ASA와 Cisco IOS 라우터 간에 사이트 대 사이트 IPSec IKEv1 터널 구성

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
구성
네트워크 다이어그램
ASA 컨피그레이션
ASA 인터페이스 구성
외부 인터페이스에서 IKEv1 정책 구성 및 IKEv1 활성화
터널 그룹 구성(LAN-to-LAN 연결 프로파일)
관심 VPN 트래픽에 대한 ACL 구성
NAT 예외 구성
IKEv1 변형 집합 구성
암호화 맵 구성 및 인터페이스에 적용
ASA 최종 컨피그레이션
Cisco IOS 라우터 CLI 컨피그레이션
인터페이스 구성
ISAKMP(IKEv1) 정책 구성
암호화 ISAKMP 키 구성
관심 VPN 트래픽에 대한 ACL 구성
NAT 예외 구성
변형 집합 구성
암호화 맵 구성 및 인터페이스에 적용
Cisco IOS 최종 컨피그레이션
다음을 확인합니다.
1단계 확인
2단계 검증
1단계 및 2단계 검증
문제 해결
IPSec LAN-to-LAN 검사기 도구
ASA 디버그
Cisco IOS 라우터 디버깅
참조

소개

이 문서에서는 Cisco ASA와 Cisco IOS® 소프트웨어를 실행하는 라우터 간에 CLI를 통해 사이트 간(LAN-to-LAN) IKEv1 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS란
- Cisco ASA(Adaptive Security Appliance)
- 일반적인 IPSec 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.4(1)를 실행하는 Cisco 5512-X Series ASA
- Cisco IOS 소프트웨어 버전 15.4(3)M2를 실행하는 Cisco 1941 Series ISR(Integrated Services Router)

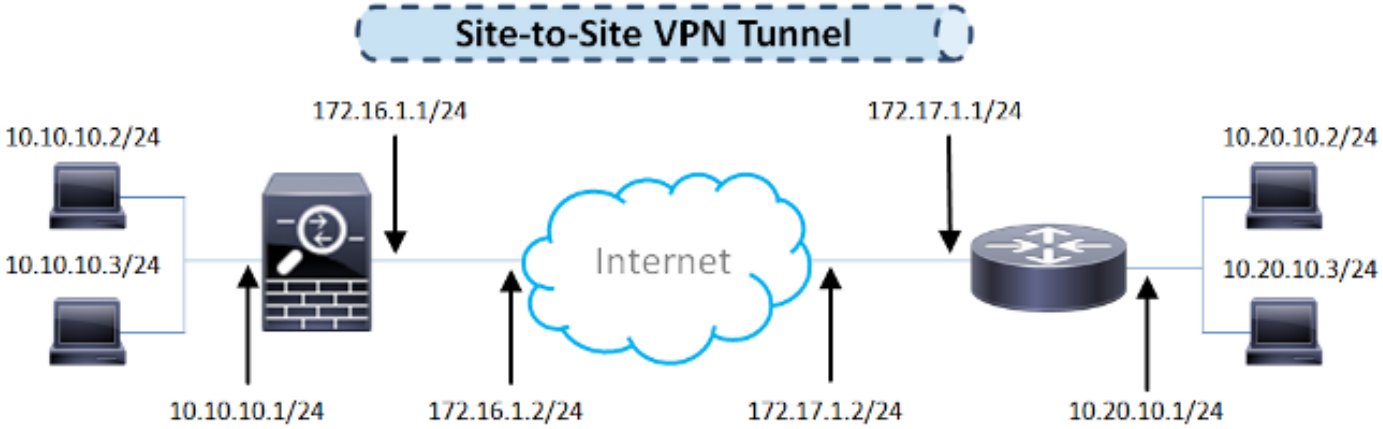
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 ASA 및 Cisco IOS 라우터 CLI 컨피그레이션을 완료하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 문서의 정보는 다음 네트워크 설정을 사용합니다.



ASA 컨피그레이션

ASA 인터페이스 구성

ASA 인터페이스가 구성되지 않은 경우 IP 주소, 인터페이스 이름 및 보안 수준 이상을 구성해야 합니다.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **참고**: 내부 및 외부 네트워크에 모두 연결되었는지, 특히 사이트 간 VPN 터널을 설정하는 데 사용되는 원격 피어에 연결되었는지 확인하십시오. 기본 연결을 확인하려면 ping을 사용할 수 있습니다.

외부 인터페이스에서 IKEv1 정책 구성 및 IKEv1 활성화

IPSec IKEv1(Internet Key Exchange Version 1) 연결을 위한 ISAKMP(Internet Security Association and Key Management Protocol) 정책을 구성하려면 crypto ikev1 policy 명령을 사용합니다:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **참고:** 두 피어의 두 정책이 모두 동일한 인증, 암호화, 해시 및 Diffie-Hellman 매개변수 값을 포함할 경우 IKEv1 정책 일치가 존재합니다. IKEv1의 경우 원격 피어 정책도 개시자가 전송하는 정책의 수명보다 작거나 같은 수명을 지정해야 합니다. 수명이 동일하지 않으면 ASA에서 더 짧은 수명을 사용합니다.

> **참고:** 지정된 정책 매개변수에 대한 값을 지정하지 않으면 기본값이 적용됩니다.

VPN 터널을 종료하는 인터페이스에서 IKEv1을 활성화해야 합니다. 일반적으로 외부(또는 공용) 인터페이스입니다. IKEv1을 활성화하려면 crypto ikev1 enable 전역 컨피그레이션 모드의 명령:

```
crypto ikev1 enable outside
```

터널 그룹 구성(LAN-to-LAN 연결 프로파일)

LAN-to-LAN 터널의 경우 연결 프로파일 유형은 ipsec-l2l . IKEv1 사전 공유 키를 구성하려면 tunnel-group ipsec-attributes 구성 모드:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

관심 VPN 트래픽에 대한 ACL 구성

ASA는 IPSec 암호화로 보호해야 하는 트래픽과 보호가 필요하지 않은 트래픽을 구분하기 위해 ACL(Access Control List)을 사용합니다. 허용 ACE(Application Control Engine)와 일치하는 아웃바운드 패킷을 보호하고 허용 ACE와 일치하는 인바운드 패킷이 보호되는지 확인합니다.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

참고: VPN 트래픽에 대한 ACL은 NAT(Network Address Translation) 이후에 소스 및 목적지 IP 주소를 사용합니다.

참고: VPN 트래픽에 대한 ACL은 두 VPN 피어 모두에서 미러링되어야 합니다.

참고: 보호되는 트래픽에 새 서브넷을 추가해야 하는 경우 해당 개체 그룹에 서브넷/호스트를 추가하고 원격 VPN 피어에서 미러 변경을 완료하면 됩니다.

NAT 예외 구성

참고: 이 섹션에서 설명하는 컨피그레이션은 선택 사항입니다.

일반적으로 VPN 트래픽에 대해 수행되는 NAT는 없어야 합니다. 해당 트래픽을 제외하려면 ID NAT 규칙을 생성해야 합니다. 아이덴티티 NAT 규칙은 단순히 주소를 동일한 주소로 변환합니다.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

IKEv1 변형 집합 구성

IKEv1 변형 집합은 ASA가 데이터를 보호하는 방법을 정의하는 보안 프로토콜과 알고리즘의 조합입니다. IPSec SA(Security Association) 협상 중에 피어는 두 피어에 대해 동일한 변형 집합 또는 제안을 식별해야 합니다. 그런 다음 ASA는 암호화 맵의 액세스 목록에서 데이터 흐름을 보호하는 SA를 생성하기 위해 일치하는 변형 집합 또는 제안서를 적용합니다.

IKEv1 변형 집합을 구성하려면 crypto ipsec ikev1 transform-set 명령을 사용합니다:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

암호화 맵 구성 및 인터페이스에 적용

암호화 맵은 IPSec SA에서 협상할 IPSec 정책을 정의하며 다음을 포함합니다.

- IPSec 연결이 허용하고 보호하는 패킷을 식별하기 위한 액세스 목록
- 피어 식별
- IPSec 트래픽의 로컬 주소
- IKEv1 변형 집합

예를 들면 다음과 같습니다.

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

그런 다음 암호화 맵을 인터페이스에 적용할 수 있습니다.

```
crypto map outside_map interface outside
```

ASA 최종 컨피그레이션

다음은 ASA의 최종 컨피그레이션입니다.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
```

```
static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

Cisco IOS 라우터 CLI 컨피그레이션

인터페이스 구성

Cisco IOS 라우터 인터페이스가 아직 구성되지 않은 경우 적어도 LAN 및 WAN 인터페이스를 구성해야 합니다. 예를 들면 다음과 같습니다.

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
no shutdown
```

내부 및 외부 네트워크 모두에, 특히 사이트 간 VPN 터널을 설정하는 데 사용되는 원격 피어에 대한 연결이 있는지 확인합니다. 기본 연결을 확인하려면 ping을 사용할 수 있습니다.

ISAKMP(IKEv1) 정책 구성

IKEv1 연결에 대한 ISAKMP 정책을 구성하려면 crypto isakmp policy 전역 컨피그레이션 모드의 명령입니다. 예를 들면 다음과 같습니다.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **참고:** IPSec에 참여하는 각 피어에서 여러 IKE 정책을 구성할 수 있습니다. IKE 협상이 시작되면 두 피어 모두에 구성된 공통 정책을 찾으려고 시도하며, 원격 피어에 지정된 우선순위가 가장 높은 정책으로 시작합니다.

암호화 ISAKMP 키 구성

사전 공유 인증 키를 구성하려면 crypto isakmp key 전역 컨피그레이션 모드의 명령:

```
crypto isakmp key cisco123 address 172.16.1.1
```

관심 VPN 트래픽에 대한 ACL 구성

암호화로 보호해야 하는 트래픽을 지정하려면 확장 또는 명명된 액세스 목록을 사용합니다. 예를 들면 다음과 같습니다.

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

참고: VPN 트래픽에 대한 ACL은 NAT 뒤에 소스 및 목적지 IP 주소를 사용합니다.

참고: VPN 트래픽에 대한 ACL은 두 VPN 피어 모두에서 미러링되어야 합니다.

NAT 예외 구성

참고: 이 섹션에서 설명하는 컨피그레이션은 선택 사항입니다.

일반적으로 VPN 트래픽에 대해 수행되는 NAT는 없어야 합니다. NAT 오버로드가 사용되는 경우 변환에서 관심 VPN 트래픽을 제외하려면 경로 맵을 사용해야 합니다. 경로 맵에서 사용되는 access-list에서 관심 VPN 트래픽은 거부되어야 합니다.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

변형 집합 구성

IPSec 변형 집합(보안 프로토콜과 알고리즘의 적절한 조합)을 정의하려면 crypto ipsec transform-set 전역 컨피그레이션 모드의 명령입니다. 예를 들면 다음과 같습니다.

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

암호화 맵 구성 및 인터페이스에 적용

암호화 맵 엔트리를 생성하거나 수정하고 암호화 맵 컨피그레이션 모드를 시작하려면 crypto map 글로벌 **컨피그레이션** 명령을 입력합니다. 암호화 맵 엔트리를 완료하려면 몇 가지 측면을 정의해야 합니다.

- 보호된 트래픽을 전달할 수 있는 IPsec 피어를 정의해야 합니다. SA를 설정할 수 있는 피어입니다. 암호화 맵 엔트리에서 IPSec 피어를 지정하려면 set peer 명령을 실행합니다.
- 보호된 트래픽과 함께 사용할 수 있는 변형 집합을 정의해야 합니다. 암호화 맵 엔트리와 함께 사용할 수 있는 변환 세트를 지정하려면 set transform-set 명령을 실행합니다.
- 보호해야 하는 트래픽을 정의해야 합니다. 암호화 맵 엔트리에 대한 확장 액세스 목록을 지정하려면 match address 명령을 실행합니다.

예를 들면 다음과 같습니다.

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

마지막 단계는 이전에 정의된 암호화 맵 세트를 인터페이스에 적용하는 것입니다. 이를 적용하려면 crypto map interface configuration 명령:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Cisco IOS 최종 컨피그레이션

다음은 최종 Cisco IOS 라우터 CLI 컨피그레이션입니다.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
```

```
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

다음을 확인합니다.

터널이 작동 중인지, 트래픽을 전달하는지 확인하기 전에 해당 트래픽이 ASA 또는 Cisco IOS 라우터로 전송되는지 확인해야 합니다.

> **참고:** ASA에서는 IPSec 터널을 시작하기 위해 관심 트래픽과 일치하는 패킷 추적기 툴을 사용할 수 있습니다(예: packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed 예를 들어).

1단계 확인

ASA에서 IKEv1 1단계가 작동 중인지 확인하려면 show crypto isakmp **sa 명령을** 입력합니다. 예상 출력은 MM_ACTIVE 상태:

```
ciscoasa# 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: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

IKEv1 1단계가 Cisco IOS에서 작동 중인지 확인하려면 show crypto isakmp sa 명령을 실행합니다. 예상 출력은 ACTIVE 상태:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
Router#
```

2단계 검증

ASA에서 IKEv1 2단계가 작동 중인지 확인하려면 show crypto ipsec sa 명령을 실행합니다. 필요한 출력은 인바운드 및 아웃바운드 SPI(Security Parameter Index)를 모두 보는 것입니다. 트래픽이 터널을 통과하는 경우 encaps/decaps 카운터가 증가해야 합니다.

> **참고:** 각 ACL 항목에 대해 별도의 인바운드/아웃바운드 SA가 생성되므로 시간이 오래 걸릴 수 있습니다 show crypto ipsec sa 명령 출력(암호화 ACL의 ACE 항목 수에 따라 다름)

예를 들면 다음과 같습니다.

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
 10.20.10.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


#pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #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.: 172.17.1.1/0
     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: 8A9FE619
     current inbound spi : D8639BD0

inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
```

```
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

IKEv1 2단계가 Cisco IOS에서 작동 중인지 확인하려면 show crypto ipsec sa 명령을 실행합니다. 필요한 출력은 인바운드 및 아웃바운드 SPI를 모두 보는 것입니다. 트래픽이 터널을 통과하는 경우 encaps/decaps 카운터가 증가해야 합니다.

예를 들면 다음과 같습니다.

```
Router#show crypto ipsec sa peer 172.16.1.1

interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
```

```
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

1단계 및 2단계 검증

이 섹션에서는 1단계와 2단계 모두의 세부사항을 확인하기 위해 ASA 또는 Cisco IOS에서 사용할 수 있는 명령에 대해 설명합니다.

다음을 입력합니다. show vpn-sessiondb 확인할 ASA의 명령:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
 Tunnel ID    : 2.1
 UDP Src Port : 500                   UDP Dst Port : 500
 IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
 Encryption   : AES128                Hashing      : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 Filter Name  :

IPsec:
 Tunnel ID    : 2.2
 Local Addr   : 10.10.10.0/255.255.255.0/0/0
 Remote Addr  : 10.20.10.0/255.255.255.0/0/0
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds          Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes            Idle TO Left : 26 Minutes
 Bytes Tx     : 100500                Bytes Rx     : 101400
 Pkts Tx      : 1005                  Pkts Rx      : 1014

NAC:
 Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds             EoU Age(T)   : 309 Seconds
 Hold Left (T): 0 Seconds             Posture Token:
 Redirect URL :

ciscoasa#
```

다음을 입력합니다. show crypto session 확인을 위한 Cisco IOS 명령:

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

문제 해결

이 섹션에서는 컨피그레이션의 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:** 를 사용하기 전에 Debug Commands and IP Security Troubleshooting - Understanding and Using debug Commands Cisco 문서에 대한 중요 정보를 참조하십시오 debug 명령을 사용합니다.

IPSec LAN-to-LAN 검사기 도구

ASA와 Cisco IOS 간의 IPSec LAN-to-LAN 컨피그레이션이 유효한지 자동으로 확인하려면 IPSec LAN-to-LANChecker 툴을 사용할 수 있습니다. 이 툴은 Firepower Threat Defense에서 show tech 또는 show running-config ASA 또는 Cisco IOS 라우터의 명령입니다. 컨피그레이션을 검사하고 암호화 맵 기반 LAN-to-LAN IPSec 터널이 구성되었는지 탐지를 시도합니다. 구성된 경우, 컨피그레이션의 다중 지점 확인을 수행하고 협상할 터널에 대한 컨피그레이션 오류 및 설정을 강조 표시합니다.

ASA 디버그

ASA 방화벽에서 IPSec IKEv1 터널 협상 문제를 해결하려면 다음 명령을 사용할 수 있습니다 debug 명령:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

참고: ASA의 VPN 터널 수가 많은 경우 debug crypto condition peer A.B.C.D 지정된 피어만 포함하도록 디버그 출력을 제한하려면 디버그를 활성화하기 전에 명령을 사용해야 합니다.

Cisco IOS 라우터 디버깅

Cisco IOS 라우터에서 IPSec IKEv1 터널 협상 문제를 해결하려면 다음 debug 명령을 사용할 수 있습니다.

```
debug crypto ipsec
debug crypto isakmp
```

참고: Cisco IOS의 VPN 터널 수가 많은 경우 debug crypto condition peer ipv4 A.B.C.D 디버그 출력이 지정된 피어만 포함하도록 제한하려면 디버그를 활성화하기 전에 사용해야 합니다.

팁: Site-to-Site VPN 문제 해결 방법에 대한 자세한 내용은 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션 Cisco 문서를 참조하십시오.

참조

- 디버그 명령에 대한 중요 정보
- IP 보안 트러블슈팅 - 디버그 명령 이해 및 사용
- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- IPSec LAN-to-LAN 검사기
- 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.