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

Índice

Introdução

Nesta configuração de exemplo, nós queremos usar filtros para permitir que um usuário alcance somente um server (10.1.1.2) dentro da rede e obstrua o acesso a todos recursos restantes. O Cisco VPN 3000 Concentrator pode estabelecer-se 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 nas regras, que são similares 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 concentrador VPN seria estabelecer um filtro com regras.

Nossa primeira regra do concentrador VPN é o **permit_server_rule**, que é equivalente à **licença IP do** roteador **todo o** comando de **10.1.1.2 do host**. Nossa segunda regra do concentrador VPN é o **deny_server_rule** que é equivalente ao **comando deny ip any any do** roteador.

Nosso filtro do concentrador VPN é **filter_with_2_rules**, que é equivalente à lista de acessos do roteador 101; usa o **permit_server_rule** e o **deny_server_rule** (nessa ordem). Supõe-se que os clientes podem conectar corretamente antes de adicionar filtros; recebem seus endereços IP de Um ou Mais Servidores Cisco ICM NT de um pool no concentrador VPN.

Refira PIX/ASA 7.x ASDM: Restrinja o acesso de rede de usuários do acesso remoto VPN a fim aprender mais sobre a encenação onde o bloco PIX/ASA 7.x o acesso dos usuários VPN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

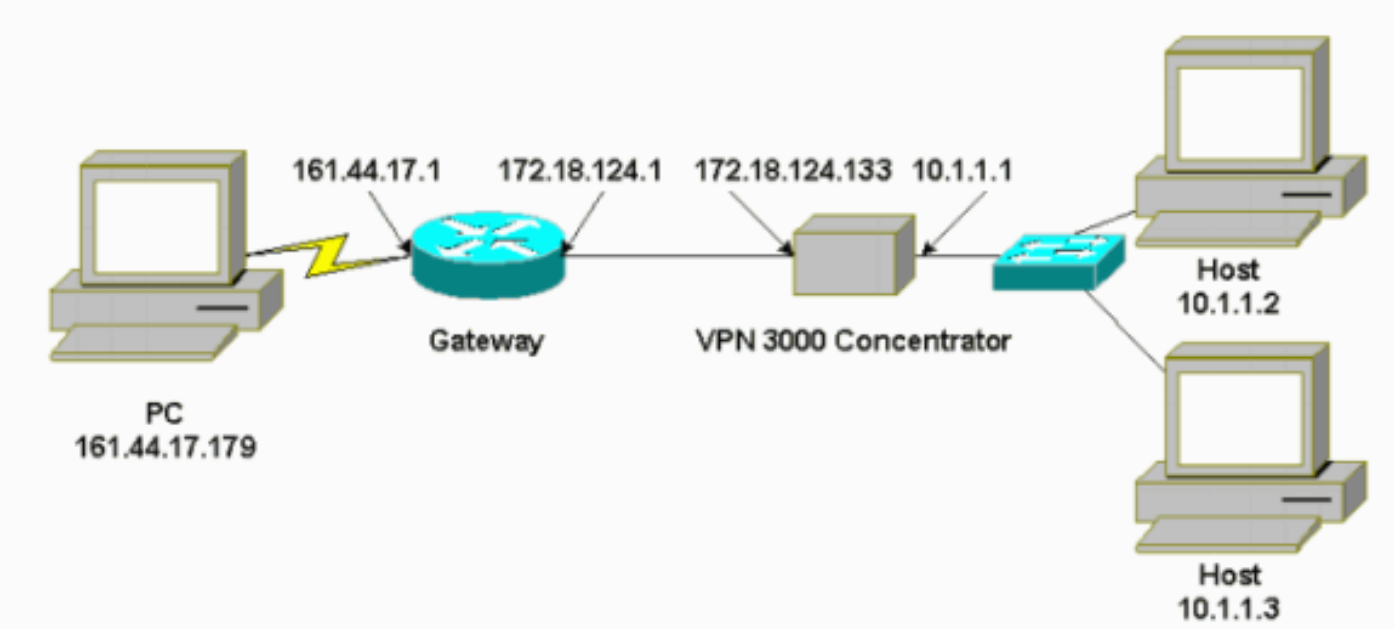
Componentes Utilizados

A informação neste documento é baseada na versão 2.5.2.D do Cisco VPN 3000 Concentrator.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Convenções

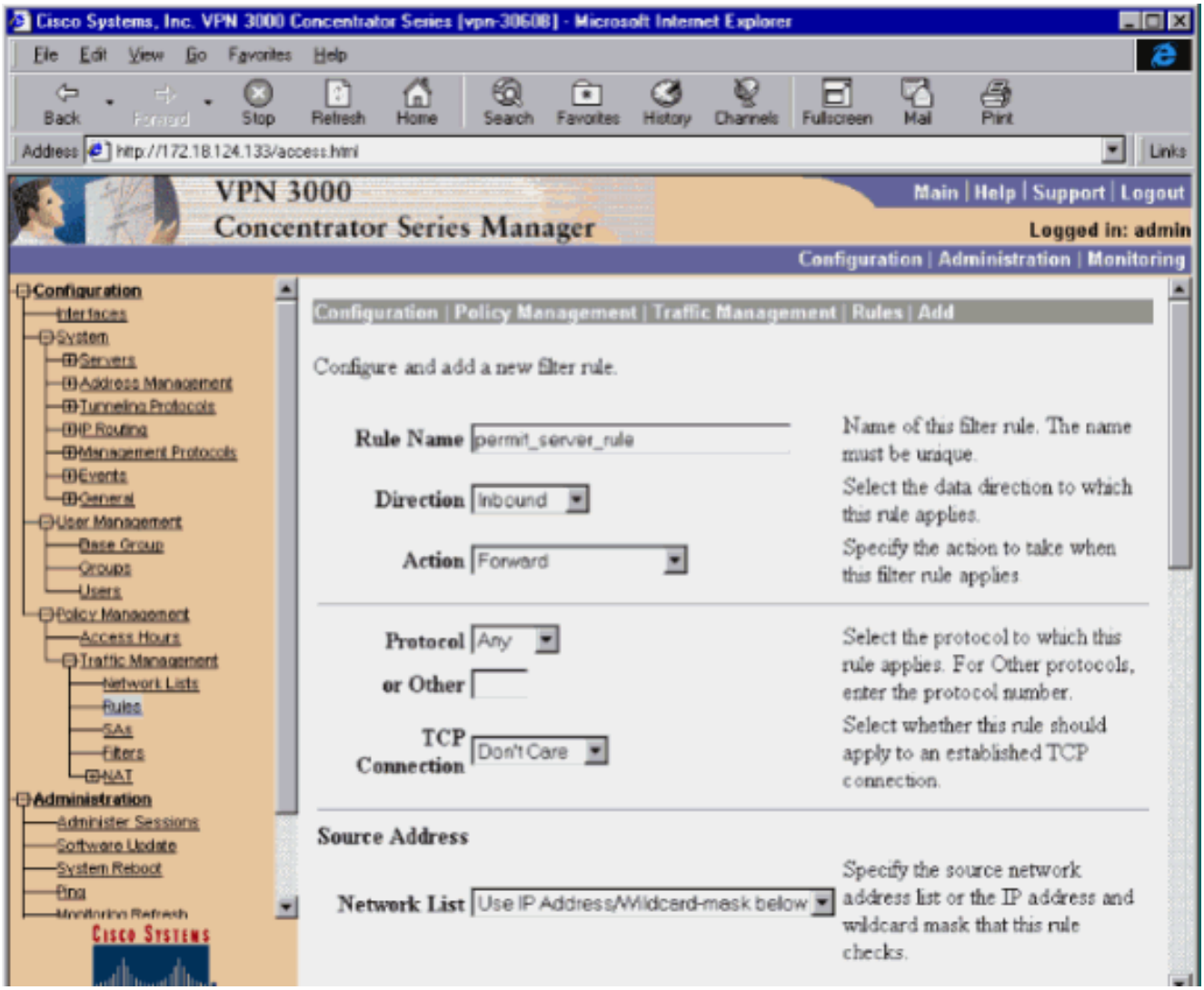
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

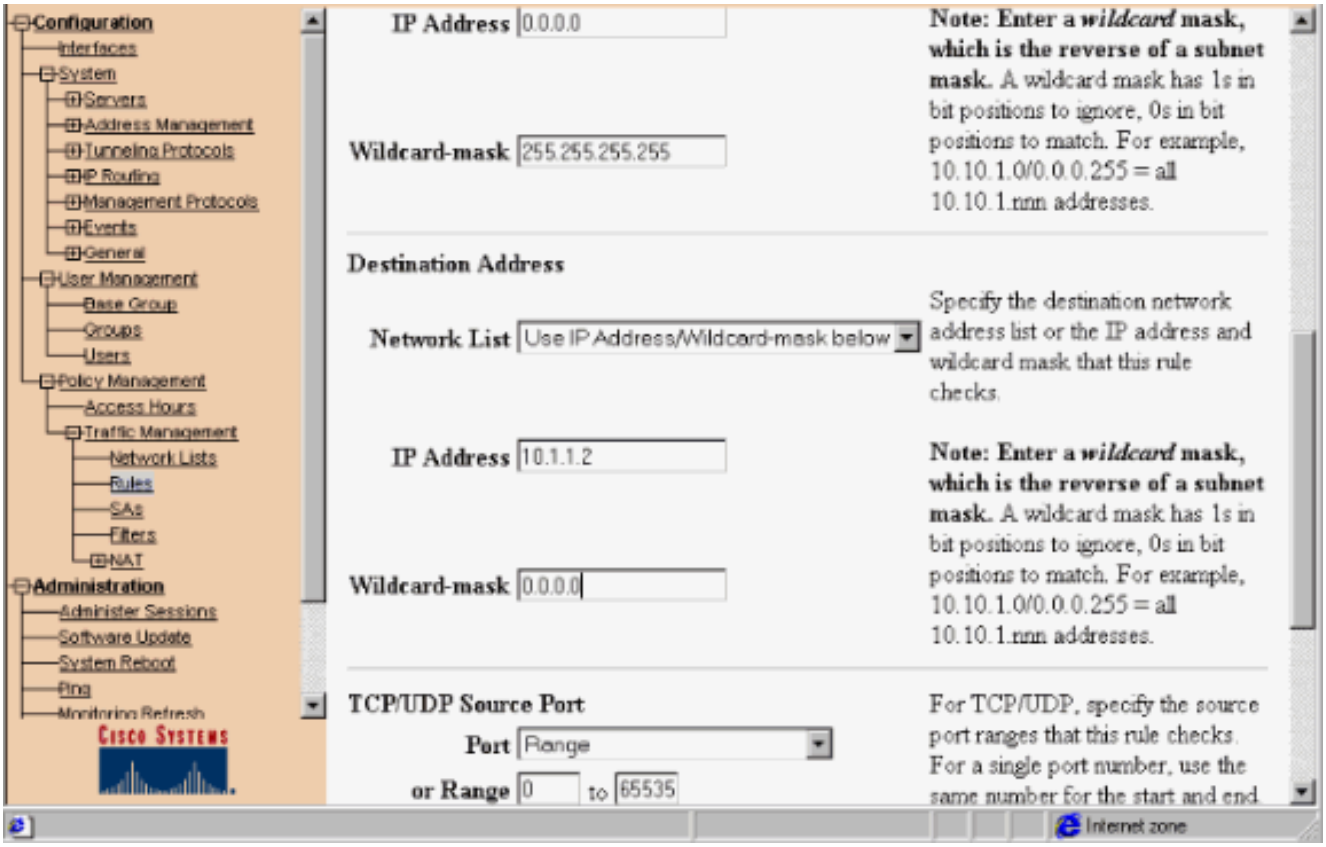
Configuração do VPN 3000

Termine estas etapas a fim configurar o VPN 3000 concentrator.

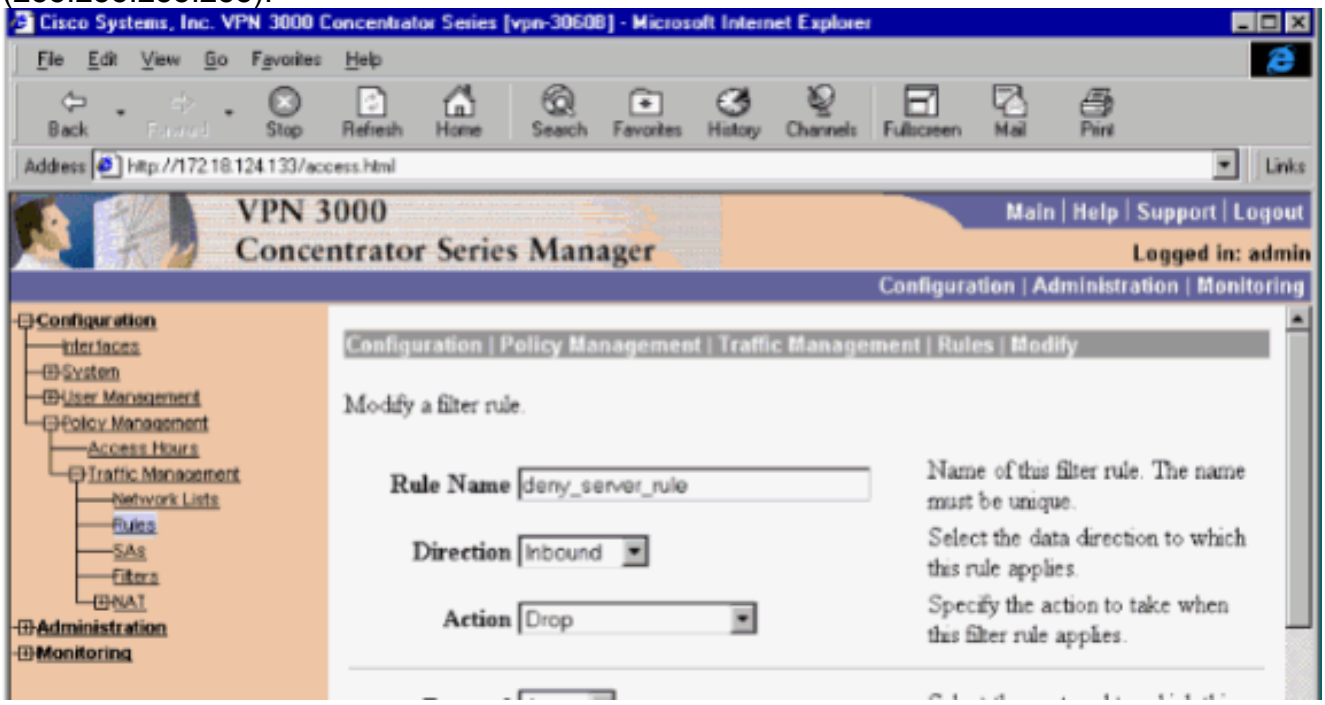
1. Escolha o **> Add do Gerenciamento > da gerência do tráfego > das regras do >Policy da**

configuração e defina primeira o **permit_server_rule** chamado do concentrador VPN regra com estes ajustes:Sentido — **De entrada**Ação — **Dianteiro**Endereço de origem — **255.255.255.255**Endereço de destino — **10.1.1.2**Wildcard mask — **0.0.0.0**

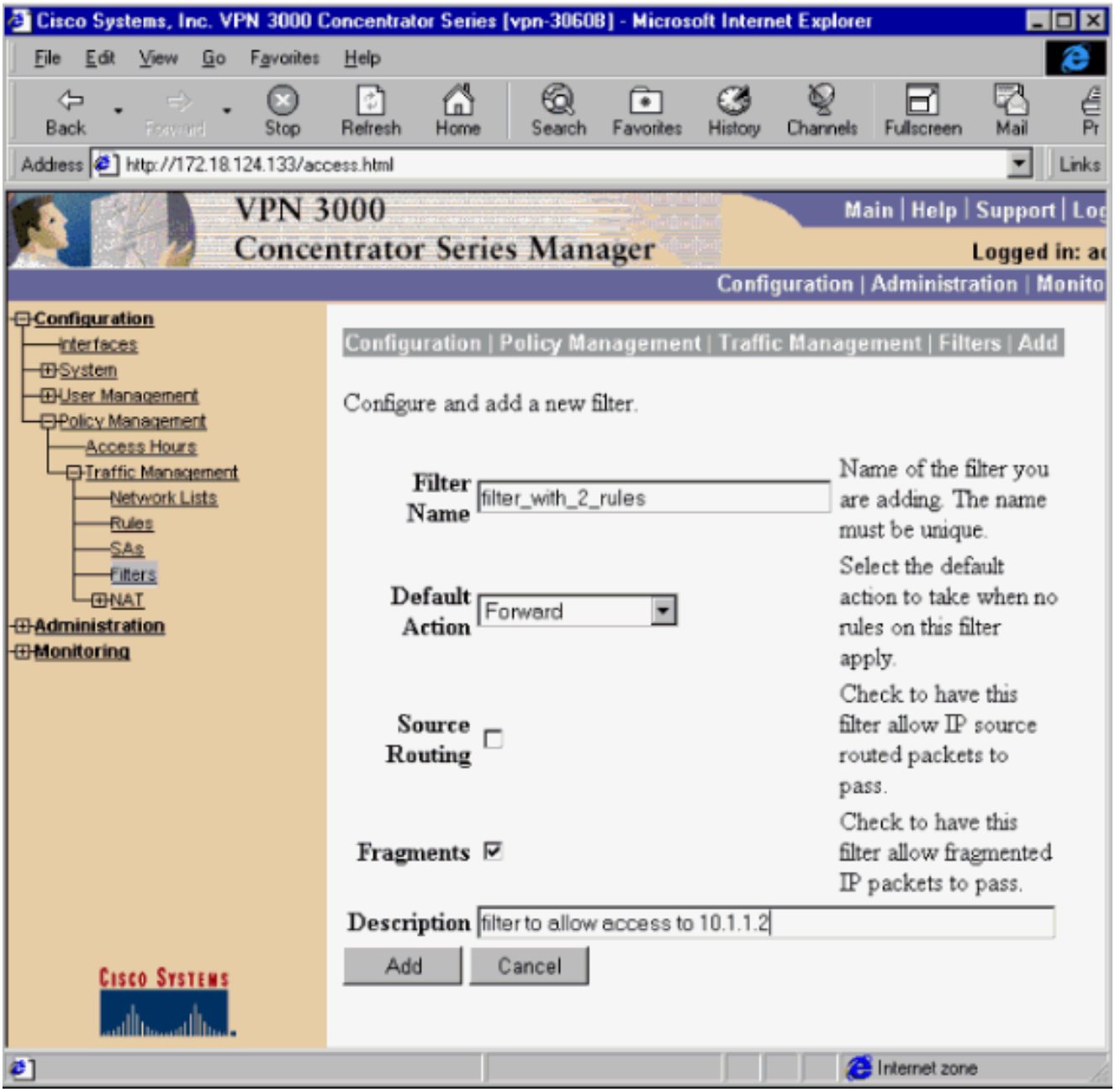




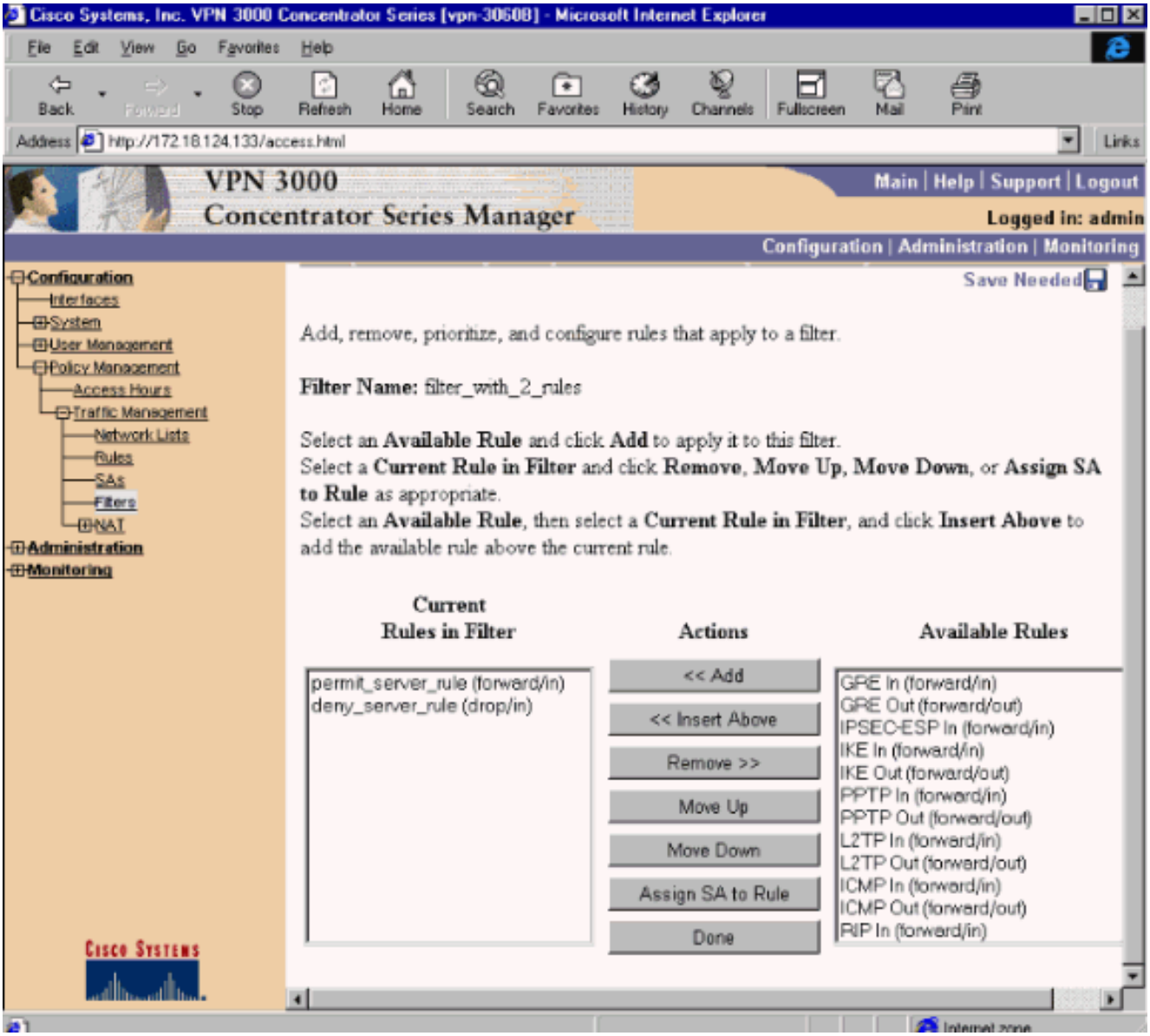
2. Na mesma área, defina a segunda regra do concentrador VPN chamada **deny_server_rule** com estes padrões:Sentido — **De entrada**Ação — **Gota**Endereços de rementente e destinatário de qualquer coisa (255.255.255.255):



3. Escolha o **Configuração > Gerenciamento de Política > Gerenciamento de tTáfego > Filtros** e adicionar seu filtro do **filter_with_2_rules**.



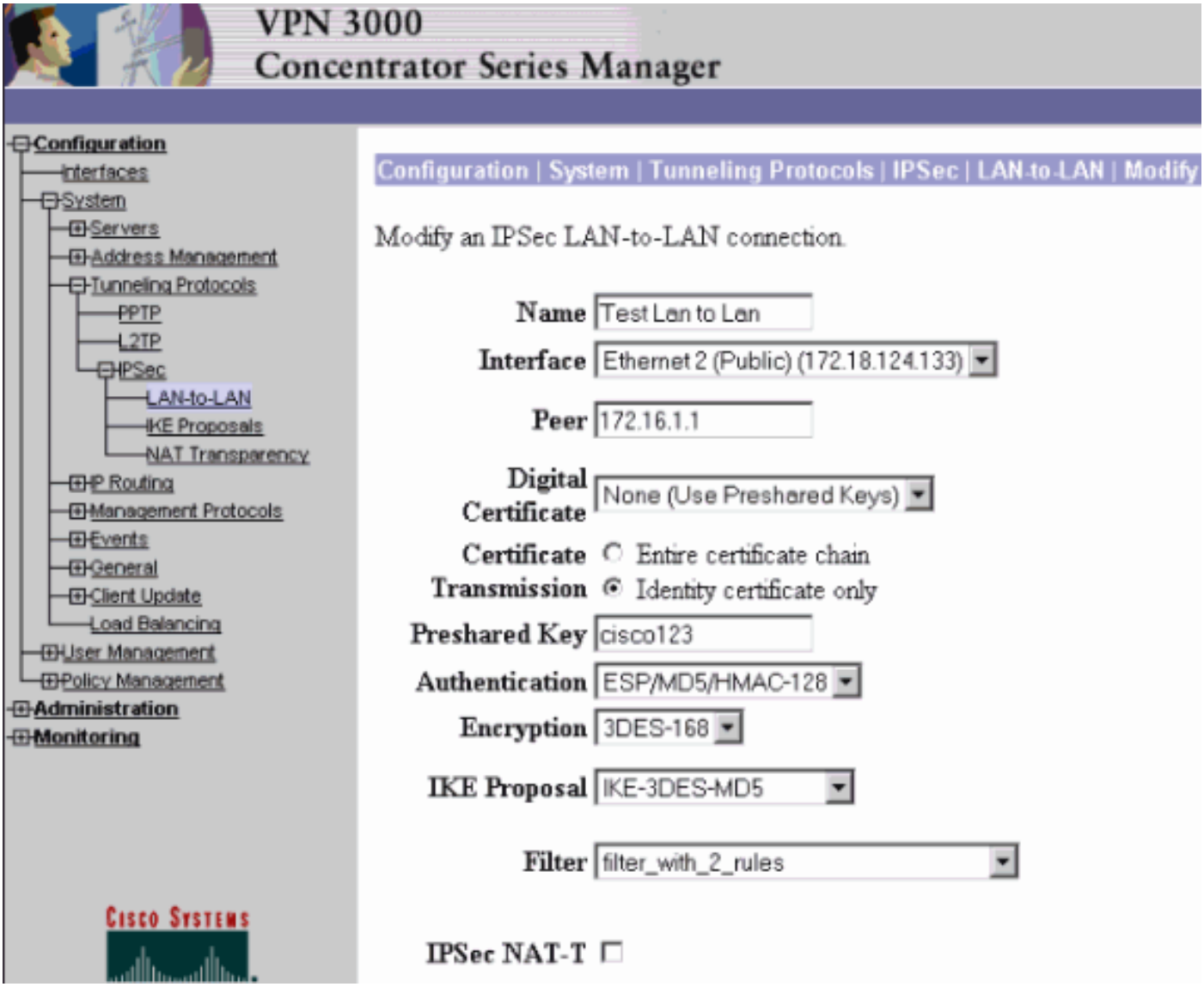
4. Adicionar as duas regras ao filter_with_2_rules:



5. Escolha o **configuration > user management > os grupos** e aplique o filtro ao grupo:

Filtros para um Túnel VPN de Lan para Lan

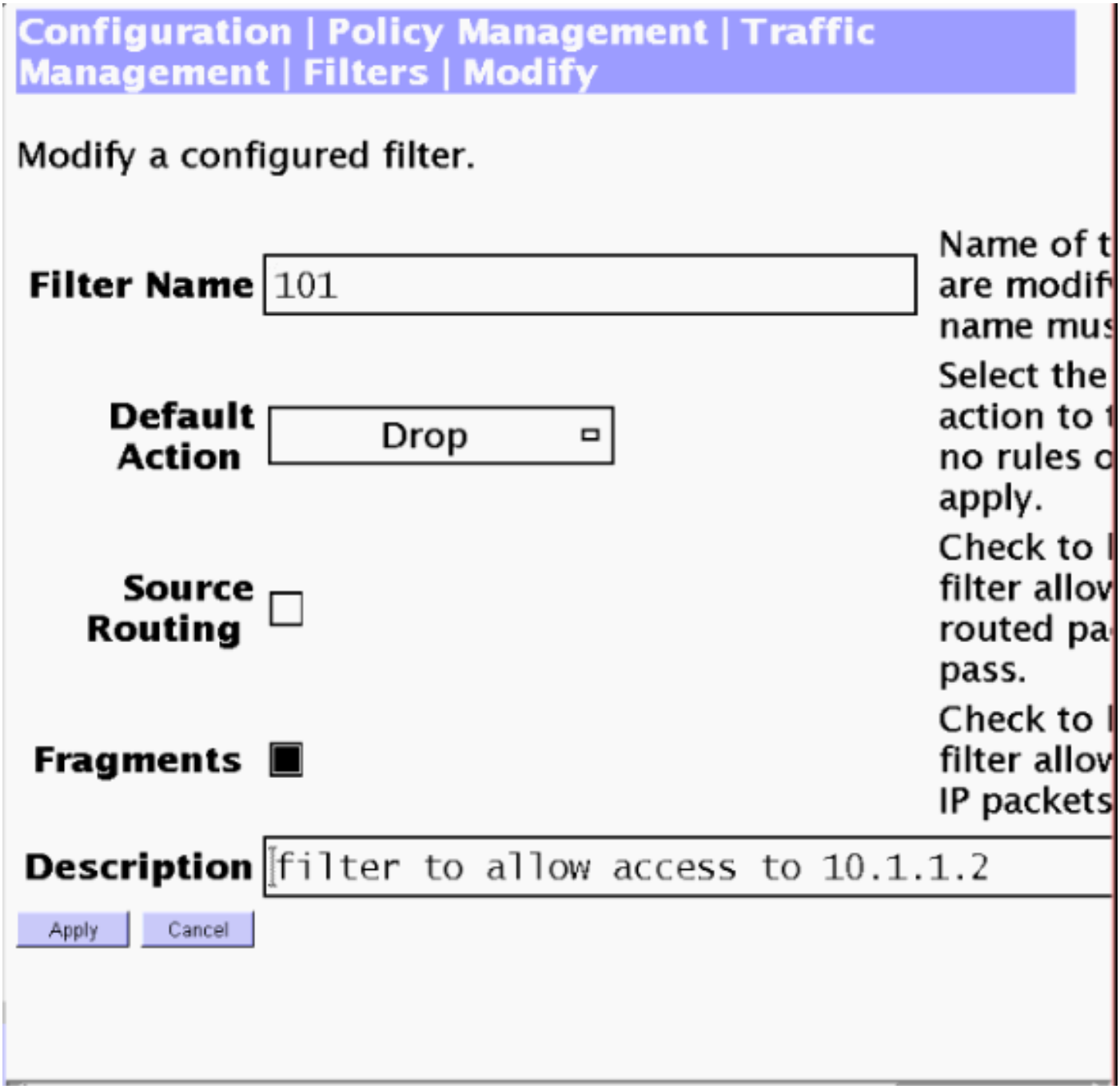
Do 3.6 e mais recente do código do concentrador VPN, você pode filtrar tráfego para cada túnel do IPSec VPN do LAN para LAN. Por exemplo, se você constrói um túnel de LAN para LAN a um outro concentrador VPN com o endereço 172.16.1.1, e queira permitir o acesso de 10.1.1.2 do host ao túnel quando você negar todo tráfego restante, você pode aplicar o **filter_with_2_rules** quando você escolhe o **Configuration > System > Tunneling Protocols > IPsec > LAN para LAN > Modify** e seleciona o **filter_with_2_rules** sob o **filtro**.



Configuração do VPN 3000 - atribuição de filtro RADIUS

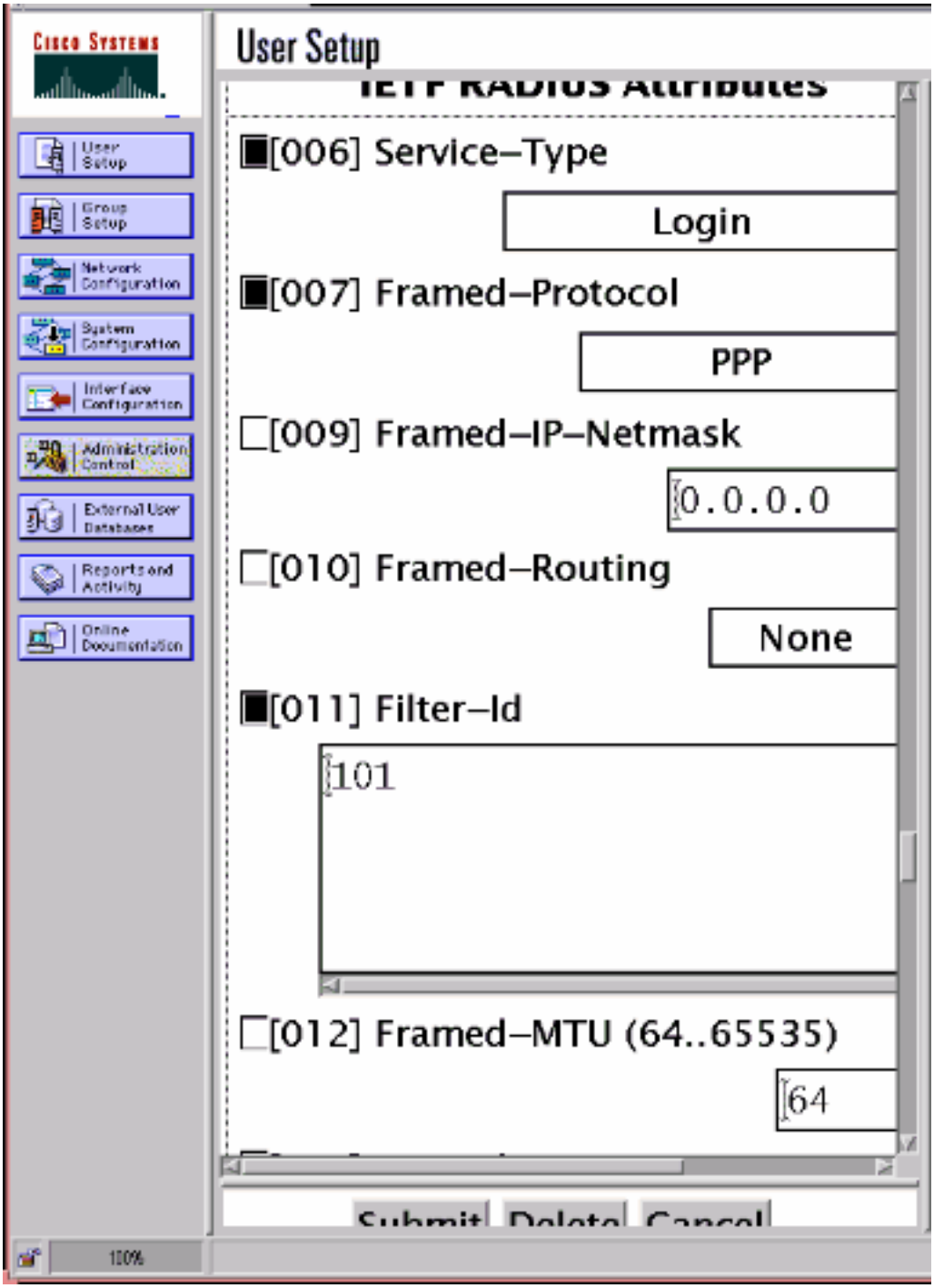
Éigualmente possível definir um filtro no concentrador VPN e para passar então abaixo do número de filtro de um servidor Radius (em termos do RAIO, o atributo 11 é ID de filtro), de modo que quando o usuário for autenticado no servidor Radius, o ID de filtro seja associado com essa conexão. Neste exemplo, a suposição é que a autenticação RADIUS para usuários do concentrador VPN é já operacional e somente o ID de filtro deve ser adicionado.

Defina o filtro no concentrador VPN como no exemplo anterior:



Configuração do Servidor CSNT – Atribuição de Filtros RADIUS

Configurar o atributo 11, ID de filtro no server do Cisco Secure NT para ser **101**:



Depuração - Atribuição de Filtro RADIUS

Se o AUTHDECODE (severidade 1-13) está sobre no concentrador VPN, o log mostra que o server do Cisco Secure NT envia abaixo do access-list 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.

Troubleshooting

Para propósitos de Troubleshooting somente, você pode girar sobre a eliminação de erros do filtro quando você escolhe o **configuração > sistema > eventos > classes** e adiciona a classe **FILTERDBG** com **severidade para registrar = 13**. Nas regras, mude a ação padrão de dianteiro (ou da gota) **enviar e registrar** (ou para deixar cair e log). Quando o log de eventos é recuperado na **monitoração > no log de eventos**, 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 mais frequentes do VPN 3000 concentrator
- Suporte RADIUS
- Apoio do Cisco VPN 3000 Concentrator
- Apoio do Cisco VPN 3000 Client
- Apoio do Cisco Secure ACS for Windows
- Request For Comments (RFC)
- Suporte Técnico e Documentação - Cisco Systems