# PIX/ASA 7.x： 既存の L2L VPN のトンネルでのネットワークの追加/削除の設定例

## 目次



## 概要

このドキュメントでは、既存の VPN トンネルに新しいネットワークを追加する設定例を説明します。

## 前提条件

### 要件

この設定を試みる前に 7.x コードを実行する PIX/ASA セキュリティ アプライアンス モデルがあることを確認して下さい。

### 使用するコンポーネント

この文書に記載されている情報は 2 つの Cisco 5500 セキュリティ アプライアンス モデル デバイスに基づいています。

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

この設定も PIX 500 セキュリティ アプライアンス モデルと使用することができます。

## 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

現在 LAN-to-LAN な（L2L）VPN トンネルがあります NY および TN オフィスの間にある。 NY オフィスはちょうど CSI 開発 グループが使用される新しいネットワークを追加しました。 このグループは TN オフィスに常駐するリソースにアクセスを必要とします。 手もとタスクは既に存在 VPN トンネルへ新しいネットワークを追加することです。

# 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。

## IPSecトンネルにネットワークを追加する方法

このドキュメントでは次の設定を使用しています。

**NY（HQ）ファイアウォール構成**

```
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 nameif Cisco
security-level 70 ip address 172.16.40.2 255.255.255.0 !
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 !--- You must be
sure that you configure the !--- opposite of these
access control lists !--- on the other end of the VPN
tunnel. access-list inside_nat0_outbound extended permit
ip 172.16.40.0 255.255.255.0 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 !---
```

```
You must be sure that you configure the !--- opposite of
these access control lists !--- on the other end of the
VPN tunnel. access-list outside_20_cryptomap extended
permit ip 172.16.40.0 255.255.255.0 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 !--- The new network is also required to
have access to the Internet. !--- So enter an entry into
the NAT statement for this new network. nat (inside) 1
172.16.40.0 255.255.255.0 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 * !--- Output is suppressed. : end ASA-
NY-HQ#
```

## IPSecトンネルからネットワークを取除くこと

この IPSecトンネル configuation からネットワークを取除くステップを使用して下さい。ネットワーク 172.16.40.0/24 が NY （ HQ ） Secuirty アプライアンス 設定から取除かれたとここでは、考慮して下さい。

1. トンネルからネットワークを取除きなさい前に、またフェーズ 2.に関するセキュリティ結合をクリアする IPSec接続を中断 して下さい。
   **ASA-NY-HQ# clear crypto ipsec sa** フェーズ 1 に次の通り関するセキュリティ結合をクリアします
   **ASA-NY-HQ# clear crypto isakmp sa**
2. IPSecトンネルのための関連 トラフィック ACL を取除いて下さい。
   **ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0**
3. トラフィックが NAT から除かれるので、ACL （ inside_nat0_outbound ）を取除いて下さい。
   **ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0**
4. 示されているように NAT 変換をクリアして下さい
   **ASA-NY-HQ# clear xlate**
5. トンネル設定を修正するとき、この outside インターフェイスの後期コンフィギュレーションを奪取 する 暗号コマンドを削除し、再適用して下さい
   **ASA-NY-HQ(config)# crypto map outside_map interface outside ASA-NY-HQ(config)# crypto isakmp enable outside**
6. フラッシュ「write memory」にアクティブコンフィギュレーションを保存して下さい。
7. コンフィギュレーションを取除くためにもう一方の端のための同じプロシージャに- TN セキ

ユリティ アプライアンス モデル従って下さい。
8. Initate は IPSecトンネル接続を確認し。

## 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。

- 172.16.40.20 の中で ping して下さい
- show crypto isakmp sa
- show crypto ipsec sa

## トラブルシューティング

トラブルシューティング情報詳細についてはこれらの文書を参照して下さい:

- IPSec VPN トラブルシューティングソリューション
- 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）暗号化入門
- 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
- セキュリティ アプライアンス モデル コマンドレファレンス
- IP アクセス リストの設定 [英語]
- テクニカルサポートとドキュメント - Cisco Systems