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
```

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。

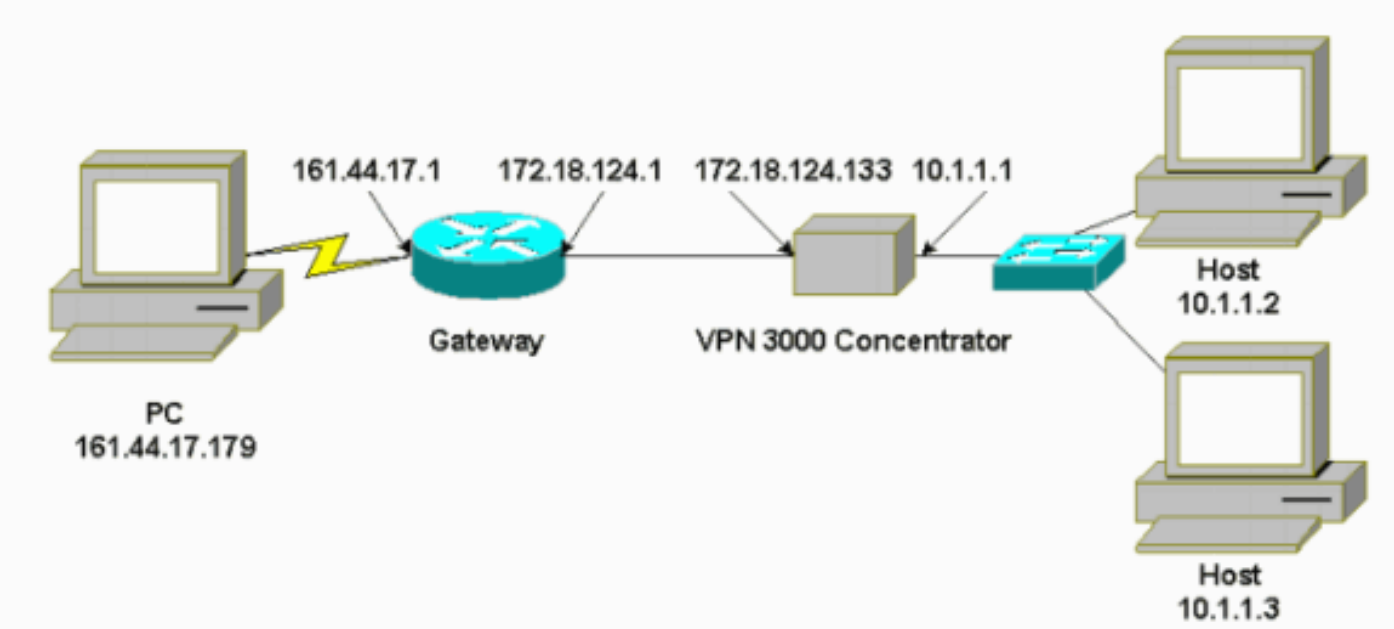
使用するコンポーネント

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。



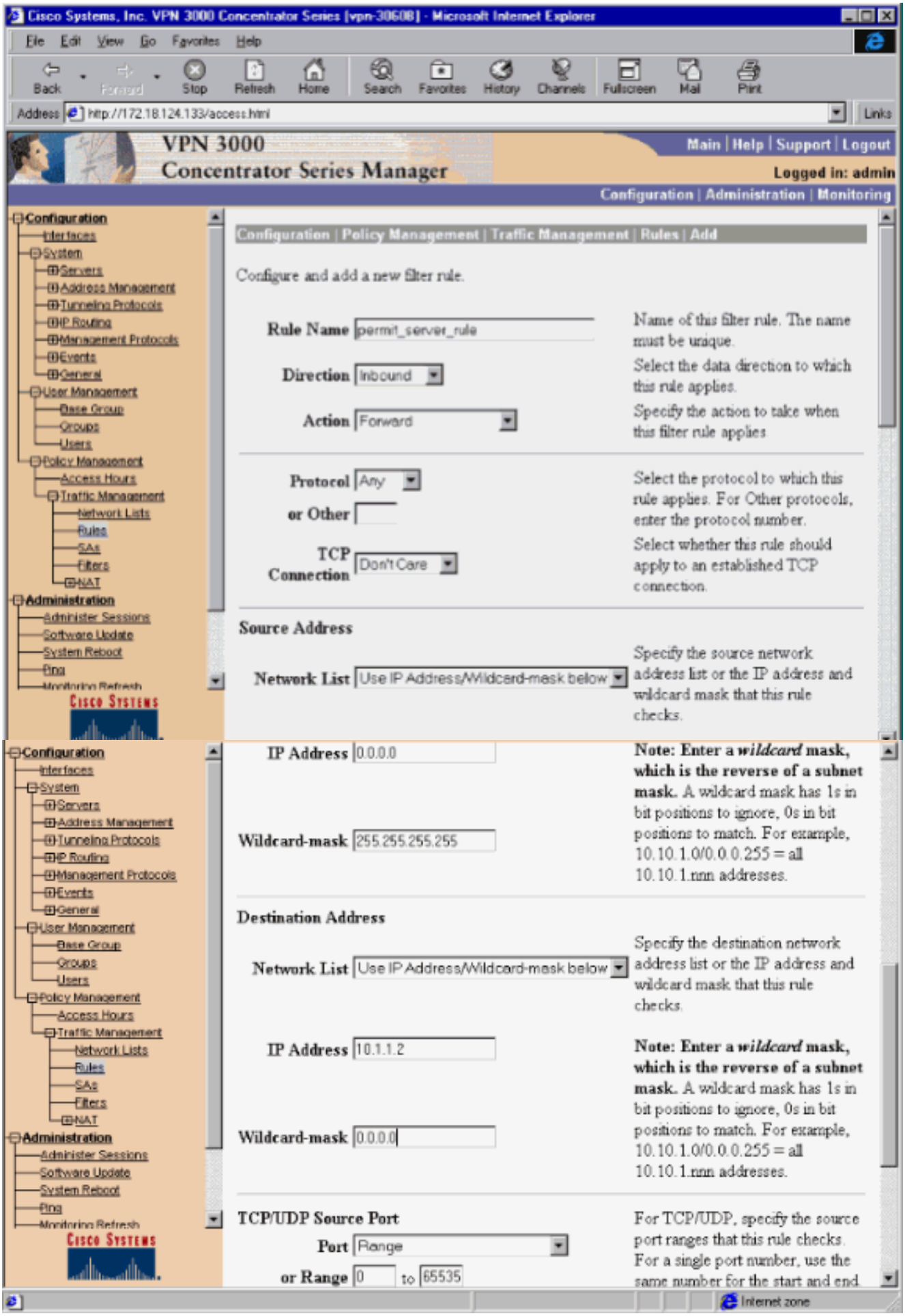
表記法

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

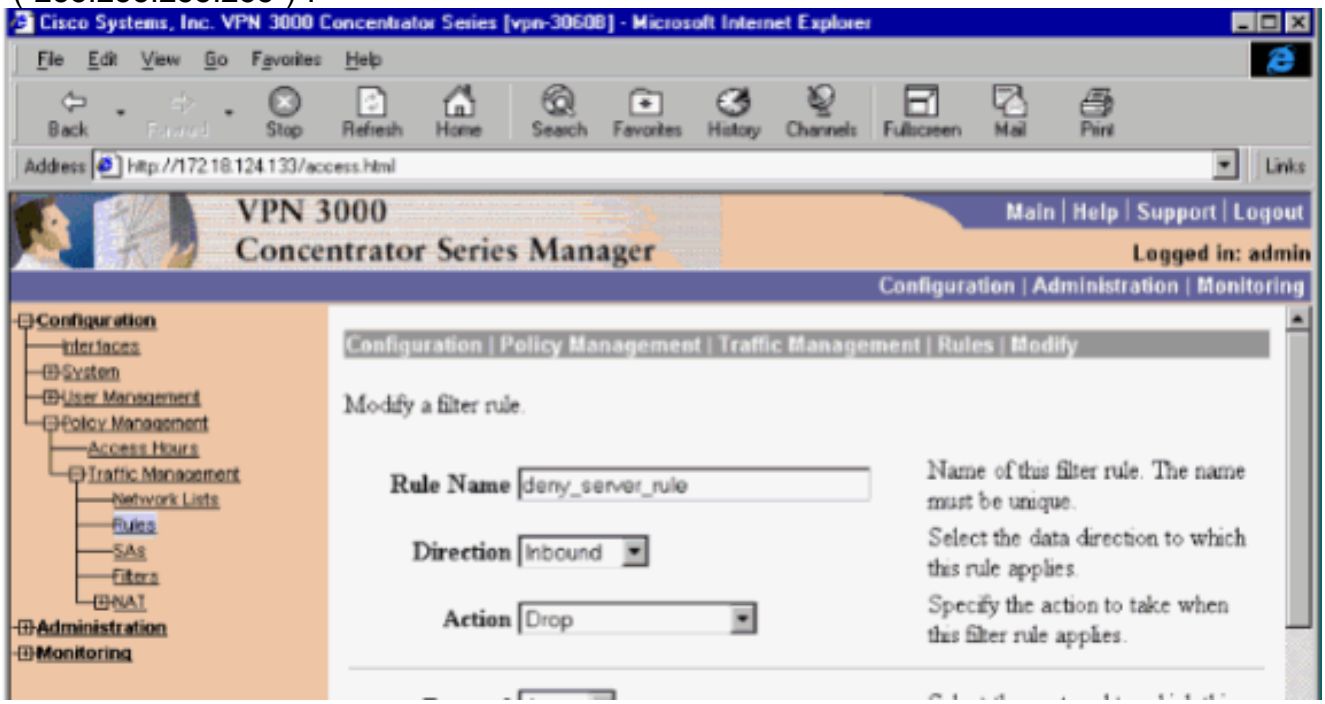
VPN 3000 コンセントレータを設定するためにこれらのステップを完了して下さい。

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**

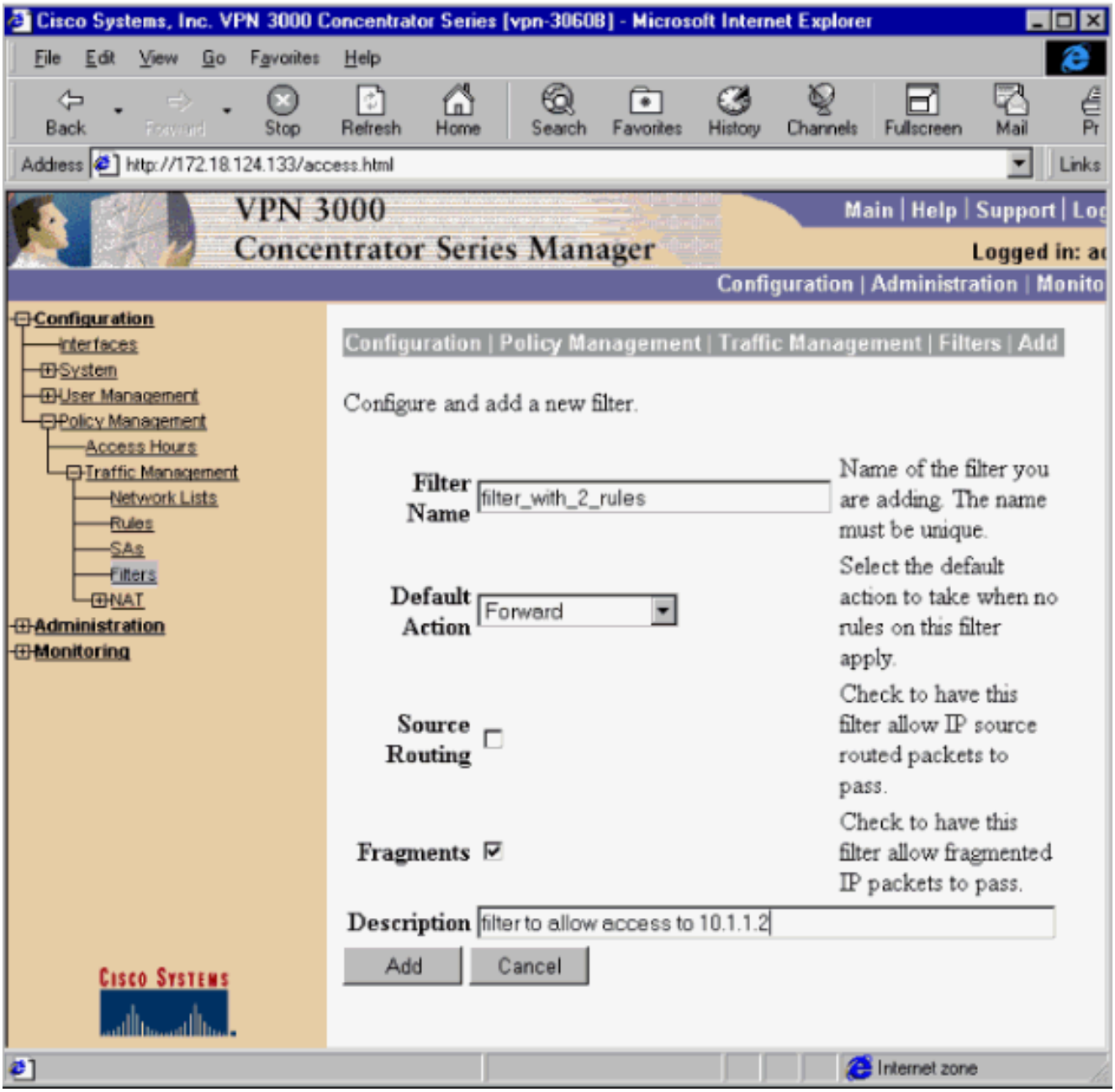


2. 同じエリアでは、第 2 VPN コンセントレータ ルールを呼出されたこれらのデフォルトの **deny_server_rule** 定義して下さい:方向か。**Inbound**処理か。**[Drop]**何でもの送信元 および 宛先アドレス

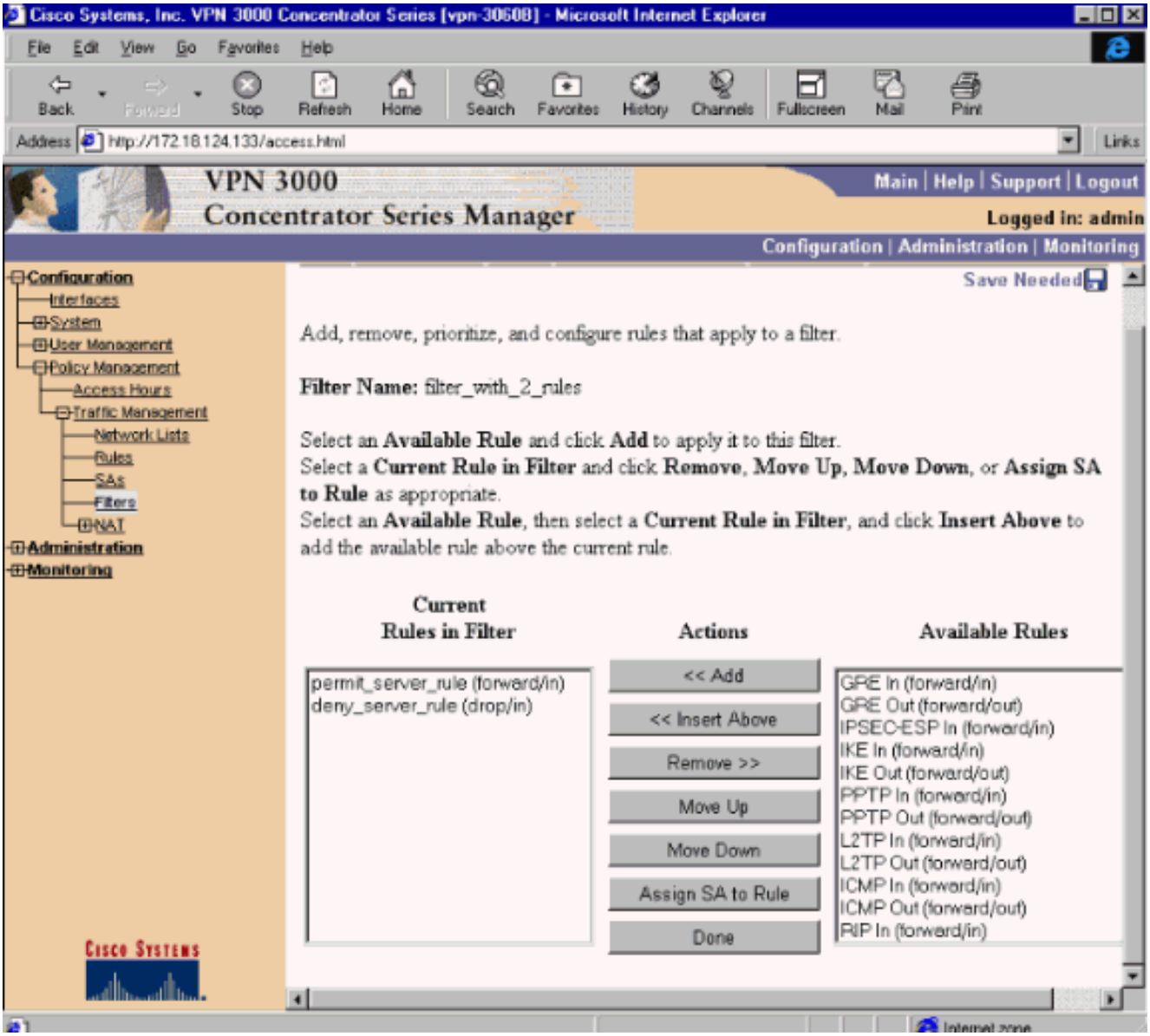
（255.255.255.255）：



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。



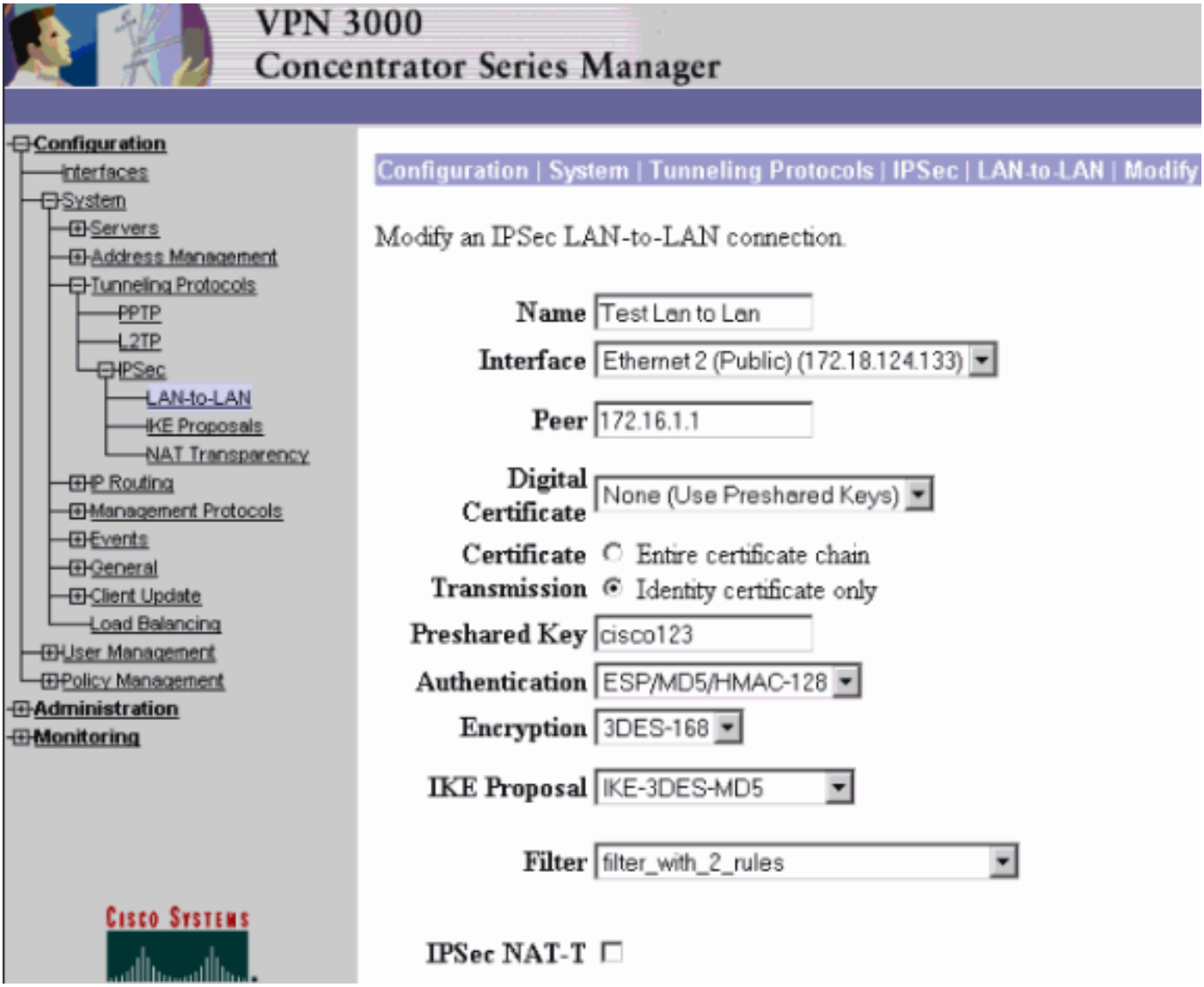
4. filter_with_2_rules に 2 つのルールを追加して下さい
   :



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
:

LAN-to-LAN VPN トンネルのためのフィルター

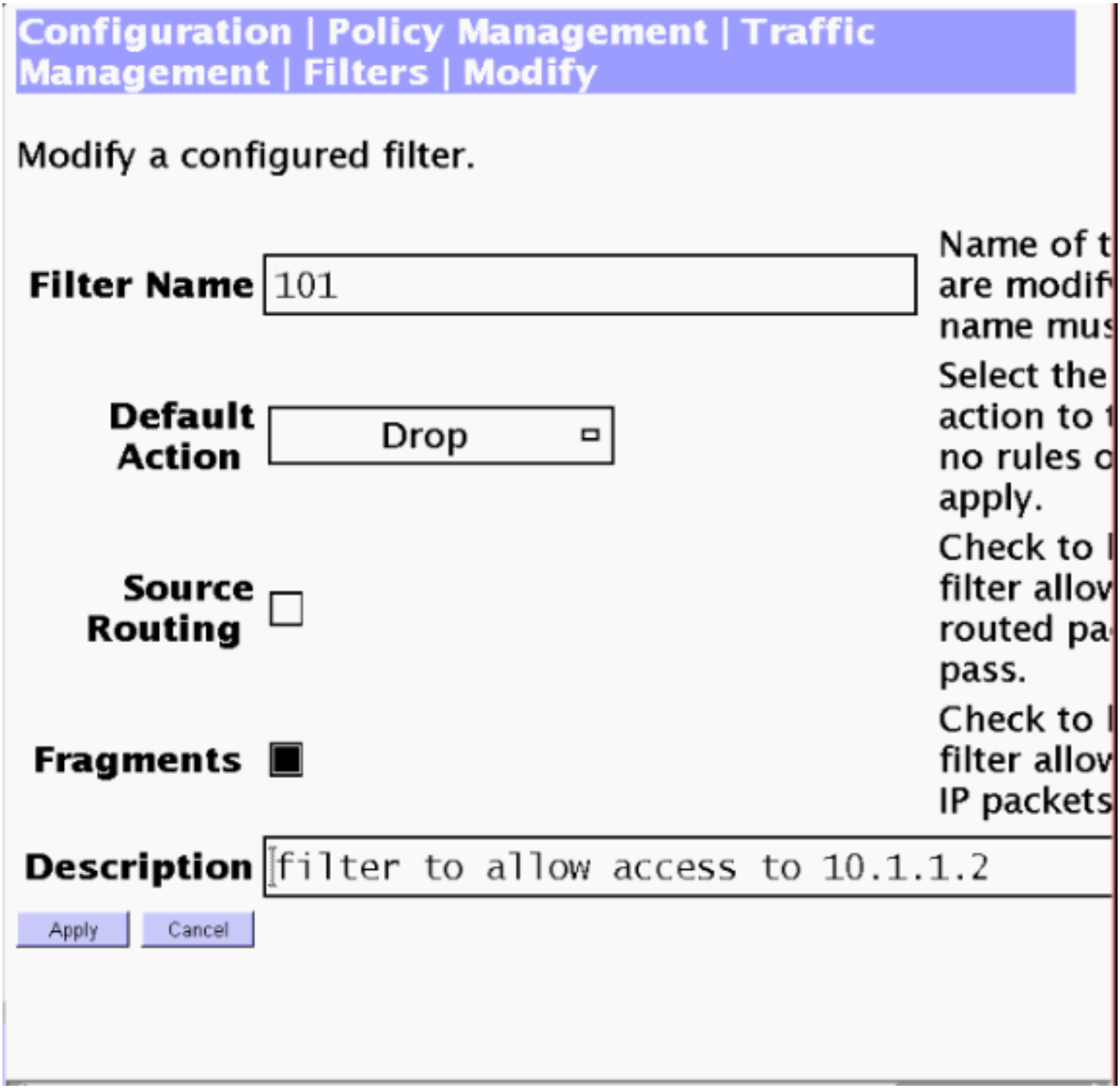
VPN コンセントレータ コード 3.6 および それ以降から、各々の LAN-to-LAN な IPSec VPN トンネルのためのフィルタ トラフィックできます。 たとえばアドレス 172.16.1.1 の別の VPN コンセントレータに LAN-to-LAN トンネルを構築したら、他のトラフィックをすべて拒否する間、**フィルタ**の下で **filter_with_2_rules を** Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify の順に選択 し、選択するとき、**filter_with_2_rules 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 の設定 - RADIUSフィルタ割り当て

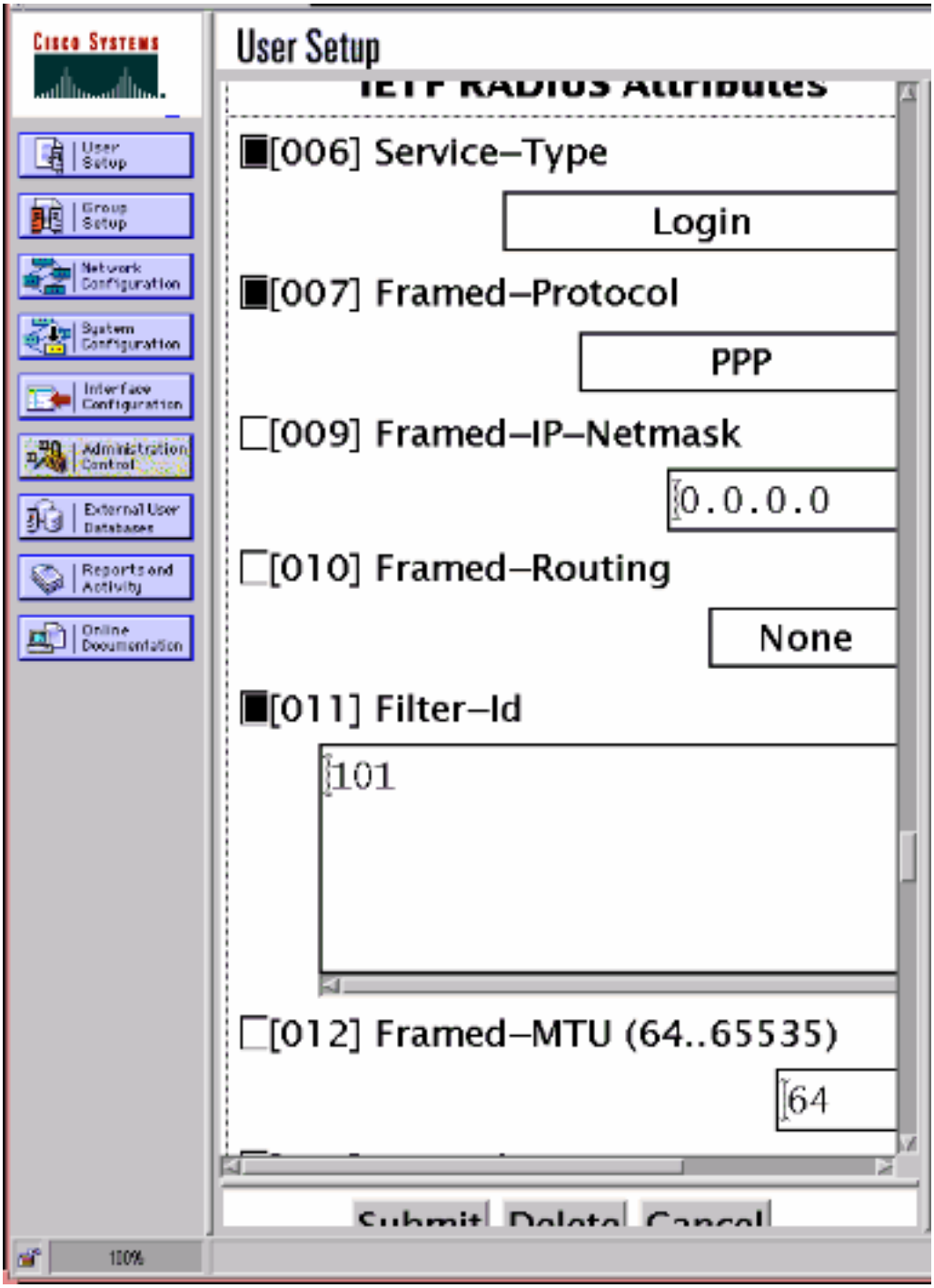
、フィルタid がその接続と関連付けられるように、VPN コンセントレータのフィルタを定義することもまた可能性のあるであり、ユーザが RADIUSサーバで認証される時 RADIUSサーバからのフィルタ番号の下でそれから渡るため (RADIUS 用語で、アトリビュート 11 はフィルタid です) 。 この例では、想定は VPN コンセントレータ ユーザ向けの RADIUS認証が既に正常に動作して、フィルタid だけ追加されるべきであることです。

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:



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 FFFFFF                  ..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（かドロップする）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口グ）。 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 8222 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