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

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しては個別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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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]**
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。
4. 2 つのルールを filter_with_2_rules に追加します。
5. [Configuration] > [User Management] > [Groups] を選択し、フィルタをグループに適用します。

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 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。

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口グから分かります。

```
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 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

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