

중복 시나리오로 ASA VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[두 VPN 엔드포인트 모두에서 변환](#)

[ASA 1](#)

[사용 중인 서브넷에 필요한 개체를 만듭니다.](#)

[NAT 문 구성](#)

[변환된 서브넷으로 암호화 ACL 구성](#)

[관련 암호화 컨피그레이션](#)

[ASA 2](#)

[사용 중인 서브넷에 필요한 개체를 만듭니다.](#)

[NAT 문 구성](#)

[변환된 서브넷으로 암호화 ACL 구성](#)

[관련 암호화 컨피그레이션](#)

[다음을 확인합니다.](#)

[ASA 1](#)

[ASA 2](#)

[접치는 스포크가 있는 허브 및 스포크 토폴로지](#)

[ASA1](#)

[사용 중인 서브넷에 필요한 개체를 만듭니다.](#)

[번역할 수동 명령문 만들기:](#)

[변환된 서브넷으로 암호화 ACL 구성](#)

[관련 암호화 컨피그레이션](#)

[ASA2\(SPOKE1\)](#)

[변환된 서브넷으로 가는 암호화 ACL을 구성합니다\(10.20.20.0/24\).](#)

[관련 암호화 컨피그레이션](#)

[R1\(SPOKE2\)](#)

[변환된 서브넷으로 가는 암호화 ACL을 구성합니다\(10.30.30.0/24\).](#)

[관련 암호화 컨피그레이션](#)

[다음을 확인합니다.](#)

[ASA 1](#)

[ASA2\(SPOKE1\)](#)

[R1\(SPOKE2\)](#)

[문제 해결](#)

[보안 연결 지우기](#)

[NAT 컨피그레이션 검토](#)

[트러블슈팅 명령](#)

[관련 정보](#)

소개

이 문서에서는 중복 시나리오에서 두 ASA(Adaptive Security Appliance) 간의 LAN-to-LAN(L2L) IPsec 터널을 통해 이동하는 VPN 트래픽과 인터넷 트래픽의 PAT(Port Address Translation)를 변환하는 데 사용되는 단계를 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션 예를 진행하기 전에 Cisco ASA를 인터페이스에 IP 주소로 구성하고 기본 연결이 되어 있는지 확인하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 8.3 이상

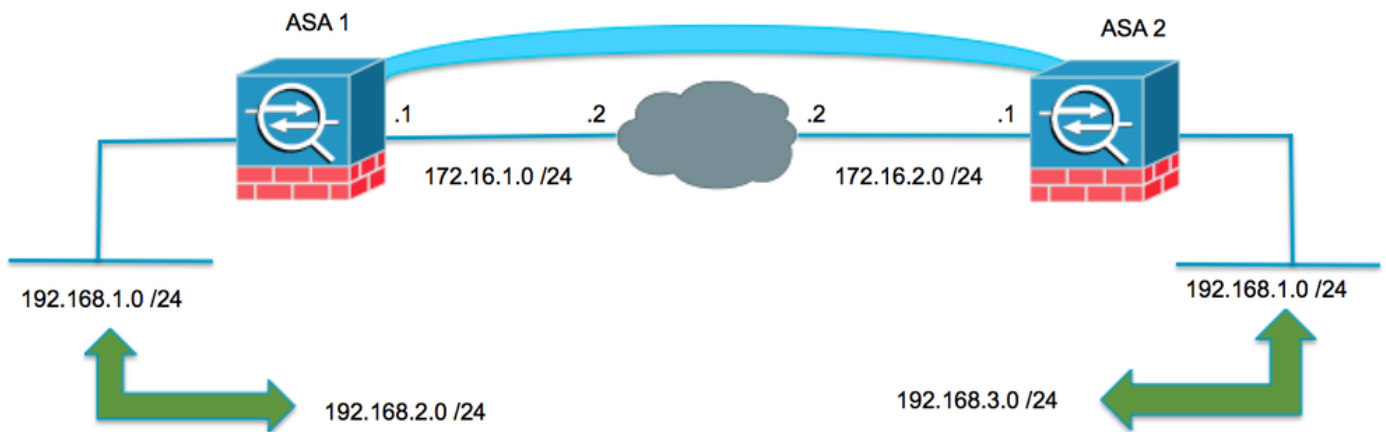
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

각 디바이스에는 보호 대상 프라이빗 네트워크가 있습니다. 중복 시나리오에서는 트래픽이 동일한 서브넷의 IP 주소로 전송되기 때문에 패킷이 로컬 서브넷을 벗어나지 않으므로 VPN을 통한 통신이 발생하지 않습니다. 다음 섹션에서 설명한 대로 NAT(Network Address Translation)를 사용하여 이 작업을 수행할 수 있습니다.

두 VPN 엔드포인트 모두에서 변환

VPN 보호 네트워크가 중복되고 두 엔드포인트에서 컨피그레이션을 수정할 수 있는 경우 NAT는 원격 변환된 서브넷으로 이동할 때 로컬 네트워크를 다른 서브넷으로 변환하는 데 사용할 수 있습니다.



ASA 1

사용 중인 서브넷에 필요한 개체를 만듭니다.

```
object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.3.0 255.255.255.0
```

NAT 문 구성

원격 서브넷으로 이동할 때만 로컬 네트워크를 다른 서브넷으로 변환하는 수동 명령문을 만듭니다 (변환됨).

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE
```

변환된 서브넷으로 암호화 ACL 구성

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

관련 암호화 컨피그레이션

```
crypto ikev1 enable outside
```

```

crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK

```

ASA 2

사용 중인 서브넷에 필요한 개체를 만듭니다.

```

object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.2.0 255.255.255.0

```

NAT 문 구성

원격 서브넷으로 이동할 때만 로컬 네트워크를 다른 서브넷으로 변환하는 수동 명령문을 만듭니다 (변환됨).

```

nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE

```

변환된 서브넷으로 암호화 ACL 구성

```

access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele

```

관련 암호화 컨피그레이션

```

crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK

```

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

ASA 1

```
ASA1(config)# sh cry isa sa
```

IKEv1 SAs:

```

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: 172.16.2.1
   Type    : L2L           Role    : initiator
   Rekey    : no           State   : MM_ACTIVE

```

There are no IKEv2 SAs

```
ASA1(config)# show crypto ipsec sa
interface: outside
```

```
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1
```

```

    access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0 255.255.255.0
    local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
    current_peer: 172.16.2.1

```

```

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: F90C149A
current inbound spi : 6CE656C7
```

inbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000003FF
```

outbound esp sas:

```
spi: 0xF90C149A (4178318490)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 16384, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28768)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

ASA 2

```
ASA2(config)# show crypto isa sa
```

IKEv1 SAs:

```
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: 172.16.1.1
   Type    : L2L                Role    : responder
   Rekey    : no                State    : MM_ACTIVE
```

There are no IKEv2 SAs

```
ASA2(config)# show crypto ipsec sa
```

```
interface: outside
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 6CE656C7
current inbound spi : F90C149A
```

inbound esp sas:

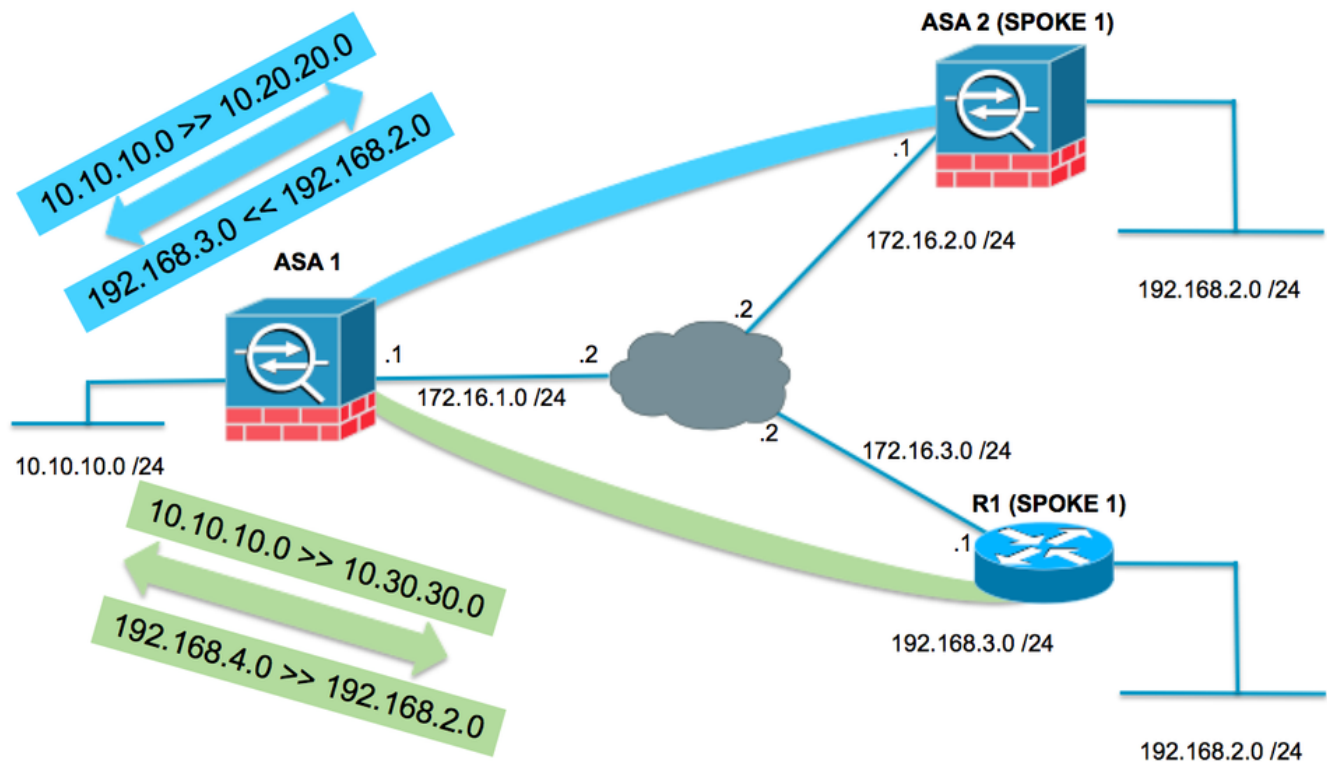
```
spi: 0xF90C149A (4178318490)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = {L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28684)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003FF
```

outbound esp sas:

```
spi: 0x6CE656C7 (1827034823)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = {L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28683)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

겹치는 스포크가 있는 허브 및 스포크 토폴로지

다음 토폴로지에서는 두 스포크의 서브넷이 동일하며, 이는 허브로 향하는 IPsec 터널을 통해 보호되어야 합니다. 스포크의 관리를 용이하게 하기 위해 NAT 컨피그레이션을 활성화하여 중첩 문제를 해결할 수 있는 작업은 허브에서만 수행됩니다.



ASA1

사용 중인 서브넷에 필요한 개체를 만듭니다.

```
object network LOCAL
  subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
  subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
  subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
  subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
  subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
  subnet 192.168.4.0 255.255.255.0
```

번역할 수동 명령문 만들기:

- SPOKE1(192.168.2.0 /24)로 이동할 때 로컬 네트워크 10.10.10.0 /24에서 10.20.20.0 /24로 이동합니다.
- 10.20.20.0 /24로 전환되는 경우 SPOKE1 네트워크 192.168.2.0 /24에서 192.168.3.0 /24로 전환됩니다.
- SPOKE3(192.168.2.0 /24)로 이동할 때 로컬 네트워크 10.10.10.0 /24에서 10.30.30.0 /24로

이동합니다.

- 10.30.30.0 /24로 전환되는 경우 SPOKE2 네트워크 192.168.2.0 /24에서 192.168.4.0 /24로 전환됩니다.

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKE1
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKE2
```

변환된 서브넷으로 암호화 ACL 구성

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

관련 암호화 컨피그레이션

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
```

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

ASA2(SPOKE1)

변환된 서브넷으로 가는 암호화 ACL을 구성합니다(10.20.20.0 /24).

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

관련 암호화 컨피그레이션

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK
```

R1(SPOKE2)

변환된 서브넷으로 가는 암호화 ACL을 구성합니다(10.30.30.0 /24).

```
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```

관련 암호화 컨피그레이션

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2

crypto isakmp key secure_PSK address 172.16.1.1

crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
  mode tunnel

crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC
```

```
interface GigabitEthernet0/1
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
media-type rj45
crypto map MYMAP
```

다음을 확인합니다.

ASA 1

```
ASA1(config)# show crypto isakmp sa
```

IKEv1 SAs:

```
Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1  IKE Peer: 172.16.3.1
   Type      : L2L           Role      : responder
   Rekey     : no           State     : MM_ACTIVE
2  IKE Peer: 172.16.2.1
   Type      : L2L           Role      : responder
   Rekey     : no           State     : MM_ACTIVE
```

There are no IKEv2 SAs

```
ASA1(config)# show crypto ipsec sa
```

interface: outside

Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

```
access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.2.1
```

```
#pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
```

current outbound spi: 79384296
current inbound spi : 2189BF7A

inbound esp sas:

spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF

outbound esp sas:

spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 12288, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/28618)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer: 172.16.3.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.3.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 65FDF4F5
current inbound spi : 05B7155D

inbound esp sas:

spi: 0x05B7155D (95884637)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:

spi: 0x65FDF4F5 (1711142133)
transform: esp-aes-256 esp-sha-hmac no compression

```
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA2(SPOKE1)

```
ASA2(config)# show crypto isakmp sa
```

IKEv1 SAs:

```
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: 172.16.1.1
   Type      : L2L                Role      : initiator
   Rekey     : no                 State     : MM_ACTIVE
```

There are no IKEv2 SAs

```
ASA2(config)# show crypto ipsec sa
interface: outside
```

```
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1
```

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 2189BF7A
current inbound spi : 79384296
```

inbound esp sas:

```
spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
```

```

in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF
outbound esp sas:
spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

R1(SPOKE2)

```

R31show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.1.1    172.16.3.1    QM_IDLE        1001 ACTIVE

IPv6 Crypto ISAKMP SA

```

```

R1#show crypto ipsec sa

interface: GigabitEthernet0/1
  Crypto map tag: MYMAP, local addr 172.16.3.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
  current outbound spi: 0x5B7155D(95884637)
  PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x65FDF4F5(1711142133)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP

```

```
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0x5B7155D(95884637)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcg sas:

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

보안 연결 지우기

문제를 해결할 때는 변경 후 기존 SA를 지워야 합니다. PIX의 특권 모드에서는 다음 명령을 사용합니다.

- clear crypto ipsec sa - 활성 IPsec SA를 삭제합니다.
- clear crypto isakmp sa - 활성 IKE SA를 삭제합니다.

NAT 컨피그레이션 검토

- show nat detail - 객체/객체 그룹이 확장된 NAT 컨피그레이션을 표시합니다.

트러블슈팅 명령

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Cisco CLI Analyzer(등록 고객만 해당)는 특정 show 명령을 지원합니다. Cisco CLI Analyzer를 사용하여 show 명령 출력의 분석을 봅니다.

 참고: 디버그 명령을 사용하기 전에 [Debug Commands](#) 및 [IP Security Troubleshooting - Understanding and Using debug Commands\(디버그 명령 및 IP 보안 문제 해결 - 디버그 명령 이해 및 사용\)](#)에 대한 중요 정보를 참조하십시오.

- debug crypto ipsec - 2단계의 IPsec 협상을 표시합니다.
- debug crypto isakmp - 1단계의 ISAKMP 협상을 표시합니다.

관련 정보

- [가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션](#)
- [IPSec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.