

# Cisco WLC ISE و IPsec نیپ قفن نیوک

تایوتھملا

## مدقمل

## قیس اس الات اپل طت مل

تابلطت ملما

## ةمدختسملا تانوكمل

## معلومات اساسی

نيوكل

## ةكبشلليطي طختلا مس رلا

ISE نیوک

## لیکشت 9800 WLC

## قصص لام ققيقحت

WLC

## قرحہ کا مدد اور فوائد (ISE)

محلات طاقت

## اچھاں اور عاطل افاسنکتسا

## WLC اطلاعات حیچست

اطلاعات حیحصت ISE

عجمان

ةمدقملا

ISE مداخو 9800 WLC نيپ (IPsec) تونرتن إلا لوكوتورب ناماً نيوكت دنتسمل اذه فصي لاصتاً نيمأتل RADIUS و TACACS.

## ةيسيس اسألا تابلطت ملأ

تابلطتما

ـ ئىلاتلا عىض اومنلاب ـ فرعون كىدل نوكت نأب Cisco يىصوت

- (ISE) كرحم فشك تامد خ وهل ئي
  - Cisco IOS® XE WLC نويوكت
  - IPSec ميھافم ۋەماعل
  - RADIUS ميھافم ۋەماعل
  - TACACS ميھافملار ل ۋەماعل

## ةمـدـخـتـسـمـلـا تـانـوـكـمـلـا

- 17.09.04a: ئيكلس الـ C9800-40-K9 مكحـتـلا ئـدـحـو
- 4 لـيـغـشـتـلا دـيـقـ 3 رـادـصـ الـا حـيـحـصـتـ جـمـانـرـبـ Cisco ISE:
- 9200-L-24P لـوحـمـلـا

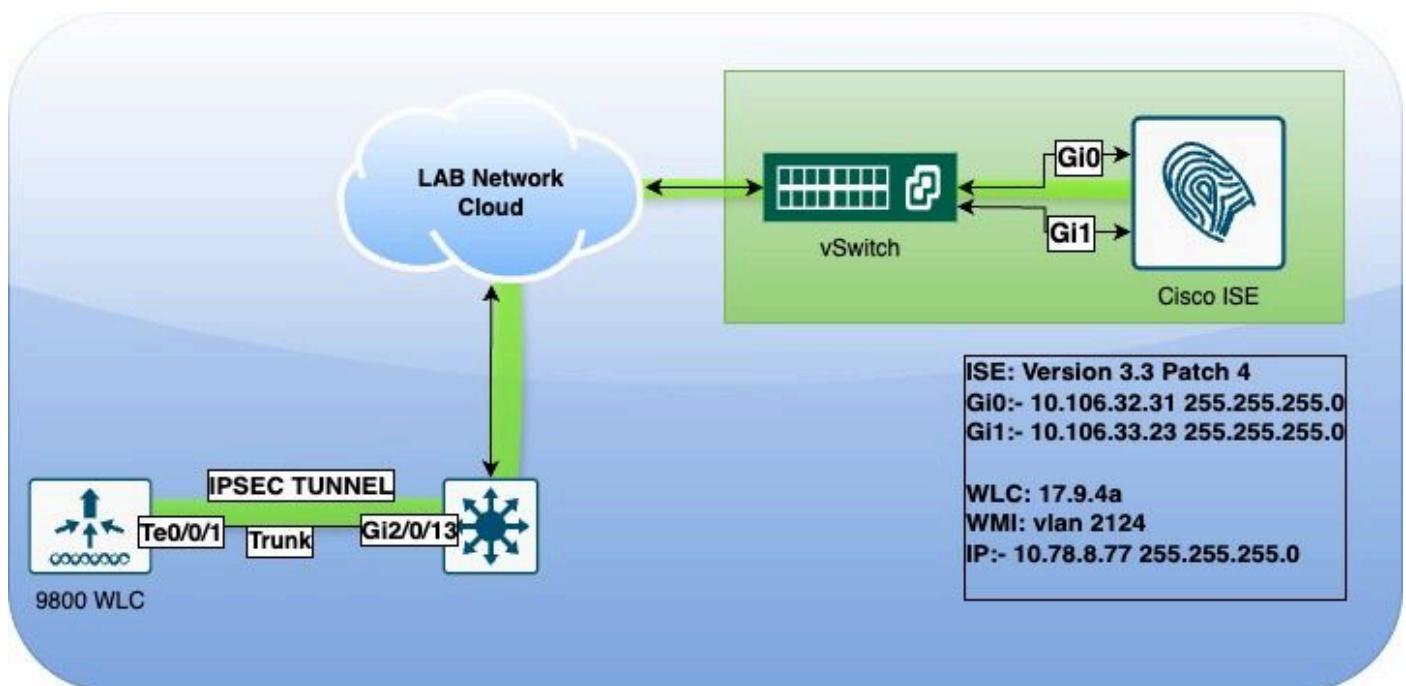
ةـصـاخـ ئـيـلـمـعـمـ ئـيـيـبـ يـفـ ئـدـوـجـوـمـلـا ئـزـهـجـأـلـا نـمـ دـنـتـسـمـلـا اـذـهـ يـفـ ئـدـرـاوـلـا تـامـوـلـعـمـلـا عـاشـنـا مـتـ تـنـاـكـ اـذـاـ. (يـضـارـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـفـ ئـمـدـخـتـسـمـلـا ئـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ، لـيـغـشـتـلا دـيـقـ كـتـكـبـشـ.

## ةـيـسـاسـأـ تـامـوـلـعـمـ

لـقـنـلـ نـاـمـأـلـا رـفـوـيـ وـهـ. ئـيـطـسـاـوبـ هـرـيـوـطـتـ مـتـ ئـحـوـتـفـمـلـا رـيـيـاعـمـلـلـ رـاطـاـ وـهـ ئـقـبـطـ يـفـ IPsec لـمـعـيـ. تـنـرـتـنـ إـلـا لـثـمـ ئـيـمـحـمـلـا رـيـغـ تـاـكـبـشـلـا رـبـعـ ئـسـاسـحـلـا تـامـوـلـعـمـلـا تـاهـجـوـمـ لـثـمـ، (ءـارـظـنـلـاـ) ئـكـراـشـمـلـا IPsec ئـزـهـجـأـنـيـبـ اـهـيـلـعـ قـدـاصـيـوـ IP مـنـجـ يـمـحـيـ اـمـ، ئـكـبـشـلـا Cisco زـارـطـ (WLC) ئـيـكـلـسـالـلـا ئـيـلـحـمـلـا ئـكـبـشـلـا يـفـ مـكـحـتـلـا ئـدـحـوـنـيـبـ IPsec مـدـخـتـسـأـ. Cisco 9800 RADIUS وـ TACACSـ مـداـخـوـ لـاـصـتـاـ نـيـمـأـتـلـ Cisco ISE.

## نـيـوـكـتـلـاـ

### ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ

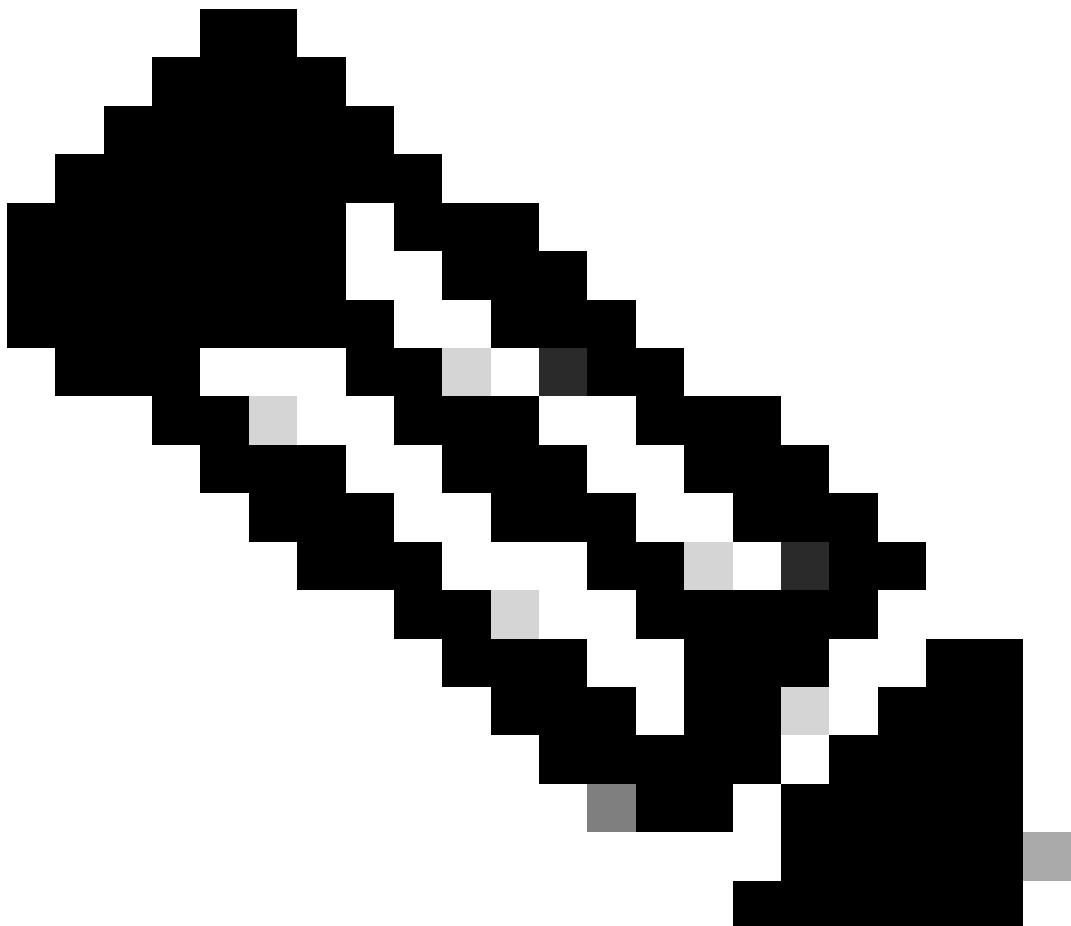
## نـيـوـكـتـ Cisco ISE

ةـجـاـوـىـلـعـ IPsec نـيـكـمـتـ دـنـعـ. لـقـنـلـاـوـ قـافـنـأـلـا عـاضـوـأـ يـفـ IPsec لـوـكـوـتـورـبـ Cisco ISE مـعـديـ. لـاـصـتـاـلـاـ نـيـمـأـتـلـ Cisco ISE وـ Cisco ISE NAD قـفـنـ عـاـشـنـاـ مـتـيـ، نـارـقـأـلـاـ نـيـوـكـتـوـ Cisco ISE.

نـكـمـيـ IPsec. ئـقـدـاصـمـلـ X.509 تـادـاهـشـ مـادـخـتـسـاـ وـأـقـبـسـمـ كـرـتـشـمـ حـاتـفـمـ دـيـدـحـتـ كـنـكـمـيـ تـاهـجـاـوـلـالـخـ نـمـ 1 تـبـاجـيـجـ تـنـرـثـيـاـ ئـلـعـ IPsec Gigabit Ethernet 5.

ISE نم ثدحألا تارادص إل او Cisco نم 2.2 تارادص إل او IPsec.

---



ةظحالم دكأت نم صيخرت كيدل نأ Cisco ISE Essentials.

---

ةكبشلا ۆزهجأ ۆذفان يف IP ىلا صاخ ناونع (NAD) ۆكبشلا ىلا لوصو زاحج ۆفاضا.

> تادادع > ماظنلا ىلا لقتنا او ۆردا لا ربع لقتنا Cisco ISE، ۆيموسرلا مدخلتسمل ۆهج او يف  
ييعيبط ىلهأ > IPsec > IPsec > تالوكوتورب.

Cisco ISE PSN و NAD. قوف رقنا نيب ناما نارتقا نيوكتل ۆفاضا.

- ۆدقعلا ددح.
- ناونع ددح NAD IP.
- ۆبولطملا IPsec ۆرورم ۆکرح ۆھج او رتخار.
- اضيأ NAD ىلع ھمادختسا متيس يذلا اقبسم كرتشملا حاتفملا لخدا.

ةددحملا ليصافتلا لخدا، ماعلا مسقلما يف.

- رت خاً IKEv2.
- قفنلا عض و ددح.
- لوكوتوربك ESP/AH.

Native IPsec Configuration > ise3genvc

Configure a security association between a Cisco ISE PSN and a NAD.

## Node-Specific Settings

Select Node  
ise3genvc

NAD IP Address  
**10.78.8.77**

Native IPsec Traffic Interface  
Gigabit Ethernet 1

Configure VTI ⓘ

Authentication Settings

Pre-shared Key .....  
 X.509 Certificate ⓘ

## General Settings

IKE Version  
**IKEv2**

Mode  
**Tunnel**

ESP/AH Protocol  
**ESP**

IKE Reauth Time  
**86400** ⓘ

نويوكت ISE ييلصألا IPSec

يـفـ اـدـاعـ تـادـعـ اـلـ حـرـمـ اـلـ اـلـ

- رت خاً AES256 زراروـخـ.

- ئەيم زراو خلا نەم پشتىي امك ددح SHA512.
- ئەيم زراو خلا نەم پشتىي امك ددح 14 دەنەجەم ك DH.

ئەين اىثلە ئەل جرملا تادادعى يە:

- رېفشت ئەيم زراو خلا AES256 رەت خا.
- ئەيم زراو خلا نەم پشتىي امك ددح SHA512.

## Phase One Settings

Configure IKE SA Configuration security settings to protect communications between two IKE daemons.

**Encryption Algorithm**  
AES256

**Hash Algorithm**  
SHA512

**DH Group**  
GROUP14

**Re-key time**  
14400 ⓘ

---

## Phase Two Settings

Configure Native IPsec SA Configuration security settings to protect IP traffic between two endpoints.

**Encryption Algorithm**  
AES256

**Hash Algorithm**  
SHA512

**DH Group (optional)**  
None

**Re-key time**  
14400 ⓘ

Cancel
Save

نەم 2 ئەل جرملا او 1 ئەل جرملا نېوكت

ئەيل حملە ئەك بىشلى يە مەكتەلە رەصنۇع ئىلە ISE رەم او رەطس ئەھجاو نەم راسىم نېوكتىب مەق

ةيكلساللـا (WLC) ةبـاوب مـادـخـتـسـاب ETH1 ةـوـطـخـلـاـكـاـلـاـ.

<#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 لـيـكـشـتـ

ةـيـكـلـسـالـلـاـ (WLC) ةـكـبـشـلـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـبـ صـاـخـلـاـ IPSec نـيـوـكـتـ ضـرـعـ مـتـيـ الـ 9800 زـارـطـ عـيـمـجـ ءـارـجـ اـمـلـاـ مـزـلـيـ كـلـذـلـ ،ـ (GUI) ةـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ةـهـجـاـوـىـلـعـ (CLI).

اـذـهـ يـفـ ةـلـصـلـاـ تـاـذـاـ CLI رـمـاـوـاـبـ ةـوـطـخـ لـكـ قـاـفـرـاـ مـتـيـ .ـISEـ مـدـاـخـلـ نـيـوـكـتـلـاـ تـاـوـطـخـ يـلـيـ اـمـيـفـ يـيـجـوـتـلـاـ رـيـفـوـتـلـاـ مـسـقـلـاـ.

## Configure IKEv2 Proposal

## Configure IKEv2 Policy

## Create IKEv2 Keyring

## Configure an IKEv2 Profile

## Create a Transform Set

## Create a Crypto Map Access Control List

## Create a Crypto Map

## Apply the Crypto Map to an Interface

نیوکت تاوظ WLC IPSec

حترقم نیوکت IKEv2

دیرف مسا نییعتب مق. حترقم ئىشنى او ماعلا نیوكتلار عضولخدا، نیوكتلار عدبلى فىرعتلار ضارغان حترقملل.

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

جەنلە اذە نەمەن اقىب سەم ھۇاشنە مەت يىذلە حارتقا لانىيىعەت و ئاسايىس نىوكتىپ مۇق، كەلذ دەعب

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

ۋەقىلەنەت لە IKE. ئەق داصلەم ئانىڭ اهمادختىسى مەتىلى رېفېشەت حېتافم ئەقلىح دىدەتلىپ مۇق ئەرىورەزلى ئەق داصلەم لە ئامەتىغا تانايىب ھەذە حېتافم لە.

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

بە ئەصاخىلا لە وادتلىل ئەلباقلى رېغ تاملىعەملە دەوت سەمك لەمۇي يىذلە IKEv2 فېرۇت فەلم نىوكت ئەحاتىم لە تامدەخلى او ئەق داصلەم لە بېلەس أو ئەدىيەب لە تايىوهەلە كەلذ نەمەن پەتىيە. مەھىلەن قەدصەم لە نارقىللە.

```
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
```

قەنلە عضو يىف لەمۇلەل اھنىوكت تو لېوحەت ئەعومەجەم ئاشناب مۇق.

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

بە طقىف لاصتا لاب حامىسىلەل (ACL) لەوصولە يىف مەكەنەت ئەمئاقد ئاشناب مۇق ISE Interface IP.

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

```
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
```

قرادإلا ٰهـج اوـنـيـعـتـ مـتـيـ ،ـ ويـرـانـيـسـلـاـ اـذـهـ يـفـ .ـ هـجـ اـوـلـاـ بـرـيـفـشـتـلـاـ ٰهـطـيـرـخـ قـاـفـرـابـ مـقـ ،ـ اـرـيـخـأـ .ـ هـرـادـإـلـاـ ٰهـجـ اوـبـ ٰصـاـخـلـاـ VLANـ ٰكـبـشـ نـمـضـ RADIUSـ رـوـرـمـ ٰكـرـحـ لـمـحـتـ يـتـلـاـ ٰهـيـكـلـسـالـلـاـ

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

# ةحصـلـا نـم قـقـحتـلـا

WLC

9800 WLC رم اوأ رفوت show IPSec نم ققحتلL ىلع

- show ip access-lists
  - ریفشتل اقتدریخ ضرع
  - show crypto ikev2 sa detail
  - ریفشتل IPsec افت ضرع

<#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

## TKFv2 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
```

```
Enr: AES-CBC, keysiz: 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 (recv) 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:
```

## ةيوجل افشـك تامـدـخ كـرحـم (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.
```

Protocols	<input type="checkbox"/> ISE Nodes	NAD IP Address	Tunnel Status	IPsec Interface	Authentication Type	VTI Enabled	IKE Version
EAP-FAST	<input checked="" type="checkbox"/> ise3gnewv	10.78.6.77	<input checked="" type="checkbox"/> ESTABLISHED	GigabitEthernet 1	Pre-shared Key	false	2

اوجه موسريلا مدخلة ملأ جهاز ISE GUI (جهاز ملء) IPSec

محلہ طاقت لہ

ةيكلساللا ةيلحملاءكبشلا يف مكحتلا رصنع ىلع (EPC) لوصولا يف مكحت ةدحو لخأ مادختساب ESP. قفن رباع ليمعلاب ةصالخلا RADIUS تانايب رورم ةكرح روبع نامضل (WLC) ريع ةلاح يف مكحتلا ىوتسم نم جرخت يتلا مزحلا ةبقارم كنكمي، مكحتلا ىوتسم طاقتلا. ةيكلساللا ةكبشلا ىلإ اهلأسراو اهريفيشت كلذ دعب متى يتلأاو، ُرفشم

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 و ISE نیب IPSec مزح

اھالص او عاطخآل ا فاشکتسا

WLC حی حصت ااطخا

جمانرب ىلع لمعي 9800 زارت (WLC) ۆيكلساللا ۆيلحملا ۆكبشلا يف مكحتلا رصنع نأ امب ىلع ۆدوجوملما كلتل ۆلثامم IPSec ەاطخأ حيحصت رماواً مادختسإ كنكمييف Cisco IOS XE، فاشكتسسال نادي فم نايسيئر نارمأ يلي امييف Cisco IOS XE نم ىرخألا ۆيساسألا ۆمظنألا اھحالص او IPSec ەاطخأ.

- debug crypto ikev2
  - اطخ debug crypto ikev2

اٹھا جی حصت ISE

رم اوأ IPSec ضرعـل ISE ب ةـصـاخـلـا (CLI) رـمـأـلـا رـطـسـهـاـوـىـلـعـ رـمـأـلـا اـذـهـ مـدـخـتـسـأـ ةـيـكـلـسـالـلـا ةـيـلـحـمـلـا ةـكـبـشـلـا يـفـ مـكـحـتـلـا رـصـنـعـىـلـعـ ةـيـرـورـضـ رـيـغـ حـيـحـصـتـلـاـ (WLC).

- show logging application strongswan/charon.log tail

## عـاجـارـمـلـاـ

[Cisco Catalyst 9800 Series Wireless Controller Software, Cisco IOS XE Cupertino 17.9.x](#)

[Cisco ISE و IPsec نـيـبـ لـاصـتـالـاـ نـيـمـأـتـلـ](#)

[\(IKEv2\) يـلـدـابـتـلـاـ تـنـرـتـنـالـاـ حـاتـفـمـ نـمـ 2ـ رـادـصـالـاـ نـيـوـكـتـ](#)

[Cisco ISE 3.3 NAD \(Cisco IOS XE\) نـامـأـىـلـاـ يـلـصـأـلـاـ لـاصـتـاـ نـيـوـكـتـ](#)

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).