配置Cisco VPN 3000集中器以使用过滤器和RADIUS过滤器分配进行阻止

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

在此示例配置中，我们希望使用过滤器允许用户仅访问网络内部的一台服务器(10.1.1.2)并阻止对所有其他资源的访问。Cisco VPN 3000集中器可设置为通过过滤器控制IPsec、点对点隧道协议(PPTP)和L2TP客户端对网络资源的访问。过滤器由规则组成，与路由器上的访问列表类似。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集中器的等效功能是设置包含规则的过滤器。

我们的第一个VPN集中器规则是permit_server_rule，这相当于路由器的permit ip any host 10.1.1.2命令。我们的第二个VPN集中器规则是deny_server_rule，它等效于路由器的deny ip any any命令。

我们的VPN集中器过滤器为filter_with_2_rules，等同于路由器的101访问列表；它使用permit_server_rule和deny_server_rule（按该顺序）。 假设客户端在添加过滤器之前可以正确连接；它们从VPN集中器上的池接收其IP地址。

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用户的网络访问，以了解有关PIX/ASA 7.x阻止来自VPN用户的访问的方案的详细信息。

先决条件

要求

本文档没有任何特定的要求。

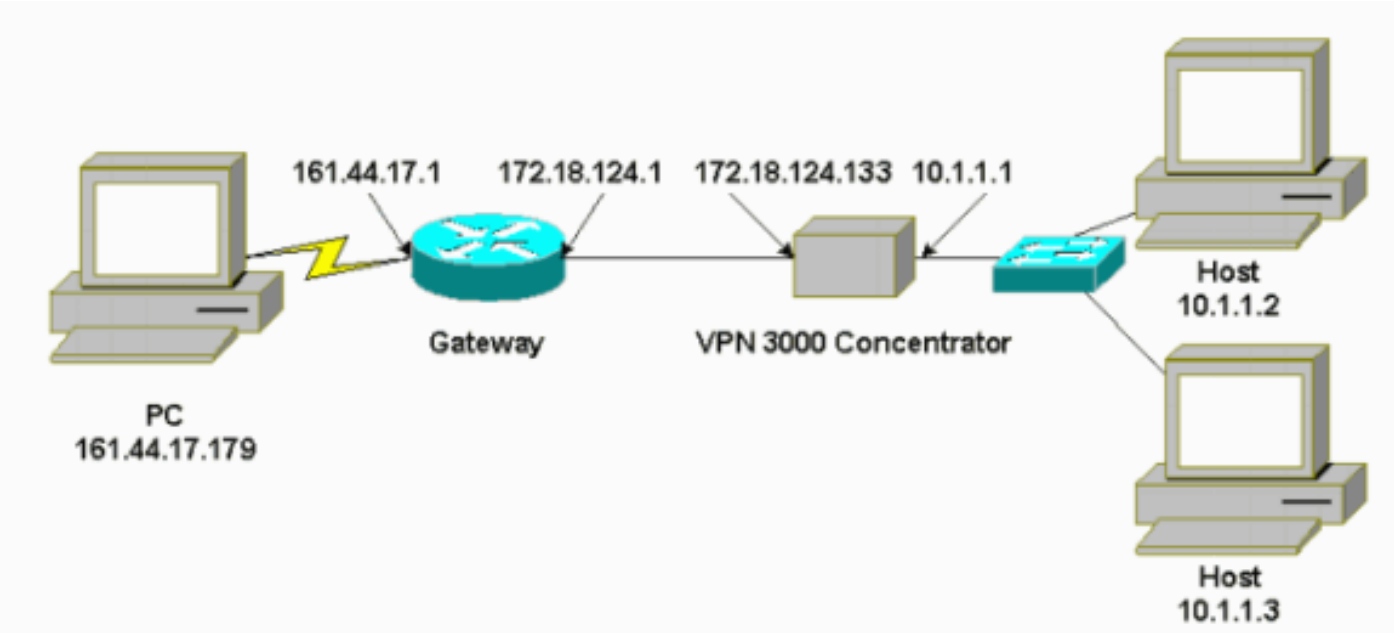
使用的组件

本文档中的信息基于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：



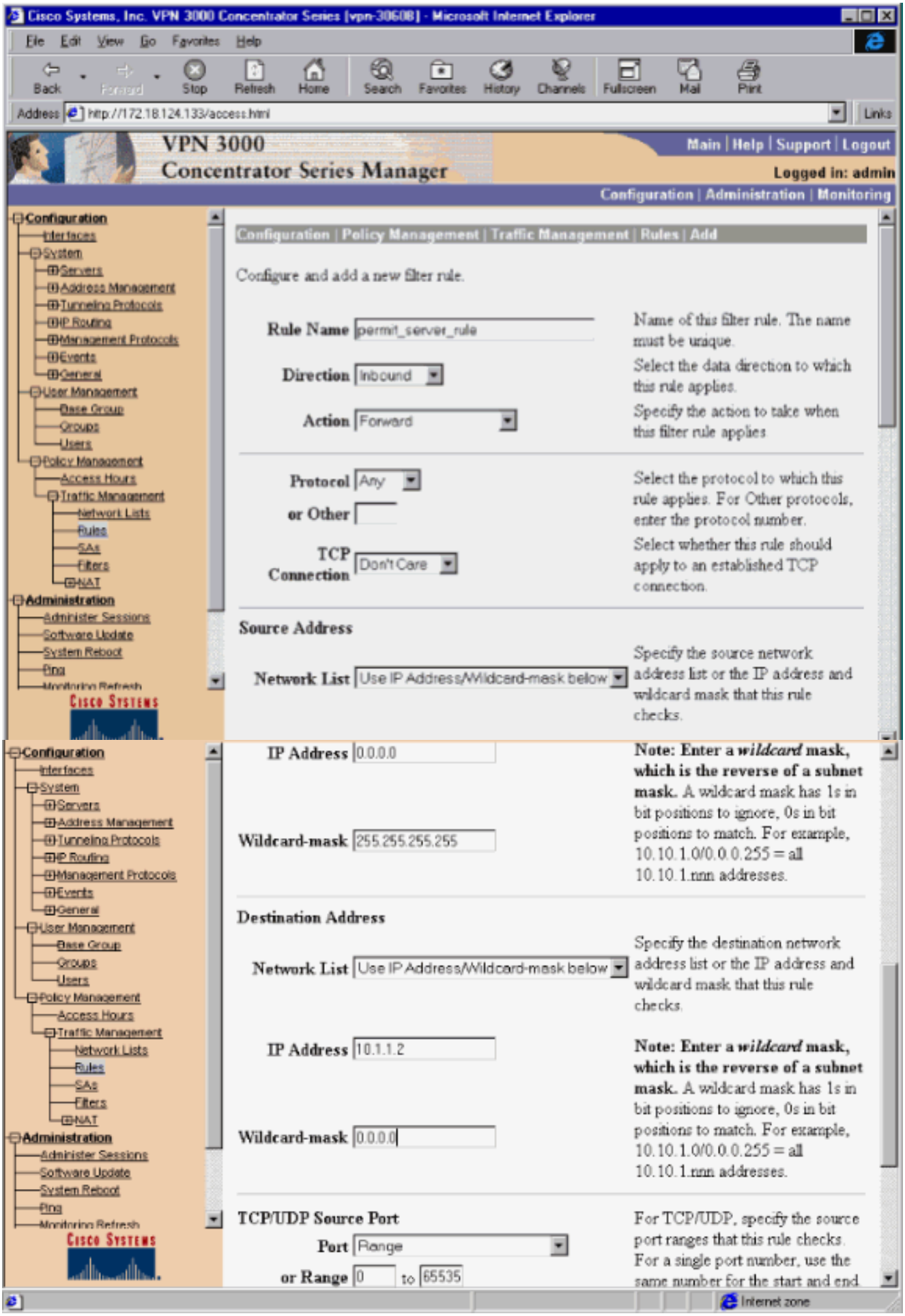
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

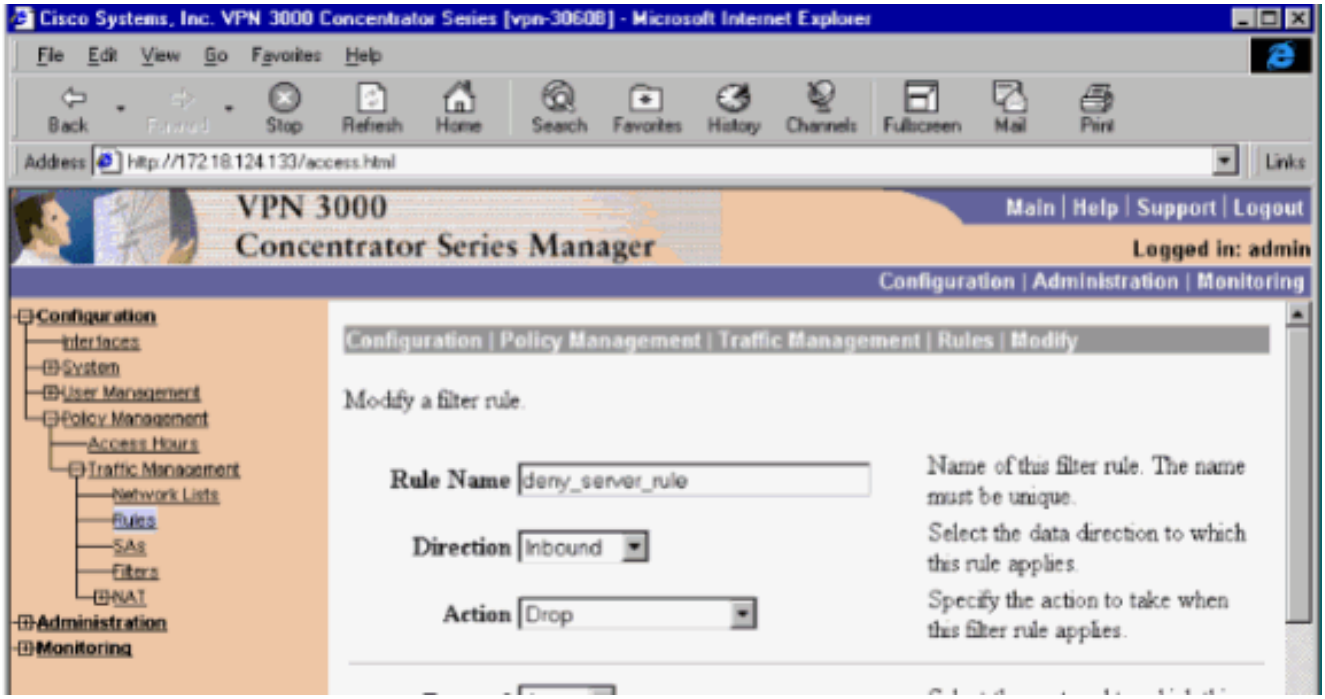
VPN 3000 配置

完成这些步骤为了配置VPN 3000集中器。

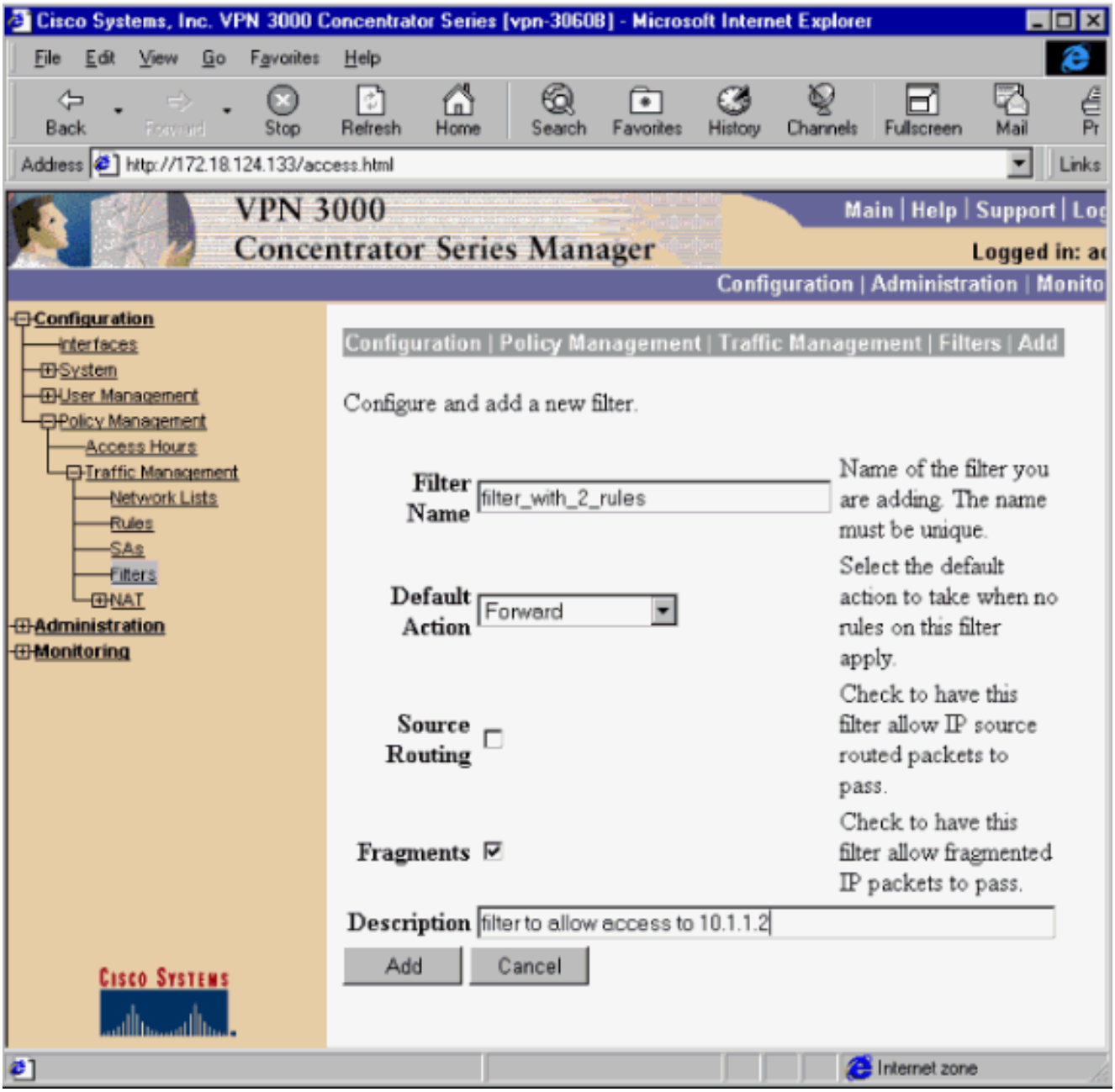
1. 选择**Configuration >Policy Management > Traffic Management > Rules > Add**，并使用以下设置定义名**为permit_server_rule的**第一个VPN集中器规则：方向 — 入**站**操作(Action)-**转发**源地址**(Source Address)- 255.255.255.255**目标地址 - 10.1.1.2通配符掩**码 — 0.0.0.0**



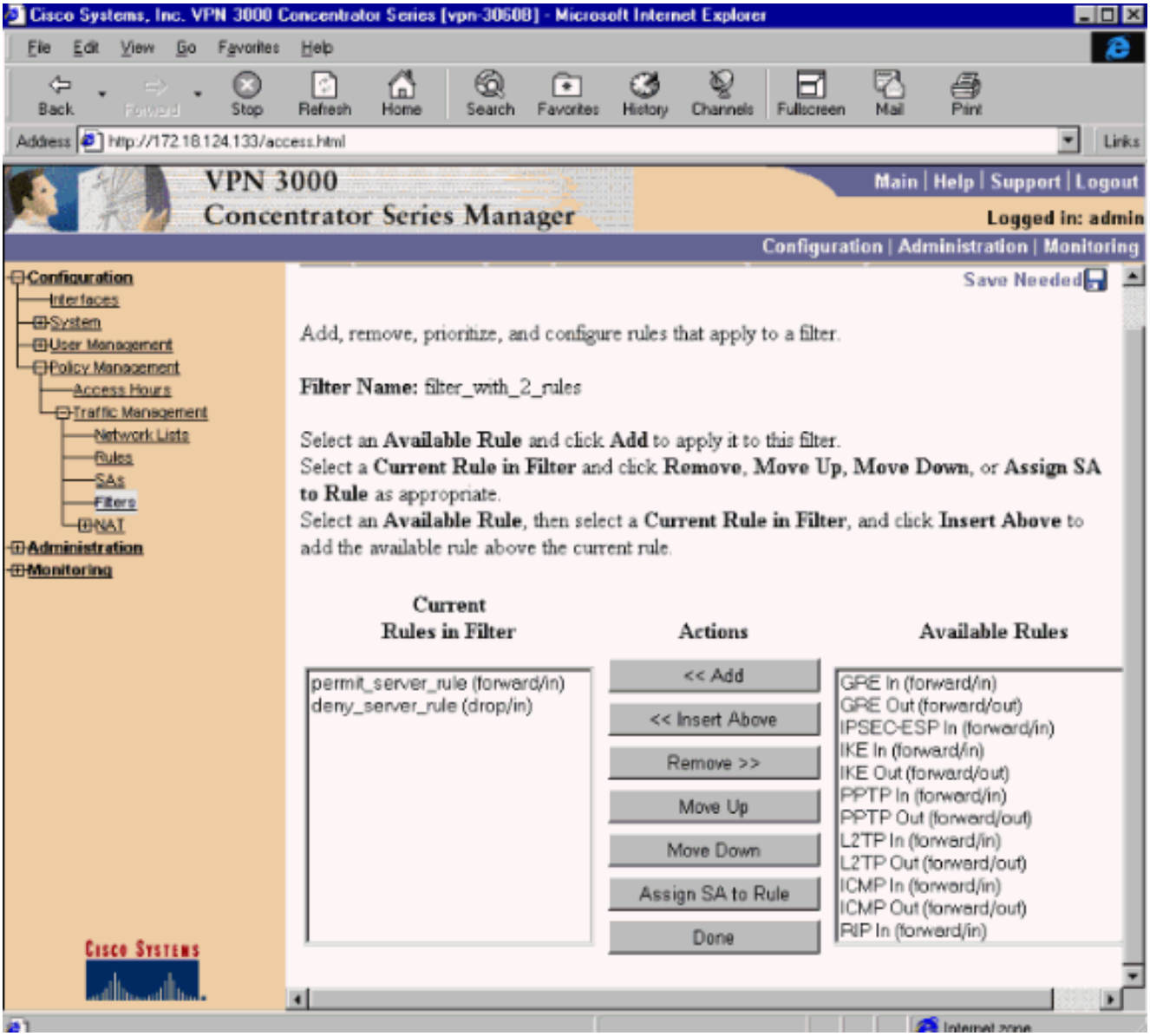
2. 在同一区域中，使用以下默认值定义名为deny_server_rule的第二个VPN集中器规则：方向 — 入站操作 — 删除任何地址(255.255.255.255)的源地址和目的地址
：



3. 选择Configuration > Policy Management > Traffic Management > Filters，然后添加filter_with_2_rules过滤器。



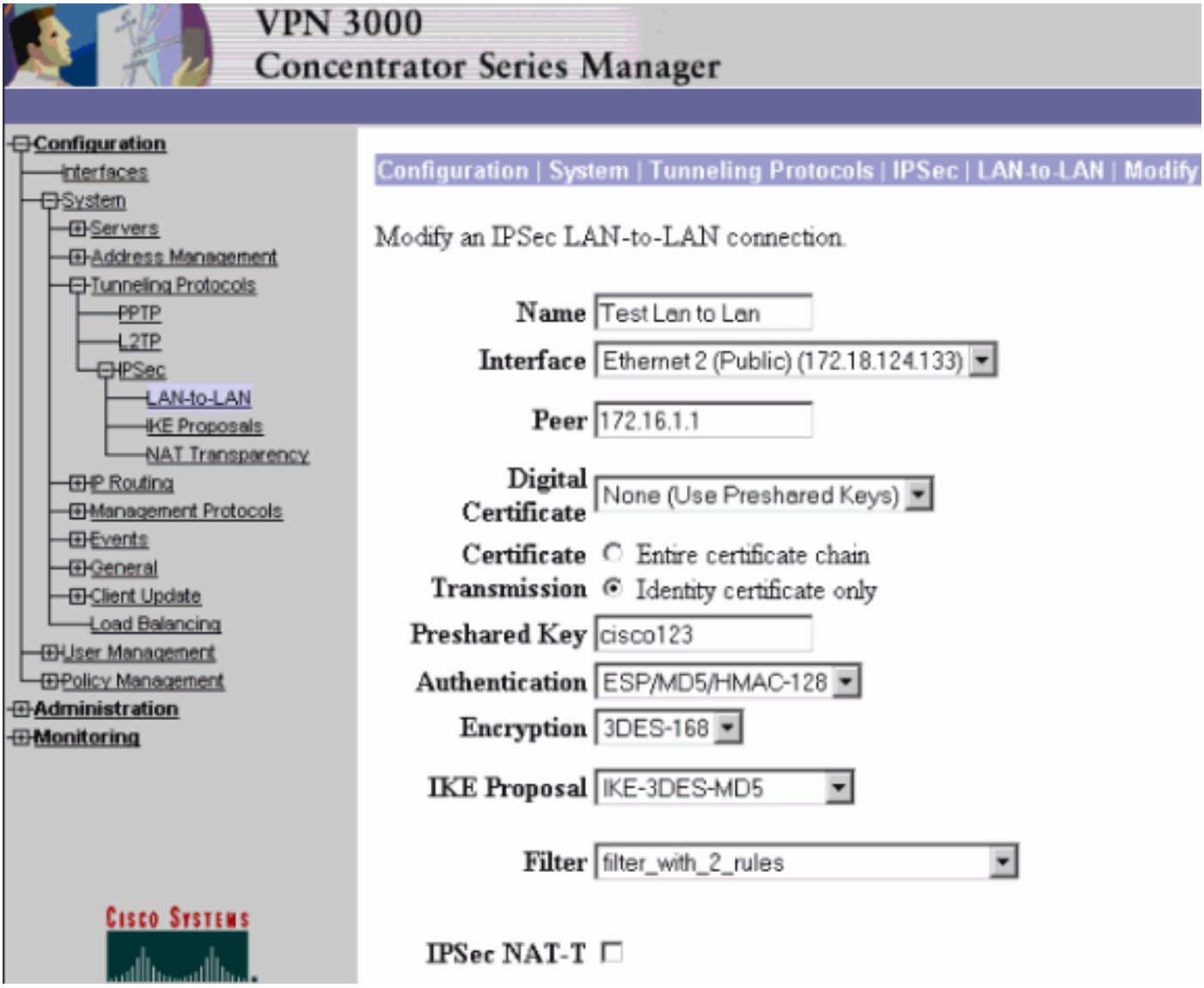
4. 将两个规则添加到 filter_with_2_rules:



5. 选择Configuration > User Management > Groups，并将过滤器应用到组：

LAN到LAN VPN隧道的过滤器

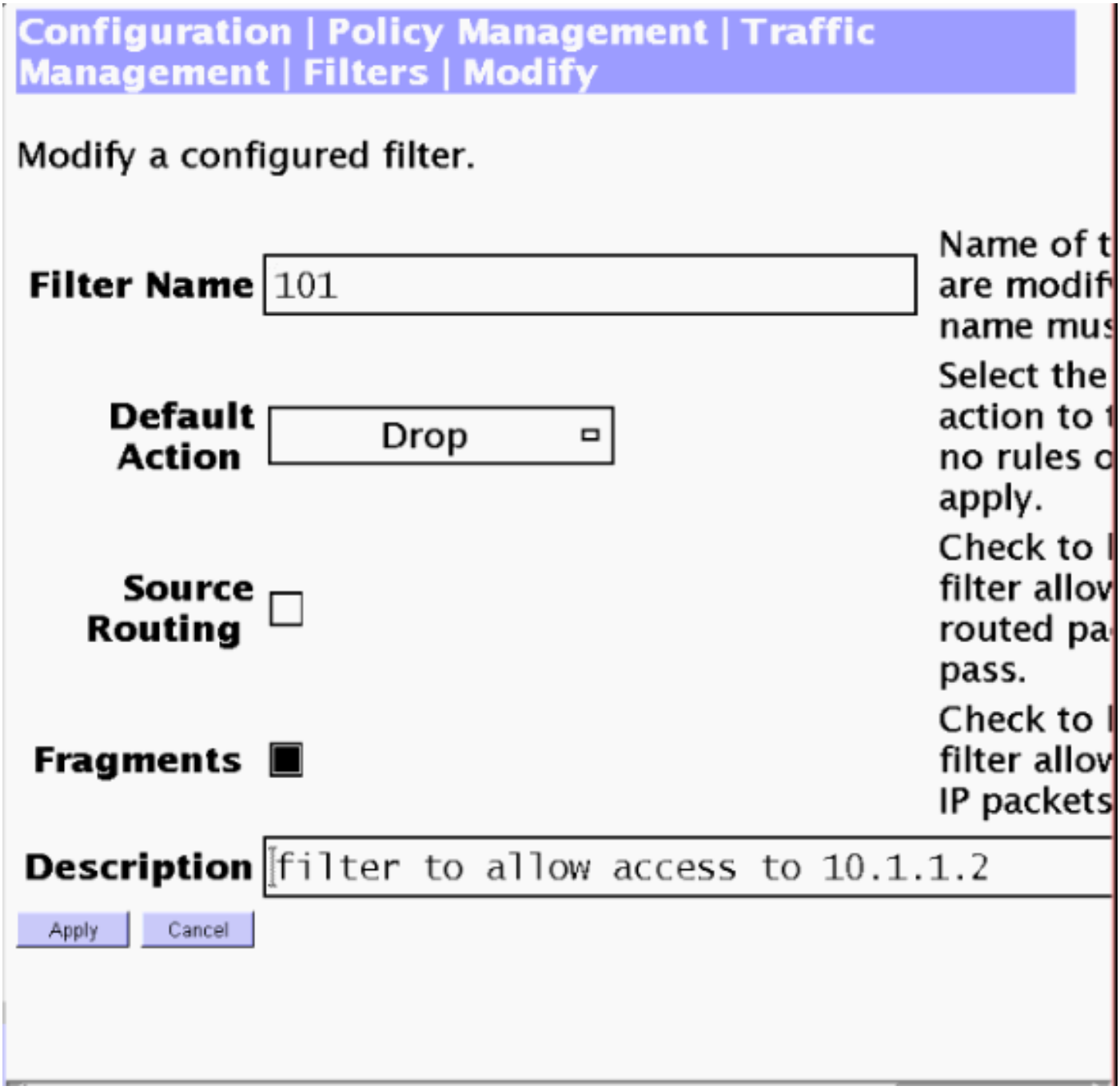
从VPN集中器代码3.6及更高版本，您可以过滤每个LAN到LAN IPsec VPN隧道的流量。例如，如果构建到地址为172.16.1.1的另一个VPN集中器的LAN到LAN隧道，并且希望允许主机10.1.1.2访问该隧道，同时拒绝所有其他流量，则可以在选择**Configuration > System > Tunneling Protocols > VPN协议**时应用**filter_with_2_rulesips ec > LAN-to-LAN > Modify**，并在**Filter**下选择**filter_with_2_rules**。



VPN 3000 配置 - RADIUS 过滤器分配

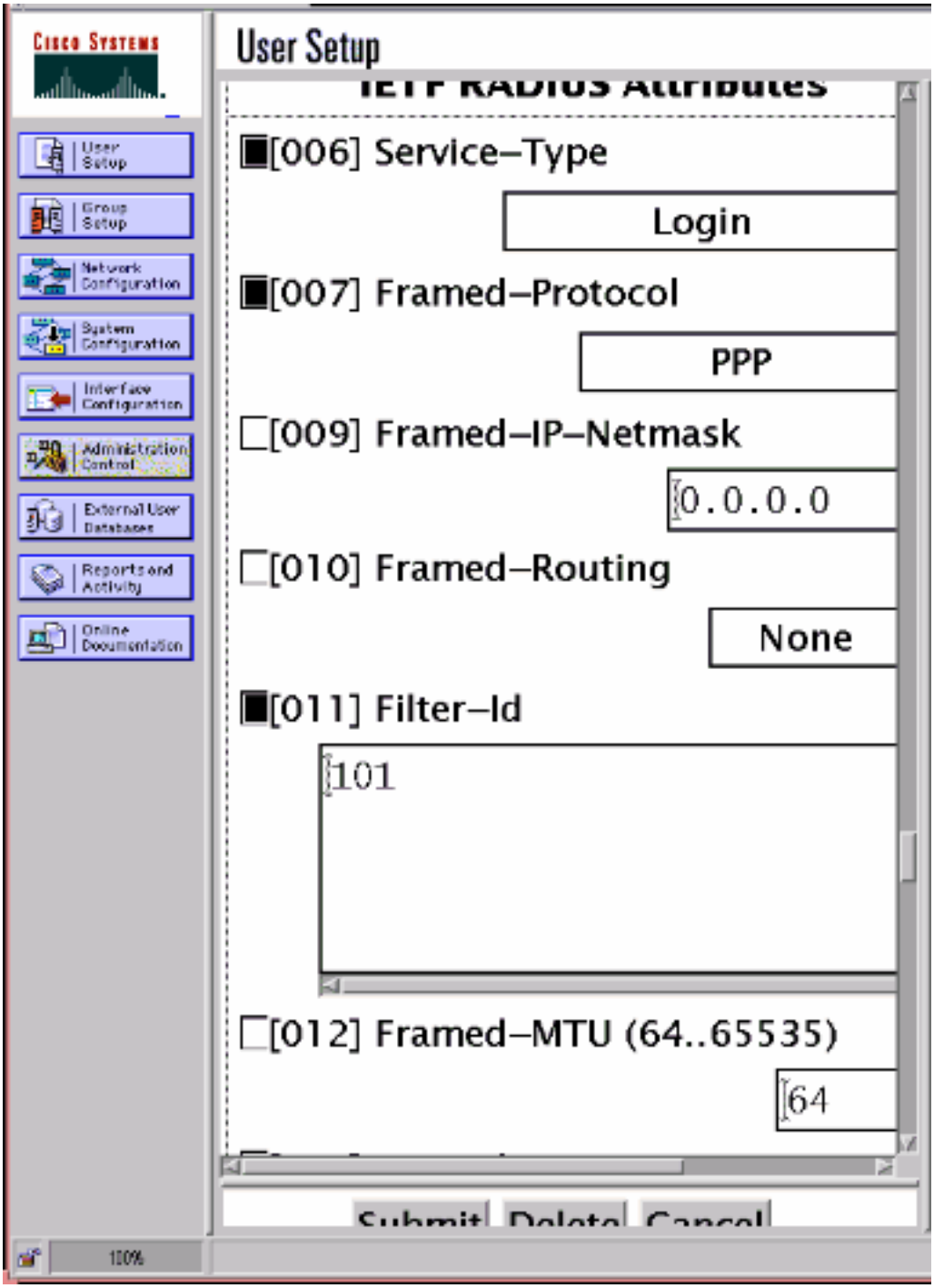
也可以在VPN集中器中定义过滤器，然后从RADIUS服务器传递过滤器编号（在RADIUS术语中，属性11是过滤器ID），以便当用户在RADIUS服务器上进行身份验证时，过滤器ID与该连接相关联。在本例中，假设VPN集中器用户的RADIUS身份验证已运行，并且仅要添加过滤器ID。

在VPN集中器上定义过滤器，如上例所示：



CSNT 服务器配置 - RADIUS 过滤器分配

将Cisco Secure NT服务器上的属性11, Filter-id配置为**101**:



调试 - RADIUS 过滤器分配

如果VPN集中器中启用了AUTHDECODE（1-13严重性），则日志显示Cisco Secure NT服务器在属性11(0x0B)中向下发送访问列表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......
```

验证

当前没有可用于此配置的验证过程。

故障排除

仅用于故障排除目的，当选择**Configuration > System > Events > Classes**并添加**Severity to Log = 13**的**FILTERDBG**类时，可以启用过滤器调试。在规则中，将Default操作从Forward（或Drop）更改为**Forward and Log**（或Drop and Log）。 在“监控”(Monitoring)>“事件日志”(**Event Log)中检索事件日**志时，它应显示以下条目：

```
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