

Konfigurieren des Cisco VPN 3000 Concentrator für Blockierung mit Filtern und RADIUS-Filterzuweisung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdigramm](#)

[Konventionen](#)

[Konfiguration des VPN 3000](#)

[Filter für einen LAN-zu-LAN-VPN-Tunnel](#)

[VPN 3000-Konfiguration - RADIUS-Filterzuweisung](#)

[CSNT-Serverkonfiguration - RADIUS-Filterzuweisung](#)

[Debuggen - RADIUS-Filterzuweisung](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In dieser Beispielkonfiguration sollen Filter verwendet werden, um einem Benutzer den Zugriff auf nur einen Server (10.1.1.2) im Netzwerk zu ermöglichen und den Zugriff auf alle anderen Ressourcen zu blockieren. Der Cisco VPN 3000 Concentrator kann so eingerichtet werden, dass er IPsec, Point-to-Point Tunneling Protocol (PPTP) und L2TP-Client-Zugriff auf Netzwerkressourcen mithilfe von Filtern steuert. Filter bestehen aus Regeln, die den Zugriffslisten auf einem Router ähneln. Wenn ein Router für konfiguriert wurde:

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

Beim Äquivalent zum VPN-Konzentrator wird ein Filter mit Regeln eingerichtet.

Unsere erste VPN Concentrator-Regel ist **permit_server_rules**, was dem Befehl **permit ip any host 10.1.1.2** des Routers entspricht. Unsere zweite VPN-Concentrator-Regel ist **deny_server_regel**, die dem Befehl **"deny ip any any"** des Routers entspricht.

Unser VPN Concentrator-Filter ist **filter_with_2_rules**, was der Zugriffsliste des Routers 101 entspricht. es verwendet **permit_server_regel** und **deny_server_regel** (in dieser Reihenfolge). Es wird davon ausgegangen, dass die Clients eine ordnungsgemäße Verbindung herstellen können, bevor sie Filter hinzufügen. sie erhalten ihre IP-Adressen aus einem Pool im VPN Concentrator.

Weitere Informationen finden Sie unter [PIX/ASA 7.x ASDM: Beschränken Sie den Netzwerkzugriff von VPN-Benutzern mit Remote-Zugriff](#), um mehr über das Szenario zu erfahren, in dem PIX/ASA 7.x den Zugriff von VPN-Benutzern blockiert.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

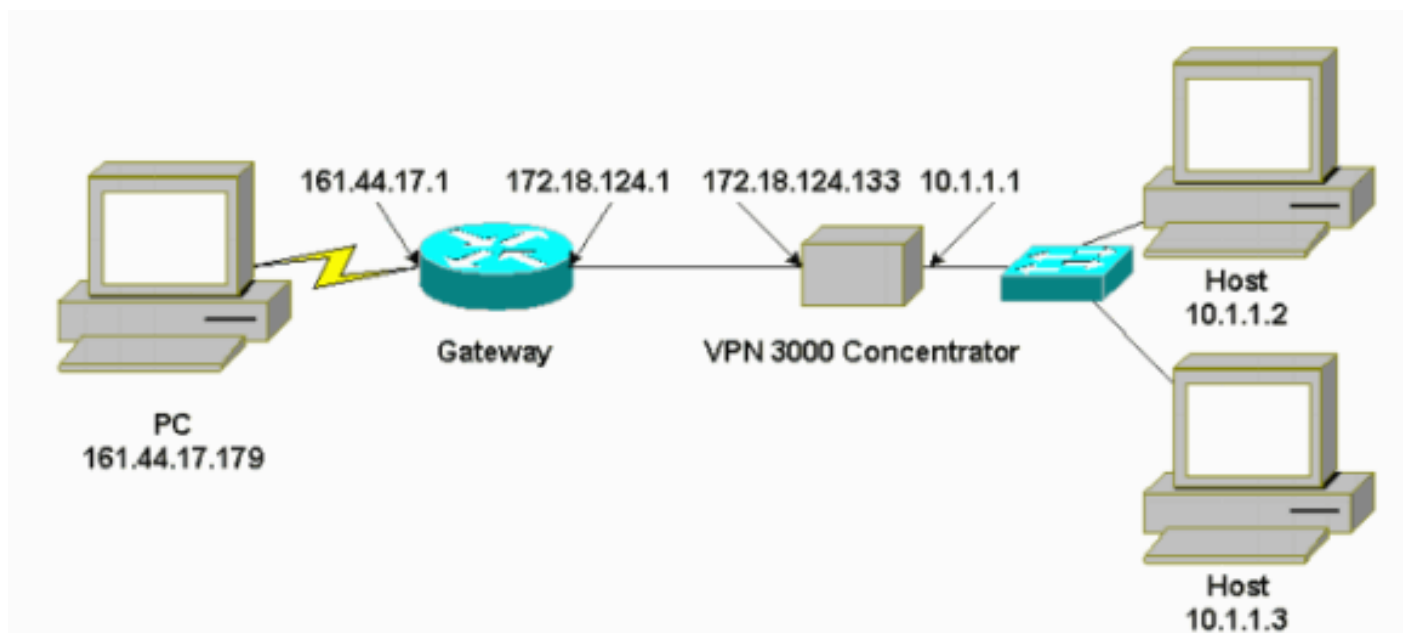
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco VPN 3000 Concentrator, Version 2.5.2.D.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Konfiguration des VPN 3000

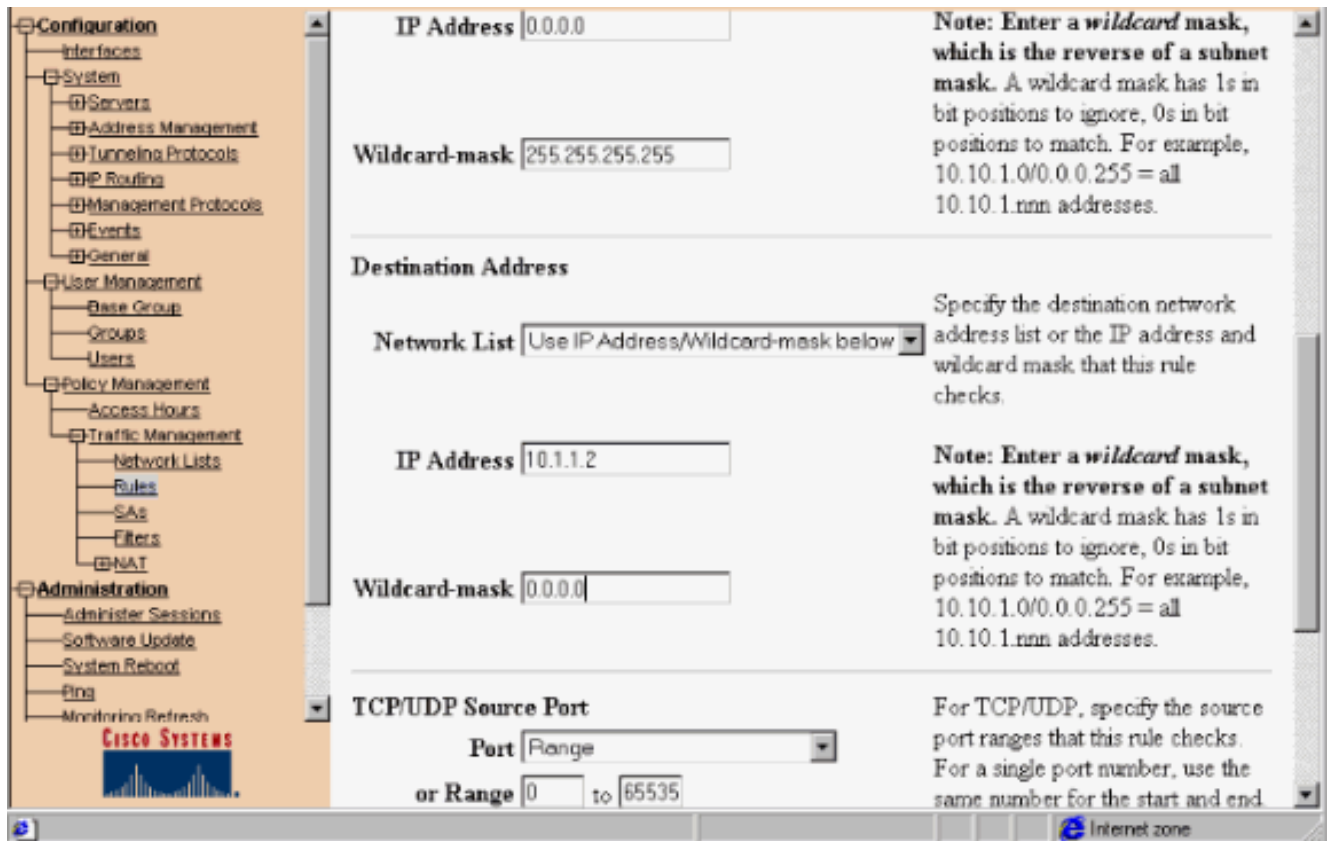
Führen Sie diese Schritte aus, um den VPN 3000-Konzentrator zu konfigurieren.

1. Wählen Sie **Konfiguration > Richtlinienmanagement > Datenverkehrsverwaltung > Regeln > Hinzufügen**, und definieren Sie die erste VPN-Konzentrator-Regel mit dem Namen **permit_server_regel** mit diesen Einstellungen: Richtung - **Eingehend** Aktion - **Weiterleiten** Quelladresse - **255.255.255.255** Zieladresse - **10.1.1.2** Platzhaltermaske: **0.0.0.0**

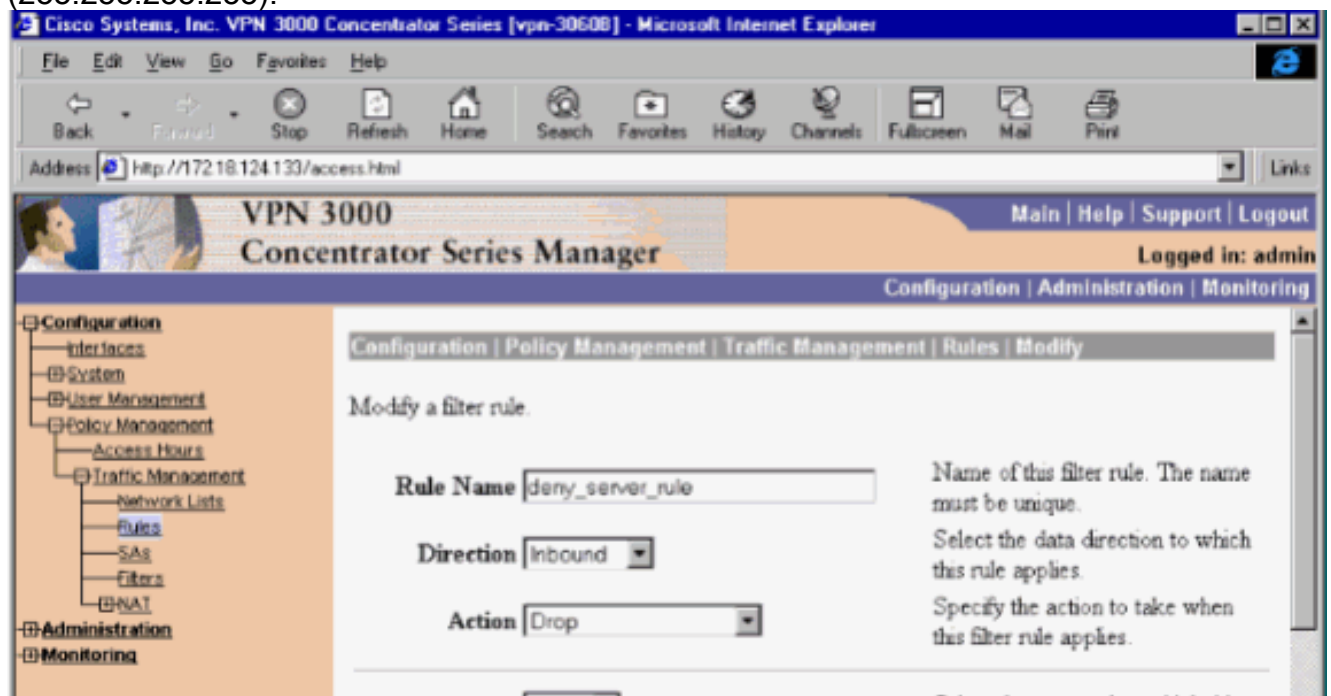
The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows <http://172.18.124.133/access.html>. The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes "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:**
 - Network List:** Specify the source network address list or the IP address and wildcard mask that this rule checks.



2. Definieren Sie im gleichen Bereich die zweite VPN-Konzentrator-Regel mit dem Namen **deny_server_regel** mit folgenden Standardwerten: Richtung - **Eingehend** Aktion - **Löschen** Quell- und Zieladressen (255.255.255.255):



3. Wählen Sie **Configuration > Policy Management > Traffic Management > Filters** aus, und fügen Sie den Filter **_with_2_rules** hinzu.

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

Logged in: ac

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

- Fügen Sie die beiden Regeln zu filter_with_2_rules hinzu:

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

5. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen**, und wenden Sie den Filter auf die Gruppe an:

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.

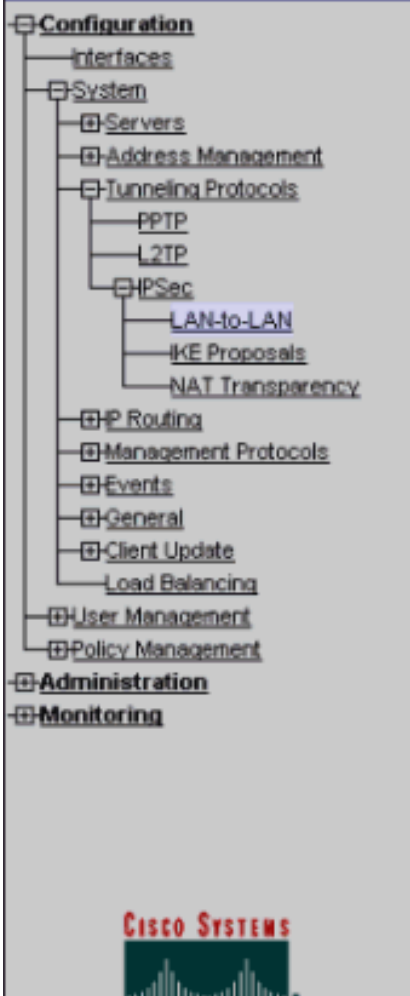
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password 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

[Filter für einen LAN-zu-LAN-VPN-Tunnel](#)

Von VPN Concentrator Code 3.6 und höher können Sie den Datenverkehr für jeden LAN-zu-LAN IPsec-VPN-Tunnel filtern. Wenn Sie z. B. einen LAN-zu-LAN-Tunnel zu einem anderen VPN-Konzentrator mit der Adresse 172.16.1.1 erstellen und Host 10.1.1.2 den Zugriff auf den Tunnel zulassen möchten, während Sie den übrigen Datenverkehr ablehnen, können Sie **filter_with_2_rules** anwenden, wenn Sie **Configuration > System > Tunneling Protocols > IPsec > LAN-** auswählen > **to-LAN > Modify** und wählen **filter_with_2_rules** unter **Filter** aus.



VPN 3000 Concentrator Series Manager



Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name	<input type="text" value="Test Lan to Lan"/>
Interface	<input type="text" value="Ethernet 2 (Public) (172.18.124.133)"/>
Peer	<input type="text" value="172.16.1.1"/>
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>
Certificate	<input type="radio"/> Entire certificate chain
Transmission	<input checked="" type="radio"/> Identity certificate only
Preshared Key	<input type="text" value="cisco123"/>
Authentication	<input type="text" value="ESP/MD5/HMAC-128"/>
Encryption	<input type="text" value="3DES-168"/>
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>
Filter	<input type="text" value="filter_with_2_rules"/>
IPSec NAT-T	<input type="checkbox"/>

[VPN 3000-Konfiguration - RADIUS-Filterzuweisung](#)

Es ist auch möglich, einen Filter im VPN Concentrator zu definieren und dann die Filternummer von einem RADIUS-Server abzugeben (in RADIUS-Begriffen lautet Attribut 11 Filter-ID), sodass die Filter-ID dieser Verbindung zugeordnet wird, wenn der Benutzer auf dem RADIUS-Server authentifiziert wird. In diesem Beispiel wird davon ausgegangen, dass die RADIUS-Authentifizierung für VPN Concentrator-Benutzer bereits aktiv ist und nur die Filter-ID hinzugefügt werden muss.

Definieren Sie den Filter auf dem VPN-Konzentrator wie im vorherigen Beispiel:

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 source routed.

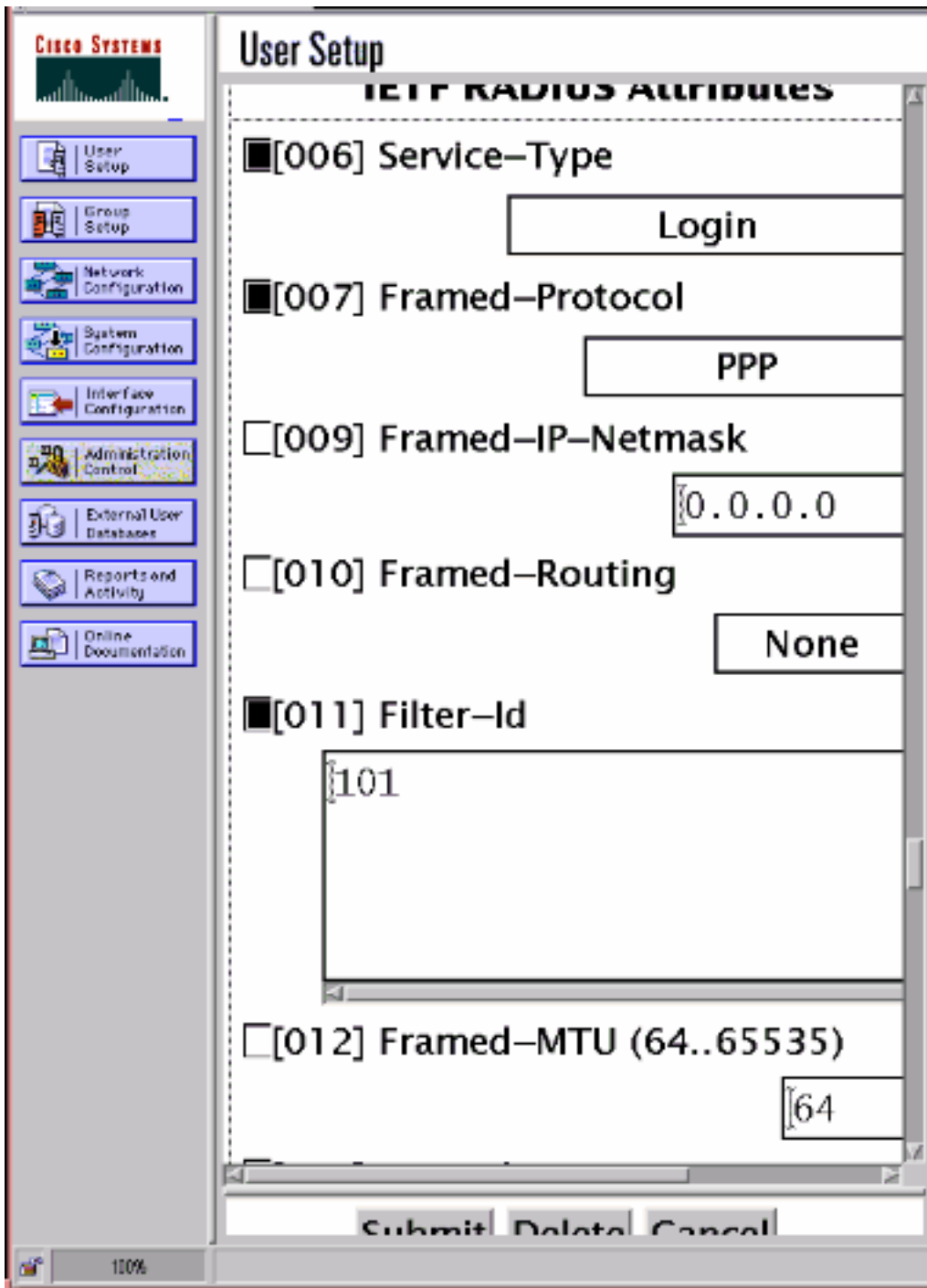
Fragments

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

Description

[CSNT-Serverkonfiguration - RADIUS-Filterzuweisung](#)

Konfigurieren Sie Attribut 11, Filter-ID auf dem Cisco Secure NT-Server auf 101:



Debuggen - RADIUS-Filterzuweisung

Wenn AUTHDECODE (1-13 Schweregrad) im VPN-Konzentrator aktiviert ist, zeigt das Protokoll, dass der Cisco Secure NT-Server die Zugriffsliste 101 in Attribut 11 (0x0B) heruntersendet:

```
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.....
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Nur zur Fehlerbehebung können Sie das Debuggen von Filtern aktivieren, wenn Sie **Configuration > System > Events > Classes** auswählen und die **FILTERDBG**-Klasse mit **Severity to Log = 13** hinzufügen. Ändern Sie in den Regeln die Standardaktion von Forward (oder Drop) in **Forward (Forward)** und Log (**Forward and Log (Forward (Weiterleiten und Protokoll))**) (oder Drop and Log (Ablegen und Protokoll)). Wenn das Ereignisprotokoll unter **Überwachung > Ereignisprotokoll** abgerufen wird, sollten folgende Einträge angezeigt werden:

```
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
```

Zugehörige Informationen

- [IPsec-Aushandlung/IKE-Protokolle](#)
- [Häufig gestellte Fragen zum VPN 300 Concentrator](#)
- [RADIUS-Unterstützung](#)
- [Unterstützung von Cisco VPN 3000 Concentrator](#)
- [Cisco VPN 3000 Client-Unterstützung](#)
- [Cisco Secure ACS für Windows-Unterstützung](#)
- [Request for Comments \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)