Configure IPsec Tunnel Between Cisco WLC and ISE

Contents

Introduction

This document describes the Internet Protocol Security (IPsec) configuration between 9800 WLC and ISE server to secure Radius & TACACS communication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE
- Cisco IOS® XE WLC Configuration
- General IPsec concepts
- General RADIUS concepts
- General TACACS concepts

Components Used

The information in this document is based on these software and hardware versions:

- Wireless controller: C9800-40-K9 running 17.09.04a

- Cisco ISE: Running Version 3 Patch 4
- Switch: 9200-L-24P

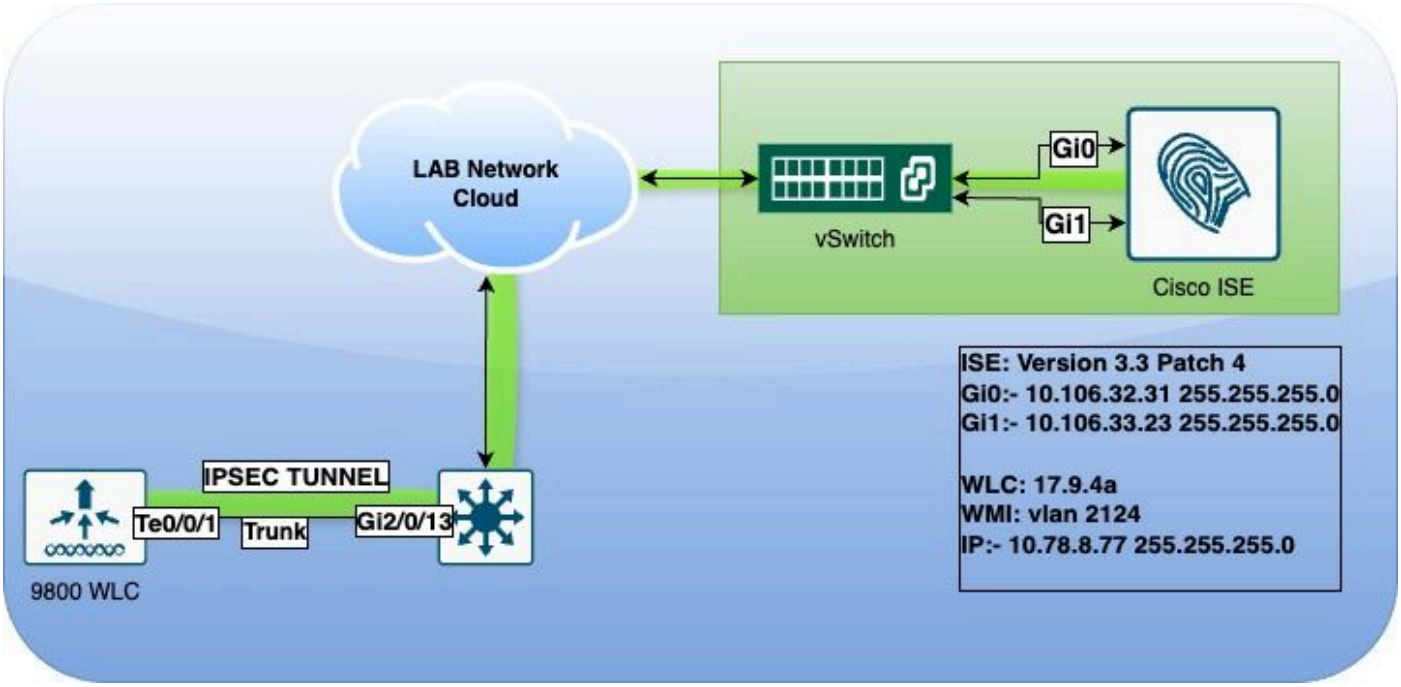
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

IPsec is a framework of open standards developed by the IETF. It provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers. Use IPsec between the 9800 WLC and the ISE server to secure RADIUS and TACACS communication.

Configure

Network Diagram



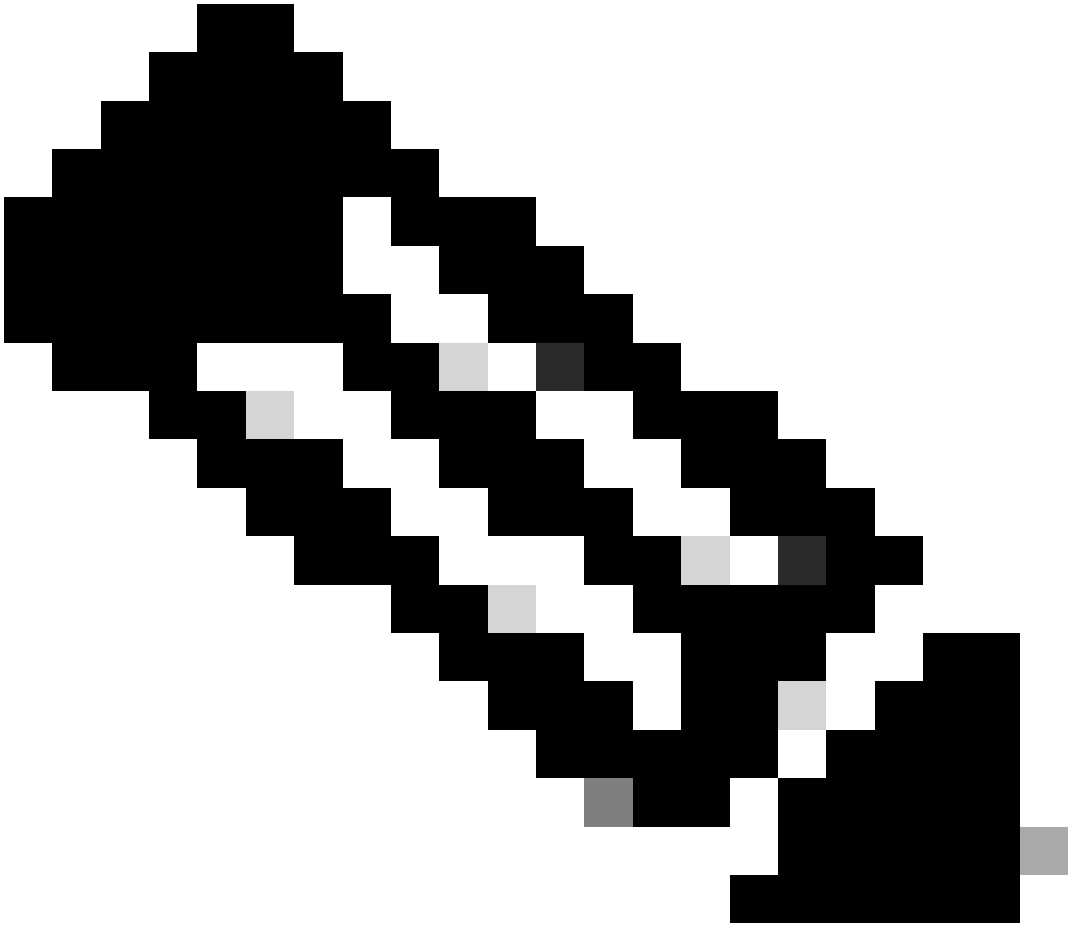
Network Diagram

ISE Configuration

Cisco ISE supports IPsec in tunnel and transport modes. When you enable IPsec on a Cisco ISE interface and configure the peers, an IPsec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPsec authentication. IPsec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces.

Cisco ISE Releases 2.2 and later support IPsec.



Note: Ensure that you have a Cisco ISE Essentials License.

Add a Network Access Device (NAD) with a specific IP address in the Network Devices window.

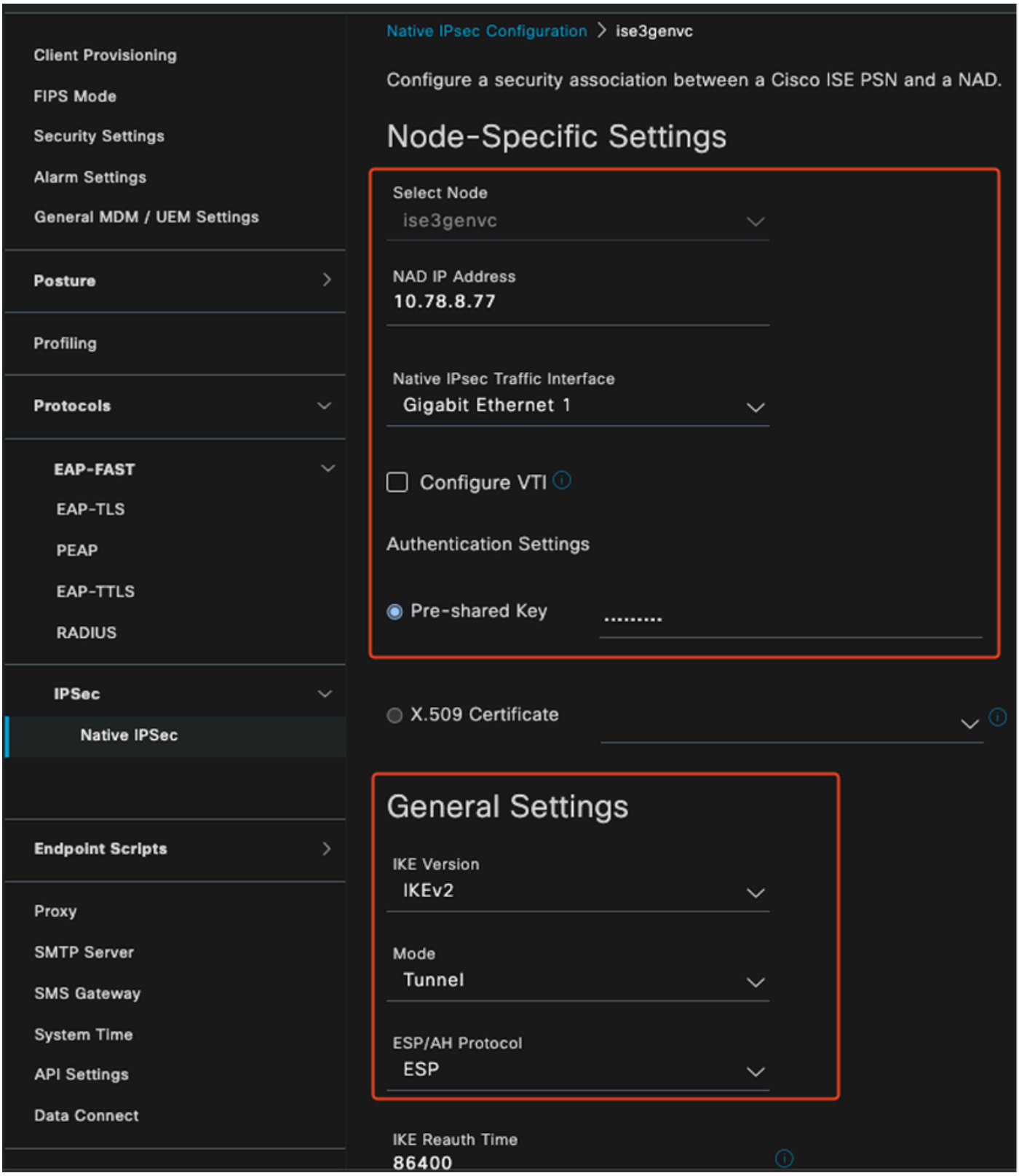
In the Cisco ISE GUI, hover over **Administration** and navigate to **System > Settings > Protocols > IPsec > Native IPsec**.

Click **Add** to configure a security association between a Cisco ISE PSN and a NAD.

- Select the **node**.
- Specify the **NAD IP address**.
- Choose the required IPsec traffic **interface**.
- Enter the **pre-shared** key to be used on NAD as well.

In the General section, enter the details specified.

- Choose the **IKEv2**.
- Select **Tunnel** mode.
- Select **ESP** as the ESP/AH protocol.



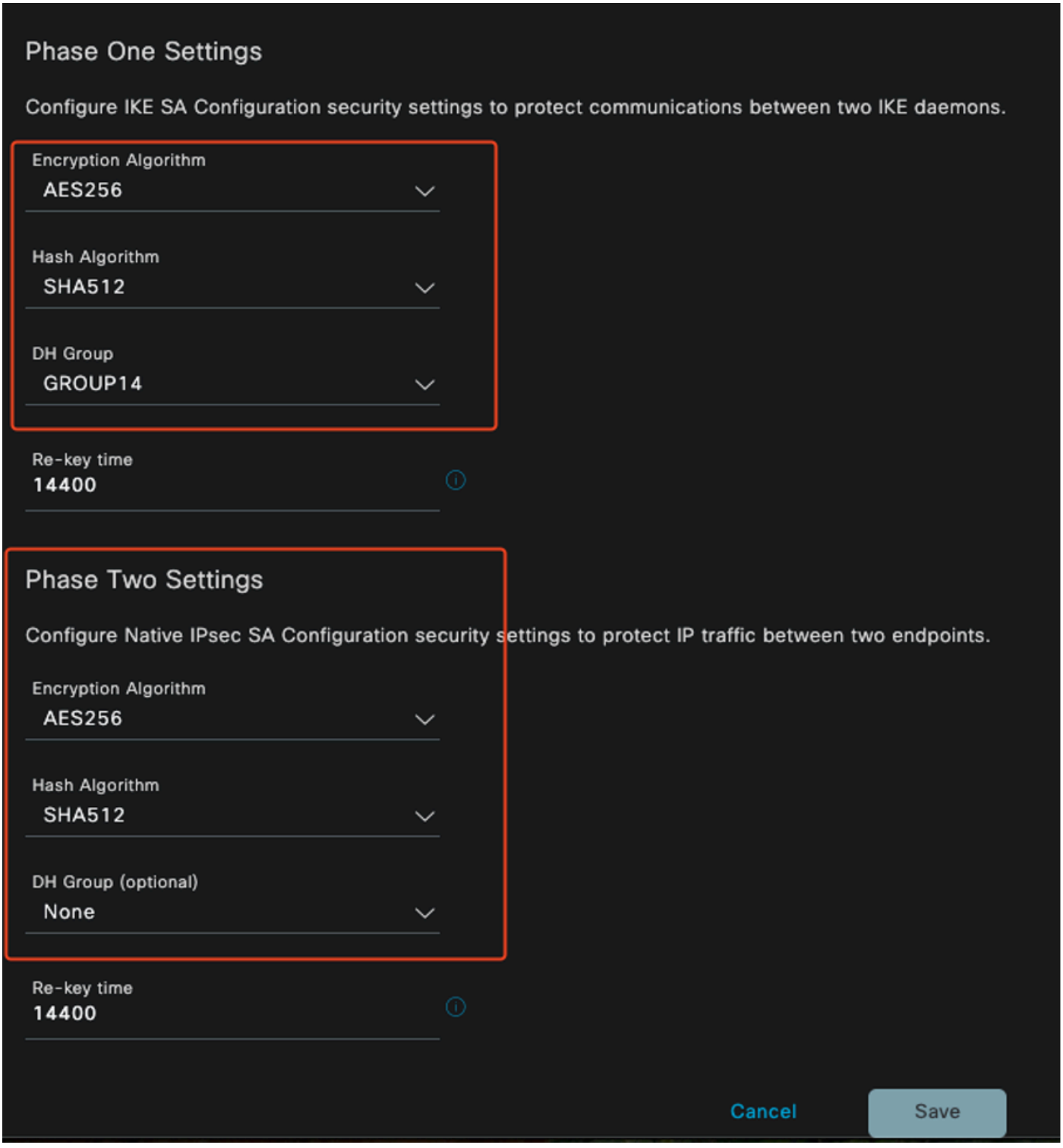
ISE Native IPSec Configuration

In Phase One settings:

- Choose **AES256** as encryption algorithm.
- Select **SHA512** as has algorithm.
- Select **GROUP14** as DH group.

In Phase Two settings:

- Choose **AES256** as encryption algorithm.
- Select **SHA512** as has algorithm.



IPSec Phase 1 and Phase 2 Configuration

Configure a route from the ISE CLI to the WLC using the eth1 gateway as the next hop.

<#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 Configuration

The IPSec configuration of the 9800 WLC is not exposed on the GUI, so all the configuration need to be done from the CLI.

Here are the configuration steps for the ISE server. Each step is accompanied by relevant CLI commands in this section to provide guidance.

WLC IPSec Configuration Steps

IKEv2 Proposal Configuration
To begin the configuration, enter the **global configuration** mode and create an **IKEv2 proposal**. Assign a **unique name** to the proposal for identification purposes.

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

Next, configure a **policy** and map the previously created **proposal** within this policy.

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

Define a **crypto keyring** to be used during IKE authentication. This keyring holds the necessary authentication credentials.

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

Configure an **IKEv2 profile** which acts as a repository for nonnegotiable parameters of the IKE SA. This includes local or remote identities, authentication methods, and available services for authenticated peers.

```
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
```

Create a **transform set** and configure it to operate in tunnel mode.

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

Create an **ACL** to allow communication only to the ISE Interface IP.

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

Configure a **crypto map** from the global configuration. Attach the **transform set**, **IPsec profile**, and **ACL** to the crypto map.

```
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
```

Finally, attach the **crypto map** to the interface. In this scenario, the Wireless management interface carrying the RADIUS traffic is mapped within the management interface VLAN.

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

Verify

WLC

Available show commands to verify IPSec on 9800 WLC.

- **show ip access-lists**
- **show crypto map**
- **show crypto ikev2 sa detailed**
- **show crypto ipsec sa detail**

<#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: BA3FFBBFCF57E6A1 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* ba3ffbbfcf57e6a1_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,
```

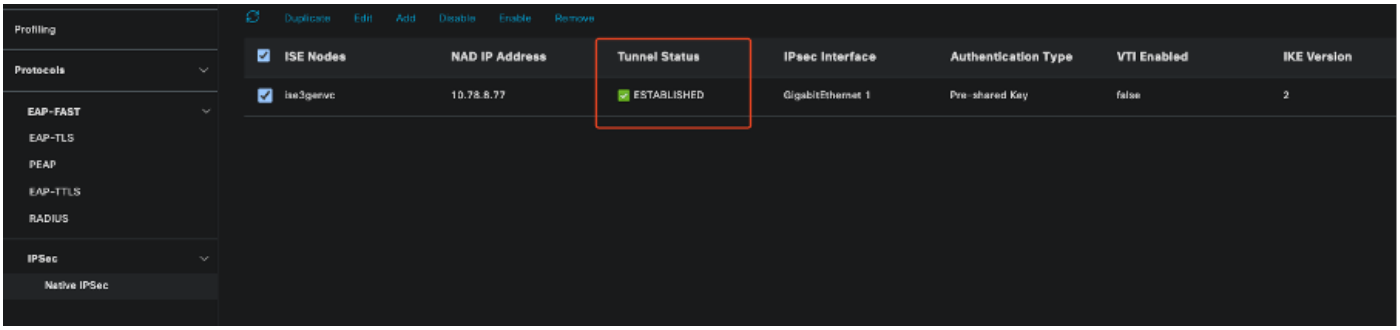
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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 GUI Showing IPSec Status

Packet Capture

Take an EPC on the WLC to ensure that client RADIUS traffic is traversing the ESP tunnel. By using a

control plane capture, you can observe packets leaving the control plane in an unencrypted state, which are then encrypted and transmitted onto the wired network.

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)

IPSec Packets between WLC and ISE

Troubleshoot

WLC Debugs

Since the 9800 WLC operates on Cisco IOS XE, you can utilize IPSec debug commands similar to those on other Cisco IOS XE platforms. Here are two key commands that are useful for troubleshooting IPSec issues.

- **debug crypto ikev2**
- **debug crypto ikev2 error**

ISE debugs

Use this command on the ISE CLI to view IPSec logs. Debugging commands are not necessary on the WLC.

- **show logging application strongswan/charon.log tail**

References

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Cupertino 17.9.x

IPsec Security to Secure Communication Between Cisco ISE and NAD

Configuring Internet Key Exchange Version 2 (IKEv2)

Configure ISE 3.3 Native IPsec to Secure NAD (Cisco IOS XE) Communication