

De Cisco VPN 3000 Concentrator configureren voor blokkeren met filters en RADIUS-filtoewijzing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[VPN 3000-configuratie](#)

[Filters voor een LAN-to-LAN VPN-tunnels](#)

[VPN 3000 Configuratie - toewijzing van RADIUS-filter](#)

[Configuratie CSNT-server - RADIUS-filtoewijzing](#)

[Debug - Toewijzing van RADIUS-filters](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

In deze voorbeeldconfiguratie willen we filters gebruiken om een gebruiker toegang te geven tot slechts één server (10.1.1.2) binnen het netwerk en de toegang tot alle andere middelen te blokkeren. De Cisco VPN 3000 Concentrator kan worden ingesteld om IPsec, Point-to-Point Tunneling Protocol (PPTP) en L2TP-clienttoegang tot netwerkbronnen met filters te controleren. Filters bestaan uit regels, die vergelijkbaar zijn met toegangslijsten op een router. Als een router is ingesteld voor:

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

Als de VPN Concentrator-waarde gelijk is, stelt u een filter met regels in.

Onze eerste VPN Concentrator regel is **ist_server_Rule**, die gelijkwaardig is aan de **vergunning van de router ip om het even welke gastheer 10.1.1.2** opdracht. Onze tweede VPN Concentrator regel is **Denken_server_Rule** die gelijkwaardig is aan de **ontkenningsip van de router om het even welke** opdracht.

Ons VPN Concentrator filter is **filter_with_2_rules**, wat gelijk is aan de 101 toegangslijst van de router; het gebruikt **Laat_server_Rule** en **ontkennen_server_regel** (in die volgorde). Er wordt aangenomen dat cliënten een goede verbinding kunnen maken voordat zij filters toevoegen; zij

ontvangen hun IP-adressen van een pool op de VPN-centrator.

Raadpleeg [PIX/ASA 7.x ASDM: Beperk de Toegang tot het netwerk van gebruikers van Remote Access VPN](#) om meer te weten te komen over het scenario waarin de PIX/ASA 7.x de toegang van de VPN-gebruikers blokkeert.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

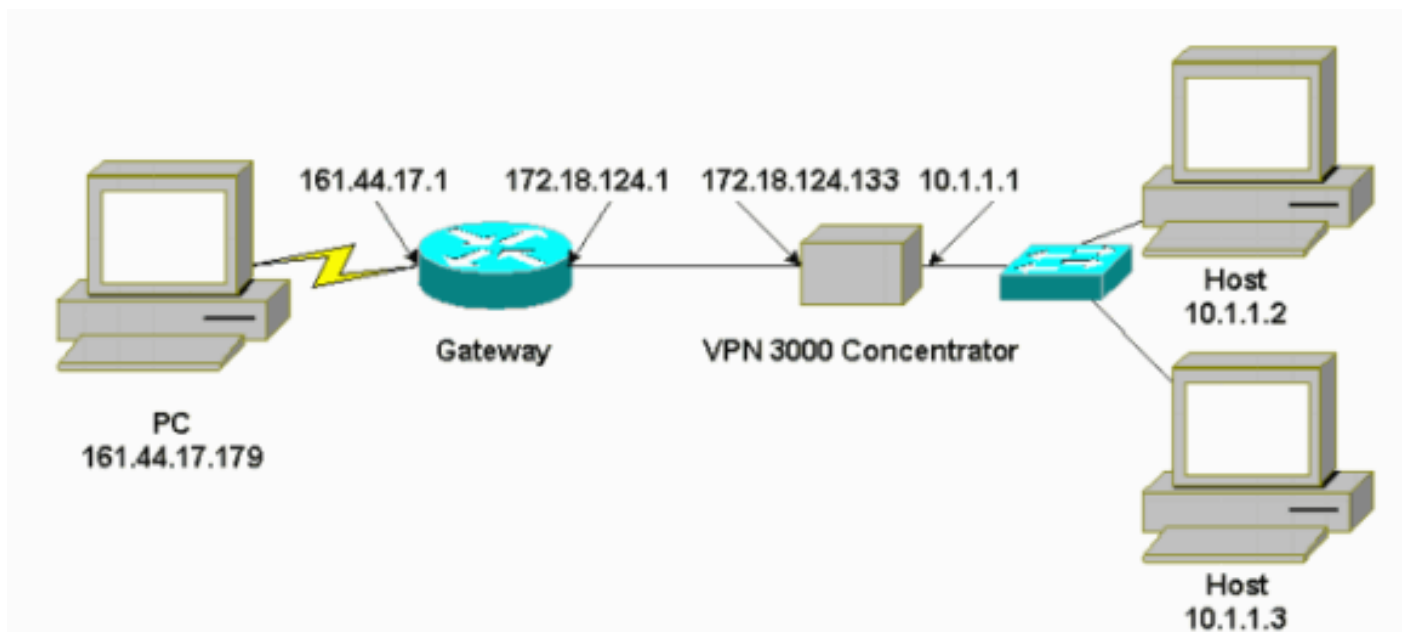
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN 3000 Concentrator versie 2.5.2.D.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



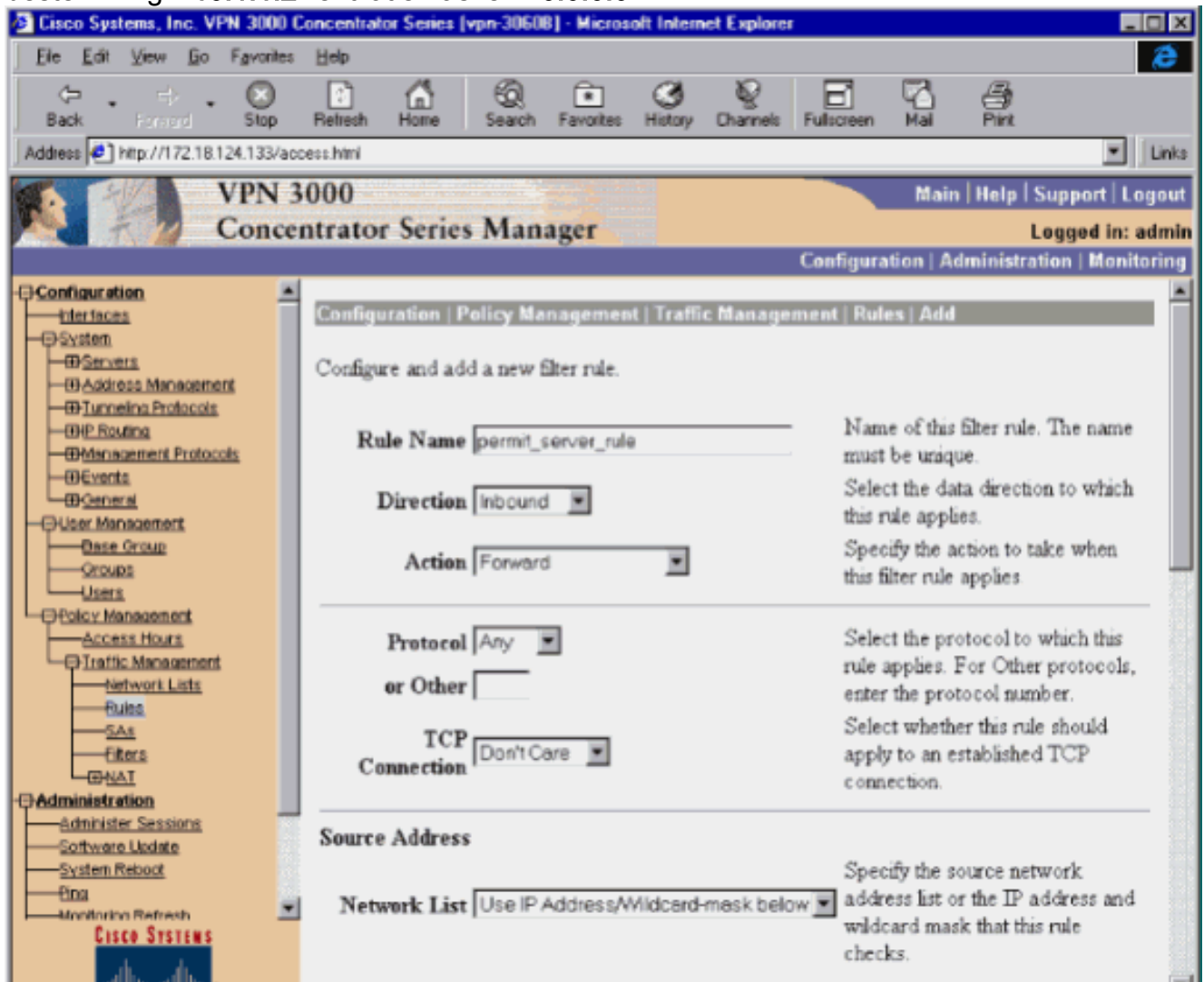
Conventies

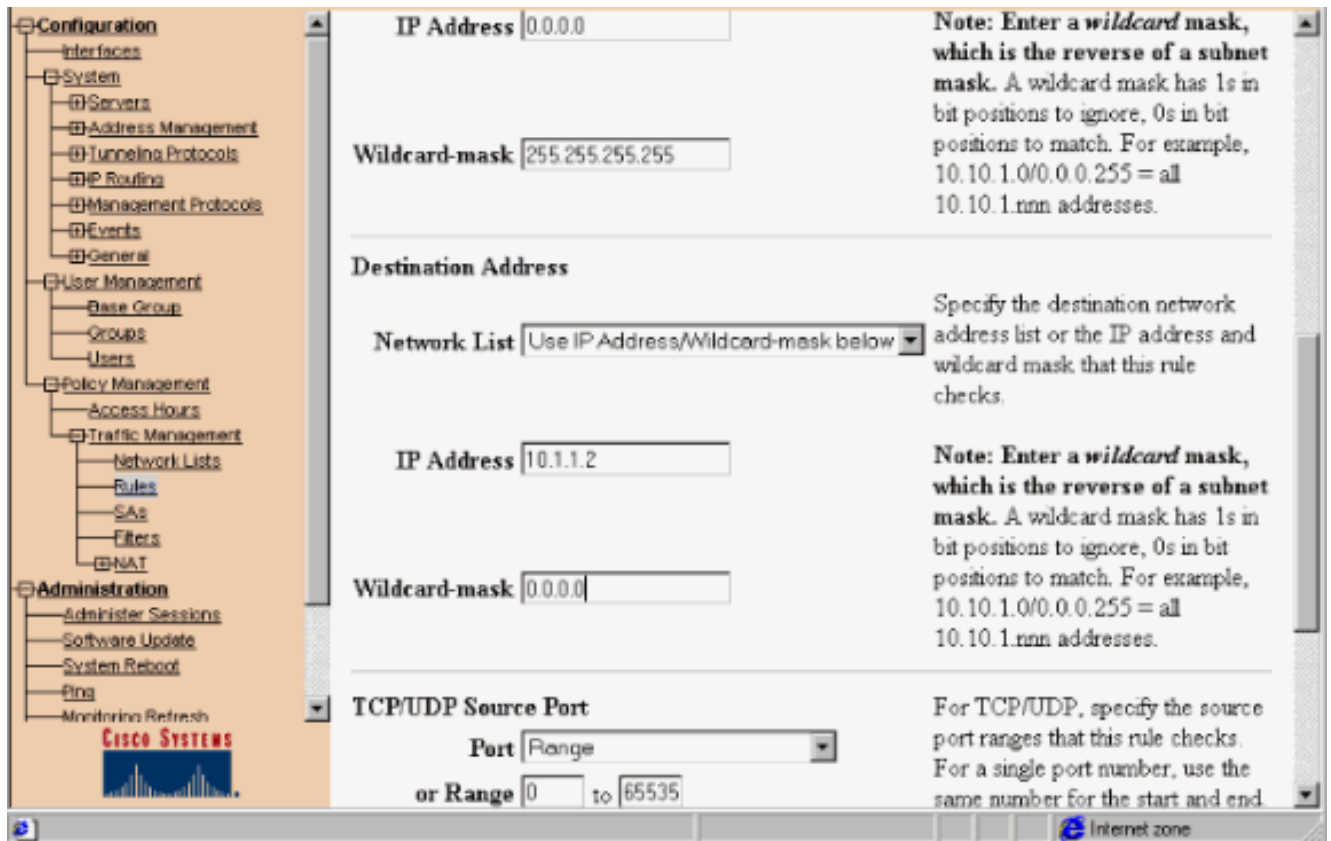
Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor meer informatie over documentconventies.

VPN 3000-configuratie

Volg deze stappen om de VPN 3000 Concentrator te configureren.

1. Kies **Configuratie >Beleidsbeheer > Verkeersbeheer > Regels > Toevoegen** en definieer de eerste VPN Concentrator-regel met de naam **Laat_server_regel** met deze instellingen:Richting — **Ingebonden**Actie—**Voorwaarts**Bron: Adres—**255.255.255.255**Adres bestemming—**10.1.1.2**Ventilatiemasker—**0.0.0.0**





2. In hetzelfde gebied, definieer de tweede VPN Concentrator regel die **ontkennen_server_Rule** wordt genoemd met deze standaardinstellingen:Richting — **IngebondenActie**—DropBron- en doeladressen van alles (255.255.255.255):



3. Kies **Configuratie > Beleidsbeheer > Verkeersbeheer > Filters** en voeg uw **filter_with_2_rules** filter toe.

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 | Log

Configuration | Administration | Monitoring

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

- Voeg de twee regels toe aan 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

Logged in: admin 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

5. Kies Configuratie > Gebruikersbeheer > Groepen en pas het filter toe op de groep:

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

Filters voor een LAN-to-LAN VPN-tunnels

Vanaf VPN Concentrator code 3.6 en hoger kunt u verkeer filteren voor elke LAN-to-LAN IPsec VPN-tunnel. Als u bijvoorbeeld een LAN-to-LAN tunnel aan een andere VPN-Concentrator met het adres 172.16.1.1 bouwt en host 10.1.1.2 toegang tot de tunnel wilt toestaan terwijl u al het andere verkeer ontkent, kunt u `filter_with_2_rules` toepassen wanneer u **Configuration > System > Tunneling Protocols > IPsec > LAN-to** kiest **LAN > Wijzigen** en selecteren `filter_with_2_rules` onder **Filter**.



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

[VPN 3000 Configuratie - toewijzing van RADIUS-filter](#)

Het is ook mogelijk om een filter in de VPN-centrator te definiëren en het filternummer vervolgens door te geven vanaf een RADIUS-server (in RADIUS-termen is attribuut 11 Filter-id), zodat wanneer de gebruiker op de RADIUS-server echt is bevonden, het filter-id gekoppeld is aan die verbinding. In dit voorbeeld is de aanname dat de RADIUS-verificatie voor VPN-Concentrator-gebruikers al operationeel is en dat alleen de filter-id moet worden toegevoegd.

Definieert het filter in de VPN-centrator zoals in het vorige voorbeeld:

Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name

Name of the filter to be modified. The name must be unique.

Default Action

Select the default action to be applied to traffic when no rules are found.

Source Routing

Check to allow the filter to apply to traffic that has been routed by a source router.

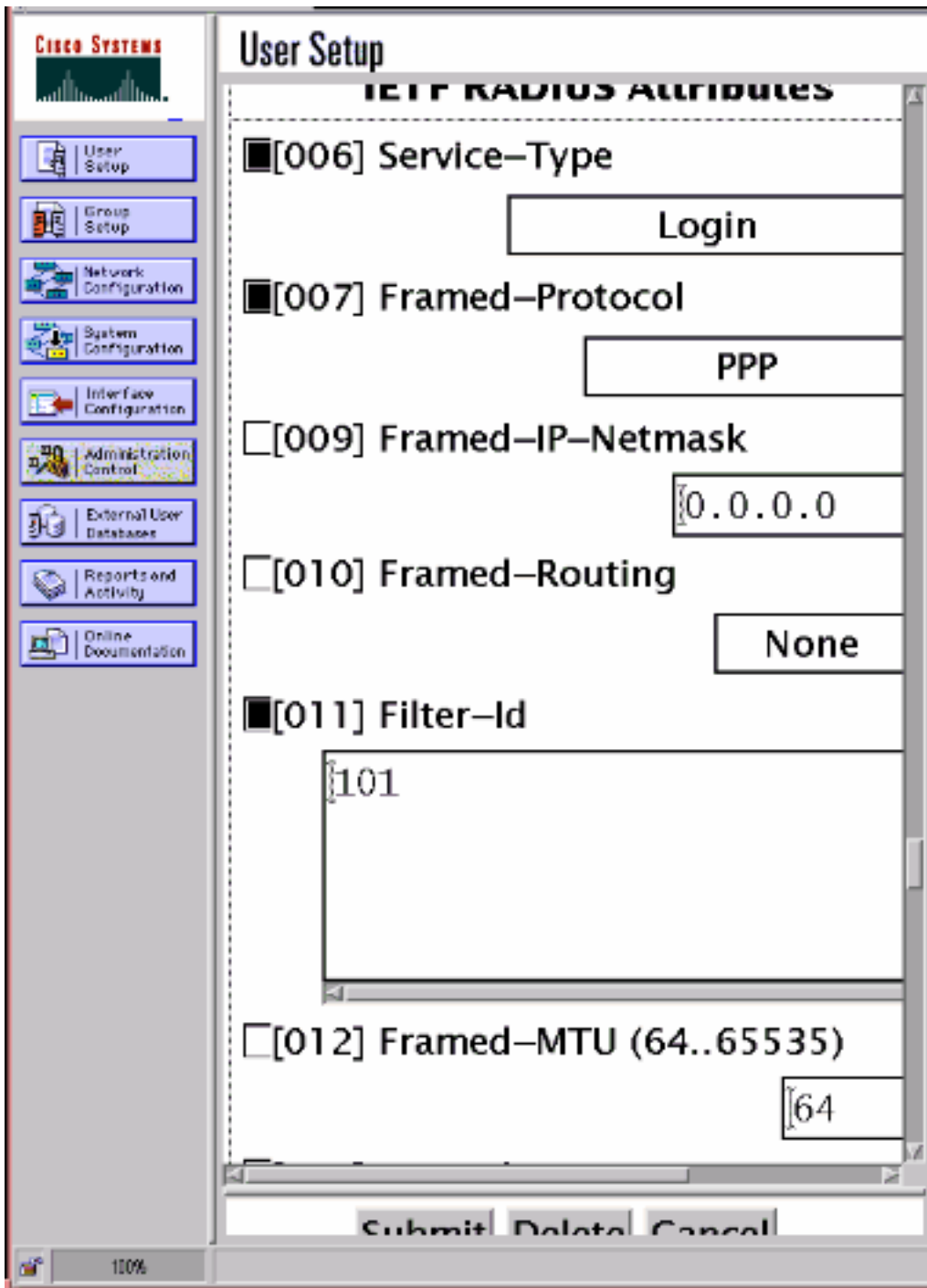
Fragments

Check to allow the filter to apply to fragmented IP packets.

Description

[Configuratie CSNT-server - RADIUS-filtertoewijzing](#)

Configureer eigenschap 11, filter-id op de Cisco Secure NT-server om 101 te zijn:



[Debug - Toewijzing van RADIUS-filters](#)

Als AUTHDECODE (1-13 Severity) in de VPN-Concentrator is ingeschakeld, toont het logbestand aan dat de Cisco Secure NT-server beneden toegangslijst 101 verstuurt in eigenschap 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.....
```

[Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Alleen voor de probleemoplossing kunt u het foutoptreden van het filter inschakelen wanneer u **Configuration > System > Events > Classes** kiest en **FILTERDBG**-klasse met **ernst** aan **Log = 13** toevoegt. In de regels wijzigt u de standaardactie van voorwaartse (of drop) naar **voorwaartse en loggen** (of Drop en Log). Wanneer het logbestand van de gebeurtenis bij **Controle > Event Log** wordt opgehaald, moet het items als:

```
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
```

Gerelateerde informatie

- [IPsec-onderhandeling/IKE-protocollen](#)
- [VPN 3000 Concentrator Vaak gestelde vragen](#)
- [RADIUS-ondersteuning](#)
- [Ondersteuning van Cisco VPN 3000 Concentrator](#)
- [Ondersteuning van Cisco VPN 3000-client](#)
- [Cisco Secure ACS voor Windows-ondersteuning](#)
- [Verzoek om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)