配置Cisco WLC和ISE之間的IPsec隧道

目錄

簡介

本檔案介紹9800 WLC和ISE伺服器之間的網際網路通訊協定安全(IPsec)組態，以保護Radius和TACACS通訊。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- Cisco IOS® XE WLC配置
- 一般IPsec概念
- 一般RADIUS概念
- 一般TACACS概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線控制器：運行17.09.04a的C9800-40-K9
- Cisco ISE:運行版本3補丁4
- 交換器:9200-L-24P

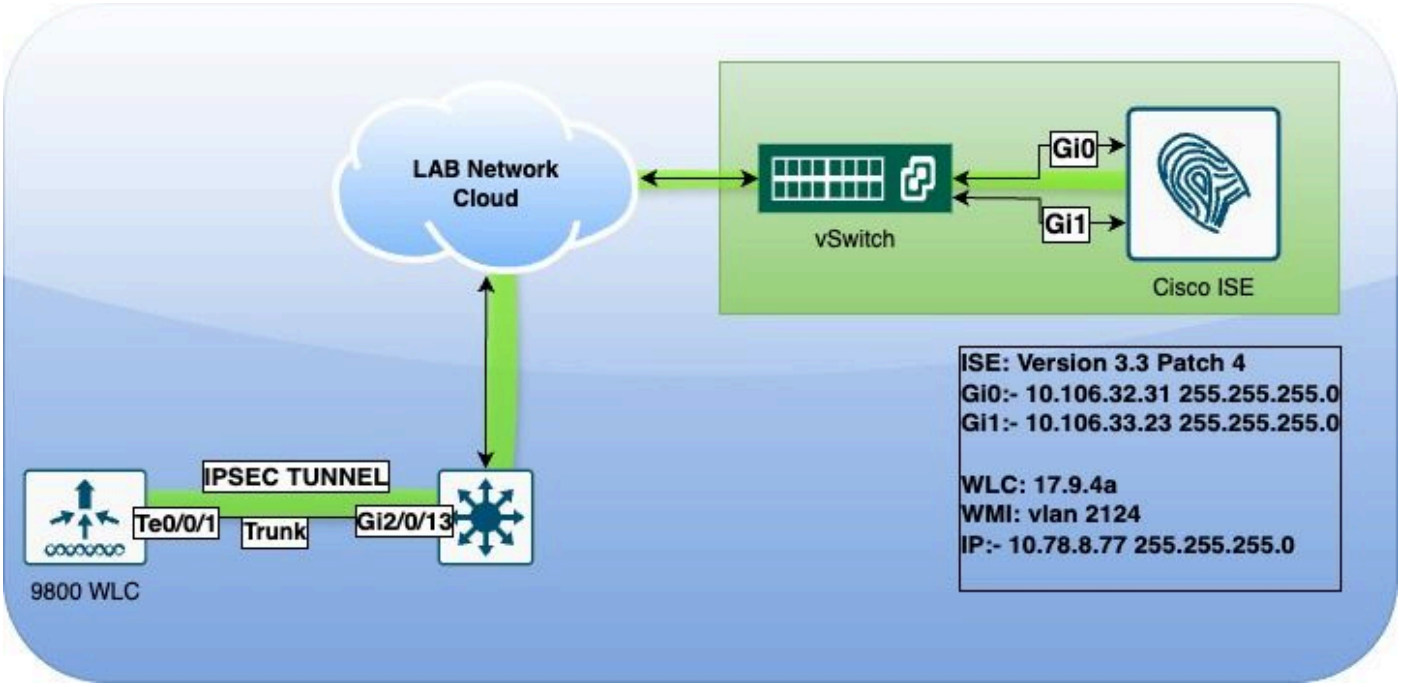
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IPsec是由IETF開發的開放式標準框架。它為通過未受保護的網路（如Internet）傳輸敏感資訊提供了安全性。IPsec在網路層起作用，保護和驗證參與IPsec裝置（對等體）之間的IP資料包，例如思科路由器。在9800 WLC和ISE伺服器之間使用IPsec來保護RADIUS和TACACS通訊。

設定

網路圖表



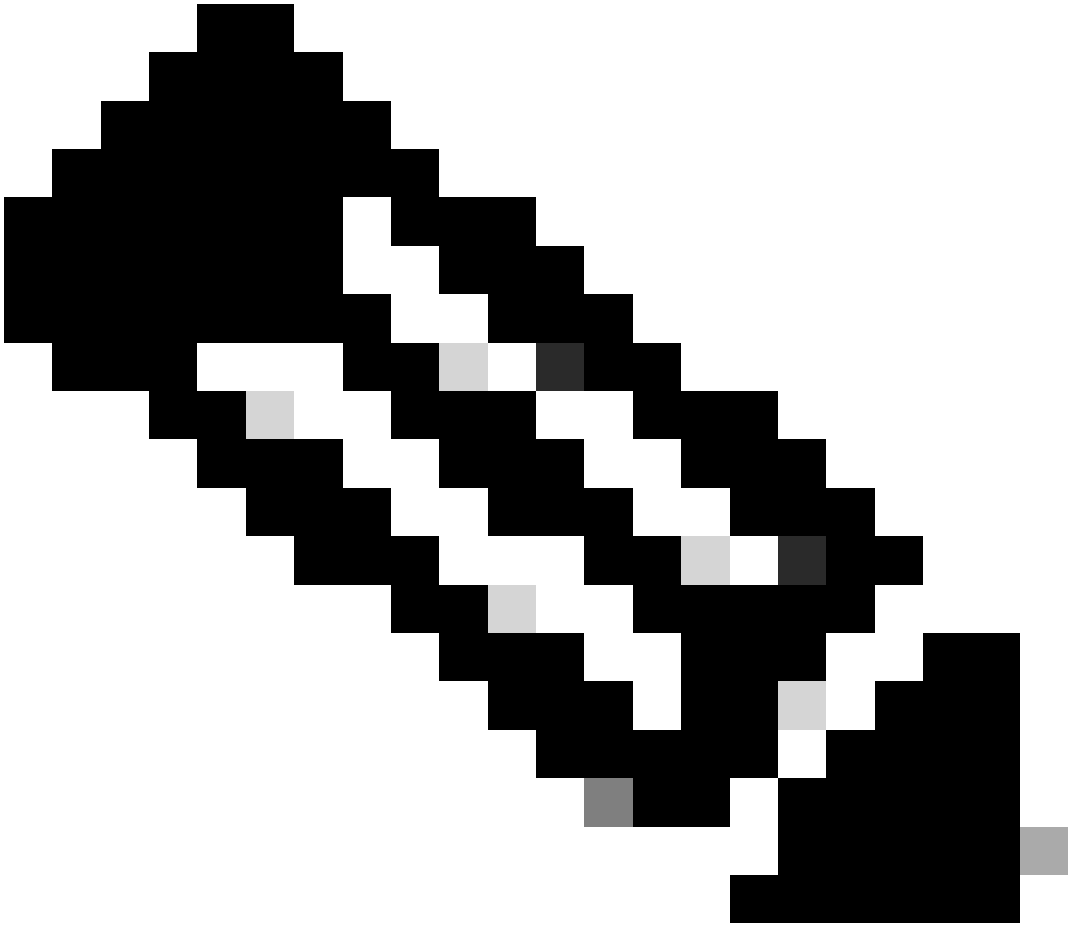
網路圖表

ISE 組態

思科ISE在隧道和傳輸模式下支援IPsec。當您在Cisco ISE介面上啟用IPsec並配置對等裝置時，會在Cisco ISE和NAD之間建立IPsec隧道以保護通訊。

您可以定義預共用金鑰或使用X.509證書進行IPsec身份驗證。IPsec可以在千兆乙太網1上通過千兆乙太網5介面啟用。

Cisco ISE版本2.2和更高版本支援IPsec。



附註：確保您擁有思科ISE基礎許可證。

在Network Devices（網路裝置）視窗中新增具有特定IP地址的網路接入裝置(NAD)。

在Cisco ISE GUI中，將滑鼠懸停在Administration上，然後導航到System > Settings > Protocols > IPsec > Native IPsec。

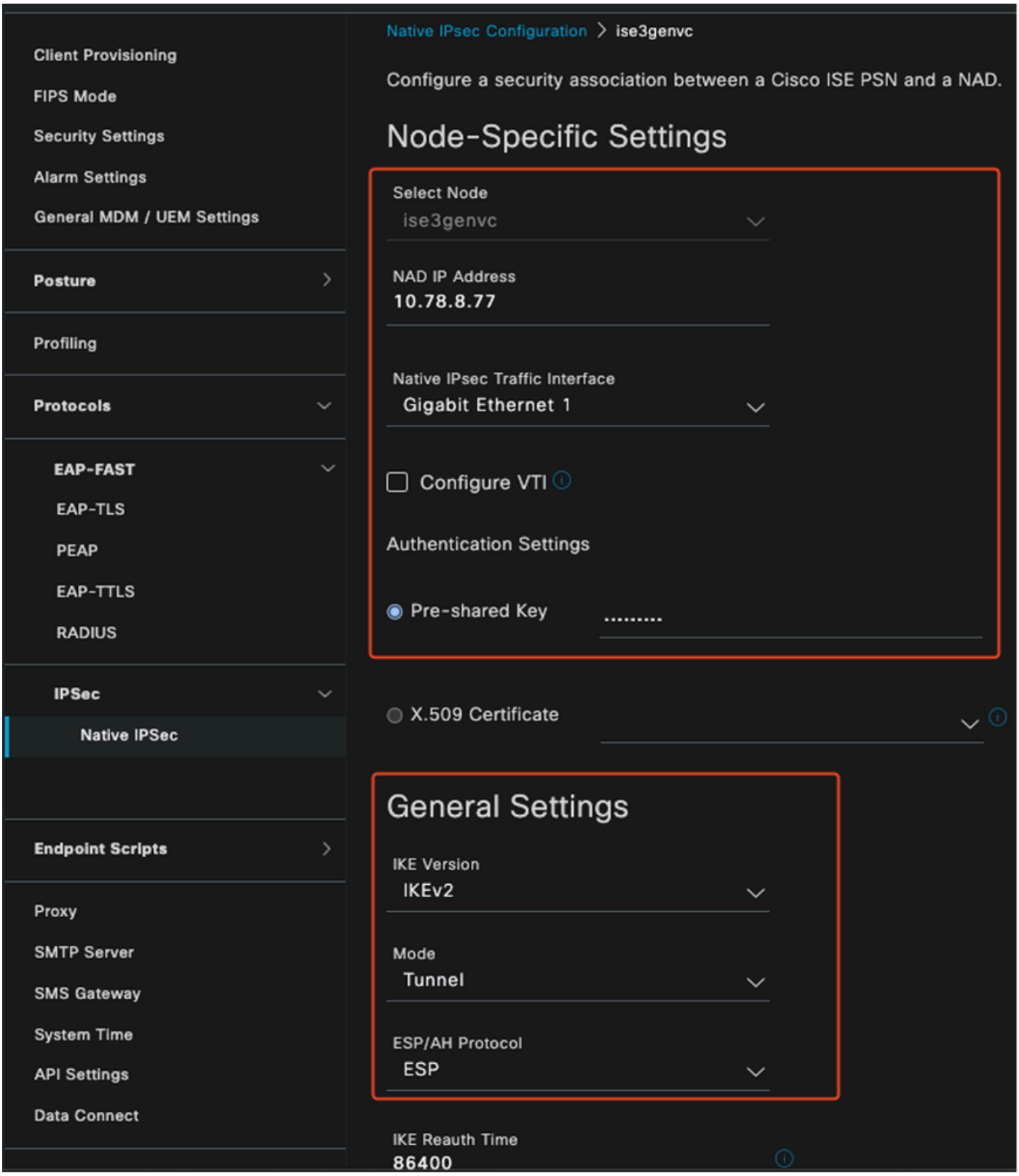
點選Add以配置思科ISE PSN和NAD之間的安全關聯。

- 選擇節點。
- 指定NAD IP地址。
- 選擇所需的IPsec流量介面。
- 輸入要用於NAD的預共用金鑰。

在「一般資訊」部分中，輸入指定的詳細資訊。

- 選擇IKEv2。
- 選擇Tunnel模式。

- 選擇ESP作為ESP/AH協定。



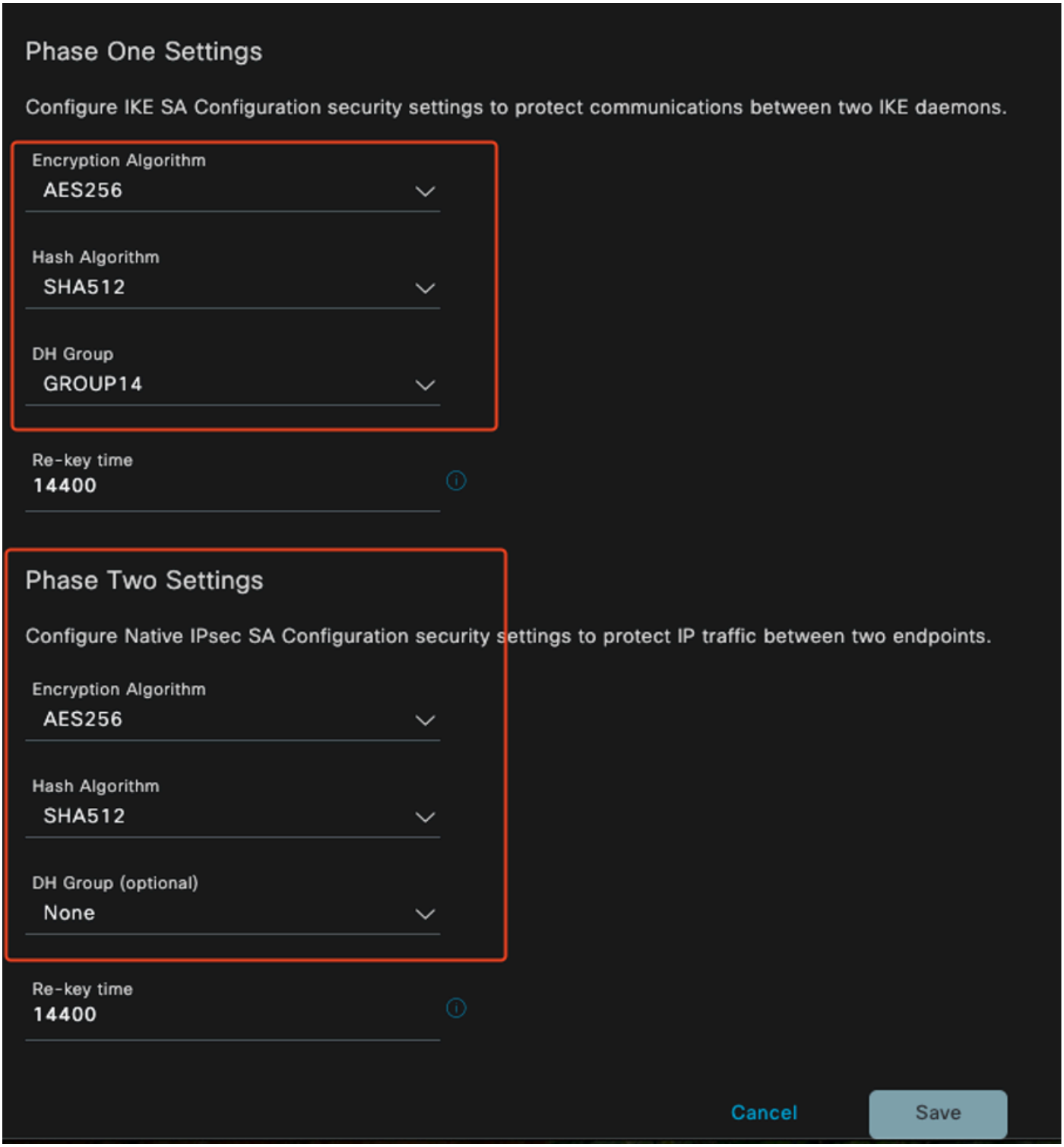
ISE本地IPSec配置

在第一階段設定中：

- 選擇AES256作為加密演算法。
- 選擇SHA512 as has演算法。
- 選擇GROUP14作為DH組。

在第2階段設定中：

- 選擇AES256作為加密演算法。
- 選擇SHA512 as has演算法。



IPSec第1階段和第2階段配置

使用eth1網關作為下一跳，配置從ISE CLI到WLC的路由。

<#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組態

9800 WLC的IPSec配置不會在GUI上公開，因此所有配置都需要在CLI上完成。

以下是ISE伺服器的配置步驟。每個步驟都附帶本部分中的相關CLI命令以提供指導。

WLC IPSec配置步驟

IKEv2建議配置

要開始配置，請進入全域性配置模式並建立IKEv2建議。為建議書分配一個唯一的名稱以標識身份。

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

接下來，配置策略並對映此策略中以前建立的建議。

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

定義要在IKE身份驗證期間使用的加密金鑰環。此金鑰環儲存必需的身份驗證憑據。

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

配置IKEv2配置檔案，該配置檔案用作IKE SA不可協商引數的儲存庫。這包括本地或遠端身份、身份驗證方法和經過身份驗證的對等體的可用服務。

```
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
```

建立轉換集並將其配置為在隧道模式下運行。

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

建立ACL，僅允許與ISE介面IP通訊。

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

從全域性配置配置加密對映。將轉換集、IPsec設定檔和ACL附加到密碼編譯對應。

```
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
```

最後，將加密對映連線到介面。在此方案中，攜帶RADIUS流量的無線管理介面在管理介面VLAN內對映。

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

驗證

WLC

可用的show命令以驗證9800 WLC上的IPSec。

- 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,
```

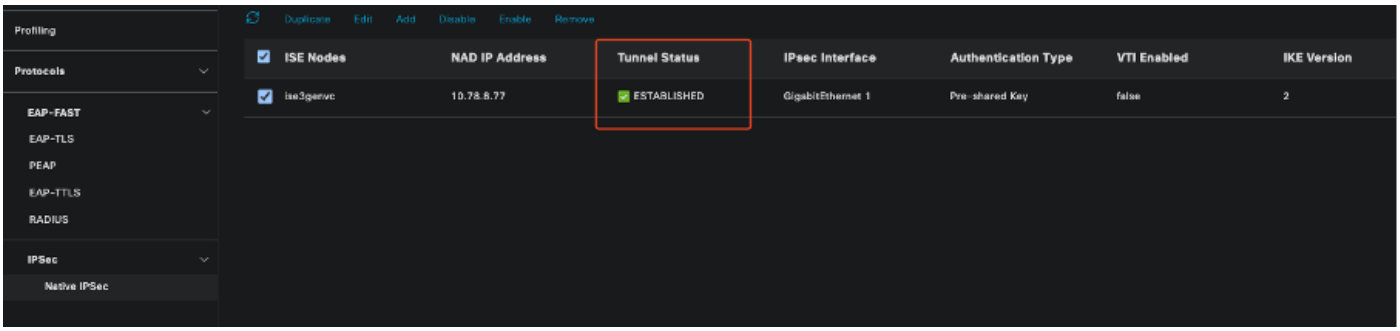
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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.
```



顯示IPSec狀態的ISE GUI

封包捕獲

在WLC上使用EPC，以確保使用者端RADIUS流量通過ESP通道。通過使用控制平面捕獲，您可以觀察資料包以未加密狀態離開控制平面，然後對資料包進行加密並將其傳輸到有線網路。

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)

WLC和ISE之間的IPSec封包

疑難排解

WLC調試

由於9800 WLC在Cisco IOS XE上運行，因此您可以使用與其他Cisco IOS XE平台上的IPSec debug命令類似的IPSec debug命令。以下是可用於排除IPSec問題的兩個關鍵命令。

- debug crypto ikev2
- debug crypto ikev2 error

ISE調試

在ISE CLI上使用此命令檢視IPSec日誌。WLC上不需要調試命令。

- show logging application strongswan/charon.log tail

參考資料

Cisco Catalyst 9800系列無線控制器軟體配置指南，Cisco IOS XE Cupertino 17.9.x

通過IPsec安全保護思科ISE和NAD之間的通訊

配置Internet金鑰交換版本2(IKEv2)

配置ISE 3.3本地IPsec以保護NAD(Cisco IOS XE)通訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。