

نېمأتل ېلصلال IPsec 3.3 ISE نېوكت NAD (IOS-XE) لاصلتال

تايوتحمل

[قمدملا](#)

[قيساسال تابلطتلا](#)

[تابلطتلا](#)

[قمدمتلا تانوكملا](#)

[قيساسا تامولعم](#)

[X.509 عدهش، قداصل مې IPsec IKEv2 قفن نېوكت](#)

[كېشلل، ېطېطختلا مسرلا](#)

[IOS-XE لوجمل، رماوالا رطس، قهجاو نېوكت](#)

[تاهجاو نېوكت](#)

[TrustPoint نېوكت](#)

[تاداهشلا داريتسا](#)

[IKEv2 جرنتقم نېوكت](#)

[رېفشتلل، IKEv2 جهن نېوكت](#)

[رېفشتلل، IKEv2 فيرعت فلم نېوكت](#)

[قېمهالا تاذ VPN رورم، رول، \(ACL\) لوصول، في م كحت قمي، اق نېوكت](#)

[ليوخت، قومجم نېوكت](#)

[قهجاو ىلع اه قىبطتو رېفشت، قطيرخ نېوكت](#)

[IOS-XE ىئاهنلا، نېوكتلا](#)

[ISE نېوكت](#)

[ISE ىلع IP ناووع نېوكت](#)

[هې قوئوملا، رجتلا، عدهش، داريتسا](#)

[ماظنلا، عدهش، داريتسا](#)

[IPsec قفن نېوكت](#)

[اقبسم كراشملا، X.509 حاتقم، قداصل مې IPsec IKEv2 قفن نېوكت](#)

[كېشلل، ېطېطختلا مسرلا](#)

[IOS-XE لوجمل، رماوالا رطس، قهجاو نېوكت](#)

[تاهجاو نېوكت](#)

[IKEv2 جرنتقم نېوكت](#)

[رېفشتلل، IKEv2 جهن نېوكت](#)

[رېفشتلل، IKEv2 فيرعت فلم نېوكت](#)

[قېمهالا تاذ VPN رورم، رول، \(ACL\) لوصول، في م كحت قمي، اق نېوكت](#)

[ليوخت، قومجم نېوكت](#)

[قهجاو ىلع اه قىبطتو رېفشت، قطيرخ نېوكت](#)

[IOS-XE ىئاهنلا، نېوكتلا](#)

[ISE نېوكت](#)

[ISE ىلع IP ناووع نېوكت](#)

[IPsec قفن نېوكت](#)

[قحصلا، نم ققختلا](#)

[IOS-XE، نم ققختلا](#)

[ISE ىلع قحصلا، نم ققختلا](#)

[اهج الص او عا طخ ال ا فاش كت س ا](#)

[اهج الص او IOS-XE ا طخ ا فاش كت س ا](#)

[ن ي ك م ت ل ل ا ط خ ال ا ح ص ت](#)

[IOS-XE ل ع ق ل م ا ع ل ا ط خ ال ا ح ص ت ن م ق ل م ا ك ع و م ح م](#)

[اهج الص او ISE ا طخ ا فاش كت س ا](#)

[ن ي ك م ت ل ل ا ط خ ال ا ح ص ت](#)

[ISE ل ع ق ل م ا ع ل ا ط خ ال ا ح ص ت ن م ق ل م ا ك ع و م ح م](#)

ة م د ق م ل ا

IPsec ب ص ا خ ل ا (NAD) ة ك ب ش ل ل ا ل و ص و ل ا ز ا ه ل ل ا ص ت ا ن ي و ك ت ة ي ف ي ك د ن ت س م ل ا ا ذ ه ف ص ي ن ك م ي 3.3 (ISE) Cisco ن م ة ي و ه ل ا م د خ ك ر ح م ن ي م ا ت ل ا ه ج ا ل ص ا و ه ا ط خ ا ف ا ش ك ت س ا و ي ل ص ا ل ا 2 ر ا د ص ا ل ا ت ن ر ت ن ا ل ا ح ا ت ف م ل د ا ب ت ق ف ن م ا د خ ت س ا ب RADIUS ت ا ن ا ي ب ر و ر م ة ك ر ح ر ي ف ش ت ا ذ ه ي ط غ ي ا ل ISE و ل و ح م ل ا ن ي ب (LAN ة ك ب ش ل ل ا -LAN) ع ق و م ل ل ا ع ق و م ن م IPsec (IKEv2) RADIUS ن ي و ك ت ع ز ج د ن ت س م ل ا

ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- (ISE) ة ي و ه ل ا ف ش ك ت ا م د خ ك ر ح م
- Cisco ل و ح م ن ي و ك ت
- ة م ا ع ل ا IPsec م ي ه ا ف م
- ة م ا ع ل a RADIUS م ي ه ا ف م

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ي ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ل ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- ج م ا ن ر ب ل ا ن م 17.6.5 ر ا د ص ا ل ا ل غ ش ي ي ذ ل ا Cisco Catalyst Switch C9200L ل و ح م ل ا
- Cisco Identity Service Engine، ر ا د ص ا ل ا 3.3
- Windows 10 ل ي غ ش ت ل ا م ا ظ ن

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ا ش ن ا م ت ت ن ا ك ا ذ ا (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ة ر ش ا ب م ك ت ك ب ش

ة ي س ا س ا ت ا م و ل ع م

TACACS و RADIUS و ة ن م ا ل ر ي غ MD5 ة ئ ز ج ت م د خ ت س ت ي ت ل ا ت ا ل و ك و ت و ر ب ل ا ن ي م ا ت و ه ف د ه ل ا ر ا ب ت ع ا ل ا ن ي ع ب ا ه ذ خ ا ب ج ي ي ت ل ا ق ئ ا ق ح ل ا ن م ل ي ل ق IPsec:

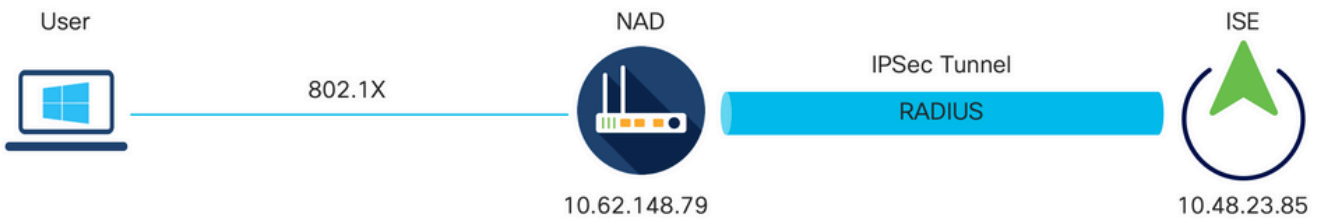
- [StrongSwan](#) ل ل ا ا د ا ن ت س ا IPsec ل ل ص ا ل ا ISE ل ح ا ا ش ن ا م ت
- NAD و Cisco ISE ن ي ب IPsec ق ف ن ا ا ش ن ا م ت ي ، Cisco ISE ة ه ج ا و ل ع IPsec ن ي و ك ت د ن ع ة ي ل ص ا ل ا IPsec ت ا د ا د ع ل ن م ض ل ص ف ن م ل ك ش ب NAD ن ي و ك ت ب ج ي . ل ا ص ت ا ل ا ن ي م ا ت ل

- IPsec ةقداصم ل X.509 تاداهش مادختسا وأ اقبس م كرتشم حاتفم ديدحت كنكمي
- GigabitEthernet5 تاهجاو لال خ نم GigabitEthernet1 ىل ع IPsec ني كمت نكمي

ققحتلا مسق زكري X.509 ةداهش ةقداصم ةيطغت وه دنتسم لل يسيئرلا زيكرتلا
 حيحصت نوكي نأ بجي و، طقف X.509 ةداهش ةقداصم ىل ع اهجالصإ و اطاخألا فاشكتسا و
 يف طقف فالخال عم، اقبس م ةكرتشم ل احي تافم ل ةقداصم ل امامت الاثامم اطاخألا
 اضيأ ققحتلل رماوأل س فن مادختسا نكمي . تاجرمل

X.509 ةداهش ةقداصم ب IPsec IKEv2 ق فن نيوكت

ةكبش لل يطيختلا مسرلا



ةكبش لل يطيختلا مسرلا

IOS-XE ل وحم ل رماوأل رطس ةهجاو نيوكت

تاهجاو نيوكت

تلکش تنك يغبني لقالا ىل ع نراق دحاو كلذ دع ب، دع ب نراق لكشي ال حاتفم IOS-XE ل ن
 لاثم يلي اميف:

```

interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 negotiation auto
 no shutdown
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
  
```

نم VPN ةكبش ق فن عاشنإل همادختسا بجي يذلا ديعبلا ريظنلاب لاصتا دوجو نم دكأت
 يساسألا لاصتالا نم ققحتلل ping رماوأل مادختسا كنكمي . عقوم ىل ع قوم

TrustPoint نيوكت

ليكشت لماش يف رم <name> crypto pkiTrustPoint ل، جهن IKEv2 ل تلکش in order to تلخد
 لاثم يلي اميف . بولسا

✎ لاثملا اذه في IOS-XE زاهج ىلع تاداهشلا تيبتتل ةددعتم قرط كانه :ةظالم ، اهتلسلسو ةيوهلا ةداهش ىلع يوتحي يذلاو ، PKCS12 فلم داريئسا مدختسن

```
crypto pki trustpoint KrakowCA
revocation-check none
```

تاداهشلا داريئسا

داريئسا crypto pki ل اهتلسلس عم ةداهش ةيوه IOS-XE تدرتسا in order to تلخد
لاثم يلي امي في . زايئسا وذبولسا ي في رم <password> ةملك <location> <trustPoint> pkcs12

```
KSEC-9248L-1#crypto pki import KrakowCA pkcs12 ftp://eugene:<ftp-password>@10.48.17.90/ISE/KSEC-9248L-1-
% Importing pkcs12...Reading file from ftp://eugene@10.48.17.90/ISE/KSEC-9248L-1.pfx!
[OK - 3474/4096 bytes]
```

```
CRYPTO_PKI: Imported PKCS12 file successfully.
KSEC-9248L-1#
```

✎ ةيوه ةداهش نأ نم دكأت ، دنتسملا قاطن چراخ عقت تاداهشلا نأ نم مغرلا ىلع :ةظالم ةداهش ISE بلطتي . اهب صاخلا IP / FQDN ناوئعب ةلوهأم SAN لوقح ىلع يوتحت IOS-XE
SAN لوقح ىلع لوصحلل ريظن .

ح:حيص لكشب تاداهشلا تيبتت نم ققحتلل

```
KSEC-9248L-1#sh crypto pki certificates KrakowCA
Certificate
  Status: Available
  Certificate Serial Number (hex): 4B6793F0FE3A6DA5
  Certificate Usage: General Purpose
  Issuer:
    cn=KrakowCA
  Subject:
    Name: KSEC-9248L-1.example.com
    IP Address: 10.62.148.79
    cn=KSEC-9248L-1.example.com
  Validity Date:
    start date: 17:57:00 UTC Apr 20 2023
    end date: 17:57:00 UTC Apr 19 2024
  Associated Trustpoints: KrakowCA
  Storage: nvram:KrakowCA#6DA5.cer
```

```
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
```

cn=KrakowCA
Subject:
cn=KrakowCA
Validity Date:
start date: 10:16:00 UTC Oct 19 2018
end date: 10:16:00 UTC Oct 19 2028
Associated Trustpoints: KrakowCA
Storage: nvram:KrakowCA#1CA.cer

KSEC-9248L-1#

IKEv2 حرتقم نيوكت

ليكشت لماش ي ف رمأ <name> ضرع crypto ikev2 ل، ةسايس IKEv2 ل تللكش in order to تلخد
لاثم يلي امي ف . بولسأ

```
crypto ikev2 proposal PROPOSAL  
encryption aes-cbc-256  
integrity sha512  
group 16  
!
```

ريفشتلل IKEv2 جهن نيوكت

لماش ي ف رمأ <name> ةسايس crypto ikev2 ل، ةسايس IKEv2 ل تللكش in order to تلخد
بولسأ ليكشت

```
crypto ikev2 policy POLICY  
proposal PROPOSAL
```

ريفشتلل IKEv2 فيرعت فلم نيوكت

ليكشت لماش ي ف رمأ <name> crypto ikev2 profile ل، بولسأ IKEv2 ل تللكش in order to تلخد
بولسأ.


```
crypto ikev2 profile PROFILE  
match address local 10.62.148.79  
match identity remote fqdn domain example.com  
authentication remote rsa-sig  
authentication local rsa-sig  
pki trustpoint KrakowCA
```

IKE هتووهك ةصاخلا هتووه ةداهش نم CN لقح يضا رتفا لكش ب ISE مدختسي :ةظحالم
فبرعت فلم ي ف "دعب نع ةيوهلا قباطت" مسق ي ف ببسلا اذهلو. IKEv2 ضوافت ي ف
ISE ب صاخلا FQDN وأ لاجملا ةبسانملا ةميقل او FQDN عون ديدحت كمزلي ، IKEv2.

ةيمهألا تاذا VPN رورم ةكرحل (ACL) لوصول ي ف مكحت ةمئاق نيوكت

اهتياحم بجي يتلا رورملا ةكرح ديدحتل ةامسمل وأ ةسوملا لوصول ةمئاق مدختسأ
لاثم ي لي امي ف .ري ف شتلاب

```
ip access-list extended 100
10 permit ip host 10.62.148.79 host 10.48.23.85
```

 ردصملا IP نيوانع VPN رورم ةكرحل لوصول ي ف مكحتلا ةمئاق مدختست :ةظحالم
دعب ةهوجل او NAT.

ليوحت ةوعومجم نيوكت

رمأل لخدأ، (تايمزراوخل او نامأل تالوكوتورب نم ةلوبقم ةوعومجم) IPsec ليوحت ةوعومجم دي دحتل لاثم يلي امي ف. ماعال نيوكتال عضو في crypto ipsec transform-set

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

ةهجاو لىلع اهقبيطت وري فشت ةطيرخ نيوكت

بولسأ ليكشت ةطيرخ crypto ل لخدأ و لخدم ةطيرخ ري فشت تلددع وأ تقلخ in order to تلخد بن اوچال ضع ب كانه، ري فشتال ةطيرخ لخدأ لم تك يى تح. رمأ ليكشت لم اش crypto map ل لىندأ دك اه فيرعت بجي يتل

- مه عالؤه. اه يلى ةيمحمم ل رورم ل ةكرح هيجوت ةداع ل نكمي يتل IPsec رئاظن دي دحت بجي ةطيرخ لخدأ في IPsec ريظن دي دحتل. ةمدخ دعاسم عاشن مه عم نكمي نيذال نارقأل ل set peer رمأل لخدأ، ري فشت
- in order to تلخد. ةيمحمم ل رورم ل ةكرح عم مادختسال ل ةلوبقم ل ليوحتال تاوعومجم دي دحت بجي لخدم ةطيرخ crypto ل عم تلمعتسا تنك عيطتسي نأ ةوعومجم ليوحتال تنيع in order to، رمأ set-ليوحت ةوعومجم ل
- ل ةمئاق ذفنم عسوم تنيع in order to تلخد. اه تي امج بجي يتل رورم ل ةكرح دي دحت بجي. رمأ ناو نع match ل، لخدم ةطيرخ crypto

لاثم يلي امي ف:

```
crypto map MAP-IKEV2 10 ipsec-isakmp
set peer 10.48.23.85
set transform-set SET
set pfs group16
set ikev2-profile PROFILE
match address 100
```

ةهجاو لىلع اق بس م ةدحمم ل ري فشتال ةطيرخ ةوعومجم قي بطت في ةريخأل ةوطخل ل ثمتت. رمأ ليكشت نراق crypto map ل، اذه تقلب in order to تلخد

```
interface Vlan480
crypto map MAP-IKEV2
```

IOS-XE يئاهن ل نيوكتال

لېكشت CLI حاتفم IOS-XE يئاهن ل انه:

```
aaa new-model
!
aaa group server radius ISE
  server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
  client 10.48.23.85
  server-key cisco
!
crypto pki trustpoint KrakowCA
  enrollment pkcs12
  revocation-check none
!
dot1x system-auth-control
!
crypto ikev2 proposal PROPOSAL
  encryption aes-cbc-256
  integrity sha512
  group 16
!
crypto ikev2 policy POLICY
  proposal PROPOSAL
!
crypto ikev2 profile PROFILE
  match address local 10.62.148.79
  match identity remote fqdn domain example.com
  authentication remote rsa-sig
  authentication local rsa-sig
  pki trustpoint KrakowCA
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
  mode tunnel
!
crypto map MAP-IKEV2 10 ipsec-isakmp
  set peer 10.48.23.85
  set transform-set SET
  set pfs group16
  set ikev2-profile PROFILE
  match address 100
!
interface GigabitEthernet1/0/23
  switchport trunk allowed vlan 1,480
  switchport mode trunk
!
interface Vlan480
  ip address 10.62.148.79 255.255.255.128
  crypto map MAP-IKEV2
!
ip access-list extended 100
  10 permit ip host 10.62.148.79 host 10.48.23.85
!
```



```
radius server ISE33-2
address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
key cisco
!
```

ISE نيوكت

ISE ىل ع IP ناووع نيوكت

ge0. م عد م تي ال ،رم اوأل رطس ةه او نم ge1-GE5 ةه اوأل ىل ع ناووع ال نيوكت بجي

```
interface GigabitEthernet 1
ip address 10.48.23.85 255.255.255.0
ipv6 address autoconfig
ipv6 enable
```

ةه اوأل ىل ع IP ناووع نيوكت دع ب قي بطت ال لي غشت ةداع م ت : ةظالم
ISE تامدخ لي غشت ةداع ىل ال IP ناووع ري غت ي دوي دق %
IP؟ ناووع ري غت عم ةع باتم ال ديرت له Y/N [N]: Y

ه ب قو ووم ال رجتم ال ةداهش داريتس

م تي ذل ا ينمزل ا قفنل ا ي ف ةم دق م ال ري ظنل ا ةداهش ب ISE ةق ت نامضل ةبولطم ةوطخل ا هذو
ىل ع رقنا .داريتس ا قوف رقنا .اه ب قو ووم تاداهش > تاداهش > ماظن > ةراد ا ىل لقتنا .هؤاشن ا
نم دكأت .ISE/IOS-XE ةي وه ةداهش ىل ع تعقو وي تال ا ق دصم ال عجرم ال ةداهش ددحو ضارعتس ا
ل.اسر ا ىل ع رقنا .ISE ل خاد ةق داصم ل ل ةق ت راي تخال ا ةنا خ دي دحت

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...
Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File

Friendly Name

Trusted For: Trust for authentication within ISE
 Trust for client authentication and Syslog
 Trust for certificate based admin authentication
 Trust for authentication of Cisco Services
 Validate Certificate Extensions

Description

ماظنل ا ةداهش داريتس

صاخ حات فم فلم و ةداهش فلم ، ةدق ع دح .ماظنل ا تاداهش > تاداهش > ماظن > ةراد ا ىل لقتنا

لأسرنا ىلع رقنا .IPsec لباقم رايخالال ةناخ دح .داريسا

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Import Server Certificate

* Select Node ise332

* Certificate File Browse... ise332.example.com.pem

* Private Key File Browse... ise332.example.com.key

Password

Friendly Name IPSEC-2

Allow Wildcard Certificates

Validate Certificate Extensions

Usage

Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

RADIUS DTLS: Use certificate for the RADSec server

pxGrid: Use certificate for the pxGrid Controller

ISE Messaging Service: Use certificate for the ISE Messaging Service

IPSEC: Use certificate for StrongSwan

SAML: Use certificate for SAML Signing

Portal: Use for portal

Submit Cancel

ىل لوصولا زاهج ظفح دعب طقف StrongSwan ىلع تاداهشلا تيبتت متي :ةظحالما
ةيلصلال IPsec تاداعل نمض ةكبشلا

IPsec قفن نيوكت

ةفاضل قوف رقنا .IPsec لصلال IPsec > IPsec > تالوكوتورب > تاداعل > ماظن > ةرادل ىل لقتنا
ربعمل او عانقلل مادختساب IP ناونع نيوكتب مقو ،IPsec قفن يهن تيلا ،ةدقعلل دح
ماظن ةداهش رتخاو X.509 ةداهش ةئيه ىلع ةقداصلل دادعل دح .IPsec ةهجاوويضارتفالل
ةتبتلل ةداهشلا

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings

Posture >
Profiling

Protocols >
EAP-FAST >
EAP-TLS
PEAP
EAP-TTLS
RADIUS

IPSec >
Legacy IPSec (ESR)
Native IPSec

Native IPSec Configuration > New

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

Node Specific Settings

Select Node
ise332

NAD IP Address with Mask
10.62.147.79/32

Default Gateway (optional)
10.48.23.1

IPSec Interface
Gigabit Ethernet 1

Authentication Settings

Pre-shared Key

X.509 Certificate IPSEC-2

قرايع نيوكت كنكمي، نارايخ كيدل، عقاولا يي. يرايخ نيوكت يه يي ضارتفالا بابوالا
ماظن يي ف راسم تيبتب موقت يتلاو، يي لصالا IPsec مدختسم هجاو يي ف يي ضارتفا
show running-config يي ف راسم الا اذه حضف متي ال. يي ساسالا ليغشتلا

```
ise332/admin#show running-config | include route
ise332/admin#
```

<#root>

```
ise332/admin#show ip route
```

Destination Gateway Iface

10.48.23.0/24 0.0.0.0 eth1

default 10.48.60.1 eth0

10.48.60.0/24 0.0.0.0 eth0

10.62.148.79 10.48.23.1 eth1

169.254.2.0/24 0.0.0.0 cni-podman1

169.254.4.0/24 0.0.0.0 cni-podman2

```
ise332/admin#
```

ققحيس اذهو، ISE يلع ايودي راسملا نيوكتو وغراف يي ضارتفالا بابوالا كرت وه رخا رايخ

هس فن ريثأتلا:

```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route
```

```
Destination Gateway Iface
-----
10.48.23.0/24 0.0.0.0 eth1
10.62.148.79 10.48.23.1 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

قباطات نأ بجي. ليولألا ةلحرمل تاداعإ نيوكت. IPsec ق فنل ةماعلا تاداعإلا نيوكت مت يتل تاداعإلا عم ةيناثلا ةلحرمل تاداعإو ليولألا ةلحرمل تاداعإو ةماعلا تاداعإلا IPsec ق فن نم رخآلا بناجلا ليلا هنيوكت

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows a navigation menu with options like Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, General MDM / UEM Settings, Posture, Profiling, Protocols, EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, RADIUS, IPsec (Legacy IPsec (ESR) and Native IPsec), and Endpoint Scripts. The main content area is titled 'General Settings' and contains several configuration fields:

- IKE Version: IKEv2
- Mode: Tunnel
- ESP/AH Protocol: esp
- IKE Reauth Time (optional): 86400
- Phase One Settings: Configure IKE SA Configuration security settings to protect communications between two IKE daemons.
- Encryption Algorithm: aes256
- Hash Algorithm: sha512
- DH Group: GROUP16
- Re-key time (optional): 14400

ظفح ةقطقو دادعإ ةيلمع ةيناثلا ةلحرمل تلاكش.

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings

Posture
Profiling
Protocols

EAP-FAST
EAP-TLS
PEAP
EAP-TTLS
RADIUS

IPSec
Legacy IPSec (ESR)
Native IPSec

Endpoint Scripts
Proxy
SMTP Server

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

Encryption Algorithm: aes256
Hash Algorithm: sha512
DH Group: GROUP16
Re-key time (optional): 14400

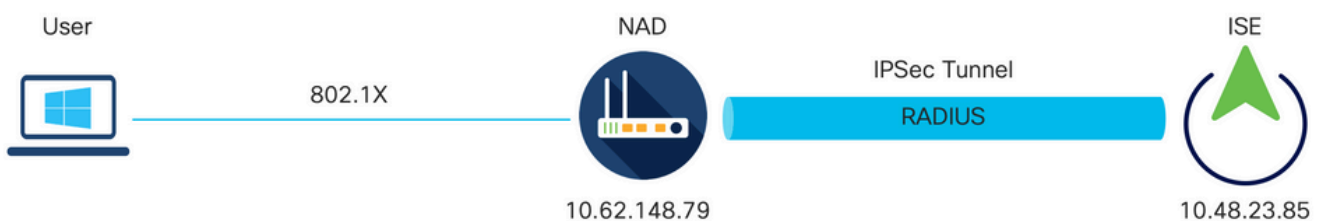
Phase Two Settings
Configure Native IPSec SA Configuration security settings to protect IP traffic between two endpoints.

Encryption Algorithm: aes256
Hash Algorithm: sha512
DH Group (optional): GROUP16
Re-key time (optional): 14400

Cancel Save

كراشمل X.509 حات فم ةقداصمب IPsec IKEv2 ق فن نيوكت اقبسم

ةكبش لل يطي طختلا مسرلا



ةكبش لل يطي طختلا مسرلا

IOS-XE لوحمل رماوالا رطس ةهجاو نيوكت

تاهجاوالا نيوكت

تلکش تنک یغبنی لقألا یلع نراق دحاو کلذ دعب ،دعب نراق لکش ی ال حاتفم IOS-XE ل ل ن
لاثم یلی امی ف:

```
interface Vlan480
 ip address 10.62.148.79 255.255.255.128
 negotiation auto
 no shutdown
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 1,480
 switchport mode trunk
!
```

نم VPN ةكبش قفن عاشنإل همادختسا بجی یذلا دیعبلا ریظنلاب لاصتا دوجو نم دکأت
یساسألا لاصتالا نم ققحتلل ping رمألا مادختسا كنكمی .عقوم یلإ عقوم

IKEv2 حرتقم نیوكت

لیكشت لماش یف رمأ <name> ضرع crypto ikev2 ل ،ةسایس ل IKEv2 ل تلکش in order to تلخد
لاثم یلی امی ف .بولسأ

```
crypto ikev2 proposal PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 16
!
```

ریفشتلل IKEv2 جهن نیوكت

لماش یف رمأ <name> ةسایس ل crypto ikev2 ل ،ةسایس ل IKEv2 ل تلکش in order to تلخد
بولسأ لیكشت

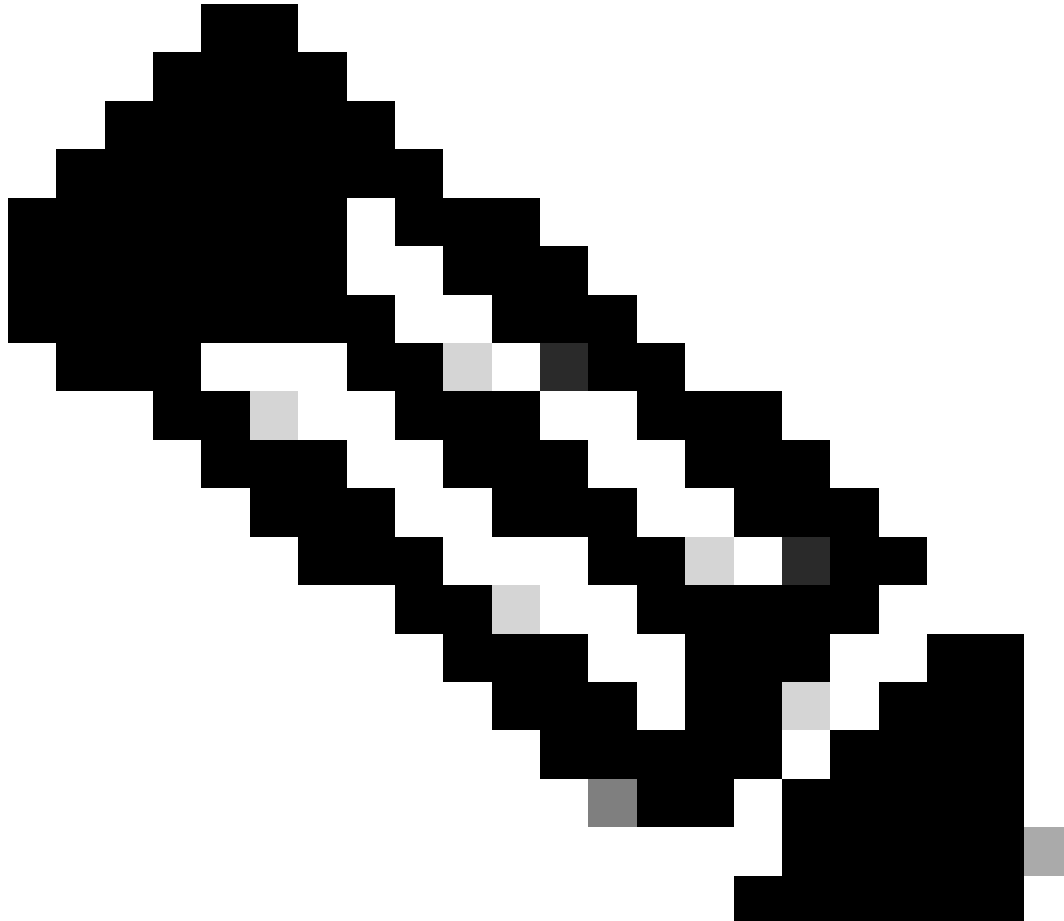
```
crypto ikev2 policy POLICY
 proposal PROPOSAL
```

ریفشتلل IKEv2 فیرعت فلم نیوكت

لیكشت لماش یف رمأ <name> crypto ikev2 profile ل ،بولسأ ل IKEv2 ل تلکش in order to تلخد
بولسأ

```
crypto ikev2 profile PROFILE
```

```
match address local 10.62.148.79
match identity remote address 10.48.23.85 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
```




IKE هو كة صاخلا هتويوه ةداهش نم CN لقح يضرارتفا لكش ب ISE مدختسي :ةطحالم
فيريغت فلم يف "دعب نع ةيوهال قباطت" مسق يف ببسلا اذهلو .IKEv2 ضوافت يف
ISE ب صاخلا FQDN وأ لاجملل ةبسانملا ةميقل او FQDN عون ديدحت كمزلي ،IKEv2.

ةيمهالا تاذ VPN رورم ةكحل (ACL) لوصولا يف مكحت ةمئاق نيوكت

اهتياحم بجي يتل رورملا ةكحل ديدحتل ةامسمل وأ ةعسوملا لوصولا ةمئاق مدختسا
لاثم يلي اميف .ريفتلاب

```
ip access-list extended 100
```

10 permit ip host 10.62.148.79 host 10.48.23.85

 ردم ل IP نيوانع VPN رورم ةكرل لوصولا يف مكحتلا ةمئاق مدختست: ةظالم NAT. دعب ةهولواو

ليوحت ةومجم نيوكت

رمأل لخدأ، (تايمزراولواو نامأل تالوكوتورب نم ةلوبقم ةومجم) IPsec ليوحت ةومجم ديحتل لاثم يلي اميف. ماعال نيوكتلا عضو يف crypto ipsec transform-set

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

ةهولواو لعل اهقيبطتو ريفشت ةطيرخ نيوكت

بولسأ ليكشت ةطيرخ crypto ل لخدأو لخددم ةطيرخ ريفشت تلددع وأ تقلخ in order to تلخد بواول ضعب كانه، ريفشتلا ةطيرخ لخدأ لمككي يتح. رمأل ليكشت لماش crypto map ل لخدأ دك اهفيرعت بجي يتل:

- مه عالؤه. اهليل ةيمحملا رورملا ةكره هيجوت ةداع نكمي يتل IPsec رئاظن ديحت بجي ةطيرخ لخدأ يف IPsec ريطان ديحتل. ةمدخ دعاسم عاشنإ مهعم نكمي نيذل انارقالا set peer. رمأل لخدأ، ريفشت
- in order to تلخد. ةيمحملا رورملا ةكره عم مادختسالل ةلوبقملا ليوحتلا تاعومجم ديحت بجي لخددم ةطيرخ crypto ل عم تلمعتسا تنك عيطتسي نأ ةومجم ليوحتلا تنيع in order to، رمأل set-ليوحت ةومجملا
- ل ةمئاق ذفنم عسوم تنيع in order to تلخد. اهتياحم بجي يتل رورملا ةكره ديحت بجي. رمأل ناووع match ل، لخددم ةطيرخ crypto

لاثم يلي اميف:

```
crypto map MAP-IKEV2 10 ipsec-isakmp
set peer 10.48.23.85
set transform-set SET
set pfs group16
set ikev2-profile PROFILE
match address 100
```

ةهولواو لعل اقبسوم ةدحملا ريفشتلا ةطيرخ ةومجم قيبطت يف ةريخالأ ةوطخل لثمتت. رمأل ليكشت نراق crypto map ل، اذه تقلب in order to تلخد

```
interface Vlan480
```



```
crypto map MAP-IKEV2
```

IOS-XE يئاهن لال نيوكتال

ليكشت CLI حاتفم IOS-XE يئاهن لال انه:

```
aaa new-model
!
aaa group server radius ISE
  server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
  client 10.48.23.85
  server-key cisco
!
dot1x system-auth-control
!
crypto ikev2 proposal PROPOSAL
  encryption aes-cbc-256
  integrity sha512
  group 16
!
crypto ikev2 policy POLICY
  proposal PROPOSAL
!
crypto ikev2 profile PROFILE
  match address local 10.62.148.79
  match identity remote address 10.48.23.85 255.255.255.255
  authentication remote pre-share key cisco123
  authentication local pre-share key cisco123
!
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
  mode tunnel
!
crypto map MAP-IKEV2 10 ipsec-isakmp
  set peer 10.48.23.85
  set transform-set SET
  set pfs group16
  set ikev2-profile PROFILE
  match address 100
!
interface GigabitEthernet1/0/23
  switchport trunk allowed vlan 1,480
  switchport mode trunk
!
interface Vlan480
  ip address 10.62.148.79 255.255.255.128
  crypto map MAP-IKEV2
!
ip access-list extended 100
  10 permit ip host 10.62.148.79 host 10.48.23.85
!
```

```
radius server ISE33-2
address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
key cisco
!
```

ISE نيوكت

ISE ىل ع IP ناووع نيوكت

ge0. م عدد م تي ال ،رم اوأل رطس ةهجاو نم ge1-GE5 ةهجاوأل ىل ع ناووعأل نيوكت بجي

```
interface GigabitEthernet 1
ip address 10.48.23.85 255.255.255.0
ipv6 address autoconfig
ipv6 enable
```



ةهجاوأل ىل ع IP ناووع نيوكت دع ب قي بطتأل ليغشت ةداع| م مت :ةظحال م
ISE تامدخ ليغشت ةداع| ىل ع IP ناووع ريغت ي دوي دق %
IP؟ ناووع ريغت عم ةعباتأل ديرت له Y/N [N]: Y

IPsec قفن نيوكت

ةفاض| قوف رقنا .يصلأل IPsec > IPsec > تالوكوتورب > تاداع| > ماظن > ةراد| ىل ع لقتنا
ربعمأل اوغانقلال مادختساب IP ناووع نيوكتب مقو ،IPsec قفن يهنت ي تلل ،ةدقعلال ددح
ماظن ةداهش رتخاو X.509 ةداهش ةئيه ىل ع ةقداصلال دادع| ددح .IPsec ةهجاوو يضارتفال
ةتبتملال ةداهشأل

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings

Posture >
Profiling
Protocols >

EAP-FAST >
EAP-TLS
PEAP
EAP-TTLS
RADIUS

IPSec >
Legacy IPSec (ESR)
Native IPSec

Native IPSec Configuration > New

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

Node-Specific Settings

Select Node
ise332

NAD IP Address with Mask
10.62.147.79/32

Default Gateway (optional)
10.48.23.1

Native IPSec Traffic Interface
Gigabit Ethernet 1

Authentication Settings

Pre-shared Key

X.509 Certificate

قربان نيوكت كنكمي، نارايخ كيدل، عقاولا ي ف. يرايخ| نيوكت يه ةيضارتفالا ةباوبلا
ماظن ي ف راسم تيبتت موقت يتلاو، ةيلصال IPsec مدختسم ةهجاو ي ف ةيضارتفا
show running-config ي ف راسملا اذه حضف متي ال. يساسال ليغشتلا

```
ise332/admin#show running-config | include route
ise332/admin#
```

<#root>

```
ise332/admin#show ip route
```

Destination Gateway Iface

10.48.23.0/24 0.0.0.0 eth1

default 10.48.60.1 eth0

10.48.60.0/24 0.0.0.0 eth0

10.62.148.79 10.48.23.1 eth1

169.254.2.0/24 0.0.0.0 cni-podman1

169.254.4.0/24 0.0.0.0 cni-podman2

```
ise332/admin#
```

ققحيس اذهو، ISE ىلع ايودي راسملا نيوكتو ةغراف ةيضارتفالا ةباوبلا كرت وه رخا رايخ

هس فن ريثأتلا:

```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route
```

```
Destination Gateway Iface
-----
10.48.23.0/24 0.0.0.0 eth1
10.62.148.79 10.48.23.1 eth1
default 10.48.60.1 eth0
10.48.60.0/24 0.0.0.0 eth0
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

قباطت نأ بجي. لولألا ةلحرمل تاداعإ نيوكت. IPsec ق فنل ةماعل تاداعإل نيوكت مت يتل تاداعإل عم ةيناثلل ةلحرمل تاداعإو لولألا ةلحرمل تاداعإو ةماعل تاداعإل مت يتل تاداعإل عم ةيناثلل ةلحرمل تاداعإو لولألا ةلحرمل تاداعإل نيوكت.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows the navigation menu with 'IPSec' selected under 'Protocols'. The main content area is titled 'General Settings' and contains several configuration fields:

- IKE Version: IKEv2
- Mode: Tunnel
- ESP/AH Protocol: esp
- IKE Reauth Time (optional): 86400
- Phase One Settings: Configure IKE SA Configuration security settings to protect communications between two IKE daemons.
- Encryption Algorithm: aes256
- Hash Algorithm: sha512
- DH Group: GROUP16
- Re-key time (optional): 14400

ظفح ةقطقو دادعإ ةيلمع ةيناثلل ةلحرمل تلاكش.

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings

Posture >
Profiling
Protocols >

EAP-FAST >
EAP-TLS
PEAP
EAP-TTLS
RADIUS

IPSec >
Legacy IPSec (ESR)
Native IPSec

Endpoint Scripts >
Proxy
SMTP Server

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

Encryption Algorithm
aes256

Hash Algorithm
sha512

DH Group
GROUP16

Re-key time (optional)
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)
GROUP16

Re-key time (optional)
14400

Cancel Save

ةحصل ال نم ققحت ال

وأ MAB ةقداصم ذيفنت وأ test aaa رمأل مدختسأ IPsec ق فن ربع لمعي RADIUS نأ نم دكأت لل ةيلعفل ال 1X. 802 ةقداصم

```
KSEC-9248L-1#test aaa group ISE alice Krakow123 new-code
User successfully authenticated
```

USER ATTRIBUTES

```
username 0 "alice"
vn 0 "vn1"
security-group-tag 0 "000f-00"
KSEC-9248L-1#
```

ال IOS-XE نم ققحت ال

<#root>

KSEC-9248L-1#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/f/ivrf	Status
1	10.62.148.79/500	10.48.23.85/500	none/none	

READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:16, Auth sign: RSA, Auth verify: R
Life/Active Time: 86400/1439 sec

IPv6 Crypto IKEv2 SA

KSEC-9248L-1#

show crypto ipsec sa

interface: Vlan480

Crypto map tag: MAP-IKEV2, local addr 10.62.148.79

protected vrf: (none)

local ident (addr/mask/prot/port): (10.62.148.79/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (10.48.23.85/255.255.255.255/0/0)

current_peer 10.48.23.85 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1

#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.62.148.79, remote crypto endpt.: 10.48.23.85

plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb Vlan480

current outbound spi: 0xC17542E9(3245687529)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xF7A68F69(4154888041)

transform: esp-256-aes esp-sha512-hmac ,

in use settings = {Tunnel, }

conn id: 72, flow_id: SW:72, sibling_flags 80000040, crypto map: MAP-IKEV2

sa timing: remaining key lifetime (k/sec): (4173813/84954)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xC17542E9(3245687529)
transform: esp-256-aes esp-sha512-hmac ,
in use settings ={Tunnel, }
conn id: 71, flow_id: SW:71, sibling_flags 80000040, crypto map: MAP-IKEV2
sa timing: remaining key lifetime (k/sec): (4173813/84954)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

```
KSEC-9248L-1#
KSEC-9248L-1#show crypto session
Crypto session current status
```

```
Interface: Vlan480
Profile:
```

PROFILE

Session status:

UP-ACTIVE

```
Peer: 10.48.23.85 port 500
Session ID: 5
IKEv2 SA: local 10.62.148.79/500 remote 10.48.23.85/500
```

Active

```
IPSEC FLOW: permit ip host 10.62.148.79 host 10.48.23.85
Active SAs: 2, origin: crypto map
```

KSEC-9248L-1#

إدارة إعدادات ISE

إعدادات إعدادات ISE

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Native IPSec Configuration

Establish security associations between Cisco ISE Policy Service Nodes (PSNs) and Network Access Devices (NADs) across an IPSec tunnel using IKEv1 and IKEv2 protocols. Ensure that the IPSec configurations on Cisco ISE and the NADs are the same.

Rows/Page 1 << 1 >>

Duplicate Edit Add Disable Remove

ISE Nodes	NAD IP Address	Tunnel Status	IPSec Interface	Authentication Type	IKE Version
<input type="checkbox"/> Ise332	10.62.148.79/32	<input checked="" type="checkbox"/> ESTABLISHED	GigabitEthernet 1	X.509	2

(رم أوألا رطس ةهجاو) CLI نم قف نلا ةلا ح نم ققحتلل قيبطتلل ل configure ise رمألا مدختسأ

<#root>

ise332/admin#application configure ise

Selection configuration option

- [1]Reset M&T Session Database
- [2]Rebuild M&T Unusable Indexes
- [3]Purge M&T Operational Data
- [4]Reset M&T Database
- [5]Refresh Database Statistics
- [6]Display Profiler Statistics
- [7]Export Internal CA Store
- [8]Import Internal CA Store
- [9]Create Missing Config Indexes
- [10]Create Missing M&T Indexes
- [12]Generate Daily KPM Stats
- [13]Generate KPM Stats for last 8 Weeks
- [14]Enable/Disable Counter Attribute Collection
- [15]View Admin Users
- [16]Get all Endpoints
- [19]Establish Trust with controller
- [20]Reset Context Visibility
- [21]Synchronize Context Visibility With Database
- [22]Generate Heap Dump
- [23]Generate Thread Dump
- [24]Force Backup Cancellation
- [25]CleanUp ESR 5921 IOS Crash Info Files
- [26]Recreate undotablespace
- [27]Reset Upgrade Tables
- [28]Recreate Temp tablespace
- [29]Clear Sysaux tablespace
- [30]Fetch SGA/PGA Memory usage
- [31]Generate Self-Signed Admin Certificate
- [32]View Certificates in NSSDB or CA_NSSDB
- [33]Recreate REPLUGINS tablespace
- [34]View Native IPsec status
- [0]Exit

34

7212b70a-1405-429a-94b8-71a5d4beb1e5: #114,

ESTABLISHED

, IKEv2, 0ca3c29e36290185_i 08c7fb6db177da84_r*
local 'CN=ise332.example.com' @ 10.48.23.85[500]
remote '10.62.148.79' @ 10.62.148.79[500]
AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096
established 984s ago, rekeying in 10283s, reauth in 78609s
net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5: #58, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-256/HMAC_S
installed 984s ago, rekeying in 12296s, expires in 14856s
in c17542e9, 100 bytes,

1 packets

, 983s ago
out f7a68f69, 100 bytes,

1 packets

, 983s ago

local 10.48.23.85/32
remote 10.62.148.79/32

اهحال صإو ءاطخأل فاشك تسأ

اهحال صإو IOS-XE ءاطخأ فاشك تسأ

نيك متلل ءاطخأل حي حصت

<#root>

KSEC-9248L-1#

debug crypto ikev2

IKEv2 default debugging is on
KSEC-9248L-1#

debug crypto ikev2 error

IKEv2 error debugging is on
KSEC-9248L-1#

debug crypto ipsec

Crypto IPSEC debugging is on
KSEC-9248L-1#

debug crypto ipsec error

Crypto IPSEC Error debugging is on
KSEC-9248L-1#

IOS-XE ىل ءلماعل ءاطخأل حي حصت نم ءلماك ءومجم

```
Apr 25 18:57:36.572: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 10.62.148.79:500, remote= 10.48.23.85:500,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0,
protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
lifedur= 86400s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Searching Policy with fvrf 0, local address 10.62.148.79
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Found Policy 'POLICY'
Apr 25 18:57:36.573: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Start PKI Session
Apr 25 18:57:36.574: IKEv2:(SA ID = 1):[PKI -> IKEv2] Starting of PKI Session PASSED
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public key,
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Compu
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH key
```

Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKEv2 initiator - no config data to send in IKE_SA_INIT message
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_SA_INIT message
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial negotiation)
Num. transforms: 4
AES-CBC SHA512 SHA512 DH_GROUP_4096_MODP/Group 16

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Insert SA

Apr 25 18:57:36.640: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(Unknown -)

Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Verify SA init message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificate
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the trustpoint KrakowCA
Apr 25 18:57:36.643: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the trustpoint PASSED
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):Checking NAT discovery
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):NAT not found
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret key,
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computed
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH secret
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKD
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculated
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Completed SA init exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Generate my authentication data
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication data generated
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Get my authentication method
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):My authentication method is 'RSA'
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Sign authentication data
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting private key
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of private key PASSED
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Sign authentication data
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Signing of authentication data PASSED
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Authentication material has been successfully signed
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_AUTH message
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Constructing IDi payload: '10.62.148.79' of type ID_IPV4_ADDR
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured trustpoint(s)
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Get Public Key Hashes of trustpoints
Apr 25 18:57:36.946: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of Public Key Hashes of trustpoints PASSED
Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotiation)
Num. transforms: 3
AES-CBC SHA512 Don't use ESN

Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):Building packet for encryption.
Payload contents:
VID IDi CERT CERTREQ AUTH SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO)

Apr 25 18:57:36.947: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148.79:500]

Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Apr 25 18:57:37.027: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
IDr CERT AUTH SA TSi TSr

Apr 25 18:57:37.029: IKEv2:(SESSION ID = 5,SA ID = 1):Process auth response notify
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching policy based on peer's identity 'cn=ise332.example.com'
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching Policy with fvrf 0, local address 10.62.148.79
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Found Policy 'POLICY'
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's policy
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's policy verified
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Get peer's authentication method
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's authentication method is 'RSA'
Apr 25 18:57:37.033: IKEv2:Validation list created with 1 trustpoints
Apr 25 18:57:37.033: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating certificate chain
Apr 25 18:57:37.043: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain PASSED
Apr 25 18:57:37.043: IKEv2:(SESSION ID = 5,SA ID = 1):Save pubkey
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's authentication data
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication data generated
Apr 25 18:57:37.045: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Verify signed authentication data
Apr 25 18:57:37.047: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of signed authentication data PASSED
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_AUTH message
Apr 25 18:57:37.050: IKEv2:(SESSION ID = 5,SA ID = 1):IPSec policy validate request sent for profile PR1

Apr 25 18:57:37.051: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.62.148.79:0, remote= 10.48.23.85:0,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0,
protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0

Apr 25 18:57:37.051: Crypto mapdb : proxy_match
src addr : 10.62.148.79
dst addr : 10.48.23.85
protocol : 0
src port : 0
dst port : 0

Apr 25 18:57:37.051: (ipsec_process_proposal)Map Accepted: MAP-IKEV2, 10

Apr 25 18:57:37.051: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Callback received for SA

Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Close PKI Session
Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[PKI -> IKEv2] Closing of PKI Session PASSED
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):IKEV2 SA created; inserting SA into database. SA ID= 1
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Session with IKE ID PAIR (cn=ise332.example.com, local address 10.62.148.79)
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 0,SA ID = 0):IKEv2 MIB tunnel started, tunnel index 1
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Load IPSEC key material
Apr 25 18:57:37.054: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into database
Apr 25 18:57:37.054: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Apr 25 18:57:37.054: Crypto mapdb : proxy_match
src addr : 10.62.148.79
dst addr : 10.48.23.85
protocol : 256

```
src port : 0
dst port : 0
Apr 25 18:57:37.054: IPSEC:(SESSION ID = 5) (crypto_ipsec_create_ipsec_sas) Map found MAP-IKEV2, 10
Apr 25 18:57:37.054: IPSEC:(SESSION ID = 5) (crypto_ipsec_sa_find_ident_head) reconnecting with the same
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (get_old_outbound_sa_for_peer) No outbound SA found for peer
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (create_sa) sa created,
(sa) sa_dest= 10.62.148.79, sa_proto= 50,
sa_spi= 0xF7A68F69(4154888041),
sa_trans= esp-aes 256 esp-sha512-hmac , sa_conn_id= 72
sa_lifetime(k/sec)= (4608000/86400),
(identity) local= 10.62.148.79:0, remote= 10.48.23.85:0,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0
Apr 25 18:57:37.055: ipsec_out_sa_hash_idx: sa=0x46CFF474, hash_idx=232, port=500/500, addr=0x0A3E944F/
Apr 25 18:57:37.055: crypto_ipsec_hook_out_sa: ipsec_out_sa_hash_array[232]=0x46CFF474
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (create_sa) sa created,
(sa) sa_dest= 10.48.23.85, sa_proto= 50,
sa_spi= 0xC17542E9(3245687529),
sa_trans= esp-aes 256 esp-sha512-hmac , sa_conn_id= 71
sa_lifetime(k/sec)= (4608000/86400),
(identity) local= 10.62.148.79:0, remote= 10.48.23.85:0,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0
Apr 25 18:57:37.056: IPSEC: Expand action denied, notify RP
Apr 25 18:57:37.056: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA
Apr 25 18:57:37.056: IKEv2:(SESSION ID = 5,SA ID = 1):Checking for duplicate IKEv2 SA
Apr 25 18:57:37.057: IKEv2:(SESSION ID = 5,SA ID = 1):No duplicate IKEv2 SA found
```

اه حال ص او ISE اءاطخأ فاشك تسأ

نيك مت لل اءاطخأ ال اءي حصت

مكحت لل ءءو ال اءاطخأ ال اءي حصت ءءءاطل ISE، ال ءه نيك مت متي ل ءه نيم ءءاطخأ ءءو ال
رم ال اف:

```
ise332/admin#show logging application strongswan/charon.log tail
```

ISE ال ءه لءءاطخأ ال اءي حصت نم ءه لءءءو ءءو مء

```
Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 13[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 0000000000000000_r
Apr 26 00:57:36 13[MGR] created IKE_SA (unnamed)[114]
Apr 26 00:57:36 13[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (774 bytes)
Apr 26 00:57:36 13[ENC] <114> parsed IKE_SA_INIT request 0 [ SA KE No V V V N(NATD_S_IP) N(NATD_D_IP)
Apr 26 00:57:36 13[CFG] <114> looking for an IKEv2 config for 10.48.23.85...10.62.148.79
Apr 26 00:57:36 13[CFG] <114> candidate: 10.48.23.85...10.62.148.79, prio 3100
Apr 26 00:57:36 13[CFG] <114> found matching ike config: 10.48.23.85...10.62.148.79 with prio 3100
Apr 26 00:57:36 13[IKE] <114> local endpoint changed from 0.0.0.0[500] to 10.48.23.85[500]
Apr 26 00:57:36 13[IKE] <114> remote endpoint changed from 0.0.0.0 to 10.62.148.79[500]
Apr 26 00:57:36 13[IKE] <114> received Cisco Delete Reason vendor ID
```

Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:2d:30:32
Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:43:2d:52:
Apr 26 00:57:36 13[IKE] <114> received Cisco FlexVPN Supported vendor ID
Apr 26 00:57:36 13[IKE] <114> 10.62.148.79 is initiating an IKE_SA
Apr 26 00:57:36 13[IKE] <114> IKE_SA (unnamed)[114] state change: CREATED => CONNECTING
Apr 26 00:57:36 13[CFG] <114> selecting proposal:
Apr 26 00:57:36 13[CFG] <114> proposal matches
Apr 26 00:57:36 13[CFG] <114> received proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MO
Apr 26 00:57:36 13[CFG] <114> configured proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512
Apr 26 00:57:36 13[CFG] <114> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MO
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=KrakowCA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "DC=com, DC=example, CN=LAB CA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Endpoint Sub CA - ise33
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Node CA - ise332"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "O=Cisco, CN=Cisco Manufacturing CA SHA2"
Apr 26 00:57:36 13[ENC] <114> generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) CE
Apr 26 00:57:36 13[NET] <114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500] (809 bytes)
Apr 26 00:57:36 13[MGR] <114> checkin IKEv2 SA (unnamed)[114] with SPIs 0ca3c29e36290185_i 08c7fb6db177
Apr 26 00:57:36 13[MGR] <114> checkin of IKE_SA successful
Apr 26 00:57:36 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 09[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 08c7fb6db177da84_r
Apr 26 00:57:36 09[MGR] IKE_SA (unnamed)[114] successfully checked out
Apr 26 00:57:36 09[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (1488 bytes)
Apr 26 00:57:37 09[ENC] <114> parsed IKE_AUTH request 1 [V IDi CERT CERTREQ AUTH SA TSi TSr N(INIT_CON
Apr 26 00:57:37 09[IKE] <114> received cert request for "CN=KrakowCA"
Apr 26 00:57:37 09[IKE] <114> received end entity cert "CN=KSEC-9248L-1.example.com"
Apr 26 00:57:37 09[CFG] <114> looking for peer configs matching 10.48.23.85[%any]...10.62.148.79[10.62.
Apr 26 00:57:37 09[CFG] <114> candidate "7212b70a-1405-429a-94b8-71a5d4beb1e5", match: 1/1/3100 (me/oth
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected peer config '7212b70a-1405-
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using certificate "CN=KSEC-9248L-1.e
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KSEC-9248L-1.example
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using trusted ca certificate "CN=Kra
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KrakowCA" key: 2048
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> reached self-signed root ca with a p
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checking certificate status of "CN=K
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> ocsf check skipped, no ocsf found
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate status is not available
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of '10.62.148.79' wit
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received ESP_TFC_PADDING_NOT_SUPPORT
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of 'CN=ise332.example
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending end entity cert "CN=ise332.e
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling rekeying in 11267s
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling reauthentication in 79593
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> maximum IKE_SA lifetime 19807s
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> looking for a child config for 10.48
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for us:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.48.23.85/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for othe
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.62.148.79/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> candidate "net-net-7212b70a-1405-429
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> found matching child config "net-net
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting proposal:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposal matches
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received proposals: ESP:AES_CBC_256/
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> configured proposals: ESP:AES_CBC_25
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected proposal: ESP:AES_CBC_256/HI
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> got SPI c17542e9
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for us:

Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for other
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 10
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 10
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using AES_CBC for encryption
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using HMAC_SHA2_512_256 for integrity
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding inbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xc17542e9, src 10.62.148.79 dst 10.48.23.85
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI c17542e9 and SPI f7a68f69
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC with integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 32 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding outbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xf7a68f69, src 10.48.23.85 dst 10.62.148.79
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI f7a68f69 and SPI c17542e9
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC with integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 0 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10.62.148.79/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10.62.148.79/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.48.23.85/32 === 10.48.23.85/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting a local address in traffic selector
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using host 10.48.23.85
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface name for index 22
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using 10.48.23.1 as nexthop and eth1 as interface
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> installing route: 10.62.148.79/32 via 10.48.23.1
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface index for eth1
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[ENC] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> generating IKE_AUTH response 1 [IDr=0, SA=7212b70a-1405-429a-94b8-71a5d4beb1e5, SPI=0xc17542e9, src=10.48.23.85, dst=10.62.148.79]
Apr 26 00:57:37 09[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin IKEv2 SA 7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin of IKE_SA successful
Apr 26 00:57:37 04[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500]

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلال دن تسمل