配置ISE 3.3本地IPsec以保護NAD (IOS-XE)通訊

目錄

簡介

本文檔介紹如何配置本機IPsec並對其進行故障排除，以保護思科身份服務引擎(ISE) 3.3 -網路訪問裝置(NAD)通訊。可以在交換機和ISE之間使用站點到站點（LAN到LAN） IPsec Internet Key Exchange Version 2 (IKEv2)隧道加密RADIUS流量。本文檔不包括RADIUS配置部分。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- 思科交換器組態
- 一般IPsec概念
- 一般RADIUS概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本17.6.5的Cisco Catalyst交換器C9200L
- 思科身分辨識服務引擎版本3.3
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

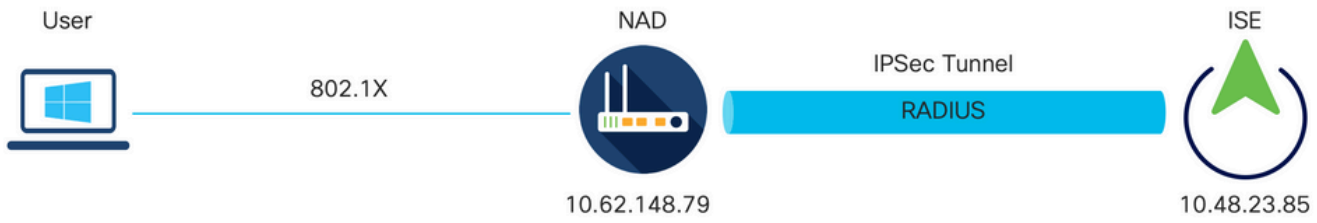
目標是保護使用不安全的MD5雜湊、RADIUS和具有IPsec的TACACS的協定。需要考慮的事實很少：

- Cisco ISE本地IPsec解決方案基於StrongSwan
- 在思科ISE介面上配置IPsec時，思科ISE和需要保護裝置之間會建立IPsec隧道以保護通訊。NAD應在Native IPsec Settings（本地IPsec設定）下單獨配置。
- 您可以定義預共用金鑰或使用X.509證書進行IPsec身份驗證。
- IPsec可在GigabitEthernet1到GigabitEthernet5介面上啟用。

本文檔主要介紹X.509證書身份驗證。「驗證與疑難排解」一節只專注於X.509憑證驗證，而預先共用金鑰驗證的偵錯應完全相同，且輸出只有差異。相同的命令也可用於驗證。

配置採用X.509證書身份驗證的IKEv2 IPsec隧道

網路圖表



網路圖表

IOS-XE交換機CLI配置

配置介面

如果尚未配置IOS-XE交換機介面，則至少應配置一個介面。以下是範例：

```
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
!
```

確儲存在與遠端對等體的連線，該連線應用於建立站點到站點VPN隧道。您可以使用ping驗證基本連線。

配置信任點

要配置IKEv2策略，請在全局配置模式下輸入crypto pki trustpoint <name>命令。 以下是範例：

> 注意：在IOS-XE裝置上安裝證書的方法有多種。在本例中，我們使用pkcs12檔案的導入，該檔案包含身份證書及其鏈

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

匯入憑證

要導入IOS-XE身份證書及其鏈，請在特權模式下輸入crypto pki import <trustpoint> pkcs12 <location> password <password>命令。 以下是範例：

```
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#
```

注意：即使證書不在文檔範圍內，也請確保IOS-XE身份證書的SAN欄位已填充其FQDN/IP地址。ISE要求對等證書具有SAN欄位。

為了驗證憑證已正確安裝：

```
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#
```

配置IKEv2方案

要配置IKEv2策略，請在全局配置模式下輸入crypto ikev2 proposal <name>命令。 以下是範例：

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

配置加密IKEv2策略

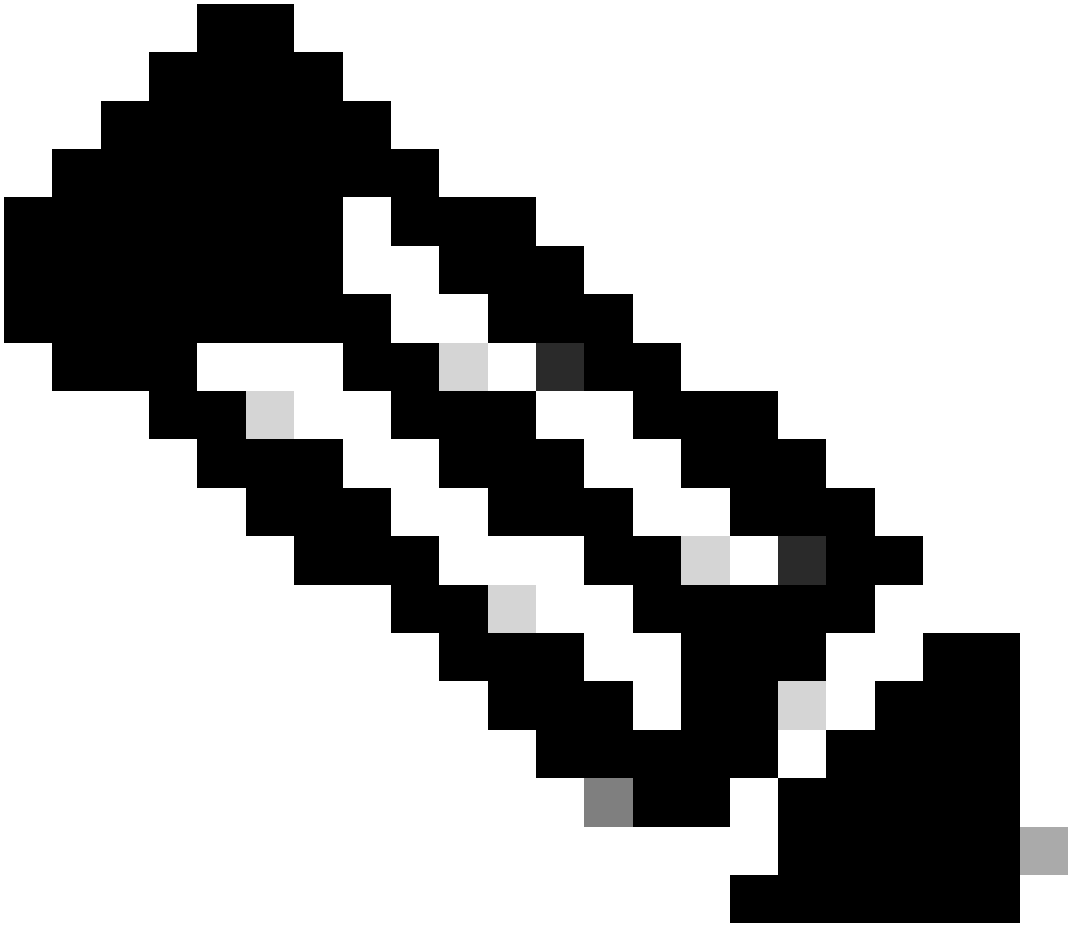
要配置IKEv2策略，請在全局配置模式下輸入crypto ikev2 policy <name>命令：

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

配置加密IKEv2配置檔案

要配置IKEv2配置檔案，請在全局配置模式下輸入crypto ikev2 profile <name>命令。

```
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
```



注意：預設情況下，ISE在IKEv2協商中使用CN欄位作為其自己的身份證書的IKE身份。因此，在IKEv2配置檔案的「匹配身份遠端」部分，您需要指定FQDN型別和域或ISE的FQDN的正確值。

為相關的VPN流量配置ACL

使用擴展或命名訪問清單以指定應受加密保護的流量。以下是範例：

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

注意：VPN流量的ACL在NAT後使用源和目標IP地址。

配置轉換集

要定義IPsec轉換集（安全協定和演算法的可接受組合），請在全局配置模式下輸入crypto ipsec transform-set命令。以下是範例：

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

配置加密對映並將其應用到介面

要建立或修改加密對映條目並進入加密對映配置模式，請輸入crypto map全局配置命令。要使加密對映條目完整，必須至少定義以下某些方面：

- 必須定義可向其轉發受保護流量的IPsec對等體。以下是可以建立SA的對等裝置。要在加密對映條目中指定IPsec對等體，請輸入set peer命令。
- 必須定義可用於受保護流量的轉換集。要指定可與加密對映條目一起使用的轉換集，請輸入set transform-set命令。
- 必須定義應該保護的流量。要為加密對映條目指定擴展訪問清單，請輸入match address命令。

以下是範例：

```
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
```

最後一步是將之前定義的加密對映集應用到介面。要應用此命令，請輸入crypto map介面配置命令：

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

IOS-XE最終配置

以下是最終的IOS-XE交換機CLI配置：

```
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 組態

在ISE上配置IP地址

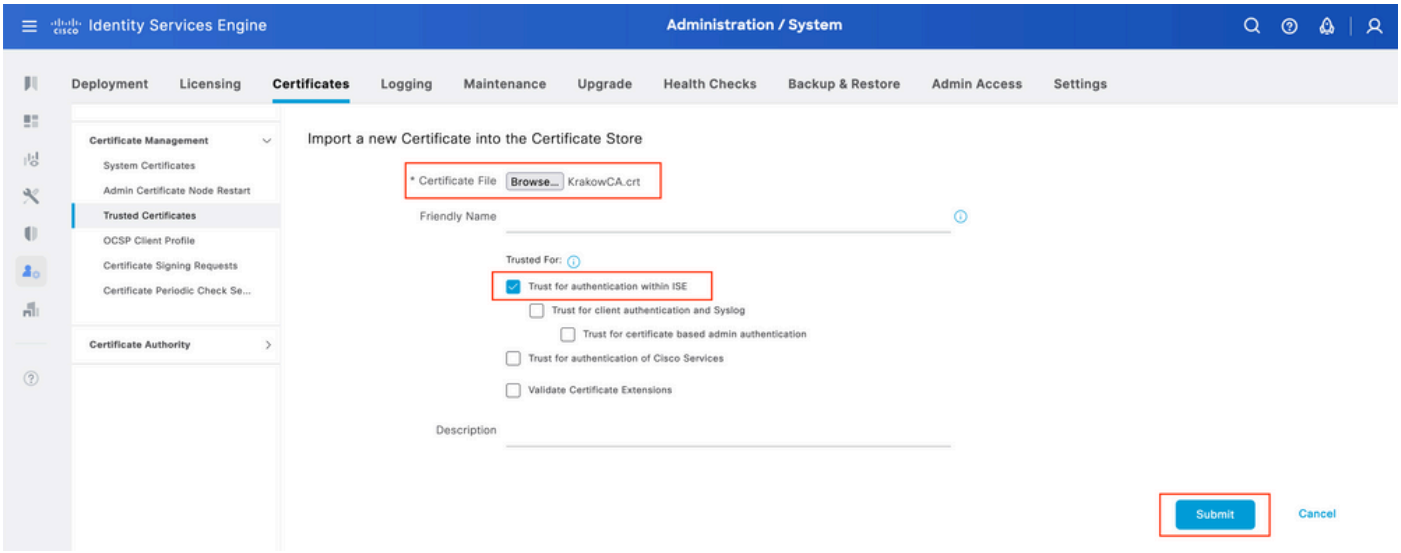
應該從CLI在介面GE1-GE5上配置地址，不支援GE0。

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

注意：在介面上配置了IP地址後，應用程式將重新啟動：
%更改IP地址可能導致ISE服務重新啟動
是否繼續更改IP地址？ Y/N [N]：Y

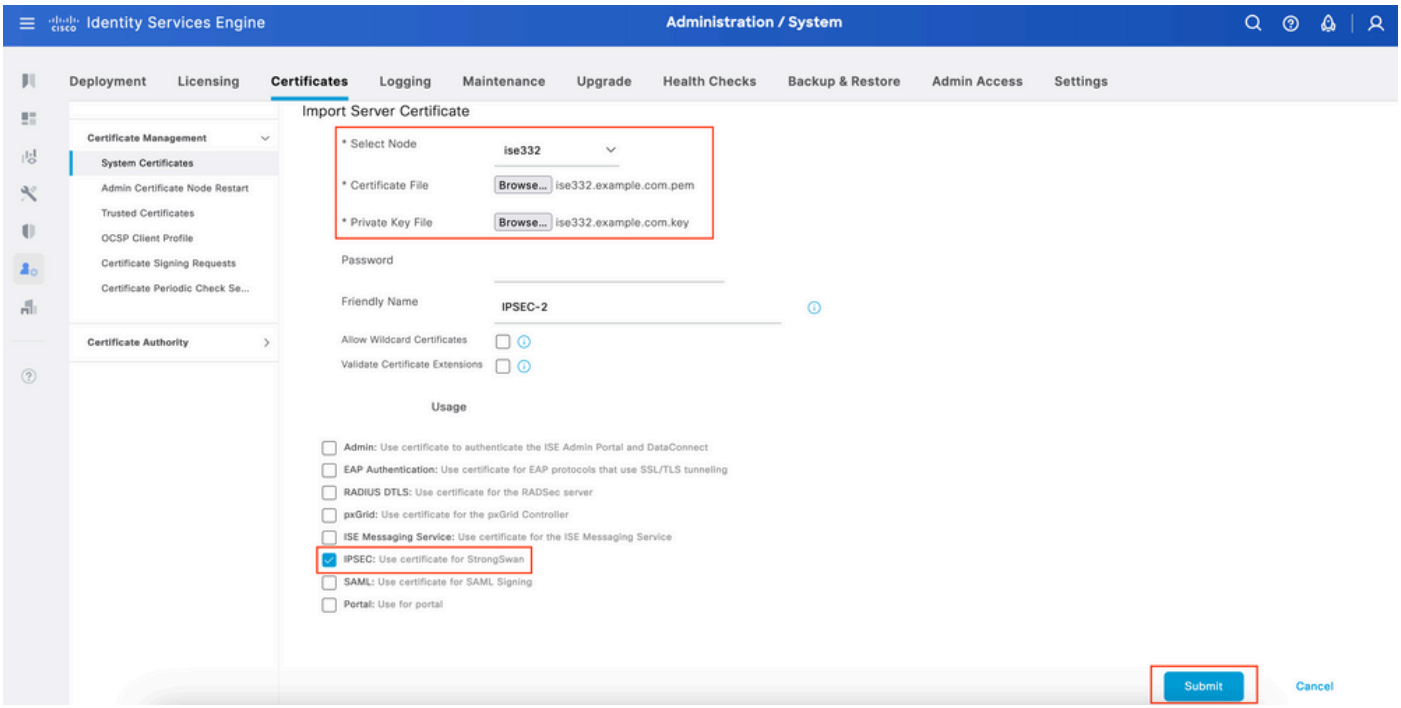
導入受信任的儲存證書

此步驟是確保ISE信任隧道建立時顯示的對等體證書所必需的。導航到管理>系統>證書>受信任證書。按一下「Import」（匯入）。按一下Browse並選擇已簽名ISE/IOS-XE身份證書的CA證書。確保選中Trust for authentication within ISE覈取方塊。按一下Submit。



匯入系統憑證

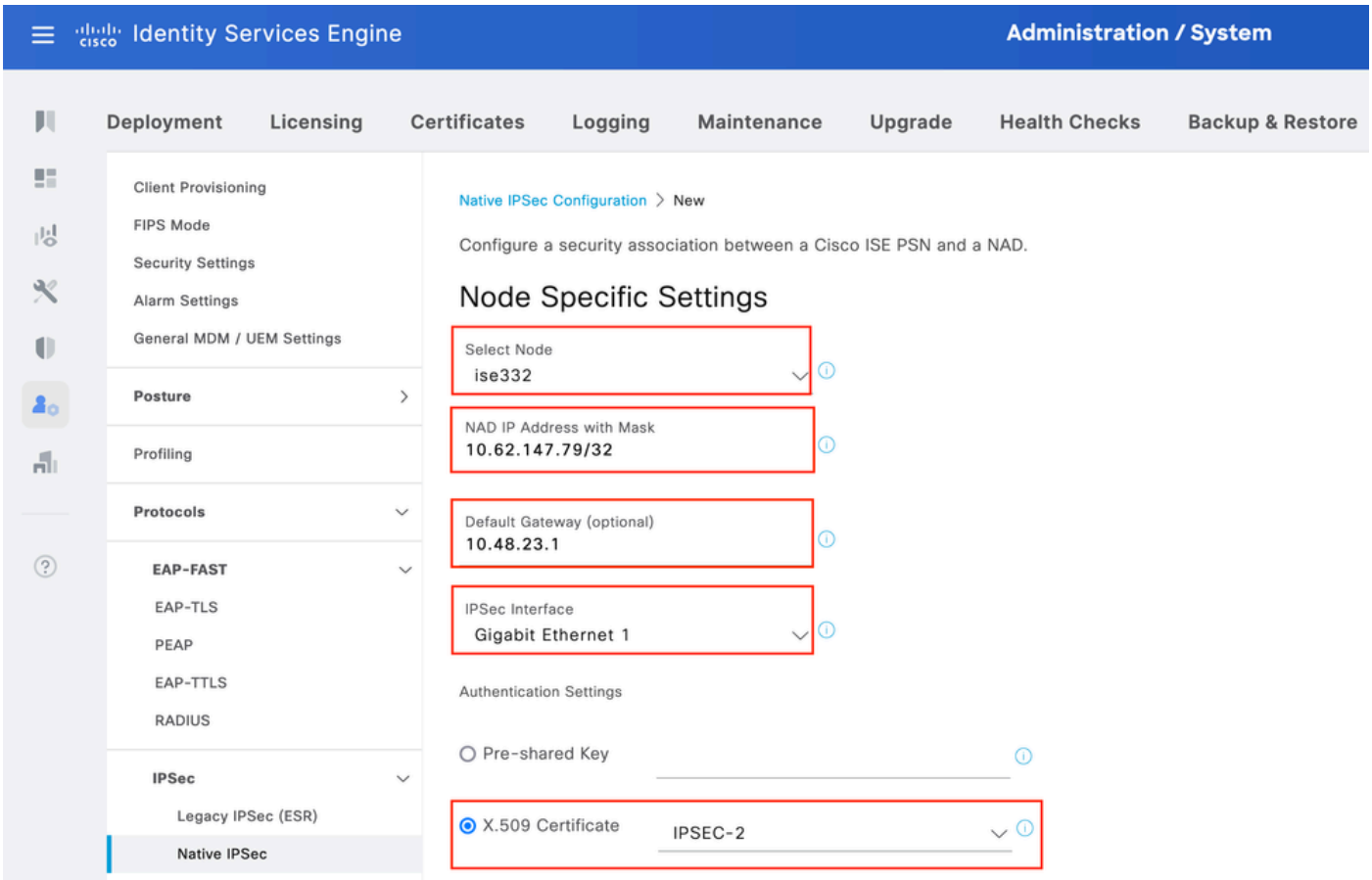
導航到管理>系統>證書>系統證書。選擇Node、Certificate File和Private key File Import。選中IPsec所對應的覈取方塊。按一下Submit。



注意：只有在「本地IPsec設定」下儲存網路訪問裝置後，證書才會安裝在StrongSwan上。

配置IPSec隧道

導航到管理>系統>設定>協定> IPsec >本地IPsec。按一下Add。選擇終止IPSec隧道的節點，配置帶掩碼的NAD IP地址、預設網關和IPSec介面。 選擇Authentication Setting as X.509 Certificate，然後選擇Certificate System Certificate Installed。



預設網關是可選配置。事實上，您有兩個選項，可以在本地IPsec UI中配置預設網關，從而在底層作業系統中安裝路由。此路由未在show running-config：中公開

```
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

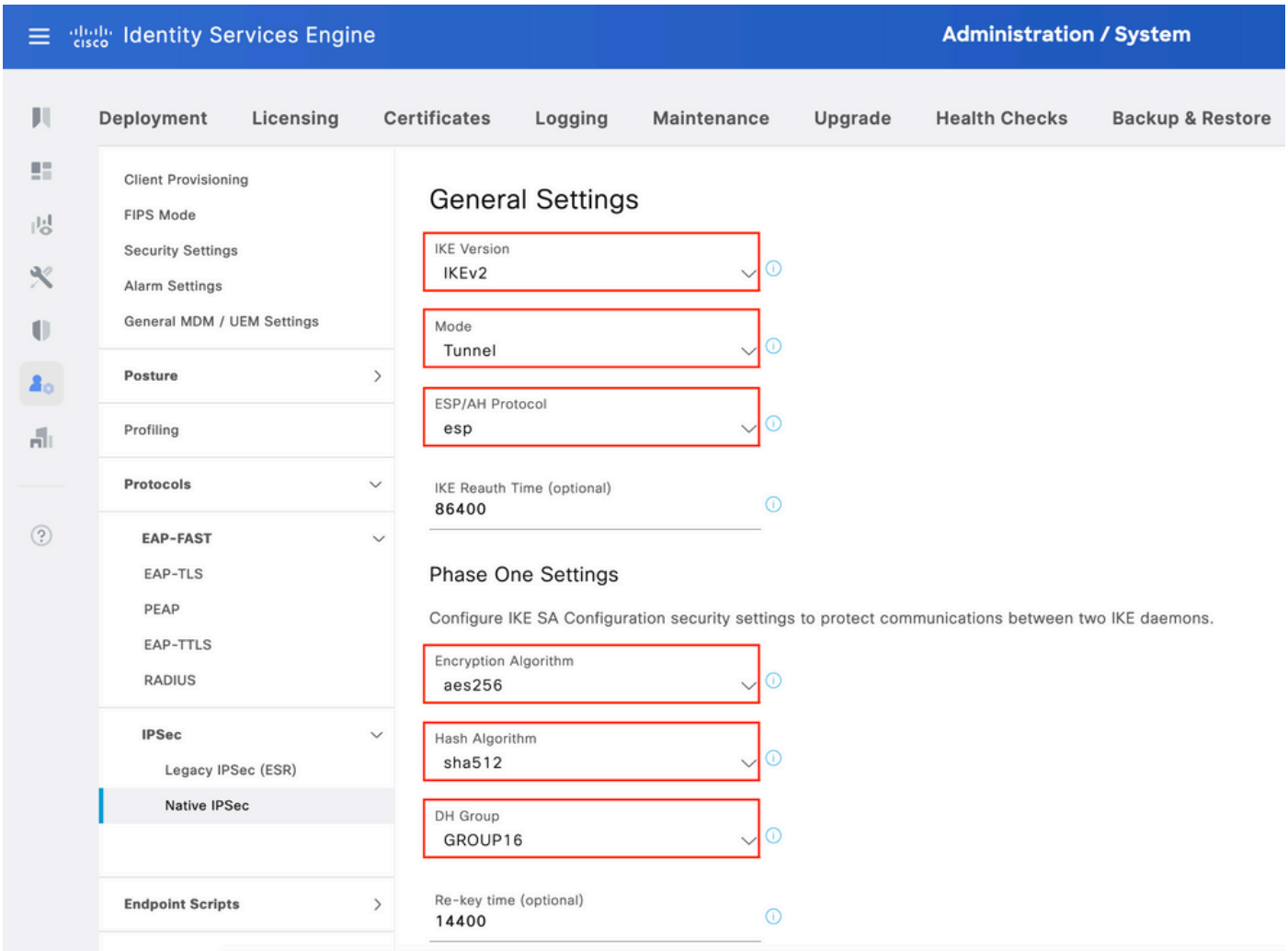
```
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

另一個選項是保留預設網關為空，並在ISE上手動配置路由，這將實現相同的效果：

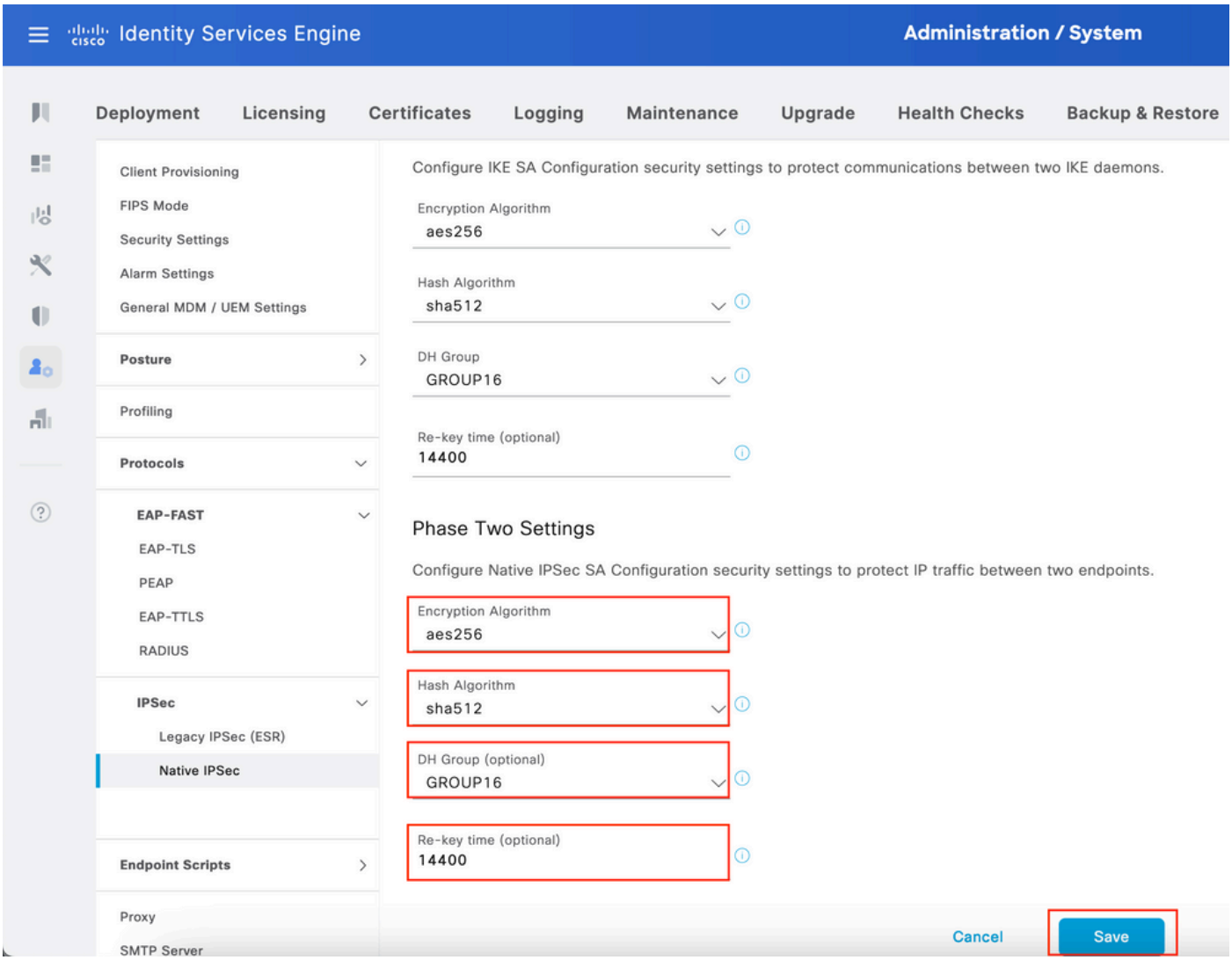
```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route

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#
```

配置IPSec隧道的常規設定。配置Phase One設定。常規設定、階段一設定和階段二設定應與IPSec隧道另一端上配置的設定匹配。

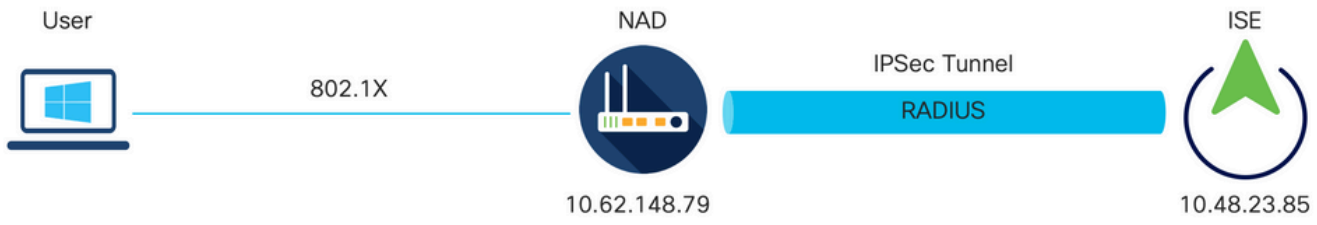


配置Phase Two Settings並按一下Save。



配置採用X.509預共用金鑰身份驗證的IKEv2 IPsec隧道

網路圖表



網路圖表

IOS-XE交換機CLI配置

配置介面

如果尚未配置IOS-XE交換機介面，則至少應配置一個介面。以下是範例：

```
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
!
```

確儲存在與遠端對等體的連線，該連線應用於建立站點到站點VPN隧道。您可以使用ping驗證基本連線。

配置IKEv2方案

要配置IKEv2策略，請在全局配置模式下輸入crypto ikev2 proposal <name>命令。 以下是範例：

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

配置加密IKEv2策略

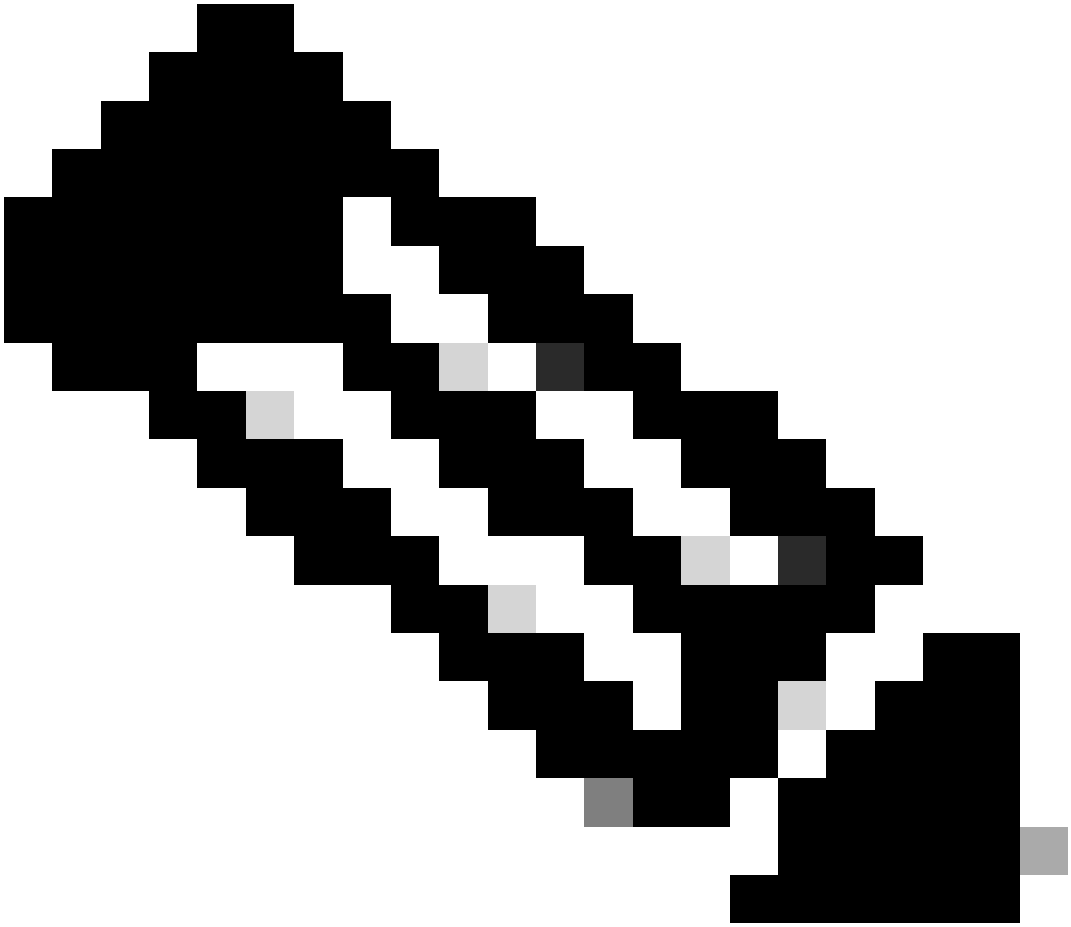
要配置IKEv2策略，請在全局配置模式下輸入crypto ikev2 policy <name>命令：

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

配置加密IKEv2配置檔案

要配置IKEv2配置檔案，請在全局配置模式下輸入crypto ikev2 profile <name>命令。

```
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
```



注意：預設情況下，ISE在IKEv2協商中使用CN欄位作為其自己的身份證書的IKE身份。因此，在IKEv2配置檔案的「匹配身份遠端」部分，您需要指定FQDN型別和域或ISE的FQDN的正確值。

為相關的VPN流量配置ACL

使用擴展或命名訪問清單以指定應受加密保護的流量。以下是範例：

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

注意：VPN流量的ACL在NAT後使用源和目標IP地址。

配置轉換集

要定義IPsec轉換集（安全協定和演算法的可接受組合），請在全局配置模式下輸入crypto ipsec transform-set命令。以下是範例：

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

配置加密對映並將其應用到介面

要建立或修改加密對映條目並進入加密對映配置模式，請輸入crypto map全局配置命令。要使加密對映條目完整，必須至少定義以下某些方面：

- 必須定義可向其轉發受保護流量的IPsec對等體。以下是可以建立SA的對等裝置。要在加密對映條目中指定IPsec對等體，請輸入set peer命令。
- 必須定義可用於受保護流量的轉換集。要指定可與加密對映條目一起使用的轉換集，請輸入set transform-set命令。
- 必須定義應該保護的流量。要為加密對映條目指定擴展訪問清單，請輸入match address命令。

以下是範例：

```
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
```

最後一步是將之前定義的加密對映集應用到介面。要應用此命令，請輸入crypto map介面配置命令：

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

IOS-XE最終配置

以下是最終的IOS-XE交換機CLI配置：

```
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 組態

在ISE上配置IP地址

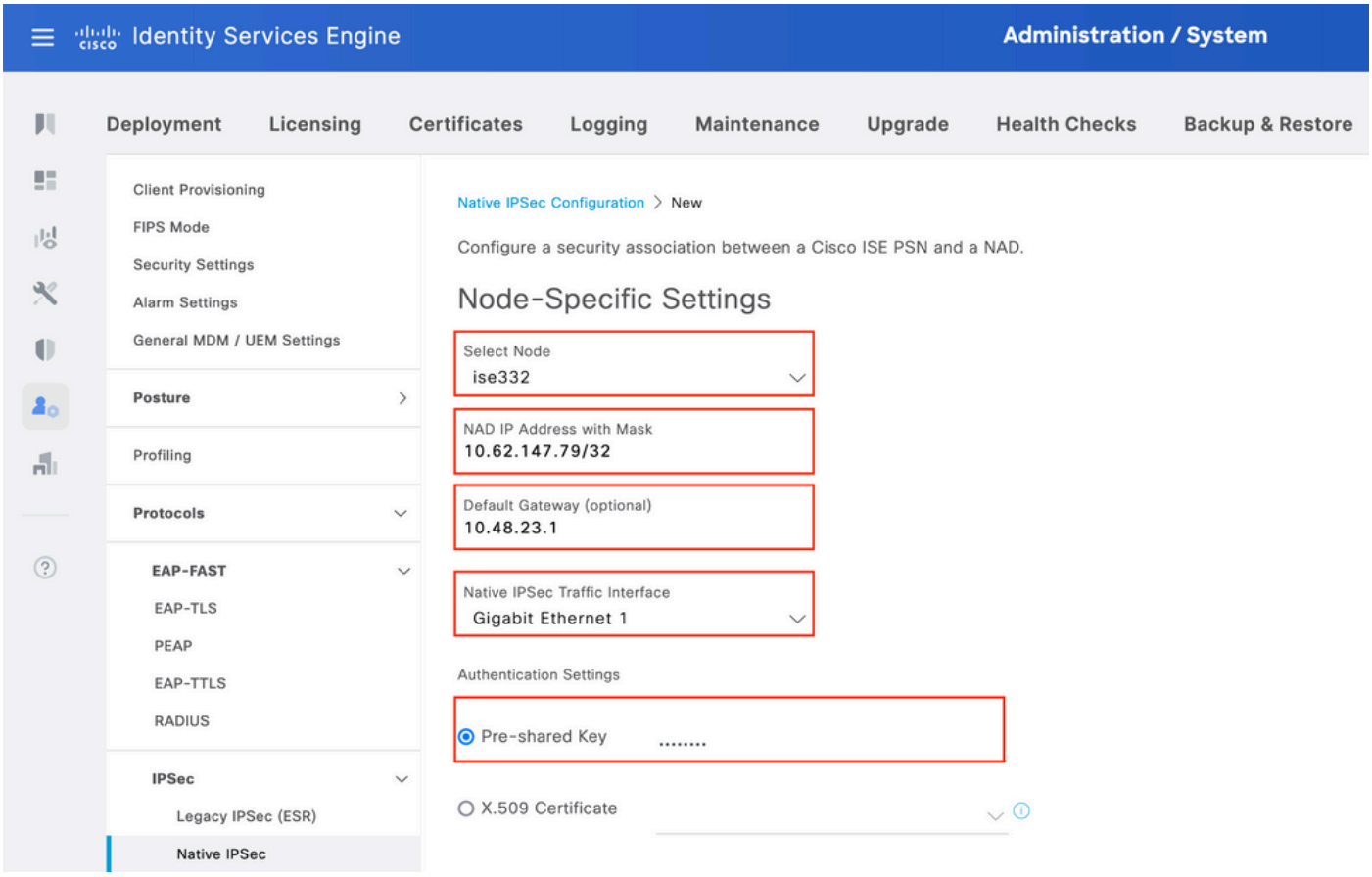
應該從CLI在介面GE1-GE5上配置地址，不支援GE0。

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

注意：在介面上配置了IP地址後，應用程式將重新啟動：
%更改IP地址可能導致ISE服務重新啟動
是否繼續更改IP地址？ Y/N [N]：Y

配置IPSec隧道

導航到管理>系統>設定>協定> IPsec >本地IPsec。按一下Add。選擇終止IPSec隧道的節點，配置帶掩碼的NAD IP地址、預設網關和IPSec介面。 選擇Authentication Setting as X.509 Certificate，然後選擇Certificate System Certificate Installed。



預設網關是可選配置。事實上，您有兩個選項，可以在本地IPsec UI中配置預設網關，從而在底層作業系統中安裝路由。此路由未在show running-config：中公開

```
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

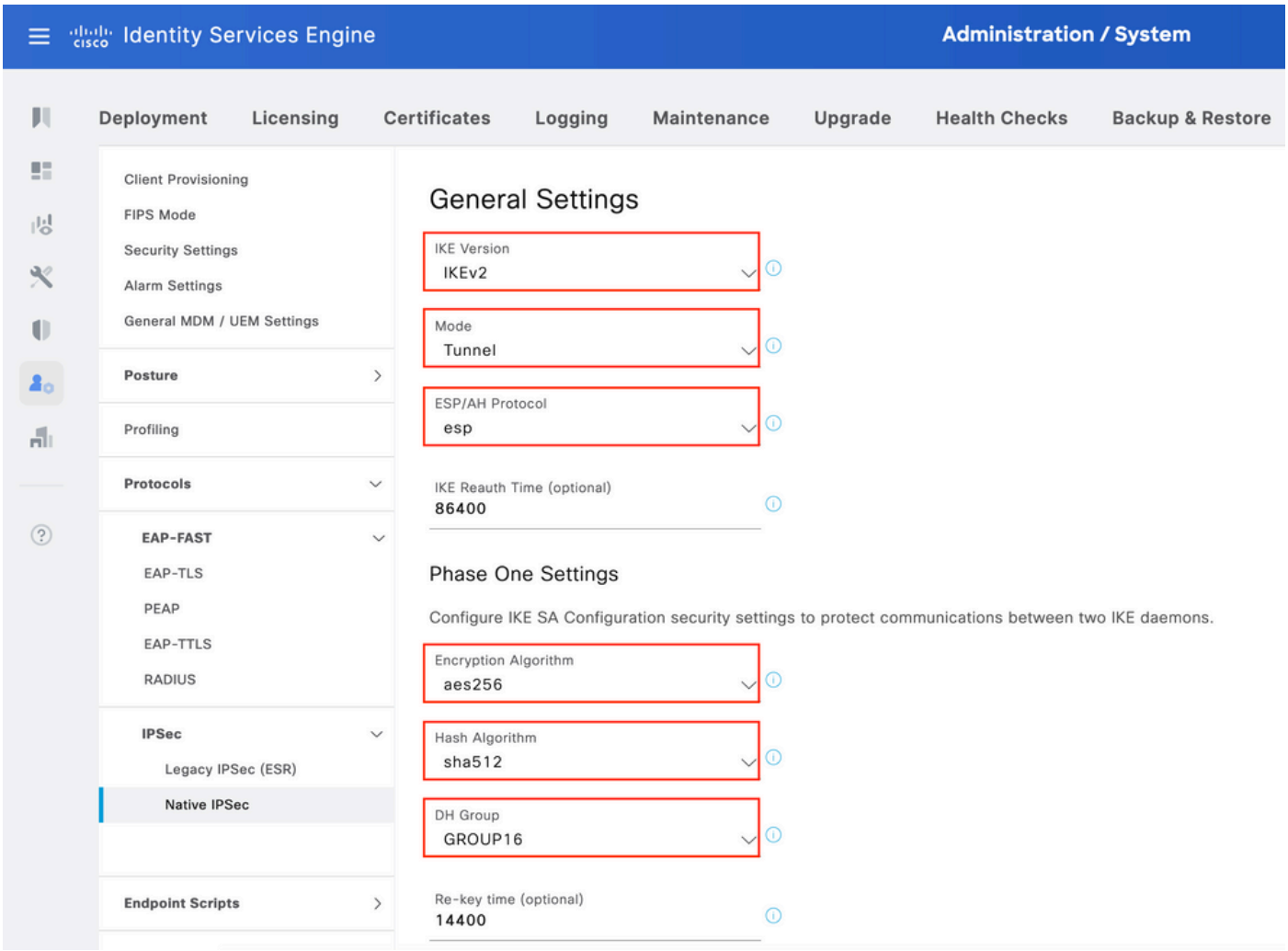
```
169.254.2.0/24 0.0.0.0 cni-podman1
169.254.4.0/24 0.0.0.0 cni-podman2
ise332/admin#
```

另一個選項是保留預設網關為空，並在ISE上手動配置路由，這將實現相同的效果：

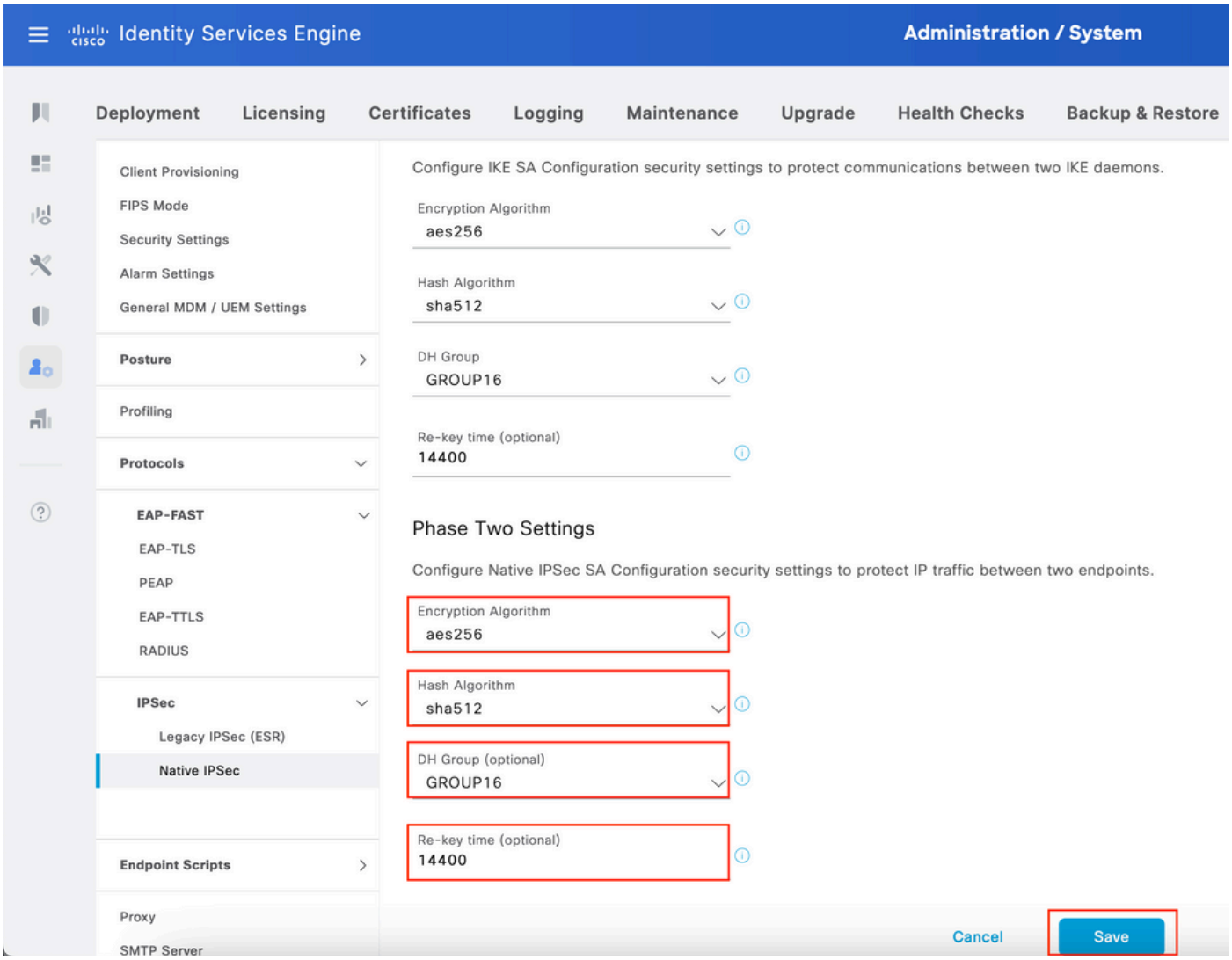
```
ise332/admin(config)#ip route 10.62.148.79 255.255.255.255 gateway 10.48.23.1
ise332/admin(config)#exit
ise332/admin#show ip route

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#
```

配置IPSec隧道的常規設定。配置Phase One設定。常規設定、階段一設定和階段二設定應與IPSec隧道另一端上配置的設定匹配。



配置Phase Two Settings並按一下Save。



驗證

要確保RADIUS透過IPSec隧道工作，請使用test aaa命令或執行實際的MAB或802.1X身份驗證

```
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#
```

在IOS-XE上驗證

<#root>

```
KSEC-9248L-1#
```

show crypto ikev2 sa

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/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
```

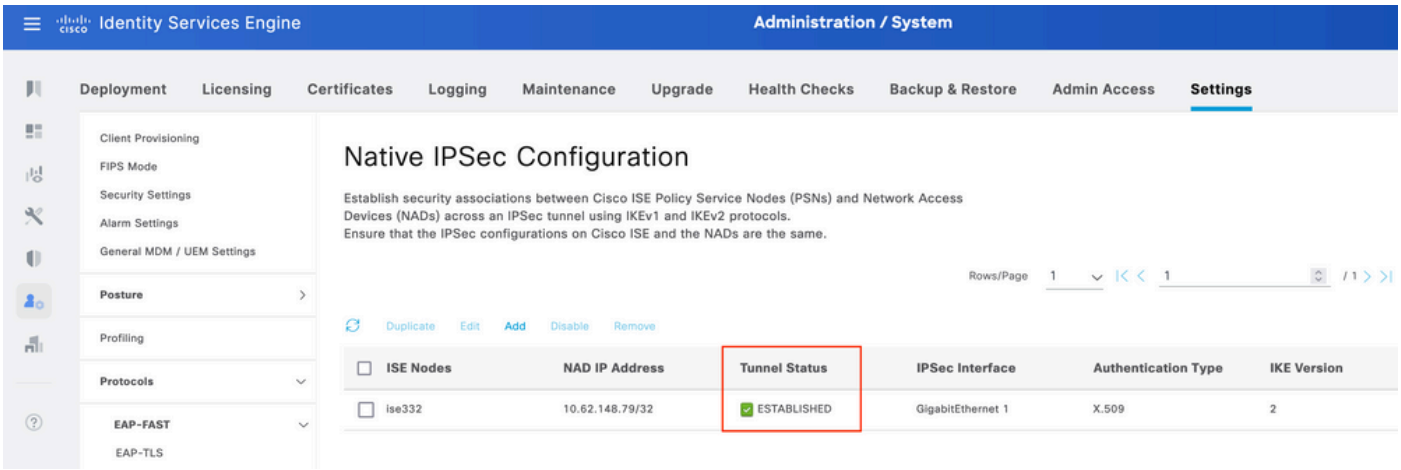
Active

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

KSEC-9248L-1#
```

在ISE上進行驗證

隧道的狀態可以透過GUI進行驗證



使用application configure ise命令從CLI驗證隧道的狀態

<#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 REPLOGNS 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
```

疑難排解

IOS-XE故障排除

要啟用的調試

<#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上的完整工作調試集

```
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
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_S
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
Initiator SPI : 0CA3C29E36290185 - 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 10.62.14
Initiator SPI : 0CA3C29E36290185 - 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 certificat
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 Compu
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 SK
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED cal
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 authentic
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication dat
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 sucessfully sign
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
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 PASSE
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
Initiator SPI : 0CA3C29E36290185 - 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 10.62.14
Initiator SPI : 0CA3C29E36290185 - 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=ise
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching Policy with fvrf 0, local address 10.62
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 authentic
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication dat
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 d
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 PR

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 fo

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
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Session with IKE ID PAIR (cn=ise332.example.com,
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
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 sam
```

```
Apr 25 18:57:37.055: IPSEC:(SESSION ID = 5) (get_old_outbound_sa_for_peer) No outbound SA found for pee
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
```

在ISE上進行故障排除

要啟用的調試

沒有要在ISE上啟用的特定調試，要將調試列印到控制檯發出命令：

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

在ISE上執行全部工作調試

```
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 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/M
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> ocsp check skipped, no ocsp 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/H
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 othe
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1
```

```
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-
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 integrit
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
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI c17542e9 a
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC w
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_
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
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI f7a68f69 a
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC w
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_
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
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.48.23.85/32 === 10.
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting a local address in traffic s
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
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> installing route: 10.62.148.79/32 vi
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-
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-
Apr 26 00:57:37 09[ENC] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> generating IKE_AUTH response 1 [ IDr
Apr 26 00:57:37 09[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin IKEv2 SA 7212b70a-1405-429a-
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] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
```

關於此翻譯
思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。