

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ー](#)

[VPN 3000 の設定 - RADIUS フィルタ割り当て](#)

[CSNT サーバ設定 - RADIUS フィルタ割り当て](#)

[デバッグ - RADIUS フィルタ割り当て](#)

[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ー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、フィルターを使用して設定できます。フィルターは、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
```

VPN コンセントレータ等量はルールのフィルタを設定することです。

最初 VPN コンセントレータ ルールはルータの割り当て IP と同等ホスト 10.1.1.2 あらゆるコマンドの `permit_server_rule` です。第 2 VPN コンセントレータ ルールはルータの `deny ip any any` コマンドと同等の `deny_server_rule` です。

VPN コンセントレータ フィルタはルータ 101 のアクセス リストと同等の `filter_with_2_rules` です、;それは `permit_server_rule` および `deny_server_rule` を使用します (その順序で)。クライアントがフィルターを追加する前にきちんと接続できることが仮定されます;それらは VPN コンセントレータのプールから IP アドレスを受け取ります。

リモート アクセス サーバの設定方法とアクセスの制限方法については、『[PIX/ASA 7.x ASDM : シナリオについて詳細を学ぶためにリモートアクセス VPN ユーザのネットワークアクセスを PIX/ASA 7.x ブロック VPN ユーザからアクセス制限しなさい](#)』。

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。

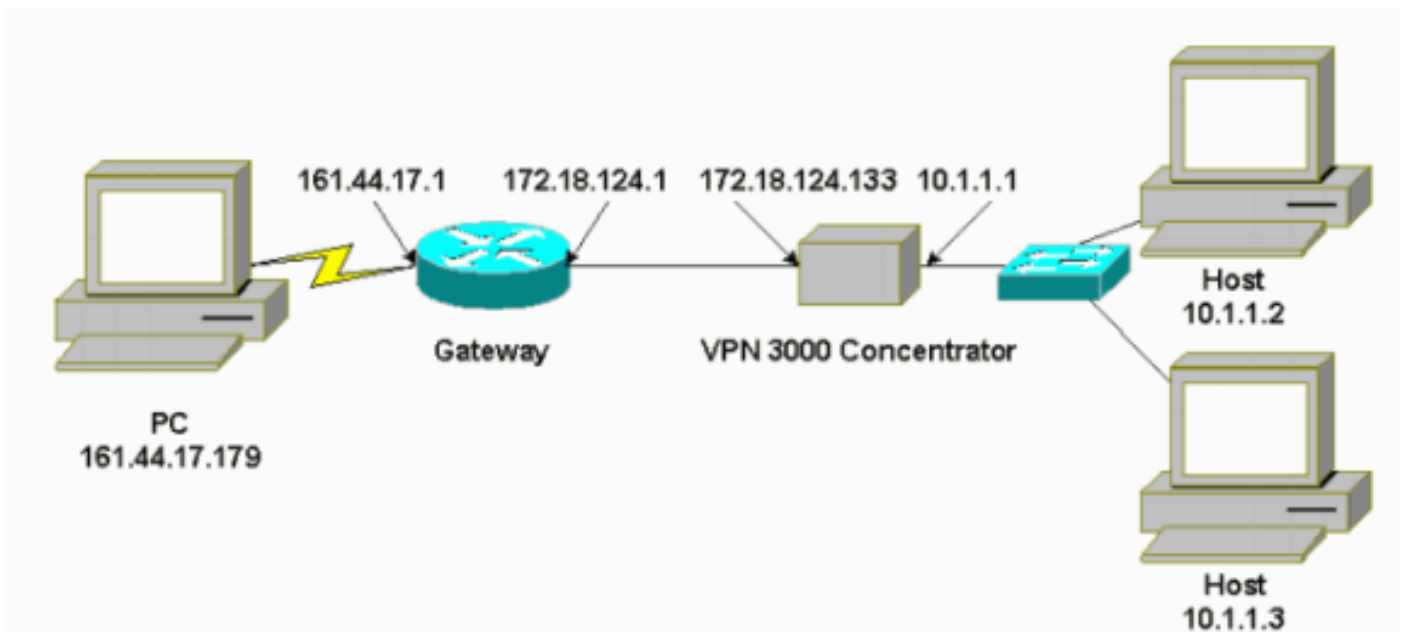
使用するコンポーネント

この文書に記載されている情報は Cisco VPN 3000 コンセントレータ バージョン 2.5.2.D に基づいています。

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ためにこれらのステップを完了して下さい。

1. >Policy 管理 > Traffic Management > ルール > Add を『Configuration』を選択し、これらの設定が付いている最初の VPN コンセントレータ ルールによって呼出される `permit_server_rule` を定義して下さい:方向か。Inbound処理か。転送送信元アドレスか。255.255.255.255宛先アドレスか。10.1.1.2ワイルドカード マスクか。0.0.0.0

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - 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

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

TCP Connection

Source Address

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

IP Address **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**

Wildcard-mask

Destination Address

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

IP Address **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**

Wildcard-mask

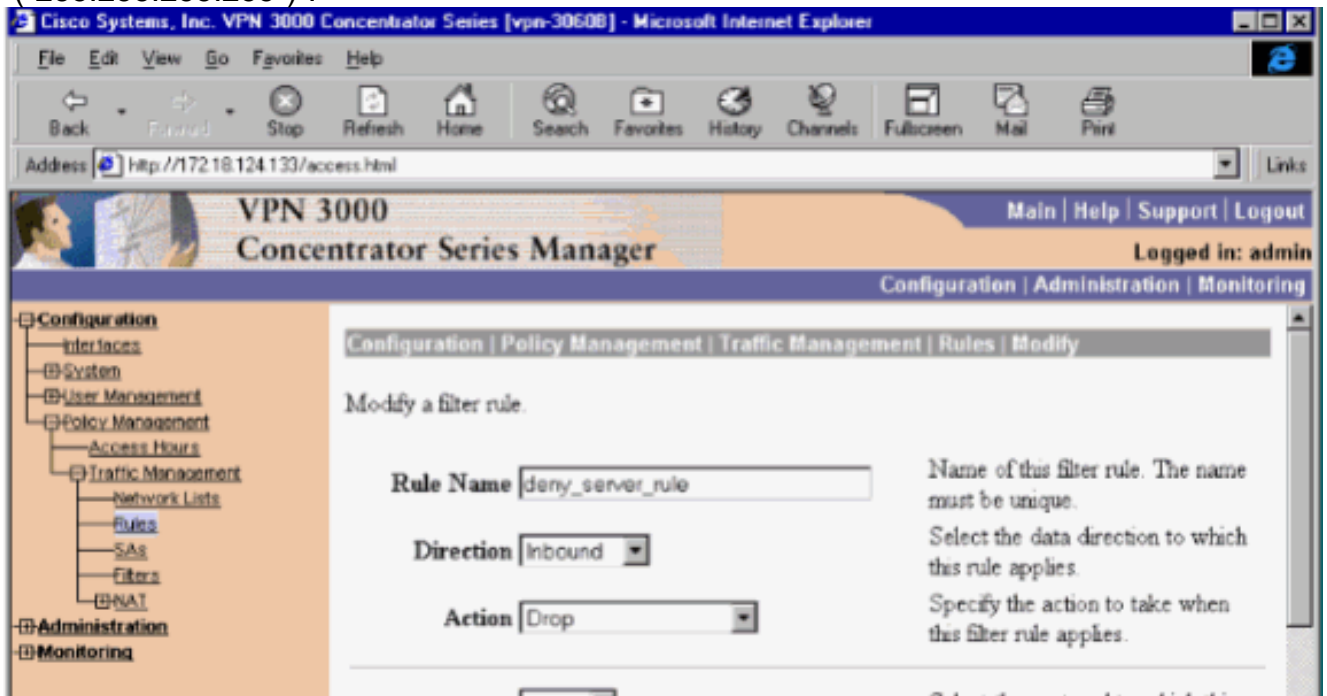
TCP/UDP Source Port

Port For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.

or Range to

2. 同じエリアでは、第2 VPN コンセントレーター ルールを呼出されたこれらのデフォルトの deny_server_rule 定義して下さい:方向が。Inbound処理か。[Drop]何でもの送信元 および 宛先アドレス

(255.255.255.255) :



3. > フィルタ Configuration > Policy Management > Traffic Management の順に選択し、filter_with_2_rules フィルタを追加して下さい。

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. filter_with_2_rules に 2 つのルールを追加して下さい

:

Configuration | Administration | Monitoring

Save Needed

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) |

5. グループにフィルタを Configuration > User Management > Groups の順に選択し、適用して下さい

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ー

VPN コンセントレータ コード 3.6 および それ以降から、各々の LAN-to-LAN な IPSec VPN トンネルのためのフィルタ トラフィックできます。たとえばアドレス 172.16.1.1 の別の VPN コンセントレータに LAN-to-LAN トンネルを構築したら、他のトラフィックをすべて拒否する間、**フィルタ**の下で **filter_with_2_rules** を Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify の順に選択し、選択するとき、**filter_with_2_rules** を適用できますトンネルにホスト 10.1.1.2 アクセスを許可したいと思えば。



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フィルタ割り当て

、フィルタid がその接続と関連付けられるように、VPN コンセントレータのフィルタを定義することもまた可能性のあるであり、ユーザが RADIUSサーバで認証される時 RADIUSサーバからのフィルタ番号の下でそれから渡るため (RADIUS 用語で、アトリビュート 11 はフィルタid です)。この例では、想定は VPN コンセントレータ ユーザ向けの RADIUS認証が既に正常に動作して、フィルタid だけ追加されるべきであることです。

VPN コンセントレータ 次のフィルタを前例定義して下さい:

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 through the network.

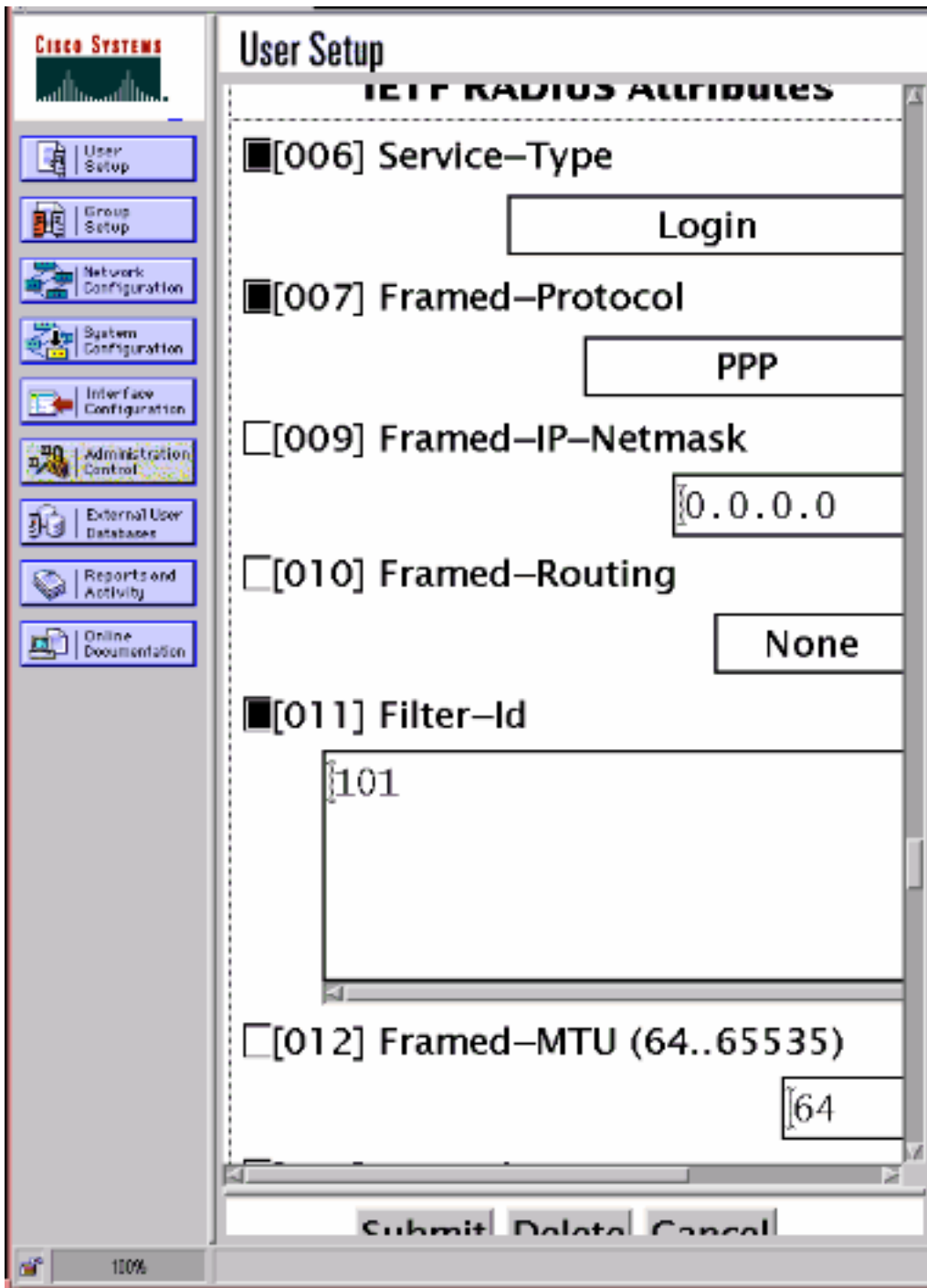
Fragments

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

Description

[CSNTサーバ設定 - RADIUSフィルタ割り当て](#)

101 であるためにアトリビュート 11 を、Cisco Secure NT サーバのフィルタid 設定して下さい:



[デバッグ - RADIUSフィルタ割り当て](#)

AUTHDECODE が (1-13 重大度) VPN コンセントレータにオンになっている場合、ログは Cisco Secure NT サーバがアトリビュート 11 (0x0B) の access-list 101 の下で送信 することを示します:

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=2280000: 020C002B 768825C5 C29E439F 4C8A727A
...+v.%...C.L.rz0010: 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

= 13 を記録するために重大度の FILTERDBG クラスを Configuration > System > Events > Classes の順に選択し、追加するときトラブルシューティングを行うのにただ、デバッグしているフィルタをつけることができます。ルールでは、転送し、記録する前方(カドロップする)からデフォルトアクションを変更して下さい(または廃棄するためおよびログ)。イベントログは Monitoring > Event Log で取得されるとき、エントリを示す必要があります(以下を参照):

```
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 FAQ](#)
- [RADIUSサポート](#)
- [Cisco VPN 3000 コンセントレータのサポート](#)
- [Cisco VPN 3000 Client サポート](#)
- [Cisco Secure ACS for Windows サポート](#)
- [Requests for Comment \(RFC \)](#) 
- [テクニカルサポートとドキュメント - Cisco Systems](#)