

Configuración del Concentrador VPN 3000 de Cisco para bloquear con filtros y la asignación de filtro RADIUS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Configuración de VPN 3000](#)

[Filtros para un túnel VPN de LAN a LAN](#)

[Configuración de VPN 3000 – Asignación de filtro de RADIUS](#)

[Configuración del servidor CSNT - Asignación de filtro de RADIUS](#)

[Depuración – Asignación de filtro RADIUS](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

En esta configuración de muestra, queremos utilizar los filtros para permitir que un usuario acceda solamente un servidor (10.1.1.2) dentro de la red y bloquee el acceso al resto de los recursos. El Cisco VPN 3000 Concentrator se puede configurar para controlar el IPsec, el Point-to-Point Tunneling Protocol (PPTP), y el acceso al cliente L2TP a los recursos de red con los filtros. Los filtros consisten en las reglas, que son similares a las Listas de acceso en un router. Si configuraron a un router para:

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

el equivalente del concentrador VPN sería configurar un filtro con las reglas.

Nuestra primera regla del concentrador VPN es el **permit_server_rule**, que es equivalente al **IP del permiso del router cualquier** comando de **10.1.1.2 del host**. Nuestra segunda regla del concentrador VPN es **deny_server_rule** que es equivalente al **comando deny ip any any del router**.

Nuestro filtro del concentrador VPN es **filter_with_2_rules**, que es equivalente a la lista de acceso del router 101; utiliza el **permit_server_rule** y el **deny_server_rule** (en esa orden). Se asume que los clientes pueden conectar correctamente antes de agregar los filtros; reciben sus IP Addresses de un pool en el concentrador VPN.

Refiera al [ASDM del PIX/ASA 7.x: Restrinja el acceso a la red de los usuarios del VPN de acceso remoto](#) para aprender más sobre el escenario donde el bloque del PIX/ASA 7.x el acceso de los usuarios de VPN.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

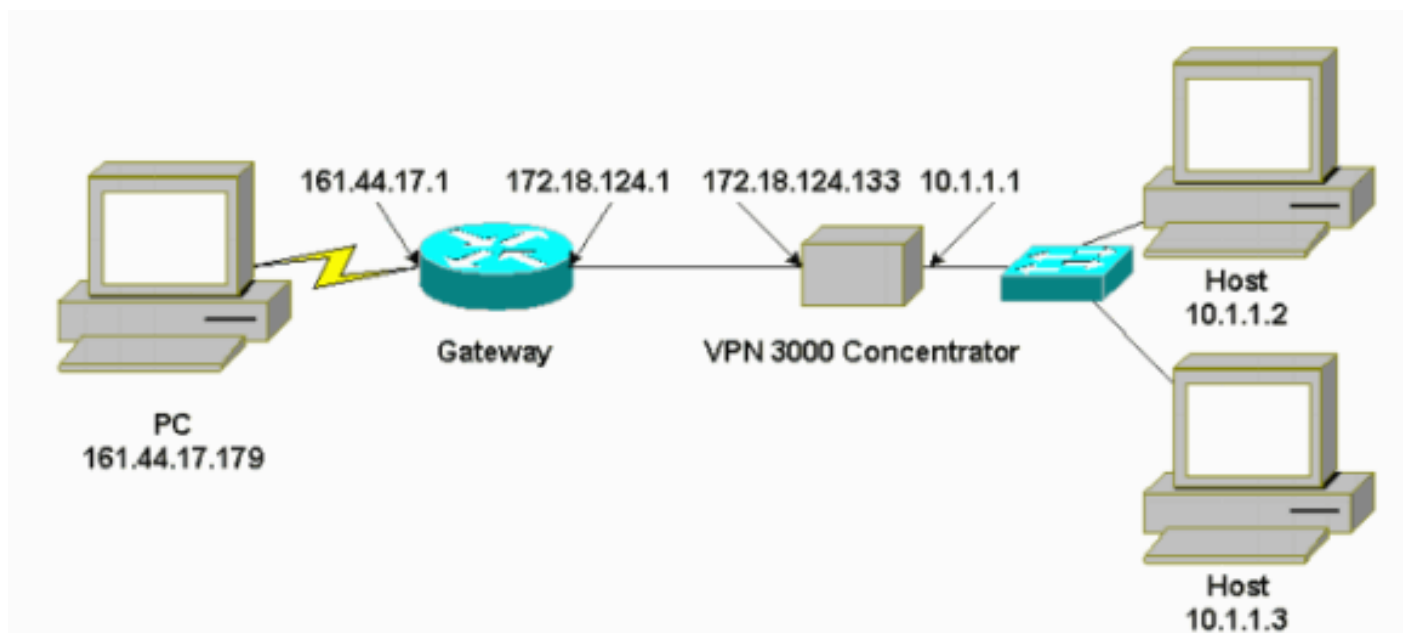
Componentes Utilizados

La información en este documento se basa en la versión 2.5.2.D del Cisco VPN 3000 Concentrator.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Configuración de VPN 3000

Complete estos pasos para configurar el concentrador VPN 3000.

1. Elija la **Administración del >Policy de la configuración > Traffic Management > las reglas > Add** y defina primera el **permit_server_rule** llamado del concentrador VPN regla con estas configuraciones: Dirección — **Entrante** Acción — **Delantero** Dirección de origen — **255.255.255.255** Dirección destino — **10.1.1.2** Máscara comodín — **0.0.0.0**

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.133/access.html". The page header includes "VPN 3000 Concentrator Series Manager" and "Logged in: admin". The navigation menu on the left shows "Configuration" expanded, with "Traffic Management" > "Rules" selected. The main content area is titled "Configuration | Policy Management | Traffic Management | Rules | Add".

Configure and add a new filter rule.

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.

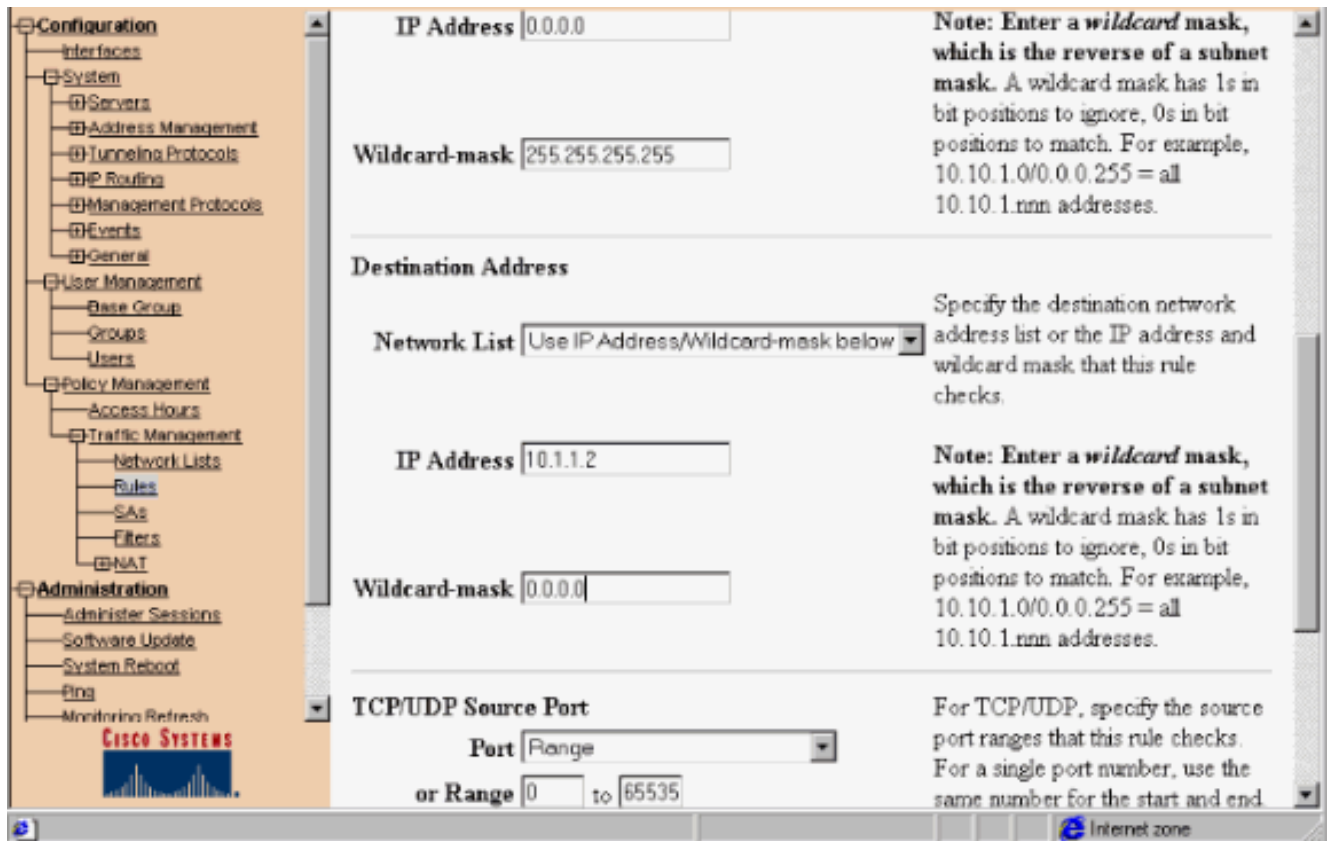
Protocol Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

or Other Enter the protocol number.

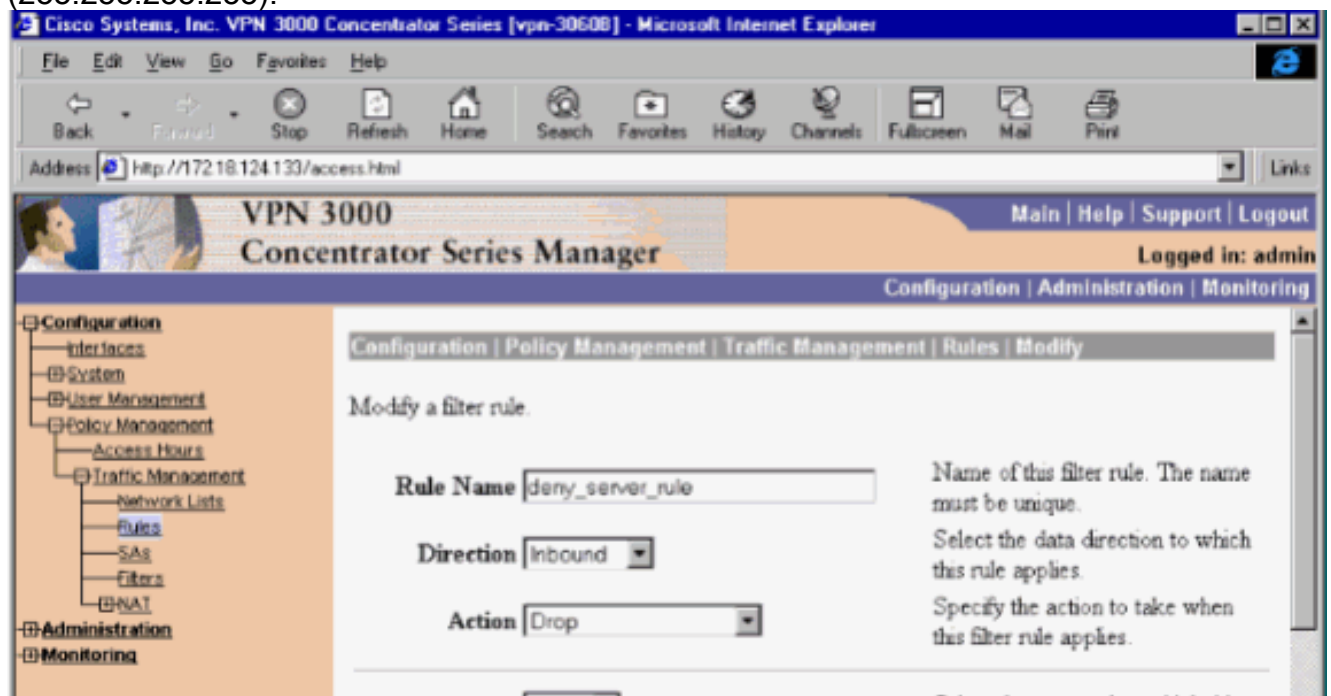
TCP Connection Select whether this rule should apply to an established TCP connection.

Source Address

Network List Specify the source network address list or the IP address and wildcard mask that this rule checks.



2. En la misma área, defina la segunda regla del concentrador VPN llamada **deny_server_rule** con estos valores por defecto: Dirección — **Entrante** Acción — **Descenso** Direcciones de origen y de destino cualquier cosa (255.255.255.255):



3. Elija el Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Filters (Filtros) y agregue su filtro del 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 | 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

Add Cancel

CISCO SYSTEMS

Internet zone

4. Agregue las dos reglas al 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. Elija el Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos) y aplique el filtro al 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 un túnel VPN de LAN a LAN](#)

Del 3.6 y posteriores del código del concentrador VPN, usted puede filtrar tráfico para cada túnel del IPSec VPN del LAN a LAN. Por ejemplo, si usted construye un túnel de LAN a LAN a otro concentrador VPN con el direccionamiento 172.16.1.1, y quiera permitir el acceso de 10.1.1.2 del host al túnel mientras que usted niega el resto del tráfico, usted puede aplicar el **filter_with_2_rules** cuando usted elige el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > LAN-to-LAN (LAN a LAN) > Modify (Modificar)** y selecciona el **filter_with_2_rules** bajo el 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

[Configuración de VPN 3000 – Asignación de filtro de RADIUS](#)

Es también posible definir un filtro en el concentrador VPN y entonces pasar abajo del número de filtro de un servidor de RADIUS (en los términos RADIUS, el atributo 11 es id del filtro), para cuando autentican al usuario en el servidor de RADIUS, asociar el id del filtro a esa conexión. En este ejemplo, la suposición es que la autenticación de RADIUS para los usuarios del concentrador VPN es ya operativa y solamente el id del filtro debe ser agregado.

Defina el filtro en el concentrador VPN como en el ejemplo anterior:

Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name

101

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

Default Action

Drop

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

Source Routing

Check to allow the filter to apply to source-routed packets.

Fragments

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

Description

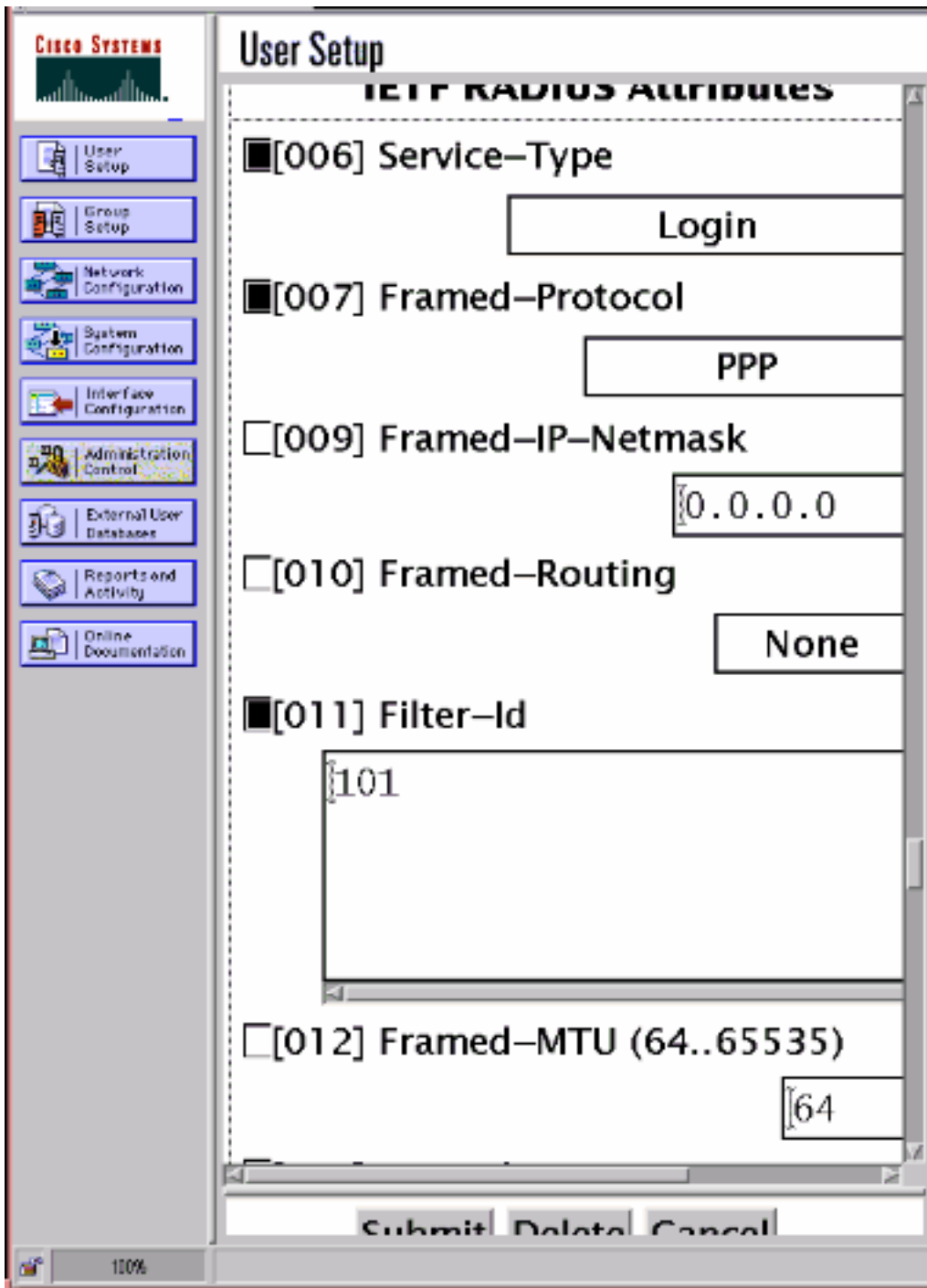
filter to allow access to 10.1.1.2

Apply

Cancel

[Configuración del servidor CSNT - Asignación de filtro de RADIUS](#)

Atributo 11 de la configuración, id del filtro en el servidor del Cisco Secure NT a ser 101:



Depuración – Asignación de filtro RADIUS

Si el AUTHDECODE (gravedad 1-13) está encendido en el concentrador VPN, el registro muestra que el servidor del Cisco Secure NT envía abajo del access-list 101 en el 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.....
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Para los propósitos de Troubleshooting solamente, usted puede girar el debugging del filtro cuando usted elige el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases)** y agrega la clase **FILTERDBG** con la **gravedad para registrar = 13**. En las reglas, cambie la acción predeterminada de delantero (o del descenso) **para remitir y para registrar** (o caer y registro). Cuando el registro de acontecimientos se extrae en el **Monitoring (Monitoreo) > Event Log (Registro de evento)**, debe mostrar las entradas por ejemplo:

```
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
```

Información Relacionada

- [Negociación IPSec/Protocolos IKE](#)
- [Preguntas frecuentes concentradoras VPN 3000](#)
- [Soporte a RADIUS](#)
- [Soporte del Cisco VPN 3000 Concentrator](#)
- [Soporte del Cliente Cisco VPN 3000](#)
- [Soporte del Cisco Secure ACS for Windows](#)
- [Request For Comments \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)