Configuration du tunnel IPsec entre Cisco WLC et ISE

Table des matières

Introduction

Ce document décrit la configuration IPsec (Internet Protocol Security) entre le WLC 9800 et le serveur ISE pour sécuriser les communications Radius et TACACS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Configuration WLC Cisco IOS® XE
- Concepts généraux d'IPSec
- Concepts généraux de RADIUS
- Concepts généraux de TACACS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur sans fil : C9800-40-K9 exécutant 17.09.04a
- Cisco ISE : Exécution du correctif 4 de la version 3
- Commutateur : 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

IPsec est un cadre de normes ouvertes développé par l'IETF. Elle assure la sécurité de la transmission d'informations sensibles sur des réseaux non protégés tels qu'Internet. IPsec agit au niveau de la couche réseau, protégeant et authentifiant les paquets IP entre les périphériques IPsec participants (homologues), tels que les routeurs Cisco. Utilisez IPsec entre le WLC 9800 et le serveur ISE pour sécuriser les communications RADIUS et TACACS.

Configurer

Diagramme du réseau

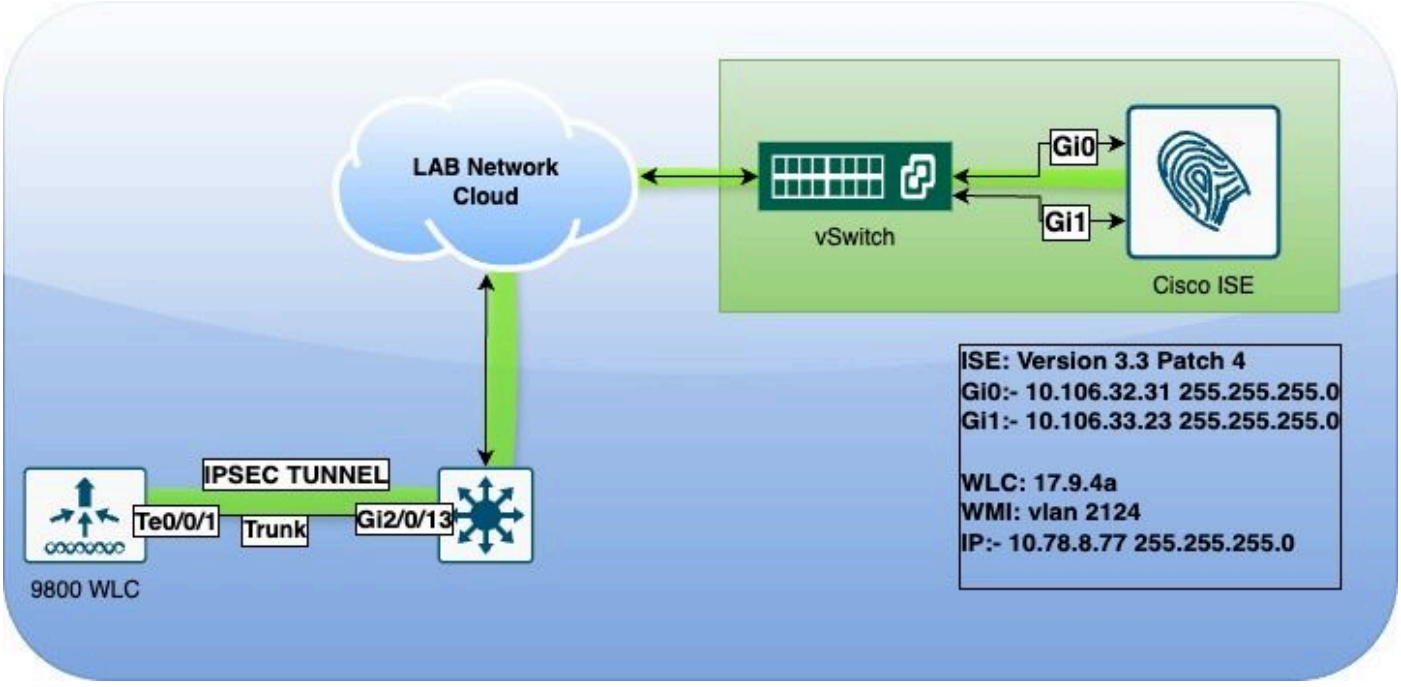


Diagramme du réseau

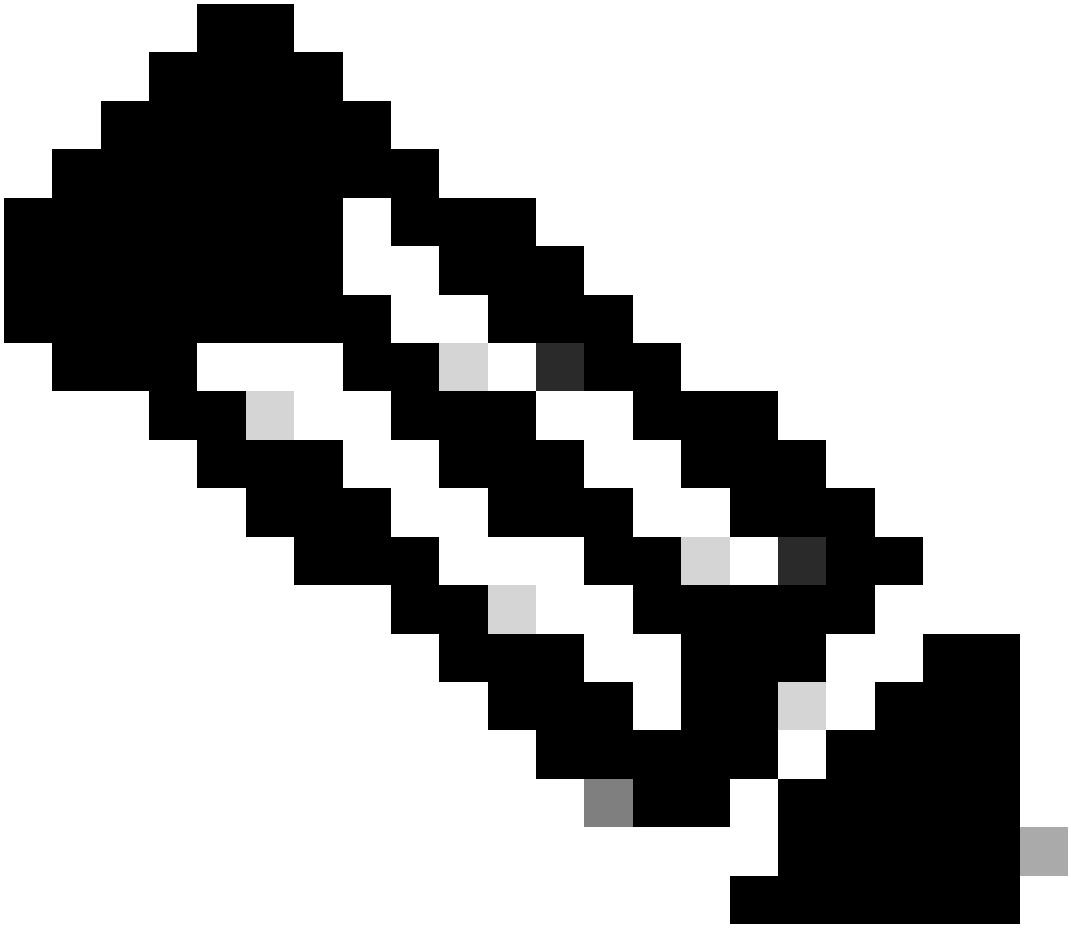
Configuration ISE

Cisco ISE prend en charge IPsec en mode tunnel et transport. Lorsque vous activez IPsec sur une interface Cisco ISE et que vous configurez les homologues, un tunnel IPsec est créé entre Cisco

ISE et le NAD pour sécuriser la communication.

Vous pouvez définir une clé pré-partagée ou utiliser des certificats X.509 pour l'authentification IPsec. IPsec peut être activé sur les interfaces Gigabit Ethernet 1 à Gigabit Ethernet 5.

Cisco ISE versions 2.2 et ultérieures prennent en charge IPsec.



Remarque : Assurez-vous que vous disposez d'une licence Cisco ISE Essentials.

Ajoutez un périphérique d'accès réseau (NAD) avec une adresse IP spécifique dans la fenêtre Périphériques réseau.

Dans l'interface utilisateur graphique de Cisco ISE, passez le curseur sur Administration et naviguez jusqu'à System > Settings > Protocols > IPsec > Native IPsec.

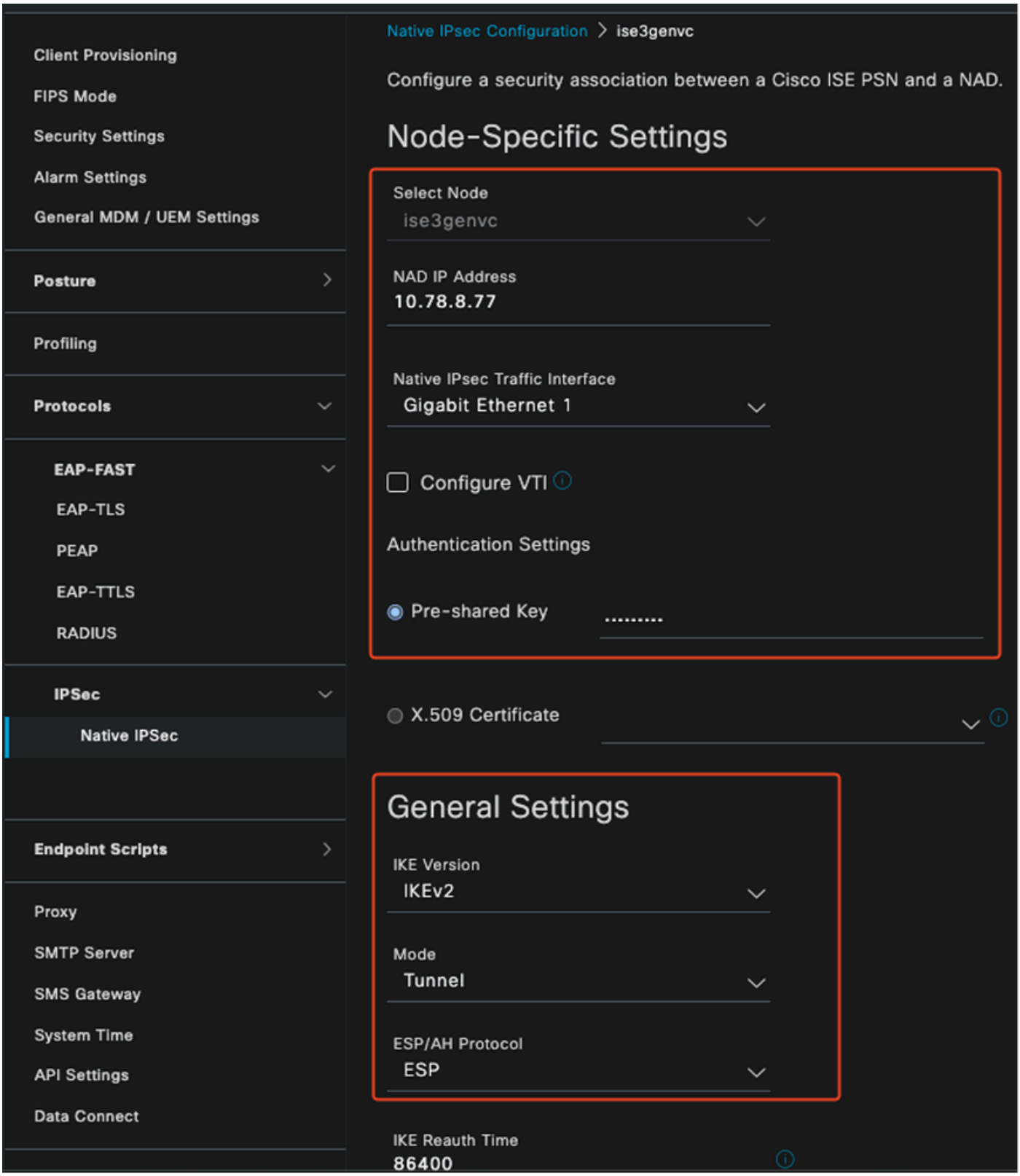
Cliquez sur Add pour configurer une association de sécurité entre un PSN Cisco ISE et un NAD.

- Sélectionnez le noeud.

- Spécifiez l'adresse IP NAD.
- Sélectionnez l'interface de trafic IPsec requise.
- Entrez également la clé pré-partagée à utiliser sur NAD.

Dans la section Général, entrez les détails spécifiés.

- Sélectionnez l'IKEv2.
- Sélectionnez Tunnel mode.
- Sélectionnez ESP comme protocole ESP/AH.



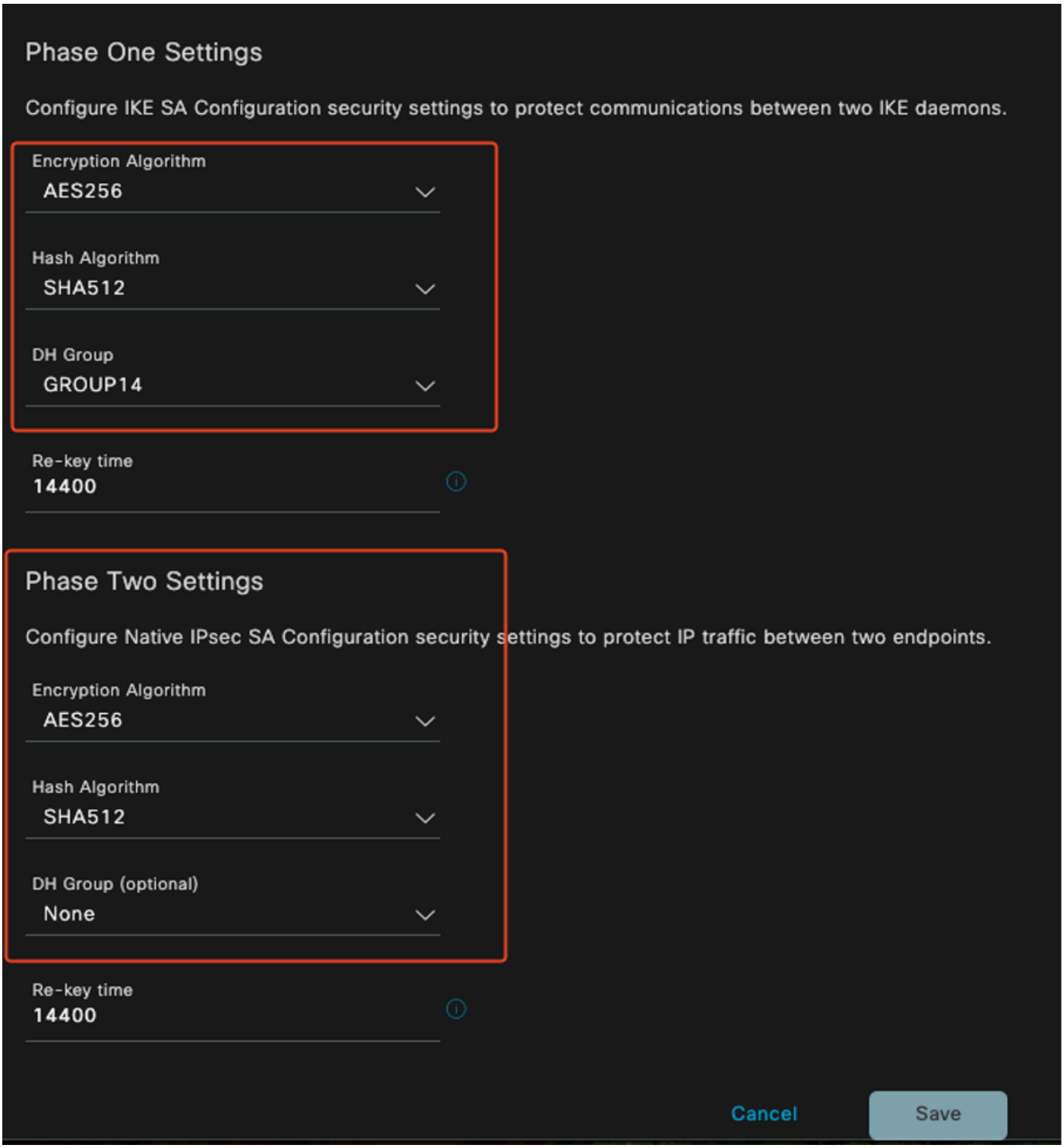
Configuration IPSec native ISE

Dans les paramètres de la phase 1 :

- Sélectionnez AES256 comme algorithme de chiffrement.
- Sélectionnez SHA512 comme a algorithm.
- Sélectionnez GROUP14 comme groupe DH.

Dans les paramètres de la phase 2 :

- Sélectionnez AES256 comme algorithme de chiffrement.
- Sélectionnez SHA512 comme a algorithm.



Configuration IPSec Phase 1 et Phase 2

Configurez une route de l'interface de ligne de commande ISE vers le WLC en utilisant la passerelle eth1 comme tronçon suivant.

<#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
```

Configuration du WLC 9800

La configuration IPSec du WLC 9800 n'étant pas exposée sur l'interface graphique utilisateur, toute la configuration doit être effectuée à partir de l'interface de ligne de commande.

Voici les étapes de configuration du serveur ISE. Chaque étape est accompagnée des commandes CLI appropriées dans cette section pour vous guider.

Étapes de configuration WLC IPSec

Configuration de la proposition IKEv2

Pour commencer la configuration, passez en mode de configuration globale et créez une proposition IKEv2. Attribuer un nom unique à la proposition à des fins d'identification.

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

Configurez ensuite une stratégie et mappez la proposition précédemment créée dans cette stratégie.

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

Définissez un trousseau de chiffrement à utiliser lors de l'authentification IKE. Ce trousseau de chiffrement contient les informations d'identification d'authentification nécessaires.

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

Configurez un profil IKEv2 qui sert de référentiel pour les paramètres non négociables de l'association de sécurité IKE. Cela inclut les identités locales ou distantes, les méthodes d'authentification et les services disponibles pour les homologues authentifiés.

```
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
```

Créez un jeu de transformation et configurez-le pour qu'il fonctionne en mode tunnel.

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

Créez une ACL pour autoriser la communication uniquement vers l'IP de l'interface ISE.

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

Configurez une crypto-carte à partir de la configuration globale. Associez le jeu de transformation, le profil IPsec et la liste de contrôle d'accès à la crypto-carte.

```
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
```

Enfin, associez la crypto-carte à l’interface. Dans ce scénario, l’interface de gestion sans fil transportant le trafic RADIUS est mappée au sein du VLAN de l’interface de gestion.

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

Vérifier

WLC

Commandes show disponibles pour vérifier IPSec sur le 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,
```

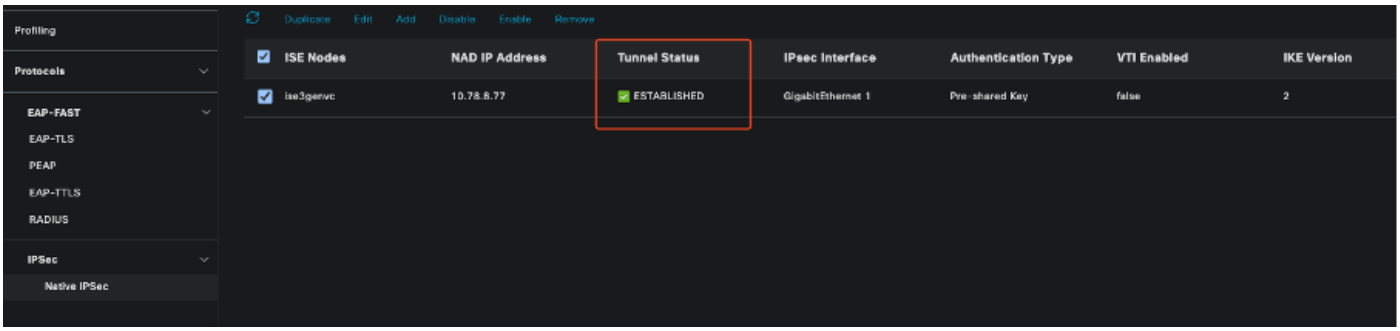
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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.
```



Interface utilisateur graphique ISE affichant l'état IPSec

Capture de paquets

Prenez un EPC sur le WLC pour vous assurer que le trafic RADIUS client traverse le tunnel ESP. En utilisant une capture de plan de contrôle, vous pouvez observer les paquets quittant le plan de contrôle dans un état non chiffré, qui sont ensuite chiffrés et transmis sur le réseau câblé.

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)

Paquets IPSec entre WLC et ISE

Dépannage

Débogages WLC

Puisque le WLC 9800 fonctionne sur Cisco IOS XE, vous pouvez utiliser des commandes de débogage IPSec similaires à celles des autres plates-formes Cisco IOS XE. Voici deux commandes clés qui sont utiles pour le dépannage des problèmes IPSec.

- debug crypto ikev2
- debug crypto ikev2 error

Débogages ISE

Utilisez cette commande sur l'ILC ISE pour afficher les journaux IPSec. Les commandes de

débogage ne sont pas nécessaires sur le WLC.

- show logging application strongswan/charon.log tail

Références

Guide de configuration du logiciel du contrôleur sans fil Cisco Catalyst 9800, Cisco IOS XE Cupertino 17.9.x

Sécurité IPsec pour sécuriser la communication entre Cisco ISE et NAD

Configuration d'IKEv2 (Internet Key Exchange Version 2)

Configuration d'ISE 3.3 Native IPsec pour sécuriser la communication NAD (Cisco IOS XE)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.