

# Configuratie van ISE 3.3 Native IPsec voor beveiligde en beveiligde communicatie (IOS-XE)

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[IKEv2 IPsec-tunnel configureren met X.509-certificaatverificatie](#)

[Netwerkdigram](#)

[IOS-XE Switch CLI-configuratie](#)

[De interfaces configureren](#)

[Trustpoint configureren](#)

[Invoercertificaten](#)

[Het IKEv2-voorstel configureren](#)

[Een Crypto IKEv2-beleid configureren](#)

[Een Crypto IKEv2-profiel configureren](#)

[Configureer een ACL voor VPN-verkeer van belang](#)

[Een transformatieset configureren](#)

[Configureer een Crypto-kaart en pas deze toe op een interface](#)

[IOS-XE definitieve configuratie](#)

[ISE-configuratie](#)

[IP-adres op ISE configureren](#)

[Trusted Store-certificaat importeren](#)

[Certificaat voor het invoersysteem](#)

[IPsec-tunnel configureren](#)

[Configureer IKEv2 IPsec-tunnel met X.509 vooraf gedeelde sleutelverificatie](#)

[Netwerkdigram](#)

[IOS-XE Switch CLI-configuratie](#)

[De interfaces configureren](#)

[Het IKEv2-voorstel configureren](#)

[Een Crypto IKEv2-beleid configureren](#)

[Een Crypto IKEv2-profiel configureren](#)

[Configureer een ACL voor VPN-verkeer van belang](#)

[Een transformatieset configureren](#)

[Configureer een Crypto-kaart en pas deze toe op een interface](#)

[IOS-XE definitieve configuratie](#)

[ISE-configuratie](#)

[IP-adres op ISE configureren](#)

[IPsec-tunnel configureren](#)

[Verifiëren](#)

[Verifiëren op IOS-XE](#)

[Verifiëren op ISE](#)

---

## [Problemen oplossen](#)

[Probleemoplossing op IOS-XE](#)

[Debugs om in te schakelen](#)

[Volledige set van werkende debugs op IOS-XE](#)

[Probleemoplossing op ISE](#)

[Debugs om in te schakelen](#)

[Volledige set van werkende debugs op ISE](#)

---

# Inleiding

Dit document beschrijft hoe u Native IPsec kunt configureren en probleemoplossing biedt om de communicatie met Cisco Identity Service Engine (ISE) 3.3 - Network Access Device (NAD) te beveiligen. Radius-verkeer kan worden versleuteld met de IPsec Internet Key Exchange versie 2 (IKEv2)-tunnel tussen Switch en ISE. Dit document is niet van toepassing op het onderdeel RADIUS-configuratie.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Cisco-Switch configureren
- Algemene IPsec-concepten
- Algemene RADIUS-concepten

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst Switch C9200L waarop software versie 17.6.5 wordt uitgevoerd
- Cisco Identity Service Engine versie 3.3
- Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Achtergrondinformatie

Het doel is om protocollen te beveiligen die onveilige MD5 hash, RADIUS en TACACS met IPsec gebruiken. Weinig feiten waarmee rekening moet worden gehouden:

- Cisco ISE-native IPsec-oplossing is gebaseerd op [StrongSwan](#)
- Wanneer u IPsec op een Cisco ISE-interface configureert, wordt er een IPsec-tunnel

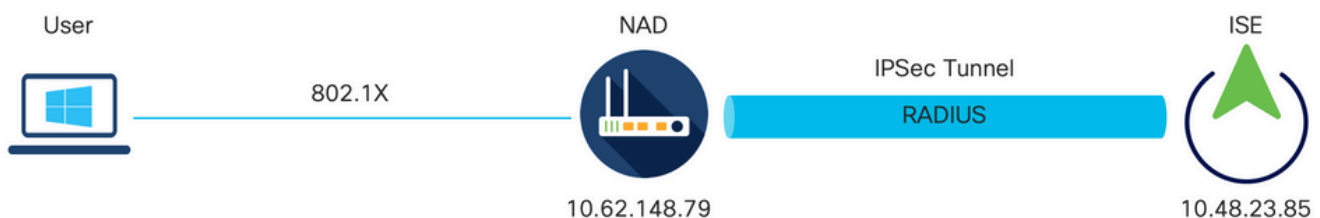
gemaakt tussen Cisco ISE en de NAD om de communicatie te beveiligen. NAD moet afzonderlijk worden geconfigureerd onder native IPsec-instellingen.

- U kunt een vooraf gedeelde sleutel definiëren of X.509-certificaten gebruiken voor IPsec-verificatie.
- IPsec kan worden ingeschakeld op Gigabit Ethernet1 via Gigabit Ethernet5-interfaces.

Het document zal zich vooral richten op de X.509-certificaatverificatie. Verifieer en probleemoplossing sectie richt zich alleen op X.509-certificaatverificatie, de debugging zou precies hetzelfde moeten zijn voor Pre-Shared Key Verificatie, met alleen verschil in uitgangen. De zelfde bevelen kunnen voor controle eveneens worden gebruikt.

## IKEv2 IPsec-tunnel configureren met X.509-certificaatverificatie

### Netwerkdigram



Netwerkdigram

### IOS-XE Switch CLI-configuratie

#### De interfaces configureren

Als de IOS-XE Switch interfaces nog niet geconfigureerd zijn, moet ten minste één interface worden geconfigureerd. Hierna volgt een voorbeeld:


```
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
!
```

Zorg ervoor dat er connectiviteit is met de externe peer die moet worden gebruikt om een site-to-site VPN-tunnel te maken. U kunt gebruiken pingelt om basisconnectiviteit te verifiëren.

## Trustpoint configureren

Om het IKEv2-beleid te configureren voert u de opdracht `crypto pki trustpoint <name>` in in de globale configuratiemodus. Hierna volgt een voorbeeld:

---

 **Opmerking:** er zijn meerdere manieren om certificaten te installeren op IOS-XE-apparaten. In dit voorbeeld gebruiken we import van pkcs12-bestand, dat het identiteitsbewijs en de bijbehorende keten bevat

---

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


## Invoercertificaten

Als u IOS-XE-identiteitscertificaat en de bijbehorende keten wilt importeren, voert u de opdracht `crypto-pincode importeren <trustpoint> pkcs12 <location>`, wachtwoord `<wachtwoord>` in in de geprivilegieerde modus. Hierna volgt een voorbeeld:

```
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#
```

---

 **N.B.:** Ook al vallen certificaten buiten het bereik van het document, zorg er dan voor dat IOS-XE identiteitsbewijs SAN-velden met zijn FQDN/IP-adres bevat. ISE vereist peer-certificaat om SAN-veld te hebben.

---

Om te controleren of de certificaten correct zijn geïnstalleerd:

```
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#

### Het IKEv2-voorstel configureren

Om het IKEv2-beleid te configureren voert u de opdracht `crypto ikev2 voorstel <naam>` in in de globale configuratiemodus. Hierna volgt een voorbeeld:

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

### Een Crypto IKEv2-beleid configureren

Als u het IKEv2-beleid wilt configureren, voert u de opdracht `crypto ikev2-beleid <naam>` in in de globale configuratiemodus:

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

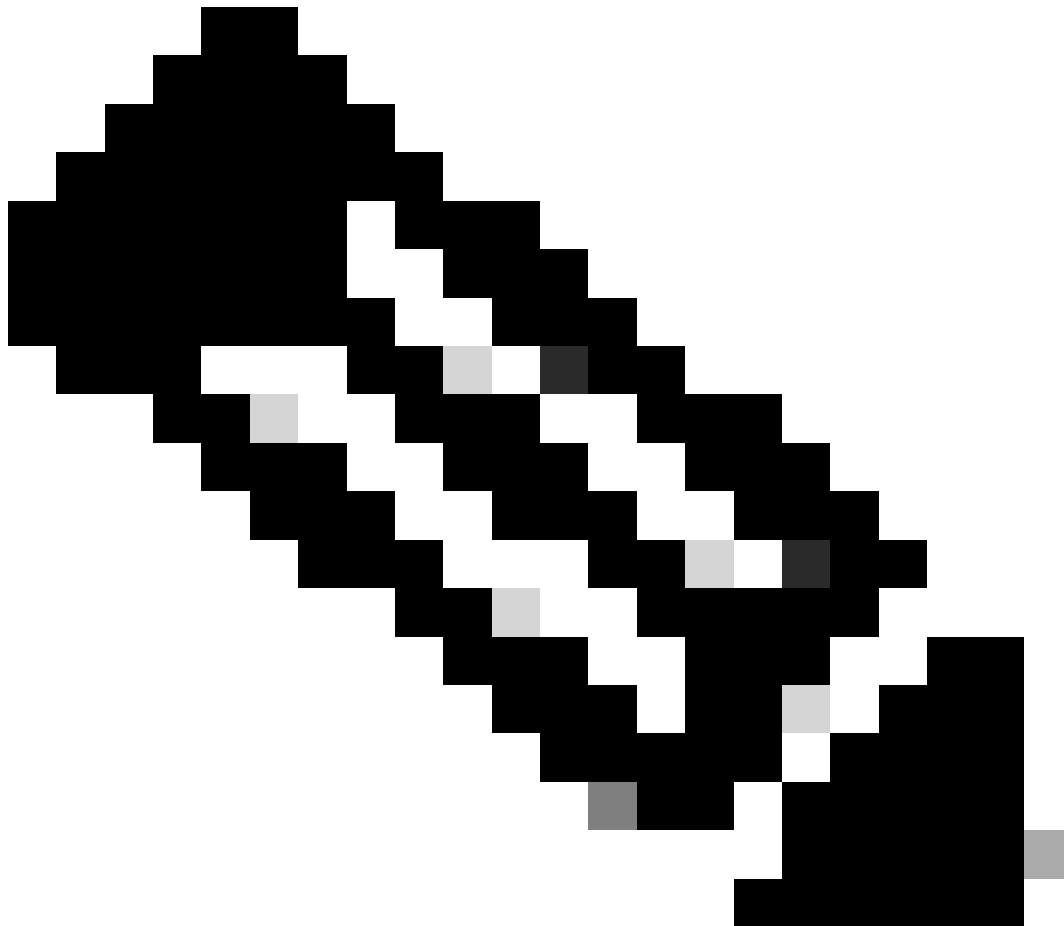
### Een Crypto IKEv2-profiel configureren

Als u het IKEv2-profiel wilt configureren, voert u de opdracht `crypto ikev2-profiel <naam>` in in de globale configuratiemodus.

```
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
```

---



Opmerking: standaard gebruikt ISE CN-veld van zijn eigen identiteitscertificaat als IKE-identiteit in IKEv2-onderhandeling. Daarom moet u in de sectie "match identiteits remote" van het IKEv2-profiel het FQDN-type en de juiste waarde van het domein of FQDN van ISE specificeren.

---

Configureer een ACL voor VPN-verkeer van belang

Gebruik de uitgebreide of benoemde toegangslijst om aan te geven welk verkeer door codering moet worden beveiligd. Hierna volgt een voorbeeld:

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

---

 N.B.: Een ACL voor VPN-verkeer gebruikt de IP-adressen van bron en bestemming na NAT.

---

## Een transformatieset configureren

Als u een IPsec-transformatieset (een aanvaardbare combinatie van beveiligingsprotocollen en algoritmen) wilt definiëren, voert u de opdracht `crypto ipsec transform-set` in in de globale configuratiemodus. Hierna volgt een voorbeeld:

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

## Configureer een Crypto-kaart en pas deze toe op een interface

Om een crypto kaartingang te creëren of te wijzigen en de crypto kaartconfiguratiemodus in te gaan, ga het globale configuratiebevel van de kaart `crypto in`. Om de crypto-kaartvermelding volledig te maken, zijn er bepaalde aspecten die op zijn minst moeten worden gedefinieerd:

- De IPsec-peers waarnaar het beveiligde verkeer kan worden doorgestuurd, moeten worden gedefinieerd. Dit zijn de peers waarmee een SA kan worden opgericht. Voer de ingestelde peer-opdracht in om een IPsec-peer in een cryptografische toewijzingsopdracht te specificeren.
- De transformatiesets die acceptabel zijn voor gebruik met het beschermde verkeer moeten worden gedefinieerd. Om de transformatiereeksen te specificeren die met de crypto kaartingang kunnen worden gebruikt, ga het vastgestelde transformatie-vastgestelde bevel in.
- Het verkeer dat beschermd moet worden, moet gedefinieerd worden. Om een uitgebreide toegangslijst voor een crypto kaartingang te specificeren, ga het bevel van het matchadres in.

Hierna volgt een voorbeeld:

```
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
```

De laatste stap is om de eerder gedefinieerde crypto map toe te passen die is ingesteld op een

interface. Om dit toe te passen, ga het bevel van de interfaceconfiguratie van de crypto kaart in:

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

## IOS-XE definitieve configuratie

Hier is de definitieve CLI-configuratie van de IOS-XE switch:

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



```
match address 100
!
interface GigabitEthernet1/0/23
switchport trunk allowed vlan 1,480
switchport mode trunk
!
interface Vlan480
ip address 10.62.148.79 255.255.255.128
crypto map MAP-IKEV2
!
ip access-list extended 100
10 permit ip host 10.62.148.79 host 10.48.23.85
!
radius server ISE33-2
address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
key cisco
!
```

## ISE-configuratie

### IP-adres op ISE configureren

Adres moet op interface GE1-GE5 van de CLI zijn geconfigureerd, GE0 wordt niet ondersteund.

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



Opmerking: toepassing wordt opnieuw gestart nadat IP-adres op de interface is geconfigureerd:

% Als u het IP-adres wijzigt, kunnen de ISE-services opnieuw worden gestart

Doorgaan met wijziging van IP-adres? J/N [N]: Y

---

### Trusted Store-certificaat importeren

Deze stap is nodig om ervoor te zorgen dat ISE het certificaat van de peer die bij de tijdtunnel wordt gepresenteerd, vertrouwt. Navigeer naar Beheer > Systeem > Certificaten > Betrouwbare certificaten. Klik op Import (Importeren). Klik op Bladeren en selecteer CA-certificaat dat is ondertekend door ISE/IOS-XE. Zorg ervoor dat het selectievakje Vertrouwen voor verificatie is ingeschakeld in ISE. Klik op Verzenden.

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 IPsec
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services
- Validate Certificate Extensions

Description

## Certificaat voor het invoersysteem

Navigeer naar Beheer > Systeem > Certificaten > Systeemcertificaten. Selecteer Knooppunt, certificaatbestand en Private-key bestand importeren. Selecteer het aanvinkvakje tegen IPsec. Klik op Verzenden.

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



Opmerking: Certificaten worden ALLEEN op de StrongSwan geïnstalleerd nadat u Netwerktogangsapparaat hebt opgeslagen onder Native IPsec-instellingen.

## IPsec-tunnel configureren

Ga naar Beheer > Systeem > Instellingen > Protocollen > IPsec > Native IPsec. Klik op Toevoegen. Selecteer knooppunt, waarmee IPsec-tunnel wordt beëindigd, en IP-adres configureren met masker, standaardgateway en IPsec-interface. Selecteer Verificatie-instelling als

X.509-certificaat en kies Certificaatsysteemcertificaat geïnstalleerd.

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 v

EAP-FAST v  
EAP-TLS  
PEAP  
EAP-TTLS  
RADIUS

IPsec v  
Legacy IPsec (ESR)  
Native IPsec

Native IPsec Configuration > New

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

### Node Specific Settings

Select Node  
ise332

NAD IP Address with Mask  
10.62.147.79/32

Default Gateway (optional)  
10.48.23.1

IPsec Interface  
Gigabit Ethernet 1

Authentication Settings

Pre-shared Key

X.509 Certificate IPSEC-2

Default Gateway is een optionele configuratie. In feite, hebt u twee opties, kunt u een StandaardGateway in Inheemse IPsec UI vormen, die een route in onderliggende OS installeert. Deze route wordt niet blootgesteld in show in werking stelt -in werking stellen-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#
```

Een andere optie is om Default Gateway leeg te laten en de route handmatig te configureren op ISE, dit zal hetzelfde effect bereiken:

```
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#
```

Algemene instellingen voor IPsec-tunnel configureren. Configureer de instellingen voor fase één. Algemene instellingen, fase één instellingen en fase twee instellingen moeten overeenkomen met de instellingen die aan de andere kant van de IPsec-tunnel zijn ingesteld.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The top navigation bar includes 'Administration / System' and a menu icon. Below the navigation bar, there are tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', and 'Backup & Restore'. The main content area is divided into a left sidebar and a main panel. The sidebar contains a 'Protocols' section with a dropdown menu showing 'EAP-FAST', 'EAP-TLS', 'PEAP', 'EAP-TTLS', 'RADIUS', 'IPSec' (with sub-items 'Legacy IPsec (ESR)' and 'Native IPsec'), and 'Endpoint Scripts'. The main panel displays the 'General Settings' for IPsec. The settings are grouped into 'General Settings' and 'Phase One Settings'. The 'General Settings' section includes: 'IKE Version' (IKEv2), 'Mode' (Tunnel), 'ESP/AH Protocol' (esp), 'IKE Reauth Time (optional)' (86400). The 'Phase One Settings' section includes: 'Encryption Algorithm' (aes256), 'Hash Algorithm' (sha512), 'DH Group' (GROUP16), and 'Re-key time (optional)' (14400). Each setting is enclosed in a red box, and there is a help icon (i) next to each one.

Configureer fase twee instellingen en klik op Opslaan.

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

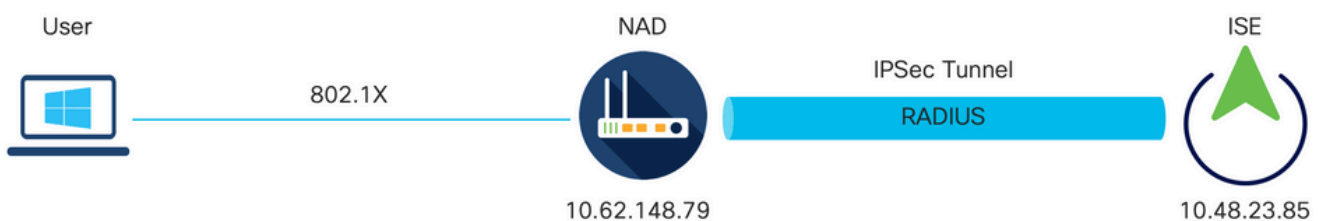
Phase Two Settings  
Configure Native IPSec SA Configuration security settings to protect IP traffic between two endpoints.

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

Cancel Save

## Configureer IKEv2 IPsec-tunnel met X.509 vooraf gedeelde sleutelverificatie

### Netwerkdigram



Netwerkdigram

### IOS-XE Switch CLI-configuratie

De interfaces configureren

Als de IOS-XE Switch interfaces nog niet geconfigureerd zijn, moet ten minste één interface worden geconfigureerd. Hierna volgt een voorbeeld:

```
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
!
```

Zorg ervoor dat er connectiviteit is met de externe peer die moet worden gebruikt om een site-to-site VPN-tunnel te maken. U kunt gebruiken pingelt om basisconnectiviteit te verifiëren.

### Het IKEv2-voorstel configureren

Om het IKEv2-beleid te configureren voert u de opdracht `crypto ikev2 voorstel <naam>` in in de globale configuratiemodus. Hierna volgt een voorbeeld:

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

### Een Crypto IKEv2-beleid configureren

Als u het IKEv2-beleid wilt configureren, voert u de opdracht `crypto ikev2-beleid <naam>` in in de globale configuratiemodus:

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

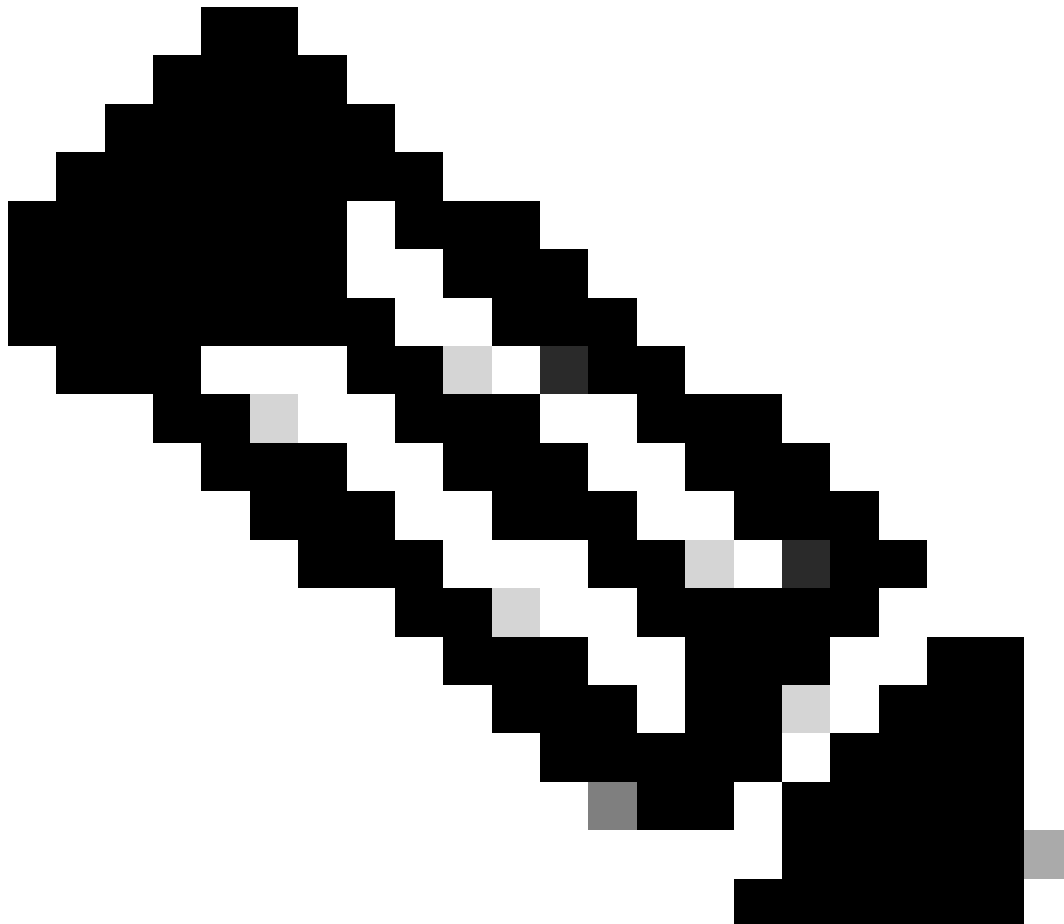
### Een Crypto IKEv2-profiel configureren

Als u het IKEv2-profiel wilt configureren, voert u de opdracht `crypto ikev2-profiel <naam>` in in de globale configuratiemodus.

```
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
```

---



Opmerking: standaard gebruikt ISE CN-veld van zijn eigen identiteitscertificaat als IKE-identiteit in IKEv2-onderhandeling. Daarom moet u in de sectie "match identiteits remote" van het IKEv2-profiel het FQDN-type en de juiste waarde van het domein of FQDN van ISE specificeren.

---

Configureer een ACL voor VPN-verkeer van belang

Gebruik de uitgebreide of benoemde toegangslijst om aan te geven welk verkeer door codering moet worden beveiligd. Hierna volgt een voorbeeld:

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

---

 N.B.: Een ACL voor VPN-verkeer gebruikt de IP-adressen van bron en bestemming na NAT.

---

## Een transformatieset configureren

Als u een IPsec-transformatieset (een aanvaardbare combinatie van beveiligingsprotocollen en algoritmen) wilt definiëren, voert u de opdracht `crypto ipsec transform-set` in in de globale configuratiemodus. Hierna volgt een voorbeeld:

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

## Configureer een Crypto-kaart en pas deze toe op een interface

Om een crypto kaartingang te creëren of te wijzigen en de crypto kaartconfiguratiemodus in te gaan, ga het globale configuratiebevel van de kaart `crypto` in. Om de crypto-kaartvermelding volledig te maken, zijn er bepaalde aspecten die op zijn minst moeten worden gedefinieerd:

- De IPsec-peers waarnaar het beveiligde verkeer kan worden doorgestuurd, moeten worden gedefinieerd. Dit zijn de peers waarmee een SA kan worden opgericht. Voer de ingestelde peer-opdracht in om een IPsec-peer in een cryptografische toewijzingsopdracht te specificeren.
- De transformatiesets die acceptabel zijn voor gebruik met het beschermde verkeer moeten worden gedefinieerd. Om de transformatiereksen te specificeren die met de crypto kaartingang kunnen worden gebruikt, ga het vastgestelde transformatie-vastgestelde bevel in.
- Het verkeer dat beschermd moet worden, moet gedefinieerd worden. Om een uitgebreide toegangslijst voor een crypto kaartingang te specificeren, ga het bevel van het matchadres in.

Hierna volgt een voorbeeld:

```
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
```

De laatste stap is om de eerder gedefinieerde crypto map toe te passen die is ingesteld op een



interface. Om dit toe te passen, ga het bevel van de interfaceconfiguratie van de crypto kaart in:

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

## IOS-XE definitieve configuratie

Hier is de definitieve CLI-configuratie van de IOS-XE switch:

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

```
ip address 10.62.148.79 255.255.255.128
crypto map MAP-IKEV2
!
ip access-list extended 100
 10 permit ip host 10.62.148.79 host 10.48.23.85
!
radius server ISE33-2
  address ipv4 10.48.23.85 auth-port 1812 acct-port 1813
  key cisco
!
```

## ISE-configuratie

### IP-adres op ISE configureren

Adres moet op interface GE1-GE5 van de CLI zijn geconfigureerd, GE0 wordt niet ondersteund.

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



Opmerking: toepassing wordt opnieuw gestart nadat IP-adres op de interface is geconfigureerd:

% Als u het IP-adres wijzigt, kunnen de ISE-services opnieuw worden gestart

Doorgaan met wijziging van IP-adres? J/N [N]: Y

---

### IPsec-tunnel configureren

Ga naar Beheer > Systeem > Instellingen > Protocollen > IPsec > Native IPsec. Klik op Toevoegen. Selecteer knooppunt, waarmee IPsec-tunnel wordt beëindigd, en IP-adres configureren met masker, standaardgateway en IPsec-interface. Selecteer Verificatie-instelling als X.509-certificaat en kies Certificaatsysteemcertificaat geïnstalleerd.

Default Gateway is een optionele configuratie. In feite, hebt u twee opties, kunt u een StandaardGateway in Inheemse IPsec UI vormen, die een route in onderliggende OS installeert. Deze route wordt niet blootgesteld in show in werking stelt -in werking stellen-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#
```

Een andere optie is om Default Gateway leeg te laten en de route handmatig te configureren op

ISE, dit zal hetzelfde effect bereiken:

```
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#
```

Algemene instellingen voor IPsec-tunnel configureren. Configureer de instellingen voor fase één. Algemene instellingen, fase één instellingen en fase twee instellingen moeten overeenkomen met de instellingen die aan de andere kant van de IPsec-tunnel zijn ingesteld.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar contains a navigation menu with options: 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), and Endpoint Scripts. 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
- 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

Configureer fase twee instellingen en klik op Opslaan.

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains navigation options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. Under the Protocols section, Native IPsec is selected. The main area displays the Phase Two Settings for Native IPsec, which are used to protect IP traffic between two endpoints. The settings include: Encryption Algorithm (aes256), Hash Algorithm (sha512), DH Group (optional) (GROUP16), and Re-key time (optional) (14400). A red box highlights the Save button at the bottom right of the configuration area.

## Verifiëren

Om er zeker van te zijn dat RADIUS via IPsec Tunnel werkt, gebruikt u de opdracht Test Aa of voert u de daadwerkelijke MAB- of 802.1X-verificatie uit

```
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#
```

## Verifiëren op 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#

## Verifiëren op ISE

De status van de tunnel kan worden geverifieerd vanuit GUI

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes 'Administration / System' and 'Settings'. The left sidebar contains various configuration options like 'Client Provisioning', 'FIPS Mode', 'Security Settings', 'Alarm Settings', 'General MDM / UEM Settings', 'Posture', 'Profiling', 'Protocols', 'EAP-FAST', and 'EAP-TLS'. The main content area is titled 'Native IPsec Configuration' and contains a table with the following data:

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

Gebruik applicatie configureren ISE-opdracht om de status van de tunnel vanaf CLI te verifiëren

<#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
```

## Problemen oplossen

### Probleemoplossing op IOS-XE

#### Debugs om in te schakelen

```
<#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#
```

#### Volledige set van werkende debugs op 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 SKID  
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  
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

```

## Probleemoplossing op ISE

### Debugs om in te schakelen

Er zijn geen specifieke debugs die op ISE moeten worden ingeschakeld, om de debugs af te drukken naar de console problemen het commando:

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

### Volledige set van werkende debugs op 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 - 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 successfu  
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]
```

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.