PIX/ASA 7.x:기존 L2L VPN 터널 컨피그레이션의 네트워크 추가/제거 예

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
관련 제품
표기 규칙
배경 정보
구성
네트워크 다이어그램
IPSec 터널에 네트워크 추가
IPSec 터널에서 네트워크 제거
다음을 확인합니다.
문제 해결
관련 정보

소개

이 문서에서는 기존 VPN 터널에 새 네트워크를 추가하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 7.x 코드를 실행하는 PIX/ASA Security Appliance가 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 두 개의 Cisco 5500 Security Appliance 디바이스를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 PIX 500 Security Appliance와 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

현재 NY와 TN 사무실 사이에 LAN-to-LAN(L2L) VPN 터널이 있습니다.뉴욕 사무소는 방금 CSI 개발 그룹에서 사용할 새로운 네트워크를 추가했다.이 그룹에서는 TN 사무실에 있는 리소스에 액세스해야 합니다.현재 작업은 기존 VPN 터널에 새 네트워크를 추가하는 것입니다.

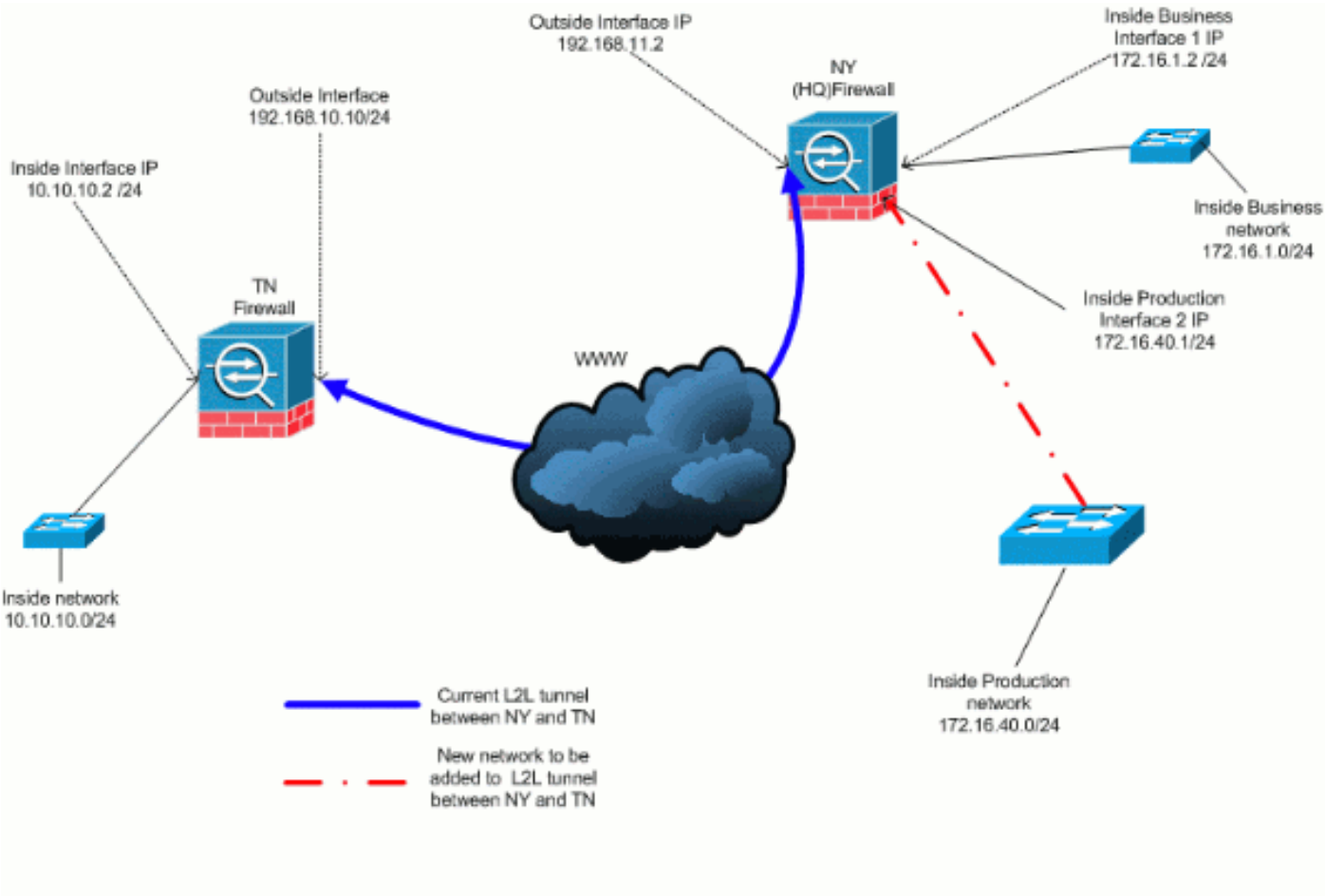
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



IPSec 터널에 네트워크 추가

이 문서에서는 다음 구성을 사용합니다.

NY(HQ) 방화벽 구성

```
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 터널에서 네트워크 제거

이 단계를 사용하여 IPSec 터널 구성에서 네트워크를 제거합니다.여기서 네트워크 172.16.40.0/24이 NY(HQ) 보안 어플라이언스 컨피그레이션에서 제거되었습니다.

1. 터널에서 네트워크를 제거하기 전에 IPSec 연결을 해제하여 2단계와 관련된 보안 연결도 지웁니다.

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

   다음과 같이 1단계와 관련된 보안 연결을 지웁니다.

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

2. IPSec 터널에 대한 흥미로운 트래픽 ACL을 제거합니다.

```
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. 트래픽이 nat에서 제외되므로 ACL(inside_nat0_outbound)을 제거합니다.

```
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. 표시된 대로 NAT 변환을 지웁니다.

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

5. 터널 컨피그레이션을 수정하면 이 암호화 명령을 제거하고 다시 적용하여 외부 인터페이스에서 최신 컨피그레이션을 가져옵니다.

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

6. 활성 컨피그레이션을 플래시 **"쓰기 메모리"에 저장합니다**.
7. 구성을 제거하려면 다른 쪽 끝인 TN Security Appliance에 대해 동일한 절차를 수행합니다.
8. IPSec 터널을 시작하고 연결을 확인합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **172.16.40.20 내에서 ping을**

```
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
```

- **crypto isakmp sa 표시**

```
    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
```

- **crypto ipsec sa 표시**

```
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
```

문제 해결

자세한 문제 해결 정보는 다음 문서를 참조하십시오.

- IPsec VPN 문제 해결 솔루션
- 디버그 명령 이해 및 사용
- PIX 및 ASA를 통한 연결 문제 해결

관련 정보

- IPsec(IP Security) 암호화 소개
- IPsec 협상/IKE 프로토콜 지원 페이지
- 보안 어플라이언스 명령 참조
- IP 액세스 목록 구성
- 기술 지원 및 문서 – Cisco Systems