

Cisco WLC와 ISE 간의 IPsec 터널 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[ISE 구성](#)

[9800 WLC 컨피그레이션](#)

[다음을 확인합니다.](#)

[WLC](#)

[ISE](#)

[패킷 캡처](#)

[문제 해결](#)

[WLC 디버깅](#)

[ISE 디버깅](#)

[참조](#)

소개

이 문서에서는 Radius 및 TACACS 통신을 보호하기 위해 9800 WLC와 ISE 서버 간의 IPsec(Internet Protocol Security) 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE
- Cisco IOS® XE WLC 컨피그레이션
- 일반 IPsec 개념
- 일반 RADIUS 개념
- 일반 TACACS 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 무선 컨트롤러: 17.09.04a를 실행하는 C9800-40-K9
- Cisco ISE: 버전 3 패치 4 실행
- 스위치: 9200-L-24P

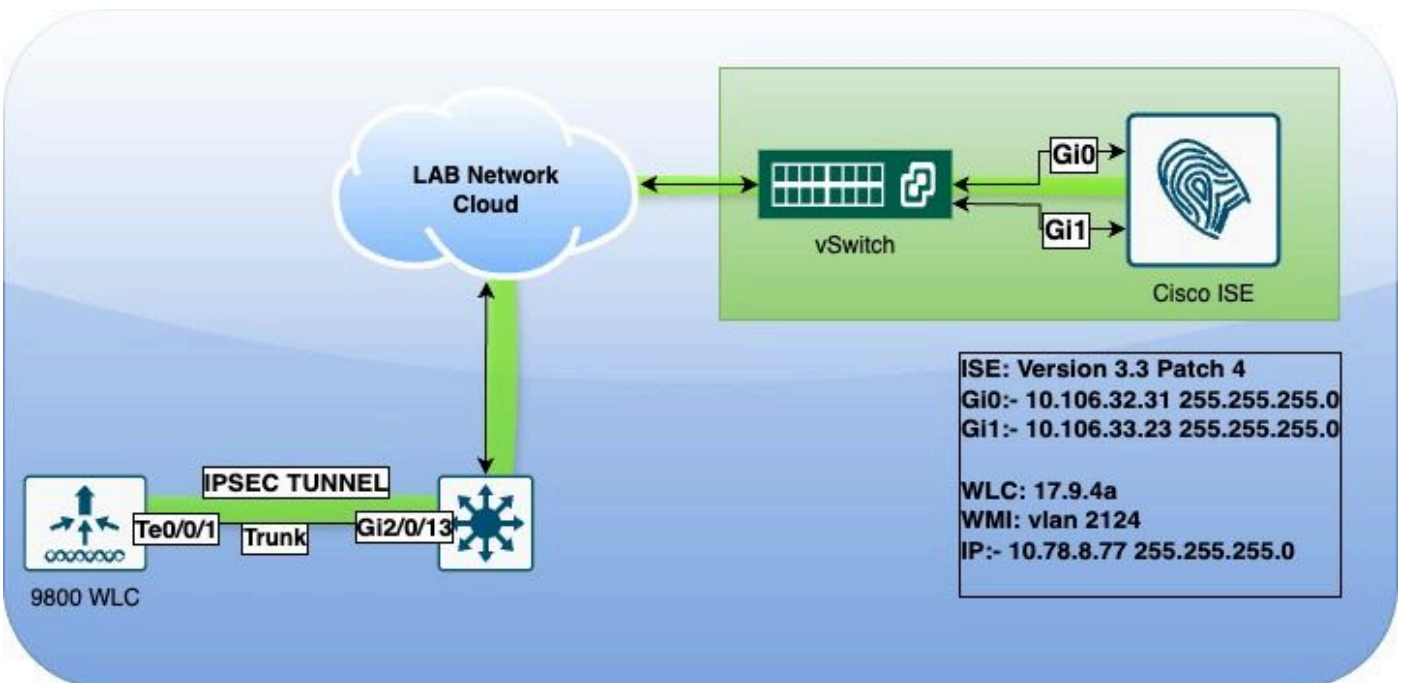
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

IPsec은 IETF에서 개발한 개방형 표준의 프레임워크입니다. 인터넷과 같은 보호되지 않는 네트워크를 통해 민감한 정보를 전송할 때 보안을 제공합니다. IPsec은 네트워크 레이어에서 작동하여 Cisco 라우터와 같은 참여 IPsec 장치(피어) 간 IP 패킷을 보호하고 인증합니다. 9800 WLC와 ISE 서버 간 IPsec을 사용하여 RADIUS 및 TACACS 통신을 보호합니다.

구성

네트워크 다이어그램



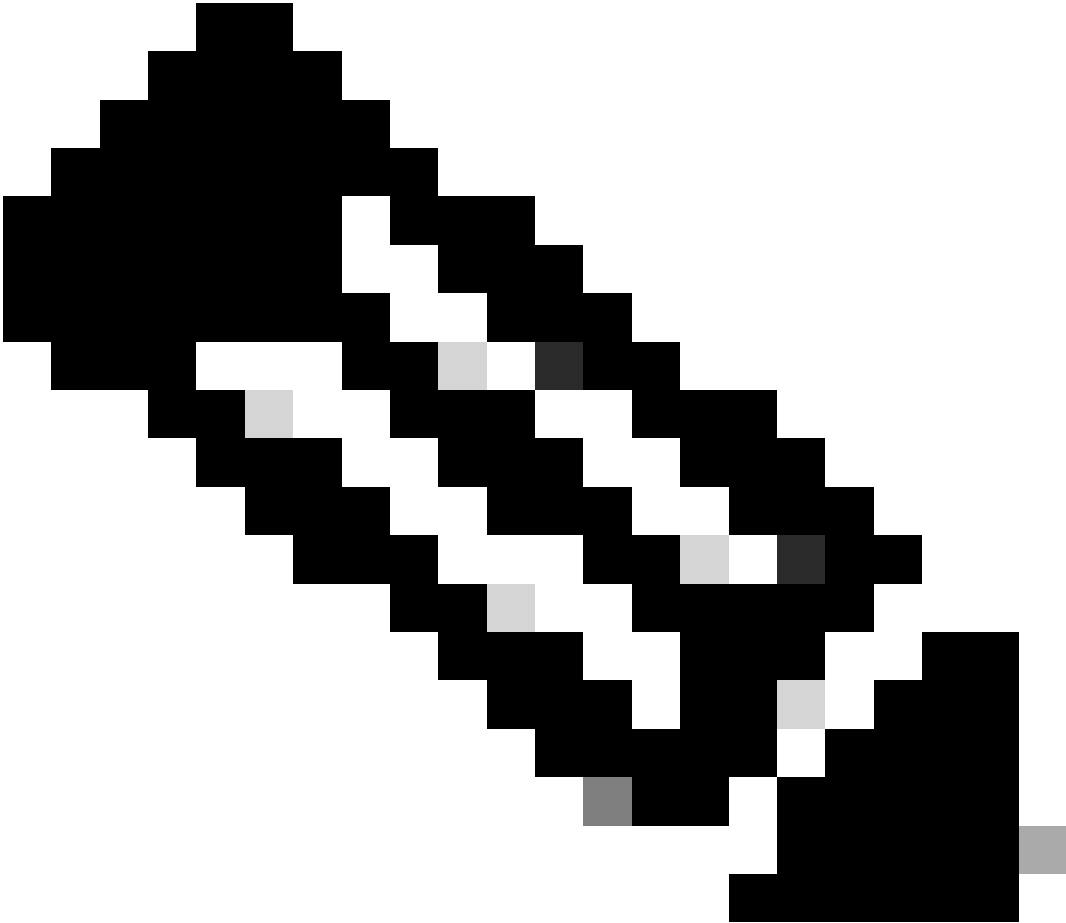
네트워크 다이어그램

ISE 구성

Cisco ISE는 터널 및 전송 모드에서 IPsec을 지원합니다. Cisco ISE 인터페이스에서 IPsec을 활성화하고 피어를 구성하면 Cisco ISE와 NAD 간에 IPsec 터널이 생성되어 통신을 보호합니다.

사전 공유 키를 정의하거나 IPsec 인증에 X.509 인증서를 사용할 수 있습니다. IPsec은 기가비트 이더넷 1~기가비트 이더넷 5 인터페이스에서 활성화할 수 있습니다.

Cisco ISE 릴리스 2.2 이상은 IPsec을 지원합니다.



참고: Cisco ISE Essentials 라이선스가 있는지 확인합니다.

Network Devices(네트워크 디바이스) 창에서 특정 IP 주소로 NAD(Network Access Device)를 추가합니다.

Cisco ISE GUI에서 Administration(관리) 위에 마우스를 놓고 System(시스템) > Settings(설정) > Protocols(프로토콜) > IPsec > Native IPsec으로 이동합니다.

Cisco ISE PSN과 NAD 간의 보안 연결을 구성하려면 Add(추가)를 클릭합니다.

- 노드를 선택합니다.
- NAD IP 주소를 지정합니다.
- 필요한 IPsec 트래픽 인터페이스를 선택합니다.
- NAD에서도 사용할 사전 공유 키를 입력합니다.

General(일반) 섹션에서 지정된 세부 정보를 입력합니다.

- IKEv2를 선택합니다.

- 터널 모드를 선택합니다.
- ESP/AH 프로토콜로 ESP를 선택합니다.

Native IPsec Configuration > ise3genvc

Configure a security association between a Cisco ISE PSN and a NAD.

Node-Specific Settings

Select Node
ise3genvc

NAD IP Address
10.78.8.77

Native IPsec Traffic Interface
Gigabit Ethernet 1

Configure VTI ⓘ

Authentication Settings

Pre-shared Key

X.509 Certificate ⓘ

General Settings

IKE Version
IKEv2

Mode
Tunnel

ESP/AH Protocol
ESP

IKE Reauth Time
86400 ⓘ

ISE 네이티브 IPsec 컨피그레이션

1단계 설정:

- 암호화 알고리즘으로 AES256을 선택합니다.
- SHA512를 알고리즘으로 선택합니다.

- GROUP14를 DH 그룹으로 선택합니다.

2단계 설정에서

- 암호화 알고리즘으로 AES256을 선택합니다.
- SHA512를 알고리즘으로 선택합니다.

The image shows a configuration interface for IPsec. It is divided into two main sections: 'Phase One Settings' and 'Phase Two Settings'. Both sections are highlighted with a red border. In the 'Phase One Settings' section, the 'Encryption Algorithm' is set to 'AES256', the 'Hash Algorithm' is 'SHA512', and the 'DH Group' is 'GROUP14'. Below these are 'Re-key time' and '14400'. The 'Phase Two Settings' section has 'Encryption Algorithm' set to 'AES256', 'Hash Algorithm' set to 'SHA512', and 'DH Group (optional)' set to 'None'. It also has 'Re-key time' and '14400'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Phase One Settings

Configure IKE SA Configuration security settings to protect communications between two IKE daemons.

Encryption Algorithm
AES256

Hash Algorithm
SHA512

DH Group
GROUP14

Re-key time
14400

Phase Two Settings

Configure Native IPsec SA Configuration security settings to protect IP traffic between two endpoints.

Encryption Algorithm
AES256

Hash Algorithm
SHA512

DH Group (optional)
None

Re-key time
14400

Cancel Save

IPSec 1단계 및 2단계 구성

eth1 게이트웨이를 다음 홉으로 사용하여 ISE CLI에서 WLC로의 경로를 구성합니다.

<#root>

```
ise3genvc/admin#configure t  
Entering configuration mode terminal
```

```
ise3genvc/admin(config)#ip route 10.78.8.77 255.255.255.255 gateway 10.106.33.1
```

```
ise3genvc/admin(config)#end  
ise3genvc/admin#show ip route | include 10.78.8.77  
10.78.8.77 10.106.33.1 eth1
```

9800 WLC 컨피그레이션

9800 WLC의 IPSec 컨피그레이션은 GUI에 표시되지 않으므로 모든 컨피그레이션은 CLI에서 수행해야 합니다.

다음은 ISE 서버의 컨피그레이션 단계입니다. 각 단계에는 이 섹션의 관련 CLI 명령이 함께 제공되어 지침을 제공합니다.



WLC IPsec 컨피그레이션 단계

IKEv2 제안 컨피그레이션

컨피그레이션을 시작하려면 글로벌 컨피그레이션 모드로 들어가서 IKEv2 제안서를 생성합니다. 식별 목적으로 제안에 고유한 이름을 지정합니다.

```
crypto ikev2 proposal ipsec-prop
encryption aes-cbc-256
integrity sha512
group 14
exit
```

다음으로, 정책을 구성하고 이전에 생성한 제안을 이 정책 내에 매핑합니다.

```
crypto ikev2 policy ipsec-policy
proposal ipsec-prop
exit
```

IKE 인증에 사용할 암호화 키링을 정의합니다. 이 키링에는 필요한 인증 자격 증명이 저장됩니다.

```
crypto ikev2 keyring mykey
peer ise
address 10.106.33.23 255.255.255.255
pre-shared-key Cisco!123
exit
```

IKE SA의 협상 불가능한 매개변수에 대한 리포지토리 역할을 하는 IKEv2 프로파일을 구성합니다. 여기에는 로컬 또는 원격 ID, 인증 방법, 인증된 피어에 대해 사용 가능한 서비스가 포함됩니다.

```
crypto ikev2 profile ipsec-profile
match identity remote address 10.106.33.23 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local mykey
exit
```

변형 집합을 생성하고 터널 모드에서 작동하도록 구성합니다.

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

ISE 인터페이스 IP에 대한 통신만 허용하도록 ACL을 생성합니다.


```
ip access-list extended ISE_ALLOW
10 permit ip host 10.78.8.77 host 10.106.33.23
```

전역 컨피그레이션에서 암호화 맵을 구성합니다. 변형 집합, IPsec 프로파일 및 ACL을 암호화 맵에 첨부합니다.

```
crypto map ikev2-cryptomap 1 ipsec-isakmp
set peer 10.106.33.23
set transform-set TSET
set ikev2-profile ipsec-profile
match address ISE_ALLOW
```

마지막으로, 암호화 맵을 인터페이스에 연결합니다. 이 시나리오에서 RADIUS 트래픽을 전달하는 무선 관리 인터페이스는 관리 인터페이스 VLAN 내에서 매핑됩니다.

```
int vlan 2124
crypto map ikev2-cryptomap
```

다음을 확인합니다.

WLC

9800 WLC에서 IPsec을 확인하는 데 사용할 수 있는 show 명령입니다.

- ip 액세스 목록 표시
- 암호화 맵 표시
- show crypto ikev2 sa detailed
- crypto ipsec sa 세부 정보 표시

<#root>

```
POD6_9800#show ip access-lists ISE_ALLOW
Extended IP access list ISE_ALLOW
10 permit ip host 10.78.8.77 host 10.106.33.23 (6 matches)
```

```
POD6_9800#show crypto map
Interfaces using crypto map MAP-IKEV2:
```

```
Crypto Map IPv4 "ikev2-cryptomap" 1 ipsec-isakmp
```

```
Peer = 10.106.33.23
```

```
IKEv2 Profile:
```

```
ipsec-profile
```

Access-List SS dynamic: False
Extended IP access list ISE_ALLOW

access-list ISE_ALLOW

permit ip host 10.78.8.77 host 10.106.33.23
Current peer: 10.106.33.23
Security association lifetime: 4608000 kilobytes/3600 seconds
Dualstack (Y/N): N

Responder-Only (Y/N): N
PFS (Y/N): N
Mixed-mode : Disabled

Transform sets={

TSET: { esp-256-aes esp-sha512-hmac } ,

}

Interfaces using crypto map ikev2-cryptomap:

Vlan2124

POD6_9800#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1

10.78.8.77/500 10.106.33.23/500

none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/617 sec
CE id: 1699, Session-id: 72
Local spi: BA3FFBFCF57E6A1 Remote spi: BEE60CB887998D58
Status Description: Negotiation done

Local id: 10.78.8.77

Remote id: 10.106.33.23

Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 1
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Dynamic Route Update: disabled
Extended Authentication not configured.

NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
PEER TYPE: Other

IPv6 Crypto IKEv2 SA

POD6_9800#show crypto ipsec sa detail

interface: Vlan2124

Crypto map tag: ikev2-cryptomap, local addr 10.78.8.77

protected vrf: (none)

local ident (addr/mask/prot/port): (10.78.8.77/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (10.106.33.23/255.255.255.255/0/0)

current_peer 10.106.33.23 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 285, #pkts encrypt: 285, #pkts digest: 285

#pkts decaps: 211, #pkts decrypt: 211, #pkts verify: 211

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#pkts no sa (send) 0, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (recv) 0, #pkts verify failed: 0

#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts tagged (send): 0, #pkts untagged (rcv): 0

#pkts not tagged (send): 0, #pkts not untagged (rcv): 0

#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 10.78.8.77, remote crypto endpt.: 10.106.33.23

plaintext mtu 1022, path mtu 1100, ip mtu 1100, ip mtu idb Vlan2124

current outbound spi: 0xCCC04668(3435153000)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xFEACCF3E(4272738110)

transform: esp-256-aes esp-sha512-hmac ,

in use settings ={Tunnel, }

conn id: 2379, flow_id: HW:379, sibling_flags FFFFFFFF80000048, crypto map: ikev2-cryptomap, initiator

sa timing: remaining key lifetime (k/sec): (4607994/2974)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xCCC04668(3435153000)
transform: esp-256-aes esp-sha512-hmac ,
in use settings ={Tunnel, }
conn id: 2380, flow_id: HW:380, sibling_flags FFFFFFFF80000048, crypto map: ikev2-cryptomap, initiator
sa timing: remaining key lifetime (k/sec): (4607994/2974)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

ISE

<#root>

ise3genvc/admin#application configure ise

It will present multiple options. Select option 34.

[34]View Native IPsec status

```
45765332-52dd-4311-93ed-44fd64c55585: #1, ESTABLISHED, IKEv2, bee60cb887998d58_i* ba3ffbbfbcf57e6a1_r
local '10.106.33.23' @ 10.106.33.23[500]
remote '10.78.8.77' @ 10.78.8.77[500]
AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048
established 1133s ago, rekeying in 6781s, reauth in 78609s
net-net-45765332-52dd-4311-93ed-44fd64c55585: #2, reqid 1, INSTALLED,
```

TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
installed 1133s ago, rekeying in 12799s, expires in 14707s
in ccc04668, 5760 bytes, 96 packets, 835s ago
out feaccf3e, 5760 bytes, 96 packets, 835s ago
```

local 10.106.33.23/32

remote 10.78.8.77/32

Enter 0 to exit from this context.

ISE Nodes	NAD IP Address	Tunnel Status	IPsec Interface	Authentication Type	VTI Enabled	IKE Version
<input checked="" type="checkbox"/> ise3gwerc	10.78.8.77	ESTABLISHED	GigabitEthernet 1	Pre-shared Key	false	2

IPSec 상태를 보여주는 ISE GUI

패킷 캡처

WLC에서 EPC를 수행하여 클라이언트 RADIUS 트래픽이 ESP 터널을 통과하는지 확인합니다. 컨트롤 플레인 캡처를 사용하면 암호화되지 않은 상태로 컨트롤 플레인을 떠나는 패킷을 관찰할 수 있습니다. 그런 다음 패킷이 암호화되어 유선 네트워크로 전송됩니다.

No.	Time	Source	Destination	Protocol	Length	Info
136	13:...	10.78.8.77	10.106.33.23	RADIUS	432	Access-Request id=119
137	13:...	10.78.8.77	10.106.33.23	ESP	526	ESP (SPI=0xc3a824d7)
138	13:...	10.106.33.23	10.78.8.77	ESP	254	ESP (SPI=0xc19b26e9)
139	13:...	10.106.33.23	10.78.8.77	RADIUS	165	Access-Challenge id=119
144	13:...	10.78.8.77	10.106.33.23	RADIUS	705	Access-Request id=120
145	13:...	10.78.8.77	10.106.33.23	ESP	798	ESP (SPI=0xc3a824d7)
194	13:...	10.106.33.23	10.78.8.77	ESP	1262	ESP (SPI=0xc19b26e9)
195	13:...	10.106.33.23	10.78.8.77	RADIUS	1177	Access-Challenge id=120
214	13:...	10.78.8.77	10.106.33.23	RADIUS	507	Access-Request id=121
215	13:...	10.78.8.77	10.106.33.23	ESP	590	ESP (SPI=0xc3a824d7)
216	13:...	10.106.33.23	10.78.8.77	ESP	1262	ESP (SPI=0xc19b26e9)
217	13:...	10.106.33.23	10.78.8.77	RADIUS	1173	Access-Challenge id=121
240	13:...	10.78.8.77	10.106.33.23	RADIUS	507	Access-Request id=122
241	13:...	10.78.8.77	10.106.33.23	ESP	590	ESP (SPI=0xc3a824d7)
242	13:...	10.106.33.23	10.78.8.77	ESP	414	ESP (SPI=0xc19b26e9)

WLC와 ISE 간의 IPSec 패킷

문제 해결

WLC 디버깅

9800 WLC는 Cisco IOS XE에서 작동하므로 다른 Cisco IOS XE 플랫폼에서와 유사한 IPSec 디버그 명령을 사용할 수 있습니다. 다음은 IPSec 문제를 해결하는 데 유용한 두 가지 핵심 명령입니다.

- crypto ikev2 디버그
- 디버그 crypto ikev2 오류

ISE 디버깅

IPSec 로그를 보려면 ISE CLI에서 이 명령을 사용합니다. 디버깅 명령은 WLC에서 필요하지 않습니다.

- show logging application strongswan/charon.log tail

참조

[Cisco Catalyst 9800 Series Wireless Controller 소프트웨어 컨피그레이션 가이드, Cisco IOS XE Cupertino 17.9.x](#)

[Cisco ISE와 NAD 간의 통신을 보호하는 IPsec 보안](#)

[IKEv2\(Internet Key Exchange 버전 2\) 구성](#)

[ISE 3.3 Native IPsec to Secure NAD\(Cisco IOS XE\) 통신 구성](#)

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.