

Configuration de la communication IPsec native ISE 3.3 vers NAD sécurisé (IOS-XE)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration du tunnel IPsec IKEv2 avec authentification par certificat X.509](#)

[Diagramme du réseau](#)

[Configuration CLI du commutateur IOS-XE](#)

[Configurer les interfaces](#)

[Configurer le point de confiance](#)

[Importer des certificats](#)

[Configuration de la proposition IKEv2](#)

[Configuration d'une stratégie de cryptage IKEv2](#)

[Configuration d'un profil IKEv2 de chiffrement](#)

[Configurer une ACL pour le trafic VPN d'intérêt](#)

[Configurer un ensemble de transformation](#)

[Configurer une carte cryptographique et l'appliquer à une interface](#)

[Configuration finale d'IOS-XE](#)

[Configuration ISE](#)

[Configurer l'adresse IP sur ISE](#)

[Importer un certificat de magasin approuvé](#)

[Importer un certificat système](#)

[Configuration du tunnel IPsec](#)

[Configuration du tunnel IPsec IKEv2 avec authentification de clé prépartagée X.509](#)

[Diagramme du réseau](#)

[Configuration CLI du commutateur IOS-XE](#)

[Configurer les interfaces](#)

[Configuration de la proposition IKEv2](#)

[Configuration d'une stratégie de cryptage IKEv2](#)

[Configuration d'un profil IKEv2 de chiffrement](#)

[Configurer une ACL pour le trafic VPN d'intérêt](#)

[Configurer un ensemble de transformation](#)

[Configurer une carte cryptographique et l'appliquer à une interface](#)

[Configuration finale d'IOS-XE](#)

[Configuration ISE](#)

[Configurer l'adresse IP sur ISE](#)

[Configuration du tunnel IPsec](#)

[Vérifier](#)

[Vérification sur IOS-XE](#)

[Vérifier sur ISE](#)

[Dépannage](#)

[Dépannage sur IOS-XE](#)

[Débogages à activer](#)

[Ensemble complet de débogages de travail sur IOS-XE](#)

[Dépannage sur ISE](#)

[Débogages à activer](#)

[Ensemble complet de débogages de travail sur ISE](#)

Introduction

Ce document décrit comment configurer et dépanner IPsec natif pour sécuriser la communication de Cisco Identity Service Engine (ISE) 3.3 - Network Access Device (NAD). Le trafic Radius peut être chiffré avec le tunnel IPsec IKEv2 (Internet Key Exchange Version 2) de site à site (LAN à LAN) entre le commutateur et ISE. Ce document ne couvre pas la partie configuration RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Configuration du commutateur Cisco
- Concepts généraux d'IPSec
- Concepts généraux de RADIUS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Cisco Catalyst C9200L qui exécute la version logicielle 17.6.5
- Cisco Identity Service Engine version 3.3
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'objectif est de sécuriser les protocoles qui utilisent le hachage MD5 non sécurisé, RADIUS et TACACS avec IPsec. Quelques faits à prendre en considération :

- La solution IPsec native Cisco ISE est basée sur [StrongSwan](#)
- Lorsque vous configurez IPsec sur une interface Cisco ISE, un tunnel IPsec est créé entre Cisco ISE et le NAD pour sécuriser la communication. NAD doit être configuré séparément

sous Native IPsec Settings.

- Vous pouvez définir une clé pré-partagée ou utiliser des certificats X.509 pour l'authentification IPsec.
- IPsec peut être activé sur les interfaces GigabitEthernet1 à GigabitEthernet5.

L'objectif principal du document est de couvrir l'authentification par certificat X.509. La section Vérifier et dépanner se concentre sur l'authentification de certificat X.509 uniquement, le débogage doit être exactement le même pour l'authentification de clé prépartagée, avec seulement une différence dans les résultats. Les mêmes commandes peuvent également être utilisées pour la vérification.

Configuration du tunnel IPsec IKEv2 avec authentification par certificat X.509

Diagramme du réseau

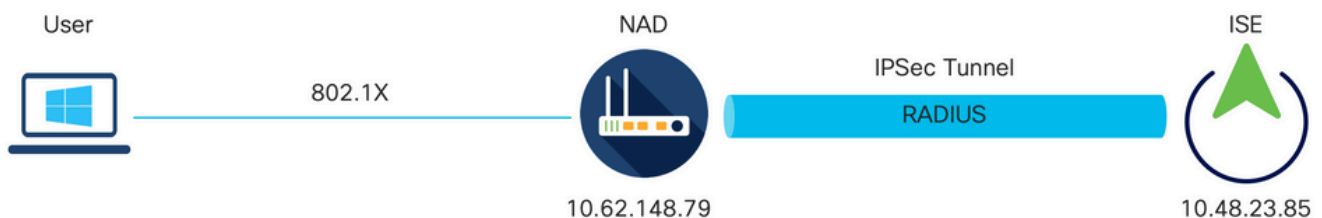


Diagramme du réseau

Configuration CLI du commutateur IOS-XE

Configurer les interfaces


Si les interfaces du commutateur IOS-XE ne sont pas encore configurées, au moins une interface doit être configurée. Voici un exemple :

```
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
!
```

Assurez-vous que la connectivité à l'homologue distant doit être utilisée afin d'établir un tunnel VPN site à site. Vous pouvez utiliser un message ping pour vérifier la connectivité de base.

Configurer le point de confiance

Afin de configurer les stratégies IKEv2, entrez la commande `crypto pki trustpoint <name>` en mode de configuration globale. Voici un exemple :

 Remarque : il existe plusieurs façons d'installer des certificats sur un périphérique IOS-XE. Dans cet exemple, nous utilisons l'importation du fichier pkcs12, qui contient le certificat d'identité et sa chaîne


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

Importer des certificats

Afin d'importer le certificat d'identité IOS-XE avec sa chaîne, entrez la commande `crypto pki import <trustpoint> pkcs12 <location> password <password>` en mode privilégié. Voici un exemple :

```
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#
```

 Remarque : même si les certificats ne sont pas couverts par le document, assurez-vous que le certificat d'identité IOS-XE comporte des champs SAN renseignés avec son nom de domaine complet (FQDN) ou son adresse IP. ISE nécessite un certificat homologue pour avoir un champ SAN.

Afin de vérifier que les certificats sont installés correctement :

```
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#

Configuration de la proposition IKEv2

Afin de configurer les stratégies IKEv2, entrez la commande `crypto ikev2 proposition <name>` en mode de configuration globale. Voici un exemple :

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

Configuration d'une stratégie de cryptage IKEv2

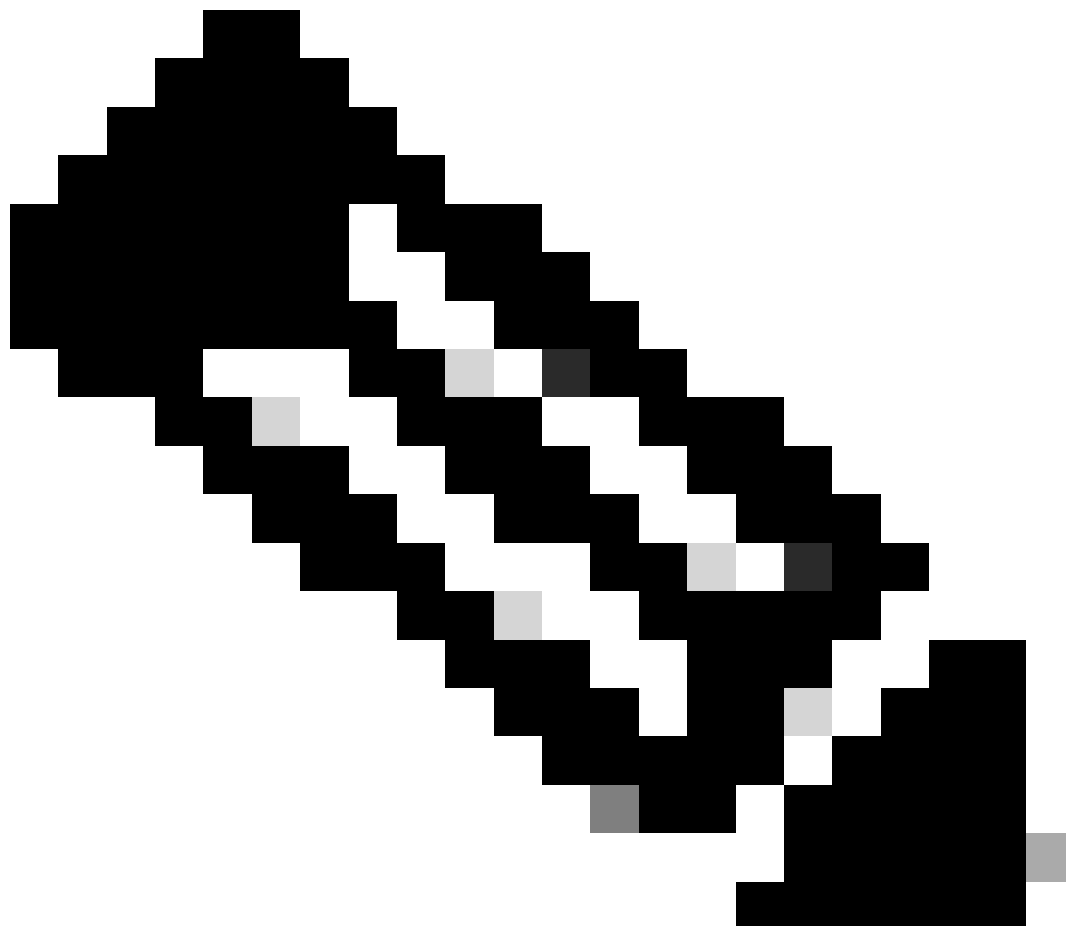
Afin de configurer les stratégies IKEv2, entrez la commande `crypto ikev2 policy <name>` en mode de configuration globale :

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

Configuration d'un profil IKEv2 de chiffrement

Afin de configurer le profil IKEv2, entrez la commande `crypto ikev2 profile <name>` en mode de configuration globale.

```
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
```




Remarque : par défaut, ISE utilise le champ CN de son propre certificat d'identité comme identité IKE dans la négociation IKEv2. C'est pourquoi dans la section « match identity remote » du profil IKEv2, vous devez spécifier le type de FQDN et la valeur appropriée du domaine ou du FQDN d'ISE.

Configurer une ACL pour le trafic VPN d'intérêt

Utilisez la liste d'accès étendue ou nommée afin de préciser le trafic qui est à protéger au moyen du chiffrement. Voici un exemple :

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

 Remarque : une liste de contrôle d'accès pour le trafic VPN utilise les adresses IP source et de destination après NAT.

Configurer un ensemble de transformation

Afin de définir un ensemble de transformation IPSec (une combinaison acceptable de protocoles et d'algorithmes de sécurité), entrez la commande `crypto ipsec transform-set` dans le mode de configuration globale. Voici un exemple :

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

Configurer une carte cryptographique et l'appliquer à une interface

Pour créer ou modifier une entrée de carte cryptographique et saisir le mode de configuration de la carte cryptographique, entrez la commande de configuration globale `crypto map`. Pour que l'entrée de la carte cryptographique soit complète, certains aspects doivent être réglés au minimum :

- Les homologues IPSec auxquels le trafic protégé peut être transféré doivent être définis. Il s'agit des homologues avec lesquels une SA peut être établie. Afin de préciser un homologue IPSec dans une entrée de carte cryptographique, saisissez la commande `set peer`.
- Les ensembles de transformation pouvant être utilisés avec le trafic protégé doivent être définis. Afin de préciser quels ensembles de transformation peuvent être utilisés avec l'entrée de carte cryptographique, saisissez la commande `set transform-set`.
- Le trafic à protéger doit être défini. Pour indiquer une liste d'accès étendu pour une entrée de carte cryptographique, entrez la commande `match address`.

Voici un exemple :

```
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
```

La dernière étape consiste à appliquer l'ensemble de cartes cryptographiques précédemment

défini à une interface. Pour ce faire, il suffit d'inscrire la commande de configuration de l'interface crypto map.

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

Configuration finale d'IOS-XE

Voici la configuration finale de l'interface de ligne de commande du commutateur 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
!
```

Configuration ISE

Configurer l'adresse IP sur ISE

L'adresse doit être configurée sur l'interface GE1-GE5 à partir de l'interface de ligne de commande, GE0 n'est pas pris en charge.

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

 Remarque : l'application redémarre après la configuration de l'adresse IP sur l'interface :
% La modification de l'adresse IP peut entraîner le redémarrage des services ISE
Poursuivre le changement d'adresse IP ? O/N [N] : O

Importer un certificat de magasin approuvé

Cette étape est nécessaire pour s'assurer qu'ISE fait confiance au certificat de l'homologue présenté au moment de l'établissement du tunnel. Accédez à Administration > System > Certificates > Trusted Certificates. Cliquez sur Import. Cliquez sur Browse et sélectionnez le certificat CA qui a signé le certificat d'identité ISE/IOS-XE. Assurez-vous que la case Trust for authentication within ISE est cochée. Cliquez sur Submit.

Identity Services Engine Administration / System

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

Certificate Management

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

Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File 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

Importer un certificat système

Accédez à Administration > System > Certificates > System Certificates. Sélectionnez Noeud, Fichier de certificat et Fichier de clé privée Importer. Cochez la case en regard de IPsec. Cliquez sur Submit.

Identity Services Engine Administration / System

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

Certificate Management

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

Certificate Authority

Import 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



Remarque : les certificats sont installés sur le StrongSwan UNIQUEMENT après l'enregistrement du périphérique d'accès réseau sous les paramètres IPsec natifs.

Configuration du tunnel IPsec

Accédez à Administration > System > Settings > Protocols > IPsec > Native IPsec. Cliquez sur Add. Sélectionnez Node, qui met fin au tunnel IPsec, configurez l'adresse IP NAD avec le masque, la passerelle par défaut et l'interface IPsec. Sélectionnez Authentication Setting as X.509

Certificate et choisissez Certificate System Certificate Installed.

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

Default Gateway est une configuration facultative. En fait, vous avez deux options, vous pouvez configurer une passerelle par défaut dans l'interface utilisateur IPsec native, qui installe une route dans le système d'exploitation sous-jacent. Cette route n'est pas exposée dans 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#
```

Une autre option consiste à laisser la passerelle par défaut vide et à configurer la route manuellement sur ISE, ce qui aura le même effet :

```
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#
```

Configurer les paramètres généraux du tunnel IPsec. Configurez les paramètres de la phase 1. Les paramètres généraux, les paramètres de phase un et les paramètres de phase deux doivent correspondre aux paramètres configurés de l'autre côté du tunnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The main navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', and 'Backup & Restore'. The left sidebar shows a tree view of configuration options, 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 this is the 'Phase One Settings' section, which includes the instruction: '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

Configurez les paramètres de la phase deux et cliquez sur Enregistrer.

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

Configuration du tunnel IPsec IKEv2 avec authentification de clé prépartagée X.509

Diagramme du réseau

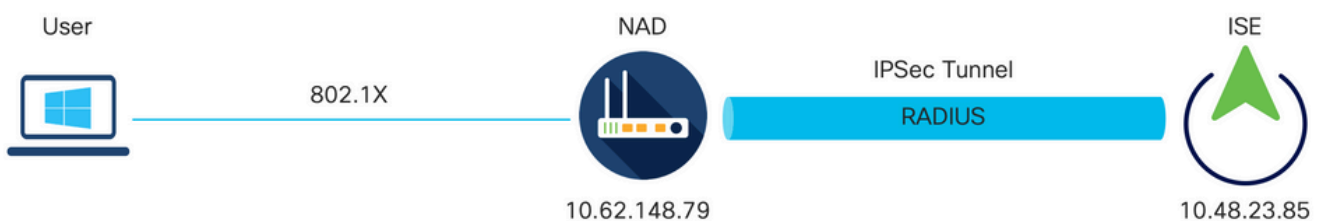


Diagramme du réseau

Configuration CLI du commutateur IOS-XE

Configurer les interfaces

Si les interfaces du commutateur IOS-XE ne sont pas encore configurées, au moins une interface doit être configurée. Voici un exemple :

```
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
!
```

Assurez-vous que la connectivité à l'homologue distant doit être utilisée afin d'établir un tunnel VPN site à site. Vous pouvez utiliser un message ping pour vérifier la connectivité de base.

Configuration de la proposition IKEv2

Afin de configurer les stratégies IKEv2, entrez la commande `crypto ikev2 proposition <name>` en mode de configuration globale. Voici un exemple :

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

Configuration d'une stratégie de cryptage IKEv2

Afin de configurer les stratégies IKEv2, entrez la commande `crypto ikev2 policy <name>` en mode de configuration globale :

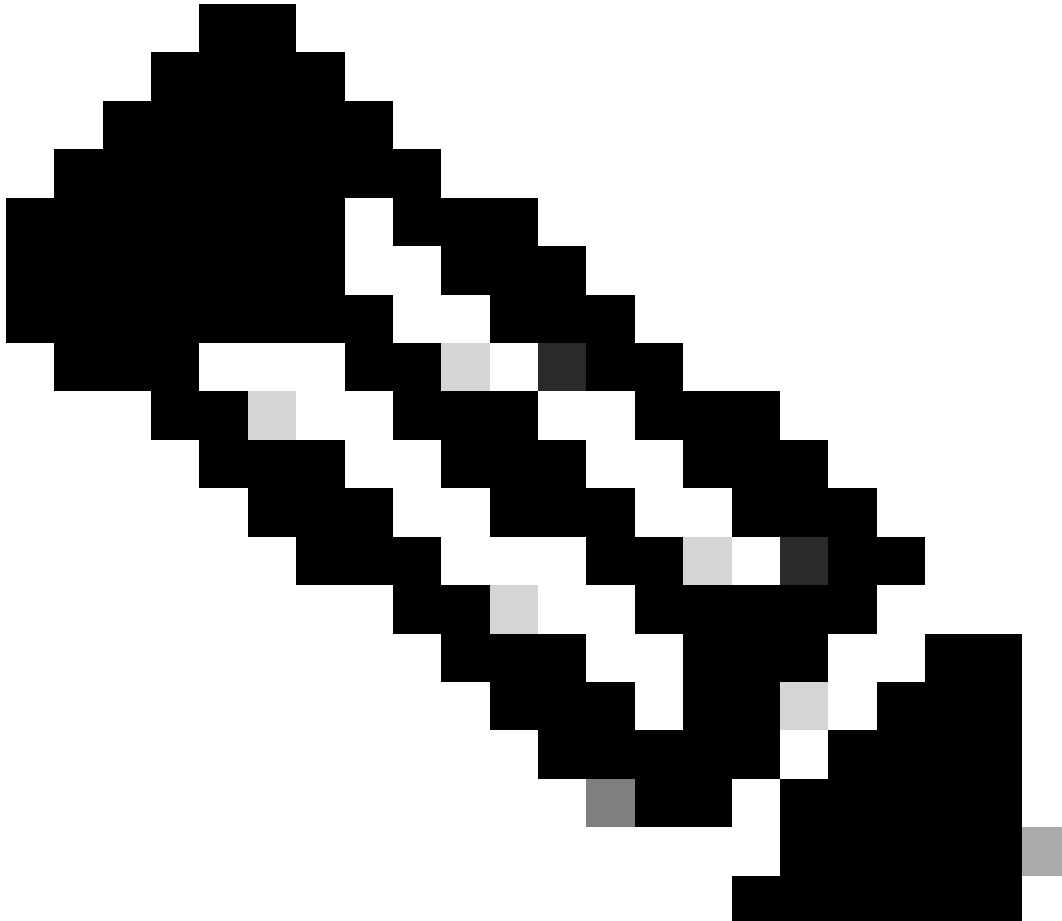
```
crypto ikev2 policy POLICY
 proposal PROPOSAL
```

Configuration d'un profil IKEv2 de chiffrement

Afin de configurer le profil IKEv2, entrez la commande `crypto ikev2 profile <name>` en mode de configuration globale.

```
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
```




Remarque : par défaut, ISE utilise le champ CN de son propre certificat d'identité comme identité IKE dans la négociation IKEv2. C'est pourquoi dans la section « match identity remote » du profil IKEv2, vous devez spécifier le type de FQDN et la valeur appropriée du domaine ou du FQDN d'ISE.

Configurer une ACL pour le trafic VPN d'intérêt

Utilisez la liste d'accès étendue ou nommée afin de préciser le trafic qui est à protéger au moyen du chiffrement. Voici un exemple :

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

 Remarque : une liste de contrôle d'accès pour le trafic VPN utilise les adresses IP source et de destination après NAT.

Configurer un ensemble de transformation

Afin de définir un ensemble de transformation IPSec (une combinaison acceptable de protocoles et d'algorithmes de sécurité), entrez la commande `crypto ipsec transform-set` dans le mode de configuration globale. Voici un exemple :

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

Configurer une carte cryptographique et l'appliquer à une interface

Pour créer ou modifier une entrée de carte cryptographique et saisir le mode de configuration de la carte cryptographique, entrez la commande de configuration globale `crypto map`. Pour que l'entrée de la carte cryptographique soit complète, certains aspects doivent être réglés au minimum :

- Les homologues IPSec auxquels le trafic protégé peut être transféré doivent être définis. Il s'agit des homologues avec lesquels une SA peut être établie. Afin de préciser un homologue IPSec dans une entrée de carte cryptographique, saisissez la commande `set peer`.
- Les ensembles de transformation pouvant être utilisés avec le trafic protégé doivent être définis. Afin de préciser quels ensembles de transformation peuvent être utilisés avec l'entrée de carte cryptographique, saisissez la commande `set transform-set`.
- Le trafic à protéger doit être défini. Pour indiquer une liste d'accès étendu pour une entrée de carte cryptographique, entrez la commande `match address`.

Voici un exemple :

```
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
```

La dernière étape consiste à appliquer l'ensemble de cartes cryptographiques précédemment

défini à une interface. Pour ce faire, il suffit d'inscrire la commande de configuration de l'interface crypto map.

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

Configuration finale d'IOS-XE

Voici la configuration finale de l'interface de ligne de commande du commutateur 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
!
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
 !
```

Configuration ISE

Configurer l'adresse IP sur ISE

L'adresse doit être configurée sur l'interface GE1-GE5 à partir de l'interface de ligne de commande, GE0 n'est pas pris en charge.

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

 Remarque : l'application redémarre après la configuration de l'adresse IP sur l'interface :
% La modification de l'adresse IP peut entraîner le redémarrage des services ISE
Poursuivre le changement d'adresse IP ? O/N [N] : O

Configuration du tunnel IPsec

Accédez à Administration > System > Settings > Protocols > IPsec > Native IPsec. Cliquez sur Add. Sélectionnez Node, qui met fin au tunnel IPsec, configurez l'adresse IP NAD avec le masque, la passerelle par défaut et l'interface IPsec. Sélectionnez Authentication Setting as X.509 Certificate et choisissez Certificate System Certificate Installed.

Default Gateway est une configuration facultative. En fait, vous avez deux options, vous pouvez configurer une passerelle par défaut dans l'interface utilisateur IPsec native, qui installe une route dans le système d'exploitation sous-jacent. Cette route n'est pas exposée dans 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#
```

Une autre option consiste à laisser la passerelle par défaut vide et à configurer la route manuellement sur ISE, ce qui aura le même effet :

```
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#
```

Configurer les paramètres généraux du tunnel IPsec. Configurez les paramètres de la phase 1. Les paramètres généraux, les paramètres de phase un et les paramètres de phase deux doivent correspondre aux paramètres configurés de l'autre côté du tunnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows the 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 the General Settings is the 'Phase One Settings' section, which includes the instruction: '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

Configurez les paramètres de la phase deux et cliquez sur Enregistrer.

Vérifier

Pour vous assurer que RADIUS fonctionne sur le tunnel IPsec, utilisez la commande test aaa ou exécutez l'authentification MAB ou 802.1X réelle

```
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#
```

Vérification sur 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#

Vérifier sur ISE

L'état du tunnel peut être vérifié à partir de l'interface utilisateur graphique

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The main content area displays the 'Native IPSec Configuration' page, which includes a table of IPSec configurations. The 'Tunnel Status' column is highlighted with a red box, indicating that the tunnel is 'ESTABLISHED'.

ISE Nodes	NAD IP Address	Tunnel Status	IPSec Interface	Authentication Type	IKE Version
<input type="checkbox"/> ise332	10.62.148.79/32	<input checked="" type="checkbox"/> ESTABLISHED	GigabitEthernet 1	X.509	2

Utilisez la commande application configure ise pour vérifier l'état du tunnel à partir de l'interface de ligne de commande

```
<#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

Dépannage

Dépannage sur IOS-XE

Débugages à activer

```
<#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#
```

Ensemble complet de débugages de travail sur 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
```

```
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 : 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 10.62.14
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 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 Comput
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 10.62.148.79:500]
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
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
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 IPSEC

Apr 25 18:57:37.051: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1
Apr 25 18:57:37.051: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.62.148.79:0, remote= 10.48.23.85:0,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0,
protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
Apr 25 18:57:37.051: Crypto mapdb : proxy_match
src addr : 10.62.148.79
dst addr : 10.48.23.85
protocol : 0
src port : 0
dst port : 0
Apr 25 18:57:37.051: (ipsec_process_proposal)Map Accepted: MAP-IKEV2, 10
Apr 25 18:57:37.051: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Callback received for SA

Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Close PKI Session
Apr 25 18:57:37.052: IKEv2:(SA ID = 1):[PKI -> IKEv2] Closing of PKI Session PASSED
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):IKEV2 SA created; inserting SA into database. SA ID= 1
Apr 25 18:57:37.053: IKEv2:(SESSION ID = 5,SA ID = 1):Session with IKE ID PAIR (cn=ise332.example.com, local=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
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

```

Dépannage sur ISE

Débugages à activer

Aucun débogage spécifique ne doit être activé sur ISE. Pour imprimer les débogages sur la console, exécutez la commande suivante :

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

Ensemble complet de débogages de travail sur 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 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 - ise332"
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 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 successfu
Apr 26 00:57:37 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.