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

内容

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

この設定を試す前に、7.xコードが稼働するPIX/ASAセキュリティアプライアンスがあ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、2台のCisco 5500セキュリティアプライアンスデバイスに基づくものです。

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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、PIX 500セキュリティアプライアンスでも使用できます。

表記法

ドキュメント表記の詳細については、『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、NYオフィスとTNオフィスの間にLAN-to-LAN(L2L)VPNトンネルがあります。NYオフィスは、CSI開発グループが使用する新しいネットワークを追加しました。このグループには、TNオフィス内のリソースへのアクセスが必要です。現在の作業は、既存のVPNトンネルに新しいネットワークを追加することです。

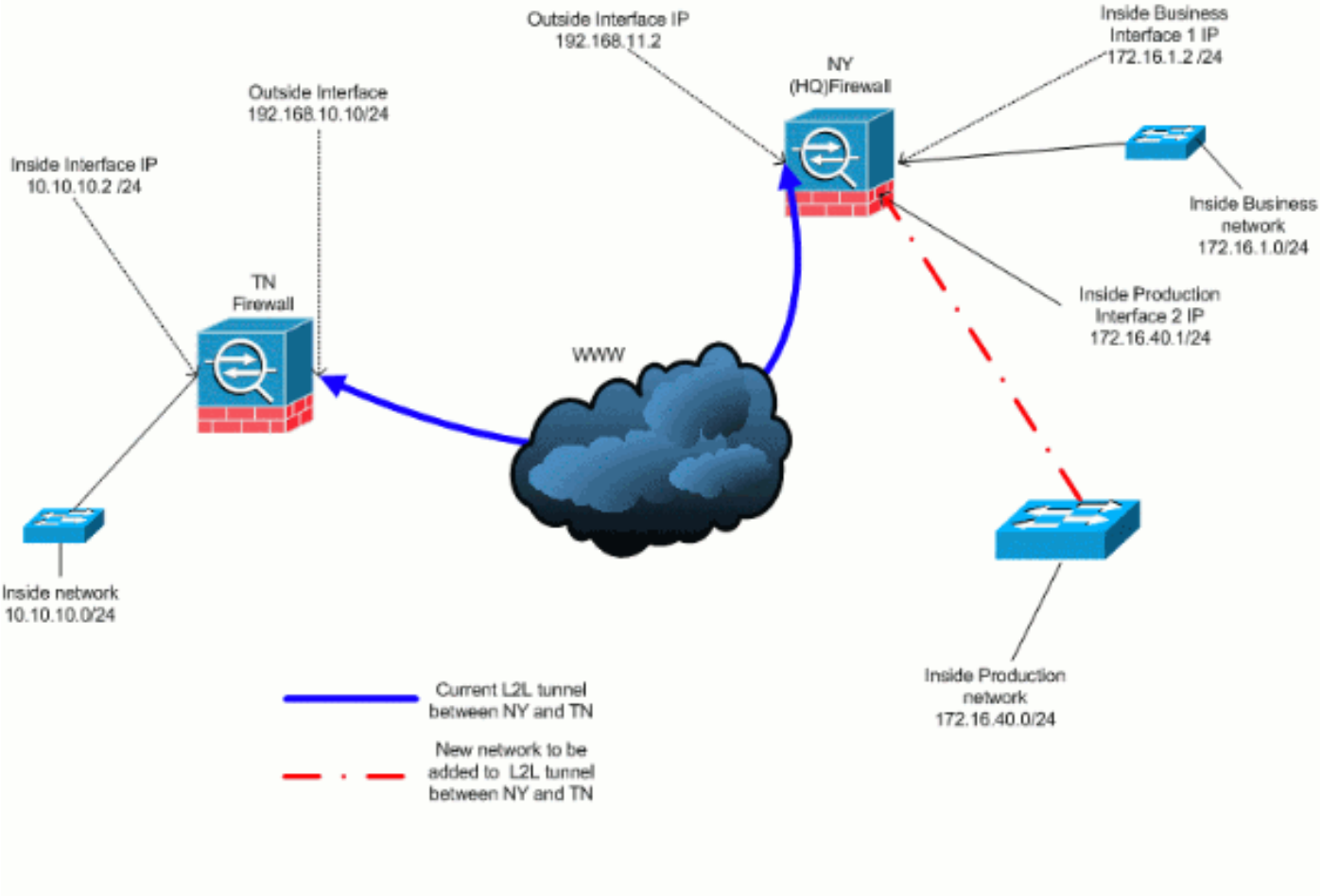
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

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 セットアップを使用します。



IPSecトンネルへのネットワークの追加

このドキュメントでは、次の設定を使用しています。

NY(HQ)ファイアウォールの設定

```
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
 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トンネルからのネットワークの削除

次の手順を使用して、IPSecトンネル設定からネットワークを削除します。ここでは、ネットワーク172.16.40.0/24がNY(HQ)セキュリティアプライアンス設定から削除されていることを検討します。

1. トンネルからネットワークを削除する前に、IPSec接続を切断します。これにより、フェーズ2に関連するセキュリティアソシエーションもクリアされます。

   ```
   ASA-NY-HQ# clear crypto ipsec sa
   ```

   次のように、フェーズ1に関連するセキュリティアソシエーションをクリアします

   ```
   ASA-NY-HQ# clear crypto isakmp sa
   ```

2. IPSecトンネルの対象トラフィックACLを削除します。

   ```
   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から除外されるため、ACL(inside_nat0_outbound)を削除します。

   ```
   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. 次に示すように、NAT変換をクリアします

   ```
   ASA-NY-HQ# clear xlate
   ```

5. トンネル設定を変更する場合は、この暗号コマンドを削除して再適用し、外部インターフェイスの最新の設定を取得します

   ```
   ASA-NY-HQ(config)# crypto map outside_map interface outside
   ASA-NY-HQ(config)# crypto isakmp enable outside
   ```

6. アクティブな設定をフラッシュ「書き込み**メモリ」に保存します。**
7. 相手側のTNセキュリティアプライアンスと同じ手順に従って、設定を削除します。
8. IPSecトンネルを開始し、接続を確認します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **ping inside**
  172.16.40.20

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.40.20, timeout is 2 seconds:
?!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

- **show crypto 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: 192.168.10.10
   Type    : L2L          Role    : initiator
   Rekey   : no           State   : MM_ACTIVE
```

- **show crypto ipsec**
  sa

```
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

      access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 172.16.40.0 255.255.255.0
      local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.40.0/255.255.255.0/0/0)
      current_peer: 192.168.10.10

      #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
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 4C0547DE

    inbound esp sas:
      spi: 0x0EB40138 (246677816)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28476)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x4C0547DE (1275414494)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28476)
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

      access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      current_peer: 192.168.10.10

      #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 14, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 5CC4DE89

    inbound esp sas:
      spi: 0xF48286AD (4102194861)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/28271)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x5CC4DE89 (1556405897)
         transform: esp-3des esp-sha-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274998/28271)
         IV size: 8 bytes
         replay detection support: Y
```

トラブルシュート

トラブルシューティングの詳細については、次のドキュメントを参照してください。

- 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
- セキュリティアプライアンスコマンドリファレンス
- IP アクセス リストの設定
- テクニカル サポートとドキュメント – Cisco Systems