IPsec-tunnel configureren tussen Cisco WLC en ISE

Inhoud

Inleiding

Dit document beschrijft de IPsec-configuratie (Internet Protocol Security) tussen de 9800 WLC- en ISE-server om de RADIUS- en TACACS-communicatie te beveiligen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Cisco IOS® XE WLC-configuratie
- Algemene IPsec-concepten
- Algemene RADIUS-concepten
- Algemene TACACS-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze controller: C9800-40-K9 met 17.09.04a
- Cisco ISE-lijnkaart: Patch 4 uitvoeren, versie 3
- Switch: NCS 920-L-24P

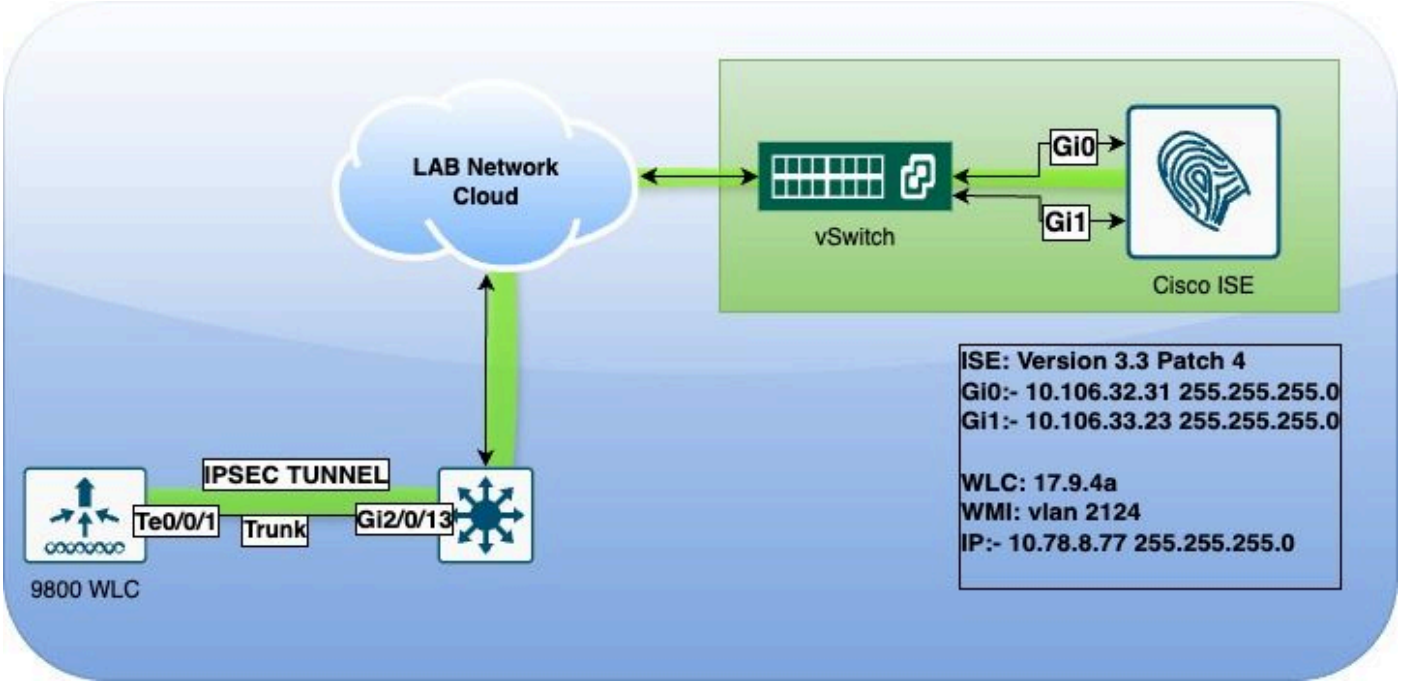
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

IPsec vormt een kader van open standaarden die door de IETF zijn ontwikkeld. Het biedt beveiliging voor de overdracht van gevoelige informatie via onbeschermde netwerken zoals het internet. IPsec treedt op op de netwerklaag en beschermt en verifieert IP-pakketten tussen deelnemende IPsec-apparaten (peers), zoals Cisco-routers. Gebruik IPsec tussen de 9800 WLC en de ISE-server om de RADIUS- en TACACS-communicatie te beveiligen.

Configureren

Netwerkdiagram



Netwerkdiagram

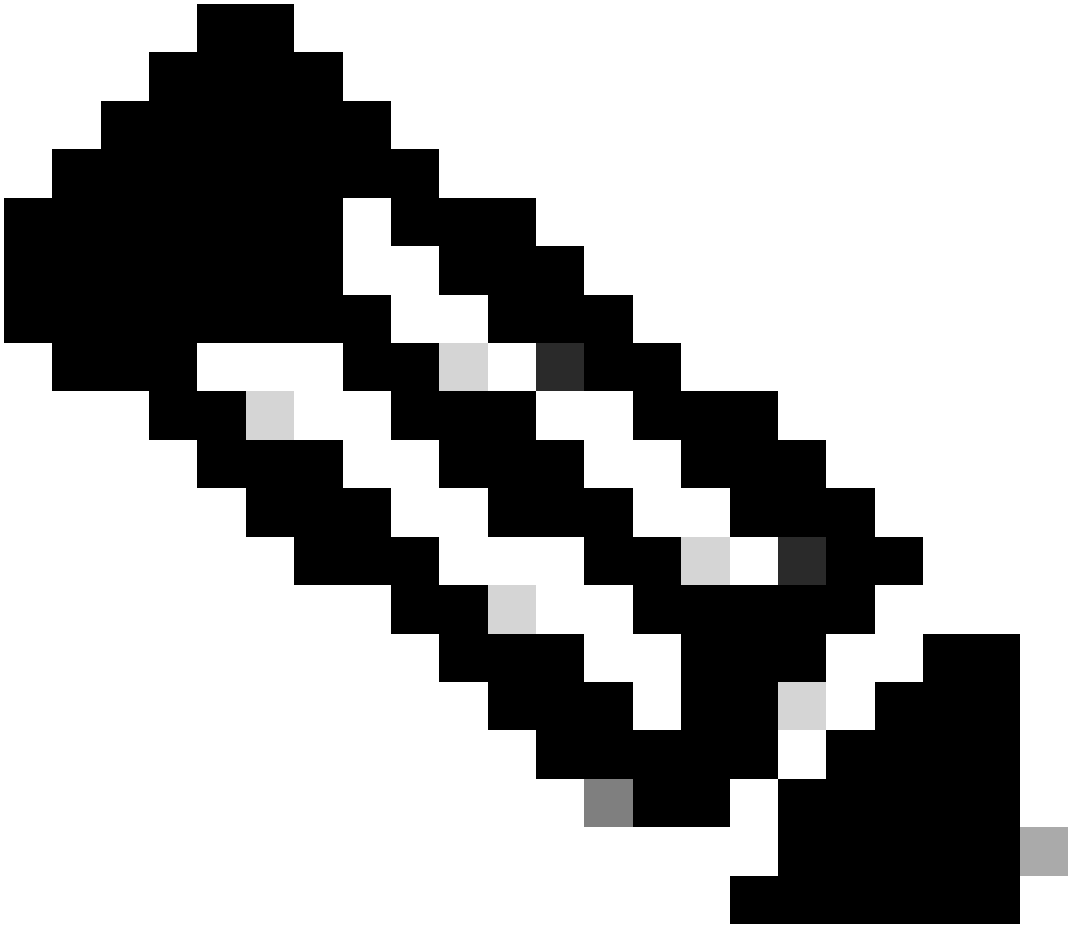
ISE-configuratie

Cisco ISE ondersteunt IPsec in tunnel- en transportmodi. Wanneer u IPsec op een Cisco ISE-interface inschakelt en de peers configureert, wordt er een IPsec-tunnel gemaakt tussen Cisco

ISE en de NAD om de communicatie te beveiligen.

U kunt een vooraf gedeelde sleutel definiëren of X.509-certificaten gebruiken voor IPsec-verificatie. IPsec kan worden ingeschakeld op Gigabit Ethernet 1 met Gigabit Ethernet 5-interfaces.

Cisco ISE-softwarereleases 2.2 en hoger ondersteunen IPsec.



Opmerking: Zorg ervoor dat u een Cisco ISE Essentials-licentie hebt.

Voeg een netwerktoegangsapparaat (NAD) toe met een specifiek IP-adres in het venster Netwerkapparaten.

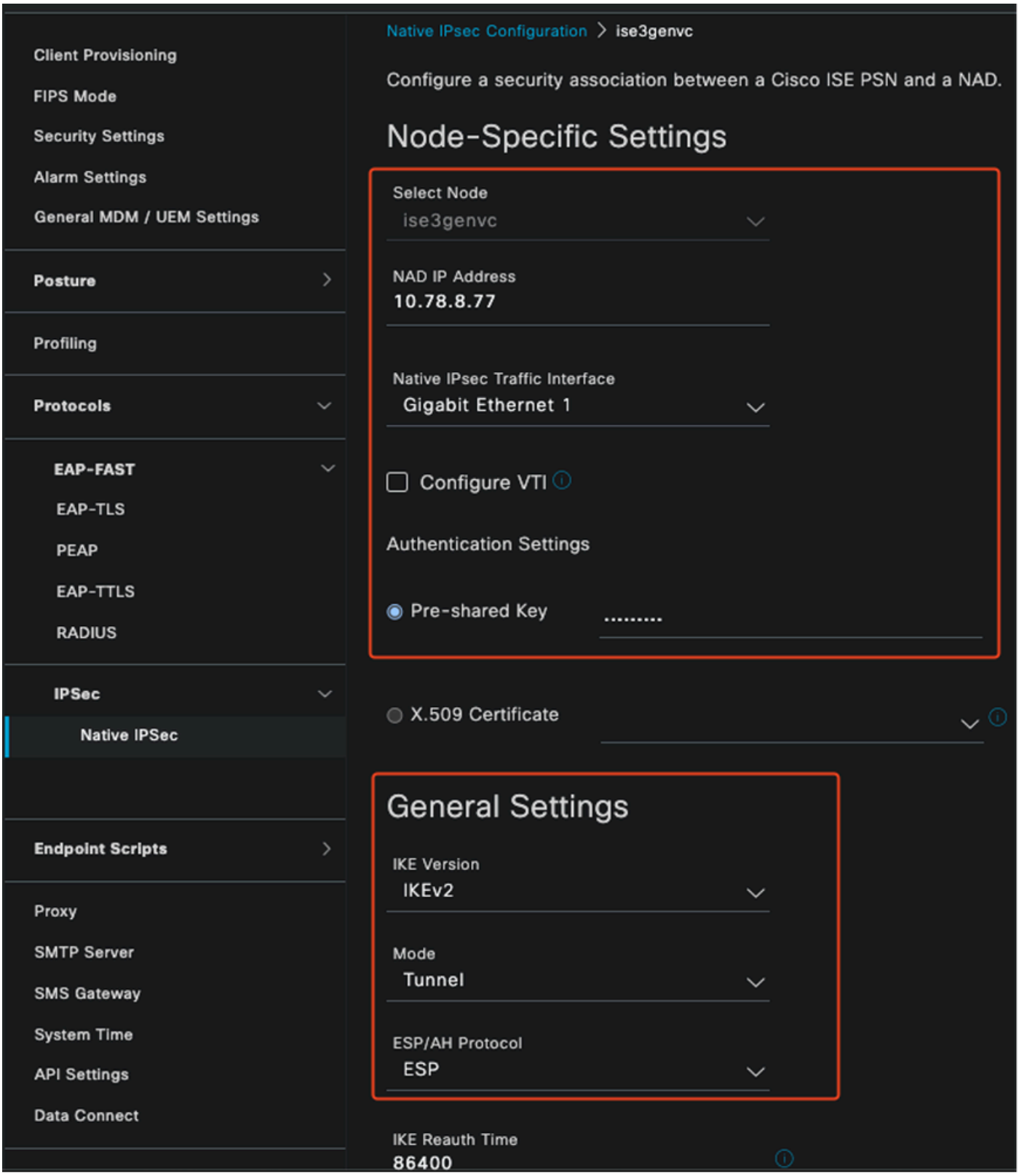
In de Cisco ISE GUI, zweef via Beheer en navigeer naar Systeem > Instellingen > Protocollen > IPsec > Native IPsec.

Klik op Add om een beveiligingskoppeling te configureren tussen een Cisco ISE-netwerkmodule en een netwerkmodule.

- Selecteer het knooppunt.
- Geef het NAD IP-adres op.
- Kies de gewenste IPsec-verkeersinterface.
- Voer ook de vooraf gedeelde sleutel in die op NAD moet worden gebruikt.

Voer in het vak Algemeen de opgegeven gegevens in.

- Kies de IKEv2.
- Selecteer de modus Tunnel.
- Selecteer ESP als het ESP/AH-protocol.



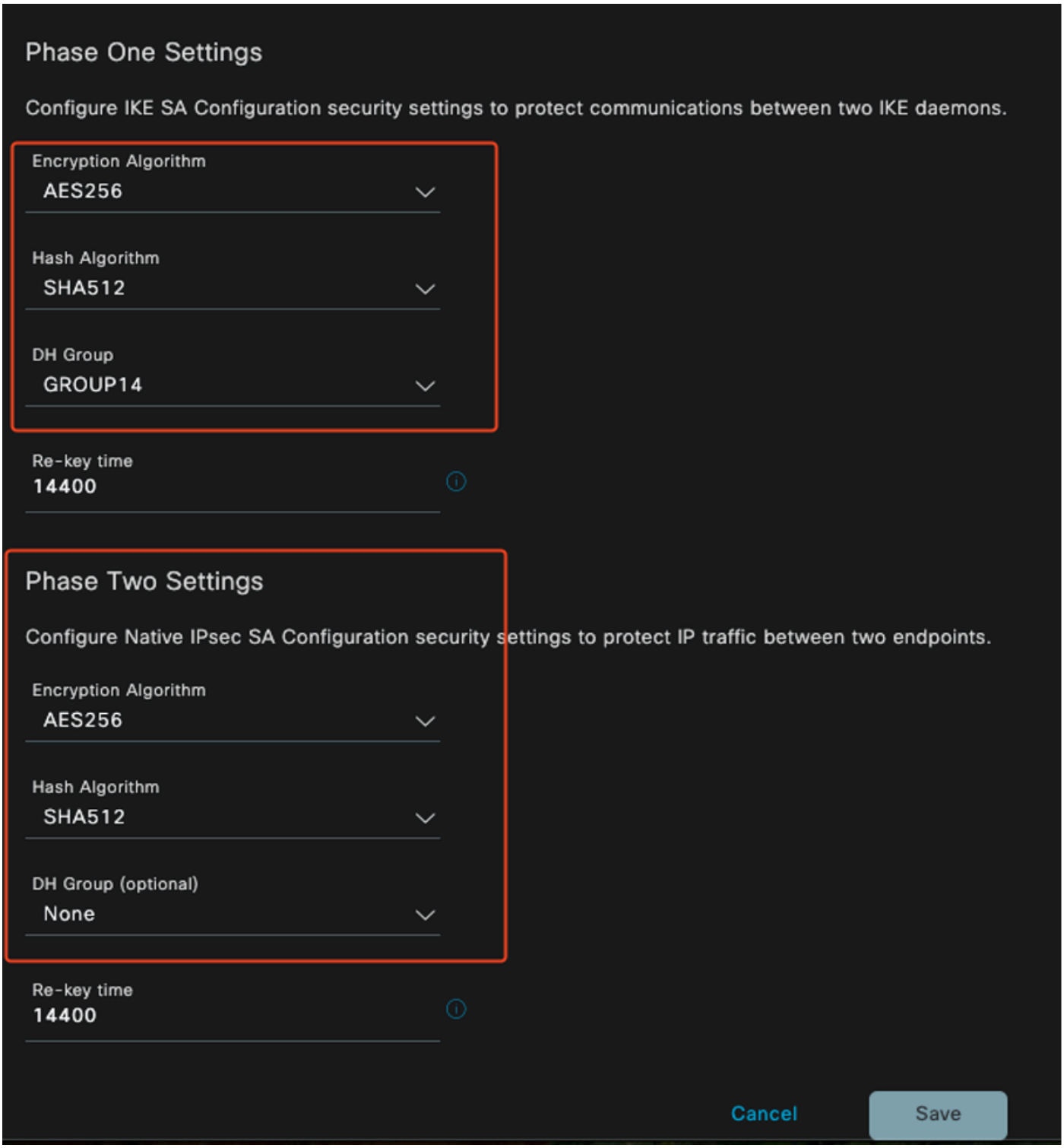
ISE-native IPSec-configuratie

In fase één-instellingen:

- Kies AES256 als encryptie-algoritme.
- Selecteer SHA512 zoals algoritme heeft.
- Selecteer GROUP14 als DH-groep.

In fase twee instellingen:

- Kies AES256 als encryptie-algoritme.
- Selecteer SHA512 zoals algoritme heeft.



Configuratie van IPSec fase 1 en fase 2

Configureer een route van de ISE CLI naar de WLC met behulp van de eth1 gateway als de volgende hop.

<#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
```

Configuratie 9800 WLC

De IPSec-configuratie van de 9800 WLC wordt niet blootgesteld op de GUI, dus moet alle configuratie worden uitgevoerd vanuit de CLI.

Hier volgen de configuratiestappen voor de ISE-server. Elke stap wordt begeleid door relevante CLI-opdrachten in deze sectie.

Configuratiestappen WLC IPSec

Configuratie IKEv2-voorstel

Als u met de configuratie wilt beginnen, voert u de globale configuratiemodus in en maakt u een IKEv2-voorstel. Een unieke naam aan het voorstel toewijzen ter identificatie.

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

Daarna, vorm een beleid en breng het eerder gecreëerde voorstel binnen dit beleid in kaart.

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

Bepaal een crypto-sleutelring die tijdens IKE-verificatie moet worden gebruikt. Deze sleutelring bevat de benodigde verificatiereferenties.

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

Configureer een IKEv2-profiel dat fungeert als een opslagplaats voor niet-verhandelbare parameters van IKE SA. Dit omvat lokale of externe identiteiten, verificatiemethoden en beschikbare services voor geverifieerde peers.

```
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
```

Maak een transformatieset en configureer deze om in tunnelmodus te werken.

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

Maak een ACL om alleen communicatie met de ISE-interface IP toe te staan.

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

Configureer een cryptokaart vanuit de algemene configuratie. Hang de transformatieset, het IPsec-profiel en ACL op de cryptokaart.

```
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
```

Tot slot, maak de crypto kaart aan de interface vast. In dit scenario, wordt de Draadloze beheersinterface die het verkeer van RADIUS draagt in kaart gebracht binnen de beheersinterface VLAN.

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

Verifiëren

WLC

Beschikbare showopdrachten om IPSec op 9800 WLC te verifiëren.

- IP-toegangslijsten tonen
- cryptokaart weergeven
- crypto ikev2 tonen als gedetailleerd
- crypto ipsec als detail tonen

<#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,

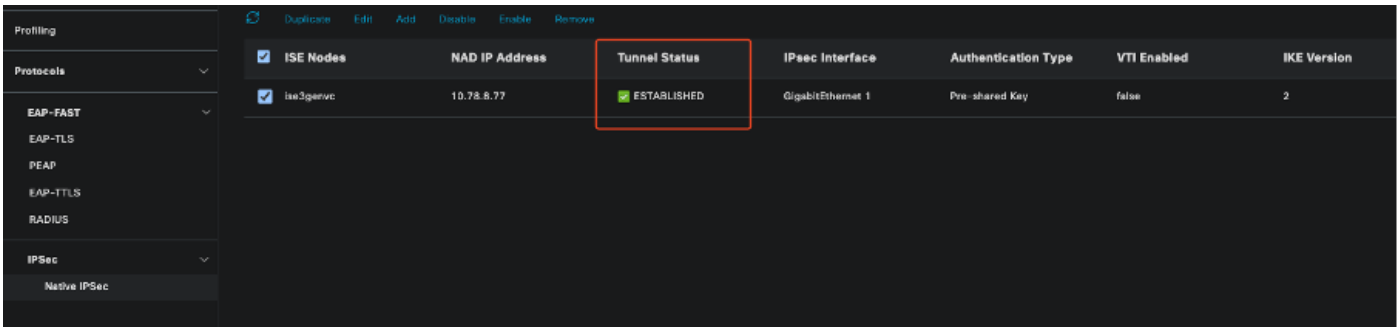
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

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.



ISE GUI met IPSec-status

PacketCapture

Neem een EPC op de WLC om er zeker van te zijn dat client RADIUS-verkeer door de ESP-tunnel gaat. Met behulp van een besturingsplane opname kunt u pakketten waarnemen die het besturingsplane verlaten in een niet-versleutelde staat, die vervolgens versleuteld en verzonden worden naar het bekabelde netwerk.

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)

IPsec-pakketten tussen WLC en ISE

Problemen oplossen

WLC-debugs

Aangezien de 9800 WLC op Cisco IOS XE werkt, kunt u debug-opdrachten van IPSec gebruiken die vergelijkbaar zijn met die op andere Cisco IOS XE-platforms. Hier zijn twee belangrijke opdrachten die handig zijn voor het oplossen van IPSec-problemen.

- debug crypto ikev2
- debug crypto ikev2 error

ISE-debugs

Gebruik deze opdracht op de ISE-CLI om IPSec-logbestanden te bekijken. Debugging commando's zijn niet nodig op de WLC.

- logboektoepassing tonen strongswan/charon.log tail

Referenties

Software voor Cisco Catalyst 9800 Series softwareconfiguratiehandleiding voor draadloze controllers, Cisco IOS XE Nexus 17.9.x

IPsec-beveiliging voor beveiligde communicatie tussen Cisco ISE en NAD

Internet Key Exchange versie 2 configureren (IKEv2)

Configuratie van ISE 3.3 Native IPsec voor beveiligde en beveiligde communicatie (Cisco IOS XE)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.