在Cisco WLC和ISE之间配置IPsec隧道

目录

简介

本文档介绍9800 WLC和ISE服务器之间的互联网协议安全(IPsec)配置，以保护Radius和TACACS通信。

先决条件

要求

Cisco 建议您了解以下主题：

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线控制器:运行17.09.04a的C9800-40-K9
- 思科ISE:运行版本3补丁4
- 交换机：9200-L-24P

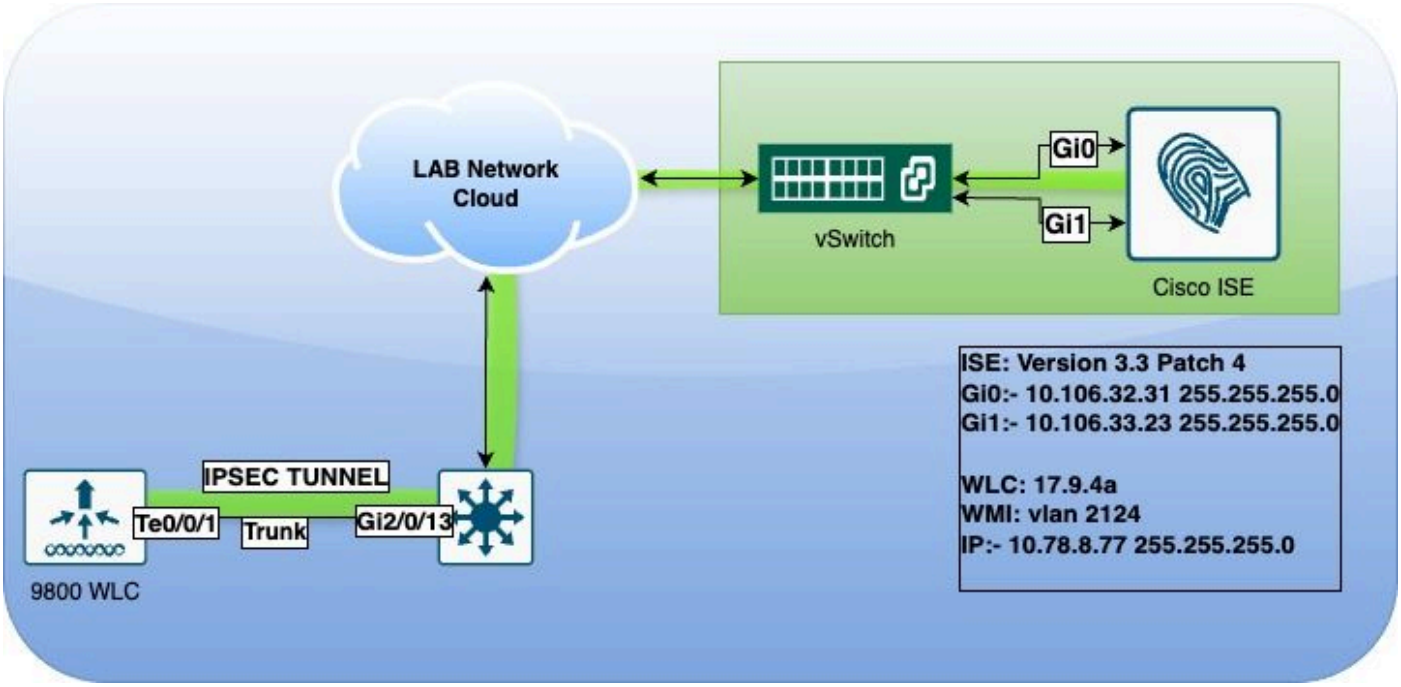
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

IPsec是由IETF开发的开放式标准框架。它为通过未受保护的网络（例如Internet）传输敏感信息提供了安全性。IPsec在网络层起作用，保护和验证参与的IPsec设备（对等体）（例如Cisco路由器）之间的IP数据包。在9800 WLC和ISE服务器之间使用IPsec来保护RADIUS和TACACS通信。

配置

网络图



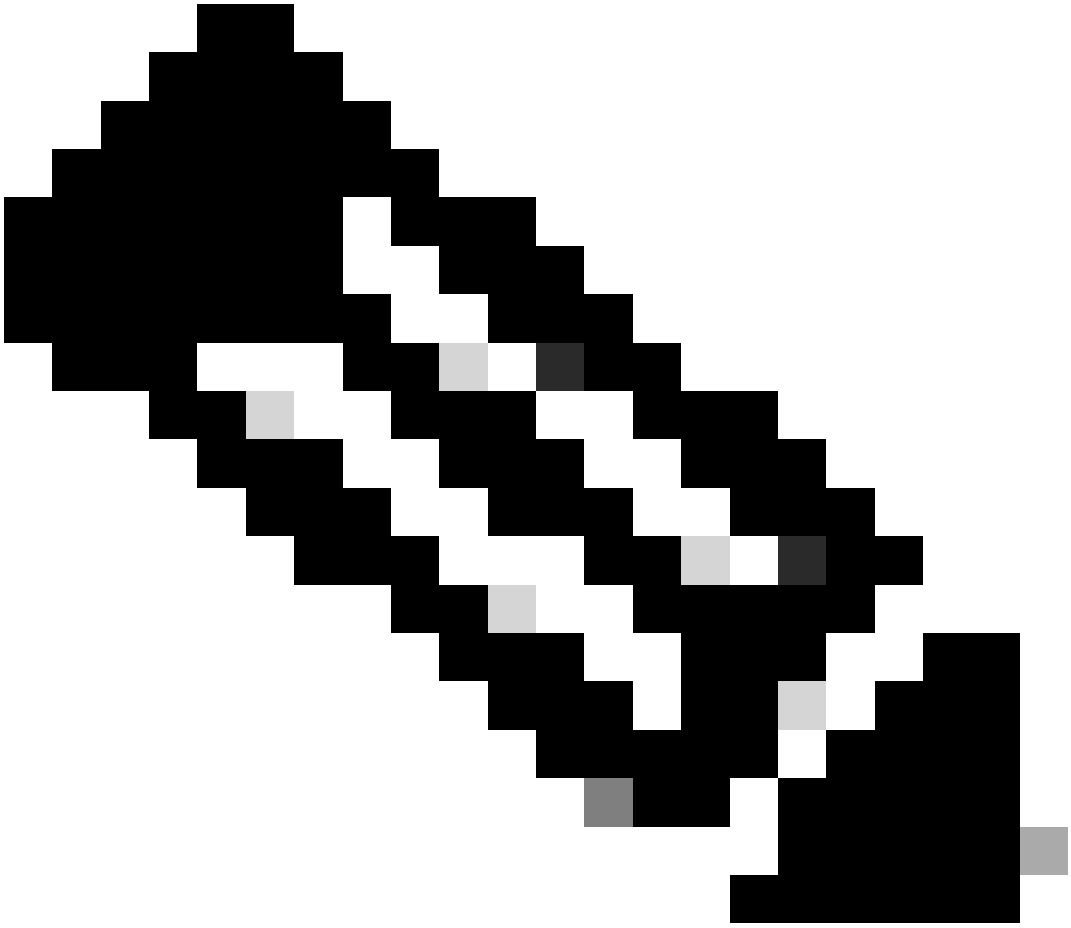
网络图

ISE 配置

思科ISE在隧道和传输模式下支持IPsec。当您在思科ISE接口上启用IPsec并配置对等体时，会在思科ISE和需要之间创建IPsec隧道以保护通信。

您可以定义预共享密钥或使用X.509证书进行IPsec身份验证。IPsec可在千兆以太网1到千兆以太网5接口上启用。

Cisco ISE版本2.2及更高版本支持IPsec。



注意：确保您拥有思科ISE基础版许可证。

在Network Devices窗口中添加具有特定IP地址的网络接入设备(NAD)。

在Cisco ISE GUI中，将鼠标悬停在Administration上，然后导航到System > Settings > Protocols > IPsec > Native IPsec。

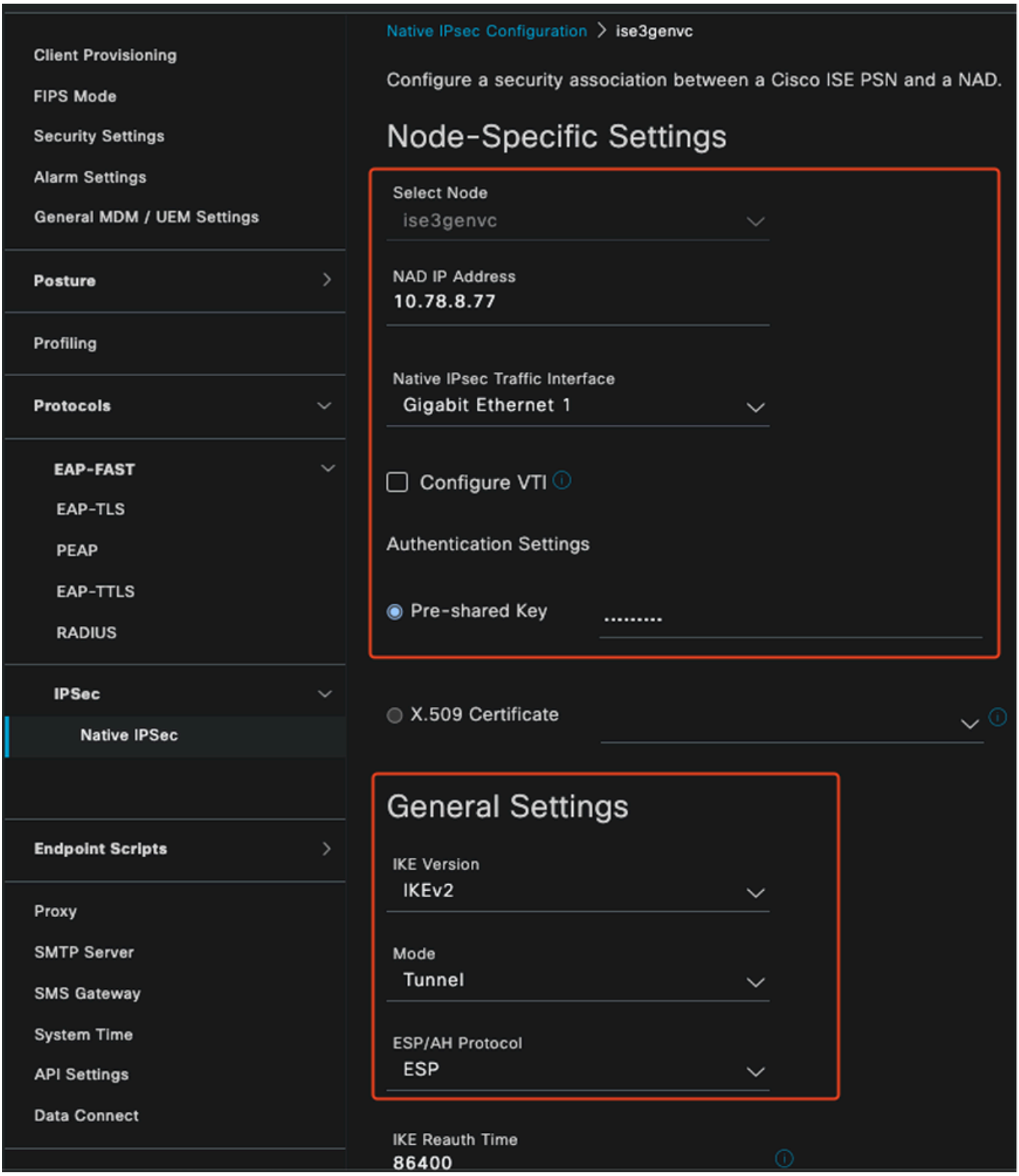
单击Add以配置思科ISE PSN和NAD之间的安全关联。

- 选择节点。
- 指定NAD IP地址。
- 选择所需的IPsec流量接口。
- 输入要在NAD上使用的预共享密钥。

在“一般信息”部分中，输入指定的详细信息。

- 选择IKEv2。
- 选择Tunnel模式。

- 选择ESP作为ESP/AH协议。



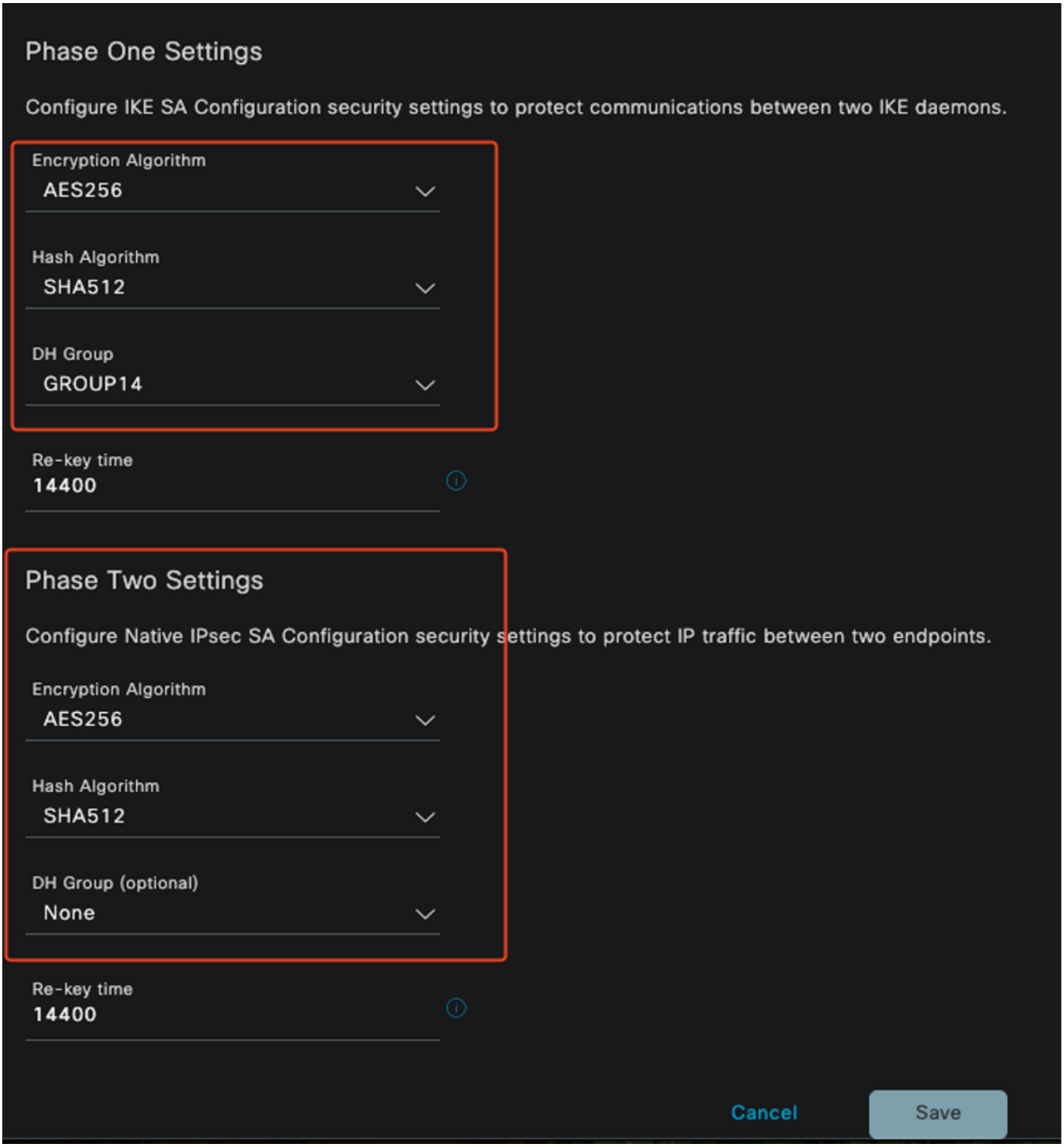
ISE本地IPSec配置

在第一阶段设置中：

- 选择AES256作为加密算法。
- 选择SHA512作为算法。
- 选择GROUP14作为DH组。

在第2阶段设置中：

- 选择AES256作为加密算法。
- 选择SHA512作为算法。



IPSec第1阶段和第2阶段配置

使用eth1网关作为下一跳，配置从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配置

9800 WLC的IPSec配置不会显示在GUI上，因此所有配置都需要从CLI中完成。

以下是ISE服务器的配置步骤。每个步骤都附带本部分中的相关CLI命令以提供指导。

WLC IPSec配置步骤

IKEv2建议配置

要开始配置，请进入全局配置模式并创建IKEv2提议。为建议书分配唯一名称，以便进行标识。

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

接下来，配置策略并在此策略中映射之前创建的建议。

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

定义要在IKE身份验证期间使用的加密密钥环。此密钥环拥有必要的身份验证身份证明。

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

配置IKEv2配置文件，该配置文件用作IKE SA不可协商参数的存储库。这包括本地或远程身份、身份验证方法以及经过身份验证的对等体的可用服务。

```
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
```

创建转换集并将其配置为在隧道模式下运行。

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

创建ACL，仅允许与ISE接口IP通信。

```
ip access-list extended ISE_ALLOW
```

```
 10 permit ip host  10.78.8.77 host 10.106.33.23
```

从全局配置配置加密映射。将转换集、IPsec配置文件和ACL附加到加密映射。

```
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
```

最后，将加密映射附加到接口。在此方案中，携带RADIUS流量的无线管理接口在管理接口VLAN内映射。

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

验证

WLC

可用的show命令用于检验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,
```

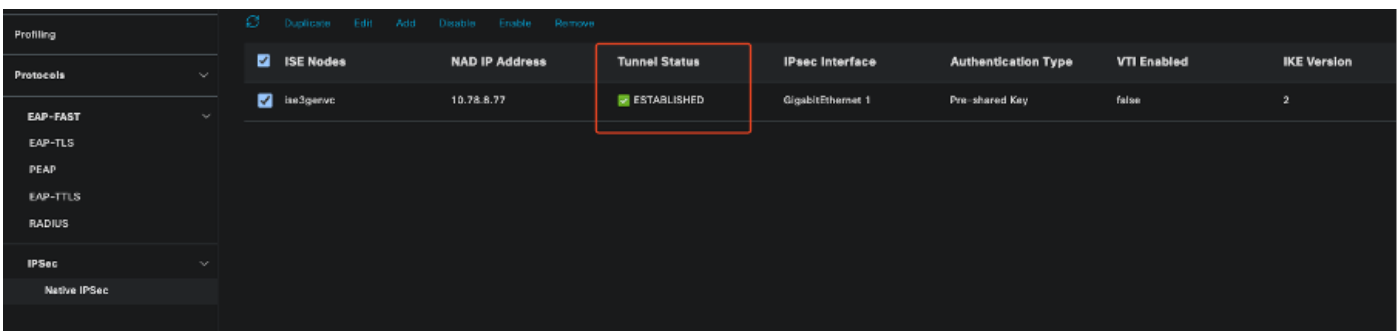
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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.



显示IPSec状态的ISE GUI

数据包捕获

在WLC上采用EPC以确保客户端RADIUS流量通过ESP隧道。通过使用控制平面捕获，您可以观察以未加密状态离开控制平面的数据包，然后这些数据包将被加密并传输到有线网络。

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之间的IPSec数据包

故障排除

WLC调试

由于9800 WLC在Cisco IOS XE上运行，因此您可以使用与其他Cisco IOS XE平台类似的IPSec debug命令。下面是对IPSec问题故障排除非常有用的两个关键命令。

- debug crypto ikev2
- debug crypto ikev2 error

ISE调试

在ISE CLI上使用此命令查看IPSec日志。WLC不需要调试命令。

- show logging application strongswan/charon.log tail

参考

Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS XE Cupertino 17.9.x

IPsec安全保护思科ISE和需要之间的通信

配置Internet密钥交换版本2(IKEv2)

配置ISE 3.3本地IPsec以保护NAD(Cisco IOS XE)通信

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。