

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Convenções](#)

[Configuração do VPN 3000](#)

[Filtros para um Túnel VPN de Lan para Lan](#)

[Configuração do VPN 3000 - atribuição de filtro RADIUS](#)

[Configuração do Servidor CSNT – Atribuição de Filtros RADIUS](#)

[Depuração - Atribuição de Filtro RADIUS](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

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.

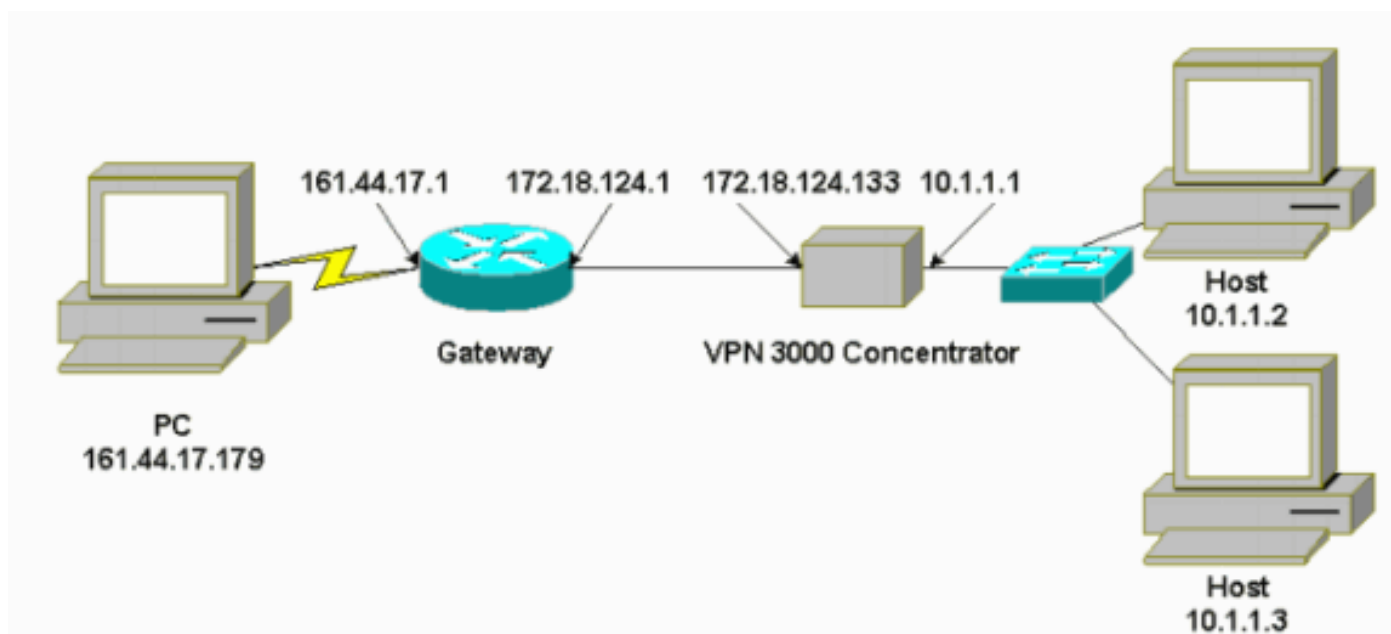
Componentes Utilizados

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.

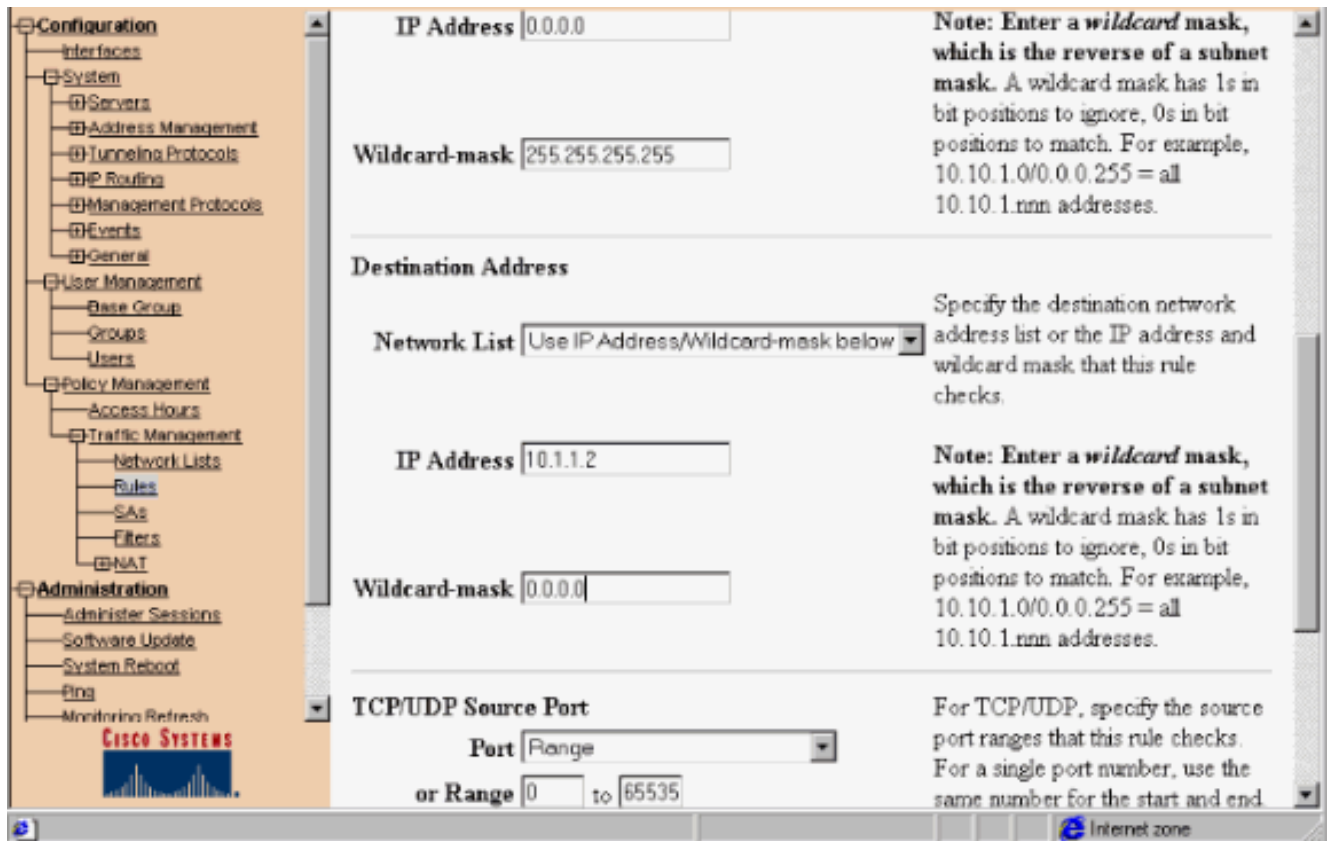
1. Escolha o > **Add do Gerenciamento** > da gerência do tráfego > das regras do >Policy da

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**

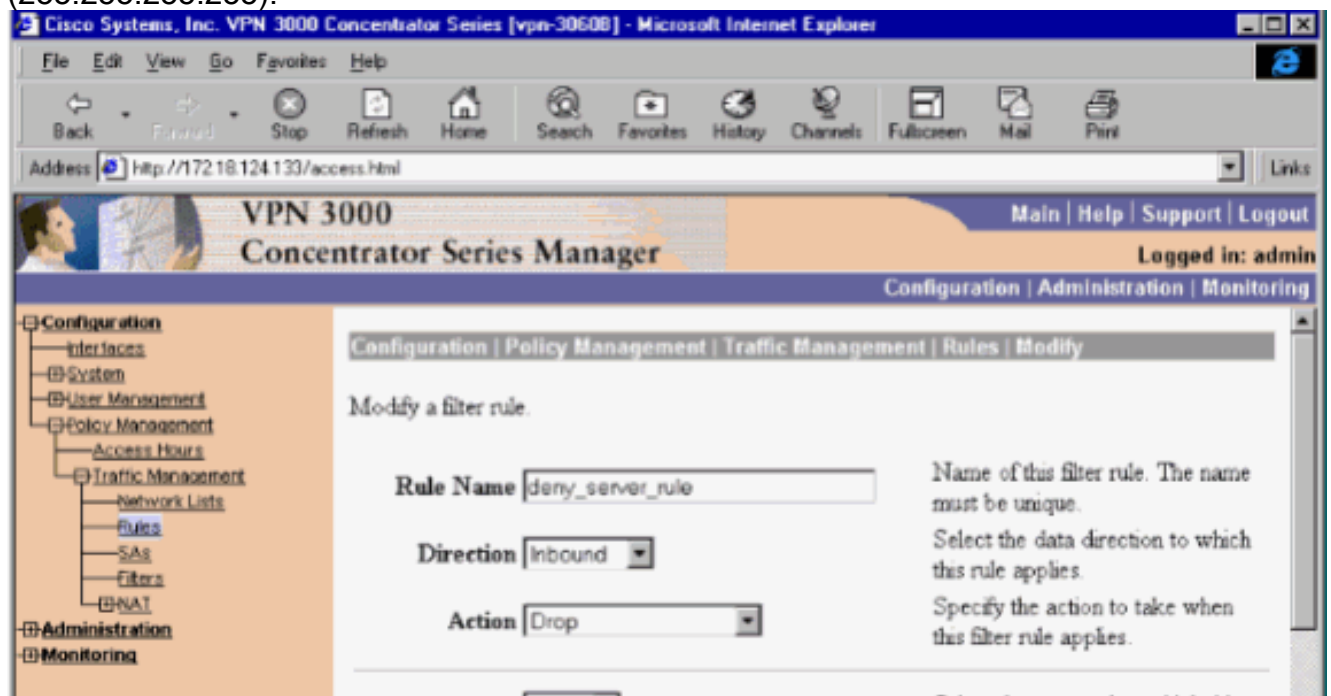
The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.133/access.html". The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes "Configuration", "Administration", and "Monitoring". The "Configuration" menu is expanded, showing "Policy Management" > "Traffic Management" > "Rules" > "Add".

The "Add" rule page contains the following configuration fields:

- 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 for other protocols.
- TCP Connection:** Select whether this rule should apply to an established TCP connection.
- Source Address:** Specify the source network address list or the IP address and wildcard mask that this rule checks.



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 remente e destinatário de qualquer coisa (255.255.255.255):



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

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

Logged in: ac

Configuration | Administration | Monitor

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

CISCO SYSTEMS

Internet zone

4. Adicionar as duas regras ao filter_with_2_rules:

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 Links

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

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)

CISCO SYSTEMS

- Escolha o configuration > user management > os grupos e aplique o filtro ao grupo:

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.
		<input type="checkbox"/>	Enter the IP address of the

[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.



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

[Configuração do VPN 3000 - atribuição de filtro RADIUS](#)

É igualmente possível definir um filtro no concentrador VPN e para passar então abaixo do número de filtro de um servidor Radius (em termos do RADIUS, 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:

Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name

Name of the filter. If the filter name is modified, the name must be unique.

Default Action

Select the default action to take when no rules are applied.

Source Routing

Check to allow the filter to allow traffic to pass through the source routing.

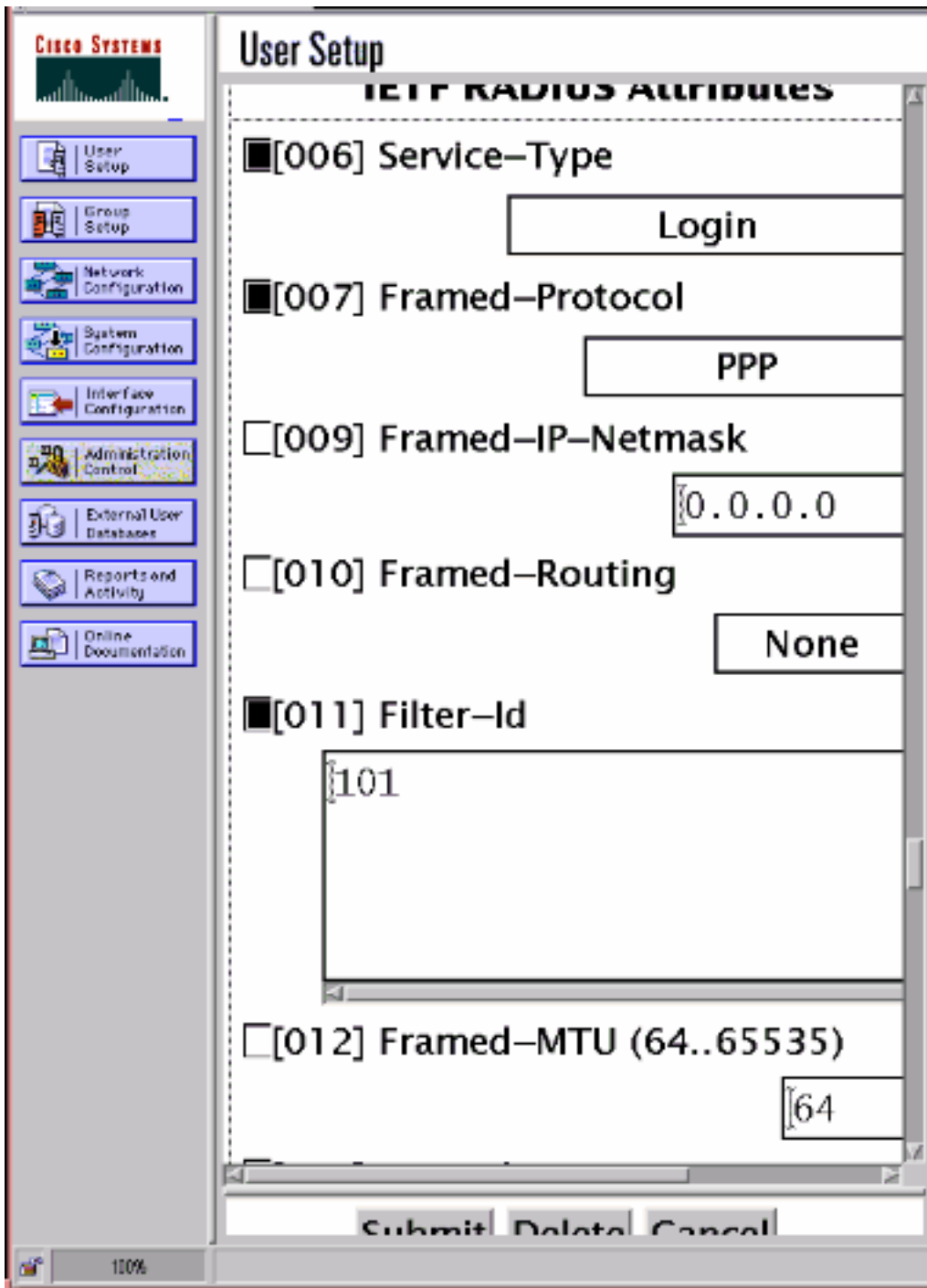
Fragments

Check to allow the filter to allow traffic to pass through IP packets.

Description

[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 FFFFFFFF ..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](#)