ASA/PIX： ASA で VPN クライアントのスプリット トンネリングを許可するための設定例

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
関連製品
表記法
背景説明
ASA でのスプリット トンネリングの設定
Adaptive Security Device Manager (ASDM) 5.x による ASA 7.x の設定
Adaptive Security Device Manager (ASDM) 6.x による ASA 8.x の設定
CLI による ASA 7.x 以降の設定
CLI による PIX 6.x の設定
確認
VPN Client を使用した接続
VPN Client ログの表示
Ping によるローカル LAN アクセスのテスト
トラブルシューティング
スプリット トンネル ACL でのエントリ数の制限
関連情報

概要

このドキュメントでは、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスにトンネル接続している VPN クライアントにインターネット アクセスを許可する手順について説明します。 この設定により VPN クライアントは、IPsec を使用した企業リソースへのセキュアなアクセスと、セキュリティ保護されていないインターネット アクセスの両方を実現できます。

注: インターネットと企業 LAN の両方に対するデバイスの同時アクセスがイネーブルにならないため、フル トンネリングは最も安全な設定と見なされます。 フル トンネリングとスプリット トンネリングとの妥協により、VPN クライアントはローカル LAN アクセスのみが可能です。 ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： VPN クライアントでローカル LAN アクセスを許可するための設定例』を参照してください。

前提条件

要件

このドキュメントでは、ASA でリモート アクセス VPN 設定がすでに機能していることを前提としています。 未設定の場合は、『ASDM を使用したリモート VPN サーバとしての PIX/ASA 7.x の設定例』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA 5500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Cisco Systems VPN Client バージョン 4.0.5

注: このドキュメントでは、Cisco VPN Client 3.x. と互換性がある PIX 6.x CLI 設定についても説明しています。

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

VPN クライアントは一般的な SOHO ネットワーク上にあり、インターネット経由で本社に接続しています。

関連製品

この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x にも適用できます。

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。

背景説明

VPN Client と ASA の基本的な接続シナリオでは、宛先に関係なく、VPN Client からのすべてのトラフィックは暗号化されて ASA に送信されます。 企業の構成とサポートしているユーザ数によっては、このような設定は帯域幅を多く消費します。 スプリット トンネリングでは、トンネル接続で、企業ネットワーク向けトラフィックの送信だけがユーザに許可されるため、この問題の軽減に役立ちます。 インスタント メッセージ、電子メール、または通常の Web 閲覧など、その他すべてのトラフィックは、VPN Client のローカル LAN 経由でインターネットに送出されます。

ASA でのスプリット トンネリングの設定

Adaptive Security Device Manager（ASDM）5.x による ASA 7.x の設定

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。

1. [Configuration] > [VPN] > [General] > [Group Policy] を順に選択して、ローカル LAN アクセスをイネーブルにするグループ ポリシーを選択します。 次に [Edit] をクリックします。
2. Client Configuration タブに移動します。
3. Split Tunnel Policy の [Inherit] ボックスのチェックマークを外し、[Tunnel Network List Below] を選択します。
4. [Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。
5. ACL Manager で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。
6. ACL に名前を指定して [OK] をクリックします。
7. ACL 名が作成されてから、[Add > [Add ACE...] の順に選択してアクセス コントロール エントリ (ACE) を追加します。
8. ASA の背後にある LAN に対応する ACE を定義します。 この場合、10.0.1.0/24 のネットワークです。[Permit] を選択します。**10.0.1.0** の IP アドレスを選択します。**255.255.255.0** のネットマスクを選択します。*((オプション)* 説明を入力します。[OK] をクリックします。
9. [OK] をクリックして ACL Manager を終了します。
10. Split Tunnel Network List で、作成した ACL が選択されていることを確認します。
11. [**OK**] をクリックして、グループ ポリシー設定に戻ります。
12. コマンドを ASA に送信するために、[**Apply**] をクリックしてから [**Send**] (必要な場合) をクリックします。

Adaptive Security Device Manager (ASDM) 6.x による ASA 8.x の設定

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、ユーザがローカル LAN アクセスをイネーブルするグループ ポリシーを選択します。 次に [Edit] をクリックします。
2. [Split Tunneling] をクリックします。
3. Split Tunnel Policy の [Inherit] ボックスのチェックマークを外し、[Tunnel Network List Below] を選択します。
4. [Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。
5. ACL Manager で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。
6. ACL に名前を指定して [OK] をクリックします。
7. ACL 名が作成されてから、[Add > [Add ACE...] の順に選択してアクセス コントロール エントリ (ACE) を追加します。
8. ASA の背後にある LAN に対応する ACE を定義します。 この場合、10.0.1.0/24 のネットワークです。[Permit] オプション ボタンをクリックします。マスク **10.0.1.0/24** を持つネットワーク アドレスを選択します。 (オプション) 説明を入力します。[OK] をクリックします。
9. [OK] をクリックして ACL Manager を終了します。
10. Split Tunnel Network List で、作成した ACL が選択されていることを確認します。

11. [OK] をクリックして、グループ ポリシー設定に戻ります。
12. コマンドを ASA に送信するために、[Apply] をクリックしてから [Send]（必要な場合）をクリックします。

CLI による ASA 7.x 以降の設定

ASDM を使用する代わりに、ASA CLI で次の手順を実施して、ASA でスプリット トンネリングを許可できます。

注: CLI スプリット トンネリング設定は ASA 7.x と 8.x. の両方で同じです。

1. コンフィギュレーションモードに入ります。
```
ciscoasa>enable
Password: ********
ciscoasa#configure terminal
ciscoasa(config)#
```
2. ASA 背後のネットワークを定義するアクセス リストを作成します。
```
ciscoasa(config)#access-list Split_Tunnel_List remark The corporate network behind the ASA.
ciscoasa(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```
3. 修正するポリシーのグループ ポリシー コンフィギュレーション モードに入ります。
```
ciscoasa(config)#group-policy hillvalleyvpn attributes
ciscoasa(config-group-policy)#
```
4. スプリット トンネル ポリシーを指定します。 この例では、ポリシーは tunnelspecified です。
```
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
```
5. スプリット トンネル アクセス リストを指定します。 この例では、リストは Split_Tunnel_List です。
```
ciscoasa(config-group-policy)#split-tunnel-network-list value Split_Tunnel_List
```
6. 次のコマンドを発行します。
```
ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes
```
7. グループ ポリシーをトンネル グループに関連付けます。
```
ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
```
8. 2 つのコンフィギュレーション モードを終了します。
```
ciscoasa(config-group-policy)#exit
ciscoasa(config)#exit
ciscoasa#
```
9. この設定を Non-Volatile RAM（NVRAM; 不揮発性 RAM）に保存して、ソース ファイル名を指定するようにプロンプトが表示されたら、Enter キーを押します。
```
ciscoasa#copy running-config startup-config

Source filename [running-config]?
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec)
ciscoasa#
```

CLI による PIX 6.x の設定

次の手順を実行します。

1. PIX 背後のネットワークを定義するアクセス リストを作成します。

   ```
   PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
   ```

2. VPN グループ *vpn3000* を作成し、次に示すようにスプリット トンネル ACL を指定します。

   ```
   PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
   ```

   注: PIX 6.x.のリモート アクセス VPN 設定の詳細は、『Cisco Secure PIX Firewall 6.x および Cisco VPN Client 3.5 for Windows で Microsoft Windows 2000/2003 IAS RADIUS 認証を使用するための設定』を参照してください。

確認

設定を確認するには、次のセクションの手順を実施します。

- VPN Client を使用した接続
- VPN Client ログの表示
- Ping によるローカル LAN アクセスのテスト

VPN Client を使用した接続

VPN Client を VPN コンセントレータに接続して、設定を確認します。

1. リストから接続エントリを選択して **[Connect]** をクリックします。
2. ユーザ クレデンシャルを入力します。
3. [Status] > [Statistics...] の順に選択して、[Tunnel Details] ウィンドウを表示します。ここでトンネルの詳細を調べ、トラフィックの流れを確認できます。
4. Route Details タブに移動し、VPN Client によりセキュリティ保護されている ASA へのルートを確認します。この例では、VPN Client は 10.0.1.0/24 へのアクセスをセキュリティ保護しています。その他のすべてのトラフィックは暗号化されず、トンネル経由では送信されません。

VPN Client ログの表示

VPN Client ログを調査すると、スプリット トンネリングを指定するパラメータが設定されているかどうかを確認できます。 ログを表示するために、VPN Client の [Log] タブに移動します。 次に [Log Settings] をクリックして、記録される内容を調整します。 この例では、IKE が **3 - High**、その他のログ要素が **1 - Low** に設定されています。

```
PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
```

Ping によるローカル LAN アクセスのテスト

VPN Client が ASA とトンネル接続しながらスプリット トンネリングを実現できる設定になっているかどうかは、Windows コマンドラインで **ping** コマンドを発行する方法でも確認できます。

VPN Client のローカル LAN は 192.168.0.0/24 で、もう一方のホストも同じネットワーク上に存在し、IP アドレス 192.168.0.3 が付与されています。

```
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

トラブルシューティング

スプリット トンネル ACL でのエントリ数の制限

スプリット トンネルに使用される ACL 内のエントリ数には制限があります。 機能を適切に動作させるには、50 ~ 60 ACE エントリを使用しないことを推奨します。 IP アドレスの範囲をカバーするサブネット化機能を実装行することを推奨します。

関連情報

- ASDM を使用したリモート VPN サーバとしての PIX/ASA 7.x の設定例
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカル サポートとドキュメント – Cisco Systems