PIX 7.x および VPN 3000 コンセントレータ間の IPsec トンネルの設定例

目次

はじめに

このドキュメントでは、PIX ファイアウォール 7.x と Cisco VPN 3000 コンセントレータ間に LAN-to-LAN IPsec VPN トンネルを確立する方法について、設定例を示して説明します。

複数の PIX 間の LAN-to-LAN トンネルが、VPN クライアントがハブ PIX を介してスポーク PIX にアクセスすることを許可するシナリオの詳細については、『TACACS+ 認証を使用した PIX/ASA 7.x 拡張 Spoke-to-Client VPN の設定例』を参照してください。

PIX/ASA と IOS ルータ間に LAN-to-LAN トンネルを確立するシナリオの詳細は、『IOS ルータの LAN-to-LAN IPSec トンネルに対する PIX/ASA 7.x セキュリティ アプライアンスの設定例』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- このドキュメントの内容は、IPsec プロトコルに関する基本的知識が前提となっています。IPsec に関する知識を深めるには、『IP Security（IPSec）暗号化の概要』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。

- ソフトウェア バージョン 7.1(1) が稼働している 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 4.7.2(B) が稼働している Cisco VPN 3060 コンセントレータ

注: PIX 506/506E では、7.x はサポートされません。

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。

PIX 6.x を設定するには、『コンセントレータ、Cisco VPN 3000 コンセントレータ、PIX ファイアウォール間の接続』を参照してください。

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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

- PIX の設定
- VPN 3000 コンセントレータの設定

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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。

PIX の設定

PIX

```
PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

```
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any
!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
 pre-shared-key *
!--- Output is suppressed. ! : end PIX7#
```

VPN 3000 コンセントレータの設定

VPN コンセントレータは、工場出荷時に IP アドレスが事前にプログラムされていません。 メニュー ベースのコマンドライン インターフェイス (CLI) で初期設定を行うには、コンソール ポー

トを使用する必要があります。 コンソール経由で設定を行う方法の詳細は、『コンソール経由での VPN コンセントレータの設定』を参照してください。

イーサネット 1（プライベート）インターフェイス上の IP アドレスを設定し終えたら、CLI または ブラウザ インターフェイスのいずれかを使用して、残りの項目を設定できます。 ブラウザ インターフェイスでは HTTP と HTTP over Secure Socket Layer（SSL）の両方がサポートされています。

次のパラメータは、コンソールを使用して設定されます。

- **時間/日付**：時間と日付を正確に設定することはきわめて重要です。 これにより口ギングとアカウンティングのエントリが正確になり、システムが有効なセキュリティ認証を作成するのに役立ちます。
- **イーサネット 1（プライベート）インターフェイス**：IP アドレスおよびマスク（ネットワーク トポロジ 172.16.5.100/16）。

これで、内部ネットワークから HTML ブラウザを使用して、VPN コネクタにアクセスできるようになります。 CLI モードでの VPN コネクタの設定方法の詳細は、『クイック コンフィギュレーションでのコマンドライン インターフェイスの使用』を参照してください。

GUI インターフェイスをイネーブルにするために、Web ブラウザからプライベート インターフェイスの IP アドレスを入力します。

[save needed] アイコンをクリックして、変更をメモリに保存します。 工場出荷時のデフォルトのユーザ名およびパスワードは、**admin** です（大文字と小文字は区別されます）。

1. GUI を起動し、[Configuration] > [Interfaces] を選択して、パブリック インターフェイスおよびデフォルト ゲートウェイの IP アドレスを設定します。
2. [Configuration] > [Policy Management] > Traffic Management] > [Network Lists] > [Add or Modify] を選択して、暗号化されるトラフィックを定義するネットワーク リストを作成します。ローカルとリモートの両方のネットワークをここに追加します。 IP アドレスは、リモート PIX に設定されたアクセス リストのアドレスと一致させる必要があります。次の例では、2 つのネットワーク リストは、それぞれ **remote_network** と **VPN Client Local LAN** です。
3. [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN] > [Add] を選択して、IPsec LAN-to-LAN トンネルを設定します。 終了したら **[Apply]** をクリックします。ピアの IP アドレス、ステップ 2 で作成したネットワーク リスト、IPsec と ISAKMP のパラメータ、および事前共有鍵を入力します。次の例では、ピアの IP アドレスは **10.1.1.1**、ネットワーク リストは **remote_network** と **VPN Client Local LAN**、そして **cisco** が事前共有鍵です。
4. [Configuration] > [User Management] > [Groups] > [Modify 10.1.1.1] を選択して、自動生成されたグループに関する情報を表示します。**注:** これらのグループ設定は変更しないでください。

確認

ここでは、設定が正常に動作していることを確認します。

- PIX の確認
- VPN 3000 コンセントレータの確認

PIX の確認

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show isakmp sa**：ピアにおける現在の IKE Security Associations（SA; セキュリティ アソシエーション）をすべて表示します。 MM_ACTIVE というステートは、IPsec VPN トンネルのセットアップにメイン モードが使用されていることを示します。次の例では、PIX ファイアウォールによって IPsec 接続が開始されています。 ピアの IP アドレスは 172.30.1.1 であり、メイン モードを使用して接続を確立します。

```
PIX7#show isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.30.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- **show ipsec sa**：現在の SA で使用されている設定を表示します。 ピア IP アドレス、ローカルとリモートの両端のアクセスが可能なネットワーク、および使用されている変換セットをチェックします。 2 つの ESP SA が、各方向に 1 つずつあります。

```
PIX7#show ipsec sa
interface: outside
    Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

      access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
      current_peer: 172.30.1.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 136580F6

    inbound esp sas:
      spi: 0xF24F4675 (4065281653)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (3824999/28747)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x136580F6 (325419254)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (3824999/28745)
         IV size: 16 bytes
```

```
replay detection support: Y
```

clear ipsec sa および clear isakmp sa コマンドを使用して、トンネルをリセットします。

VPN 3000 コンセントレータの確認

[Monitoring] > [Statics] > [IPsec] を選択して、VPN 3000 コンセントレータでトンネルがアップ状態になっているかどうかを確認します。 IKE パラメータと IPsec パラメータの両方に関する統計情報が表示されます。

[Monitoring] > [Sessions] では、セッションをアクティブに監視できます。 たとえば、ここで IPsec トンネルをリセットできます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- PIX のトラブルシューティング
- VPN 3000 コンセントレータのトラブルシューティング
- PFS

PIX のトラブルシューティング

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

次に、PIX で VPN トンネルに使用できる **debug** コマンドを示します。

- **debug crypto isakmp**：ISAKMP SA ネゴシエーションをデバッグします。
- **debug crypto ipsec**：IPsec SA ネゴシエーションをデバッグします。

VPN 3000 コンセントレータのトラブルシューティング

Cisco ルータの debug コマンドと同様に、イベント クラスを設定してすべてのアラームを表示できます。 [Configuration] > [System] > [Events] > [Class] > [Add] を選択して、イベント クラスのロギングをオンにします。

[Monitoring] > [Filterable Event Log] を選択して、イネーブルなイベントを監視します。

PFS

IPSec のネゴシエーションでは、Perfect Forward Secrecy（PFS; 完全転送秘密）によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。 両方のトンネル ピアで PFS をイネーブルまたはディセーブルにします。そうでないと、PIX/ASA で LAN-to-LAN（L2L）の IPSec トンネルが確立されません。

PFS はデフォルトでディセーブルになっています。 PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用し

ます。 PFS を無効にするには、disable キーワードを指定します。

```
hostname(config-group-policy)#pfs {enable | disable}
```

実行コンフィギュレーションから PFS アトリビュートを削除するには、このコマンドの no 形式を入力します。 グループ ポリシーでは PFS に関する値を他のグループ ポリシーから継承できます。 値を継承しないようにするには、このコマンドの no 形式を使用します。

```
hostname(config-group-policy)#no pfs
```

関連情報

- Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ
- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco PIX 500 シリーズ セキュリティ アプライアンス、コマンド リファレンス
- テクニカル サポートとドキュメント – Cisco Systems