PIX/ASA 7.X： 既存の L2L VPN への新しいトンネルまたはリモート アクセスの追加

目次

概要

このドキュメントでは、新しい VPN トンネルまたはリモート アクセス VPN を既存の L2L VPN 設定に追加するために必要な手順を説明します。 初期 IPSec VPN トンネルの作成方法とその他の設定例については、「Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス - 設定例とテクニカルノート」を参照してください。

前提条件

要件

この設定を実行する前に、現在動作している L2L IPSec VPN トンネルが正しく設定されていることを確認してください。

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。

- 7.x コードを実行する 2 台の ASA セキュリティ アプライアンス

- 7.x コードを実行する 1 台の PIX セキュリティ アプライアンス

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。

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。

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。

この出力は、NY（HUB）セキュリティ アプライアンスで実行中の設定です。 この設定では、NY（HQ）と TN 間に設定されている IPSec L2L トンネルがあります。

現在の NY（HQ）ファイアウォール設定

```
ASA-NY-HQ#show running-config : Saved : ASA Version
7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable
password WwXYvtKrnjXqGbu1 encrypted names ! interface
Ethernet0/0 nameif outside security-level 0 ip address
192.168.11.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name
corp2.com access-list inside_nat0_outbound extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0 access-list outside_20_cryptomap extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0 !--- Output is suppressed. nat-control
global (outside) 1 interface nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 172.16.1.0
255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.100 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10 crypto
map outside_map 20 set transform-set ESP-3DES-SHA crypto
map outside_map interface outside crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp nat-traversal 20 tunnel-group 192.168.10.10 type
ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes
pre-shared-key * telnet timeout 1440 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
```

```
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end
ASA-NY-HQ#
```

背景説明

現在、NY (HQ) オフィスと TN オフィス間には既存の L2L トンネルが設定されています。 最近 TX に会社の新しいオフィスが設立されました。 この新しいオフィスでは、NY と TN のオフィスにあるローカル リソースへの接続が必要です。 さらに、従業員が自宅から安全に内部ネットワークにあるリソースにリモートでアクセスできるようにする必要もあります。 この例では、新しい VPN トンネルと NY オフィスにあるリモート アクセス VPN サーバを設定します。

この例では、2 つのコマンドを使用して、VPN ネットワーク間での通信を許可し、トンネルまたは暗号化する必要があるトラフィックを識別します。 これにより、トラフィックを VPN トンネルに送信しなくてもインターネットにアクセスできるようになります。 これら 2 つのオプションを設定するには、**split-tunnel** コマンドと **same-security-traffic** コマンドを発行します。

スプリット トンネリングを設定すると、パケットをリモート アクセス IPSec クライアントから暗号化された形式で条件に応じて IPSec トンネル経由で送信したり、ネットワーク インターフェイスにクリア テキスト形式で送信したりできます。 スプリット トンネリングをイネーブルにすると、IPSec トンネルのもう一方の宛先に送信されていないパケットを暗号化して、トンネルを介して送信し、復号化して、最終的な宛先にルーティングする必要がありません。 このコマンドは、このスプリット トンネリング ポリシーを、指定したネットワークに適用します。 デフォルトでは、すべてのトラフィックをトンネルします。 スプリット トンネリング ポリシーを設定するには、**split-tunnel-policy** コマンドをグループ ポリシー コンフィギュレーション モードで発行します。 split-tunneling-policy を設定から削除するには、このコマンドの **no** 形式を発行します。

セキュリティ アプライアンスには、IPSec で保護されたトラフィックを同じインターフェイスで送受信できるようにして、それらのトラフィックを VPN クライアントから他の VPN ユーザに送信できる機能が含まれています。 また、ヘアピニングと呼ばれる機能は、VPN ハブ (セキュリティ アプライアンス) を介して接続する VPN スポーク (クライアント) としても機能できます。 別のアプリケーションでこの機能を使用すると、着信 VPN トラフィックを暗号化されていないトラフィックとして、同じインターフェイスからリダイレクトして返すことができます。 この機能は、スプリット トンネリングは設定されていないが、VPN へのアクセスと Web のブラウズが必要な VPN クライアントなどに便利です。 この機能を設定するには、グローバル コンフィギュレーション モードで **same-security-traffic intra-interface** コマンドを発行します。

設定への新しい L2L トンネルの追加

次に、この設定のネットワーク図を示します。

手順説明

このセクションでは、ハブ (NY ファイアウォール) セキュリティ アプライアンスで実行する必要のある手順を説明します。 スポーク クライアント (TX ファイアウォール) を設定する方法の詳細は、『PIX/ASA 7.x： 簡単な PIX-to-PIX VPN トンネル設定の例』を参照してください。

次の手順を実行します。

1. 対象トラフィックを定義するために、クリプト マップで使用される次の 2 つの新しいアクセス リストを作成します。`ASA-NY-HQ(config)#access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list outside_30_cryptomap extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0`**警告：** 通信を行うには、この特定のネットワークとは反対の Access Control List (ACL; アクセス コントロール リスト) エントリを、もう一方のトンネルに設定する必要があります。
2. 次のネットワーク間で NAT を免除するには、no nat ステートメントにこれらのエントリを追加します。`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0`**警告：** 通信を行うには、この特定のネットワークとは反対の ACL エントリを、もう一方のトンネルに設定する必要があります。
3. TX VPN ネットワークでホストをイネーブルにして、TN VPN トンネルにアクセスするには、次のコマンドを発行します。`ASA-NY-HQ(config)#same-security-traffic permit intra-interface`これにより、VPN ピア間で通信できるようになります。
4. 新しい VPN トンネルのクリプト マップ設定を作成します。 すべてのフェーズ 2 設定は同じであるため、最初の VPN 設定と同じトランスフォーム セットを使用します。`ASA-NY-HQ(config)#crypto map outside_map 30 match address outside_30_cryptomapASA-NY-HQ(config)#crypto map outside_map 30 set peer 192.168.12.2ASA-NY-HQ(config)#crypto map outside_map 30 set transform-set ESP-3DES-SHA`
5. このトンネルに指定したトンネル グループを作成して、リモート ホストに接続するために必要な属性を設定します。`ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type ipsec-l2lASA-NY-HQ(config)#tunnel-group 192.168.12.2 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key cisco123`**注:** 事前共有鍵はトンネルの両側で完全に一致する必要があります。
6. これで新しいトンネルの設定が完了したため、トンネルを介して対象トラフィックを送信して、トンネルを起動する必要があります。 これを行うには、**source ping** コマンドを発行して、リモート トンネルの内部ネットワークにあるホストに ping を送信します。この例では、トンネルのもう一方にある、20.20.20.16 のアドレスが指定されているワークステーションに ping が送信されます。 これにより、NY と TX 間のトンネルが起動します。 以上で 2 つのトンネルが HQ オフィスに接続されました。 トンネルの背後にあるシステムにアクセスできない場合、『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』で、management-access を使用する別のソリューションを参照してください。

設定例

設定例 1

```
ASA-NY-HQ#show running-config : Saved : ASA Version
7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable
password WwXYvtKrnjXqGbu1 encrypted names ! interface
Ethernet0/0 nameif outside security-level 0 ip address
192.168.11.1 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
```

255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-level no ip address ! interface Ethernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name corp2.com **same-security-traffic permit intra-interface** access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0 **access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0 access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0 access-list inside_nat0_outbound extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0** access-list outside_20_cryptomap extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0 access-list outside_20_cryptomap extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0 **access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0 access-list outside_30_cryptomap extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0** logging enable logging asdm informational mtu outside 1500 mtu inside 1500 mtu man 1500 no failover icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 nat-control global (outside) 1 interface nat (inside) 0 access-list inside_nat0_outbound nat (inside) 1 172.16.1.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0 192.168.11.1 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute username sidney password 3xsopMX9gN5Wnf1W encrypted privilege 15 aaa authentication telnet console LOCAL no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto map outside_map 20 match address outside_20_cryptomap crypto map outside_map 20 set peer 192.168.10.10 crypto map outside_map 20 set transform-set ESP-3DES-SHA **crypto map outside_map 30 match address outside_30_cryptomap crypto map outside_map 30 set peer 192.168.12.2 crypto map outside_map 30 set transform-set ESP-3DES-SHA** crypto map outside_map interface outside crypto isakmp enable outside crypto isakmp policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 crypto isakmp nat-traversal 20 tunnel-group 192.168.10.10 type ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes pre-shared-key * **tunnel-group 192.168.12.2 type ipsec-l2l tunnel-group 192.168.12.2 ipsec-attributes pre-shared-key *** telnet timeout 1440 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map 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 prompt hostname context

```
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae : end
ASA-NY-HQ#
```

設定へのリモート アクセス VPN の追加

次に、この設定のネットワーク図を示します。

手順説明

このセクションでは、リモート アクセス機能を追加して、リモート ユーザがすべてのサイトにアクセスできるようにするために必要な手順を説明します。 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。

次の手順を実行します。

1. VPN トンネルを介して接続するクライアントが使用する IP アドレス プールを作成します。また、設定の完了後に VPN にアクセスするための基本ユーザを作成します。`ASA-NY-HQ(config)#ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask 255.255.255.0ASA-NY-HQ(config)#username cisco password cisco111`
2. 特定のトラフィックを NAT から免除します。`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.120.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 20.20.20.0 255.255.255.0`この例では、VPN トンネル間の NAT 通信が免除されていることに注目してください。
3. すでに作成されている L2L トンネル間の通信を許可します。`ASA-NY-HQ(config)#access-list outside_20_cryptomap extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-NY-HQ(config)#access-list outside_30_cryptomap extended permit ip 10.10.120.0 255.255.255.0 20.20.20.0 255.255.255.0`これにより、リモート アクセス ユーザは指定したトンネルの背後にあるネットワークと通信できるようになります。**警告：** 通信を行うには、この特定のネットワークとは反対の ACL エントリを、もう一方のトンネルに設定する必要があります。
4. 暗号化して VPN トンネルを介して送信されるトラフィックを設定します。`ASA-NY-HQ(config)#access-list Hillvalley_splitunnel standard permit 172.16.1.0 255.255.255.0ASA-NY-HQ(config)#access-list Hillvalley_splitunnel standard permit 10.10.10.0 255.255.255.0ASA-NY-HQ(config)#access-list Hillvalley_splitunnel standard permit 20.20.20.0 255.255.255.0`
5. VPN クライアントの WINS、DNS、IPSec プロトコルなどのローカル認証とポリシー情報を設定します。`ASA-NY-HQ(config)#group-policy Hillvalley internalASA-NY-HQ(config)#group-policy Hillvalley attributesASA-NY-HQ(config-group-policy)#wins-server value 10.10.10.20ASA-NY-HQ(config-group-policy)#dns-server value 10.10.10.20ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol IPSec`
6. 事前共有キーと IP アドレス プールなどの IPSec と一般属性を設定します。これらは、Hillvalley VPN トンネルで使用されます。`ASA-NY-HQ(config)#tunnel-group Hillvalley`

```
 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234ASA-NY-HQ(config)#tunnel-group Hillvalley
 general-attributesASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IPASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. ステップ 4 で作成された ACL を使用するスプリット トンネル ポリシーを作成して、暗号化するトラフィックとトンネルを通過するトラフィックを指定します。`ASA-NY-HQ(config)#split-tunnel-policy tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value Hillvalley_splitunnel`
8. VPN トンネルの作成に必要なクリプト マップ情報を設定します。`ASA-NY-HQ(config)#crypto ipsec transform-set Hill-trans esp-3des esp-sha-hmacASA-NY-HQ(config)#crypto dynamic-map outside_dyn_map 20 set transform-set Hill-transASA-NY-HQ(config)#crypto dynamic-map dyn_map 20 set reverse-routeASA-NY-HQ(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map`

設定例

設定例 2

```
ASA-NY-HQ#show running-config : Saved hostname ASA-NY-HQ
ASA Version 7.2(2) enable password WwXYvtKrnjXqGbu1
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 192.168.11.2 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 172.16.1.2 255.255.255.0 ! interface
Ethernet0/2 shutdown no nameif no security-level no ip
address ! interface Ethernet0/3 shutdown no nameif no
security-level no ip address ! interface Management0/0
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name corp2.com same-
security-traffic permit intra-interface !--- This is
required for communication between VPN peers. access-
list inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 20.20.20.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.120.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
outside_20_cryptomap extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
outside_20_cryptomap extended permit ip 20.20.20.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
outside_20_cryptomap extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
Hillvalley_splitunnel standard permit 172.16.1.0
255.255.255.0 access-list Hillvalley_splitunnel standard
permit 10.10.10.0 255.255.255.0 access-list
Hillvalley_splitunnel standard permit 20.20.20.0
255.255.255.0 access-list outside_30_cryptomap extended
```

```
permit ip 172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0 access-list outside_30_cryptomap extended
permit ip 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0 access-list outside_30_cryptomap extended
permit ip 10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0 logging enable logging asdm informational
mtu outside 1500 mtu inside 1500 mtu man 1500 ip local
pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400
nat-control global (outside) 1 interface nat (inside) 0
access-list inside_nat0_outbound nat (inside) 1
172.16.1.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.1 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute group-policy Hillvalley
internal group-policy Hillvalley attributes wins-server
value 10.10.10.20 dns-server value 10.10.10.20 vpn-
tunnel-protocol IPSec split-tunnel-policy
tunnelspecified split-tunnel-network-list value
Hillvalley_splitunnel default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted aaa
authentication telnet console LOCAL no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set Hill-trans esp-3des esp-sha-
hmac crypto dynamic-map outside_dyn_map 20 set
transform-set Hill-trans crypto dynamic-map dyn_map 20
set reverse-route crypto map outside_map 20 match
address outside_20_cryptomap crypto map outside_map 20
set peer 192.168.10.10 crypto map outside_map 20 set
transform-set ESP-3DES-SHA crypto map outside_map 30
match address outside_30_cryptomap crypto map
outside_map 30 set peer 192.168.12.1 crypto map
outside_map 30 set transform-set ESP-3DES-SHA crypto map
outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside crypto isakmp
enable outside crypto isakmp policy 10 authentication
pre-share encryption 3des hash sha group 2 lifetime
86400 crypto isakmp nat-traversal 20 tunnel-group
192.168.10.10 type ipsec-l2l tunnel-group 192.168.10.10
ipsec-attributes pre-shared-key * tunnel-group
192.168.12.2 type ipsec-l2l tunnel-group 192.168.12.2
ipsec-attributes pre-shared-key * tunnel-group
Hillvalley type ipsec-ra tunnel-group Hillvalley
general-attributes address-pool Hill-V-IP default-group-
policy Hillvalley tunnel-group Hillvalley ipsec-
attributes pre-shared-key * telnet timeout 1440 ssh
timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
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
prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48 ASA-NY-
HQ#
```

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。

- **ping inside x.x.x.x（トンネルの反対側のホストの IP アドレス）**：このコマンドを使用すると、内部インターフェイスの送信元アドレスを使用して、トラフィックをトンネルに送信できます。

トラブルシューティング

設定のトラブルシューティングに使用できる情報については、次のドキュメントを参照してください。

- もっとも一般的な IPSec VPN トラブルシューティングソリューション
- IP Security のトラブルシューティング：debug コマンドの説明と使用
- PIX および ASA を経由した接続のトラブルシューティング

関連情報

- **IP セキュリティ（IPSec）暗号化の概要**
- **IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ**
- **Cisco ASA 5500 シリーズ適応型セキュリティ 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**