

フィルタおよび RADIUS フィルタ割り当てを使用するブロッキングのためのCisco VPN 3000 コンセントレータの設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[VPN 3000 の設定](#)

[LAN-to-LAN VPN トンネルのためのフィルタ](#)

[VPN 3000 の設定 : RADIUS フィルタの割り当て](#)

[CSNT サーバの設定 : RADIUS フィルタの割り当て](#)

[デバッグ : RADIUS フィルタの割り当て](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この設定例では、ユーザにネットワーク内の 1 つのサーバ (10.1.1.2) のみへのアクセスを許可し、その他のすべてのリソースへのアクセスをブロックするためにフィルタを使用する必要があります。Cisco VPN 3000 コンセントレータは、ネットワーク リソースへの IPSec、ポイントツーポイント トンネリング プロトコル (PPTP)、L2TP クライアントのアクセスを制御するように、フィルタを使用して設定できます。フィルタは、ルータのアクセス リストのようなルールから構成されます。ルータが次のように設定されている場合、

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

同等の VPN コンセントレータがルールのあるフィルタを設定します。

最初の VPN コンセントレータのルールは `permit_server_rule` であり、ルータの `permit ip any host 10.1.1.2` コマンドと同等です。2 番目の VPN コンセントレータのルールは `deny_server_rule` であり、ルータの `deny ip any any` コマンドと同等です。

VPN コンセントレータのフィルタは `filter_with_2_rules` であり、ルータの 101 アクセス リストと同等です。`permit_server_rule` と `deny_server_rule` を (この順序で) 使用しています。クライアントがフィルタを追加する前に適切に接続できていることが想定されています。IP アドレスを VPN コンセントレータのプールから受信します。

PIX/ASA 7.x が VPN ユーザからのアクセスをブロックするシナリオの詳細については、『[PIX/ASA 7.x ASDM：リモートアクセス VPN ユーザのネットワークアクセスの制限](#)』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

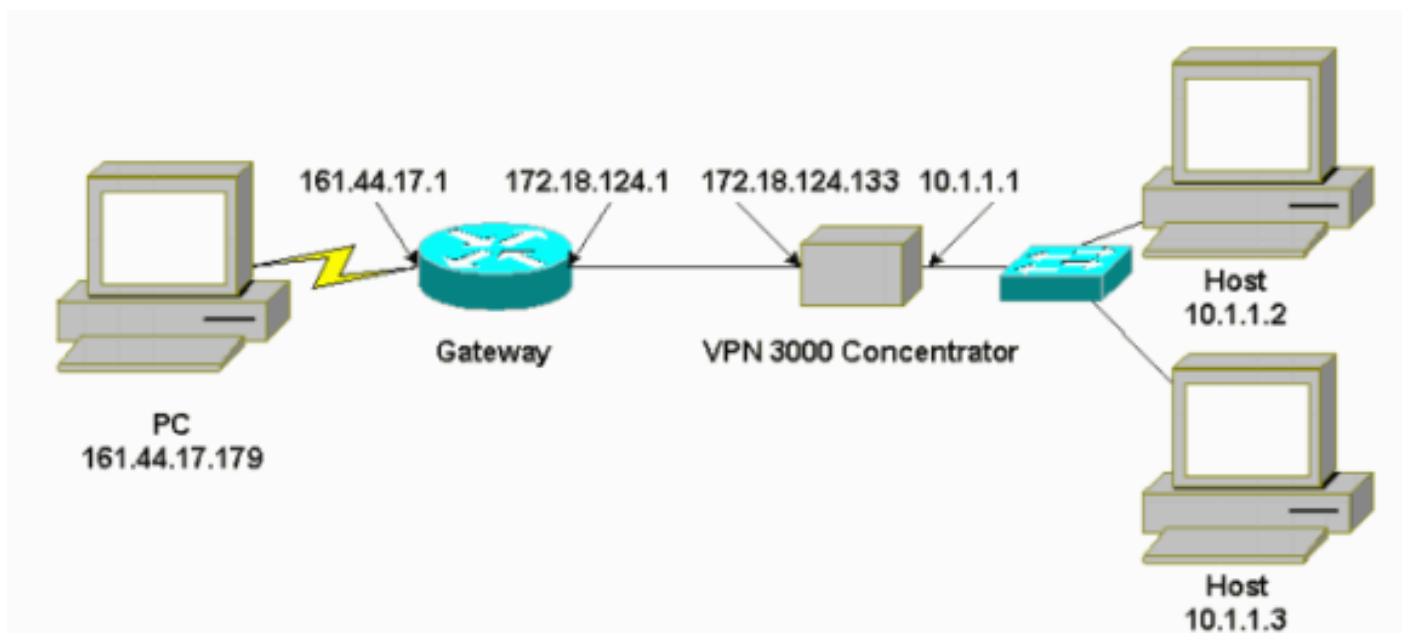
使用するコンポーネント

このドキュメントの情報は、Cisco VPN 3000 コンセントレータ バージョン 2.5.2.D に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

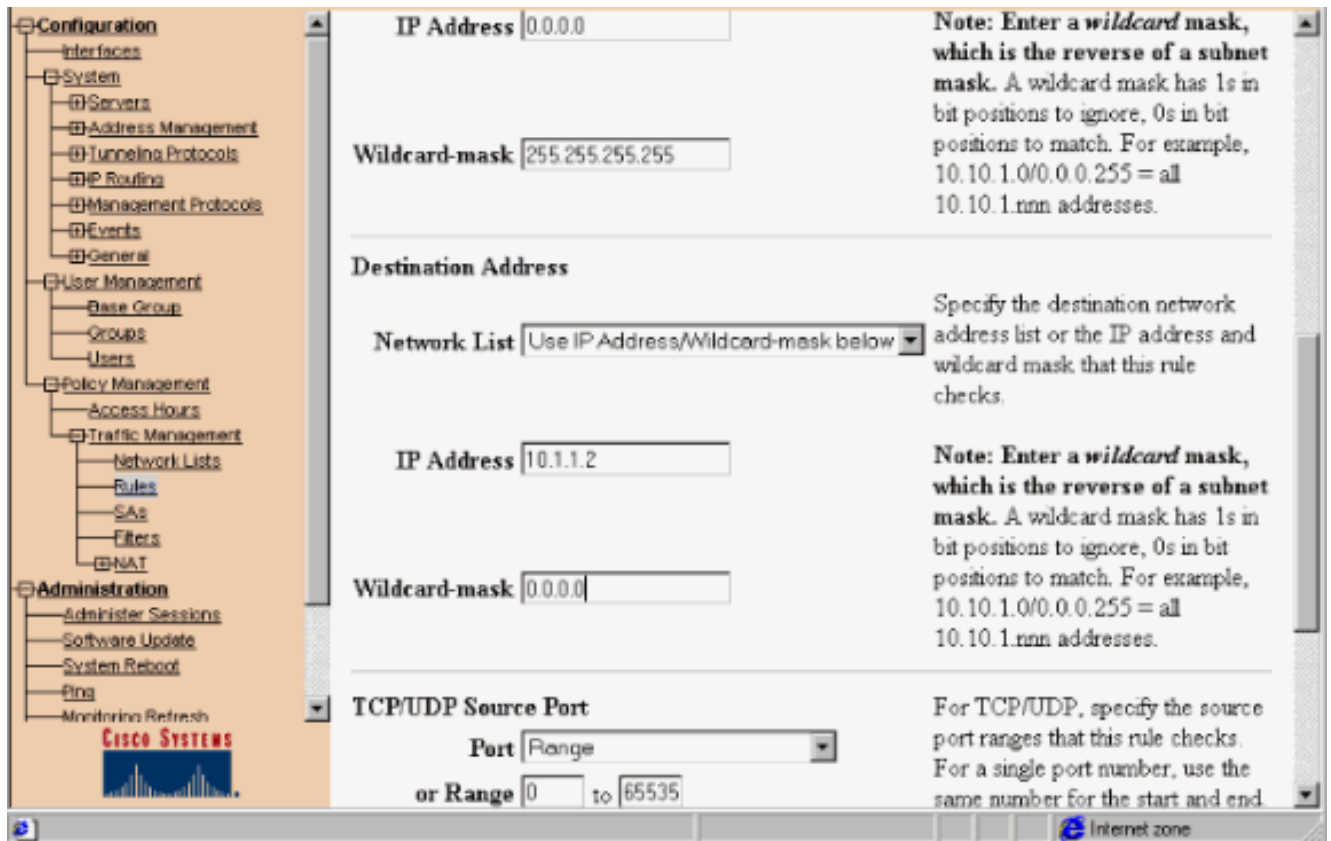
VPN 3000 の設定

VPN 3000 コンセントレータを設定するには、次の手順を実行します。

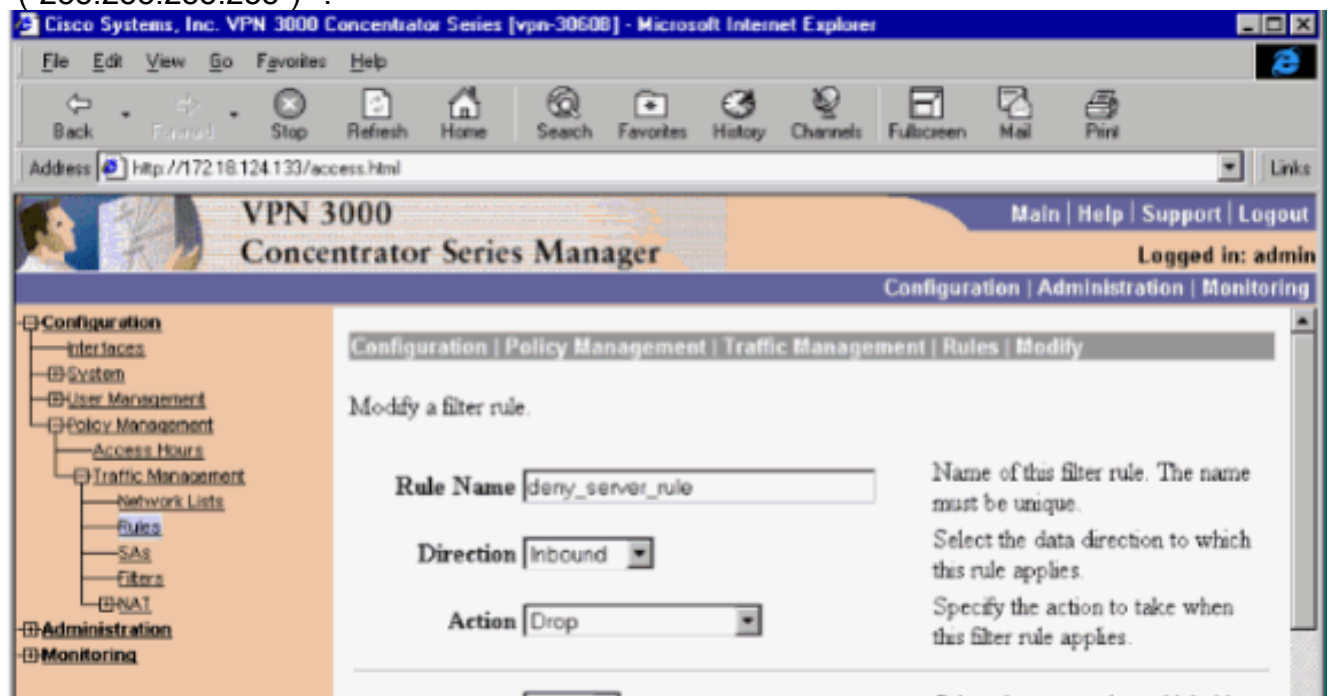
1. [Configuration] > [Policy Management] > [Traffic Management] > [Rules] > [Add] の順に選択し、以下の設定で、**permit_server_rule** という最初の VPN コンセントレータのルールを定義します。[Direction] : [Inbound][Action] : [Forward][Source Address] : [255.255.255.255][Destination Address] : [10.1.1.2][Wildcard Mask] : [0.0.0.0]

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 has a tree view with "Configuration" expanded, showing "Policy Management" > "Traffic Management" > "Rules" > "Add". 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. 同じエリアで、以下のデフォルトを使用して、**deny_server_rule** という 2 番目の VPN コンセントレータのルールを定義します。[Direction] : [Inbound][Action] : [Drop]すべての送信元と宛先のアドレス (255.255.255.255) :



3. [Configuration] > [Policy Management] > [Traffic Management] > [Filters] を選択し、**filter_with_2_rules** フィルタを追加します。

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

4. 2つのルールを filter_with_2_rules に追加します。

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. [Configuration] > [User Management] > [Groups] を選択し、フィルタをグループに適用します。

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

LAN-to-LAN VPN トンネルのためのフィルタ

VPN コンセントレータ コード 3.6 以降から、各 LAN-to-LAN IPsec VPN トンネルのトラフィックをフィルタできます。たとえば、アドレスが 172.16.1.1 の別の VPN コンセントレータへの LAN-to-LAN トンネルを構築して、ホスト 10.1.1.2 がトンネルにアクセスするのを許可し、ほかのトラフィックはすべて拒否する場合、[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [LAN-to-LAN] > [Modify] を選択し、[Filter] で filter_with_2_rules をで選択すると、filter_with_2_rules を適用できます。



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 の設定 : RADIUS フィルタの割り当て

VPN コンセントレータでフィルタを定義して、RADIUS サーバからフィルタ番号を渡し (RADIUS の用語では属性 11 がフィルタ ID)、ユーザが RADIUS サーバで認証されたときにフィルタ ID がその接続と関連付けられるようにすることもできます。この例では、VPN コンセントレータのユーザの RADIUS 認証がすでに運用され、フィルタ ID のみが追加されることを前提としています。

前の例のように、VPN コンセントレータのフィルタを定義します。

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 source-routed packets.

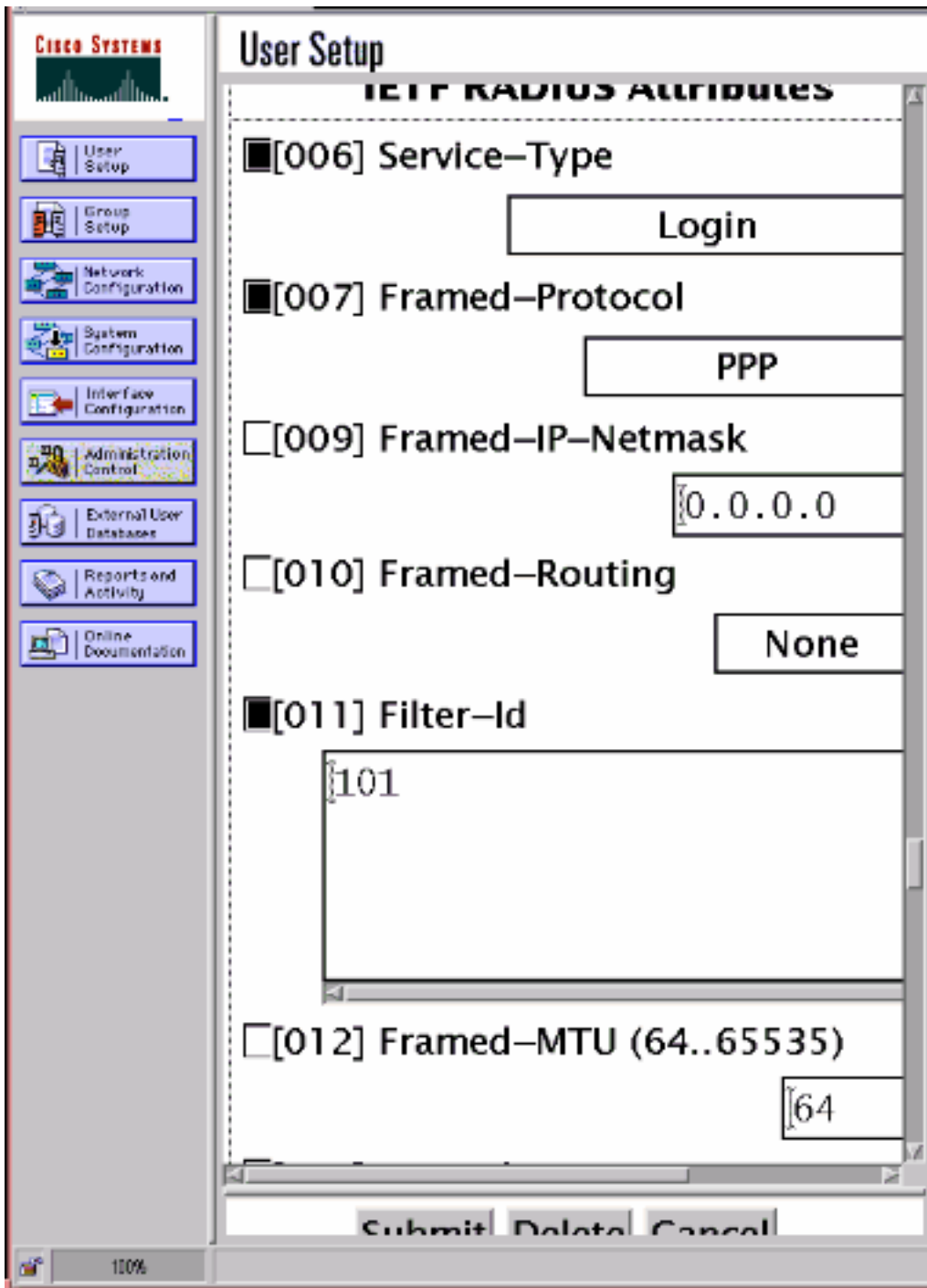
Fragments

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

Description

[CSNT サーバの設定 : RADIUS フィルタの割り当て](#)

Cisco Secure NT サーバのフィルタ ID である属性 11 を 101 に設定します。



デバッグ : RADIUS フィルタの割り当て

AUTHDECODE (1 ~ 13 の重大度) が VPN コンセントレータでオンになっている場合、Cisco Secure NT サーバが属性 11 (0x0B) でアクセス リスト 101 を送信していることがログから分かります。

```
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.....
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

トラブルシューティングのみを目的としている場合は、[Configuration] > [System] > [Events] > [Classes] を選択し、**Severity to Log = 13** を指定して FILTERDBG クラスを追加するときに、フィルタのデバッグをオンにできます。ルールでは、デフォルトのアクションを [Forward] (または [Drop]) から [Forward and Log] (または [Drop and Log]) に変更します。イベント ログが [Monitoring] > [Event Log] で取得された場合、次のようなエントリが表示されます。

```
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
```

関連情報

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [VPN 3000 コンセントレータに関してよく寄せられる質問 \(FAQ\)](#)
- [RADIUS のサポート](#)
- [Cisco VPN 3000 コンセントレータのサポート](#)
- [Cisco VPN 3000 クライアントのサポート](#)
- [Cisco Secure ACS for Windows のサポート](#)
- [Request for Comments \(RFC\)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)