Configurar o túnel IPsec entre Cisco WLC e ISE

Contents

Introdução

Este documento descreve a configuração do Internet Protocol Security (IPsec) entre a WLC 9800 e o servidor ISE para proteger a comunicação Radius & TACACS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Configuração da WLC Cisco IOS® XE
- Conceitos gerais de IPsec
- Conceitos gerais do RADIUS
- Conceitos gerais do TACACS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador sem fio: C9800-40-K9 executando 17.09.04a
- Cisco ISE: Executando o Patch 4 da Versão 3
- Switch: 9200-L-24P

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O IPsec é uma estrutura de padrões abertos desenvolvida pela IETF. Ele fornece segurança para a transmissão de informações confidenciais por redes desprotegidas, como a Internet. O IPsec atua na camada de rede, protegendo e autenticando pacotes IP entre dispositivos IPsec participantes (pares), como roteadores Cisco. Use o IPsec entre a WLC 9800 e o servidor ISE para proteger a comunicação RADIUS e TACACS.

Configurar

Diagrama de Rede

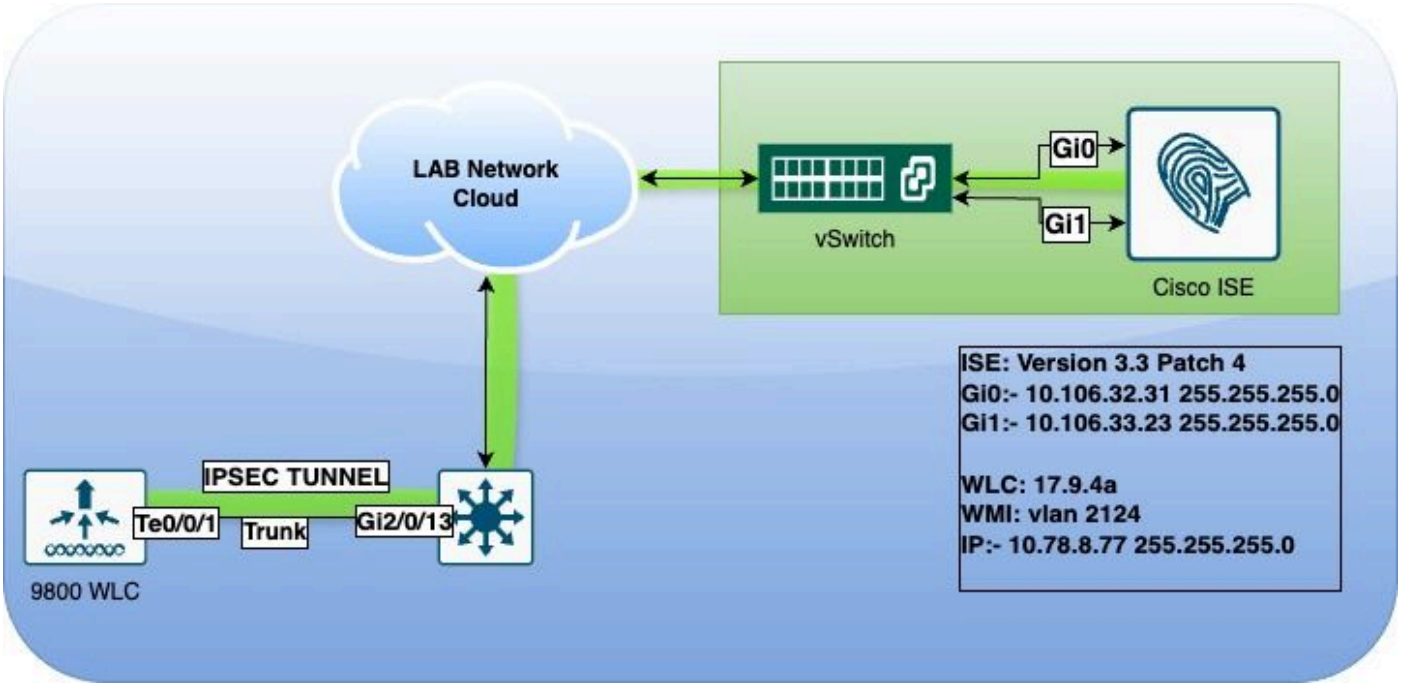


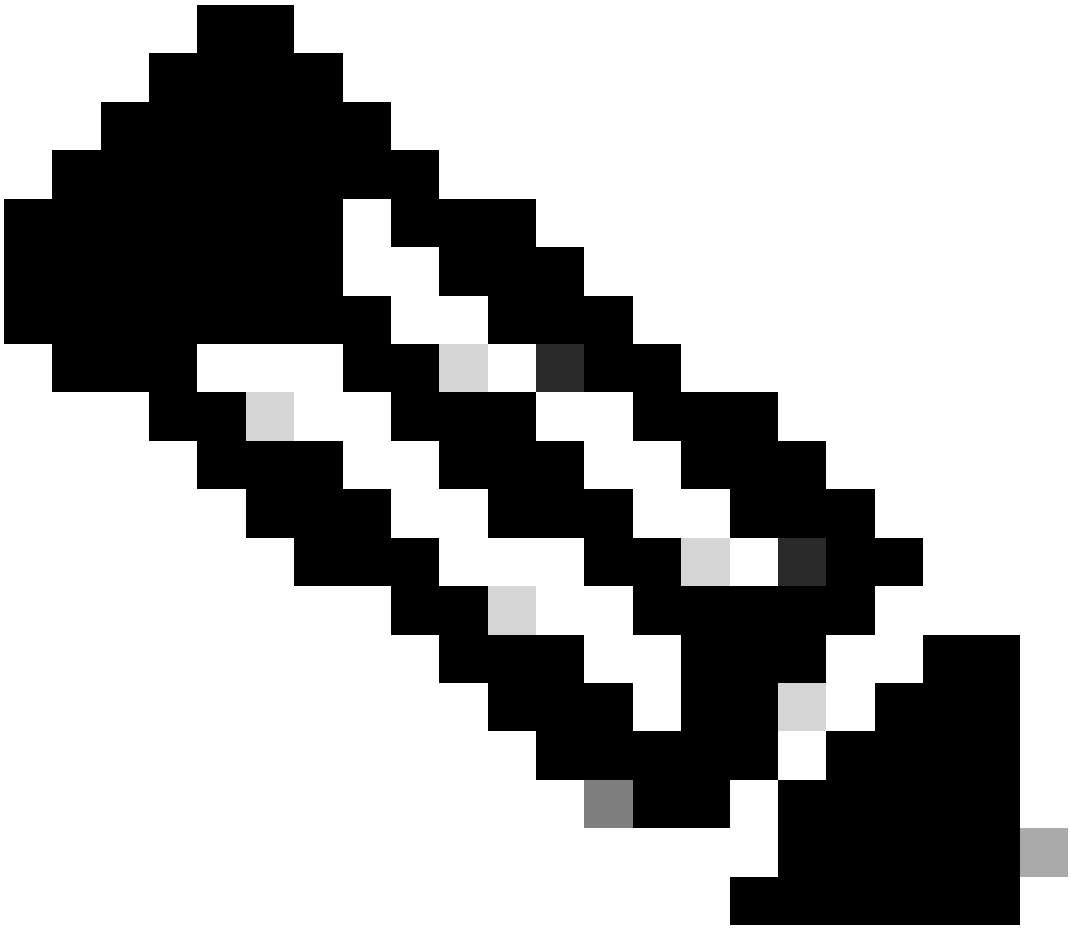
Diagrama de Rede

Configuração do ISE

O Cisco ISE suporta IPsec em modos de túnel e transporte. Quando você habilita o IPsec em uma interface Cisco ISE e configura os correspondentes, um túnel IPsec é criado entre o Cisco ISE e o NAD para proteger a comunicação.

Você pode definir uma chave pré-compartilhada ou usar certificados X.509 para autenticação IPsec. O IPsec pode ser habilitado em interfaces Gigabit Ethernet 1 a Gigabit Ethernet 5.

O Cisco ISE versões 2.2 e posteriores oferecem suporte a IPsec.



Note: Verifique se você tem uma licença do Cisco ISE Essentials.

Adicione um dispositivo de acesso à rede (NAD) com um endereço IP específico na janela Dispositivos de rede.

Na GUI do Cisco ISE, passe o mouse sobre Administration e navegue para System > Settings > Protocols > IPsec > Native IPsec.

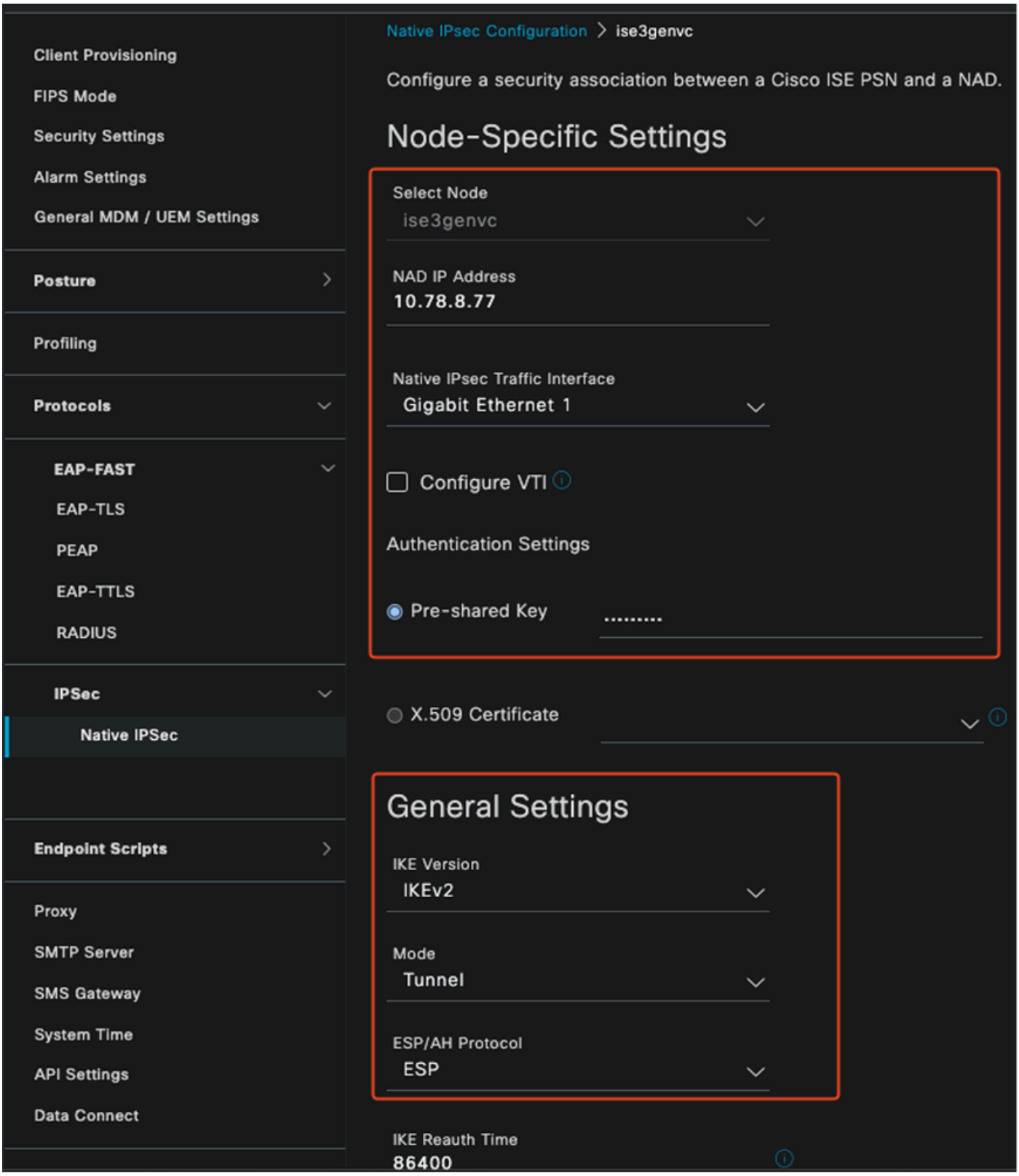
Clique em Adicionar para configurar uma associação de segurança entre um PSN do Cisco ISE e um NAD.

- Selecione o nó.
- Especifique o endereço IP NAD.

- Escolha a interface de tráfego IPsec necessária.
- Insira a chave pré-compartilhada a ser usada no NAD também.

Na seção Geral, insira os detalhes especificados.

- Escolha o IKEv2.
- Selecione o modo Tunnel.
- Selecione ESP como o protocolo ESP/AH.

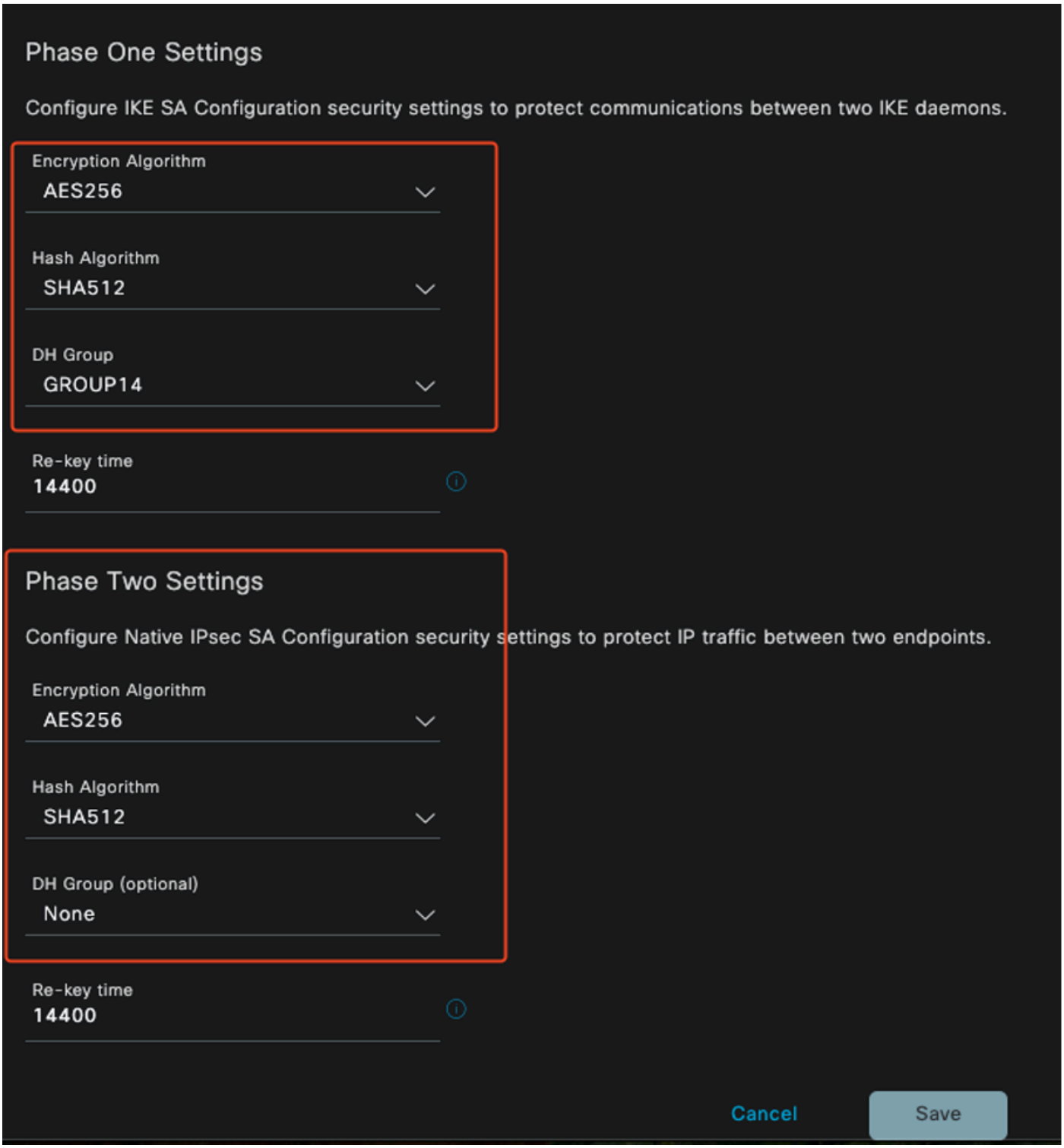


Nas configurações da Fase Um:

- Escolha AES256 como algoritmo de criptografia.
- Selecione SHA512 como possui algoritmo.
- Selecione GROUP14 como grupo DH.

Nas configurações da Fase Dois:

- Escolha AES256 como algoritmo de criptografia.
- Selecione SHA512 como possui algoritmo.



Configuração de IPSec fase 1 e fase 2

Configure uma rota da CLI do ISE para a WLC usando o gateway eth1 como o próximo salto.

<#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
```

Configuração da WLC 9800

A configuração IPSec da WLC 9800 não é exposta na GUI, portanto, toda a configuração precisa ser feita na CLI.

Estas são as etapas de configuração do servidor ISE. Cada etapa é acompanhada por comandos CLI relevantes nesta seção para fornecer orientação.

Etapas de configuração de IPSec da WLC

Configuração de proposta de IKEv2

Para iniciar a configuração, entre no modo de configuração global e crie uma proposta IKEv2. Atribua um nome exclusivo à proposta para fins de identificação.

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

Em seguida, configure uma política e mapeie a proposta criada anteriormente nessa política.

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

Defina um crypto keyring a ser usado durante a autenticação IKE. Este keyring contém as credenciais de autenticação necessárias.

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

Configure um perfil IKEv2 que atue como um repositório para parâmetros não negociáveis do SA IKE. Isso inclui identidades locais ou remotas, métodos de autenticação e serviços disponíveis para 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
```

Crie um conjunto de transformação e configure-o para operar no modo de túnel.

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

Crie uma ACL para permitir a comunicação apenas com o IP da interface do ISE.

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

Configure um mapa de criptografia da configuração global. Anexe o conjunto de transformação, o perfil IPsec e a ACL ao mapa de criptografia.

```
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, anexe o mapa de criptografia à interface. Neste cenário, a interface de gerenciamento sem fio que transporta o tráfego RADIUS é mapeada dentro da VLAN da interface de gerenciamento.

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

Verificar

WLC

Comandos show disponíveis para verificar o IPSec na 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,

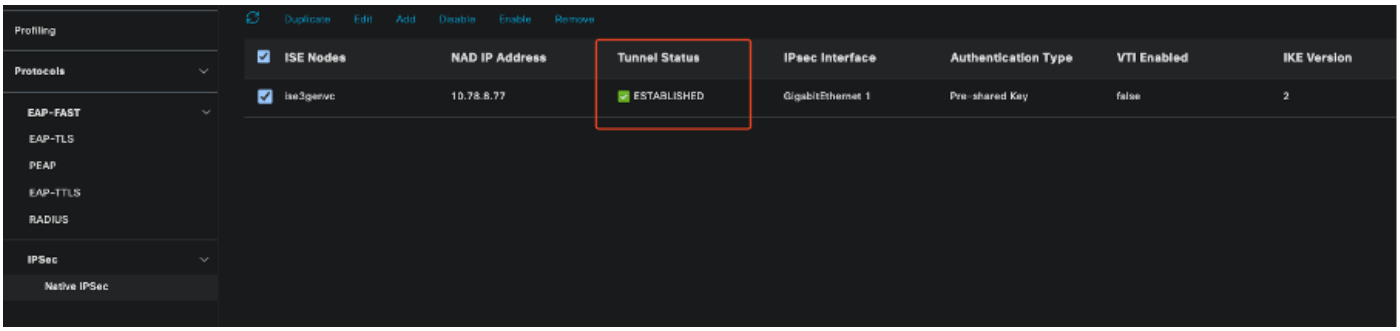
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

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 do ISE mostrando o status do IPSec

Captura do pacote

Use um EPC no WLC para garantir que o tráfego RADIUS do cliente atravesse o túnel ESP. Usando uma captura do plano de controle, você pode observar os pacotes que saem do plano de controle em um estado não criptografado, que são criptografados e transmitidos para a rede com fio.

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)

Pacotes IPSec entre WLC e ISE

Troubleshooting

Depurações de WLC

Como a WLC 9800 opera no Cisco IOS XE, você pode utilizar comandos de depuração IPSec semelhantes aos de outras plataformas Cisco IOS XE. Aqui estão dois comandos-chave úteis para solucionar problemas do IPSec.

- debug crypto ikev2
- debug crypto ikev2 error

depurações do ISE

Use esse comando na CLI do ISE para exibir logs do IPSec. Comandos de depuração não são necessários no WLC.

- show logging application strongswan/charon.log tail

Referências

Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino 17.9.x

Segurança IPsec para comunicação segura entre Cisco ISE e NAD

Configurando o Internet Key Exchange versão 2 (IKEv2)

Configurar o IPsec nativo do ISE 3.3 para comunicação NAD segura (Cisco IOS XE)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.