

# Konfigurieren der IOS-XE-Kommunikation (ISE 3.3 Native IPsec to Secure NAD)

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren des IKEv2-IPsec-Tunnels mit X.509-Zertifikatauthentifizierung](#)

[Netzwerkdiagramm](#)

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

[Schnittstellen konfigurieren](#)

[Vertrauenspunkt konfigurieren](#)

[Zertifikate importieren](#)

[Konfigurieren des IKEv2-Angebots](#)

[Konfigurieren einer IKEv2-Kryptografierichtlinie](#)

[Konfigurieren eines Krypto-IKEv2-Profiles](#)

[ACL für relevanten VPN-Datenverkehr konfigurieren](#)

[Transformationssatz konfigurieren](#)

[Crypto Map konfigurieren und auf eine Schnittstelle anwenden](#)

[IOS-XE - Abschlusskonfiguration](#)

[ISE-Konfiguration](#)

[Konfigurieren der IP-Adresse auf der ISE](#)

[Zertifikat für vertrauenswürdigen Speicher importieren](#)

[Systemzertifikat importieren](#)

[Konfigurieren von IPsec-Tunnel](#)

[Konfigurieren des IKEv2-IPsec-Tunnels mit X.509 Pre-Shared Key Authentication](#)

[Netzwerkdiagramm](#)

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

[Schnittstellen konfigurieren](#)

[Konfigurieren des IKEv2-Angebots](#)

[Konfigurieren einer IKEv2-Kryptografierichtlinie](#)

[Konfigurieren eines Krypto-IKEv2-Profiles](#)

[ACL für relevanten VPN-Datenverkehr konfigurieren](#)

[Transformationssatz konfigurieren](#)

[Crypto Map konfigurieren und auf eine Schnittstelle anwenden](#)

[IOS-XE - Abschlusskonfiguration](#)

[ISE-Konfiguration](#)

[Konfigurieren der IP-Adresse auf der ISE](#)

[Konfigurieren von IPsec-Tunnel](#)

[Überprüfung](#)

[Überprüfung auf IOS-XE](#)

[Auf ISE überprüfen](#)

---

## [Fehlerbehebung](#)

[Fehlerbehebung unter IOS-XE](#)

[Zu aktivierende Debugs](#)

[Vollständiger Satz funktionierender Debugs für IOS-XE](#)

[Fehlerbehebung auf der ISE](#)

[Zu aktivierende Debugs](#)

[Vollständiger Satz funktionierender Debugs für ISE](#)

---

# Einleitung

In diesem Dokument wird beschrieben, wie Sie native IPsec konfigurieren und Fehler beheben, um die Cisco Identity Service Engine (ISE) 3.3 - Network Access Device (NAD)-Kommunikation zu sichern. Radius-Datenverkehr kann mit einem Site-to-Site (LAN-to-LAN) IPsec Internet Key Exchange Version 2 (IKEv2)-Tunnel zwischen Switch und ISE verschlüsselt werden. In diesem Dokument wird nicht auf den RADIUS-Konfigurationsteil eingegangen.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE
- Cisco Switch-Konfiguration
- Allgemeine IPSec-Konzepte
- Allgemeine RADIUS-Konzepte

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switch C9200L mit Softwareversion 17.6.5
- Cisco Identity Service Engine Version 3.3
- Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

# Hintergrundinformationen

Ziel ist die Sicherung von Protokollen, die unsicheren MD5-Hash, RADIUS und TACACS verwenden, mit IPsec. Nur wenige Fakten, die berücksichtigt werden sollten:

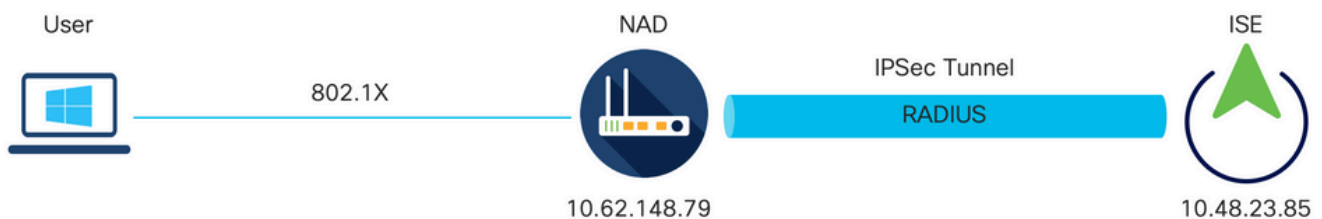
- Die Cisco ISE Native IPsec-Lösung basiert auf [StrongSwan](#)

- Wenn Sie IPsec auf einer Cisco ISE-Schnittstelle konfigurieren, wird ein IPsec-Tunnel zwischen der Cisco ISE und dem NAD erstellt, um die Kommunikation zu sichern. NAD sollte unter den nativen IPsec-Einstellungen separat konfiguriert werden.
- Sie können einen vorinstallierten Schlüssel definieren oder X.509-Zertifikate für die IPsec-Authentifizierung verwenden.
- IPsec kann auf GigabitEthernet1- bis GigabitEthernet5-Schnittstellen aktiviert werden.

Der Schwerpunkt des Dokuments liegt auf der X.509-Authentifizierung von Zertifikaten. Der Abschnitt Überprüfen und Fehlerbehebung konzentriert sich nur auf die X.509-Zertifikatauthentifizierung. Das Debuggen sollte für die Pre-Shared Key-Authentifizierung genau gleich sein, mit nur unterschiedlichen Ausgaben. Dieselben Befehle können auch zur Überprüfung verwendet werden.

## Konfigurieren des IKEv2-IPsec-Tunnels mit X.509-Zertifikatauthentifizierung

### Netzwerkdiagramm



Netzwerkdiagramm

### IOS-XE Switch CLI-Konfiguration

#### Schnittstellen konfigurieren

Wenn die IOS-XE Switch-Schnittstellen noch nicht konfiguriert sind, muss mindestens eine Schnittstelle konfiguriert werden. Hier ein Beispiel:

```


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
!
  
```

Stellen Sie sicher, dass eine Verbindung zum Remote-Peer besteht, die zum Einrichten eines Site-to-Site-VPN-Tunnels verwendet werden soll. Sie können einen Ping verwenden, um die grundlegenden Netzwerkverbindungen zu überprüfen.

## Vertrauenspunkt konfigurieren

Um die IKEv2-Richtlinien zu konfigurieren, geben Sie den Befehl `crypto pki trustpoint <name>` im globalen Konfigurationsmodus ein. Hier ein Beispiel:

---

 Hinweis: Es gibt mehrere Möglichkeiten, Zertifikate auf IOS-XE-Geräten zu installieren. In diesem Beispiel verwenden wir den Import der Datei pkcs12, die das Identitätszertifikat und seine Kette enthält

---

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


## Zertifikate importieren

Um das IOS-XE-Identitätszertifikat zusammen mit der zugehörigen Kette zu importieren, geben Sie den Befehl `crypto pki import <trustpoint> pkcs12 <location> password <password>` im privilegierten Modus ein. Hier ein Beispiel:

```
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#
```

---

 Hinweis: Auch wenn Zertifikate nicht im Umfang des Dokuments enthalten sind, stellen Sie sicher, dass das IOS-XE-Identitätszertifikat über SAN-Felder mit seiner FQDN/IP-Adresse verfügt. Für die ISE ist ein Peer-Zertifikat mit SAN-Feld erforderlich.

---

So überprüfen Sie, ob die Zertifikate ordnungsgemäß installiert sind:

```
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#

## Konfigurieren des IKEv2-Angebots

Um die IKEv2-Richtlinien zu konfigurieren, geben Sie den Befehl `crypto ikev2 offer <name>` im globalen Konfigurationsmodus ein. Hier ein Beispiel:

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

## Konfigurieren einer IKEv2-Kryptografierichtlinie

Um die IKEv2-Richtlinien zu konfigurieren, geben Sie den Befehl `crypto ikev2 policy <name>` im globalen Konfigurationsmodus ein:

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

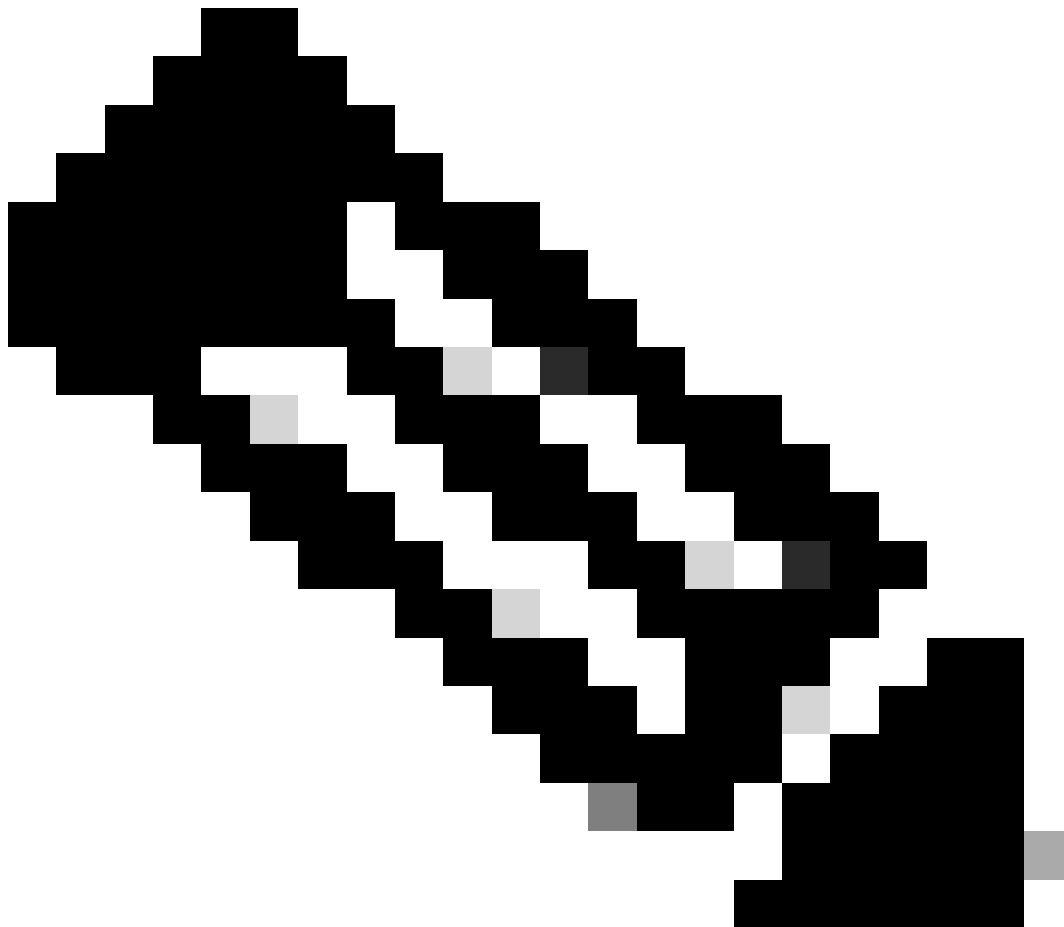
## Konfigurieren eines Krypto-IKEv2-Profiles

Um das IKEv2-Profil zu konfigurieren, geben Sie den Befehl `crypto ikev2 profile <name>` im

globalen Konfigurationsmodus ein.

```
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
```

---



Hinweis: Standardmäßig verwendet die ISE das CN-Feld ihres eigenen Identitätszertifikats als IKE-Identität in der IKEv2-Aushandlung. Aus diesem Grund müssen Sie im IKEv2-Profil im Abschnitt "match identity remote" den FQDN-Typ und den korrekten Wert der Domäne oder des FQDN der ISE angeben.


---

ACL für relevanten VPN-Datenverkehr konfigurieren

Verwenden Sie die erweiterte oder benannte Zugriffsliste, um den Datenverkehr anzugeben, der durch Verschlüsselung geschützt werden soll. Hier ein Beispiel:

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

---

 Hinweis: Eine ACL für VPN-Datenverkehr verwendet die Quell- und Ziel-IP-Adressen nach NAT.

---

## Transformationssatz konfigurieren

Geben Sie im globalen Konfigurationsmodus den Befehl `crypto ipsec transform-set` ein, um einen IPSec-Transformationssatz (eine akzeptable Kombination aus Sicherheitsprotokollen und Algorithmen) zu definieren. Hier ein Beispiel:

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

## Crypto Map konfigurieren und auf eine Schnittstelle anwenden

Geben Sie den Befehl `crypto map global configuration` ein, um einen Crypto Map-Eintrag zu erstellen oder zu ändern und den Konfigurationsmodus für Crypto Map zu aktivieren. Damit der Crypto Map-Eintrag vollständig ist, müssen einige Aspekte definiert werden:

- Die IPsec-Peers, an die der geschützte Datenverkehr weitergeleitet werden kann, müssen definiert werden. Dies sind die Peers, mit denen eine SA eingerichtet werden kann. Geben Sie den Befehl `set peer` ein, um einen IPSec-Peer in einem Crypto Map-Eintrag anzugeben.
- Die für die Verwendung mit dem geschützten Datenverkehr akzeptablen Transformationssätze müssen definiert werden. Geben Sie den Befehl `set transform-set` ein, um die Transformationssätze anzugeben, die mit dem Crypto Map-Eintrag verwendet werden können.
- Der zu schützende Datenverkehr muss definiert werden. Geben Sie den Befehl `match address` ein, um eine erweiterte Zugriffsliste für einen Crypto Map-Eintrag anzugeben.

Hier ein Beispiel:

```
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
```

Der letzte Schritt ist die Anwendung der zuvor definierten Crypto Map-Gruppe auf eine Schnittstelle. Geben Sie hierzu den Befehl crypto map für die Schnittstellenkonfiguration ein:

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

## IOS-XE - Abschlusskonfiguration

Die CLI des IOS-XE-Switches lautet wie folgt:

```
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-Konfiguration

### Konfigurieren der IP-Adresse auf der ISE


Die Adresse sollte über die CLI für die GE1-GE5-Schnittstelle konfiguriert werden. GE0 wird nicht unterstützt.

```

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

```

---

 Hinweis: Die Anwendung wird neu gestartet, nachdem die IP-Adresse auf der Schnittstelle konfiguriert wurde:

% Eine Änderung der IP-Adresse kann einen Neustart der ISE-Dienste verursachen.

Mit IP-Adressänderung fortfahren? J/N [N]: J

---

### Zertifikat für vertrauenswürdigen Speicher importieren

Dieser Schritt ist erforderlich, um sicherzustellen, dass die ISE dem Zertifikat des Peers vertraut, der zum Zeitpunkt der Tunnelerstellung präsentiert wird. Navigieren Sie zu Administration > System > Certificates > Trusted Certificates. Klicken Sie auf Importieren. Klicken Sie auf Browse (Durchsuchen), und wählen Sie ein Zertifizierungsstellenzertifikat aus, das das ISE/IOS-XE-Identitätszertifikat signiert hat. Stellen Sie sicher, dass das Kontrollkästchen Bei Authentifizierung innerhalb der ISE vertrauen aktiviert ist. Klicken Sie auf Senden.

The screenshot shows the 'Import a new Certificate into the Certificate Store' form in the Cisco Identity Services Engine Administration / System interface. The form includes the following fields and options:

- Certificate File:** KrakowCA.crt
- Friendly Name:** (empty)
- 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:** (empty)

A red box highlights the 'Submit' button at the bottom right of the form.

## Systemzertifikat importieren

Navigieren Sie zu Administration > System > Certificates > System Certificates. Wählen Sie Knoten, Zertifikatsdatei und Datei-Import mit privatem Schlüssel aus. Aktivieren Sie das Kontrollkästchen für IPsec. Klicken Sie auf Senden.

The screenshot shows the 'Import Server Certificate' form in the Cisco Identity Services Engine Administration / System interface. The form includes the following fields and options:

- Select Node:** ise332
- Certificate File:** ise332.example.com.pem
- Private Key File:** ise332.example.com.key
- Password:** (empty)
- Friendly Name:** IPSEC-2
- Allow Wildcard Certificates:**
- Validate Certificate Extensions:**
- Usage:**
  - Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect
  - EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
  - RADIUS DTLS: Use certificate for the RADSec server
  - pxGrid: Use certificate for the pxGrid Controller
  - ISE Messaging Service: Use certificate for the ISE Messaging Service
  - IPSEC: Use certificate for StrongSwan
  - SAML: Use certificate for SAML Signing
  - Portal: Use for portal

A red box highlights the 'Submit' button at the bottom right of the form.



Hinweis: Zertifikate werden NUR auf dem StrongSwan installiert, nachdem Sie das Netzwerkzugriffgerät unter den nativen IPsec-Einstellungen gespeichert haben.

## Konfigurieren von IPsec-Tunnel

Navigieren Sie zu Administration > System > Settings > Protocols > IPsec > Native IPsec. Klicken Sie auf Hinzufügen. Wählen Sie Node (Knoten) aus, der den IPsec-Tunnel beendet, und konfigurieren Sie die NAD-IP-Adresse mit Maske, Standard-Gateway und IPsec-

Schnittstelle. Wählen Sie Authentication Setting als X.509 Certificate und dann Certificate System Certificate Installed aus.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar contains navigation options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. The main content area is titled "Native IPSec Configuration > New" and contains "Node Specific Settings". Red boxes highlight the following fields:

- 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: X.509 Certificate (selected), IPSEC-2

Das Standard-Gateway ist eine optionale Konfiguration. Sie haben zwei Möglichkeiten: Sie können ein Standard-Gateway in der nativen IPsec-Benutzeroberfläche konfigurieren, die eine Route im zugrunde liegenden Betriebssystem installiert. Diese Route wird in show running-config nicht verfügbar gemacht:

```
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#
```

Eine weitere Option besteht darin, das Standard-Gateway leer zu lassen und die Route manuell auf der ISE zu konfigurieren. Dies hat denselben Effekt:

```
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#
```

Konfigurieren der allgemeinen Einstellungen für den IPsec-Tunnel Konfigurieren Sie die Einstellungen für Phase 1. Die allgemeinen Einstellungen, die ersten Einstellungen und die zweiten Einstellungen müssen mit den Einstellungen übereinstimmen, die auf der anderen Seite des IPsec-Tunnels konfiguriert wurden.

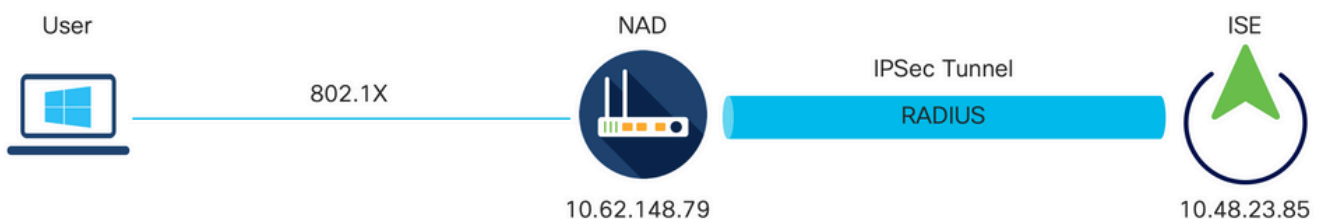
The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows a navigation menu with categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. The main content area is titled 'General Settings' and is divided into two sections: 'General Settings' and 'Phase One Settings'. The 'General Settings' section includes fields for 'IKE Version' (set to IKEv2), 'Mode' (set to Tunnel), 'ESP/AH Protocol' (set to esp), and 'IKE Reauth Time (optional)' (set to 86400). The 'Phase One Settings' section includes fields for 'Encryption Algorithm' (set to aes256), 'Hash Algorithm' (set to sha512), 'DH Group' (set to GROUP16), and 'Re-key time (optional)' (set to 14400). Each field has a dropdown arrow and a help icon.

Konfigurieren Sie die Einstellungen für Phase 2, und klicken Sie auf Speichern.

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains a navigation menu with categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. Under Protocols, the Native IPsec configuration is selected. The main content area displays the Phase Two Settings for Native IPsec, including Encryption Algorithm (aes256), Hash Algorithm (sha512), DH Group (GROUP16), and Re-key time (optional) (14400). The Save button is highlighted with a red box.

## Konfigurieren des IKEv2-IPsec-Tunnels mit X.509 Pre-Shared Key Authentication

### Netzwerkdiagramm



Netzwerkdiagramm

### IOS-XE Switch CLI-Konfiguration

## Schnittstellen konfigurieren

Wenn die IOS-XE Switch-Schnittstellen noch nicht konfiguriert sind, muss mindestens eine Schnittstelle konfiguriert werden. Hier ein Beispiel:

```
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
!
```

Stellen Sie sicher, dass eine Verbindung zum Remote-Peer besteht, die zum Einrichten eines Site-to-Site-VPN-Tunnels verwendet werden soll. Sie können einen Ping verwenden, um die grundlegenden Netzwerkverbindungen zu überprüfen.

## Konfigurieren des IKEv2-Angebots

Um die IKEv2-Richtlinien zu konfigurieren, geben Sie den Befehl `crypto ikev2 offer <name>` im globalen Konfigurationsmodus ein. Hier ein Beispiel:

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

## Konfigurieren einer IKEv2-Kryptografierichtlinie

Um die IKEv2-Richtlinien zu konfigurieren, geben Sie den Befehl `crypto ikev2 policy <name>` im globalen Konfigurationsmodus ein:

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

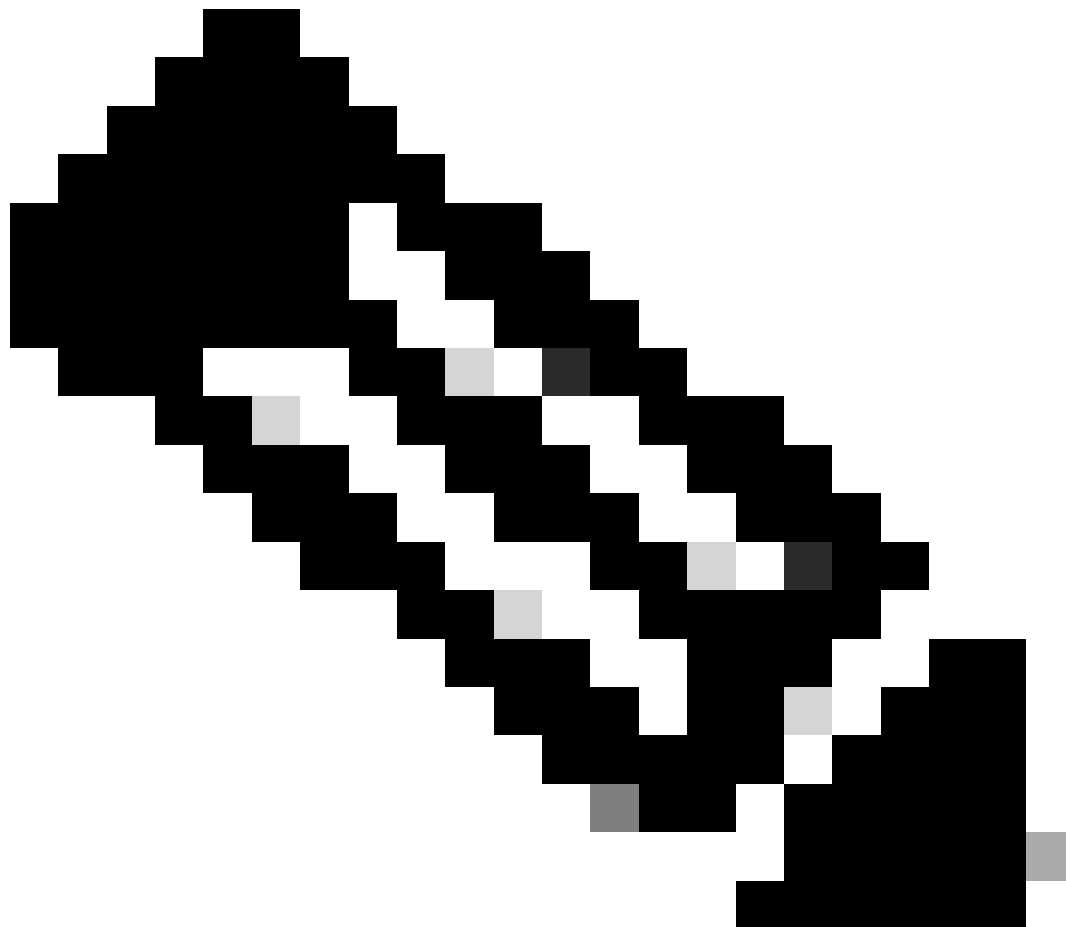
## Konfigurieren eines Krypto-IKEv2-Profiles

Um das IKEv2-Profil zu konfigurieren, geben Sie den Befehl `crypto ikev2 profile <name>` im

globalen Konfigurationsmodus ein.

```
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
```

---



Hinweis: Standardmäßig verwendet die ISE das CN-Feld ihres eigenen Identitätszertifikats als IKE-Identität in der IKEv2-Aushandlung. Aus diesem Grund müssen Sie im IKEv2-Profil im Abschnitt "match identity remote" den FQDN-Typ und den korrekten Wert der Domäne oder des FQDN der ISE angeben.


---

ACL für relevanten VPN-Datenverkehr konfigurieren

Verwenden Sie die erweiterte oder benannte Zugriffsliste, um den Datenverkehr anzugeben, der durch Verschlüsselung geschützt werden soll. Hier ein Beispiel:

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

---

 Hinweis: Eine ACL für VPN-Datenverkehr verwendet die Quell- und Ziel-IP-Adressen nach NAT.

---

## Transformationssatz konfigurieren

Geben Sie im globalen Konfigurationsmodus den Befehl `crypto ipsec transform-set` ein, um einen IPSec-Transformationssatz (eine akzeptable Kombination aus Sicherheitsprotokollen und Algorithmen) zu definieren. Hier ein Beispiel:

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

## Crypto Map konfigurieren und auf eine Schnittstelle anwenden

Geben Sie den Befehl `crypto map global configuration` ein, um einen Crypto Map-Eintrag zu erstellen oder zu ändern und den Konfigurationsmodus für Crypto Map zu aktivieren. Damit der Crypto Map-Eintrag vollständig ist, müssen einige Aspekte definiert werden:

- Die IPsec-Peers, an die der geschützte Datenverkehr weitergeleitet werden kann, müssen definiert werden. Dies sind die Peers, mit denen eine SA eingerichtet werden kann. Geben Sie den Befehl `set peer` ein, um einen IPSec-Peer in einem Crypto Map-Eintrag anzugeben.
- Die für die Verwendung mit dem geschützten Datenverkehr akzeptablen Transformationssätze müssen definiert werden. Geben Sie den Befehl `set transform-set` ein, um die Transformationssätze anzugeben, die mit dem Crypto Map-Eintrag verwendet werden können.
- Der zu schützende Datenverkehr muss definiert werden. Geben Sie den Befehl `match address` ein, um eine erweiterte Zugriffsliste für einen Crypto Map-Eintrag anzugeben.

Hier ein Beispiel:

```
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
```



Der letzte Schritt ist die Anwendung der zuvor definierten Crypto Map-Gruppe auf eine Schnittstelle. Geben Sie hierzu den Befehl crypto map für die Schnittstellenkonfiguration ein:

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

## IOS-XE - Abschlusskonfiguration

Die CLI des IOS-XE-Switches lautet wie folgt:

```
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-Konfiguration

### Konfigurieren der IP-Adresse auf der ISE

Die Adresse sollte über die CLI für die GE1-GE5-Schnittstelle konfiguriert werden. GE0 wird nicht unterstützt.

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

---

 Hinweis: Die Anwendung wird neu gestartet, nachdem die IP-Adresse auf der Schnittstelle konfiguriert wurde:  
% Eine Änderung der IP-Adresse kann einen Neustart der ISE-Dienste verursachen.  
Mit IP-Adressänderung fortfahren? J/N [N]: J

---

### Konfigurieren von IPsec-Tunnel

Navigieren Sie zu Administration > System > Settings > Protocols > IPsec > Native IPsec. Klicken Sie auf Hinzufügen. Wählen Sie Node (Knoten) aus, der den IPsec-Tunnel beendet, und konfigurieren Sie die NAD-IP-Adresse mit Maske, Standard-Gateway und IPsec-Schnittstelle. Wählen Sie Authentication Setting als X.509 Certificate und dann Certificate System Certificate Installed aus.

Das Standard-Gateway ist eine optionale Konfiguration. Sie haben zwei Möglichkeiten: Sie können ein Standard-Gateway in der nativen IPsec-Benutzeroberfläche konfigurieren, die eine Route im zugrunde liegenden Betriebssystem installiert. Diese Route wird in show running-config nicht verfügbar gemacht:

```
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#
```

Eine weitere Option besteht darin, das Standard-Gateway leer zu lassen und die Route manuell auf der ISE zu konfigurieren. Dies hat denselben Effekt:

```
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#
```

Konfigurieren der allgemeinen Einstellungen für den IPsec-Tunnel Konfigurieren Sie die Einstellungen für Phase 1. Die allgemeinen Einstellungen, die ersten Einstellungen und die zweiten Einstellungen müssen mit den Einstellungen übereinstimmen, die auf der anderen Seite des IPsec-Tunnels konfiguriert wurden.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows a navigation menu with categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. Under Protocols, the IPsec section is expanded, showing Legacy IPsec (ESR) and Native IPsec. The main content area is titled 'General Settings' and contains several configuration fields, some of which are highlighted with red boxes:

- IKE Version: IKEv2
- Mode: Tunnel
- ESP/AH Protocol: esp
- IKE Reauth Time (optional): 86400
- Encryption Algorithm: aes256
- Hash Algorithm: sha512
- DH Group: GROUP16
- Re-key time (optional): 14400

Below the Phase One Settings, there is a note: 'Configure IKE SA Configuration security settings to protect communications between two IKE daemons.'

Konfigurieren Sie die Einstellungen für Phase 2, und klicken Sie auf Speichern.

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains a navigation menu with categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. Under Protocols, EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, and RADIUS are listed. Under IPsec, Legacy IPsec (ESR) and Native IPsec are shown. The main content area is titled 'Phase Two Settings' and contains the following configuration options:

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

At the bottom right, there are 'Cancel' and 'Save' buttons. The 'Save' button is highlighted with a red box.

## Überprüfung

Um sicherzustellen, dass RADIUS über IPsec-Tunnel arbeitet, verwenden Sie den Befehl test aaa, oder führen Sie eine tatsächliche MAB- oder 802.1X-Authentifizierung durch.

```
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#
```

## Überprüfung auf 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 pcg 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#

## Auf ISE überprüfen

Der Status des Tunnels kann über die GUI überprüft werden.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The 'Settings' tab is active, and the 'Native IPsec Configuration' page is displayed. The page includes a navigation menu on the left and a main content area with a table of IPsec configurations. The table has columns for 'ISE Nodes', 'NAD IP Address', 'Tunnel Status', 'IPsec Interface', 'Authentication Type', and 'IKE Version'. The 'Tunnel Status' column for the 'ise332' entry is highlighted with a red box and shows 'ESTABLISHED' with a green checkmark.

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

Verwenden Sie den Befehl `application configure ise`, um den Status des Tunnels über die CLI zu überprüfen.

```
<#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

## Fehlerbehebung

### Fehlerbehebung unter IOS-XE

Zu aktivierende Debugs

```
<#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#
```

### Vollständiger Satz funktionierender Debugs für 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 PASSE  
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 PASSE  
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 PASSE  
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



```

    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

```

## Fehlerbehebung auf der ISE

### Zu aktivierende Debugs

Es sind keine spezifischen Debugs auf ISE zu aktivieren, um die Debugs auf der Konsole auszugeben, gibt den folgenden Befehl aus:

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

### Vollständiger Satz funktionierender Debugs für 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/H  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> got SPI c17542e9

Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for us:  
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10  
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.48.23.85/32, received: 10  
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting traffic selectors for othe  
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1  
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 1  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD\_SA net-net-7212b70a-1405-429a-  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using AES\_CBC for encryption  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using HMAC\_SHA2\_512\_256 for integrit  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding inbound ESP SA  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xc17542e9, src 10.62.148.79 dst  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI c17542e9 a  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES\_CBC w  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC\_SHA2\_  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 32 packets  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding outbound ESP SA  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xf7a68f69, src 10.48.23.85 dst  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI f7a68f69 a  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES\_CBC w  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC\_SHA2\_  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 0 packets  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.48.23.85/32 === 10.  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting a local address in traffic s  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using host 10.48.23.85  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface name for index 22  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using 10.48.23.1 as nexthop and eth1  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> installing route: 10.62.148.79/32 vi  
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface index for eth1  
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD\_SA net-net-7212b70a-1405-429a-  
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD\_SA net-net-7212b70a-1405-429a-  
Apr 26 00:57:37 09[ENC] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> generating IKE\_AUTH response 1 [ IDr  
Apr 26 00:57:37 09[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500  
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin IKEv2 SA 7212b70a-1405-429a-  
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin of IKE\_SA successfu  
Apr 26 00:57:37 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.