# Configurazione del tunnel IPsec tra Cisco WLC e ISE

## Sommario



## Introduzione

In questo documento viene descritta la configurazione di Internet Protocol Security (IPsec) tra il protocollo 9800 WLC e il server ISE per proteggere la comunicazione Radius & TACACS.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Configurazione WLC Cisco IOS® XE
- Concetti generali relativi a IPSec
- Concetti generali su RADIUS
- Nozioni generali su TACACS

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller wireless: C9800-40-K9 con 17.09.04a
- Cisco ISE Esecuzione della patch versione 3 4
- Switch: 9200-24P

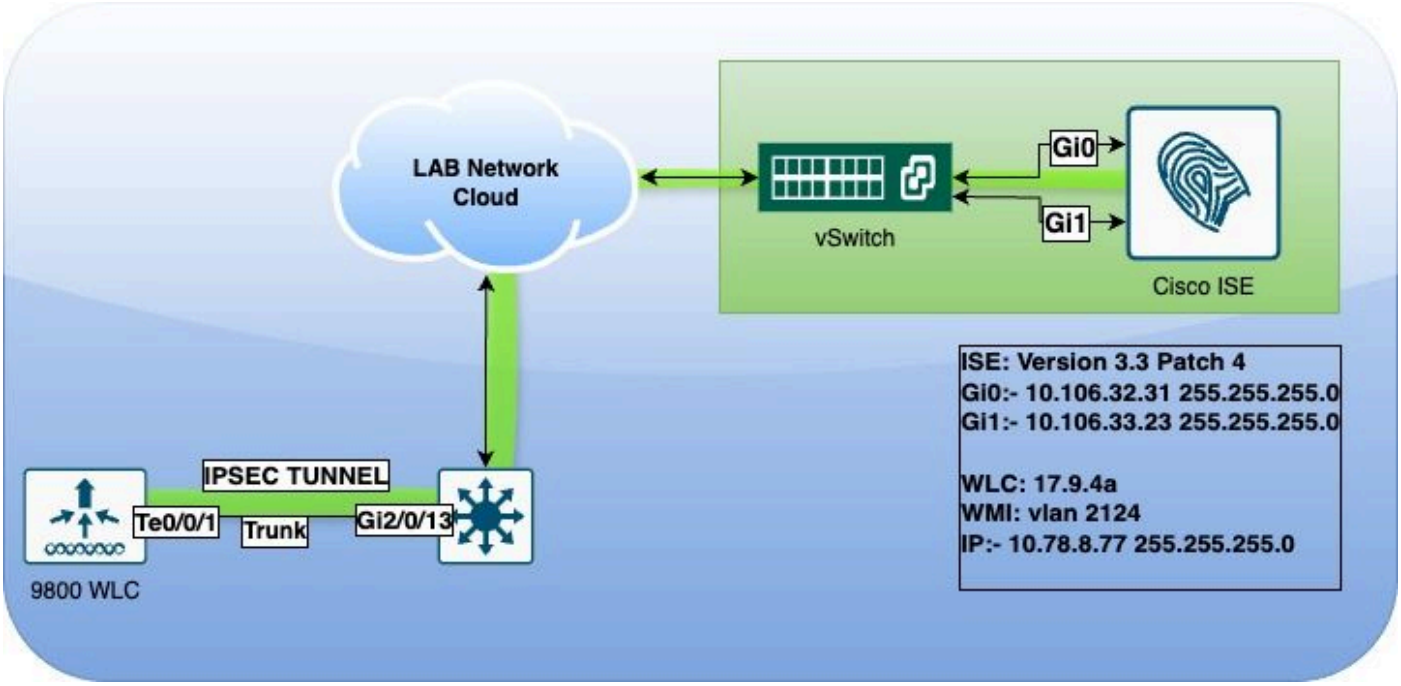
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

IPsec è una struttura di standard aperti sviluppata dall'IETF. Fornisce protezione per la trasmissione di informazioni sensibili su reti non protette, come Internet. IPsec opera a livello di rete, proteggendo e autenticando i pacchetti IP tra i dispositivi IPsec (peer) interessati, ad esempio i router Cisco. Utilizzare IPsec tra il WLC 9800 e il server ISE per proteggere la comunicazione RADIUS e TACACS.

# Configurazione

## Esempio di rete




Esempio di rete

## Configurazione di ISE

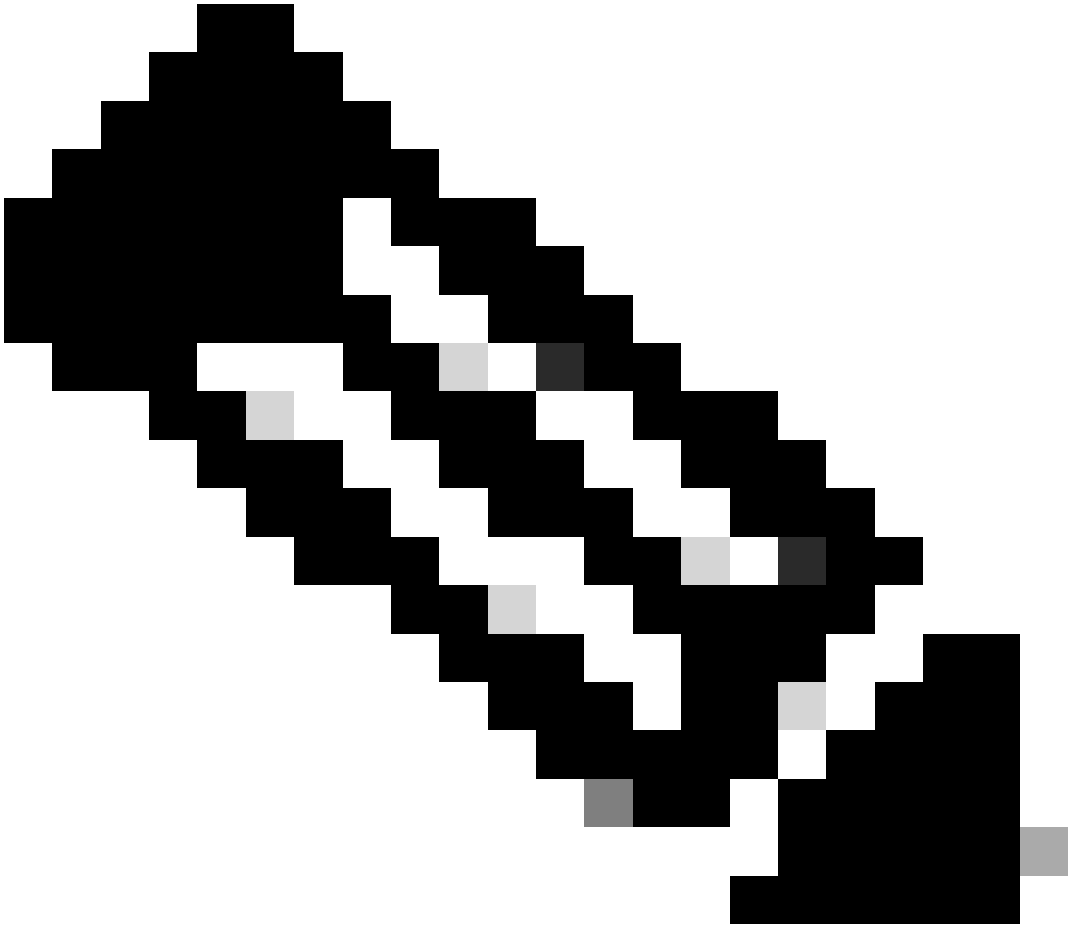
Cisco ISE supporta IPsec nelle modalità tunnel e trasporto. Quando si abilita IPsec su

un'interfaccia Cisco ISE e si configurano i peer, viene creato un tunnel IPsec tra Cisco ISE e il servizio NAD per proteggere la comunicazione.

È possibile definire una chiave già condivisa o utilizzare certificati X.509 per l'autenticazione IPSec. IPsec può essere abilitato sulle interfacce Gigabit Ethernet da 1 a Gigabit Ethernet 5.

Cisco ISE release 2.2 e successive supportano IPsec.

---



Nota: Accertarsi di disporre di una licenza Cisco ISE Essentials.

---

Aggiungere un dispositivo di accesso alla rete (NAD) con un indirizzo IP specifico nella finestra Dispositivi di rete.

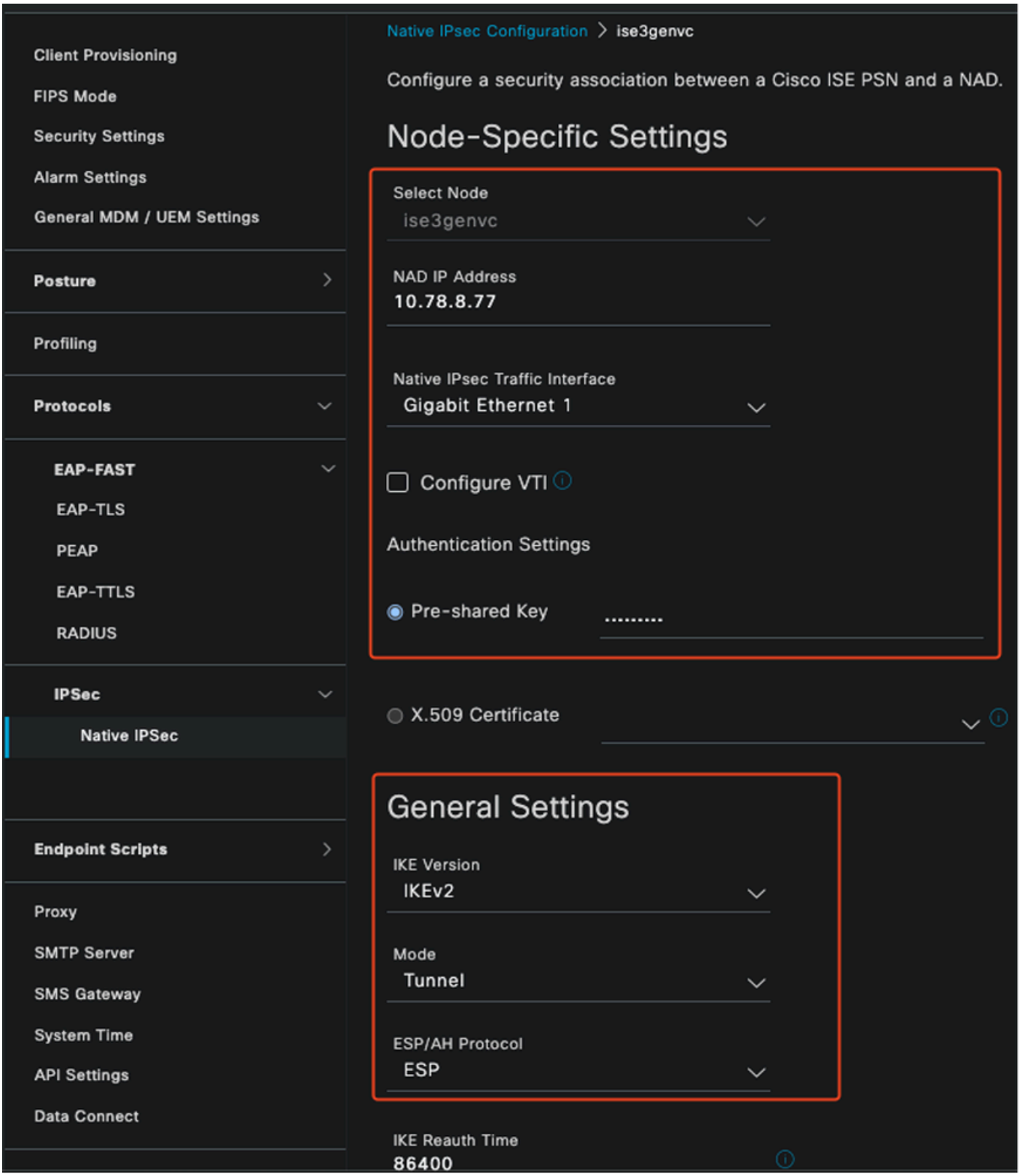
Nell'interfaccia utente di Cisco ISE, passare il mouse su Administration e selezionare System > Settings > Protocolli > IPsec > Native IPsec.

Fare clic su Add per configurare un'associazione di sicurezza tra un PSN di Cisco ISE e un NAD.

- Selezionare il nodo.
- Specificare l'indirizzo IP NAD.
- Scegliere l'interfaccia del traffico IPSec richiesta.
- Immettere la chiave già condivisa da utilizzare anche su NAD.

Nella sezione Generale immettere i dettagli specificati.

- Scegliere IKEv2.
- Selezionare la modalità tunnel.
- Selezionare ESP come protocollo ESP/AH.



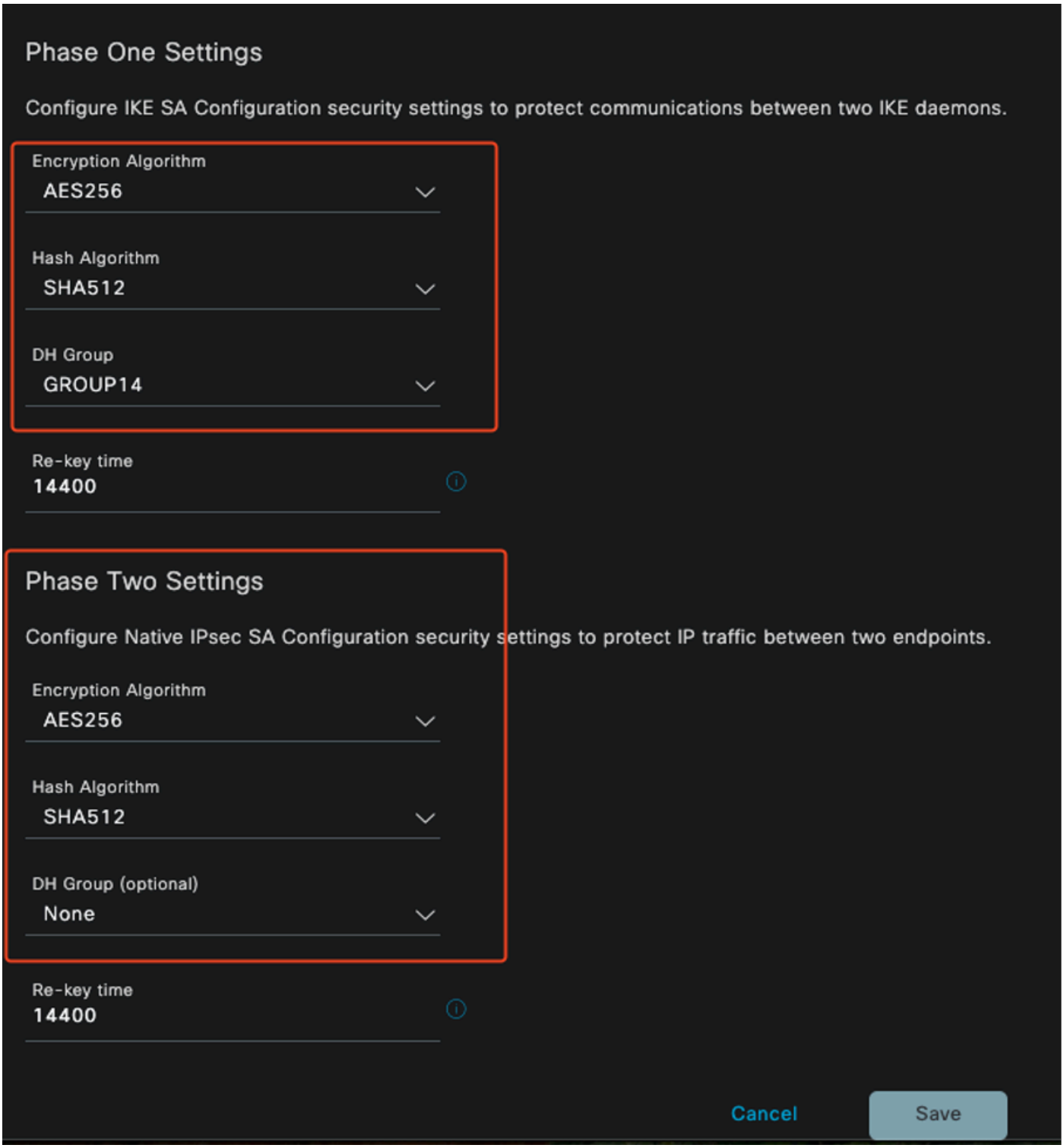

Configurazione IPSec nativa ISE

Nelle impostazioni della fase uno:

- Scegliere AES256 come algoritmo di crittografia.
- Selezionare SHA512 come algoritmo.
- Selezionare GROUP14 come gruppo DH.

Nelle impostazioni della seconda fase:

- Scegliere AES256 come algoritmo di crittografia.
- Selezionare SHA512 come algoritmo.




Configurazione di IPSec fase 1 e fase 2

Configurare un percorso dalla CLI di ISE al WLC usando il gateway eth1 come hop successivo.

<#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
```

## Configurazione 9800 WLC

La configurazione IPSec del WLC 9800 non viene esposta sulla GUI, quindi tutta la configurazione deve essere eseguita dalla CLI.

Di seguito vengono riportati i passaggi di configurazione per il server ISE. Ciascun passaggio è accompagnato dai comandi CLI appropriati in questa sezione per fornire una guida.


Procedura di configurazione IPSec WLC

Configurazione proposta IKEv2

Per iniziare la configurazione, accedere alla modalità di configurazione globale e creare una proposta IKEv2. Assegnare un nome univoco alla proposta a scopo di identificazione.

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

Configurare quindi un criterio ed eseguire il mapping della proposta creata in precedenza all'interno del criterio.

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

Definire un keyring di crittografia da utilizzare durante l'autenticazione IKE. Questo keyring contiene le credenziali di autenticazione necessarie.

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

Configurare un profilo IKEv2 che funge da repository per i parametri non negoziabili dell'associazione di protezione IKE. Sono incluse identità locali o remote, metodi di autenticazione e servizi disponibili per peer autenticati.

```
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
```

Creare un set di trasformazioni e configurarlo per funzionare in modalità tunnel.

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

Creare un ACL per consentire la comunicazione solo con l'IP dell'interfaccia ISE.

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

Configurare una mappa crittografica dalla configurazione globale. Collegare il set di trasformazioni, il profilo IPsec e l'ACL alla mappa crittografica.

```
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
```

Infine, collegare la mappa crittografica all'interfaccia. In questo scenario, l'interfaccia di gestione wireless che trasporta il traffico RADIUS viene mappata nella VLAN dell'interfaccia di gestione.

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

# Verifica

## WLC

Comandi show disponibili per verificare IPSec sul WLC 9800.

- show ip access-lists
- mostra mappa crittografica
- visualizzazione dettagliata di crypto ikev2 sa
- mostra dettagli sa crypto ipsec

<#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,
```

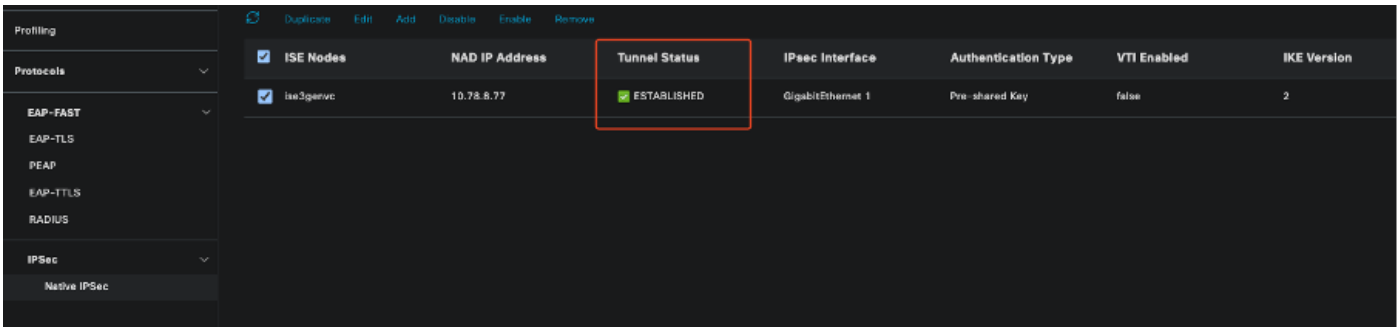
**TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256**

```
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 ISE con stato IPSec

### Acquisizione pacchetti

Prendere un EPC sul WLC per assicurarsi che il traffico RADIUS del client stia attraversando il tunnel ESP. Utilizzando un'acquisizione control plane, è possibile osservare i pacchetti che lasciano il control plane in uno stato non crittografato, che vengono quindi crittografati e trasmessi alla rete cablata.

| 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) |

Pacchetti IPSec tra WLC e ISE

## Risoluzione dei problemi

### Debug WLC

Poiché il WLC 9800 funziona su Cisco IOS XE, è possibile utilizzare comandi di debug IPSec simili a quelli di altre piattaforme Cisco IOS XE. Di seguito sono riportati due comandi chiave utili per la risoluzione dei problemi relativi a IPSec.

- debug crypto ikev2
- errore debug crypto ikev2

### Debug ISE

Utilizzare questo comando della CLI di ISE per visualizzare i registri IPSec. I comandi di debug non sono necessari sul WLC.

- show logging application strongswan/charon.log tail

## Riferimenti

Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS XE Cupertino 17.9.x

IPsec Security per proteggere le comunicazioni tra Cisco ISE e NAD

Configurazione di IKEv2 (Internet Key Exchange versione 2)

Configurazione di ISE 3.3 Native IPsec per la comunicazione protetta e non protetta (Cisco IOS XE)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).