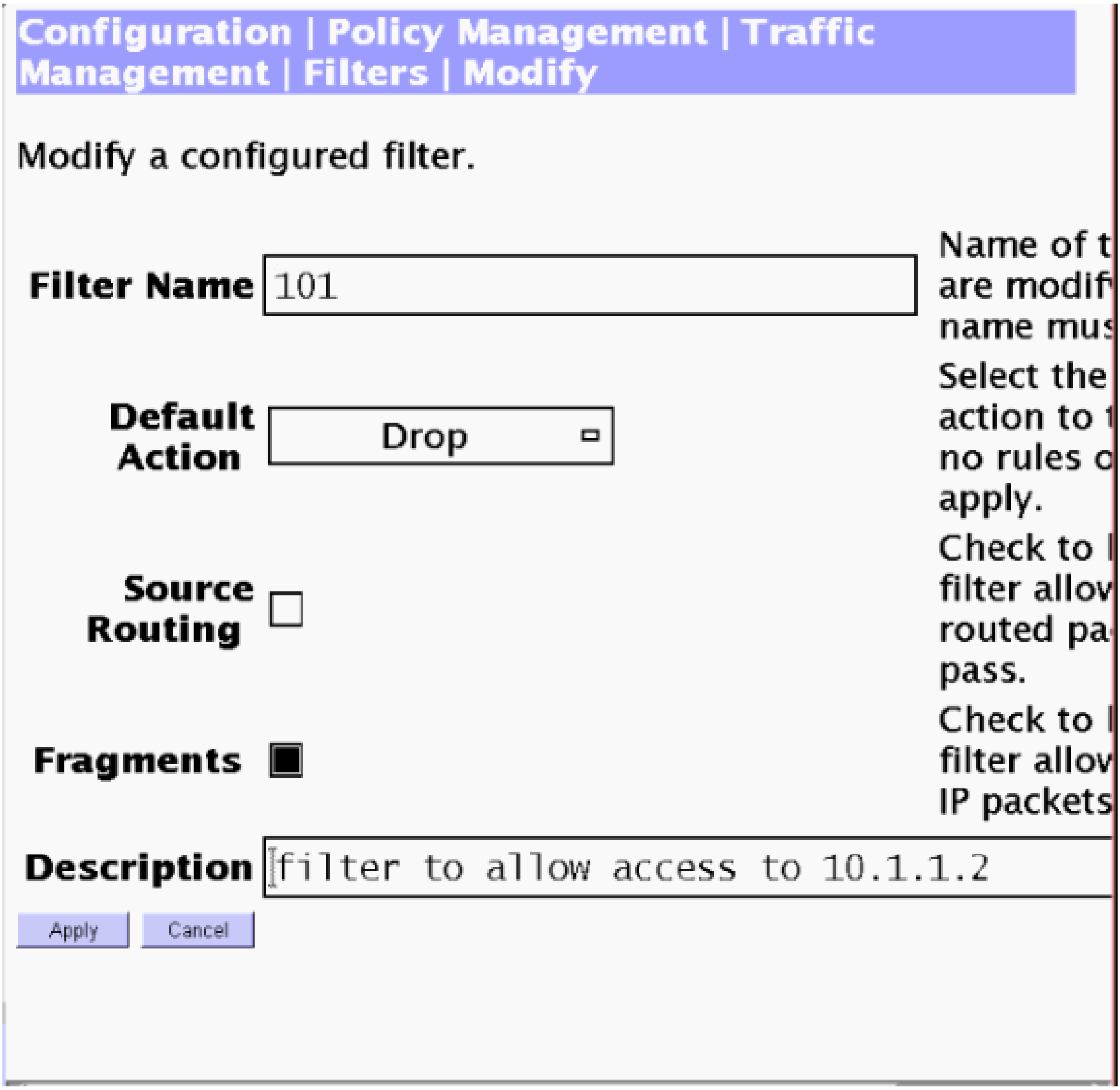
Modify an IPSec LAN-to-LAN connection.

Name	Test Lan to Lan
Interface	Ethernet 2 (Public) (172.18.124.133)
Peer	172.16.1.1
Digital Certificate	None (Use Preshared Keys)
Certificate Transmission	○ Entire certificate chain ● Identity certificate only
Preshared Key	cisco123
Authentication	ESP/MD5/HMAC-128
Encryption	3DES-168
IKE Proposal	IKE-3DES-MD5
Filter	filter_with_2_rules
IPSec NAT-T	□

VPN 3000 配置 - RADIUS 过滤器分配

定义在VPN集中器的一个过滤器也是可能的然后通过在从RADIUS服务器的过滤器编号下(用RADIUS术语，属性11是过滤器ID)，因此，当用户在RADIUS服务器验证，过滤器ID关联与该连接。在本例中，假定是VPN集中器用户的RADIUS验证已经是可操作的，并且仅过滤器ID将被添加。

定义在VPN集中器的过滤器正如在前一个示例：



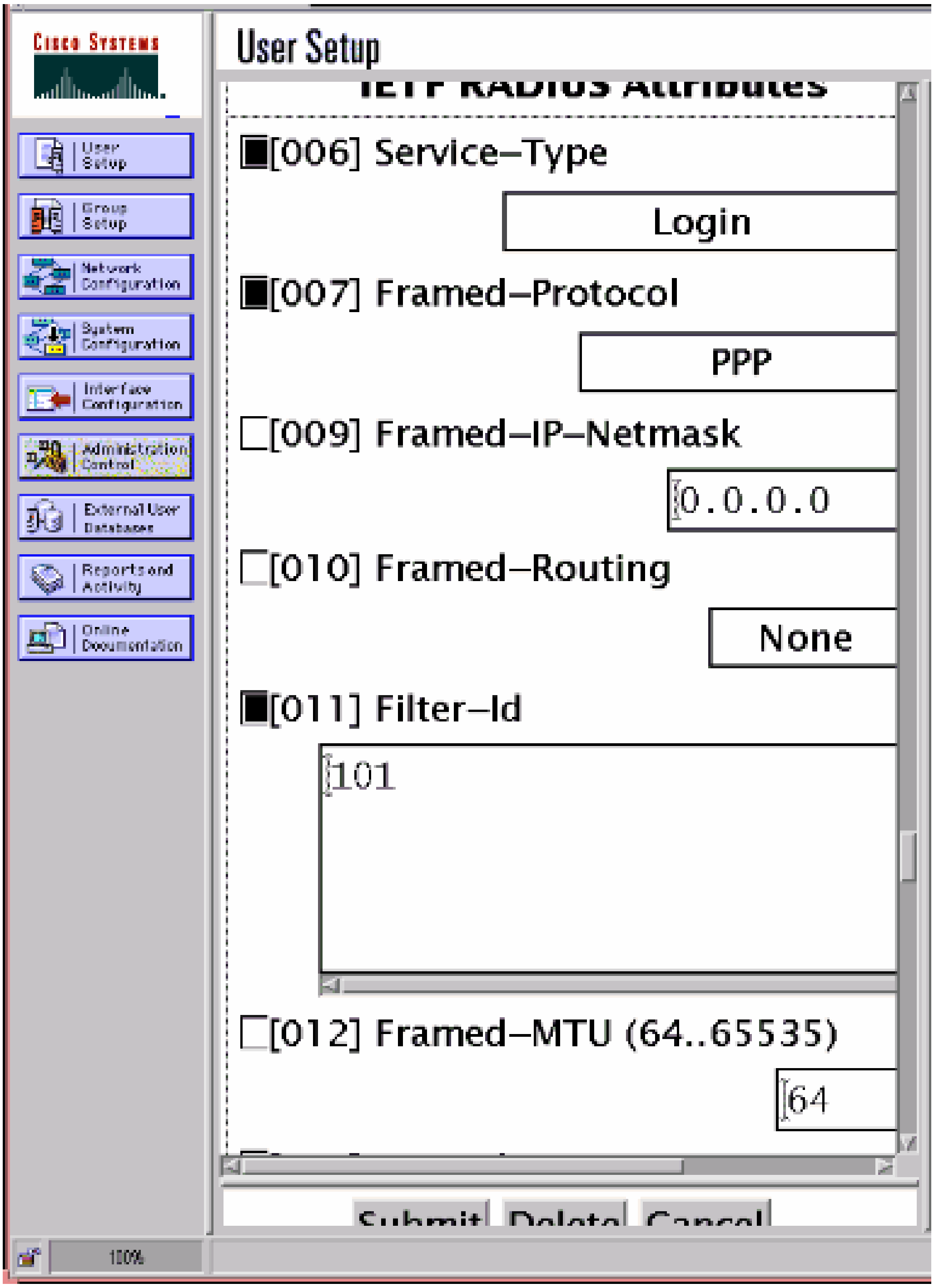
Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name	101	Name of t are modif name mus
Default Action	Drop	Select the action to t no rules o apply.
Source Routing	□	Check to l filter allov routed pa pass.
Fragments	■	Check to l filter allov IP packets
Description	filter to allow access to 10.1.1.2	

CSNT 服务器配置 - RADIUS 过滤器分配

配置属性11，在CiscoSecure NT服务器的过滤器ID是**101** ：



User Setup

IETF RADIUS Attributes

■[006] Service–Type

Login

■[007] Framed–Protocol

PPP

□[009] Framed–IP–Netmask

0.0.0.0

□[010] Framed–Routing

None

■[011] Filter–Id

101

□[012] Framed–MTU (64..65535)

64

调试 - RADIUS 过滤器分配

如果AUTHDECODE (1-13严重性)在VPN集中器，日志显示CiscoSecure NT服务器发送在access-list 101下在属性11 (0x0B) ：

```
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......
```

验证

当前没有可用于此配置的验证过程。

故障排除

为了实现故障排除目的，当您选择**Configuration > System > Events > Classes**并且添加**FILTERDBG**类以**严重性记录= 13时，**只，您能打开过滤器调试。在规则，请更改从转发(或丢弃的)默认操作**转发和记录**(或丢弃和日志)。当事件日志被检索在**Monitoring > Event Log时**，应该显示条目例如：

```
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
```

相关信息

- IPsec 协商/IKE 协议
- VPN 3000集中器常见问题
- RADIUS支持
- Cisco VPN 3000 集中器支持
- Cisco VPN 3000客户端支持
- 适用于 Windows 的 Cisco Secure ACS 支持
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems