

Configuration du concentrateur Cisco VPN 3000 en vue de blocage à l'aide de filtres et d'affectations de filtre RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Conventions](#)

[Configuration VPN 3000](#)

[Filtres pour un tunnel VPN d'entre réseaux locaux](#)

[Configuration VPN 3000 - Affectation de filtres RADIUS](#)

[Configuration de serveur CSNT - Affectation de filtres RADIUS](#)

[Affectation de filtre de debug radius](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Dans cette configuration d'échantillon, nous voulons utiliser des filtres pour permettre à un utilisateur pour accéder à seulement un serveur (10.1.1.2) à l'intérieur du réseau et pour bloquer l'accès à toutes autres ressources. Le concentrateur de Cisco VPN 3000 peut être installé pour contrôler IPsec, Protocole PPTP (Point-to-Point Tunneling Protocol), et accès client L2TP aux ressources de réseau avec des filtres. Les filtres se composent des règles, qui sont semblables aux Listes d'accès sur un routeur. Si un routeur était configuré pour :

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

l'équivalent de concentrateur VPN serait d'installer un filtre avec des règles.

Notre première règle de concentrateur VPN est un **permit_server_rule**, qui est équivalent à l'**IP de l'autorisation du routeur n'importe quelle** commande de **10.1.1.2 d'hôte**. Notre deuxième règle de concentrateur VPN est un **deny_server_rule** qui est équivalent au routeur **refuse à IP n'importe quelle n'importe quelle** commande.

Notre filtre de concentrateur VPN est **filter_with_2_rules**, qui est équivalent à la liste d'accès du routeur 101 ; il utilise le **permit_server_rule** et le **deny_server_rule** (dans cette commande). On le suppose que les clients peuvent se connecter correctement avant d'ajouter des filtres ; ils reçoivent leurs adresses IP d'un groupe sur le concentrateur VPN.

Référez-vous à [PIX/ASA 7.x ASDM : Limitez l'accès au réseau des utilisateurs de l'Accès à distance VPN](#) afin de se renseigner plus sur le scénario où le bloc PIX/ASA 7.x l'accès des utilisateurs VPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

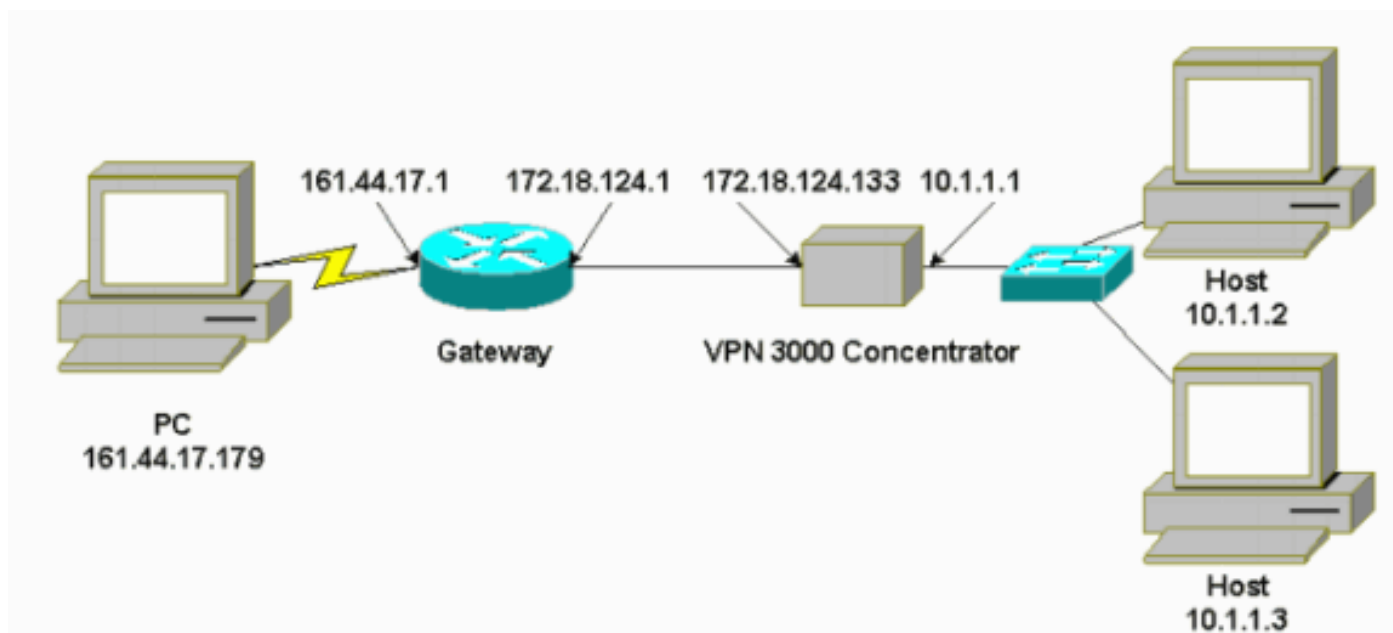
Composants utilisés

Les informations dans ce document sont basées sur la version 2.5.2.D de concentrateur de Cisco VPN 3000.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

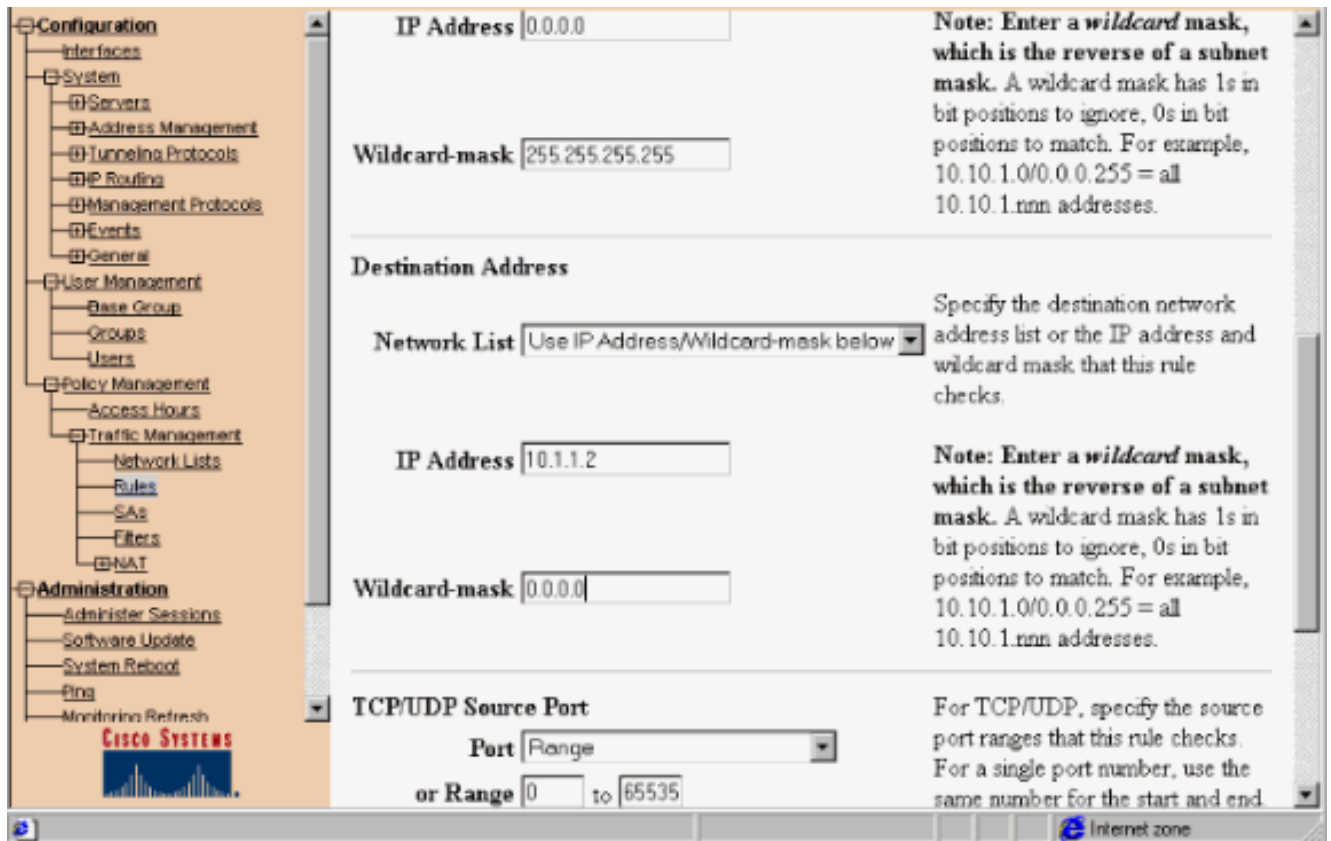
Configuration VPN 3000

Terminez-vous ces étapes afin de configurer le concentrateur VPN 3000.

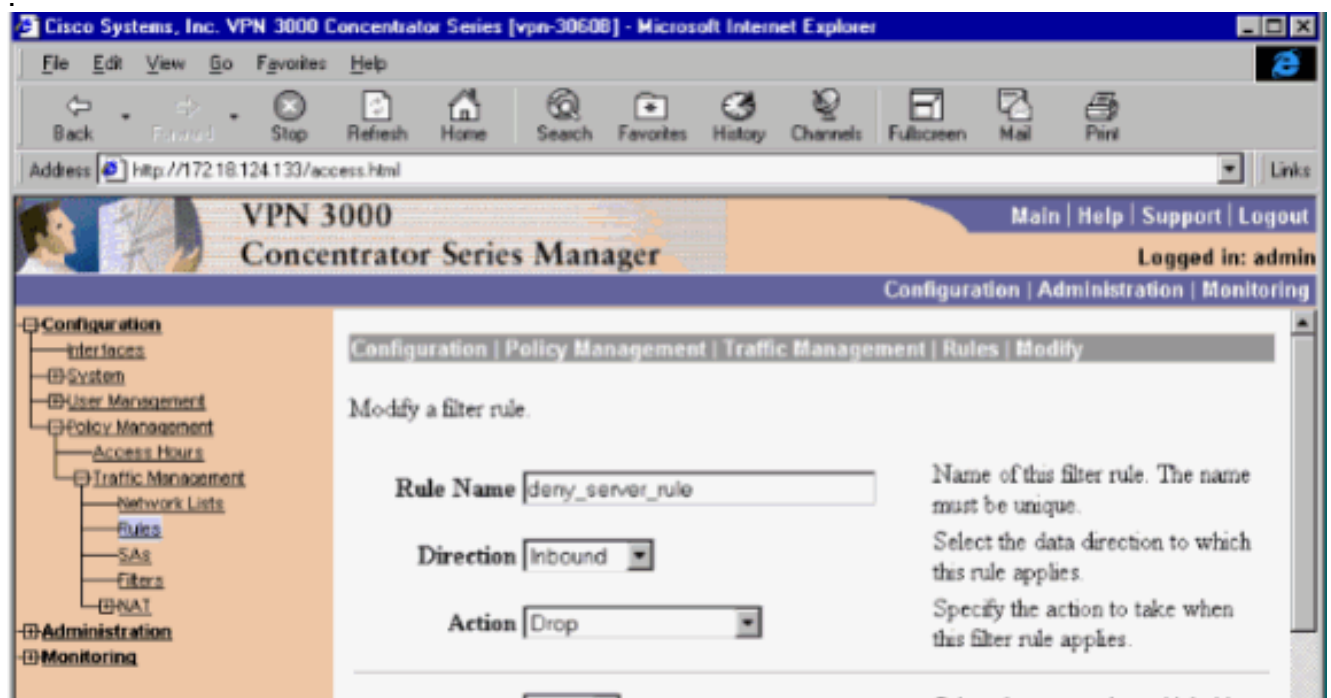
1. Choisissez la **Gestion > la gestion de trafic > les règles de >Policy de configuration > ajoutent** et définissent la première le **permit_server_rule** appelé de concentrateur VPN par règle avec ces configurations :
Direction — **D'arrivée**Action — **En avant**Adresse source — **255.255.255.255**Adresse de destination — **10.1.1.2**Masque de masque — **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 shows "Configuration | Administration | Monitoring". The left sidebar contains a tree view with categories like "Configuration", "User Management", "Policy Management", and "Administration". The main content area is titled "Configuration | Policy Management | Traffic Management | Rules | Add" and 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. Dans la même zone, définissez la deuxième règle de concentrateur VPN appelée **deny_server_rule** avec ces paramètres par défaut : Direction — **D'arrivée** Action — **Baisse** Source et adresses de destination de n'importe quoi (255.255.255.255)



3. Choisissez le Configuration > Policy Management > Traffic Management > Filters et ajoutez votre filtre **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

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

4. Ajoutez les deux règles à 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

5. Choisissez le **Configuration > User Management > Groups** et appliquez le filtre au groupe :

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

[Filtres pour un tunnel VPN d'entre réseaux locaux](#)

Du code 3.6 de concentrateur VPN et plus tard, vous pouvez filtrer le trafic pour chaque tunnel VPN d'IPsec d'entre réseaux locaux. Par exemple, si vous établissez un tunnel entre réseaux locaux à un autre concentrateur VPN avec l'adresse 172.16.1.1, et voulez permettre l'accès de 10.1.1.2 d'hôte au tunnel tandis que vous refusez tout autre trafic, vous peut appliquer **filter_with_2_rules** quand vous choisissez la **configuration > le système > les protocoles > l'IPSec > l'entre réseaux locaux de Tunnellisation > modifiez** et sélectionnez **filter_with_2_rules** sous le filtre.



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

[Configuration VPN 3000 - Affectation de filtres RADIUS](#)

Il est également possible de définir un filtre dans le concentrateur VPN et passer alors en bas du nombre de filtre d'un serveur de RAYON (en termes de RAYON, l'attribut 11 est Filtre-id), de sorte que quand l'utilisateur est authentifié sur le serveur de RAYON, le Filtre-id soit associé avec cette connexion. Dans cet exemple, la supposition est que l'authentification de RAYON pour des utilisateurs de concentrateur VPN est déjà opérationnelle et seulement le Filtre-id doit être ajouté.

Définissez le filtre sur le concentrateur VPN comme dans l'exemple précédent :

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 apply to source-routed packets.

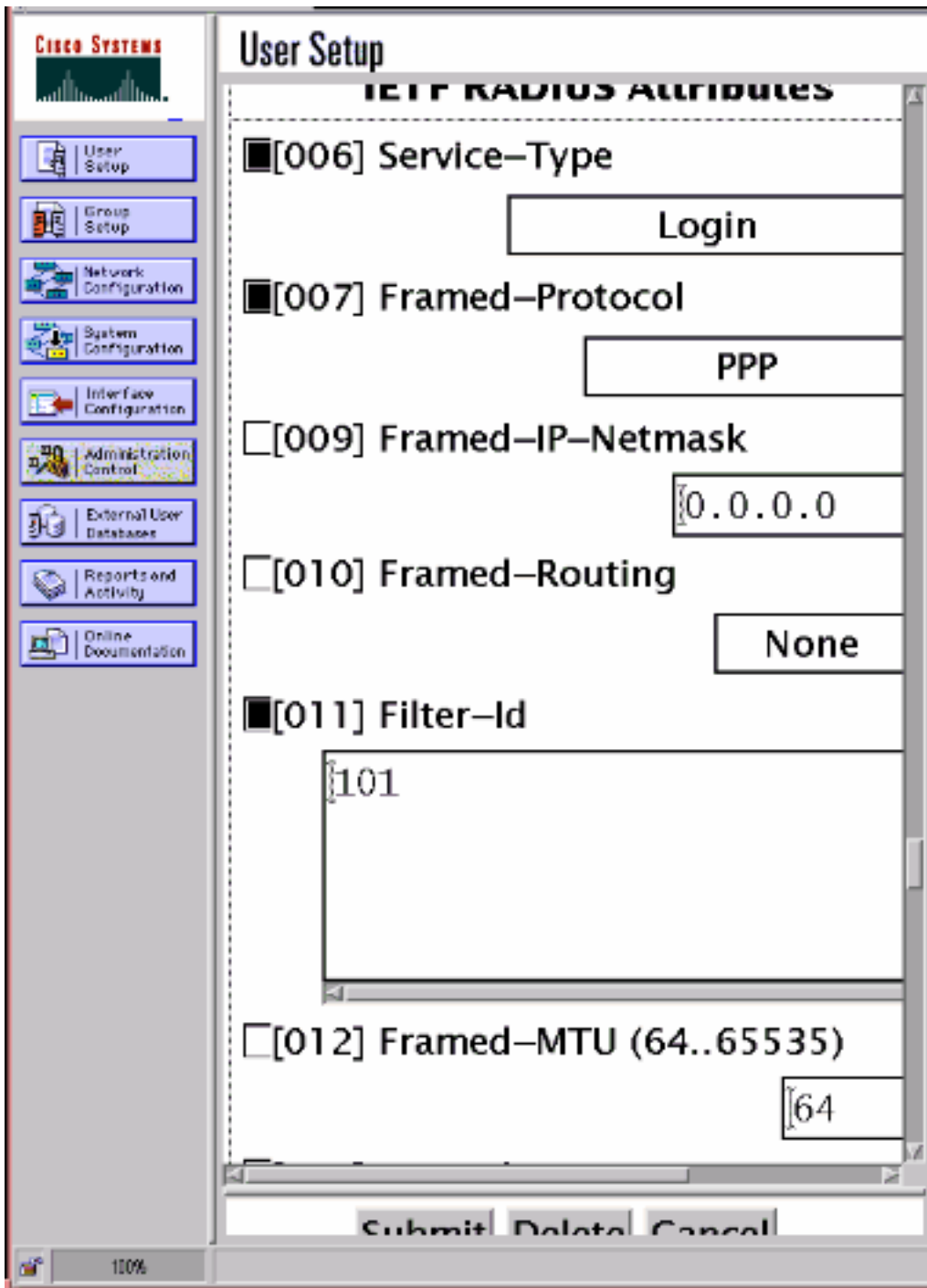
Fragments

Check to allow the filter to apply to IP packet fragments.

Description

[Configuration de serveur CSNT - Affectation de filtres RADIUS](#)

Configurez l'attribut 11, Filtre-id sur le serveur NT Cisco Secure pour être 101 :



[Affectation de filtre de debug radius](#)

Si AUTHDECODE (sévérité 1-13) est en fonction dans le concentrateur VPN, le log prouve que le serveur NT Cisco Secure envoie en bas de la liste d'accès 101 dans l'attribut 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.....
```

[Vérifiez](#)

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Pour dépannage des butts seulement, vous pouvez activer l'élimination des imperfections de filtre quand vous choisissez la **configuration > le système > les événements > les classes** et ajoutez la classe **FILTERDBG** avec la **sévérité pour se connecter = 13**. Dans les règles, changez l'action par défaut d'en avant (ou de la baisse) **d'expédier et se connecter** (ou relâcher et log). Quand le journal d'événements est récupéré à la **surveillance > au journal d'événements**, il devrait des shows entry comme :

```
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
```

Informations connexes

- [Négociation IPSec/Protocoles IKE](#)
- [Forums aux questions de concentrateur VPN 3000](#)
- [Prise en charge de RADIUS](#)
- [Support de concentrateur de Cisco VPN 3000](#)
- [Support de Cisco VPN 3000 Client](#)
- [Cisco Secure ACS pour le support de Windows](#)
- [Request For Comments \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)