Cisco WLCとISE間のIPSecトンネルの設定

内容

はじめに

このドキュメントでは、9800 WLCとISEサーバ間でRadiusおよびTACACS通信を保護するためのInternet Protocol Security(IPSec)設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE
- Cisco IOS® XE WLCの設定
- 一般的な IPSec の概念
- 一般的な RADIUS の概念
- 一般的な TACACS の概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ワイヤレスコントローラ：17.09.04aを実行するC9800-40-K9
- Cisco ISE：バージョン3パッチ4の実行
- スイッチ：9200-L-24P

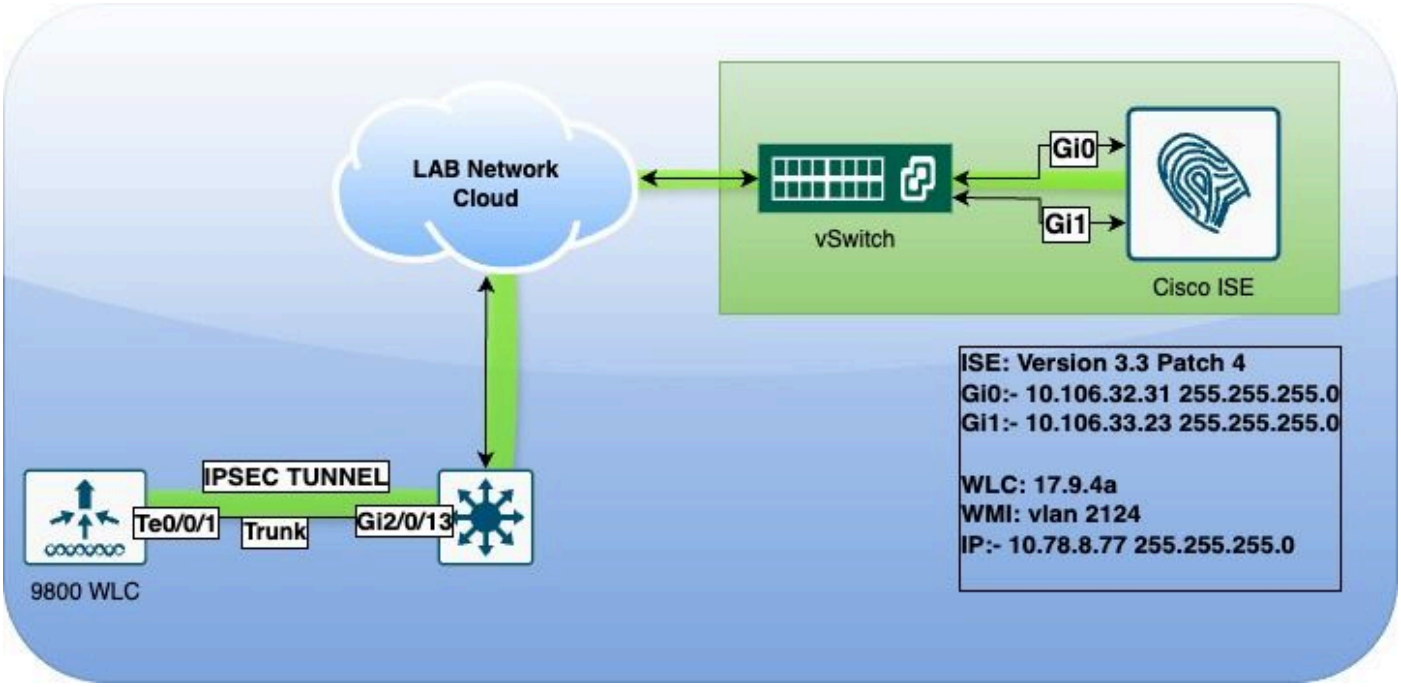
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IPSecは、IETFによって開発されたオープンスタンダードのフレームワークです。インターネットなどの保護されていないネットワークを介して機密情報を送信するためのセキュリティを提供します。IPSecはネットワーク層で動作し、Ciscoルータなどの参加IPSecデバイス（ピア）間のIPパケットを保護および認証します。 9800 WLCとISEサーバ間のIPsecを使用して、RADIUSおよびTACACS通信を保護します。

設定

ネットワーク図



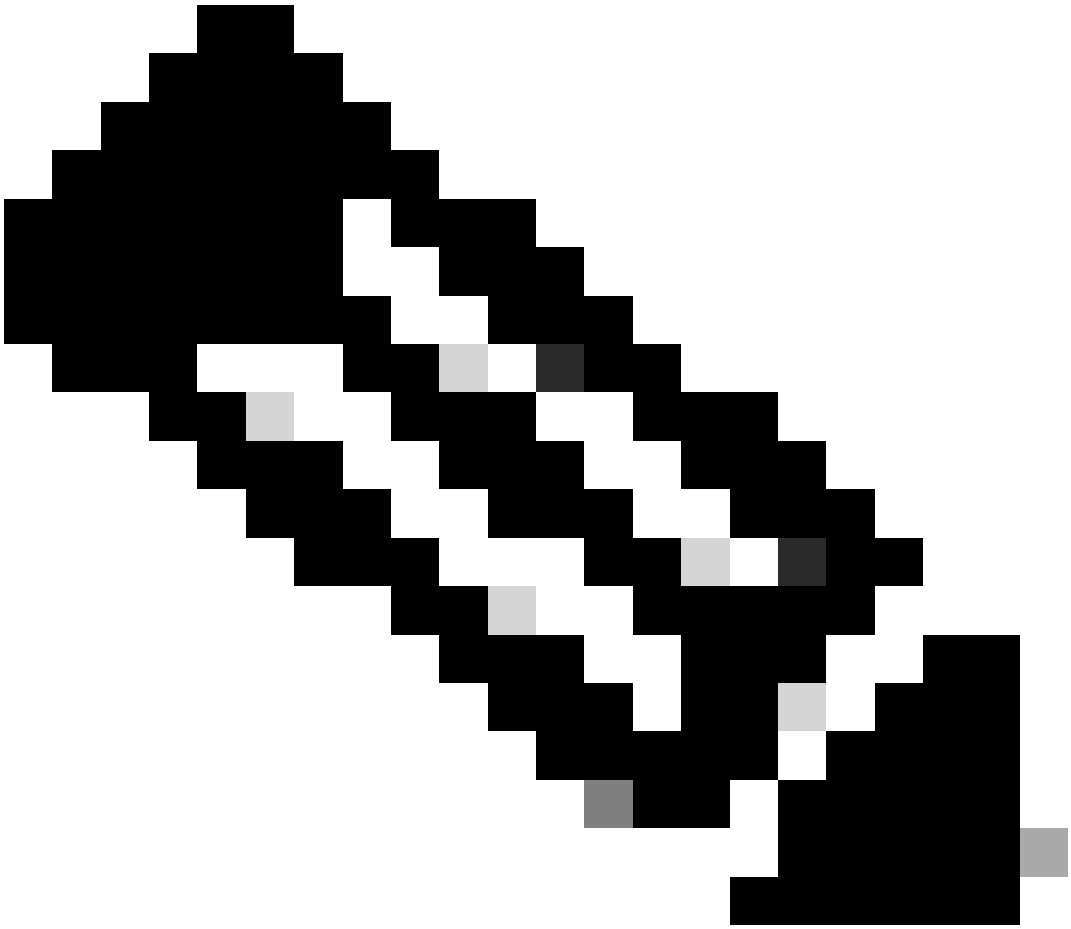
ネットワーク図

ISE 設定

Cisco ISE は、トンネル モードとトランスポート モードで IPSec をサポートします。Cisco ISEインターフェイスでIPsecを有効にしてピアを設定すると、通信を保護するためにCisco ISEとNADの間にIPsecトンネルが作成されます。

事前共有キーを定義するか、IPSec認証にX.509証明書を使用できます。IPsecは、ギガビットイーサネット1 ~ 5のインターフェイスで有効にできます。

Cisco ISEリリース2.2以降では、IPsecがサポートされています。



注:Cisco ISE Essentialsライセンスがあることを確認してください。

Network Devicesウィンドウで、特定のIPアドレスを持つNetwork Access Device（NAD；ネットワークアクセスデバイス）を追加します。

Cisco ISE GUIで、Administrationの上にカーソルを置き、System > Settings > Protocols > IPsec > Native IPsecの順に移動します。

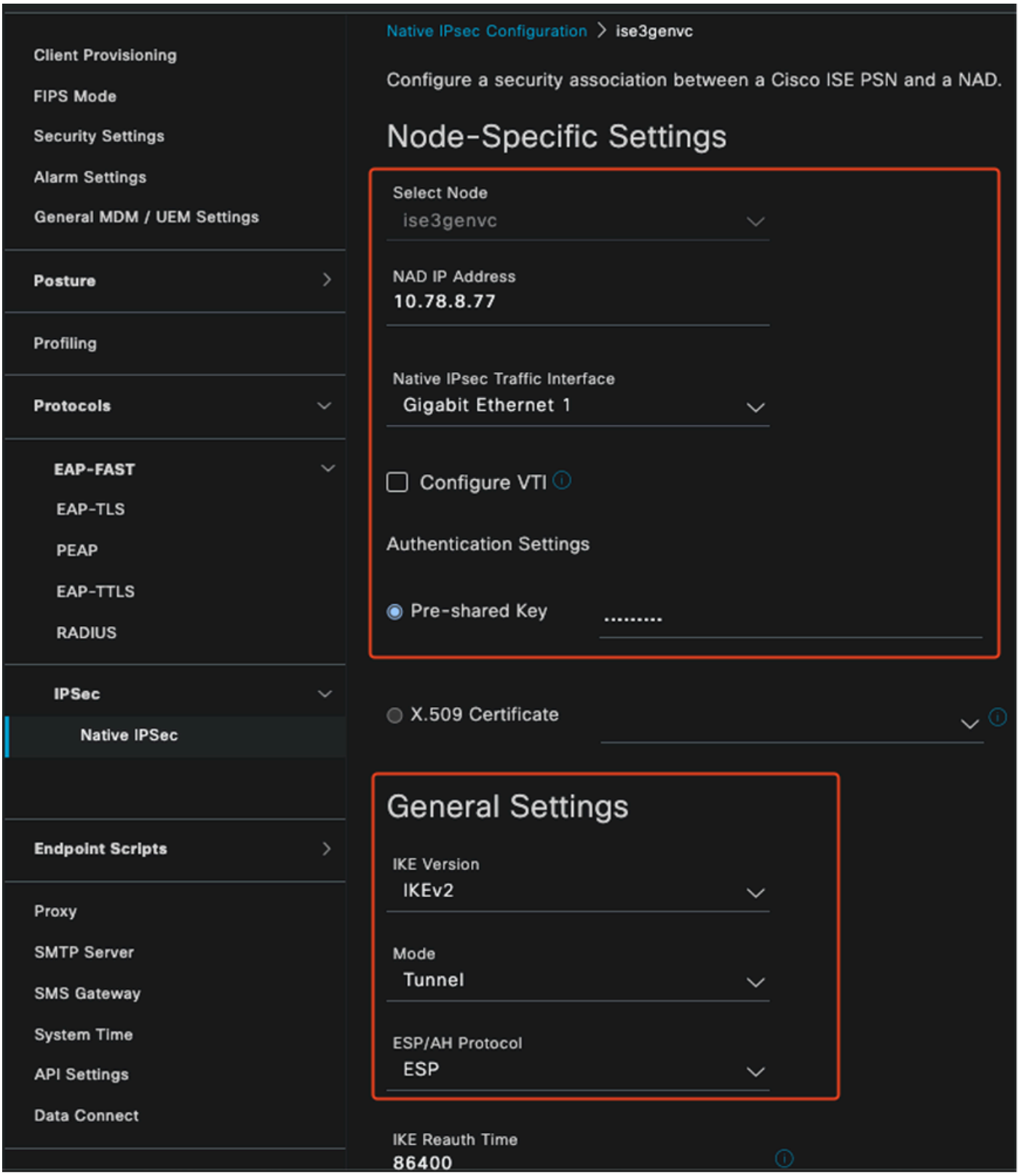
Addをクリックして、Cisco ISE PSNとNADの間のセキュリティアソシエーションを設定します。

- ノードを選択します。
- NAD IPアドレスを指定します。

- 必要なIPSecトラフィックのインターフェイスを選択します。
- NADで使用する事前共有キーも入力します。

[全般]セクションで、指定した詳細情報を入力します。

- IKEv2を選択します。
- Tunnelモードを選択します。
- ESP/AHプロトコルとしてESPを選択します。

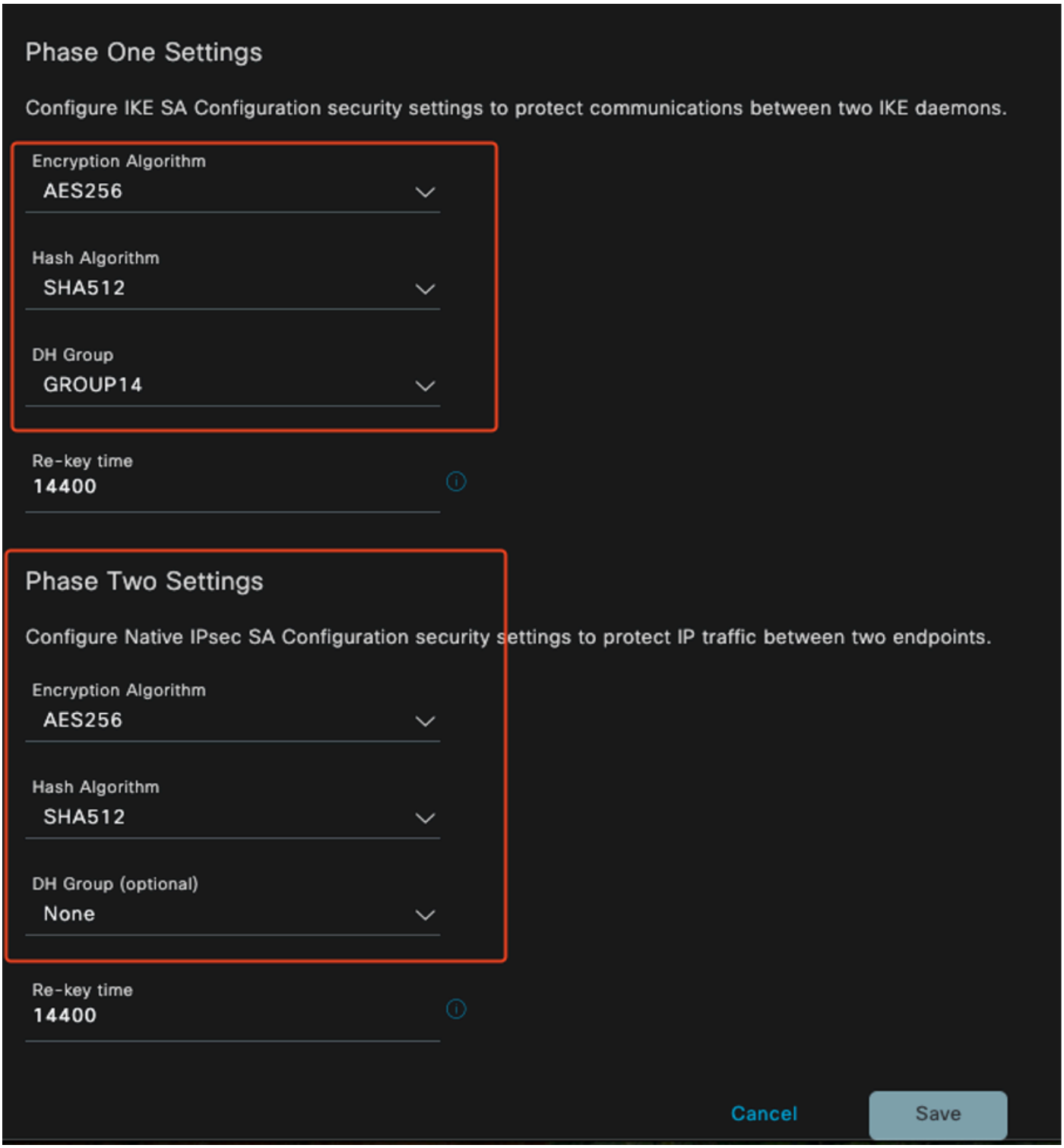


フェーズ1の設定：

- 暗号化アルゴリズムとしてAES256を選択します。
- has algorithmとしてSHA512を選択します。
- DHグループとしてGROUP14を選択します。

フェーズ2の設定：

- 暗号化アルゴリズムとしてAES256を選択します。
- has algorithmとしてSHA512を選択します。



IPSecフェーズ1およびフェーズ2の設定

ネクストホップとしてeth1ゲートウェイを使用して、ISE CLIからWLCへのルートを設定します。

<#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の設定

9800 WLCのIPSec設定はGUIには表示されないため、すべての設定をCLIから行う必要があります。

ISEサーバの設定手順を次に示します。 各ステップには、このセクションで説明する関連CLIコマンドが付属しています。

WLC IPSecの設定手順

IKEv2プロポーザルの設定
設定を開始するには、グローバルコンフィギュレーションモードに入り、IKEv2プロポーザルを作成します。特定の目的で、提案に一意の名前を割り当てます。

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

次に、ポリシーを設定し、以前に作成したプロポーザルをこのポリシー内にマッピングします。

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

IKE認証中に使用される暗号キーリングを定義します。 このキーリングは、必要な認証クレデンシャルを保持します。

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

IKE SAのネゴシエートできないパラメータのリポジトリとして機能するIKEv2プロファイルを設定します。これには、ローカルまたはリモートID、認証方式、認証済みピアで使用可能なサービスが含まれます。

```
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
```

トランスフォームセットを作成して、トンネルモードで動作するように設定します。

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

ISEインターフェイスIPへの通信のみを許可するACLを作成します。

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

グローバルコンフィギュレーションからクリプトマップを設定します。トランスフォームセット、IPsecプロファイル、およびACLをクリプトマップに添付します。

```
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
```

最後に、インターフェイスに暗号マップを添付します。 このシナリオでは、RADIUSトラフィックを伝送するワイヤレス管理インターフェイスは、管理インターフェイスVLAN内でマッピングされます。

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

確認

WLC

9800 WLC上のIPSecを確認するには、showコマンドを使用できます。

- show ip access-lists（隠しコマンド）
- 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,

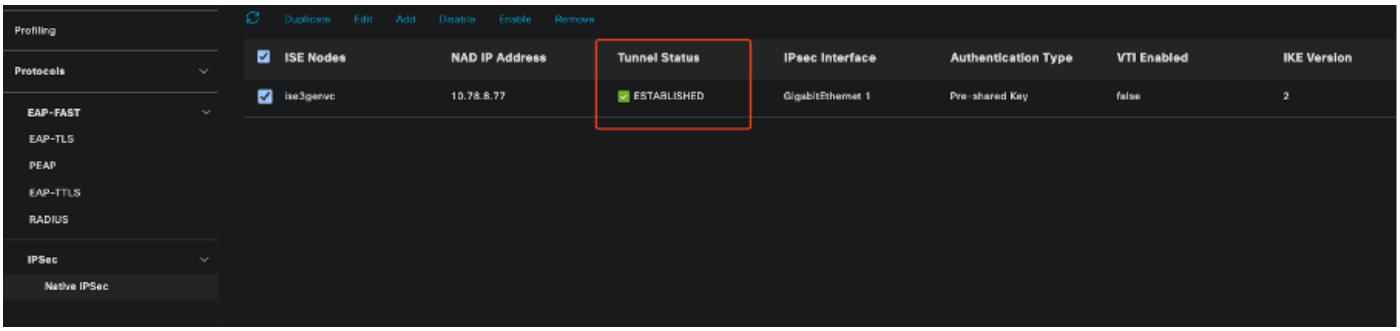
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

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.



IPSecステータスを示すISE GUI

パケット キャプチャ

WLCでEPCを実行し、クライアントRADIUSトラフィックがESPトンネルを通過していることを確認します。コントロールプレーンキャプチャを使用すると、暗号化されていない状態でコントロールプレーンから発信されたパケットを確認できます。その後、パケットは暗号化されて有線ネットワークに送信されます。

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)

WLCとISE間のIPSecパケット

トラブルシュート

WLCのデバッグ

9800 WLCはCisco IOS XEで動作するため、他のCisco IOS XEプラットフォームと同様にIPSec debugコマンドを使用できます。 IPSecに関する問題のトラブルシューティングに役立つ2つの主要なコマンドを次に示します。

- debug crypto ikev2
- debug crypto ikev2 error

ISE デバッグ

IPSecログを表示するには、ISE CLIでこのコマンドを使用します。デバッグコマンドは、WLCでは必要ありません。

- show logging application strongswan/charon.log tail（隠しコマンド）

参考資料

Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS XE Cuppertino 17.9.x

Cisco ISEとNAD間の通信を保護するIPSecセキュリティ

インターネットキーエクスチェンジバージョン2(IKEv2)の設定

NAD(Cisco IOS XE)通信を保護するためのISE 3.3ネイティブIPsecの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。