IKEv2 다중 키 교환을 사용하여 두 ASA 간에 Site-to-Site IKEv2 터널 구성

목차

소개

이 문서에서는 IKEv2 다중 키 교환을 사용하여 두 Cisco ASA 간에 사이트 대 사이트 IKEv2 VPN 연결을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA(Adaptive Security Appliance)
- 일반 IKEv2 개념

사용되는 구성 요소

이 문서의 정보는 9.20.1을 실행하는 Cisco ASA를 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

제한 사항

IKEv2 다중 키 교환에는 다음과 같은 제한이 있습니다.

- ASA CLI에서만 지원됨
- 다중 컨텍스트 및 HA 디바이스에서 지원됨
- 클러스터링된 디바이스에서 지원되지 않음

라이센싱

라이센싱 요구 사항은 ASA의 Site-to-Site VPN과 동일합니다.

배경 정보

추가 키 교환 필요

빅 양자 컴퓨터의 도래는 보안 시스템, 특히 공개 키 암호 기술을 사용하는 시스템에 큰 위험을 초래한다. 일반 컴퓨터에 매우 어렵다고 생각되었던 암호화 방법은 양자 컴퓨터에 의해 쉽게 깨질 수 있다. 따라서 포스트 양자 암호(PQC) 알고리즘이라고도 하는 새로운 양자 내성 방법으로 전환할 필요가 생긴다. 다중 키 교환을 사용하여 IPsec 통신의 보안을 강화하는 것이 목적입니다. 여기에는 전통적인 키 교환과 포스트 양자 교환이 포함됩니다. 이러한 접근 방식을 통해 기존 키 교환 못지않게 강력한 교환 기능을 확보하여 한층 강화된 보안 레이어를 구현할 수 있습니다.

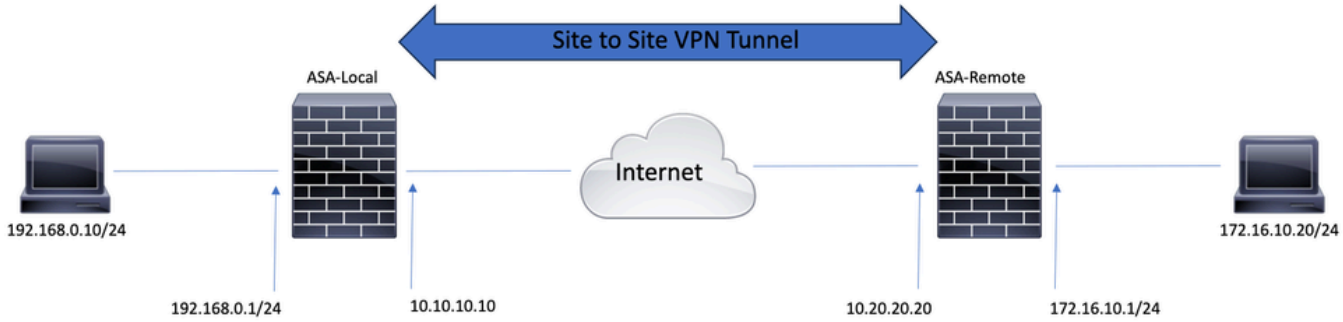
여러 키 교환에 대한 지원을 추가하여 IKEv2를 개선하는 계획입니다. 이러한 여분의 키 교환은 양자 위협으로부터 안전한 알고리즘을 처리할 수 있다. 이러한 추가 키에 대한 정보를 교환하기 위해 Intermediate Exchange라는 새 메시지 유형이 도입되었습니다. 이러한 키 교환은 SA 페이로드를 통해 일반 IKEv2 방법을 사용하여 협상됩니다.

구성

이 섹션에서는 ASA 컨피그레이션에 대해 설명합니다.

네트워크 다이어그램

이 문서의 정보는 다음 네트워크 설정을 사용합니다.

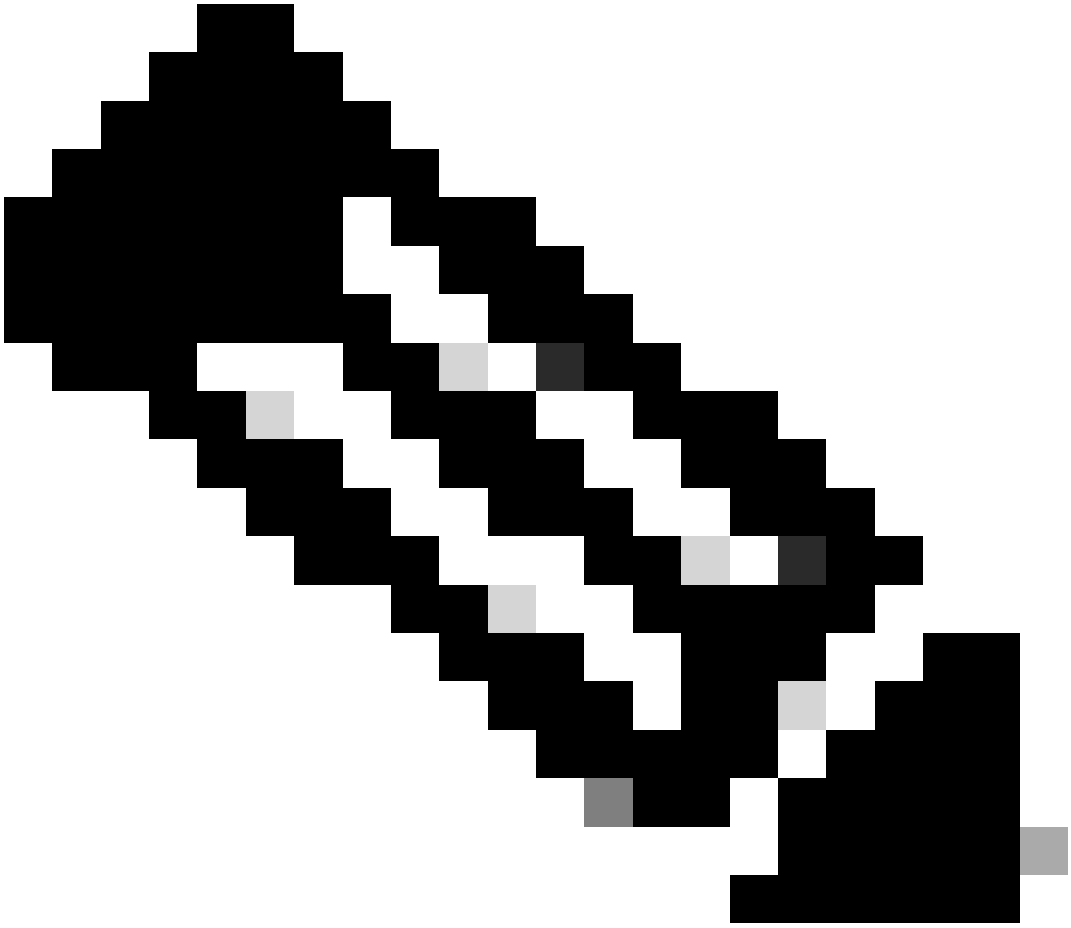


ASA 컨피그레이션

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 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```



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

다중 키 교환으로 IKEv2 정책 구성 및 외부 인터페이스에서 IKEv2 활성화

이러한 연결에 대한 IKEv2 정책을 구성하려면 다음 명령을 입력합니다.

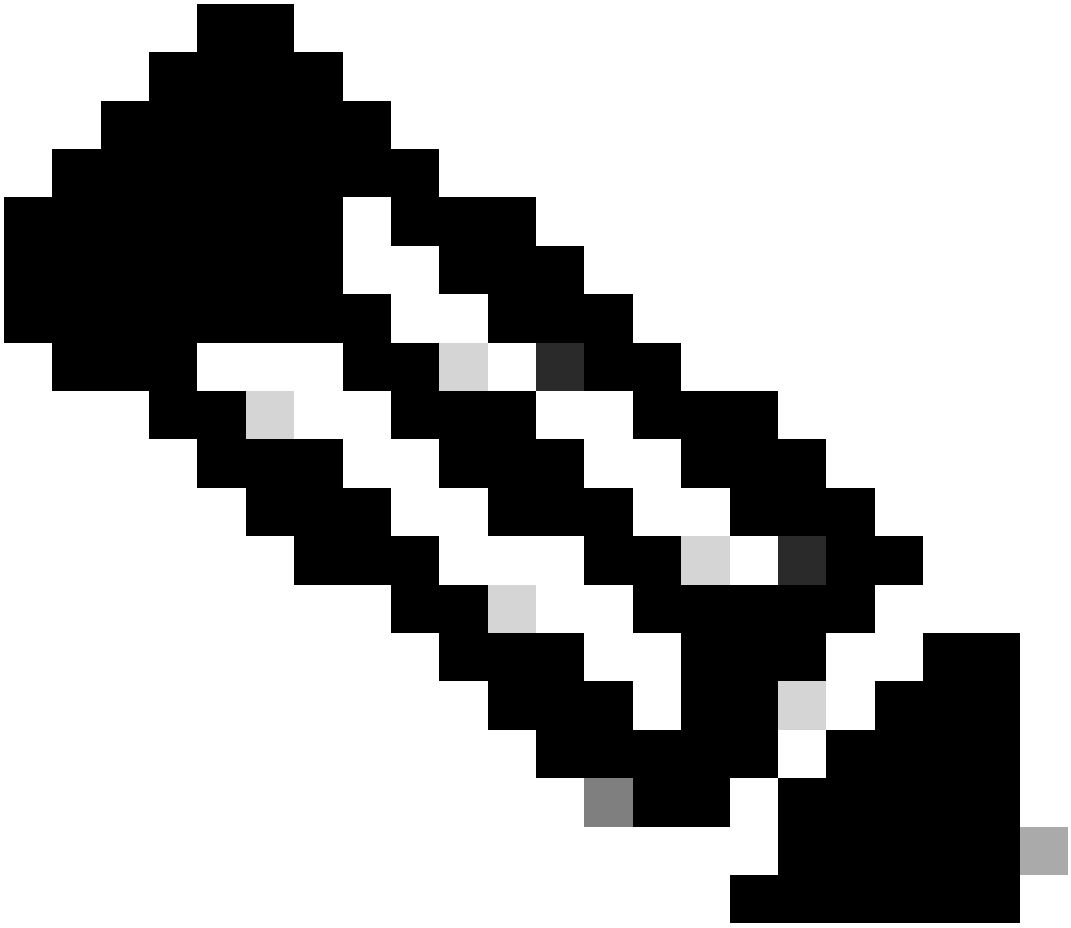
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

명령을 사용하여 추가 키 교환 변환을crypto ikev2 policy 아래에서 구성할 수 additional-key-exchange 있습니다. 총 7개의 추가 교환 변환을 구성할 수 있습니다. 이 예에서는 두 개의 추가 교환 변환이 구성되었습니다(DH 그룹 21 및 31 사용).

```
additional-key-exchange 1 key-exchange-method 21 additional-key-exchange 2 key-exchange-method 31
```

최종 IKEv2 정책은 다음과 같습니다.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



참고: 두 피어의 두 정책이 모두 동일한 인증, 암호화, 해시, Diffie-Hellman 매개변수 및 Additional Key Exchange 매개변수 값을 포함하는 경우 IKEv2 정책 일치가 존재합니다.

VPN 터널을 종료하는 인터페이스에서 IKEv2를 활성화해야 합니다. 일반적으로 외부(또는 인터넷) 인터페이스입니다. IKEv2를 활성화하려면 글로벌 컨피그레이션 모드에서crypto ikev2 enable outside 명령을 입력합니다.

터널 그룹 구성

Site-to-Site 터널의 경우 연결 프로파일 유형은 IPSec-l2l입니다. IKEv2 사전 공유 키를 구성하려면 다음 명령을 입력합니다.

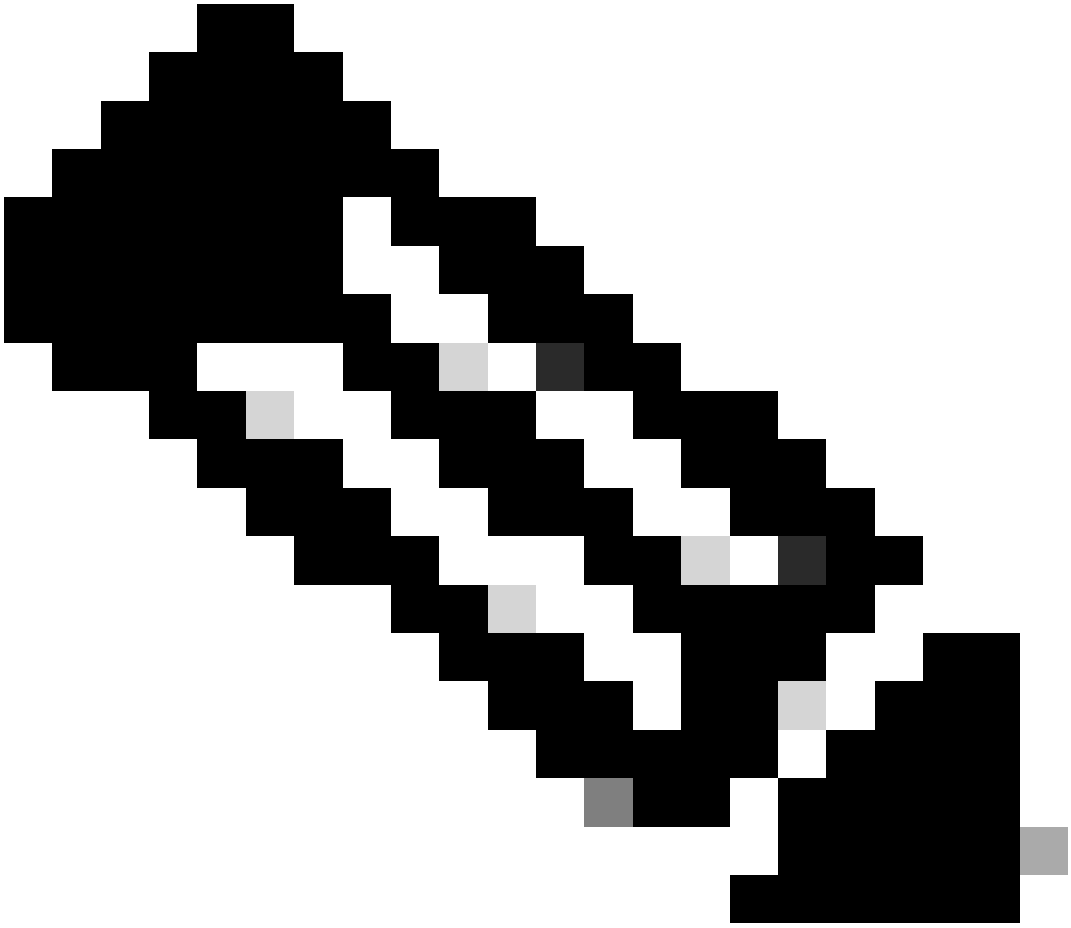
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

관심 트래픽 및 암호화 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 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
```

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



참고: VPN 피어의 ACL은 미러된 형식이어야 합니다.

ID NAT 구성(선택 사항)

일반적으로 ID NAT는 흥미로운 트래픽이 동적 NAT에 도달하는 것을 방지하기 위해 필요합니다. 이 경우 구성되는 ID NAT는 다음과 같습니다.

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

IKEv2 IPSec 제안 구성

IKEv2 IPSec 제안은 데이터 트래픽을 보호하기 위해 암호화 및 무결성 알고리즘 집합을 정의하는 데 사용됩니다. 이 제안서는 IPSec SA를 성공적으로 구축하기 위해 두 VPN 피어와 일치해야 합니다. 이 경우에 사용되는 명령은 다음과 같습니다.

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

암호화 맵을 구성하고 인터페이스에 바인딩합니다.

암호화 맵은 모든 필수 컨피그레이션을 통합하며 반드시 다음을 포함해야 합니다.

- 암호화해야 하는 트래픽과 일치하는 액세스 목록(일반적으로 암호화 ACL이라고 함)
- 피어 ID
- 하나 이상의 IKEv2 IPSec 제안

여기서 사용되는 컨피그레이션은 다음과 같습니다.

crypto map outside_map 1 match address asa-vpn crypto map outside_map 1 set peer 10.20.20.20 crypto map outside_map 1 set ikev2 ipsec-proposal IKEV

마지막 단계에서는 명령을 사용하여 외부(공용) 인터페이스에 이 암호화 맵을 crypto map outside_map interface outside 적용합니다.

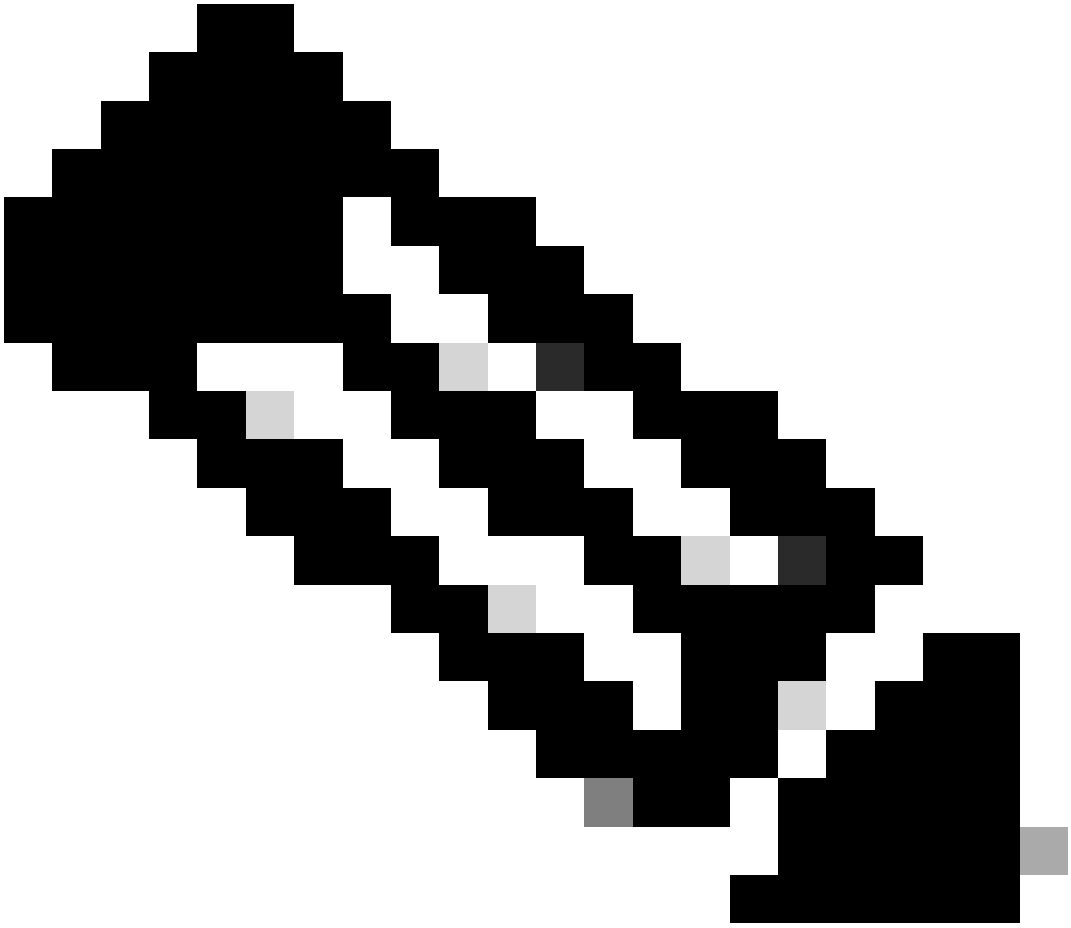
로컬 ASA 최종 컨피그레이션

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
```

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
!
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
!
access-list asa-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 ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

원격 ASA 최종 컨피그레이션

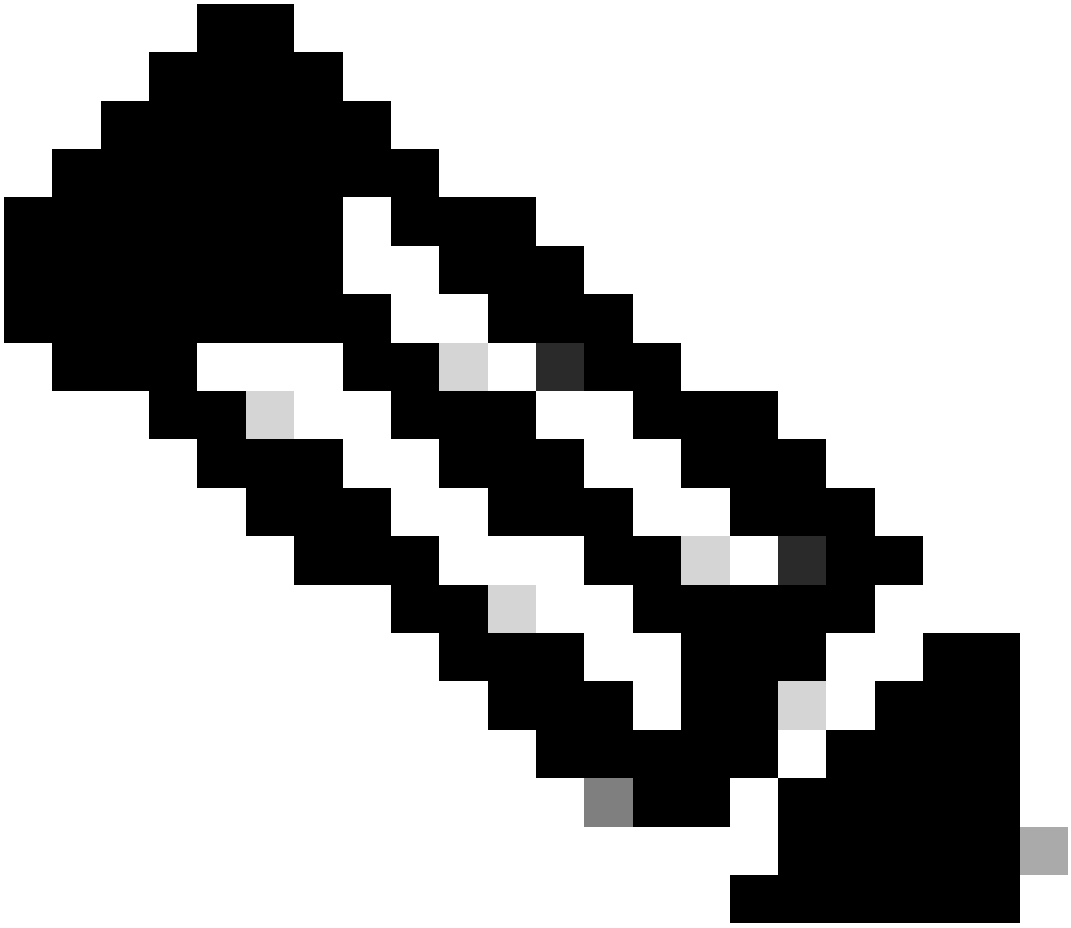
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



참고: ACL은 미러 형식이며 사전 공유 키는 양쪽 끝에서 동일합니다.

다음을 확인합니다.

터널이 작동 중인지, 그리고 트래픽을 전달 중인지 확인하기 전에 흥미로운 트래픽이 ASA로 전송되는지 확인해야 합니다.



참고: 패킷 추적기는 트래픽 흐름을 시뮬레이션하기 위해 사용되었습니다. 이 작업은 packet-tracer 명령을 사용하여 수행할 수 있습니다. packet-tracer input inside icmp Local-ASA에 대한 자세한 내용은 192.168.0.11 8 0 172.16.10.11을 참조하십시오.

추가 키 교환을 검증하려면 명령을 사용할 수 show crypto ikev2 sa 있습니다. 출력에서 볼 수 있듯이, AKE 매개변수를 확인하여 선택된 교환 알고리즘을 검증할 수 있습니다.

<#root>

Local-ASA# show crypto ikev2 sa IKEv2 SAs: Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status R

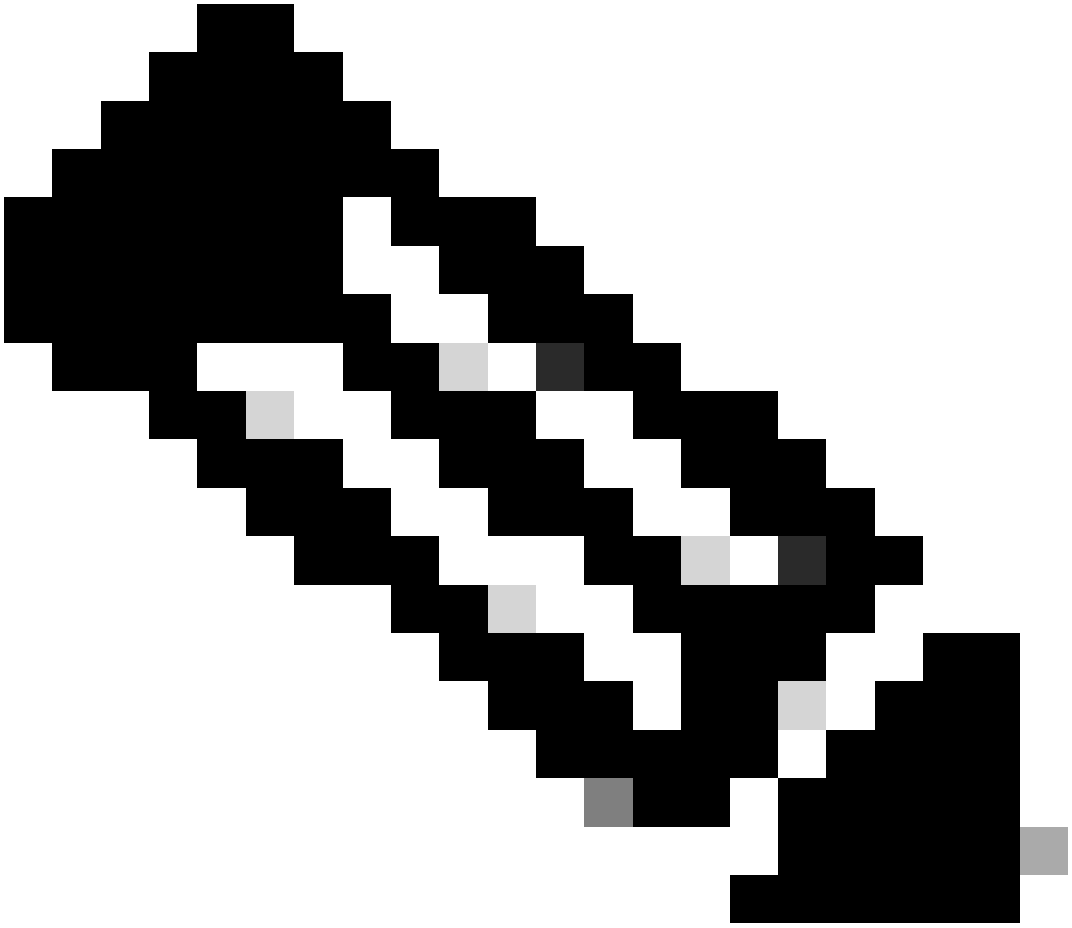
AKE1: 21 AKE2: 31

```
 Life/Active Time: 86400/7 sec Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535 remote sele
```

문제 해결

언급된 디버그는 IKEv2 터널의 문제를 해결하는 데 사용할 수 있습니다.

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```



참고: 하나의 터널만 트러블슈팅하려면(디바이스가 프로덕션 상태일 경우) debug crypto condition peer X.X.X.X 명령을 사용하여 조건부로 디버그를 활성화해야 합니다.

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.