Konfigurieren von IPsec-Tunnel zwischen Cisco WLC und ISE

Inhalt

Einleitung

In diesem Dokument wird die IPsec-Konfiguration (Internet Protocol Security) zwischen dem 9800 WLC und dem ISE-Server zum Schutz der Radius- und TACACS-Kommunikation beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE
- Cisco IOS® XE WLC-Konfiguration
- Allgemeine IPSec-Konzepte
- Allgemeine RADIUS-Konzepte
- Allgemeine TACACS-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless-Controller: C9800-40-K9 mit 17.09.04a
- Cisco ISE: Ausführung von Version 3 Patch 4
- Switch: 9200-L-24P

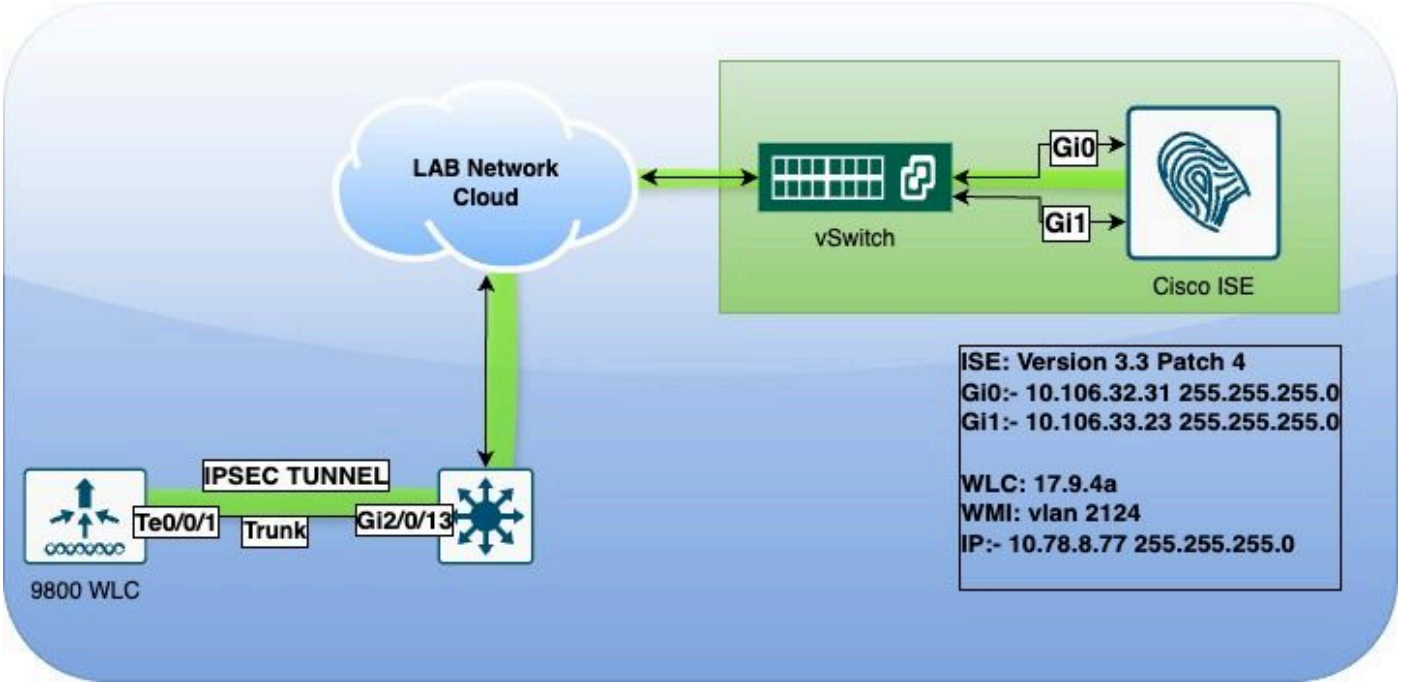
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

IPsec ist ein Framework offener Standards, das von der IETF entwickelt wurde. Es bietet Sicherheit für die Übertragung sensibler Informationen über ungeschützte Netzwerke wie das Internet. IPsec agiert auf der Netzwerkebene und schützt und authentifiziert IP-Pakete zwischen teilnehmenden IPsec-Geräten (Peers), z. B. Cisco Routern. Verwenden Sie IPsec zwischen dem 9800 WLC und dem ISE-Server, um die RADIUS- und TACACS-Kommunikation zu sichern.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

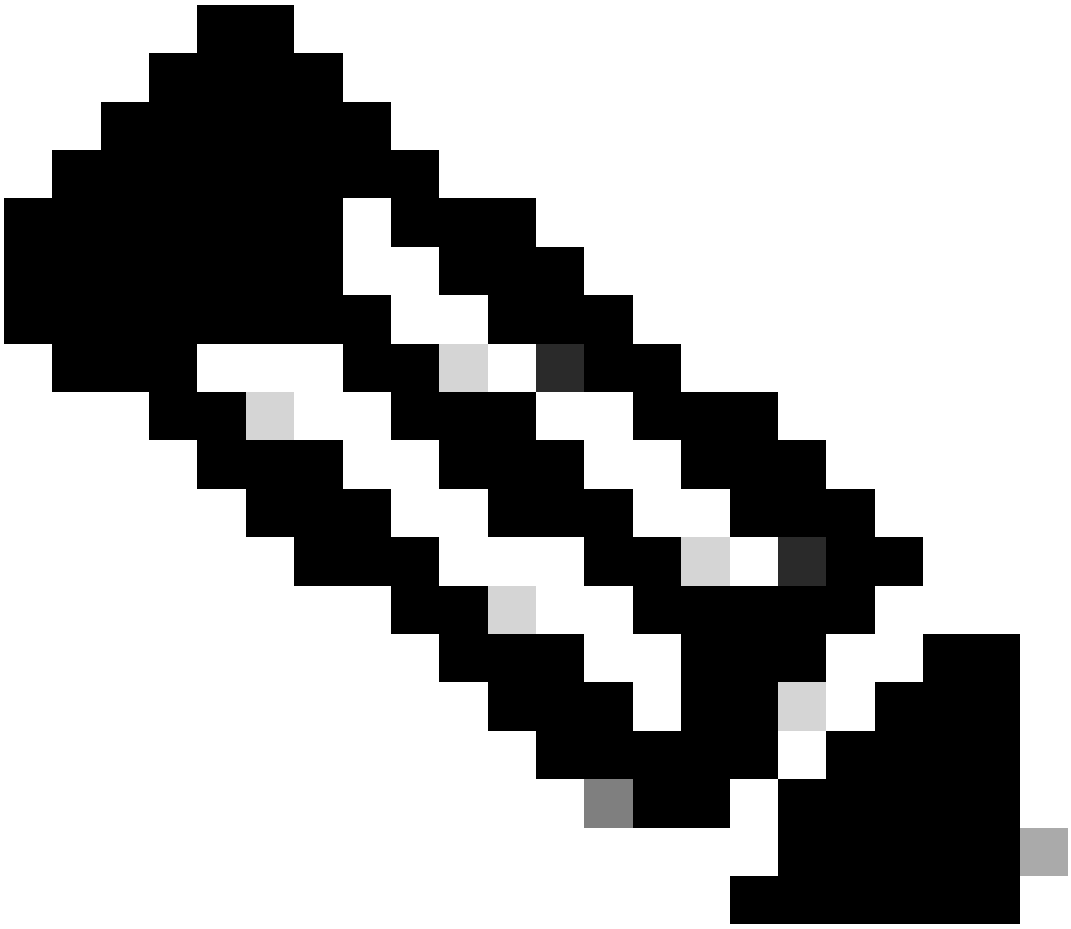
ISE-Konfiguration

Die Cisco ISE unterstützt IPsec im Tunnel- und Transportmodus. Wenn Sie IPsec auf einer Cisco

ISE-Schnittstelle aktivieren und die Peers konfigurieren, wird ein IPsec-Tunnel zwischen Cisco ISE und NAD erstellt, um die Kommunikation zu sichern.

Sie können einen vorinstallierten Schlüssel definieren oder X.509-Zertifikate für die IPsec-Authentifizierung verwenden. IPsec kann auf Gigabit Ethernet 1- bis Gigabit Ethernet 5-Schnittstellen aktiviert werden.

Cisco ISE-Versionen 2.2 und höher unterstützen IPsec.



Anmerkung: Stellen Sie sicher, dass Sie über eine Cisco ISE Essentials-Lizenz verfügen.

Fügen Sie im Fenster Netzwerkgeräte ein Netzwerkzugriffsgerät (Network Access Device, NAD) mit einer bestimmten IP-Adresse hinzu.

Bewegen Sie den Mauszeiger in der Cisco ISE-GUI über Administration, und navigieren Sie zu System > Settings > Protocols > IPsec > Native IPsec.

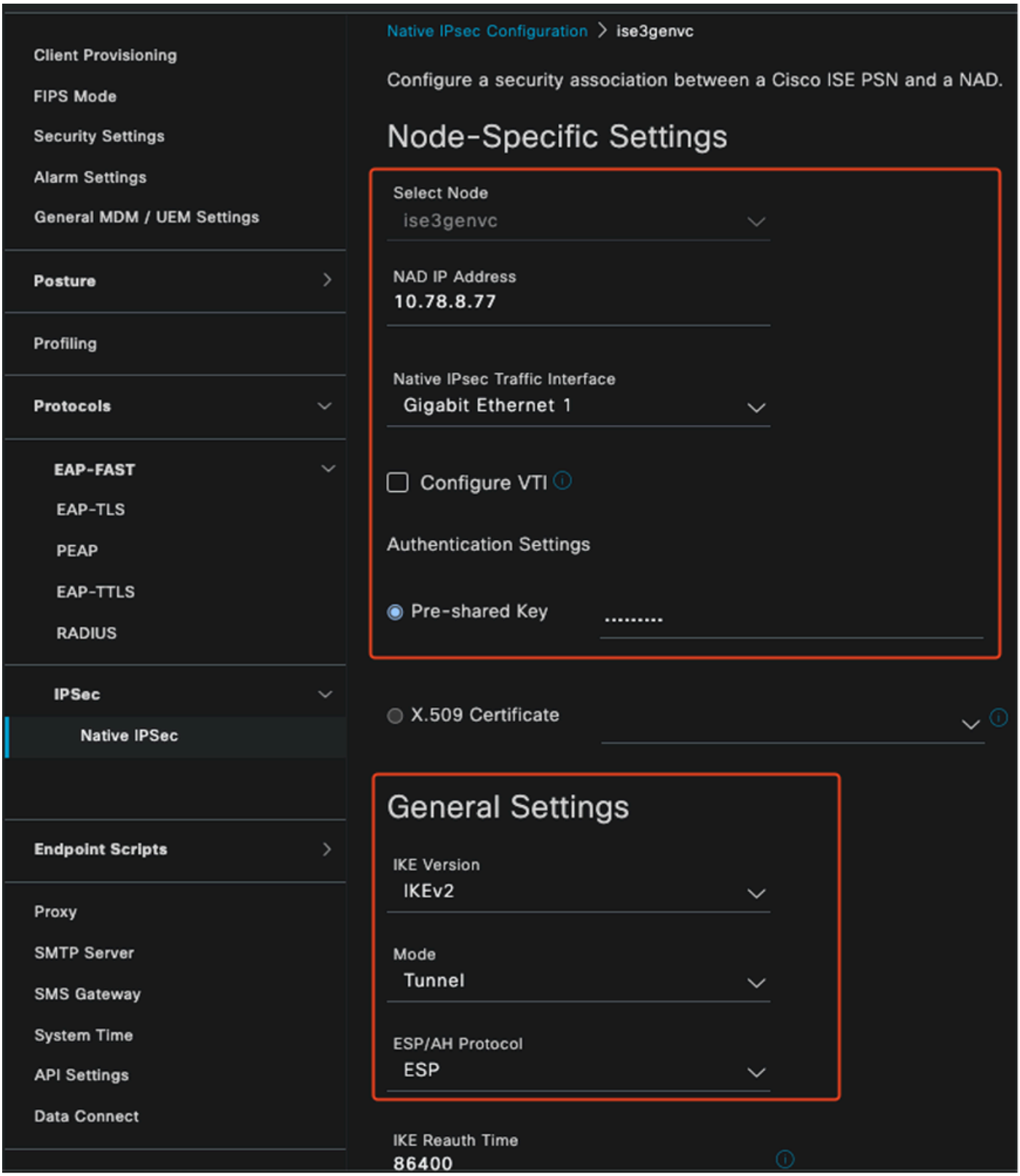
Klicken Sie auf Hinzufügen, um eine Sicherheitszuordnung zwischen einem Cisco ISE PSN und

einem NAD zu konfigurieren.

- Wählen Sie den Knoten aus.
- Geben Sie die NAD-IP-Adresse an.
- Wählen Sie die erforderliche IPsec-Datenverkehrsschnittstelle aus.
- Geben Sie den vorinstallierten Schlüssel ein, der auch für NAD verwendet werden soll.

Geben Sie im Abschnitt "Allgemein" die angegebenen Details ein.

- Wählen Sie IKEv2 aus.
- Wählen Sie den Tunnel-Modus aus.
- Wählen Sie ESP als ESP/AH-Protokoll aus.



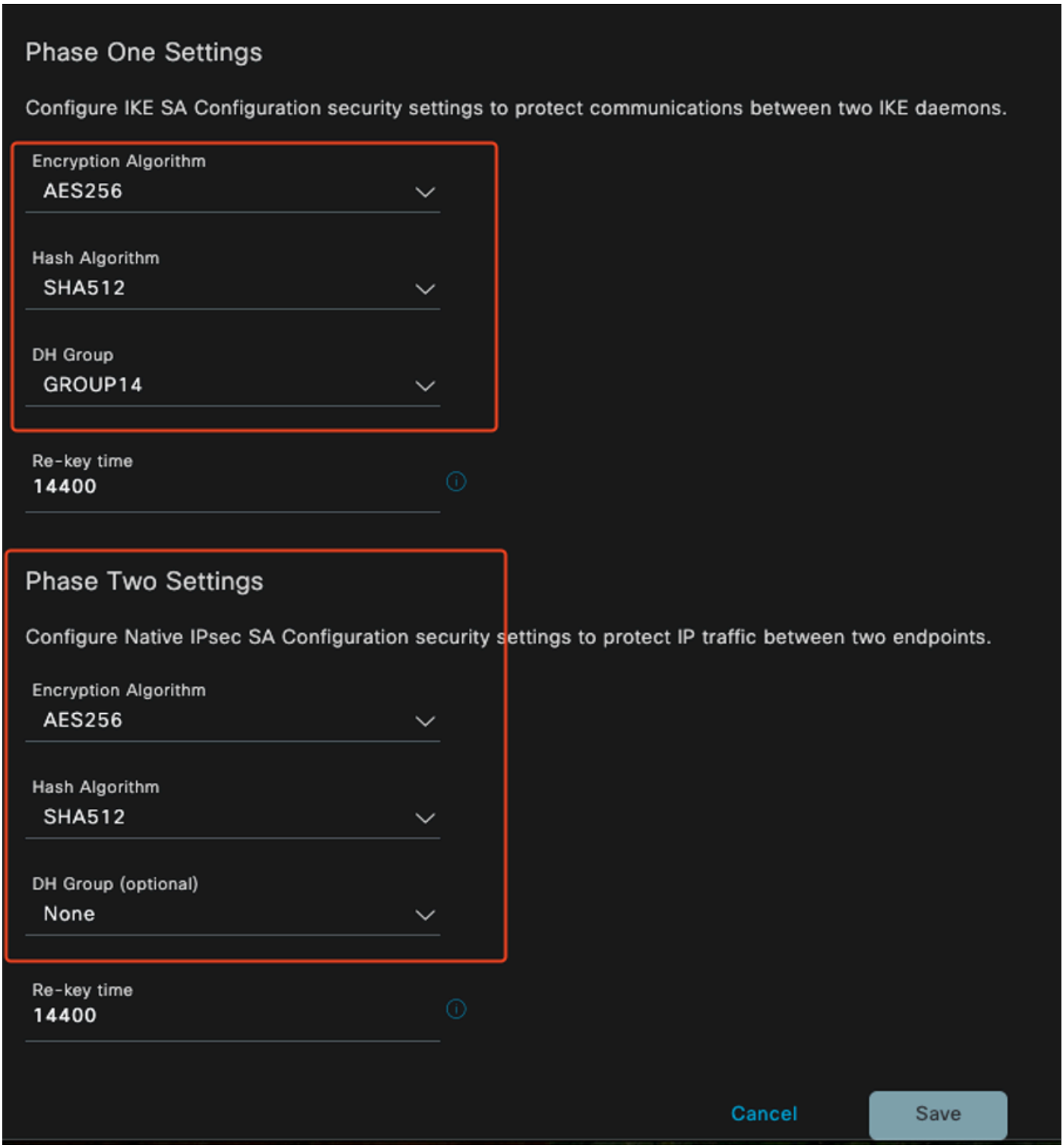
ISE Native IPSec-Konfiguration

In Phase 1:

- Wählen Sie AES256 als Verschlüsselungsalgorithmus aus.
- Wählen Sie SHA512 als vorhandenen Algorithmus aus.
- Wählen Sie GROUP14 als DH-Gruppe aus.

In Phase 2:

- Wählen Sie AES256 als Verschlüsselungsalgorithmus aus.
- Wählen Sie SHA512 als vorhandenen Algorithmus aus.



Konfiguration von IPSec Phase 1 und Phase 2

Konfigurieren Sie eine Route von der ISE-CLI zum WLC, wobei Sie das eth1-Gateway als nächsten Hop verwenden.

<#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-Konfiguration

Die IPSec-Konfiguration des 9800 WLC ist in der GUI nicht verfügbar, daher muss die gesamte Konfiguration über die CLI erfolgen.

Nachfolgend finden Sie die Konfigurationsschritte für den ISE-Server. Jedem Schritt werden in diesem Abschnitt relevante CLI-Befehle beigefügt.

WLC IPSec-Konfigurationsschritte

IKEv2-Angebotskonfiguration

Um mit der Konfiguration zu beginnen, wechseln Sie in den globalen Konfigurationsmodus, und erstellen Sie ein IKEv2-Angebot. Weisen Sie dem Angebot zur Identifizierung einen eindeutigen

Namen zu.

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

Konfigurieren Sie anschließend eine Richtlinie, und ordnen Sie dem zuvor in dieser Richtlinie erstellten Angebot zu.

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

Definieren Sie einen Krypto-Keyring, der während der IKE-Authentifizierung verwendet werden soll. Dieser Keyring enthält die erforderlichen Authentifizierungsdaten.

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

Konfigurieren Sie ein IKEv2-Profil, das als Repository für nicht übertragbare Parameter der IKE-SA fungiert. Dies umfasst lokale oder Remote-Identitäten, Authentifizierungsmethoden und verfügbare Dienste für authentifizierte 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
```

Erstellen Sie einen Transformationssatz, und konfigurieren Sie ihn für den Betrieb im Tunnelmodus.

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

```
exit
```

Erstellen Sie eine ACL, um nur die Kommunikation mit der ISE-Schnittstellen-IP zu ermöglichen.

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

Konfigurieren Sie eine Crypto Map aus der globalen Konfiguration. Verknüpfen Sie Transformationssatz, IPsec-Profil und ACL mit der Crypto Map.

```
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
```

Schließen Sie die Crypto Map an die Schnittstelle an. In diesem Szenario wird die Wireless-Verwaltungsschnittstelle, die den RADIUS-Datenverkehr überträgt, innerhalb der Verwaltungsschnittstelle VLAN zugeordnet.

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

Überprüfung

WLC

Verfügbare show-Befehle zum Überprüfen von IPSec auf dem 9800 WLC.

- IP-Zugriffslisten anzeigen
- Crypto Map anzeigen
- show crypto ikev2 sa detailliert
- 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,
```

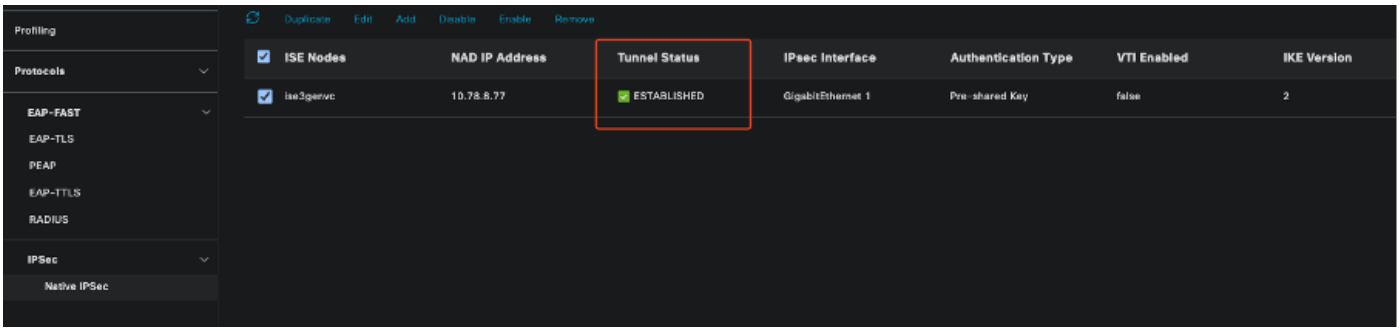
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
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.
```



ISE-GUI mit IPSec-Status

Paketerfassung

Stellen Sie mit einem EPC auf dem WLC sicher, dass der RADIUS-Client-Datenverkehr den ESP-Tunnel durchquert. Mithilfe einer Erfassung auf Kontrollebene können Sie Pakete beobachten, die die Kontrollebene unverschlüsselt verlassen, dann verschlüsselt und an das kabelgebundene Netzwerk übertragen werden.

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-Pakete zwischen WLC und ISE

Fehlerbehebung

WLC-Fehlerbehebung

Da der 9800 WLC mit Cisco IOS XE arbeitet, können Sie IPSec-Debug-Befehle verwenden, die denen auf anderen Cisco IOS XE-Plattformen ähneln. Im Folgenden sind zwei wichtige Befehle aufgeführt, die für die Behebung von IPSec-Problemen nützlich sind.

- debuggen crypto ikev2
- debug crypto ikev2 error

ISE-Debugging

Mit diesem Befehl in der ISE-CLI können Sie IPSec-Protokolle anzeigen. Auf dem WLC sind keine Debugging-Befehle erforderlich.

- show logging-Anwendung strongswan/charon.log tail

Referenzen

Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800, Cisco IOS XE Cupertino 17.9.x

IPsec-Sicherheit für sichere Kommunikation zwischen Cisco ISE und NAD

Konfigurieren von Internet Key Exchange Version 2 (IKEv2)

Konfigurieren der nativen IPsec-Verbindung von ISE 3.3 zu Secure NAD (Cisco IOS XE)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.