PIX/ASA 7.X:기존 L2L VPN에 새 터널 또는 원격 액세스 추가

목차

소개

이 문서에서는 이미 존재하는 L2L VPN 구성에 새 VPN 터널 또는 원격 액세스 VPN을 추가하는 데 필요한 단계를 제공합니다.초기 IPSec VPN 터널 생성 방법 및 자세한 컨피그레이션 예는 Cisco ASA 5500 Series Adaptive Security Appliances - 컨피그레이션 예 및 TechNotes를 참조하십시오.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 현재 작동 중인 L2L IPSEC VPN 터널을 올바르게 구성해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.x 코드를 실행하는 ASA 보안 어플라이언스 2개
- 7.x 코드를 실행하는 PIX 보안 어플라이언스 1개

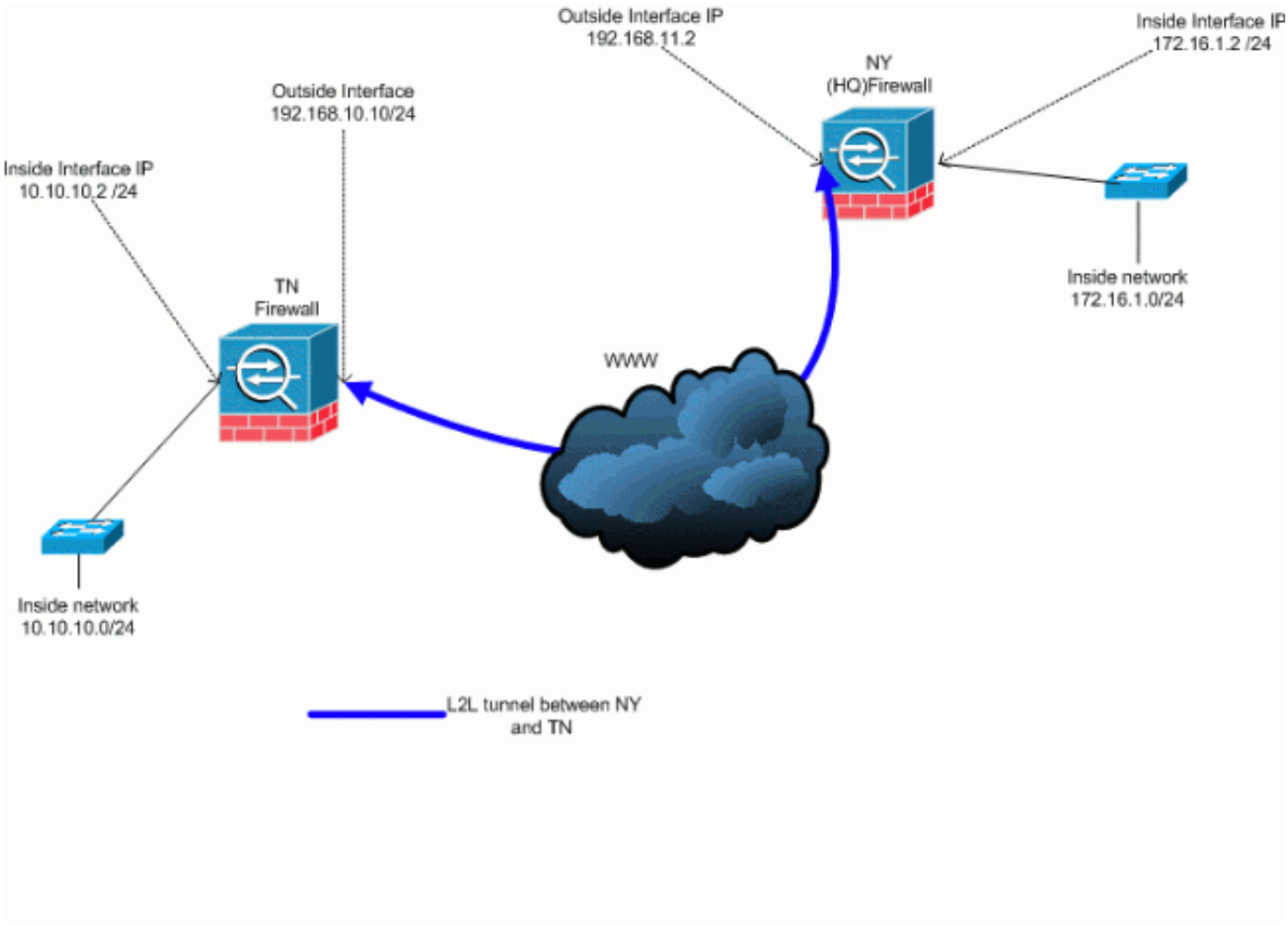
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 출력은 NY(HUB) 보안 어플라이언스의 현재 실행 중인 컨피그레이션입니다.이 컨피그레이션에는 NY(HQ)와 TN 간에 구성된 IPSec L2L 터널이 있습니다.

현재 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
 shutdown
 no nameif
 no security-level
 no ip address
!
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
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0
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 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 * telnet timeout 1440 ssh timeout 5
console timeout 0 ! class-map inspection_default match
```

```
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end
ASA-NY-HQ#
```

배경 정보

현재 NY(HQ) 사무실과 TN 사무실 사이에 설치된 기존 L2L 터널이 있습니다.귀사는 최근 TX에 위치한 새 사무실을 열었습니다.이 새로운 사무소는 NY 및 TN 사무실에 있는 로컬 리소스에 연결해야 합니다.또한 직원이 재택 근무 기회를 제공하고 내부 네트워크에 원격으로 있는 리소스에 안전하게 액세스할 수 있도록 해야 하는 추가적인 요구 사항이 있습니다.이 예에서는 새 VPN 터널과 NY 사무실에 있는 원격 액세스 VPN 서버가 구성됩니다.

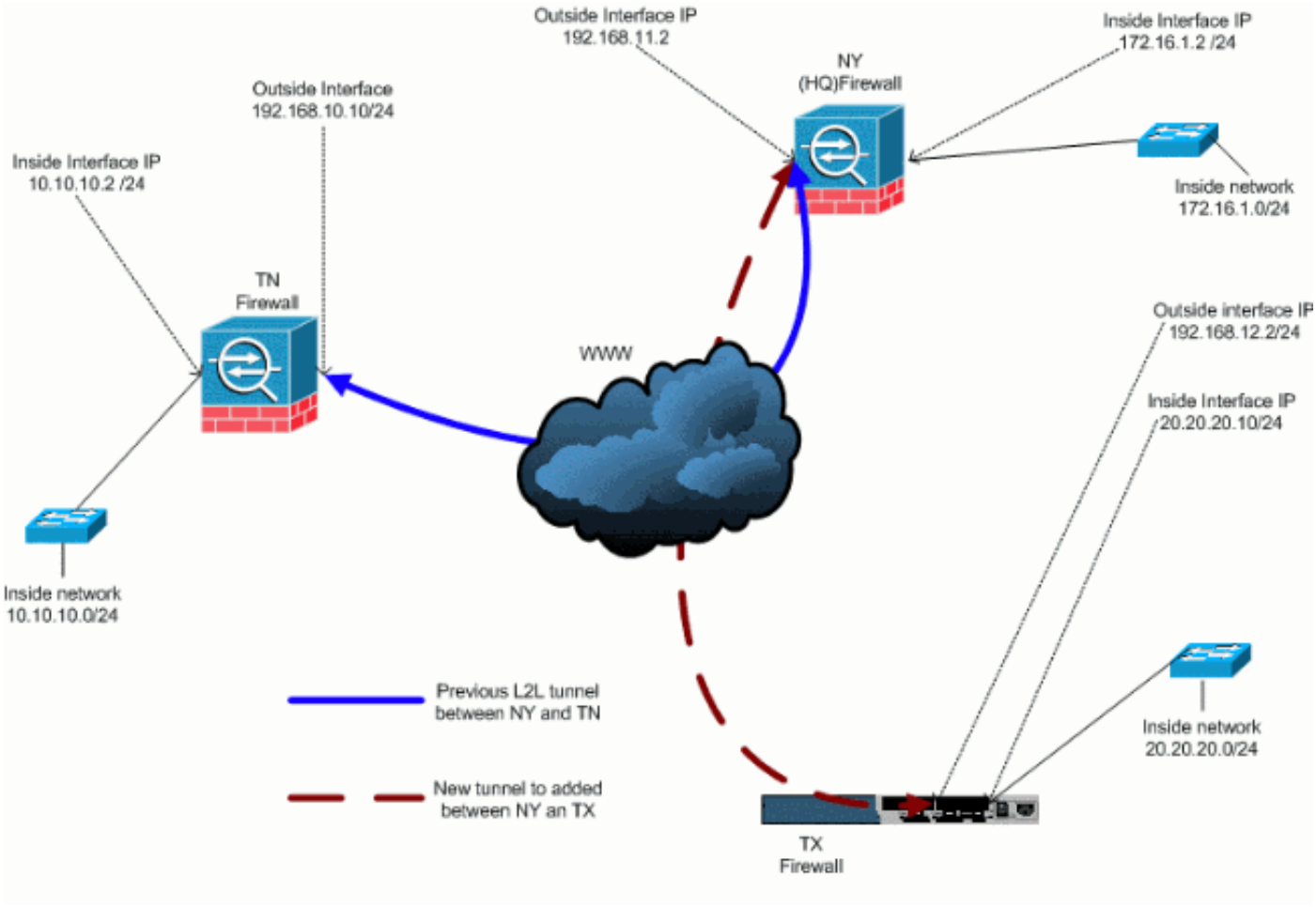
이 예에서는 VPN 네트워크 간의 통신을 허용하고 터널링 또는 암호화해야 하는 트래픽을 식별하기 위해 두 명령이 사용됩니다.이렇게 하면 VPN 터널을 통해 해당 트래픽을 보내지 않고도 인터넷에 액세스할 수 있습니다.이러한 두 옵션을 구성하려면 **split-tunnel** 및 **same-security-traffic** 명령**을** 실행합니다.

스플릿 터널링을 사용하면 원격 액세스 IPSec 클라이언트가 IPSec 터널을 통해 암호화된 형식으로 또는 일반 텍스트 형식으로 네트워크 인터페이스에 패킷을 조건부로 전달할 수 있습니다.스플릿 터널링이 활성화되면 IPSec 터널의 반대쪽에 있는 대상에 대해 바인딩되지 않은 패킷은 암호화되지 않아도 되며 터널을 통해 전송되거나 해독된 다음 최종 대상으로 라우팅될 수 있습니다.이 명령은 이 스플릿 터널링 정책을 지정된 네트워크에 적용합니다.기본값은 모든 트래픽을 터널링하는 것입니다.스플릿 터널링 정책을 설정하려면 group-policy 컨피그레이션 모드에서 **split-tunnel-policy** 명령을 실행합니다.컨피그레이션에서 스플릿 터널링 정책을 제거하려면 이 명령의 **no** 형식을 실행합니다.

보안 어플라이언스에는 VPN 클라이언트가 IPSec 보호 트래픽을 다른 VPN 사용자에게 보낼 수 있도록 허용하는 기능이 포함되어 있습니다. 이 기능은 동일한 인터페이스에서 들어오고 나가는 트래픽을 허용합니다.헤어피닝이라고도 하며, 이 기능은 VPN 허브(보안 어플라이언스)를 통해 연결하는 VPN 스포크(클라이언트)로 간주할 수 있습니다. 다른 애플리케이션에서 이 기능은 암호화되지 않은 트래픽과 동일한 인터페이스를 통해 수신 VPN 트래픽을 다시 리디렉션할 수 있습니다.예를 들어 스플릿 터널링이 없지만 VPN에 액세스하고 웹을 찾아봐야 하는 VPN 클라이언트에 유용합니다.이 기능을 구성하려면 글로벌 컨피그레이션 모드에서 **same-security-traffic** ***intra-interface*** **명령**을 실행합니다.

구성에 추가 L2L 터널 추가

이 구성에 대한 네트워크 다이어그램입니다.



단계별 지침

이 섹션에서는 HUB(NY 방화벽) 보안 어플라이언스에서 수행해야 하는 필수 절차를 설명합니다 .PIX/ASA 7.x 참조:Simple PIX-to-PIX VPN Tunnel Configuration(단순 PIX-to-PIX VPN 터널 컨피그레이션)에서 스포크 클라이언트(TX 방화벽)를 구성하는 방법에 대한 자세한 내용을 확인할 수 있습니다.

다음 단계를 완료하십시오.

1. 흥미로운 트래픽을 정의하기 위해 암호화 맵에서 사용할 다음 두 개의 새 액세스 목록을 생성합니다.
```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0


ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```
경고: 통신이 이루어지려면 터널의 반대쪽에 해당 특정 네트워크에 대한 이 ACL(Access Control List) 항목의 반대편이 있어야 합니다.
2. 이러한 네트워크 간의 연결을 제외하려면 no nat 문에 다음 항목을 추가합니다.
```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0


ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 20.20.20.0 255.255.255.0
    10.10.10.0 255.255.255.0
```

경고: 통신이 이루어지려면 터널의 반대쪽에 해당 특정 네트워크에 대한 이 ACL 항목의 반대편이 있어야 합니다.

3. TX VPN 네트워크의 호스트가 TN VPN 터널에 액세스할 수 있도록 하려면 다음 명령을 실행합니다.

```
ASA-NY-HQ(config)#same-security-traffic permit
 intra-interface
```

이렇게 하면 VPN 피어가 서로 통신할 수 있습니다.

4. 새 VPN 터널에 대한 암호화 맵 컨피그레이션을 생성합니다.모든 2단계 설정이 동일하므로 첫 번째 VPN 컨피그레이션에서 사용된 것과 동일한 변형 집합을 사용합니다.

```
ASA-NY-HQ(config)#crypto map outside_map 30 match
 address outside_30_cryptomap

ASA-NY-HQ(config)#crypto map outside_map 30 set
 peer 192.168.12.2

ASA-NY-HQ(config)#crypto map outside_map 30 set
 transform-set
 ESP-3DES-SHA
```

5. 원격 호스트에 연결하는 데 필요한 특성과 함께 이 터널에 대해 지정된 터널 그룹을 생성합니다.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
 ipsec-l2l

ASA-NY-HQ(config)#tunnel-group 192.168.12.2
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco123
```

참고: 사전 공유 키는 터널의 양쪽에서 정확히 일치해야 합니다.

6. 이제 새 터널을 구성했으므로 터널을 작동하려면 흥미로운 트래픽을 터널을 통과해야 합니다.이 작업을 수행하려면 **source ping** 명령을 실행하여 원격 터널의 내부 네트워크에서 호스트를 ping합니다.이 예에서는 20.20.20.16 주소가 있는 터널의 반대쪽에 있는 워크스테이션에 ping이 수행됩니다.그러면 NY와 TX 간에 터널이 나타납니다.이제 본사에 두 개의 터널이 연결되어 있습니다.터널 뒤의 시스템에 액세스할 수 없는 경우 Most Common IPSec VPN Troubleshooting Solutions(가장 일반적인 IPSec VPN 문제 해결 솔루션)를 참조하여 사용과 관련된 대체 솔루션을 .

컨피그레이션 예

구성 예 1

```
ASA-NY-HQ#show running-config

 : Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
```

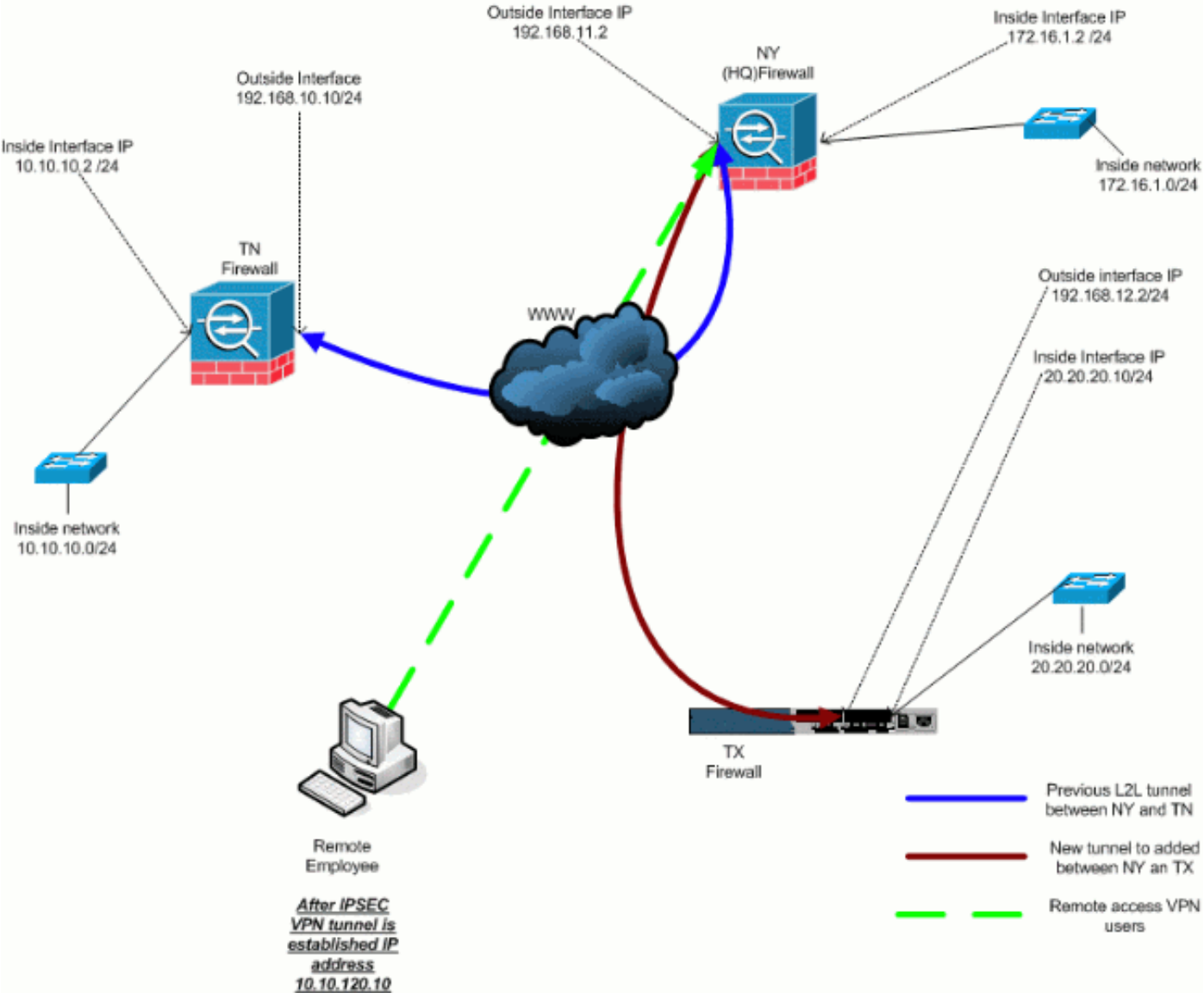
```
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 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
same-security-traffic permit intra-interface
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
```

```
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
username sidney password 3xsopMX9gN5Wnf1W encrypted
privilege 15
aaa authentication telnet console LOCAL
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 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.2
crypto map outside_map 30 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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
 pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
```

```
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae
: end
ASA-NY-HQ#
```

구성에 원격 액세스 VPN 추가

이 구성에 대한 네트워크 다이어그램입니다.



단계별 지침

이 섹션에서는 원격 액세스 기능을 추가하고 원격 사용자가 모든 사이트에 액세스할 수 있도록 하는 데 필요한 절차를 제공합니다.PIX/ASA 7.x ASDM을 참조하십시오.원격 액세스 서버 구성 및 액세스 제한 방법에 대한 자세한 내용은 Restrict the Network Access of Remote Access VPN Users(원격 액세스 VPN 사용자의 네트워크 액세스 제한)를 참조하십시오.

다음 단계를 완료하십시오.

1. VPN 터널을 통해 연결하는 클라이언트에 사용할 IP 주소 풀을 생성합니다.또한 컨피그레이션이 완료되면 VPN에 액세스하기 위해 기본 사용자를 생성합니다.
```
ASA-NY-HQ(config)#ip local pool Hill-V-IP
 10.10.120.10-10.10.120.100 mask 255.255.255.0


ASA-NY-HQ(config)#username cisco password
 cisco111
```
2. 특정 트래픽이 시작되지 않도록 합니다.
```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 172.16.1.0
    255.255.255.0 10.10.120.0 255.255.255.0


ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0


ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 20.20.20.0 255.255.255.0
```
이 예에서는 VPN 터널 간의 nat 통신이 면제됩니다.
3. 이미 생성된 L2L 터널 간의 통신을 허용합니다.
```
ASA-NY-HQ(config)#access-list
 outside_20_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0


ASA-NY-HQ(config)#access-list
 outside_30_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 20.20.20.0 255.255.255.0
```
이렇게 하면 원격 액세스 사용자가 지정된 터널 뒤의 네트워크와 통신할 수 있습니다.**경고:** 통신이 이루어지려면 터널의 반대쪽에 해당 특정 네트워크에 대한 이 ACL 항목의 반대편이 있어야 합니다.
4. VPN 터널을 통해 암호화 및 전송할 트래픽을 구성합니다.
```
ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 172.16.1.0
    255.255.255.0


ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 10.10.10.0
    255.255.255.0


ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 20.20.20.0
    255.255.255.0
```
5. VPN 클라이언트에 대한 로컬 인증 및 정책 정보(예: wins, dns, IPSec 프로토콜)를 구성합니다.
```
ASA-NY-HQ(config)#group-policy Hillvalley
 internal


ASA-NY-HQ(config)#group-policy Hillvalley
```

```
 attributes

ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20

ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20

ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. Hillvalley VPN 터널에서 사용할 IPSec 및 일반 특성(예: 사전 공유 키 및 IP 주소 풀)을 설정합니다.

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234

ASA-NY-HQ(config)#tunnel-group Hillvalley
 general-attributes

ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP

ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. 4단계에서 생성한 ACL을 사용하여 어떤 트래픽이 암호화되어 터널을 통과할지 지정하기 위해 스플릿 터널 정책을 생성합니다.

```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecified

ASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```

8. VPN 터널 생성에 필요한 암호화 맵 정보를 구성합니다.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
 Hill-trans esp-3des esp-sha-hmac

ASA-NY-HQ(config)#crypto dynamic-map
 outside_dyn_map 20 set transform-set
 Hill-trans

ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
 set reverse-route

ASA-NY-HQ(config)#crypto map outside_map 65535
 ipsec-isakmp dynamic
 outside_dyn_map
```

컨피그레이션 예

구성 예 2

```
ASA-NY-HQ#show running-config

 : Saved
```

```
hostname ASA-NY-HQ
ASA Version 7.2(2)

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
 shutdown
 no nameif
 no security-level
 no ip address
!
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
same-security-traffic permit intra-interface

!--- This is required for communication between VPN
peers. access-list inside_nat0_outbound extended permit
ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.120.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.120.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
```

```
access-list outside_20_cryptomap extended permit ip
10.10.120.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list Hillvalley_splitunnel standard permit
172.16.1.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
10.10.10.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
20.20.20.0 255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
group-policy Hillvalley internal
group-policy Hillvalley attributes
 wins-server value 10.10.10.20
 dns-server value 10.10.10.20
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Hillvalley_splitunnel
 default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted
aaa authentication telnet console LOCAL
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 ipsec transform-set Hill-trans esp-3des esp-sha-
hmac
crypto dynamic-map outside_dyn_map 20 set transform-set
Hill-trans
crypto dynamic-map dyn_map 20 set reverse-route
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 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.1
crypto map outside_map 30 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
 pre-shared-key *
tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes
 address-pool Hill-V-IP
 default-group-policy Hillvalley
tunnel-group Hillvalley ipsec-attributes
 pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48
ASA-NY-HQ#
```

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.

- **ping inside x.x.x.x(터널의 반대쪽에 있는 호스트의 IP 주소)** - 이 명령을 사용하면 내부 인터페이스의 소스 주소를 사용하여 터널을 따라 트래픽을 전송할 수 있습니다.

문제 해결

컨피그레이션 트러블슈팅을 위해 사용할 수 있는 정보는 다음 문서를 참조하십시오.

- 가장 일반적인 IPSec VPN 문제 해결 솔루션
- IP 보안 문제 해결 - 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**
- **Cisco ASA 5500 Series Adaptive Security Appliances 명령 참조**
- **기술 지원 및 문서 – Cisco Systems**