Configurando o Concentrador Cisco VPN 3000 para bloqueio com filtros e atribuição de filtro RADIUS

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Diagrama de Rede
Conventions
Configuração do VPN 3000
Filtros para um túnel VPN LAN a LAN
Configuração do VPN 3000 - atribuição de filtro RADIUS
Configuração do Servidor CSNT – Atribuição de Filtros RADIUS
Depuração - Atribuição de Filtro RADIUS
Verificar
Troubleshoot
Informações Relacionadas

Introduction

Nesta configuração de exemplo, queremos usar filtros para permitir que um usuário acesse apenas um servidor (10.1.1.2) dentro da rede e bloquear o acesso a todos os outros recursos. O Cisco VPN 3000 Concentrator pode ser configurado para controlar o IPsec, o Point-to-Point Tunneling Protocol (PPTP) e o acesso do cliente L2TP aos recursos de rede com filtros. Os filtros consistem em regras, que são semelhantes às listas de acesso em um roteador. Se um roteador foi configurado para:

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

o equivalente do VPN Concentrator seria configurar um filtro com regras.

Nossa primeira regra do VPN Concentrator é **permit_server_rule**, que é equivalente ao comando **permit ip any host 10.1.1.2** do roteador. Nossa segunda regra do VPN Concentrator é **deny_server_rule**, que é equivalente ao comando do roteador **deny ip any any**.

Nosso filtro do VPN Concentrator é **filter_with_2_rules**, que é equivalente à lista de acesso 101 do roteador; ele usa **permit_server_rule** e **deny_server_rule** (nessa ordem). Pressupõe-se que os clientes podem se conectar corretamente antes de adicionar filtros; eles recebem seus endereços IP de um pool no VPN Concentrator.

Consulte PIX/ASA 7.x ASDM: Restrinja o acesso à rede de usuários de VPN de acesso remoto para saber mais sobre o cenário em que o PIX/ASA 7.x bloqueia o acesso dos usuários de VPN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

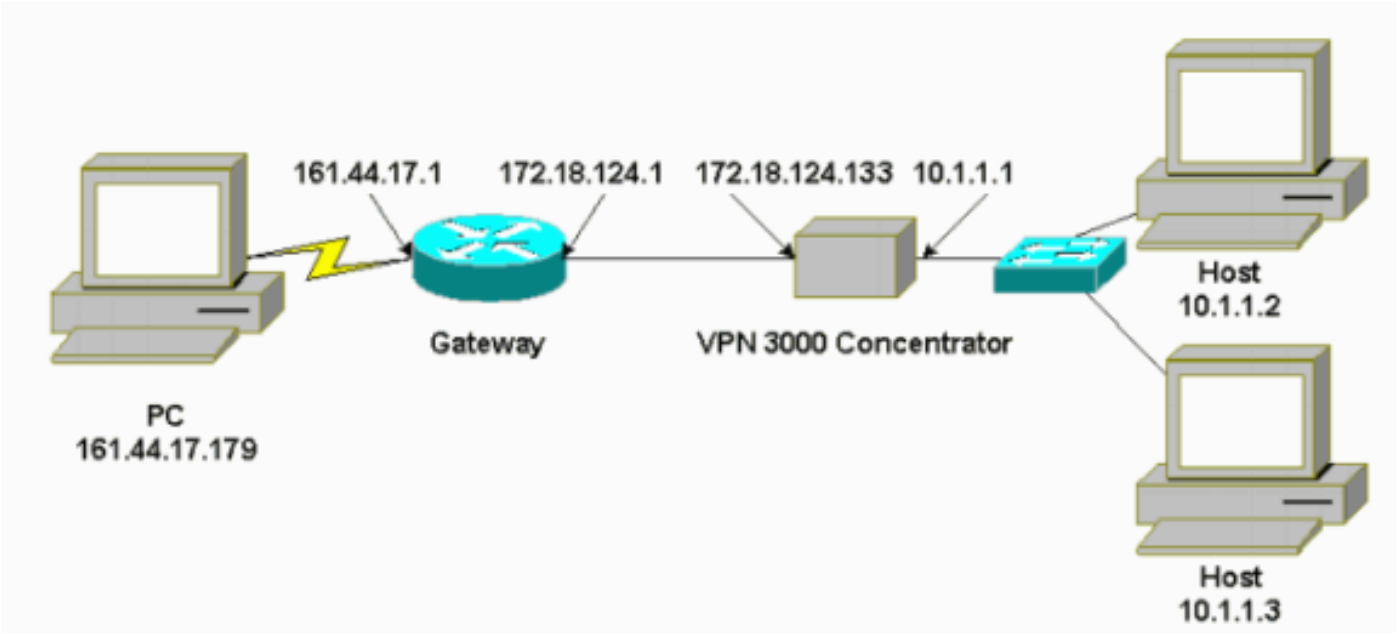
Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN 3000 Concentrator versão 2.5.2.D.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

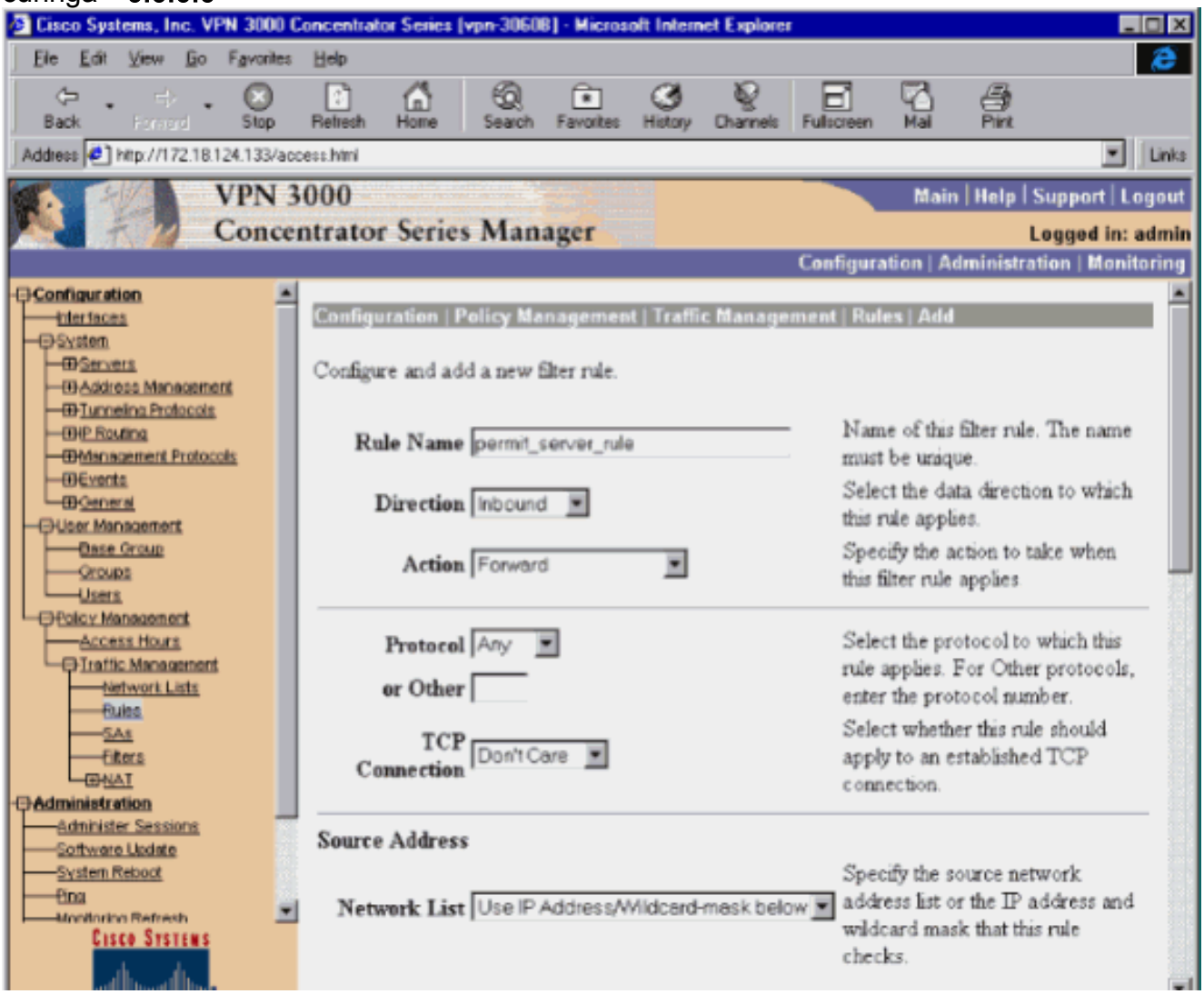
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

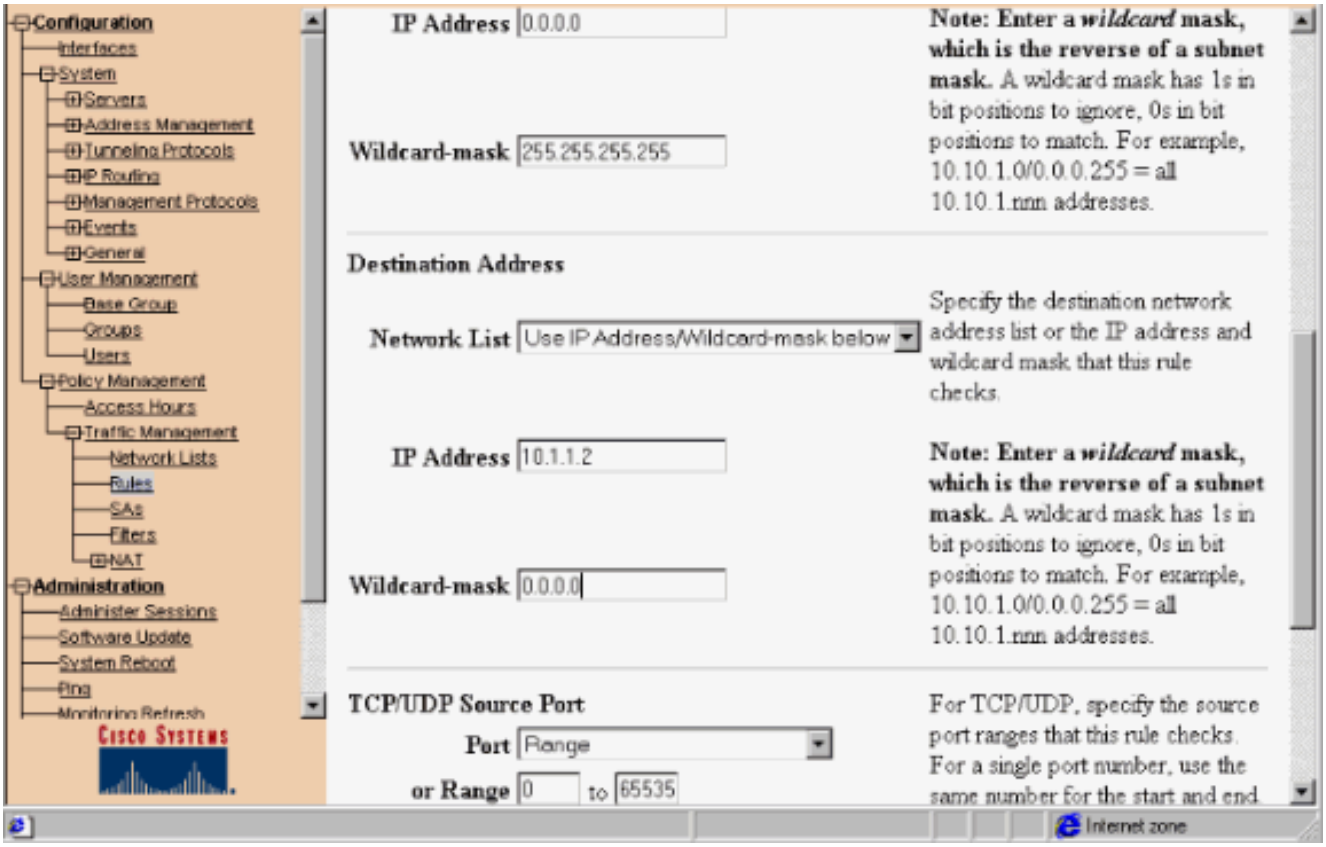
Configuração do VPN 3000

Conclua estes passos para configurar o VPN 3000 Concentrator.

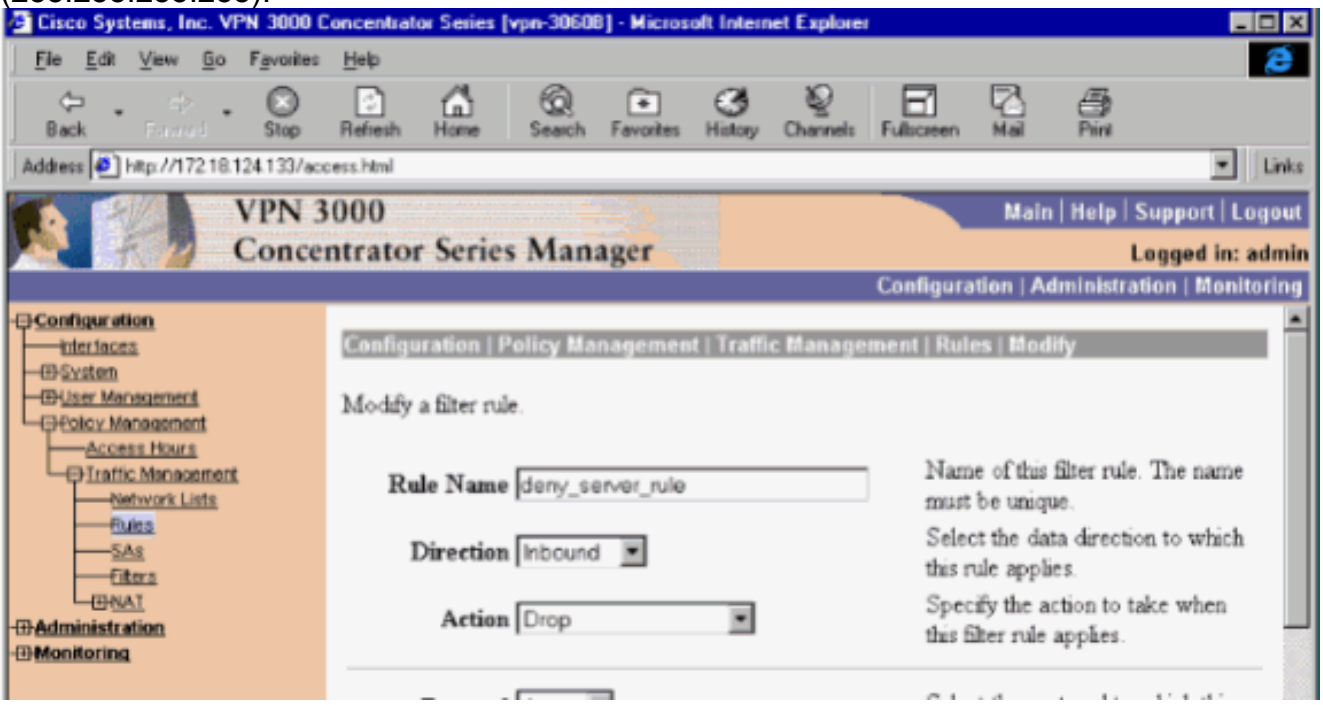
1. Escolha **Configuration > Policy Management > Traffic Management > Rules > Add** e defina a primeira regra do VPN Concentrator chamada **permit_server_rule** com estas

configurações:Direção—**Entrada**Ação—**Encaminhar**Endereço de origem—**255.255.255.255**Endereço de destino—**10.1.1.2**Máscara curinga—**0.0.0.0**

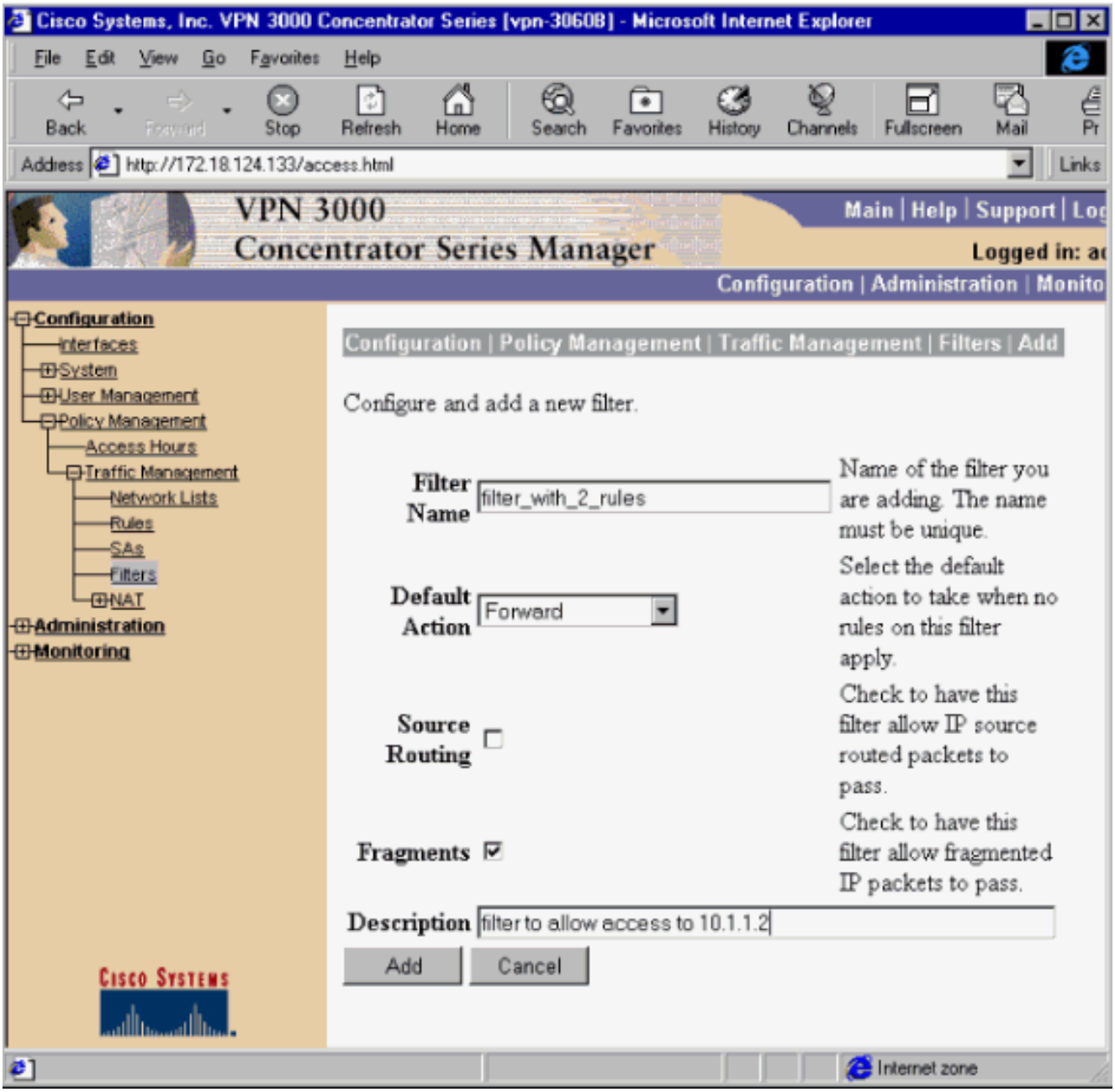




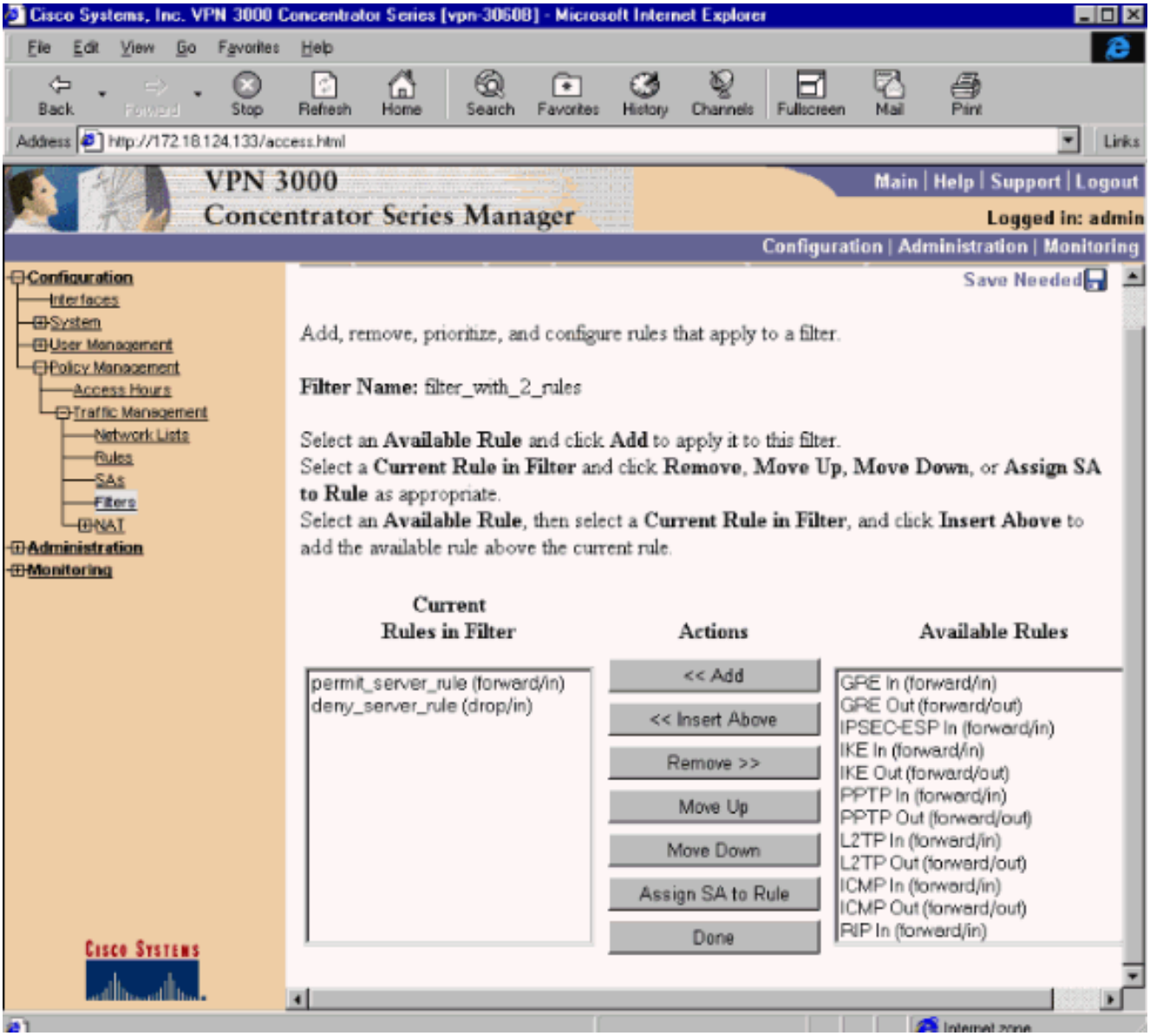
2. Na mesma área, defina a segunda regra do VPN Concentrator chamada **deny_server_rule** com estes padrões:Direção—**Entrada**Ação—**Descartar**Endereços origem e destino de qualquer coisa (255.255.255.255):



3. Escolha **Configuration > Policy Management > Traffic Management > Filters** e adicione seu filtro **filter_with_2_rules**.



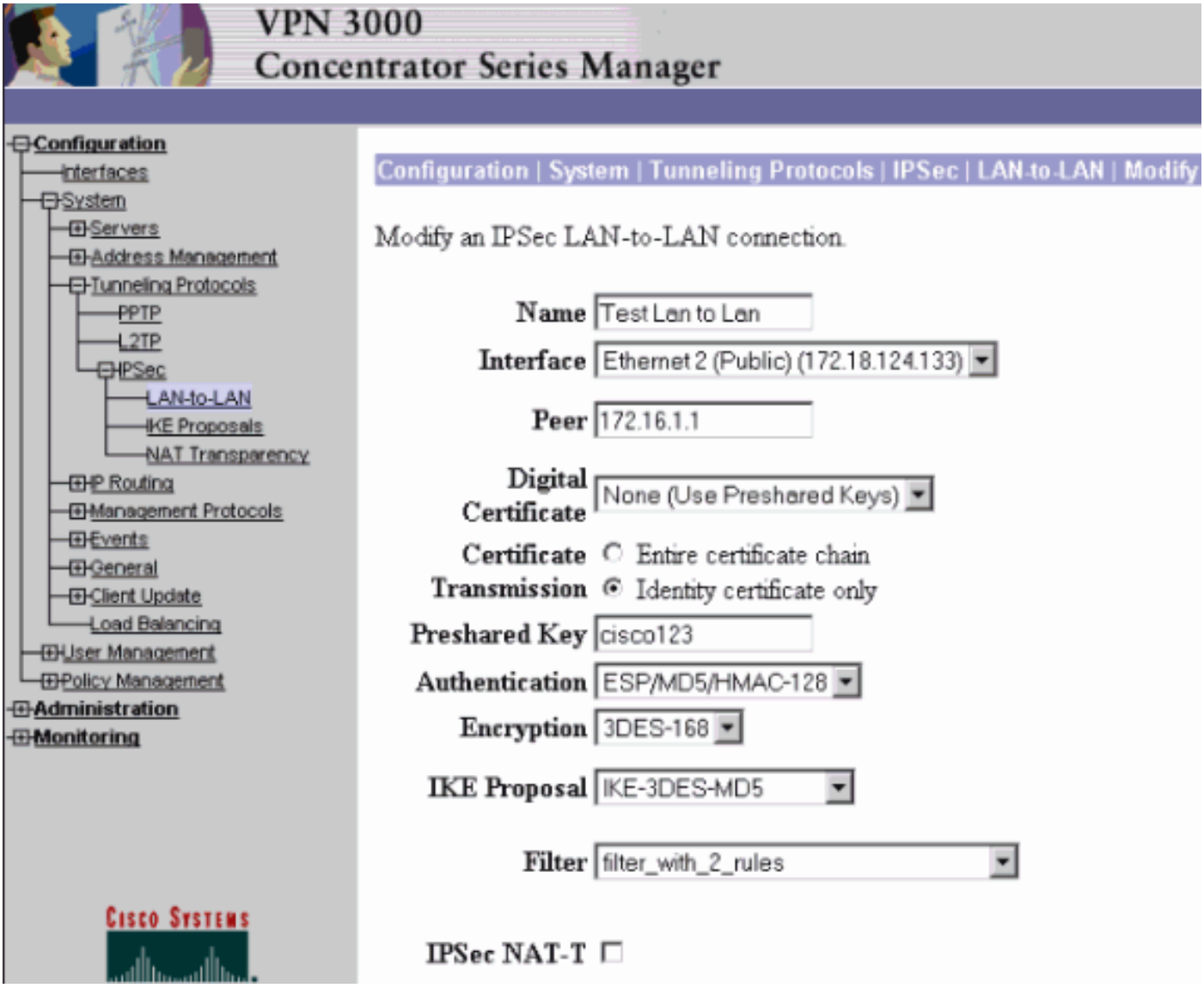
4. Adicione as duas regras para filter_with_2_rules:



5. Escolha **Configuration > User Management > Groups** e aplique o filtro ao grupo:

Filtros para um túnel VPN LAN a LAN

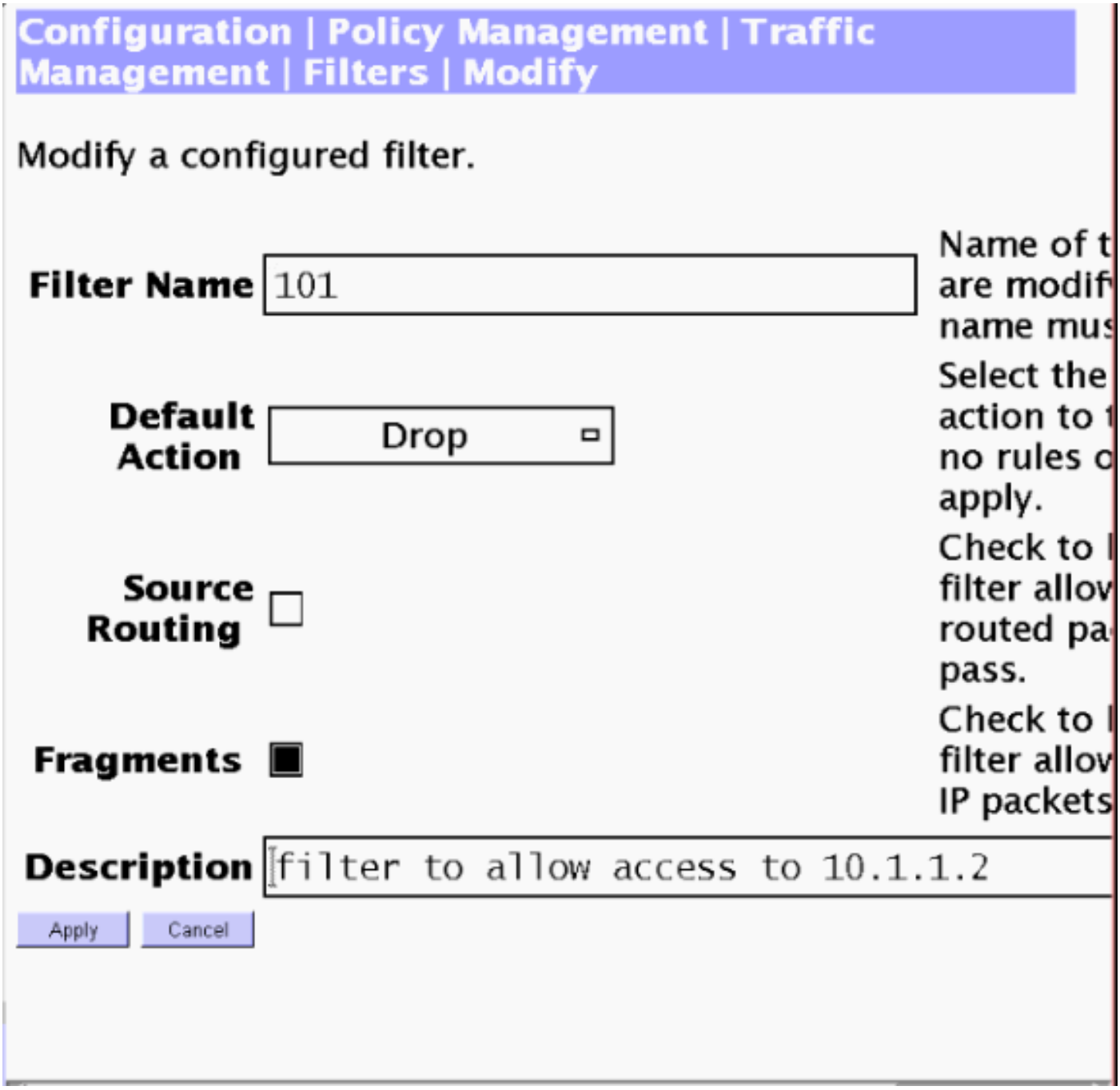
A partir do código do VPN Concentrator 3.6 e posterior, você pode filtrar o tráfego para cada túnel VPN IPsec LAN a LAN. Por exemplo, se você criar um túnel LAN a LAN para outro VPN Concentrator com o endereço 172.16.1.1 e quiser permitir o acesso do host 10.1.1.2 ao túnel enquanto nega todo o tráfego restante, você pode aplicar **filter_with_2_rules** ao escolher **Configuration > System > Tunneling Protocols > IPSec > LAN a LAN > Modifique** e selecione **filter_with_2_rules** em **Filtro**.



Configuração do VPN 3000 - atribuição de filtro RADIUS

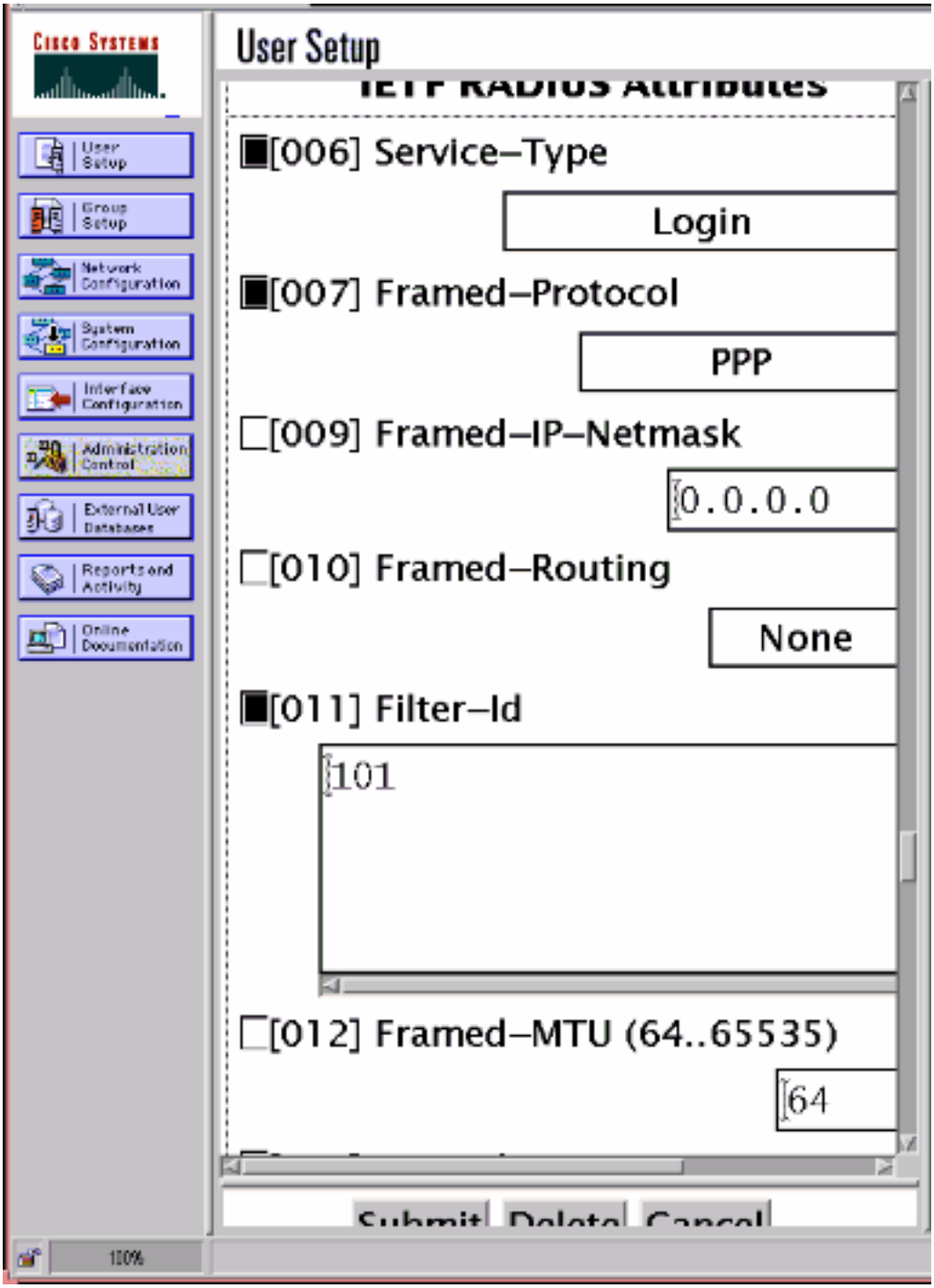
Também é possível definir um filtro no VPN Concentrator e, em seguida, passar o número do filtro de um servidor RADIUS (em termos de RADIUS, o atributo 11 é Filter-id), de modo que quando o usuário é autenticado no servidor RADIUS, o Filter-id é associado a essa conexão. Neste exemplo, presume-se que a autenticação RADIUS para usuários do VPN Concentrator já está operacional e apenas o Filter-id deve ser adicionado.

Defina o filtro no VPN Concentrator como no exemplo anterior:



Configuração do Servidor CSNT – Atribuição de Filtros RADIUS

Configure o atributo 11, Filter-id no servidor Cisco Secure NT para ser **101**:



Depuração - Atribuição de Filtro RADIUS

Se AUTHDECODE (1-13 Severity) estiver ativado no VPN Concentrator, o registro mostra que o servidor Cisco Secure NT envia uma lista de acesso 101 no atributo 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......
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Somente para fins de solução de problemas, você pode ativar a depuração de filtro ao escolher **Configuration > System > Events > Classes** e adicionar a classe **FILTERDBG** com **Severity to Log = 13**. Nas regras, altere a ação padrão de Encaminhar (ou Descartar) para **Encaminhar e Registrar** (ou Descartar e Registrar). Quando o registro de eventos é recuperado em **Monitoring > Event Log**, ele deve mostrar entradas como:

```
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
```

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Perguntas frequentes sobre o VPN 3000 Concentrator
- Suporte RADIUS
- Suporte ao Cisco VPN 3000 Concentrator
- Suporte ao cliente Cisco VPN 3000
- Suporte Cisco Secure ACS para Windows
- Solicitação de comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems