

# Configuración de IPsec nativo de ISE 3.3 para la comunicación NAD segura (IOS-XE)

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

### [Antecedentes](#)

### [Configuración del túnel IPsec IKEv2 con autenticación de certificado X.509](#)

[Diagrama de la red](#)

[Configuración CLI del switch IOS-XE](#)

[Configuración de las interfaces](#)

[Configurar Trustpoint](#)

[Importar certificados](#)

[Configuración de la propuesta IKEv2](#)

[Configurar una política Crypto IKEv2](#)

[Configuración de un perfil IKEv2 criptográfico](#)

[Configuración de una ACL para el tráfico de interés de VPN](#)

[Configuración de un conjunto de transformación](#)

[Configurar un mapa criptográfico y aplicarlo a una interfaz](#)

[Configuración final de IOS-XE](#)

[Configuración de ISE](#)

[Configuración de la dirección IP en ISE](#)

[Importar certificado de almacén de confianza](#)

[Importar certificado del sistema](#)

[Configuración del túnel IPsec](#)

### [Configuración del túnel IPsec IKEv2 con autenticación de clave precompartida X.509](#)

[Diagrama de la red](#)

[Configuración CLI del switch IOS-XE](#)

[Configuración de las interfaces](#)

[Configuración de la propuesta IKEv2](#)

[Configurar una política Crypto IKEv2](#)

[Configuración de un perfil IKEv2 criptográfico](#)

[Configuración de una ACL para el tráfico de interés de VPN](#)

[Configuración de un conjunto de transformación](#)

[Configurar un mapa criptográfico y aplicarlo a una interfaz](#)

[Configuración final de IOS-XE](#)

[Configuración de ISE](#)

[Configuración de la dirección IP en ISE](#)

[Configuración del túnel IPsec](#)

### [Verificación](#)

[Verificar en IOS-XE](#)

[Verificar en ISE](#)

---

## [Troubleshoot](#)

[Solución de problemas en IOS-XE](#)

[Depuraciones para habilitar](#)

[Conjunto completo de depuraciones en funcionamiento en IOS-XE](#)

[Resolución de problemas en ISE](#)

[Depuraciones para habilitar](#)

[Conjunto completo de depuraciones en funcionamiento en ISE](#)

---

# Introducción

Este documento describe cómo configurar y solucionar problemas de IPsec nativo para proteger la comunicación de Cisco Identity Service Engine (ISE) 3.3 - Dispositivo de acceso a la red (NAD). El tráfico RADIUS se puede cifrar con un túnel de intercambio de claves de Internet IPsec versión 2 (IKEv2) de sitio a sitio (LAN a LAN) entre el switch e ISE. Este documento no cubre la parte de configuración de RADIUS.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Configuración del switch de Cisco
- Conceptos generales de IPsec
- Conceptos generales de RADIUS

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst Switch C9200L que ejecuta la versión de software 17.6.5
- Cisco Identity Service Engine versión 3.3
- Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Antecedentes

El objetivo es proteger los protocolos que utilizan hash MD5, RADIUS y TACACS inseguros con IPsec. Pocos datos a tener en cuenta:

- La solución Cisco ISE Native IPsec se basa en [StrongSwan](#)

- Al configurar IPsec en una interfaz Cisco ISE, se crea un túnel IPsec entre Cisco ISE y NAD para proteger la comunicación. NAD se debe configurar por separado en Native IPsec Settings.
- Puede definir una clave previamente compartida o utilizar certificados X.509 para la autenticación IPsec.
- IPsec se puede habilitar en interfaces GigabitEthernet1 a GigabitEthernet5.

El objetivo principal del documento es cubrir la Autenticación de certificados X.509. La sección Verificación y solución de problemas se centra en la autenticación de certificados X.509 solamente, la depuración debe ser exactamente la misma para la autenticación de clave precompartida, con sólo diferencias en las salidas. Los mismos comandos también se pueden utilizar para la verificación.

## Configuración del túnel IPsec IKEv2 con autenticación de certificado X.509

### Diagrama de la red

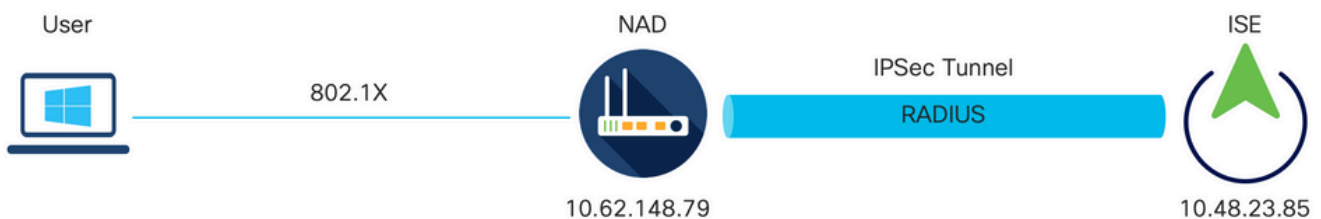


Diagrama de la red

### Configuración CLI del switch IOS-XE

#### Configuración de las interfaces

Si las interfaces del switch IOS-XE aún no están configuradas, debe configurarse al menos una interfaz. Aquí tiene un ejemplo:


```
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
!
```

Asegúrese de que haya conectividad con el peer remoto que se debe utilizar para establecer un túnel VPN de sitio a sitio. Puede utilizar un ping para verificar la conectividad básica.

## Configurar Trustpoint

Para configurar las políticas IKEv2, ingrese el comando `crypto pki trustpoint <name>` en el modo de configuración global. Aquí tiene un ejemplo:

---

 Nota: Hay varias formas de instalar certificados en un dispositivo IOS-XE. En este ejemplo, utilizamos la importación del archivo `pkcs12`, que contiene el certificado de identidad y su cadena

---

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


## Importar certificados

Para importar el certificado de identidad IOS-XE junto con su cadena, ingrese el comando `crypto pki import <trustpoint> pkcs12 <location> password <password>` en el modo privilegiado. Aquí tiene un ejemplo:

```
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#
```

---

 Nota: Aunque los certificados estén fuera del alcance del documento, asegúrese de que el certificado de identidad IOS-XE tenga campos SAN rellenos con su FQDN / dirección IP. ISE requiere un certificado de peer para tener un campo SAN.

---

Para verificar que los certificados están instalados correctamente:

```
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#

## Configuración de la propuesta IKEv2

Para configurar las políticas IKEv2, ingrese el comando `crypto ikev2 propuesta <nombre>` en el modo de configuración global. Aquí tiene un ejemplo:

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

## Configurar una política Crypto IKEv2

Para configurar las políticas IKEv2, ingrese el comando `crypto ikev2 policy <name>` en el modo de configuración global:

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

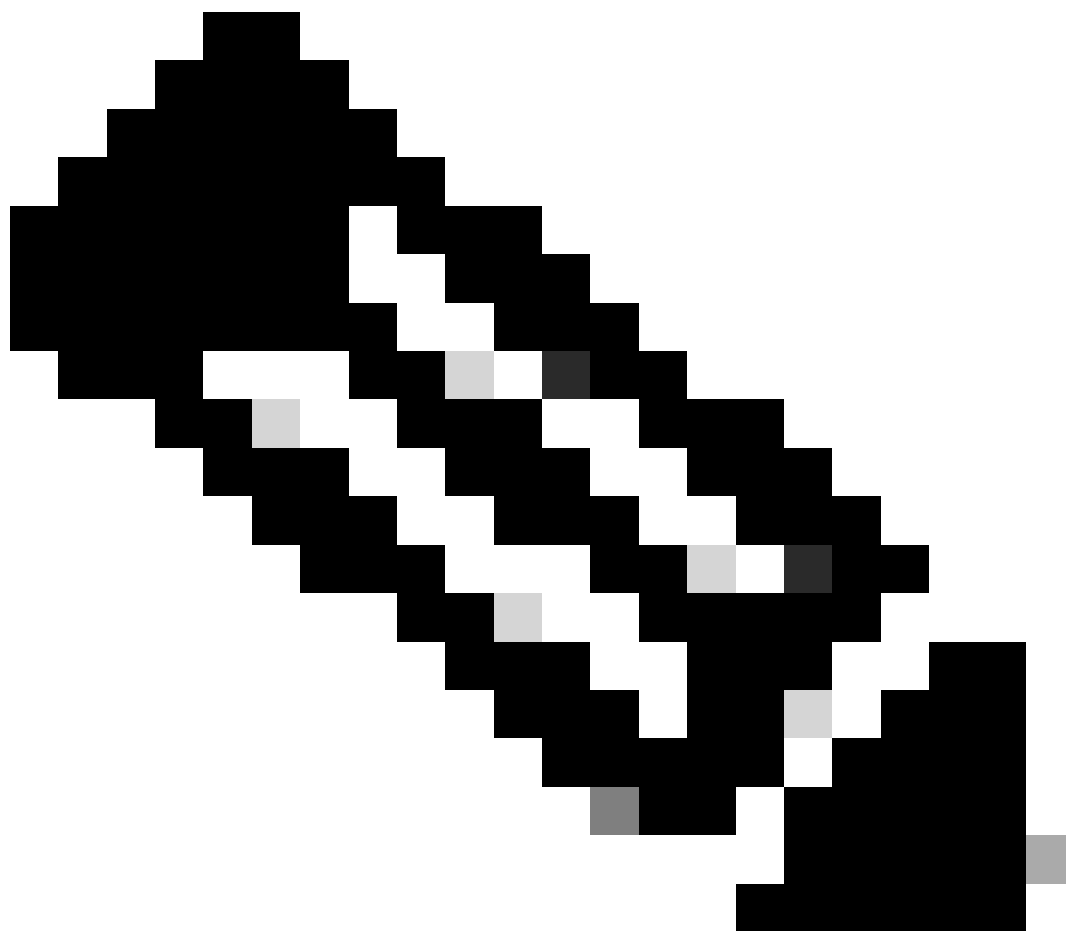
## Configuración de un perfil IKEv2 criptográfico

Para configurar el perfil IKEv2, ingrese el comando `crypto ikev2 profile <name>` en el modo de

configuración global.

```
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
```

---



Nota: de forma predeterminada, ISE utiliza el campo CN de su propio certificado de identidad como identidad IKE en la negociación IKEv2. Por eso, en la sección "coincidencia de identidad remota" del perfil IKEv2, debe especificar el tipo de FQDN y el valor adecuado del dominio o FQDN de ISE.


---

Configuración de una ACL para el tráfico de interés de VPN

Utilice la lista de acceso ampliada o con nombre para especificar el tráfico que debe protegerse mediante cifrado. Aquí tiene un ejemplo:

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

---

 Nota: Una ACL para el tráfico VPN utiliza las direcciones IP de origen y de destino después de NAT.

---

## Configuración de un conjunto de transformación

Para definir un conjunto de transformación IPsec (una combinación aceptable de protocolos y algoritmos de seguridad), ingrese el comando `crypto ipsec transform-set` en el modo de configuración global. Aquí tiene un ejemplo:

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

## Configurar un mapa criptográfico y aplicarlo a una interfaz

Para crear o modificar una entrada de mapa criptográfico e ingresar al modo de configuración de mapa criptográfico, ingrese el comando de configuración global `crypto map`. Para que la entrada de mapa criptográfico esté completa, hay algunos aspectos que deben definirse como mínimo:

- Se deben definir los pares IPsec a los que se puede reenviar el tráfico protegido. Estos son los pares con los que se puede establecer una SA. Para especificar un peer IPsec en una entrada de mapa criptográfico, ingrese el comando `set peer`.
- Se deben definir los conjuntos de transformación que son aceptables para su uso con el tráfico protegido. Para especificar los conjuntos de transformación que se pueden utilizar con la entrada de mapa criptográfico, ingrese el comando `set transform-set`.
- Se debe definir el tráfico que se debe proteger. Para especificar una lista de acceso ampliada para una entrada de mapa criptográfico, ingrese el comando `match address`.

Aquí tiene un ejemplo:

```
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
```

El paso final es aplicar el conjunto de mapas criptográficos previamente definido a una interfaz. Para aplicar esto, ingrese el comando de configuración de interfaz crypto map:

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

## Configuración final de IOS-XE

Esta es la configuración final de CLI del switch IOS-XE:

```
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-authorization
  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
!
```

## Configuración de ISE

### Configuración de la dirección IP en ISE

La dirección debe configurarse en la interfaz GE1-GE5 desde la CLI; no se admite GE0.

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



Nota: La aplicación se reinicia después de configurar la dirección IP en la interfaz:  
% El cambio de la dirección IP puede hacer que se reinicien los servicios ISE  
¿Desea continuar con el cambio de dirección IP? S/N [N]: S

---

### Importar certificado de almacén de confianza

Este paso es necesario para garantizar que ISE confíe en el certificado del par presentado en el momento en que se establece el túnel. Vaya a Administration > System > Certificates > Trusted Certificates. Haga clic en Importar. Haga clic en Browse y seleccione el certificado de CA que firmó el certificado de identidad ISE/IOS-XE. Asegúrese de que la casilla de verificación Confiar en la autenticación dentro de ISE esté seleccionada. Haga clic en Submit (Enviar).

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  KrakowCA.crt

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

## Importar certificado del sistema

Vaya a Administration > System > Certificates > System Certificates. Seleccione Node, Certificate File y Private key File Import. Seleccione la casilla de verificación contra IPsec. Haga clic en Submit (Enviar).

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 Server Certificate

\* Select Node

\* Certificate File  ise332.example.com.pem

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

Password

Friendly Name

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

 Nota: los certificados se instalan en StrongSwan SOLO después de guardar el dispositivo de acceso de red en Native IPsec Settings.

## Configuración del túnel IPsec

Vaya a Administration > System > Settings > Protocols > IPsec > Native IPsec. Haga clic en Agregar. Seleccione Node, que termina el túnel IPsec, configure NAD IP Address with Mask, Default Gateway e IPsec Interface. Seleccione Configuración de autenticación como certificado

X.509 y elija Certificado del sistema de certificados instalado.

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  
10.62.148.79/32

Default Gateway (optional)  
10.48.23.1

IPSec Interface  
Gigabit Ethernet 1

Authentication Settings

Pre-shared Key

X.509 Certificate IPSEC-2

La puerta de enlace predeterminada es una configuración opcional. De hecho, tiene dos opciones, puede configurar una puerta de enlace predeterminada en la interfaz de usuario de IPsec nativa, que instala una ruta en el sistema operativo subyacente. Esta ruta no se expone en show running-config:

```
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#
```

Otra opción consiste en dejar la puerta de enlace predeterminada en blanco y configurar la ruta manualmente en ISE, lo que tendrá el mismo efecto:

```
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#
```

Configure los parámetros generales para el túnel IPsec. Configure los parámetros de la fase uno. Los parámetros generales, los parámetros de la fase uno y los parámetros de la fase dos deben coincidir con los parámetros configurados en el otro lado del túnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows a navigation menu with 'IPSec' expanded to 'Native IPsec'. The main content area is titled 'General Settings' and contains the following configuration items:

- IKE Version:** IKEv2
- Mode:** Tunnel
- ESP/AH Protocol:** esp
- IKE Reauth Time (optional):** 86400

Below these are the 'Phase One Settings', which include a description: 'Configure IKE SA Configuration security settings to protect communications between two IKE daemons.' The configuration items are:

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

Configure Phase Two Settings y haga clic en Save.

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

## Configuración del túnel IPsec IKEv2 con autenticación de clave precompartida X.509

Diagrama de la red

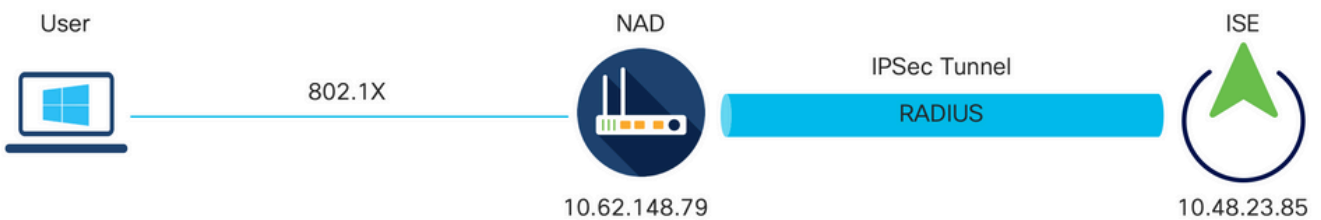


Diagrama de la red

## Configuración CLI del switch IOS-XE

Configuración de las interfaces

Si las interfaces del switch IOS-XE aún no están configuradas, debe configurarse al menos una interfaz. Aquí tiene un ejemplo:

```
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
!
```

Asegúrese de que haya conectividad con el peer remoto que se debe utilizar para establecer un túnel VPN de sitio a sitio. Puede utilizar un ping para verificar la conectividad básica.

### Configuración de la propuesta IKEv2

Para configurar las políticas IKEv2, ingrese el comando `crypto ikev2 propuesta <nombre>` en el modo de configuración global. Aquí tiene un ejemplo:

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

### Configurar una política Crypto IKEv2

Para configurar las políticas IKEv2, ingrese el comando `crypto ikev2 policy <name>` en el modo de configuración global:

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

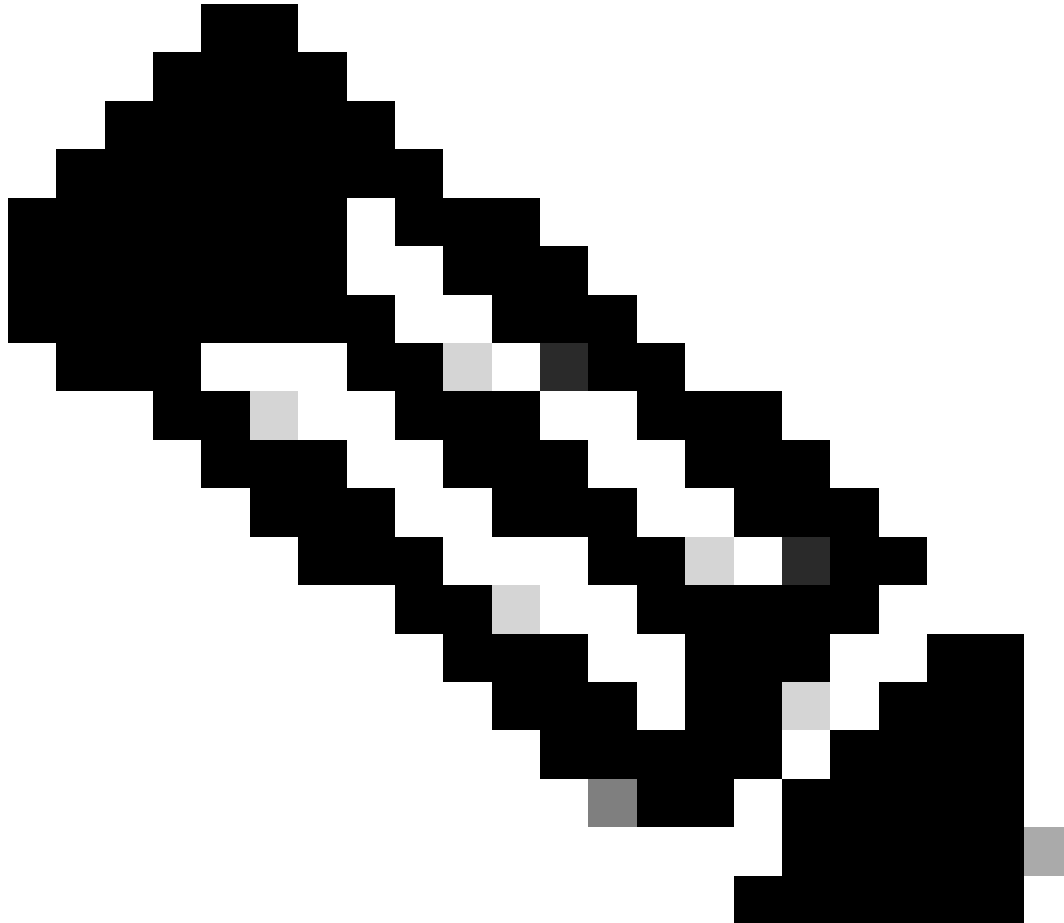
### Configuración de un perfil IKEv2 criptográfico

Para configurar el perfil IKEv2, ingrese el comando `crypto ikev2 profile <name>` en el modo de configuración global.

```
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
```

---



Nota: de forma predeterminada, ISE utiliza el campo CN de su propio certificado de identidad como identidad IKE en la negociación IKEv2. Por eso, en la sección "coincidencia de identidad remota" del perfil IKEv2, debe especificar el tipo de FQDN y el valor adecuado del dominio o FQDN de ISE.


---

## Configuración de una ACL para el tráfico de interés de VPN

Utilice la lista de acceso ampliada o con nombre para especificar el tráfico que debe protegerse mediante cifrado. Aquí tiene un ejemplo:

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

---

 Nota: Una ACL para el tráfico VPN utiliza las direcciones IP de origen y de destino después de NAT.

---

## Configuración de un conjunto de transformación

Para definir un conjunto de transformación IPsec (una combinación aceptable de protocolos y algoritmos de seguridad), ingrese el comando `crypto ipsec transform-set` en el modo de configuración global. Aquí tiene un ejemplo:

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

## Configurar un mapa criptográfico y aplicarlo a una interfaz

Para crear o modificar una entrada de mapa criptográfico e ingresar al modo de configuración de mapa criptográfico, ingrese el comando de configuración global `crypto map`. Para que la entrada de mapa criptográfico esté completa, hay algunos aspectos que deben definirse como mínimo:

- Se deben definir los pares IPsec a los que se puede reenviar el tráfico protegido. Estos son los pares con los que se puede establecer una SA. Para especificar un peer IPsec en una entrada de mapa criptográfico, ingrese el comando `set peer`.
- Se deben definir los conjuntos de transformación que son aceptables para su uso con el tráfico protegido. Para especificar los conjuntos de transformación que se pueden utilizar con la entrada de mapa criptográfico, ingrese el comando `set transform-set`.
- Se debe definir el tráfico que se debe proteger. Para especificar una lista de acceso ampliada para una entrada de mapa criptográfico, ingrese el comando `match address`.

Aquí tiene un ejemplo:

```
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
```

El paso final es aplicar el conjunto de mapas criptográficos previamente definido a una interfaz. Para aplicar esto, ingrese el comando de configuración de interfaz `crypto map`:



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

## Configuración final de IOS-XE

Esta es la configuración final de CLI del switch IOS-XE:

```
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  
!
```

## Configuración de ISE

### Configuración de la dirección IP en ISE

La dirección debe configurarse en la interfaz GE1-GE5 desde la CLI; no se admite GE0.

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



Nota: La aplicación se reinicia después de configurar la dirección IP en la interfaz:  
% El cambio de la dirección IP puede hacer que se reinicien los servicios ISE  
¿Desea continuar con el cambio de dirección IP? S/N [N]: S

---

### Configuración del túnel IPsec

Vaya a Administration > System > Settings > Protocols > IPsec > Native IPsec. Haga clic en Agregar. Seleccione Node, que termina el túnel IPsec, configure NAD IP Address with Mask, Default Gateway e IPsec Interface. Seleccione Configuración de autenticación como certificado X.509 y elija Certificado del sistema de certificados instalado.

La puerta de enlace predeterminada es una configuración opcional. De hecho, tiene dos opciones, puede configurar una puerta de enlace predeterminada en la interfaz de usuario de IPsec nativa, que instala una ruta en el sistema operativo subyacente. Esta ruta no se expone en show running-config:

```
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#
```

Otra opción consiste en dejar la puerta de enlace predeterminada en blanco y configurar la ruta manualmente en ISE, lo que tendrá el mismo efecto:

```
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#
```

Configure los parámetros generales para el túnel IPsec. Configure los parámetros de la fase uno. Los parámetros generales, los parámetros de la fase uno y los parámetros de la fase dos deben coincidir con los parámetros configurados en el otro lado del túnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows a navigation menu with categories like Client Provisioning, Security Settings, and Protocols. The 'IPSec' section is expanded, showing 'Native IPsec' selected. 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

Configure Phase Two Settings y haga clic en Save.

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains a navigation menu with the following items: Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, General MDM / UEM Settings, Posture, Profiling, Protocols (expanded to show EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, RADIUS, IPsec (expanded to show Legacy IPsec (ESR) and Native IPsec), Endpoint Scripts, Proxy, and SMTP Server. The main content area displays the configuration for Native IPsec. The 'Phase Two Settings' section is highlighted, and the following settings are visible: Encryption Algorithm (aes256), Hash Algorithm (sha512), DH Group (GROUP16), and Re-key time (optional) (14400). A 'Save' button is highlighted with a red box.

## Verificación

Para asegurarse de que RADIUS funciona sobre el túnel IPsec, utilice el comando test aaa o realice una autenticación real de MAB o 802.1X

```
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#
```

Verificar en IOS-XE

```
<#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#

## Verificar en ISE

El estado del túnel se puede verificar desde la GUI

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The 'Settings' tab is active, and the 'Native IPsec Configuration' page is displayed. The page includes a table with the following columns: ISE Nodes, NAD IP Address, Tunnel Status, IPsec Interface, Authentication Type, and IKE Version. The 'Tunnel Status' column for the 'ise332' entry is highlighted with a red box, showing 'ESTABLISHED'.

ISE Nodes	NAD IP Address	Tunnel Status	IPsec Interface	Authentication Type	IKE Version
<input type="checkbox"/>	ise332	<input checked="" type="checkbox"/> ESTABLISHED	GigabitEthernet 1	X.509	2

Utilice el comando `application configure ise` para verificar el estado del túnel desde la CLI

```
<#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
```

## Troubleshoot

### Solución de problemas en IOS-XE

#### Depuraciones para habilitar

```
<#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#
```

#### Conjunto completo de depuraciones en funcionamiento en IOS-XE

```
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 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 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= 10  
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Session with IKE ID PAIR (cn=ise332.example.com, local=10.62.148.79, remote=10.48.23.85)  
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. SA ID= 10  
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

```

## Resolución de problemas en ISE

### Depuraciones para habilitar

No hay depuraciones específicas que habilitar en ISE, para imprimir las depuraciones en la consola emite el comando:

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

### Conjunto completo de depuraciones en funcionamiento en ISE

```

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] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).