ISE 3.3 Native IPsec to Secure NAD(IOS-XE) 통신 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Service Engine) 3.3 - NAD(Network Access Device) 통신을 보호하기 위해 Native IPsec을 구성하고 문제를 해결하는 방법에 대해 설명합니다. Radius 트래픽은 Switch와 ISE 간의 Site-to-Site(LAN-to-LAN) IPsec IKEv2(Internet Key Exchange Version 2) 터널로 암호화할 수 있습니다. 이 문서에서는 RADIUS 컨피그레이션 부분을 다루지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE
- Cisco 스위치 컨피그레이션
- 일반 IPsec 개념
- 일반 RADIUS 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 17.6.5를 실행하는 Cisco Catalyst 스위치 C9200L
- Cisco Identity Service Engine 버전 3.3
- Windows 10

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.

배경 정보

목표는 IPsec을 통해 안전하지 않은 MD5 해시, RADIUS 및 TACACS를 사용하는 프로토콜을 보호하는 것입니다. 고려해야 할 몇 가지 사실:

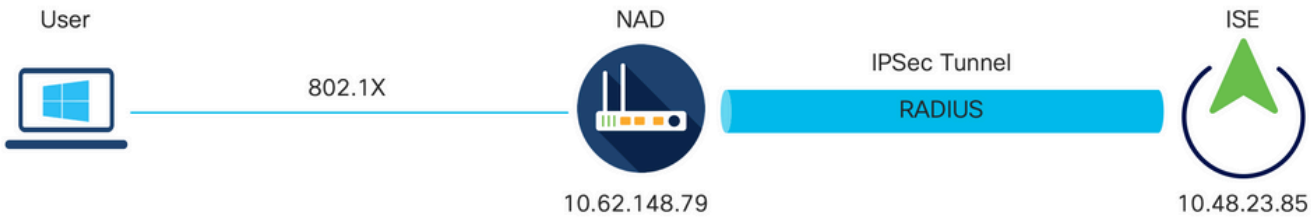
- Cisco ISE Native IPsec 솔루션은 StrongSwan을 기반으로 구축됨
- Cisco ISE 인터페이스에서 IPsec을 구성하면 Cisco ISE와 NAD 간에 IPsec 터널이 생성되어 통신을 보호합니다. NAD는 Native IPsec Settings(기본 IPsec 설정)에서 별도로 구성해야 합니다.

- 사전 공유 키를 정의하거나 IPsec 인증에 X.509 인증서를 사용할 수 있습니다.
- IPsec은 GigabitEthernet1~GigabitEthernet5 인터페이스에서 활성화할 수 있습니다.

이 문서의 주 목표는 X.509 인증서 인증을 다루는 것입니다. Verify and Troubleshoot(확인 및 트러블슈팅) 섹션에서는 X.509 인증서 인증에만 초점을 맞춥니다. 디버깅은 사전 공유 키 인증과 동일해야 하며 출력 차이만 있습니다. 동일한 명령을 검증에도 사용할 수 있습니다.

X.509 인증서 인증을 사용하여 IKEv2 IPsec 터널 구성

네트워크 다이어그램



네트워크 다이어그램

IOS-XE 스위치 CLI 컨피그레이션

인터페이스 구성

IOS-XE 스위치 인터페이스가 아직 구성되지 않은 경우 하나 이상의 인터페이스를 구성해야 합니다. 예를 들면 다음과 같습니다.

```
interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 negotiation auto
 no shutdown
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
```

Site-to-Site VPN 터널을 설정하기 위해 사용해야 하는 원격 피어에 대한 연결이 있는지 확인합니다. 기본 연결을 확인하려면 ping을 사용할 수 있습니다.

신뢰 지점 구성

IKEv2 정책을 구성하려면 글로벌 컨피그레이션 모드에서 crypto pki trustpoint <name> 명령을 입력합니다. 예를 들면 다음과 같습니다.

참고: IOS-XE 디바이스에는 여러 가지 방법으로 인증서를 설치할 수 있습니다. 이 예에서는 ID 인증서 및 해당 체인을 포함하는 pkcs12 파일 가져오기를 사용합니다

```
crypto pki trustpoint KrakowCA
 revocation-check none
```

인증서 가져오기

IOS-XE ID 인증서를 체인과 함께 가져오려면 특별 권한 모드에서 crypto pki import <trustpoint> pkcs12 <location> password <password> 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
KSEC-9248L-1#crypto pki import KrakowCA pkcs12 ftp://eugene:<ftp-password>@10.48.17.90/ISE/KSEC-9248L-1
% Importing pkcs12...Reading file from ftp://eugene@10.48.17.90/ISE/KSEC-9248L-1.pfx!
[OK - 3474/4096 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully.
KSEC-9248L-1#
```

참고: 인증서가 문서의 범위에 속하지 않더라도 IOS-XE ID 인증서에 FQDN/IP 주소로 채워진 SAN 필드가 있는지 확인하십시오. ISE에는 SAN 필드가 있어야 하는 피어 인증서가 필요합니다.

인증서가 제대로 설치되었는지 확인하려면 다음을 수행합니다.

```
KSEC-9248L-1#sh crypto pki certificates KrakowCA
Certificate
  Status: Available
  Certificate Serial Number (hex): 4B6793F0FE3A6DA5
  Certificate Usage: General Purpose
  Issuer:
    cn=KrakowCA
  Subject:
    Name: KSEC-9248L-1.example.com
    IP Address: 10.62.148.79
    cn=KSEC-9248L-1.example.com
  Validity Date:
    start date: 17:57:00 UTC Apr 20 2023
    end date: 17:57:00 UTC Apr 19 2024
  Associated Trustpoints: KrakowCA
  Storage: nvram:KrakowCA#6DA5.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
```

```
    cn=KrakowCA
  Subject:
    cn=KrakowCA
  Validity Date:
    start date: 10:16:00 UTC Oct 19 2018
    end date: 10:16:00 UTC Oct 19 2028
  Associated Trustpoints: KrakowCA
  Storage: nvram:KrakowCA#1CA.cer

KSEC-9248L-1#
```

IKEv2 제안 구성

IKEv2 정책을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 proposal <name> 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 16
!
```

암호화 IKEv2 정책 구성

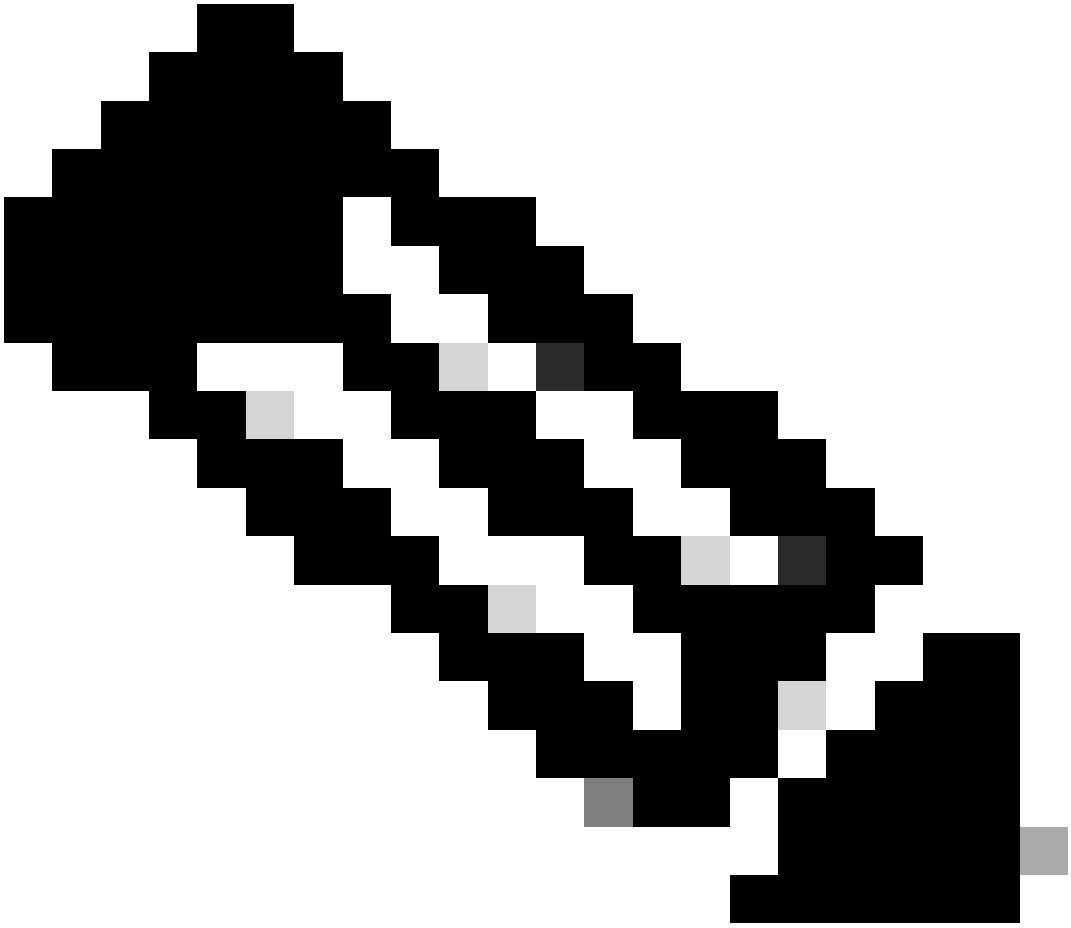
IKEv2 정책을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 policy <name> 명령을 입력합니다.

```
crypto ikev2 policy POLICY
 proposal PROPOSAL
```

암호화 IKEv2 프로파일 구성

IKEv2 프로필을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 profile <name> 명령을 입력합니다.

```
crypto ikev2 profile PROFILE
 match address local 10.62.148.79
 match identity remote fqdn domain example.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint KrakowCA
```



참고: 기본적으로 ISE는 IKEv2 협상에서 자체 ID 인증서의 CN 필드를 IKE ID로 사용합니다. 따라서 IKEv2 프로필의 "match identity remote" 섹션에서 FQDN 유형과 ISE의 도메인 또는 FQDN의 적절한 값을 지정해야 합니다.

관심 VPN 트래픽에 대한 ACL 구성

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

```
ip access-list extended 100
 10 permit ip host 10.62.148.79 host 10.48.23.85
```

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

변형 집합 구성

IPsec 변형 집합(보안 프로토콜과 알고리즘의 적절한 조합)을 정의하려면 글로벌 컨피그레이션 모드에서 crypto ipsec transform-set 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
 mode tunnel
```

암호화 맵 구성 및 인터페이스에 적용

암호화 맵 엔트리를 생성하거나 수정하고 암호화 맵 컨피그레이션 모드로 들어가려면 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 입력합니다.
- 보호된 트래픽과 함께 사용할 수 있는 변형 집합을 정의해야 합니다. 암호화 맵 엔트리와 함께 사용할 수 있는 변환 세트를 지정하려면 set transform-set 명령을 입력합니다.
- 보호해야 하는 트래픽을 정의해야 합니다. 암호화 맵 엔트리에 대한 확장 액세스 목록을 지정하려면 match address 명령을 입력합니다.

예를 들면 다음과 같습니다.

```
crypto map MAP-IKEV2 10 ipsec-isakmp
 set peer 10.48.23.85
 set transform-set SET
 set pfs group16
 set ikev2-profile PROFILE
 match address 100
```

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

```
interface Vlan480
 crypto map MAP-IKEV2
```

IOS-XE 최종 컨피그레이션

다음은 최종 IOS-XE 스위치 CLI 컨피그레이션입니다.

```
aaa new-model
!
aaa group server radius ISE
 server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
 client 10.48.23.85
 server-key cisco
!
crypto pki trustpoint KrakowCA
 enrollment pkcs12
 revocation-check none
!
dot1x system-auth-control
!
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 16
!
crypto ikev2 policy POLICY
 proposal PROPOSAL
!
crypto ikev2 profile PROFILE
 match address local 10.62.148.79
 match identity remote fqdn domain example.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint KrakowCA
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
 mode tunnel
!
crypto map MAP-IKEV2 10 ipsec-isakmp
 set peer 10.48.23.85
 set transform-set SET
 set pfs group16
 set ikev2-profile PROFILE
 match address 100
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 crypto map MAP-IKEV2
!
ip access-list extended 100
 10 permit ip host 10.62.148.79 host 10.48.23.85
!
radius server ISE33-2
 address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
 key cisco
!
```

ISE 구성

ISE에서 IP 주소 구성

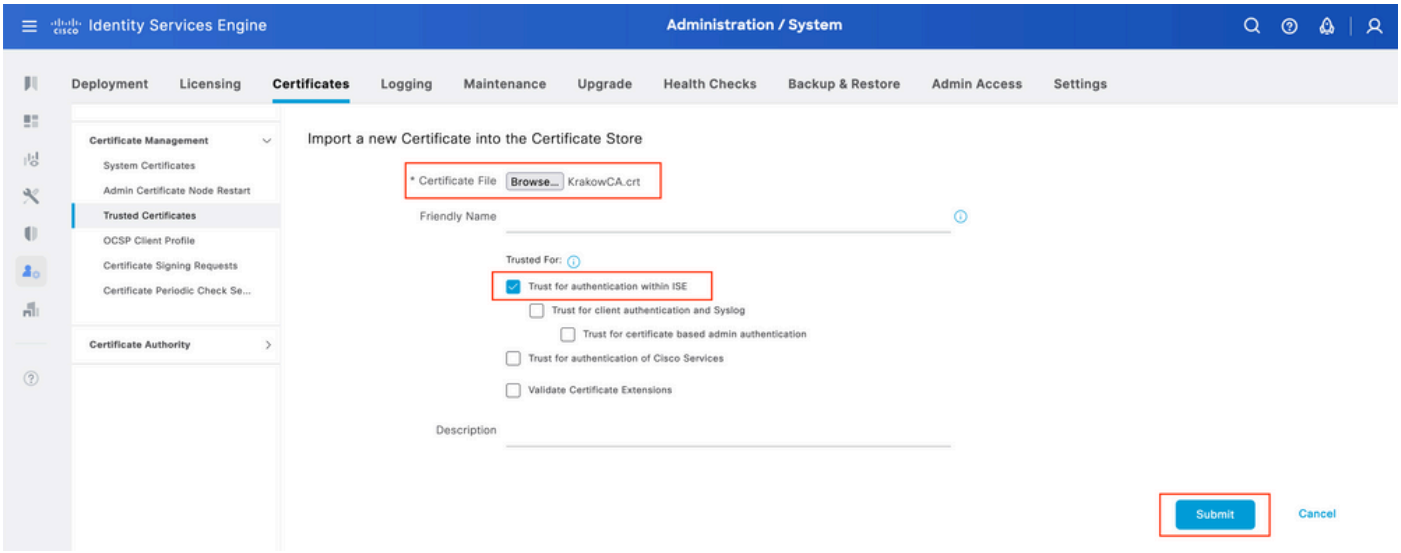
CLI에서 인터페이스 GE1-GE5에 주소를 구성해야 합니다. GE0은 지원되지 않습니다.

```
interface GigabitEthernet 1
  ip address 10.48.23.85 255.255.255.0
  ipv6 address autoconfig
  ipv6 enable
```

참고: 인터페이스에 IP 주소가 구성된 후 애플리케이션이 다시 시작됩니다.
IP 주소를 변경하면 ISE 서비스가 다시 시작될 수 있습니다.
IP 주소 변경을 계속하시겠습니까? Y/N [N]: Y

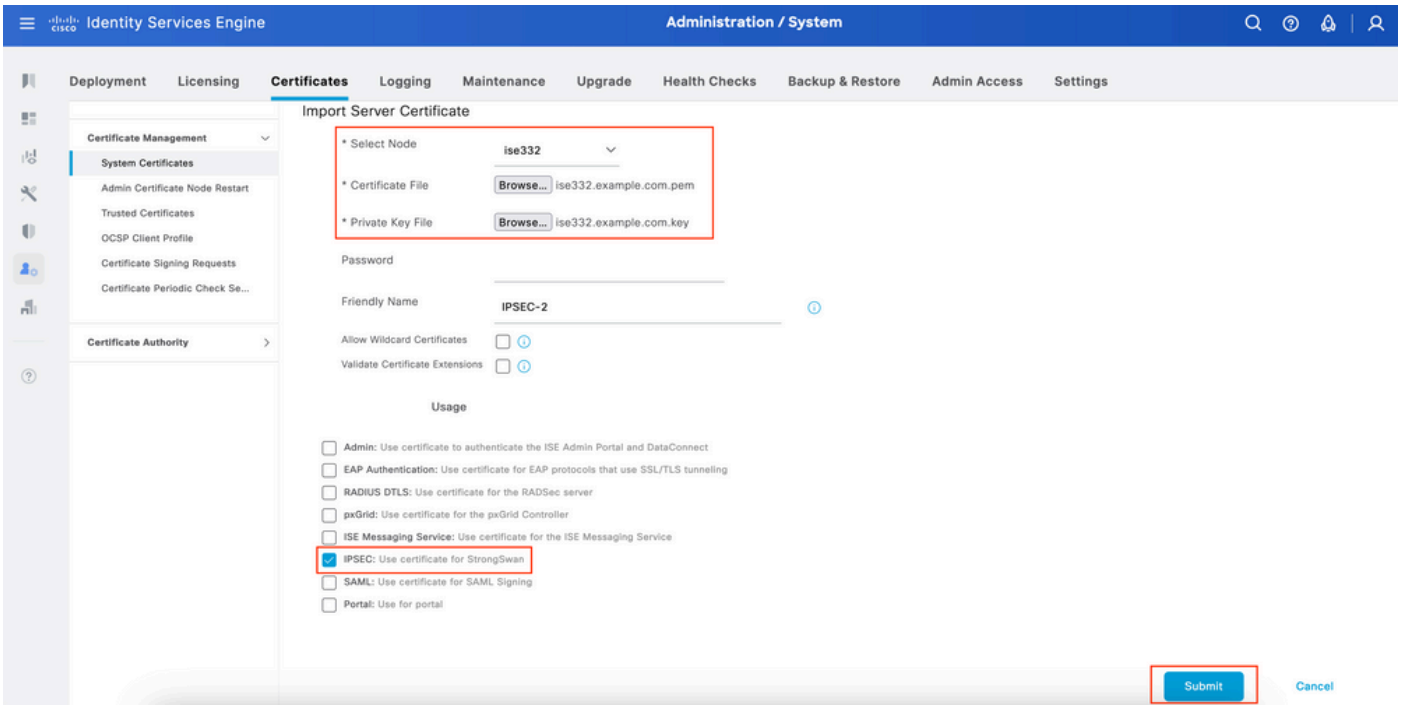
신뢰할 수 있는 저장소 인증서 가져오기

이 단계는 ISE가 터널이 설정될 때 제공되는 피어의 인증서를 신뢰하는지 확인하는 데 필요합니다. Administration(관리) > System(시스템) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동합니다. Import(가져오기)를 클릭합니다. Browse(찾아보기)를 클릭하고 ISE/IOS-XE ID 인증서를 서명한 CA 인증서를 선택합니다. Trust for authentication within ISE(ISE 내 인증 신뢰) 확인란이 선택되어 있는지 확인합니다. Submit(제출)을 클릭합니다.



시스템 인증서 가져오기

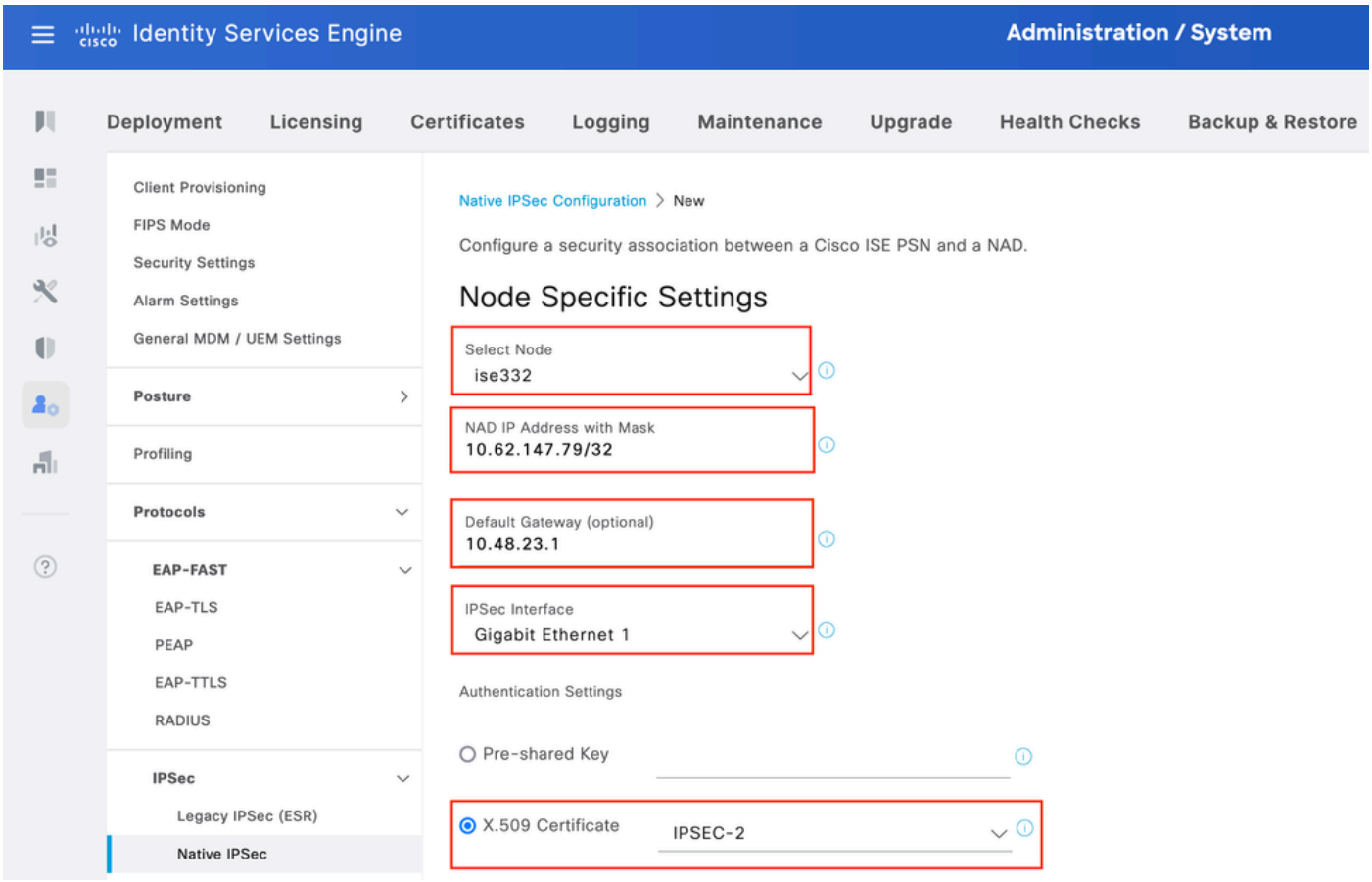
Administration(관리) > System(시스템) > Certificates(인증서) > System Certificates(시스템 인증서)로 이동합니다. Node(노드), Certificate File(인증서 파일) 및 Private Key File Import(개인 키 파일 가져오기)를 선택합니다. IPsec에 대한 확인란을 선택합니다. Submit(제출)을 클릭합니다.



참고: Native IPsec Settings(기본 IPsec 설정)에서 Save Network Access Device(네트워크 액세스 디바이스 저장)를 수행한 후에만 인증서가 StrongSwan에 설치됩니다.

IPsec 터널 구성

Administration(관리) > System(시스템) > Settings(설정) > Protocols(프로토콜) > IPsec > Native IPsec으로 이동합니다. Add(추가)를 클릭합니다. IPsec 터널을 종료하는 Node(노드)를 선택하고 NAD IP Address with Mask(마스크, 기본 게이트웨이 및 IPsec 인터페이스)를 구성합니다
. Authentication Setting as X.509 Certificate(X.509 인증서로 인증 설정)를 선택하고 Certificate System Certificate Installed(설치된 인증서 시스템 인증서)를 선택합니다.



기본 게이트웨이는 선택적 컨피그레이션입니다. 실제로 두 가지 옵션이 있습니다. 기본 OS에 경로를 설치하는 기본 IPsec UI에서 기본 게이트웨이를 구성할 수 있습니다. 이 경로는 show running-config에 표시되지 않습니다.

```
ise332/admin#show running-config | include route
ise332/admin#
```

<#root>

```
ise332/admin#show ip route

Destination Gateway Iface
----------- ------- -----
10.48.23.0/24 0.0.0.0 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
```

10.62.148.79 10.48.23.1 eth1

```
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

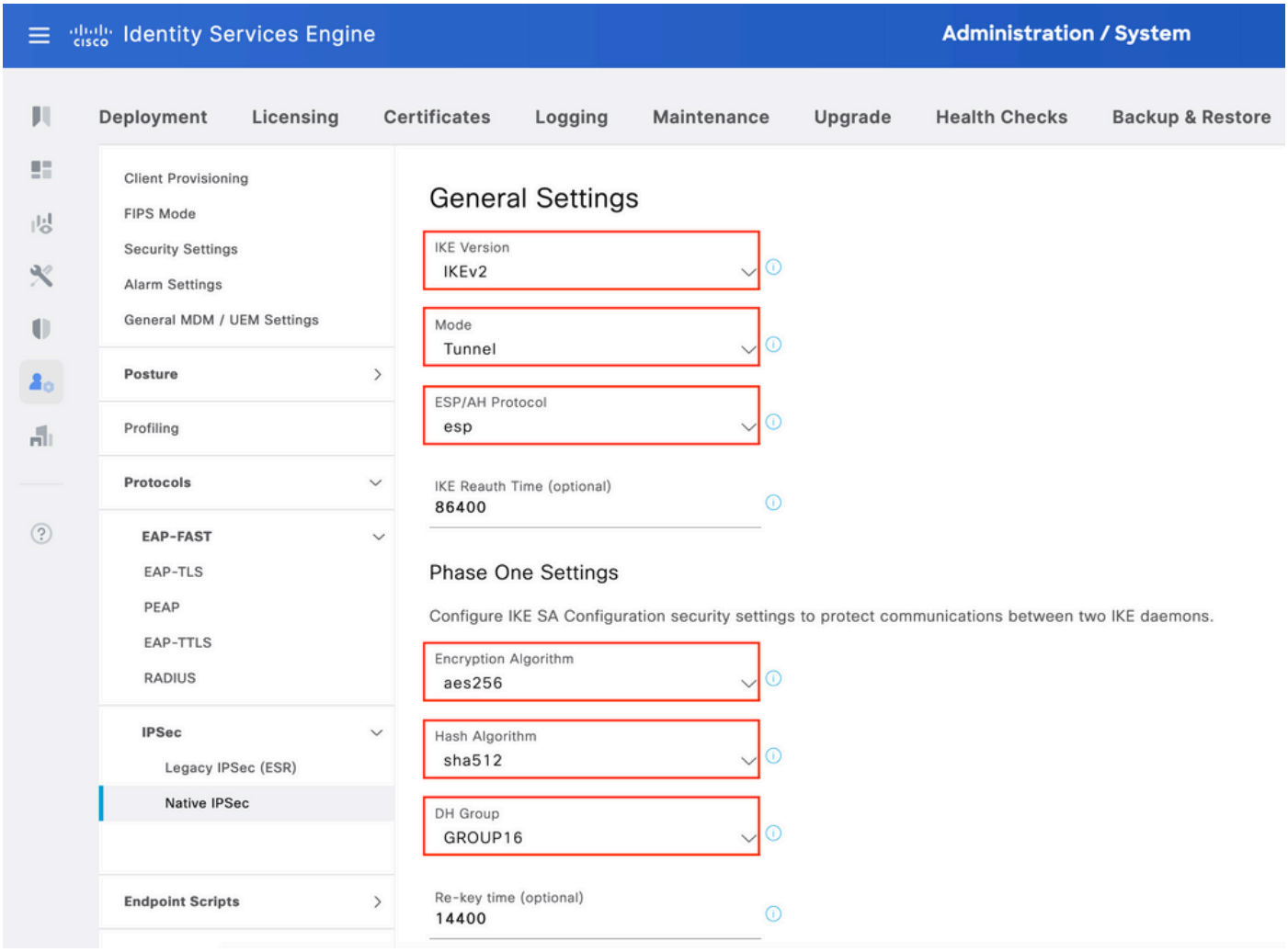
또 다른 옵션은 Default Gateway(기본 게이트웨이)를 비워 두고 ISE에서 경로를 수동으로 구성하는

것이며, 이 경우 동일한 효과가 발생합니다.

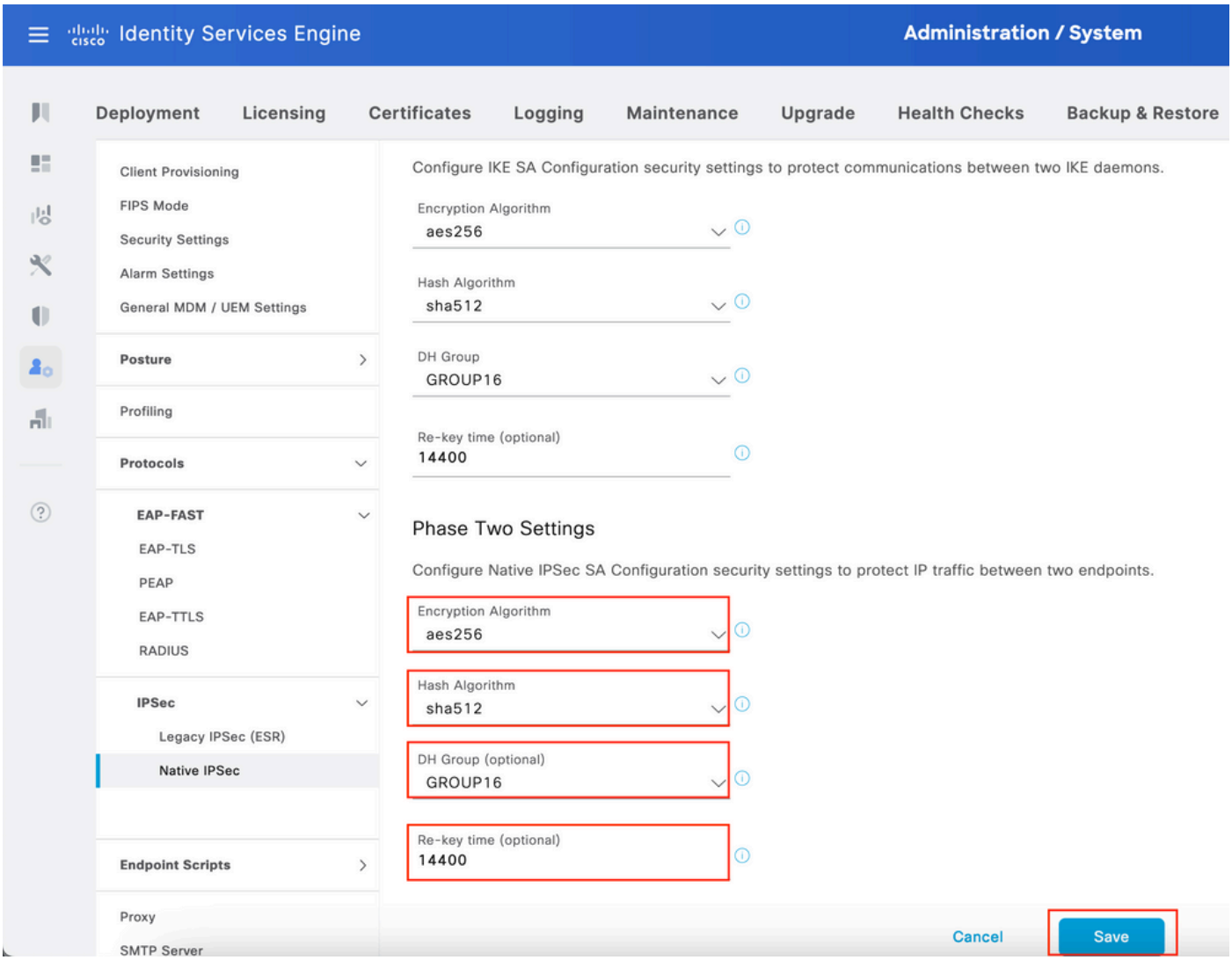
```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route

Destination Gateway Iface
----------- ------- -----
10.48.23.0/24 0.0.0.0 eth1
10.62.148.79 10.48.23.1 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

IPsec 터널에 대한 일반 설정을 구성합니다. 1단계 설정을 구성합니다. 일반 설정, 1단계 설정 및 2단계 설정은 IPsec 터널의 다른 쪽에 구성된 설정과 일치해야 합니다.

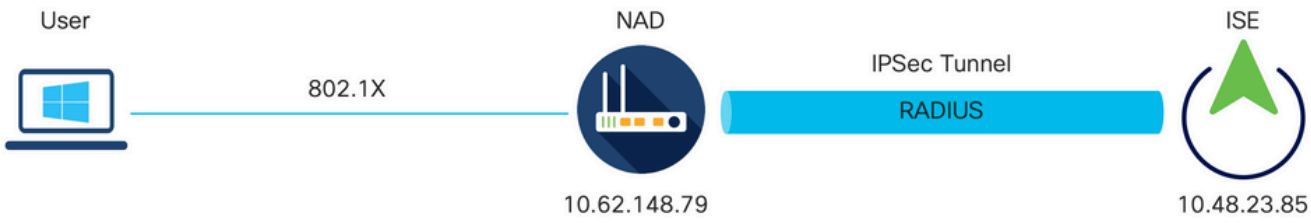


Phase 2 Settings(2단계 설정)를 구성하고 Save(저장)를 클릭합니다.



X.509 사전 공유 키 인증으로 IKEv2 IPsec 터널 구성

네트워크 다이어그램



네트워크 다이어그램

IOS-XE 스위치 CLI 컨피그레이션

인터페이스 구성

IOS-XE 스위치 인터페이스가 아직 구성되지 않은 경우 하나 이상의 인터페이스를 구성해야 합니다

. 예를 들면 다음과 같습니다.

```
interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 negotiation auto
 no shutdown
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
```

Site-to-Site VPN 터널을 설정하기 위해 사용해야 하는 원격 피어에 대한 연결이 있는지 확인합니다. 기본 연결을 확인하려면 ping을 사용할 수 있습니다.

IKEv2 제안 구성

IKEv2 정책을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 proposal <name> 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 16
!
```

암호화 IKEv2 정책 구성

IKEv2 정책을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 policy <name> 명령을 입력합니다.

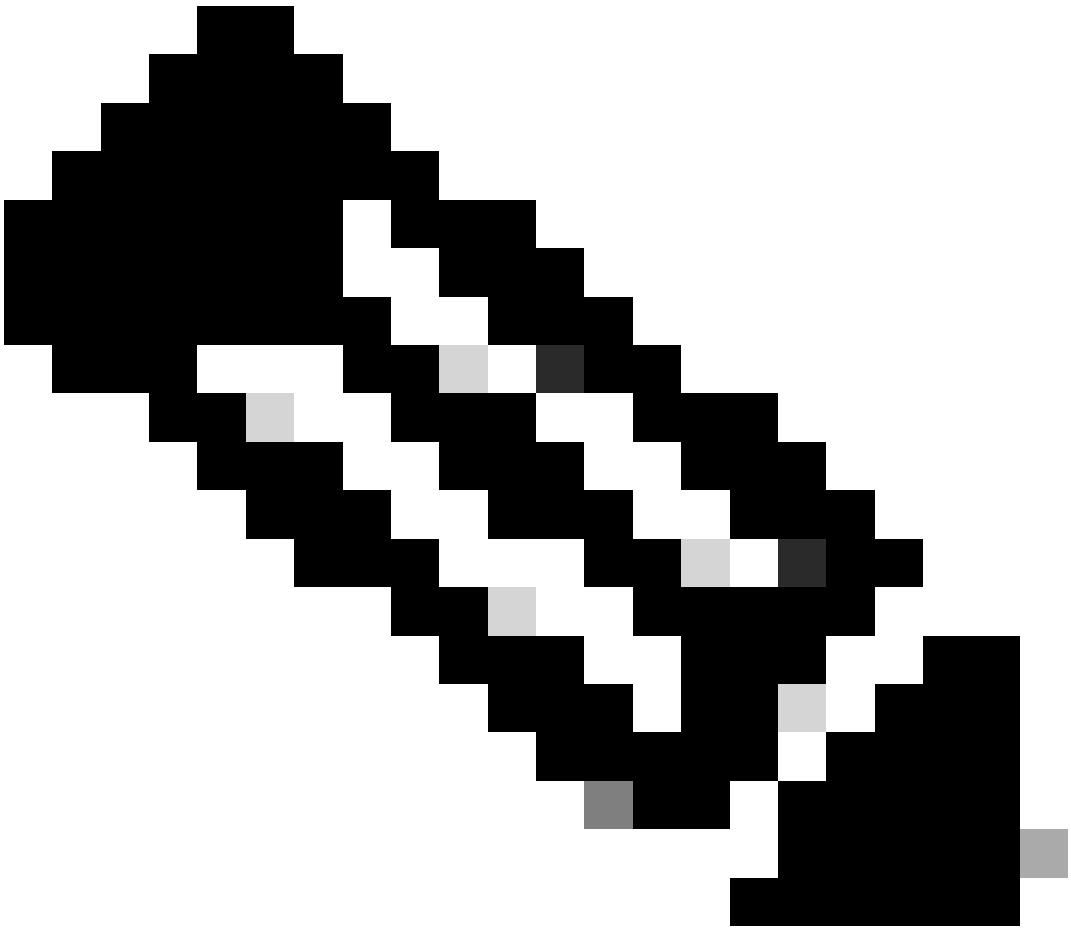
```
crypto ikev2 policy POLICY
 proposal PROPOSAL
```

암호화 IKEv2 프로파일 구성

IKEv2 프로필을 구성하려면 글로벌 컨피그레이션 모드에서 crypto ikev2 profile <name> 명령을 입력합니다.

```
crypto ikev2 profile PROFILE
 match address local 10.62.148.79
```

```
 match identity remote address 10.48.23.85 255.255.255.255
 authentication remote pre-share key cisco123
 authentication local pre-share key cisco123
```



참고: 기본적으로 ISE는 IKEv2 협상에서 자체 ID 인증서의 CN 필드를 IKE ID로 사용합니다. 따라서 IKEv2 프로필의 "match identity remote" 섹션에서 FQDN 유형과 ISE의 도메인 또는 FQDN의 적절한 값을 지정해야 합니다.

관심 VPN 트래픽에 대한 ACL 구성

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

```
ip access-list extended 100
 10 permit ip host 10.62.148.79 host 10.48.23.85
```

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

변형 집합 구성

IPsec 변형 집합(보안 프로토콜과 알고리즘의 적절한 조합)을 정의하려면 글로벌 컨피그레이션 모드에서 crypto ipsec transform-set 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
 mode tunnel
```

암호화 맵 구성 및 인터페이스에 적용

암호화 맵 엔트리를 생성하거나 수정하고 암호화 맵 컨피그레이션 모드로 들어가려면 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 입력합니다.
- 보호된 트래픽과 함께 사용할 수 있는 변형 집합을 정의해야 합니다. 암호화 맵 엔트리와 함께 사용할 수 있는 변환 세트를 지정하려면 set transform-set 명령을 입력합니다.
- 보호해야 하는 트래픽을 정의해야 합니다. 암호화 맵 엔트리에 대한 확장 액세스 목록을 지정하려면 match address 명령을 입력합니다.

예를 들면 다음과 같습니다.

```
crypto map MAP-IKEV2 10 ipsec-isakmp
 set peer 10.48.23.85
 set transform-set SET
 set pfs group16
 set ikev2-profile PROFILE
 match address 100
```

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

```
interface Vlan480
 crypto map MAP-IKEV2
```

IOS-XE 최종 컨피그레이션

다음은 최종 IOS-XE 스위치 CLI 컨피그레이션입니다.

```
aaa new-model
!
aaa group server radius ISE
 server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
 client 10.48.23.85
 server-key cisco
!
dot1x system-auth-control
!
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 16
!
crypto ikev2 policy POLICY
 proposal PROPOSAL
!
crypto ikev2 profile PROFILE
 match address local 10.62.148.79
 match identity remote address 10.48.23.85 255.255.255.255
 authentication remote pre-share key cisco123
 authentication local pre-share key cisco123
!
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
 mode tunnel
!
crypto map MAP-IKEV2 10 ipsec-isakmp
 set peer 10.48.23.85
 set transform-set SET
 set pfs group16
 set ikev2-profile PROFILE
 match address 100
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 crypto map MAP-IKEV2
!
ip access-list extended 100
 10 permit ip host 10.62.148.79 host 10.48.23.85
!
radius server ISE33-2
 address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
 key cisco
!
```

ISE 구성

ISE에서 IP 주소 구성

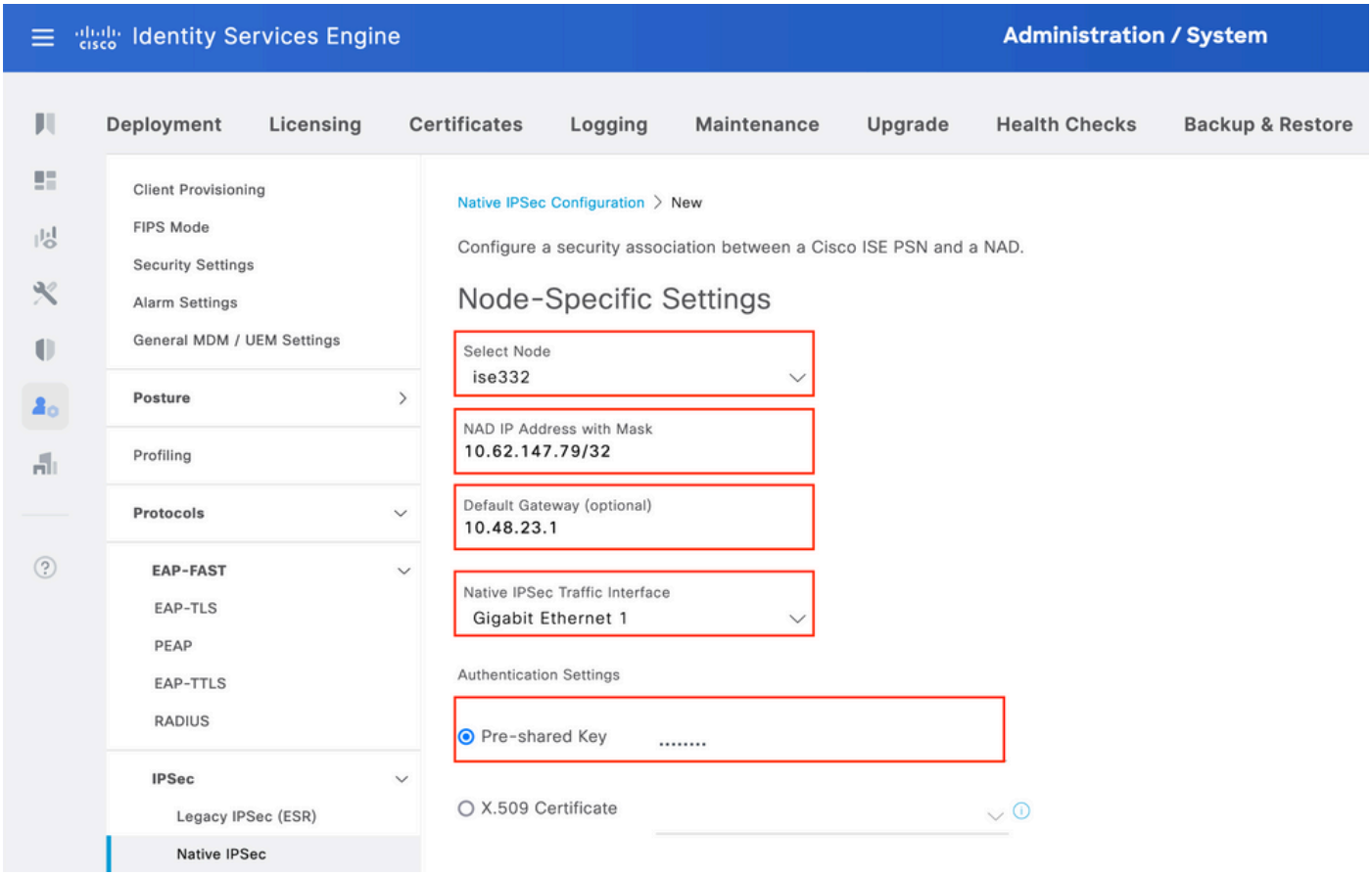
CLI에서 인터페이스 GE1-GE5에 주소를 구성해야 합니다. GE0은 지원되지 않습니다.

```
interface GigabitEthernet 1
  ip address 10.48.23.85 255.255.255.0
  ipv6 address autoconfig
  ipv6 enable
```

참고: 인터페이스에 IP 주소가 구성된 후 애플리케이션이 다시 시작됩니다.
IP 주소를 변경하면 ISE 서비스가 다시 시작될 수 있습니다.
IP 주소 변경을 계속하시겠습니까? Y/N [N]: Y

IPsec 터널 구성

Administration(관리) > System(시스템) > Settings(설정) > Protocols(프로토콜) > IPsec > Native IPsec으로 이동합니다. Add(추가)를 클릭합니다. IPsec 터널을 종료하는 Node(노드)를 선택하고 NAD IP Address with Mask(마스크, 기본 게이트웨이 및 IPsec 인터페이스)를 구성합니다
. Authentication Setting as X.509 Certificate(X.509 인증서로 인증 설정)를 선택하고 Certificate System Certificate Installed(설치된 인증서 시스템 인증서)를 선택합니다.



기본 게이트웨이는 선택적 컨피그레이션입니다. 실제로 두 가지 옵션이 있습니다. 기본 OS에 경로를 설치하는 기본 IPsec UI에서 기본 게이트웨이를 구성할 수 있습니다. 이 경로는 show running-config에 표시되지 않습니다.

```
ise332/admin#show running-config | include route
ise332/admin#
```

<#root>

```
ise332/admin#show ip route

Destination Gateway Iface
----------- ------- -----
10.48.23.0/24 0.0.0.0 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
```

10.62.148.79 10.48.23.1 eth1

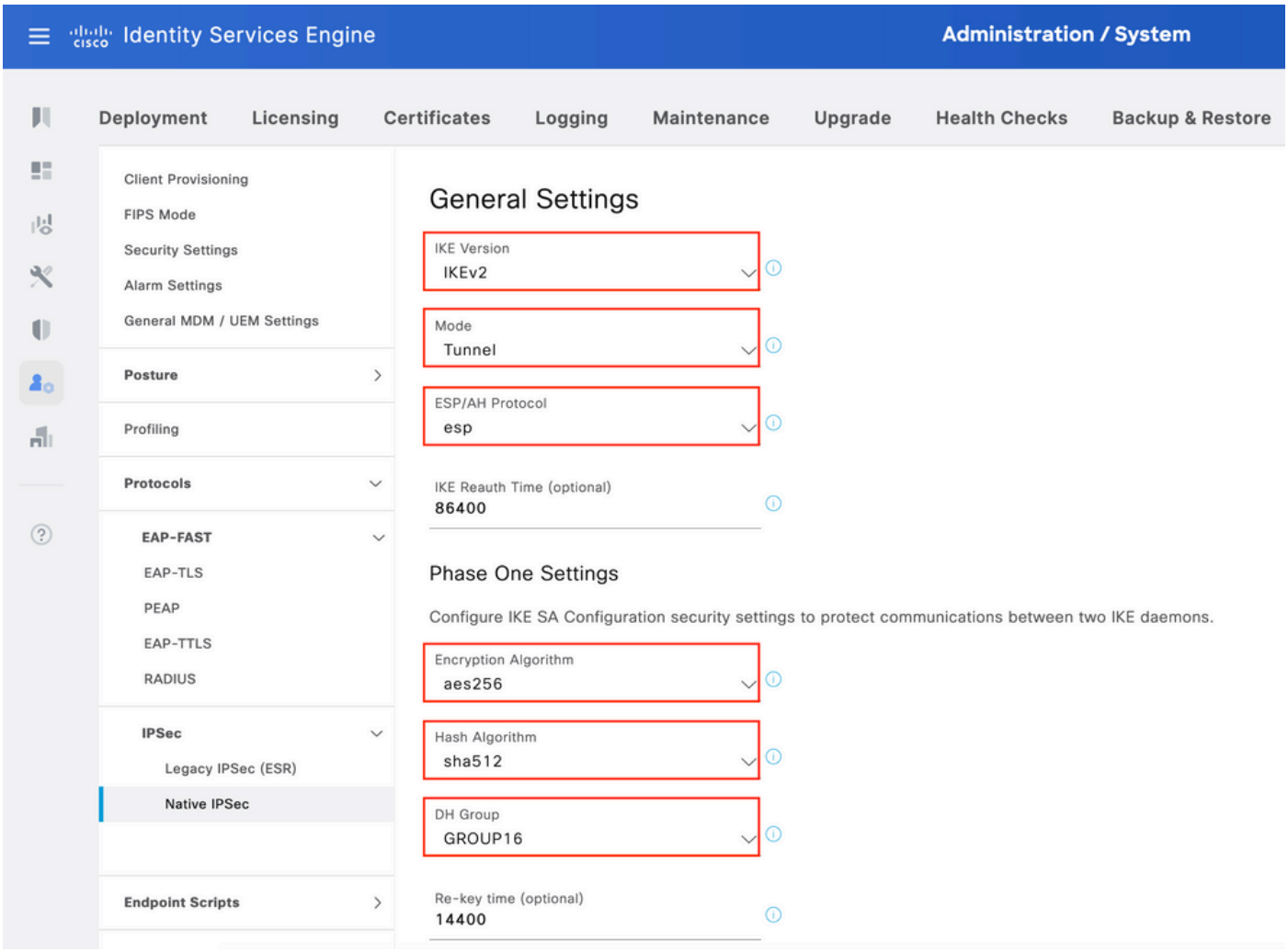
```
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

또 다른 옵션은 Default Gateway(기본 게이트웨이)를 비워 두고 ISE에서 경로를 수동으로 구성하는 것이며, 이 경우 동일한 효과가 발생합니다.

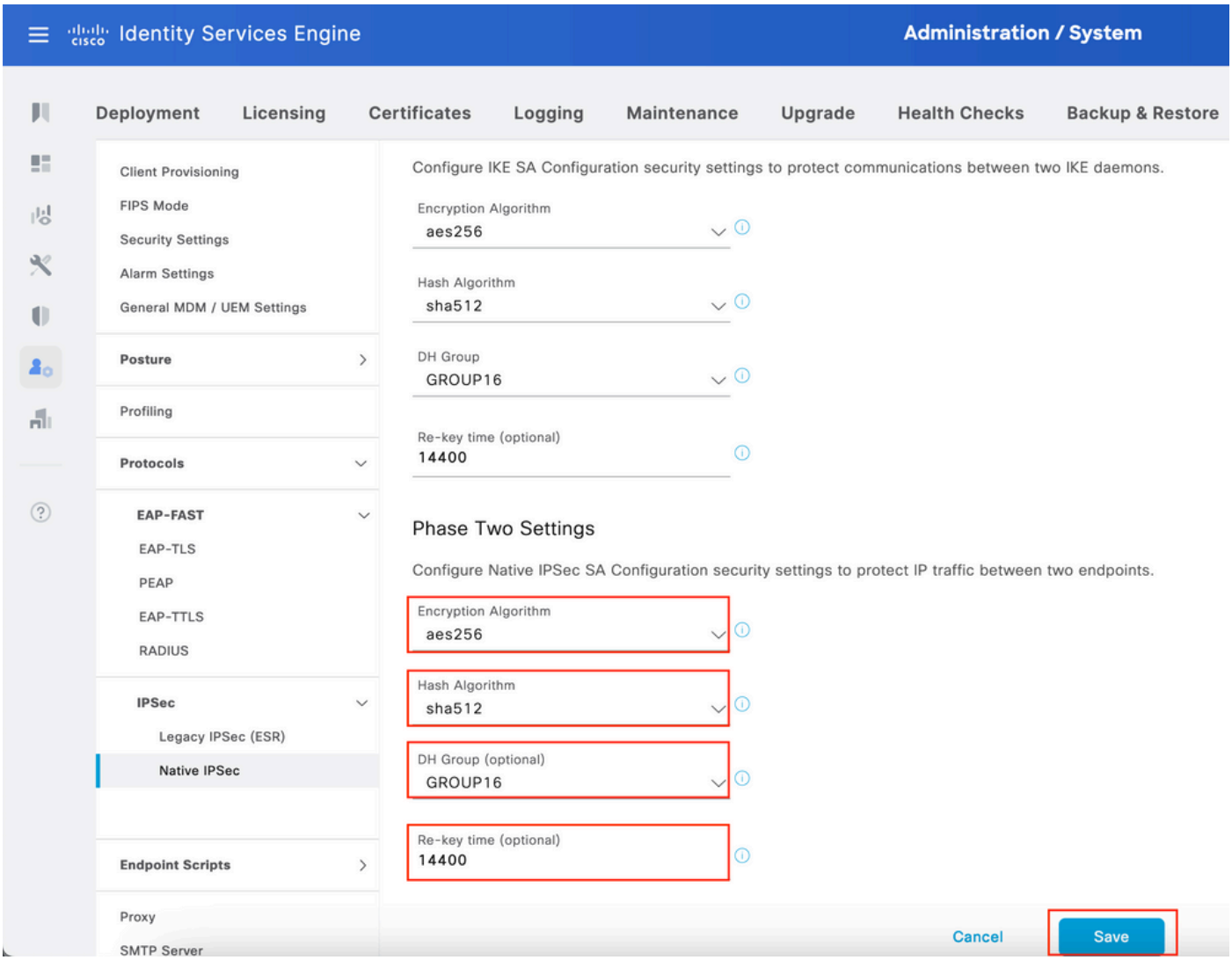
```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route

Destination Gateway Iface
----------- ------- -----
10.48.23.0/24 0.0.0.0 eth1
10.62.148.79 10.48.23.1 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

IPsec 터널에 대한 일반 설정을 구성합니다. 1단계 설정을 구성합니다. 일반 설정, 1단계 설정 및 2단계 설정은 IPsec 터널의 다른 쪽에 구성된 설정과 일치해야 합니다.



Phase 2 Settings(2단계 설정)를 구성하고 Save(저장)를 클릭합니다.



다음을 확인합니다.

RADIUS가 IPsec 터널을 통해 작동하는지 확인하려면 test aaa 명령을 사용하거나 실제 MAB 또는 802.1X 인증을 수행합니다

```
KSEC-9248L-1#test aaa group ISE alice Krakow123 new-code
User successfully authenticated

USER ATTRIBUTES

username 0 "alice"
vn 0 "vn1"
security-group-tag 0 "000f-00"
KSEC-9248L-1#
```

IOS-XE에서 확인

<#root>

```
KSEC-9248L-1#
```

show crypto ikev2 sa

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.62.148.79/500      10.48.23.85/500       none/none
```

READY

```
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:16, Auth sign: RSA, Auth verify: R
      Life/Active Time: 86400/1439 sec

 IPv6 Crypto IKEv2 SA

KSEC-9248L-1#
```

show crypto ipsec sa

```
interface: Vlan480
    Crypto map tag: MAP-IKEV2, local addr 10.62.148.79

   protected vrf: (none)
   local ident (addr/mask/prot/port): (10.62.148.79/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.48.23.85/255.255.255.255/0/0)
   current_peer 10.48.23.85 port 500
     PERMIT, flags={origin_is_acl,}
```

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1

#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1

```
    #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.: 10.62.148.79, remote crypto endpt.: 10.48.23.85
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb Vlan480
     current outbound spi: 0xC17542E9(3245687529)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF7A68F69(4154888041)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 72, flow_id: SW:72, sibling_flags 80000040, crypto map: MAP-IKEV2
         sa timing: remaining key lifetime (k/sec): (4173813/84954)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
      spi: 0xC17542E9(3245687529)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 71, flow_id: SW:71, sibling_flags 80000040, crypto map: MAP-IKEV2
         sa timing: remaining key lifetime (k/sec): (4173813/84954)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:

KSEC-9248L-1#
KSEC-9248L-1#show crypto session
Crypto session current status

Interface: Vlan480
Profile:
```

PROFILE

```
Session status:
```

UP-ACTIVE

```
Peer: 10.48.23.85 port 500
  Session ID: 5
  IKEv2 SA: local 10.62.148.79/500 remote 10.48.23.85/500
```

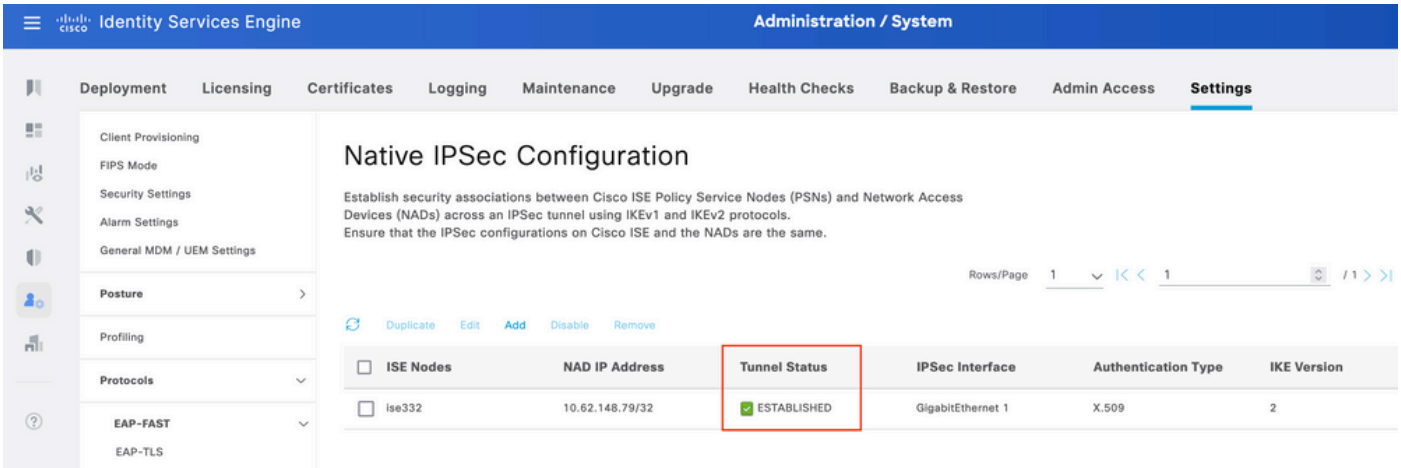
Active

```
  IPSEC FLOW: permit ip host 10.62.148.79 host 10.48.23.85
        Active SAs: 2, origin: crypto map

KSEC-9248L-1#
```

ISE에서 확인

터널의 상태는 GUI에서 확인할 수 있습니다



CLI에서 터널의 상태를 확인하려면 application configure ise 명령을 사용합니다

<#root>

```
ise332/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[0]Exit

34
7212b70a-1405-429a-94b8-71a5d4beb1e5: #114,
```

ESTABLISHED

```
, IKEv2, 0ca3c29e36290185_i 08c7fb6db177da84_r*
  local 'CN=ise332.example.com' @ 10.48.23.85[500]
  remote '10.62.148.79' @ 10.62.148.79[500]
  AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096
  established 984s ago, rekeying in 10283s, reauth in 78609s
  net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5: #58, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-256/HMAC_S
    installed 984s ago, rekeying in 12296s, expires in 14856s
    in c17542e9, 100 bytes,
```

1 packets

```
, 983s ago
    out f7a68f69, 100 bytes,
```

1 packets

```
, 983s ago
```

```
    local 10.48.23.85/32
remote 10.62.148.79/32
```

문제 해결

IOS-XE에서 문제 해결

활성화할 디버그

<#root>

KSEC-9248L-1#

debug crypto ikev2

IKEv2 default debugging is on
KSEC-9248L-1#

debug crypto ikev2 error

IKEv2 error debugging is on
KSEC-9248L-1#

debug crypto ipsec

Crypto IPSEC debugging is on
KSEC-9248L-1#

debug crypto ipsec error

Crypto IPSEC Error debugging is on
KSEC-9248L-1#

IOS-XE의 전체 작업 디버그 세트

```
Apr 25 18:57:36.572: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.62.148.79:500, remote= 10.48.23.85:500,
    local_proxy= 10.62.148.79/255.255.255.255/256/0,
    remote_proxy= 10.48.23.85/255.255.255.255/256/0,
    protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
    lifedur= 86400s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Searching Policy with fvrf 0, local address 10.62
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Found Policy 'POLICY'
Apr 25 18:57:36.573: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Start PKI Session
Apr 25 18:57:36.574: IKEv2:(SA ID = 1):[PKI -> IKEv2] Starting of PKI Session PASSED
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public key,
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Compu
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH key
```

```
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKEv2 initiator - no config data to send in IKE_SA
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_SA_INIT message
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial negotiation)
Num. transforms: 4
   AES-CBC SHA512 SHA512 DH_GROUP_4096_MODP/Group 16

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148
Initiator SPI : 0CA3C29E36290185 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Insert SA

Apr 25 18:57:36.640: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.14
Initiator SPI : 0CA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(Unknown -

Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Verify SA init message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificat
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the trustpoint KrakowCA
Apr 25 18:57:36.643: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the trustpoint PASSED
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):Checking NAT discovery
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):NAT not found
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret key,
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Comput
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH secret
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SK
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED cal
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Completed SA init exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Generate my authentication data
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentic
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication dat
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Get my authentication method
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):My authentication method is 'RSA'
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Sign authentication data
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting private key
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of private key PASSED
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Sign authentication data
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Signing of authentication data PASSED
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Authentication material has been sucessfully sign
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_AUTH message
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Constructing IDi payload: '10.62.148.79' of type
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured trustpoint(s)
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Get Public Key Hashes of trustpoints
Apr 25 18:57:36.946: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of Public Key Hashes of trustpoints PASSE
Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotiation),
Num. transforms: 3
   AES-CBC SHA512 Don't use ESN
Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDi CERT CERTREQ AUTH SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO

Apr 25 18:57:36.947: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148
```

```
Initiator SPI : 0CA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 ENCR

Apr 25 18:57:37.027: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.14
Initiator SPI : 0CA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 IDr CERT AUTH SA TSi TSr

Apr 25 18:57:37.029: IKEv2:(SESSION ID = 5,SA ID = 1):Process auth response notify
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching policy based on peer's identity 'cn=ise
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching Policy with fvrf 0, local address 10.62
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Found Policy 'POLICY'
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's policy
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's policy verified
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Get peer's authentication method
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's authentication method is 'RSA'
Apr 25 18:57:37.033: IKEv2:Validation list created with 1 trustpoints
Apr 25 18:57:37.033: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating certificate chain
Apr 25 18:57:37.043: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain PASSED
Apr 25 18:57:37.043: IKEv2:(SESSION ID = 5,SA ID = 1):Save pubkey
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's authentication data
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentic
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication dat
Apr 25 18:57:37.045: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Verify signed authentication data
Apr 25 18:57:37.047: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of signed authentication d
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_AUTH message
Apr 25 18:57:37.050: IKEv2:(SESSION ID = 5,SA ID = 1):IPSec policy validate request sent for profile PR

Apr 25 18:57:37.051: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.62.148.79:0, remote= 10.48.23.85:0,
    local_proxy= 10.62.148.79/255.255.255.255/256/0,
    remote_proxy= 10.48.23.85/255.255.255.255/256/0,
    protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
Apr 25 18:57:37.051: Crypto mapdb : proxy_match
        src addr : 10.62.148.79
        dst addr : 10.48.23.85
        protocol : 0
        src port : 0
        dst port : 0
Apr 25 18:57:37.051: (ipsec_process_proposal)Map Accepted: MAP-IKEV2, 10
Apr 25 18:57:37.051: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Callback received fo

Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Close PKI Session
Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[PKI -> IKEv2] Closing of PKI Session PASSED
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):IKEV2 SA created; inserting SA into database. SA
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Session with IKE ID PAIR (cn=ise332.example.com,
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 0,SA ID = 0):IKEv2 MIB tunnel started, tunnel index 1
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Load IPSEC key material
Apr 25 18:57:37.054: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into
Apr 25 18:57:37.054: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Apr 25 18:57:37.054: Crypto mapdb : proxy_match
       src addr : 10.62.148.79
       dst addr : 10.48.23.85
       protocol : 256
```

```
       src port : 0
       dst port : 0
Apr 25 18:57:37.054: IPSEC:(SESSION ID = 5) (crypto_ipsec_create_ipsec_sas) Map found MAP-IKEV2, 10
Apr 25 18:57:37.054: IPSEC:(SESSION ID = 5) (crypto_ipsec_sa_find_ident_head) reconnecting with the sam
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (get_old_outbound_sa_for_peer) No outbound SA found for pee
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (create_sa) sa created,
  (sa) sa_dest= 10.62.148.79, sa_proto= 50,
    sa_spi= 0xF7A68F69(4154888041),
    sa_trans= esp-aes 256 esp-sha512-hmac , sa_conn_id= 72
    sa_lifetime(k/sec)= (4608000/86400),
  (identity) local= 10.62.148.79:0, remote= 10.48.23.85:0,
    local_proxy= 10.62.148.79/255.255.255.255/256/0,
    remote_proxy= 10.48.23.85/255.255.255.255/256/0
Apr 25 18:57:37.055: ipsec_out_sa_hash_idx: sa=0x46CFF474, hash_idx=232, port=500/500, addr=0x0A3E944F/
Apr 25 18:57:37.055: crypto_ipsec_hook_out_sa: ipsec_out_sa_hash_array[232]=0x46CFF474
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (create_sa) sa created,
  (sa) sa_dest= 10.48.23.85, sa_proto= 50,
    sa_spi= 0xC17542E9(3245687529),
    sa_trans= esp-aes 256 esp-sha512-hmac , sa_conn_id= 71
    sa_lifetime(k/sec)= (4608000/86400),
  (identity) local= 10.62.148.79:0, remote= 10.48.23.85:0,
    local_proxy= 10.62.148.79/255.255.255.255/256/0,
    remote_proxy= 10.48.23.85/255.255.255.255/256/0
Apr 25 18:57:37.056: IPSEC: Expand action denied, notify RP
Apr 25 18:57:37.056: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA
Apr 25 18:57:37.056: IKEv2:(SESSION ID = 5,SA ID = 1):Checking for duplicate IKEv2 SA
Apr 25 18:57:37.057: IKEv2:(SESSION ID = 5,SA ID = 1):No duplicate IKEv2 SA found
```

ISE에서 트러블슈팅

활성화할 디버그

ISE에서 활성화할 특정 디버그가 없습니다. 디버그를 콘솔에 인쇄하려면 다음 명령을 실행합니다.

```
ise332/admin#show logging application strongswan/charon.log tail
```

ISE에서 작동하는 전체 디버그 세트

```
Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 13[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 0000000000000000_r
Apr 26 00:57:36 13[MGR] created IKE_SA (unnamed)[114]
Apr 26 00:57:36 13[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (774 bytes)
Apr 26 00:57:36 13[ENC] <114> parsed IKE_SA_INIT request 0 [ SA KE No V V V V N(NATD_S_IP) N(NATD_D_IP)
Apr 26 00:57:36 13[CFG] <114> looking for an IKEv2 config for 10.48.23.85...10.62.148.79
Apr 26 00:57:36 13[CFG] <114> candidate: 10.48.23.85...10.62.148.79, prio 3100
Apr 26 00:57:36 13[CFG] <114> found matching ike config: 10.48.23.85...10.62.148.79 with prio 3100
Apr 26 00:57:36 13[IKE] <114> local endpoint changed from 0.0.0.0[500] to 10.48.23.85[500]
Apr 26 00:57:36 13[IKE] <114> remote endpoint changed from 0.0.0.0 to 10.62.148.79[500]
Apr 26 00:57:36 13[IKE] <114> received Cisco Delete Reason vendor ID
Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:2d:30:32
```

```
Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:43:2d:52:
Apr 26 00:57:36 13[IKE] <114> received Cisco FlexVPN Supported vendor ID
Apr 26 00:57:36 13[IKE] <114> 10.62.148.79 is initiating an IKE_SA
Apr 26 00:57:36 13[IKE] <114> IKE_SA (unnamed)[114] state change: CREATED => CONNECTING
Apr 26 00:57:36 13[CFG] <114> selecting proposal:
Apr 26 00:57:36 13[CFG] <114> proposal matches
Apr 26 00:57:36 13[CFG] <114> received proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/M
Apr 26 00:57:36 13[CFG] <114> configured proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512
Apr 26 00:57:36 13[CFG] <114> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MO
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=KrakowCA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "DC=com, DC=example, CN=LAB CA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Endpoint Sub CA - ise33
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Node CA - ise332"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "O=Cisco, CN=Cisco Manufacturing CA SHA2"
Apr 26 00:57:36 13[ENC] <114> generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CE
Apr 26 00:57:36 13[NET] <114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500] (809 bytes)
Apr 26 00:57:36 13[MGR] <114> checkin IKEv2 SA (unnamed)[114] with SPIs 0ca3c29e36290185_i 08c7fb6db177
Apr 26 00:57:36 13[MGR] <114> checkin of IKE_SA successful
Apr 26 00:57:36 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 09[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 08c7fb6db177da84_r
Apr 26 00:57:36 09[MGR] IKE_SA (unnamed)[114] successfully checked out
Apr 26 00:57:36 09[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (1488 bytes)
Apr 26 00:57:37 09[ENC] <114> parsed IKE_AUTH request 1 [ V IDi CERT CERTREQ AUTH SA TSi TSr N(INIT_CON
Apr 26 00:57:37 09[IKE] <114> received cert request for "CN=KrakowCA"
Apr 26 00:57:37 09[IKE] <114> received end entity cert "CN=KSEC-9248L-1.example.com"
Apr 26 00:57:37 09[CFG] <114> looking for peer configs matching 10.48.23.85[%any]...10.62.148.79[10.62.
Apr 26 00:57:37 09[CFG] <114> candidate "7212b70a-1405-429a-94b8-71a5d4beb1e5", match: 1/1/3100 (me/oth
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected peer config '7212b70a-1405-
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using certificate "CN=KSEC-9248L-1.e
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KSEC-9248L-1.example
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using trusted ca certificate "CN=Kra
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KrakowCA" key: 2048
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> reached self-signed root ca with a p
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checking certificate status of "CN=K
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> ocsp check skipped, no ocsp found
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate status is not available
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of '10.62.148.79' wit
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received ESP_TFC_PADDING_NOT_SUPPORT
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of 'CN=ise332.example
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending end entity cert "CN=ise332.e
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling rekeying in 11267s
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling reauthentication in 79593
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> maximum IKE_SA lifetime 19807s
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> looking for a child config for 10.48
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for us:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.48.23.85/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for othe
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.62.148.79/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> candidate "net-net-7212b70a-1405-429
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> found matching child config "net-net
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting proposal:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposal matches
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received proposals: ESP:AES_CBC_256/
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> configured proposals: ESP:AES_CBC_25
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected proposal: ESP:AES_CBC_256/H
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> got SPI c17542e9
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for us:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10
```

```
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for othe
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using AES_CBC for encryption
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using HMAC_SHA2_512_256 for integrity
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding inbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xc17542e9, src 10.62.148.79 dst
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI c17542e9 a
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC w
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 32 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding outbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xf7a68f69, src 10.48.23.85 dst
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI f7a68f69 a
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC w
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 0 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.48.23.85/32 === 10.
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting a local address in traffic s
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using host 10.48.23.85
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface name for index 22
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using 10.48.23.1 as nexthop and eth1
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> installing route: 10.62.148.79/32 vi
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface index for eth1
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-
Apr 26 00:57:37 09[ENC] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> generating IKE_AUTH response 1 [ IDr
Apr 26 00:57:37 09[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin IKEv2 SA 7212b70a-1405-429a-
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin of IKE_SA successful
Apr 26 00:57:37 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
```

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.