PIX/ASA 7.x:在現有L2L VPN隧道上新增/刪除網路配置示例

目錄

簡介

本文檔提供了如何向現有VPN隧道新增新網路的配置示例。

必要條件

需求

嘗試此配置之前，請確保您具有運行7.x代碼的PIX/ASA安全裝置。

採用元件

本檔案中的資訊是根據兩部思科5500安全裝置裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與PIX 500安全裝置一起使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

目前，紐約和TN辦公室之間有一個LAN到LAN(L2L)VPN隧道。紐約辦事處剛剛新增了一個新網路，供CSI開發組使用。此組需要訪問駐留在TN辦公室中的資源。當前的任務是將新網路新增到現有的VPN隧道中。

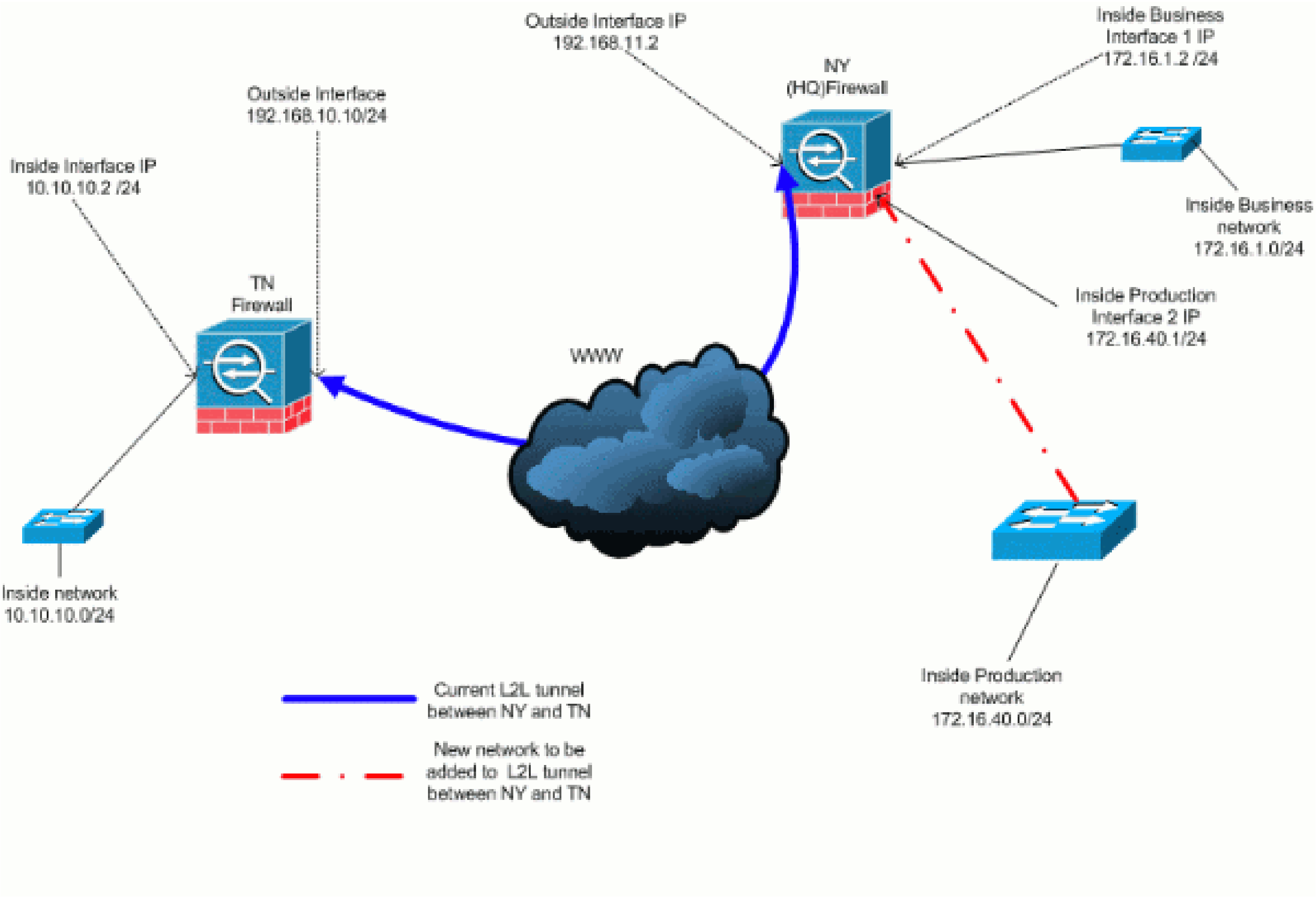
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



將網路新增到IPSec隧道

本檔案會使用以下設定：

NY(HQ)防火牆配置

```
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#
```

從IPSec隧道中刪除網路

使用此步驟從IPSec隧道配置中刪除網路。在此處，考慮已從NY(HQ)安全裝置配置中刪除網路172.16.40.0/24。

1. 從隧道中刪除網路之前，請拆除IPSec連線，這樣也會清除與第2階段相關的安全關聯。

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

   清除與第1階段相關的安全關聯，如下所示

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

2. 移除IPSec通道的相關流量ACL。

   ```
   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. 刪除ACL(inside_nat0_outbound)，因為流量會從nat中排除。

```
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. 清除NAT轉換，如圖所示

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

5. 修改隧道配置時，請刪除並重新應用此加密命令，以在外部介面中獲得最新配置

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

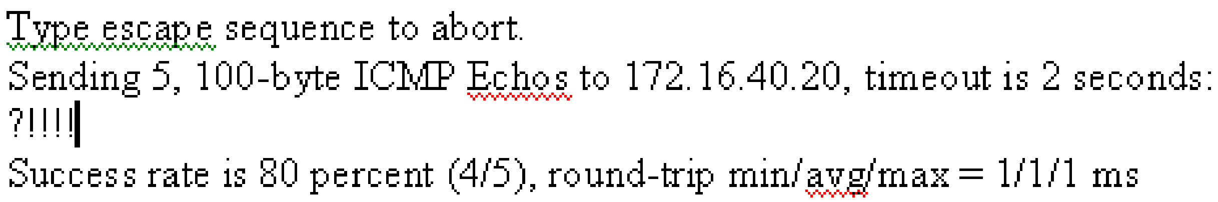
6. 將活動配置儲存到閃**存「寫記憶體」**。
7. 對另一端 — TN安全裝置執行相同的步驟以刪除配置。
8. 啟動IPSec隧道並驗證連線。

驗證

使用本節內容，確認您的組態是否正常運作。

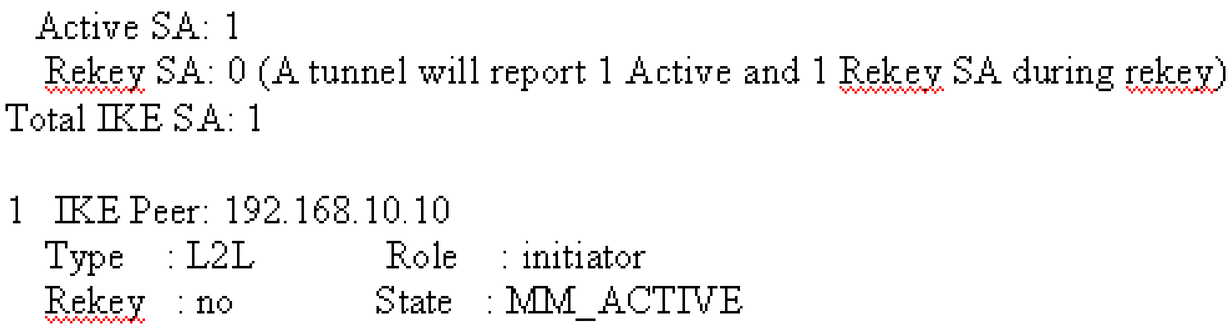
輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **ping 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
```

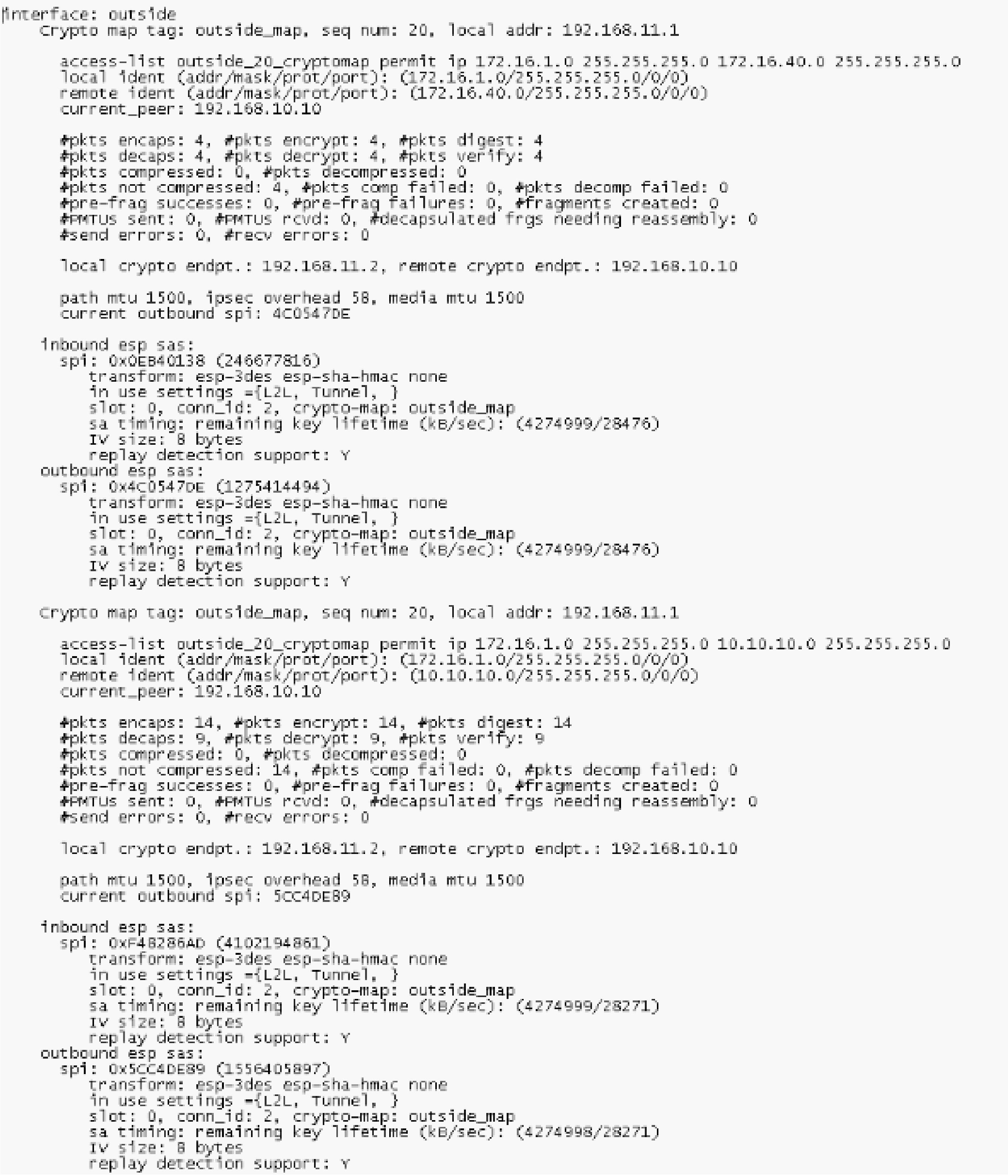
- **show crypto isakmp sa**



```
   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
```

疑難排解

如需更多疑難排解資訊，請參閱以下檔案：

- IPsec VPN故障排除解決方案
- 瞭解和使用偵錯指令
- 通過PIX和ASA排除連線故障

相關資訊

- IP安全(IPsec)加密簡介
- IPsec協商/IKE通訊協定支援頁面
- 安全裝置命令參考
- 設定 IP 存取清單
- 技術支援與文件 - Cisco Systems