PIX/ASA 7.x：在现有 L2L VPN 隧道上添加/删除网络的配置示例

目录

简介

该文档为如何向现有的 VPN 隧道中添加新网络提供示例配置。

先决条件

要求

尝试此配置之前，请确保您拥有运行 7.x 代码的 PIX/ASA 安全设备。

使用的组件

本文档中的信息基于两个 Cisco 5500 安全设备装置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也适用于 PIX 500 安全设备。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

当前在 NY 和 TN 办公室之间有一个 LAN 到 LAN (L2L) VPN 隧道。NY 办公室刚添加了一个要由 CSI 开发组使用的新网络。该组需要访问位于 TN 办公室中的资源。目前的任务是将新网络添加到已存在的 VPN 隧道中。

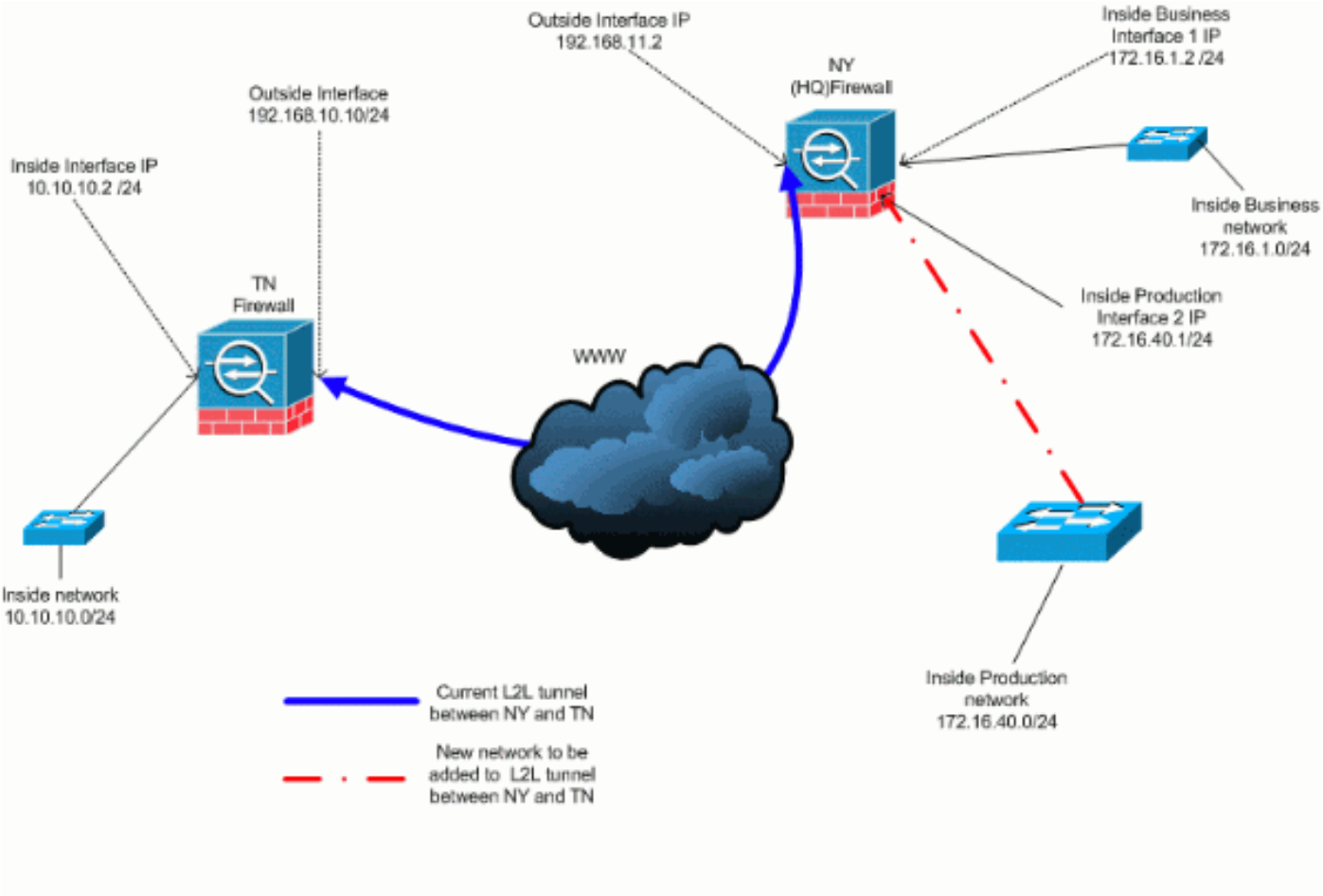
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



向 IPSec 隧道中添加网络

本文档使用以下配置：

NY (HQ) 防火墙配置

```
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#
```

从 IPSec 隧道中删除网络

使用以下步骤从 IPSec 隧道配置中删除网络。此处，考虑网络 172.16.40.0/24 已从 NY (HQ) 安全设备配置中删除。

1. 从隧道中删除网络之前，请先切断 IPSec 连接，这将同时清除与第 2 阶段相关的安全关联。
   ASA-NY-HQ# clear crypto ipsec sa 按如下所示清除与第 1 阶段相关的安全关联
   ASA-NY-HQ# clear crypto isakmp sa

2. 删除 IPSec 隧道的相关数据流 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. 由于无需对数据流进行 NAT，因此删除 ACL (inside_nat0_outbound)。
   ```
   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. 如下所示清除 NAT 转换
   ```
   ASA-NY-HQ# clear xlate
   ```
5. 每当修改隧道配置时，都请删除并重新应用以下 crypto 命令以采用外部接口中的最新配置
   ```
   ASA-NY-HQ(config)# crypto map outside_map interface outside ASA-NY-HQ(config)# crypto
   isakmp enable outside
   ```
6. 使用 **write memory** 将活动配置保存到闪存中。
7. 对另一端（TN 安全设备）执行相同的过程以删除配置。
8. 启动 IPSec 隧道并验证连接。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **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
```

故障排除

有关详细的故障排除信息，请参阅以下文档：

- IPsec VPN 故障排除解决方案
- 了解和使用调试指令
- 排除通过 PIX 和 ASA 的连接故障

相关信息

- IP 安全 (IPsec) 加密简介
- IPsec 协商/IKE 协议支持页
- 安全设备命令参考
- 配置 IP 访问列表
- 技术支持和文档 - Cisco Systems