Configuración del túnel IPsec entre Cisco WLC e ISE

Contenido

Introducción

Este documento describe la configuración del protocolo de seguridad de Internet (IPsec) entre el WLC 9800 y el servidor ISE para asegurar la comunicación Radius y TACACS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Configuración de WLC de Cisco IOS® XE
- Conceptos generales de IPsec
- Conceptos generales de RADIUS
- Conceptos generales de TACACS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico: C9800-40-K9 que ejecuta 17.09.04a
- Cisco ISE: Ejecución del Parche 4 de la Versión 3
- Switch: 9200-L-24P

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

IPSec es un marco de estándares abiertos desarrollado por el IETF. Proporciona seguridad para la transmisión de información confidencial a través de redes no protegidas como Internet. IPSec actúa en la capa de red, protegiendo y autenticando paquetes IP entre los dispositivos IPSec participantes (peers), como routers Cisco. Utilice IPSec entre el WLC 9800 y el servidor ISE para asegurar la comunicación RADIUS y TACACS.

Configurar

Diagrama de la red

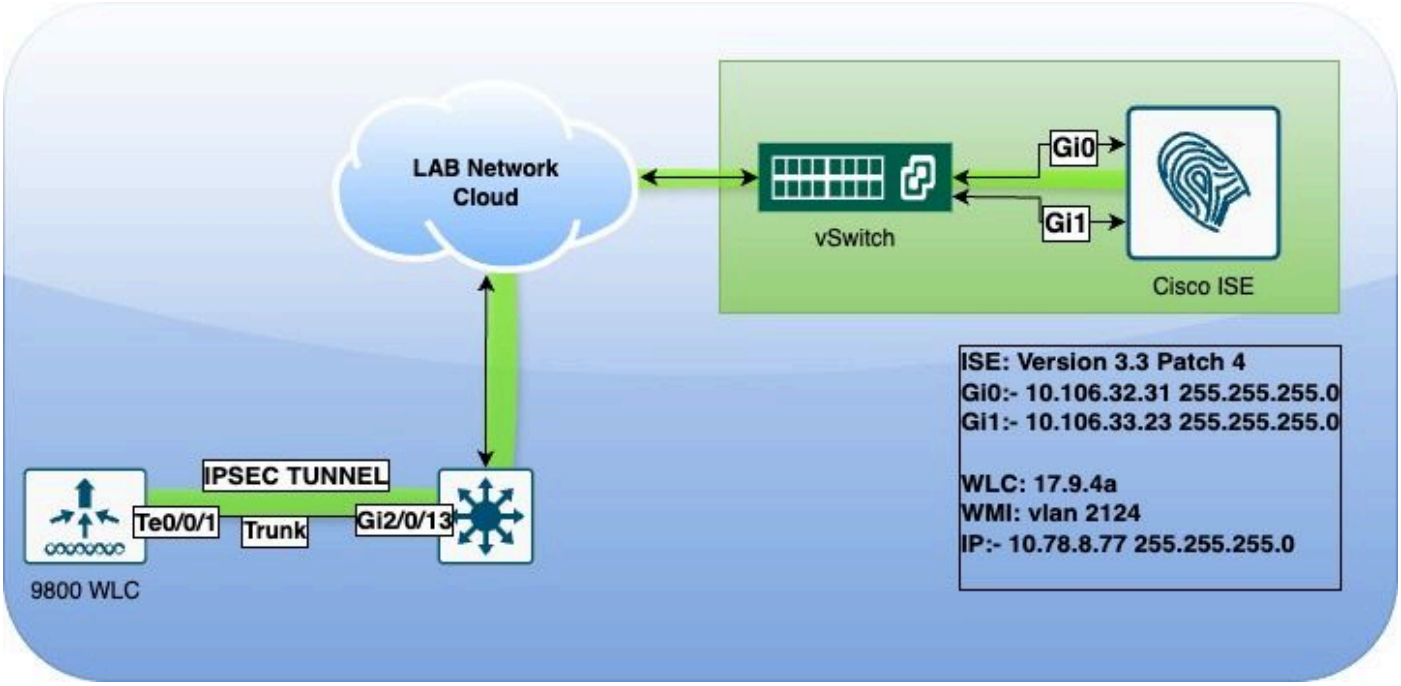


Diagrama de la red

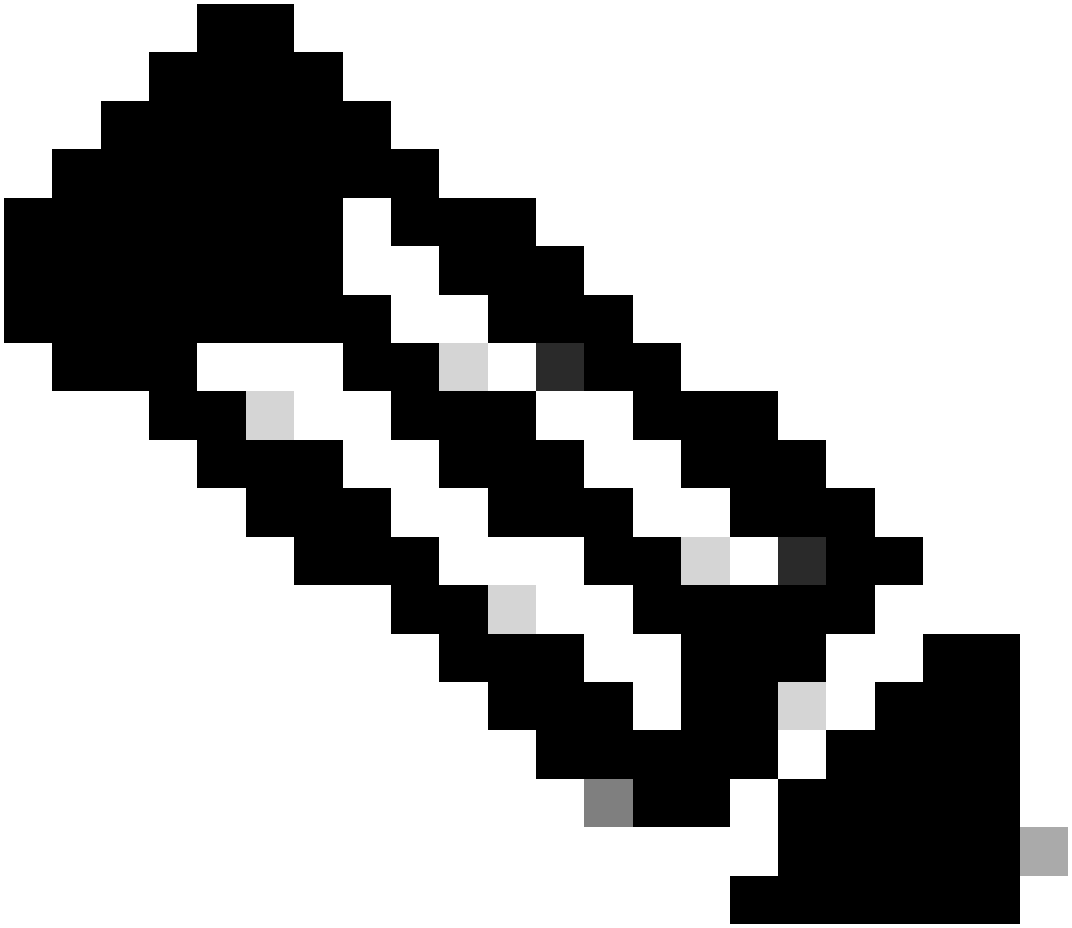
Configuración de ISE

Cisco ISE admite IPsec en los modos de túnel y transporte. Al habilitar IPsec en una interfaz

Cisco ISE y configurar los pares, se crea un túnel IPsec entre Cisco ISE y NAD para proteger la comunicación.

Puede definir una clave previamente compartida o utilizar certificados X.509 para la autenticación IPsec. IPsec se puede habilitar en interfaces Gigabit Ethernet 1 a Gigabit Ethernet 5.

Las versiones 2.2 y posteriores de Cisco ISE admiten IPsec.



Nota: Asegúrese de que dispone de una licencia Cisco ISE Essentials.

Agregue un dispositivo de acceso a la red (NAD) con una dirección IP específica en la ventana Dispositivos de red.

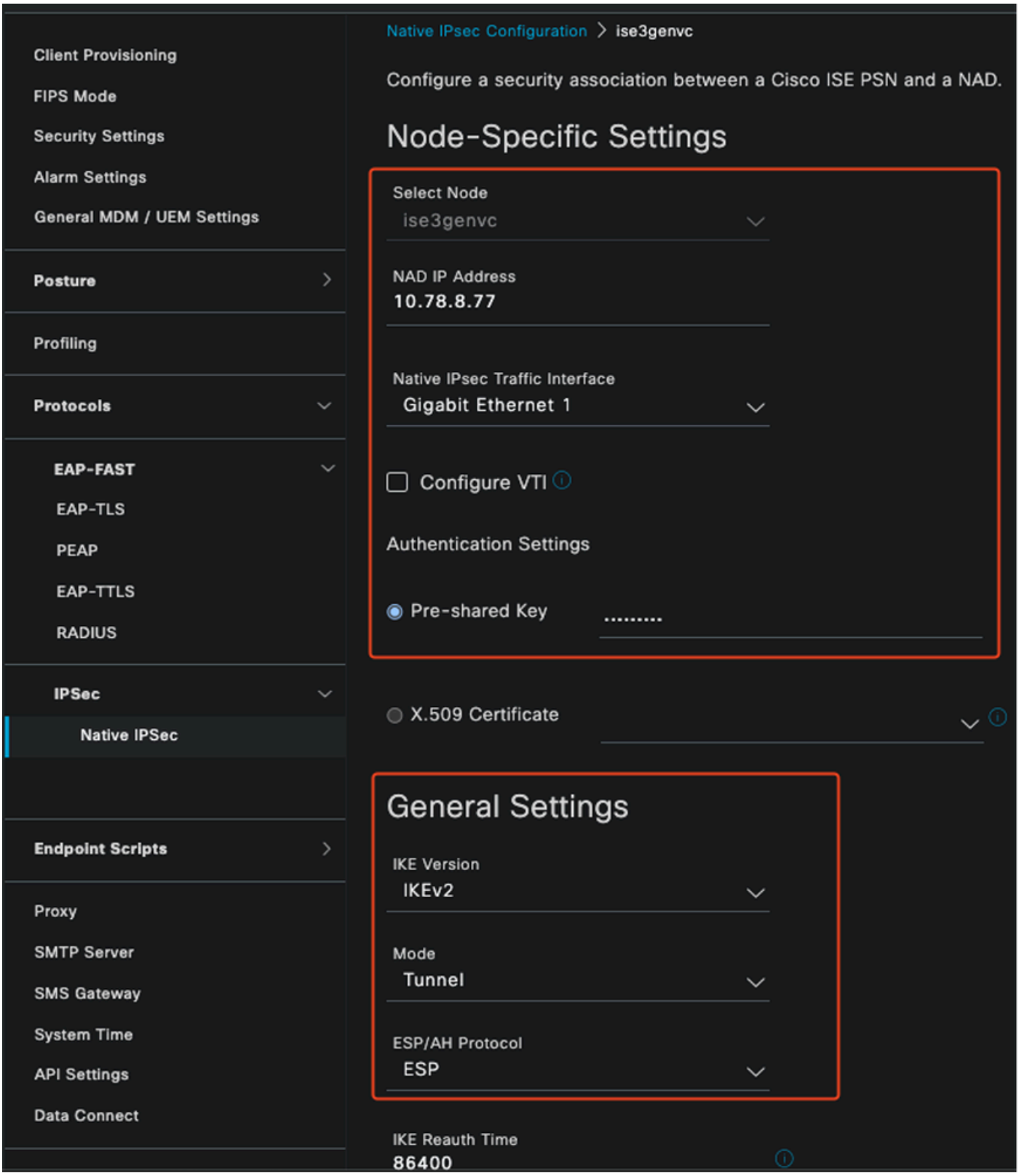
En la GUI de Cisco ISE, pase el cursor sobre Administration y navegue hasta System > Settings > Protocols > IPsec > Native IPsec.

Haga clic en Agregar para configurar una asociación de seguridad entre un Cisco ISE PSN y un NAD.

- Seleccione el nodo.
- Especifique la dirección IP de NAD.
- Elija la interfaz de tráfico IPsec requerida.
- Ingrese también la clave previamente compartida que se utilizará en NAD.

En la sección General, introduzca los detalles especificados.

- Elija el IKEv2.
- Seleccione el modo Túnel.
- Seleccione ESP como el protocolo ESP/AH.



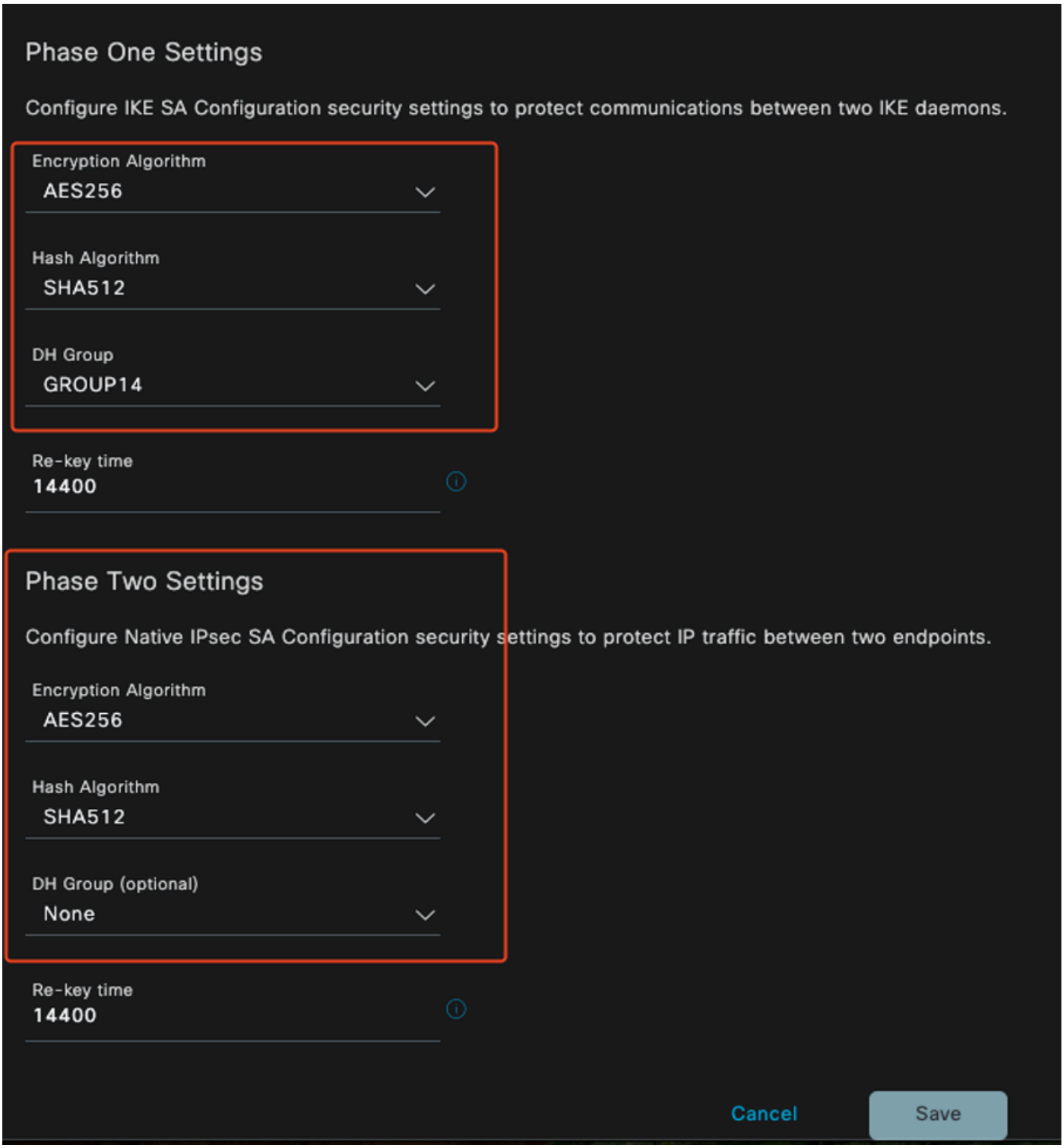
Configuración de IPSec nativo de ISE

En Configuración de la fase uno:

- Elija AES256 como algoritmo de cifrado.
- Seleccione SHA512 como tiene el algoritmo.
- Seleccione GROUP14 como grupo DH.

En la configuración de la fase dos:

- Elija AES256 como algoritmo de cifrado.
- Seleccione SHA512 como tiene el algoritmo.



Configuración de Fase 1 y Fase 2 de IPSec

Configure una ruta desde la CLI de ISE al WLC usando la gateway eth1 como el salto siguiente.

<#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
```

Configuración de 9800 WLC

La configuración IPSec del WLC 9800 no se expone en la GUI, por lo que toda la configuración debe realizarse desde la CLI.

Estos son los pasos de configuración para el servidor ISE. Cada paso se acompaña de los comandos CLI relevantes en esta sección para proporcionar orientación.

Pasos de Configuración IPSec de WLC

Configuración de la propuesta IKEv2

Para comenzar la configuración, ingrese al modo de configuración global y cree una propuesta IKEv2. Asigne un nombre único a la propuesta con fines de identificación.

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

A continuación, configure una política y asigne la propuesta creada anteriormente dentro de esta política.

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

Defina un anillo de claves criptográficas que se utilizará durante la autenticación IKE. Este anillo de claves contiene las credenciales de autenticación necesarias.

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

Configure un perfil IKEv2 que actúe como repositorio para los parámetros no negociables de la SA IKE. Esto incluye las identidades locales o remotas, los métodos de autenticación y los servicios disponibles para los pares autenticados.

```
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
```

Cree un conjunto de transformación y configúrelo para que funcione en modo de túnel.

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

Cree una ACL para permitir la comunicación solo con la IP de la interfaz de ISE.

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

Configure un mapa criptográfico desde la configuración global. Adjunte el conjunto de transformación, el perfil IPsec y la ACL al mapa criptográfico.

```
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
```

Finalmente, adjunte el mapa criptográfico a la interfaz. En este escenario, la interfaz de administración inalámbrica que transporta el tráfico RADIUS se mapea dentro de la VLAN de la interfaz de administración.

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

Verificación

WLC

Comandos show disponibles para verificar IPSec en el WLC 9800.

- 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,
```

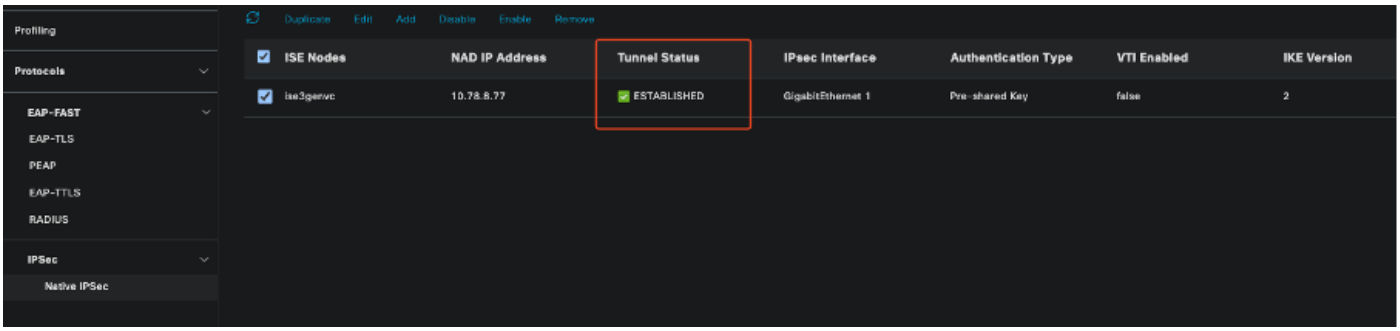
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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.
```



GUI de ISE que muestra el estado de IPSec

Captura de paquete

Tome un EPC en el WLC para asegurarse de que el tráfico RADIUS del cliente atraviese el túnel ESP. Al utilizar una captura de plano de control, puede observar los paquetes que salen del plano de control en un estado no cifrado, que se cifran y transmiten a la red con cables.

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)

Paquetes IPSec entre WLC e ISE

Troubleshoot

Depuraciones de WLC

Dado que el WLC 9800 funciona en Cisco IOS XE, puede utilizar comandos de depuración IPSec similares a los de otras plataformas Cisco IOS XE. Aquí hay dos comandos clave que son útiles para resolver problemas de IPSec.

- debug crypto ikev2
- debug crypto ikev2 error

Depuraciones de ISE

Utilice este comando en la CLI de ISE para ver los registros de IPSec. Los comandos de

depuración no son necesarios en el WLC.

- show logging application strongswan/charon.log tail

Referencias

Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800, Cisco IOS XE Cupertino 17.9.x

Seguridad IPsec para garantizar la comunicación entre Cisco ISE y NAD

Configuración de Intercambio de claves de Internet versión 2 (IKEv2)

Configuración de IPsec nativo de ISE 3.3 para la comunicación NAD segura (Cisco IOS XE)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).