公衆インターネット VPN on a Stick のための PIX/ASA および VPN Client の設定例

目次

概要

このドキュメントでは、ASA セキュリティ アプライアンス 7.2 以降を設定する方法と IPsec on a Stick を実行する方法について説明しています。 この設定は、ASA でスプリット トンネリングが許可されない特定のケースに対して適用されます。ユーザはインターネットへの接続許可が得される前に直接 ASA に接続されます。

注: PIX/ASA バージョン 7.2 以降では、intra-interface キーワードにより、IPSec トラフィックだけでなくすべてのトラフィックが同じインターフェイスから発着信できるようになります。

中央サイトのルータで同様の設定を行うには、『公衆インターネット on a Stick 用のルータおよび VPN Client の設定例』を参照してください。

ハブ PIX が VPN Client からスポーク PIX へトラフィックをリダイレクトするシナリオの詳細は、『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。

注: ネットワークでの IP アドレスのオーバーラップを避けるために、IP アドレスの完全に異なるプールを VPN Client に割り当ててください（たとえば、10.x.x.x、172.16.x.x および 192.168.x.x）。 この IP アドレッシング方式は、ネットワークのトラブルシューティングに役立

ちます。

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。

- ハブ PIX/ASA セキュリティ アプライアンスでバージョン 7.2 以降が稼働
- Cisco VPN Client バージョン 5.x

使用するコンポーネント

このドキュメントの情報は、PIX または ASA セキュリティ アプライアンス バージョン 8.0.2、および Cisco VPN Client バージョン 5.0 に基づくものです。

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。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.2 以降にも適用できます。

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

ヘアピニングまたは U ターン

この機能は、あるインターフェイスに着信した後に同じインターフェイスからルーティングされる VPN トラフィックに対して便利な機能です。 たとえば、ハブ アンド スポークの VPN ネットワークを構築していて、セキュリティ アプライアンスがハブであり、リモート VPN ネットワークがスポークであるとします。あるスポークが他のスポークと通信するためには、トラフィックがセキュリティ アプライアンスに着信した後、他のスポーク宛てに再び発信される必要があります。

トラフィックが同じインターフェイスから発着信できるようにするには、**same-security-traffic** コマンドを使用します。

```
securityappliance(config)#same-security-traffic permit intra-interface
```

注: ヘアピニングまたは U ターンは、VPN Client 間通信にも同様に適用されます。

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。

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/ASA の CLI の設定

- PIX/ASA

PIX/ASA での実行コンフィギュレーション

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface access-list 100 extended permit icmp any
any echo-reply pager lines 24 logging enable logging
```

```
buffered debugging mtu outside 1500 mtu inside 1500 ip
local pool vpnpool 192.168.10.1-192.168.10.254 mask
255.255.255.0 no failover monitor-interface outside
monitor-interface inside icmp permit any outside no asdm
history enable arp timeout 14400 nat-control !--- The
address pool for the VPN Clients. !--- The global
address for Internet access used by VPN Clients. !---
Note: Uses an RFC 1918 range for lab setup. !--- Apply
an address from your public range provided by your ISP.
global (outside) 1 172.18.124.166 !--- The NAT statement
to define what to encrypt (the addresses from the vpn-
pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat
(inside) 1 0.0.0.0 0.0.0.0 static (inside,outside)
172.16.3.102 172.16.3.102 netmask 255.255.255.255
access-group 100 in interface outside route outside
0.0.0.0 0.0.0.0 172.18.124.98 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal group-policy
clientgroup attributes vpn-idle-timeout 20 !--- Forces
VPN Clients over the tunnel for Internet access. split-
tunnel-policy tunnelall no snmp-server location no snmp-
server contact snmp-server enable traps snmp !---
Configuration of IPsec Phase 2. crypto ipsec transform-
set myset esp-3des esp-sha-hmac !--- Crypto map
configuration for VPN Clients that connect to this PIX.
crypto dynamic-map rtpdynmap 20 set transform-set myset
!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !---
Crypto map applied to the outside interface. crypto map
mymap interface outside !--- Enable ISAKMP on the
outside interface. isakmp identity address isakmp enable
outside !--- Configuration of ISAKMP policy. isakmp
policy 10 authentication pre-share isakmp policy 10
encryption 3des isakmp policy 10 hash sha isakmp policy
10 group 2 isakmp policy 10 lifetime 86400 isakmp policy
65535 authentication pre-share isakmp policy 65535
encryption 3des isakmp policy 65535 hash sha isakmp
policy 65535 group 2 isakmp policy 65535 lifetime 86400
telnet timeout 5 ssh timeout 5 console timeout 0 !---
Configuration of tunnel-group with group information for
VPN Clients. tunnel-group rtptacvpn type ipsec-ra !---
Configuration of group parameters for the VPN Clients.
tunnel-group rtptacvpn general-attributes address-pool
vpnpool !--- Disable user authentication.
authentication-server-group none !--- Bind group-policy
parameters to the tunnel-group for VPN Clients. default-
group-policy clientgroup tunnel-group rtptacvpn ipsec-
attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0 : end
```

ASDM による ASA/PIX の設定

ASDM を使用して Cisco ASA をリモート VPN サーバとして設定するには、次の手順を実行します。

1. Home ウィンドウで、**Wizards > IPsec VPN Wizard** の順に選択します。
2. **Remote Access** VPN Tunnel Type を選択して、VPN Tunnel Interface が意図どおりに設定されていることを確認します。
3. 利用可能な唯一の VPN Client Type がすでに選択されています。 [Next] をクリックします。
4. Tunnel Group Name の名前を入力します。 使用する認証方式を入力します。この例では **Pre-shared Key** が選択されています。**注:** ASDM では、事前共有キーを非表示にしたり、暗号化したりする方法はありません。 この理由は、ASDM を使用するのは ASA を設定する担当者か、この設定でカスタマーをサポートする担当者に限定されるためです。
5. リモート ユーザの認証用にローカル ユーザのデータベースか外部 AAA サーバ グループを選択します。**注:** ステップ 6 で、ローカル ユーザのデータベースにユーザを追加します。**注:** ASDM で外部 AAA サーバ グループを設定する方法についての詳細は、『PIX/ASA：ASDM/CLI による Kerberos 認証と LDAP 認可のサーバグループの VPN ユーザ向け設定例』より「ASDM を使った VPN ユーザ向けの認証および認可の設定」を参照してください。
6. 必要な場合は、ローカル データベースにユーザを追加します。**注:** このウィンドウで現行のユーザを削除しないようにしてください。 データベースの既存のエントリを編集するか、データベースから既存のエントリを削除するには、**Configuration > Device Administration > Administration > User Accounts in the main ASDM window** の順に選択します。
7. 接続時にリモート VPN クライアントにダイナミックに割り当てられるローカル アドレスのプールを定義します。
8. *オプション：* DNS と WINS のサーバ情報、およびリモート VPN Client にプッシュするデフォルトのドメイン名を指定します。
9. IKE のパラメータを指定します。これは IKE フェーズ 1 とも呼ばれます。トンネルの両側の設定は厳密に一致している必要があります。ただし、Cisco VPN Client では自身の適切な設定が自動的に選択されます。 クライアント PC での IKE 設定は必要ありません。
10. IPSec のパラメータを指定します。これは IKE Phase 2 とも呼ばれます。トンネルの両側の設定は厳密に一致している必要があります。ただし、Cisco VPN Client では自身の適切な設定が自動的に選択されます。 クライアント PC での IKE 設定は必要ありません。
11. リモート VPN ユーザに公開可能な内部ホストやネットワークが存在する場合は、これを指定します。このリストを空白にしておくと、リモート VPN ユーザは ASA の Inside ネットワーク全体にアクセスできることになります。このウィンドウでは、スプリット トンネリングを有効にすることもできます。 スプリット トンネリングでは、ここまでで指定したリソースへのトラフィックは暗号化されますが、一般にインターネットに対してはトラフィックのトンネル化は行われず、非暗号化アクセスが行われます。 スプリット トンネリングが *有効にされていない*場合、リモート VPN ユーザからのすべてのトラフィックは ASA に対してトンネリングされます。 この場合、設定によっては、帯域幅とプロセッサへの負荷が増大する可能性があります。
12. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、[Finish] をクリックします。
13. 次に示すように、チェックボックスをクリックすると同じインターフェイスに接続している 2 つ以上のホスト間でのトラフィックが可能になるように、**same-security-traffic** コマンドを設定します。
14. ASDM を使用してダイナミック トランスレーションを作成するには、**Configuration > Firewall >NAT Rules** の順に選択して **Add Dynamic NAT Rule** をクリックします。
15. **内部を**ソースインターフェイスとして選択し、NAT にほしいアドレスを入力して下さい。

インターフェイスの Translate アドレスに関しては、『outside』 を選択 し、『OK』 をクリック して下さい。

16. ソースインターフェイスとして『outside』 を選択 し、NAT にほしいアドレスを入力して下さい。 インターフェイスの Translate アドレスに関しては、『outside』 を選択 し、『OK』 をクリック して下さい。
17. **Configuration > Firewall >NAT Rules** で、Translation Rules に変換が表示されます。

注 1： sysopt connection permit-vpn コマンドを設定する必要があります。 show running-config sysopt コマンドにより、設定されているかどうかが確認されます。

注 2： この出力をオプションの UDP トランスポート（IPsec over UDP）用に追加します。

```
group-policy clientgroup attributes vpn-idle-timeout 20 ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

注 3： VPN Clients が IPSec over TCP 経由で接続するためには、PIX アプライアンスのグローバル コンフィギュレーションで、次のコマンドを設定してください。

```
isakmp ipsec-over-tcp port 10000
```

注: ヘアピニングが使用することができる 異なるシナリオに関する詳細についてはヘアピニング ASA ビデオを on Cisco 参照して下さい。

VPN Client の設定

次の手順を実行して、VPN Client を設定します。

1. **New** を選択します。
2. 認証用のパスワードとともに、PIX の Outside インターフェイスの IP アドレスとトンネル グループ名を入力します。
3. （*オプションの*）Transport タブの下で『Enable Transparent Tunneling』 をクリック して下さい。 （これはオプションであり、注 2 で説明した追加の PIX/ASA 設定が必要です）。
4. プロファイルを保存します。

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。

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 crypto isakmp sa：ピア上の現在の IKE セキュリティ アソシエーション（SA）をすべて表示します。**
- show crypto ipsec sa：現在の SA をすべて表示します。 VPN Client トラフィックを定義する SA 上の暗号化パケットと復号化パケットを検索します。

クライアントからの ping、またはパブリック IP アドレスのブラウズを試みます（たとえば www.cisco.com）。

注: グローバル コンフィギュレーション モードで management-access コマンドを設定しない限り、トンネルの形成のための PIX の Inside インターフェイスに ping することはできません。

```
PIX1(config)#management-access inside PIX1(config)# show management-access management-access
inside
```

VPN Client の確認

VPN Client を確認するには、次のステップを実行します。

1. 接続が成功した後、システム トレイにある VPN Client のロック アイコンを右クリックし、**statistics** のオプションを選択して暗号化と複合化を表示します。
2. Route Details タブをクリックして、スプリット トンネル リストがアプライアンスから渡されていないことを確認します。

トラブルシューティング

注: VPN の問題のトラブルシューティング方法の詳細は、『一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について』を参照してください。

関連情報

- PIX/ASA 7.x：TACACS+ 認証を使用した拡張 Spoke-to-Client VPN の設定例
- Cisco VPN クライアント
- IPSec ネゴシエーション/IKE プロトコル
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- ヘアピニング on Cisco ASA
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems