

Configurazione di ISE 3.3 Native IPsec per la comunicazione protetta e AD (IOS-XE)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurare il tunnel IPsec IKEv2 con autenticazione certificato X.509](#)

[Esempio di rete](#)

[Configurazione CLI switch IOS-XE](#)

[Configurazione delle interfacce](#)

[Configura Trustpoint](#)

[Importa certificati](#)

[Configurazione della proposta IKEv2](#)

[Configurare un criterio Crypto IKEv2](#)

[Configurare un profilo Crypto IKEv2](#)

[Configurazione di un ACL per il traffico VPN di interesse](#)

[Configurare un set di trasformazioni](#)

[Configurazione di una mappa crittografica e applicazione a un'interfaccia](#)

[Configurazione finale di IOS-XE](#)

[Configurazione di ISE](#)

[Configurazione dell'indirizzo IP in ISE](#)

[Importa certificato archivio attendibile](#)

[Importa certificato di sistema](#)

[Configura tunnel IPsec](#)

[Configurazione del tunnel IPsec IKEv2 con autenticazione con chiave precondivisa X.509](#)

[Esempio di rete](#)

[Configurazione CLI switch IOS-XE](#)

[Configurazione delle interfacce](#)

[Configurazione della proposta IKEv2](#)

[Configurare un criterio Crypto IKEv2](#)

[Configurare un profilo Crypto IKEv2](#)

[Configurazione di un ACL per il traffico VPN di interesse](#)

[Configurare un set di trasformazioni](#)

[Configurazione di una mappa crittografica e applicazione a un'interfaccia](#)

[Configurazione finale di IOS-XE](#)

[Configurazione di ISE](#)

[Configurazione dell'indirizzo IP in ISE](#)

[Configura tunnel IPsec](#)

[Verifica](#)

[Verifica su IOS-XE](#)

[Verifica all'ISE](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi su IOS-XE](#)

[Debug da abilitare](#)

[Serie completa dei debug operativi su IOS-XE](#)

[Risoluzione dei problemi con ISE](#)

[Debug da abilitare](#)

[Serie completa dei debug operativi su ISE](#)

Introduzione

In questo documento viene descritto come configurare IPsec nativo e risolvere i problemi relativi per proteggere la comunicazione ISE (Cisco Identity Service Engine) 3.3 - NAD (Network Access Device). Il traffico Radius può essere crittografato con il tunnel IPsec IKEv2 (Internet Key Exchange versione 2) da sito a sito (LAN a LAN) tra lo switch e ISE. Questo documento non copre la parte di configurazione RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Configurazione switch Cisco
- Concetti generali relativi a IPsec
- Concetti generali su RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst Switch C9200L con software versione 17.6.5
- Cisco Identity Service Engine versione 3.3
- Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'obiettivo è proteggere i protocolli che usano hash MD5, RADIUS e TACACS non sicuri con IPsec. Pochi fatti da considerare:

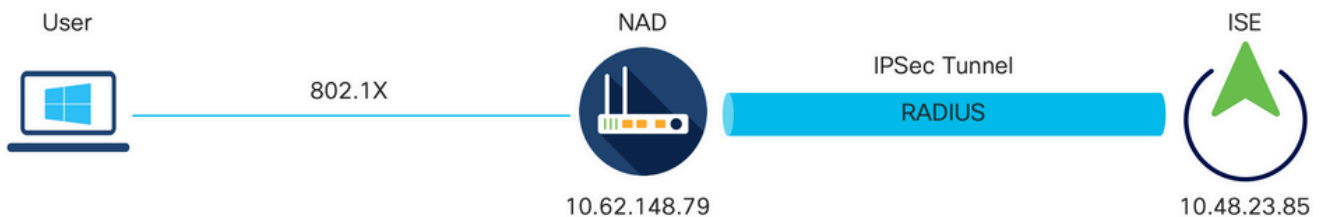
- La soluzione IPsec nativa Cisco ISE è basata su [StrongSwan](#)

- Quando si configura IPsec su un'interfaccia Cisco ISE, viene creato un tunnel IPsec tra Cisco ISE e NAD per proteggere la comunicazione. NAD deve essere configurato separatamente in Impostazioni IPsec native.
- È possibile definire una chiave già condivisa o utilizzare certificati X.509 per l'autenticazione IPsec.
- IPsec può essere abilitato su interfacce Gigabit Ethernet1, tramite interfacce Gigabit Ethernet5.

Il documento è incentrato sull'autenticazione con certificato X.509. La sezione Verifica e risoluzione dei problemi è incentrata solo sull'autenticazione con certificato X.509. Il debug deve essere esattamente lo stesso per l'autenticazione con chiave già condivisa, con una sola differenza negli output. Gli stessi comandi possono essere usati anche per la verifica.

Configurare il tunnel IPsec IKEv2 con autenticazione certificato X.509

Esempio di rete



Esempio di rete

Configurazione CLI switch IOS-XE

Configurazione delle interfacce

Se le interfacce dello switch IOS-XE non sono ancora configurate, è necessario configurare almeno un'interfaccia. Di seguito è riportato un esempio:


```

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
!
  
```

Verificare che esista una connettività al peer remoto da utilizzare per stabilire un tunnel VPN da sito a sito. È possibile usare un comando ping per verificare la connettività di base.

Configura Trustpoint

Per configurare i criteri IKEv2, immettere il comando `crypto pki trustpoint <nome>` in modalità di configurazione globale. Di seguito è riportato un esempio:

 Nota: esistono diversi modi per installare i certificati sul dispositivo IOS-XE. In questo esempio viene utilizzata l'importazione del file pkcs12, che contiene il certificato di identità e la relativa catena


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

Importa certificati

Per importare il certificato di identità IOS-XE e la relativa catena, immettere il comando `crypto pki import <trustpoint> pkcs12 <location> password <password>` in modalità privilegiata. Di seguito è riportato un esempio:

```
KSEC-9248L-1#crypto pki import KrakowCA pkcs12 ftp://eugene:<ftp-password>@10.48.17.90/ISE/KSEC-9248L-1
% Importing pkcs12...Reading file from ftp://eugene@10.48.17.90/ISE/KSEC-9248L-1.pfx!
[OK - 3474/4096 bytes]
```

```
CRYPTO_PKI: Imported PKCS12 file successfully.
KSEC-9248L-1#
```

 Nota: anche se i certificati non rientrano nell'ambito del documento, verificare che il certificato di identità IOS-XE contenga campi SAN popolati con il relativo FQDN/indirizzo IP. ISE richiede un certificato peer per avere un campo SAN.

Per verificare che i certificati siano installati correttamente:

```
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#

Configurazione della proposta IKEv2

Per configurare i criteri IKEv2, immettere il comando `crypto ikev2 draft <name>` in modalità di configurazione globale. Di seguito è riportato un esempio:

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

Configurare un criterio Crypto IKEv2

Per configurare i criteri IKEv2, immettere il comando `crypto ikev2 policy <nome>` in modalità di configurazione globale:

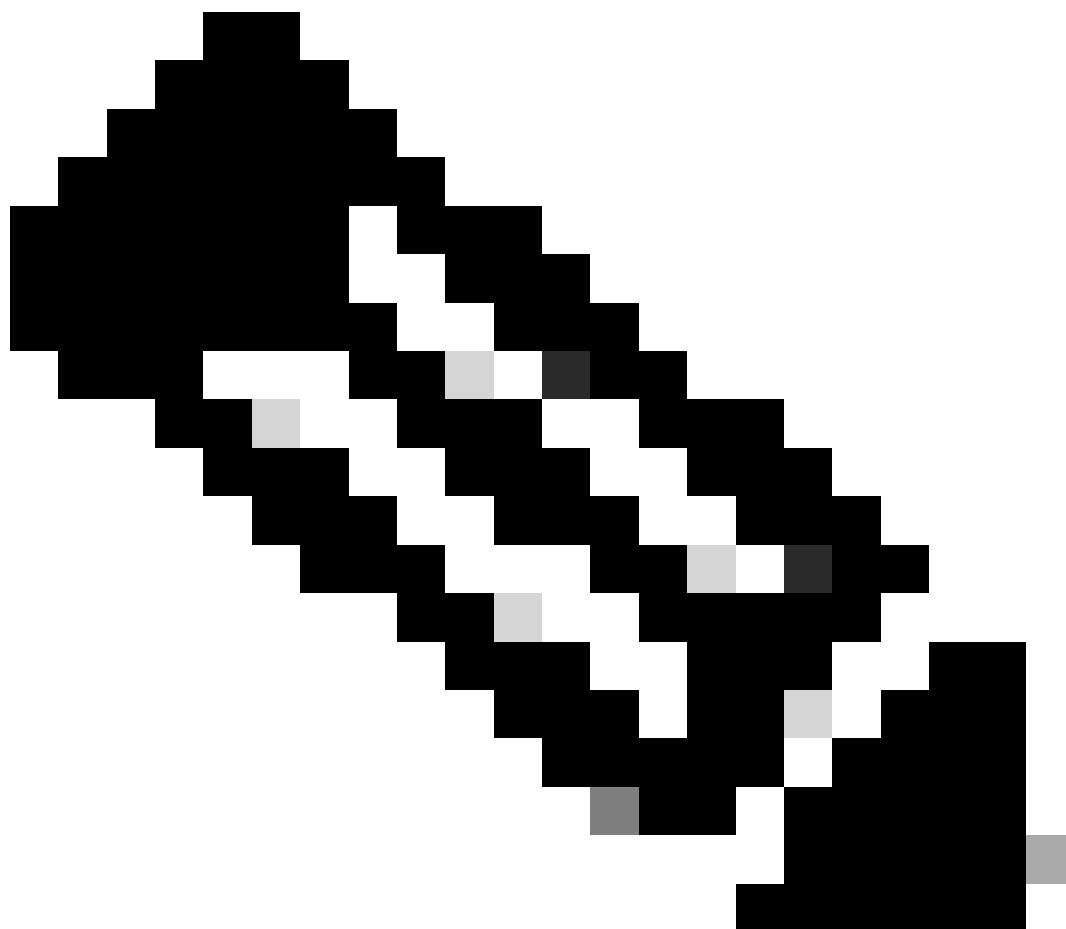
```
crypto ikev2 policy POLICY
  proposal PROPOSAL
```

Configurare un profilo Crypto IKEv2

Per configurare il profilo IKEv2, immettere il comando `crypto ikev2 profile<name>` in modalità di

configurazione globale.

```
crypto ikev2 profile PROFILE
match address local 10.62.148.79
match identity remote fqdn domain example.com
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint KrakowCA
```



Nota: per impostazione predefinita, ISE utilizza il campo CN del proprio certificato di identità come identità IKE nella negoziazione IKEv2. Per questo motivo, nella sezione "match identity remote" del profilo IKEv2, è necessario specificare il tipo di FQDN e il valore corretto di dominio o FQDN di ISE.

Configurazione di un ACL per il traffico VPN di interesse

Utilizzare l'elenco degli accessi esteso o con nome per specificare il traffico che deve essere protetto dalla crittografia. Di seguito è riportato un esempio:

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

 Nota: un ACL per il traffico VPN usa gli indirizzi IP di origine e destinazione dopo NAT.

Configurare un set di trasformazioni

Per definire un set di trasformazioni IPsec (una combinazione accettabile di protocolli e algoritmi di sicurezza), immettere il comando `crypto ipsec transform-set` in modalità di configurazione globale. Di seguito è riportato un esempio:

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

Configurazione di una mappa crittografica e applicazione a un'interfaccia

Per creare o modificare una voce della mappa crittografica e accedere alla modalità di configurazione della mappa crittografica, immettere il comando di configurazione globale `crypto map`. Affinché la voce della mappa crittografica sia completa, è necessario definire almeno alcuni aspetti:

- È necessario definire i peer IPsec a cui è possibile inoltrare il traffico protetto. Si tratta dei peer con cui è possibile stabilire un'associazione di protezione. Per specificare un peer IPsec in una voce della mappa crittografica, immettere il comando `set peer`.
- È necessario definire i set di trasformazioni che possono essere utilizzati con il traffico protetto. Per specificare i set di trasformazioni che possono essere utilizzati con la voce della mappa crittografica, immettere il comando `set transform-set`.
- È necessario definire il traffico da proteggere. Per specificare un elenco degli accessi estesi per una voce della mappa crittografica, immettere il comando `match address`.

Di seguito è riportato un esempio:

```
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
```

Il passaggio finale è l'applicazione a un'interfaccia della mappa crittografica definita in precedenza. Per applicare questa condizione, immettere il comando di configurazione dell'interfaccia crypto map:

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

Configurazione finale di IOS-XE

Di seguito è riportata la configurazione finale della CLI dello switch IOS-XE:

```
aaa new-model
!
aaa group server radius ISE
  server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
  client 10.48.23.85
  server-key cisco
!
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
!
```

Configurazione di ISE

Configurazione dell'indirizzo IP in ISE

L'indirizzo deve essere configurato sull'interfaccia GE1-GE5 dalla CLI. GE0 non è supportato.

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


 Nota: l'applicazione viene riavviata dopo che l'indirizzo IP è stato configurato sull'interfaccia:
% La modifica dell'indirizzo IP potrebbe causare il riavvio dei servizi ISE
Continuare con la modifica dell'indirizzo IP? Y/N [N]: Y

Importa certificato archivio attendibile

Questo passaggio è necessario per assicurarsi che ISE consideri attendibile il certificato del peer presentato nel momento in cui viene stabilito il tunnel. Selezionare Amministrazione > Sistema > Certificati > Certificati attendibili. Fare clic su Import (Importa). Fare clic su Browse (Sfoggia) e selezionare il certificato CA che ha firmato il certificato di identità ISE/IOS-XE. Assicurarsi che la casella di controllo Trust for authentication within ISE sia selezionata. Fare clic su Invia.

Importa certificato di sistema

Passare a Amministrazione > Sistema > Certificati > Certificati di sistema. Selezionare Nodo, File certificato e Importazione file chiave privata. Selezionare la casella di controllo IPsec. Fare clic su Invia.

 Nota: i certificati vengono installati su StrongSwan SOLO dopo aver salvato il dispositivo di accesso alla rete in Impostazioni IPsec native.

Configura tunnel IPsec

Selezionare Amministrazione > Sistema > Impostazioni > Protocolli > IPsec > IPsec nativo. Fare clic su Add. Selezionare Nodo, che termina il tunnel IPsec, configura e indirizzo IP con maschera, gateway predefinito e interfaccia IPsec. Selezionare Authentication Setting (Impostazione

autenticazione) come X.509 Certificate (Certificato X.509 certificato) e Choose Certificate System Certificate Installed (Scegli certificato di sistema certificato installato).

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings
Posture
Profiling
Protocols
EAP-FAST
EAP-TLS
PEAP
EAP-TTLS
RADIUS
IPSec
Legacy IPSec (ESR)
Native IPSec

Native IPSec Configuration > New

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

Node Specific Settings

Select Node
ise332

NAD IP Address with Mask
10.62.147.79/32

Default Gateway (optional)
10.48.23.1

IPSec Interface
Gigabit Ethernet 1

Authentication Settings

Pre-shared Key

X.509 Certificate IPSEC-2

Il gateway predefinito è una configurazione facoltativa. In effetti, sono disponibili due opzioni: è possibile configurare un gateway predefinito nell'interfaccia utente IPsec nativa, che installa una route nel sistema operativo sottostante. Questa route non è esposta in show running-config:

```
ise332/admin#show running-config | include route  
ise332/admin#
```

<#root>

```
ise332/admin#show ip route
```

```
Destination Gateway Iface
```

```
-----  
10.48.23.0/24 0.0.0.0 eth1  
default 10.48.60.1 eth0  
10.48.60.0/24 0.0.0.0 eth0  
  
10.62.148.79 10.48.23.1 eth1
```

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

In alternativa, è possibile lasciare vuoto il gateway predefinito e configurare il percorso manualmente su ISE, in modo da ottenere lo stesso effetto:

```
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#
```

Configurare le impostazioni generali per il tunnel IPsec. Configurare le impostazioni della fase uno. Le impostazioni generali, le impostazioni della fase uno e le impostazioni della fase due devono corrispondere alle impostazioni configurate sull'altro lato del tunnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The main navigation bar includes 'Administration / System' and various tabs like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', and 'Backup & Restore'. The left sidebar shows a navigation menu with 'IPSec' expanded to 'Native IPsec'. The main content area is titled 'General Settings' and contains several configuration fields, each with a red box around it and a help icon (i):

- 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

Configurare Impostazioni fase due e fare clic su Salva.

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

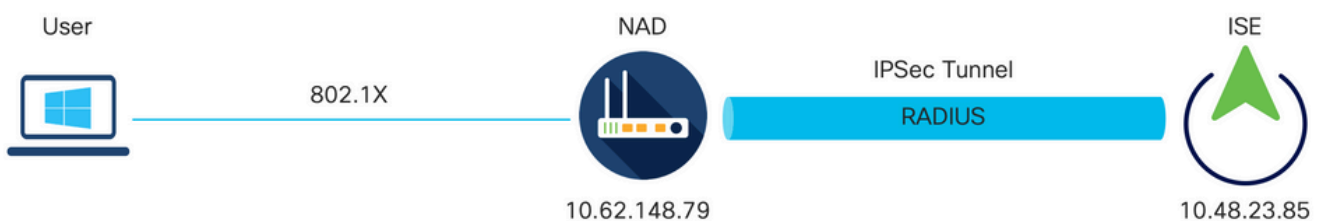
Phase Two Settings
Configure Native IPSec SA Configuration security settings to protect IP traffic between two endpoints.

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

Cancel Save

Configurazione del tunnel IPsec IKEv2 con autenticazione con chiave precondivisa X.509

Esempio di rete



Esempio di rete

Configurazione CLI switch IOS-XE

Configurazione delle interfacce

Se le interfacce dello switch IOS-XE non sono ancora configurate, è necessario configurare almeno un'interfaccia. Di seguito è riportato un esempio:

```
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
!
```

Verificare che esista una connettività al peer remoto da utilizzare per stabilire un tunnel VPN da sito a sito. È possibile usare un comando ping per verificare la connettività di base.

Configurazione della proposta IKEv2

Per configurare i criteri IKEv2, immettere il comando `crypto ikev2 draft <name>` in modalità di configurazione globale. Di seguito è riportato un esempio:

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

Configurare un criterio Crypto IKEv2

Per configurare i criteri IKEv2, immettere il comando `crypto ikev2 policy <nome>` in modalità di configurazione globale:

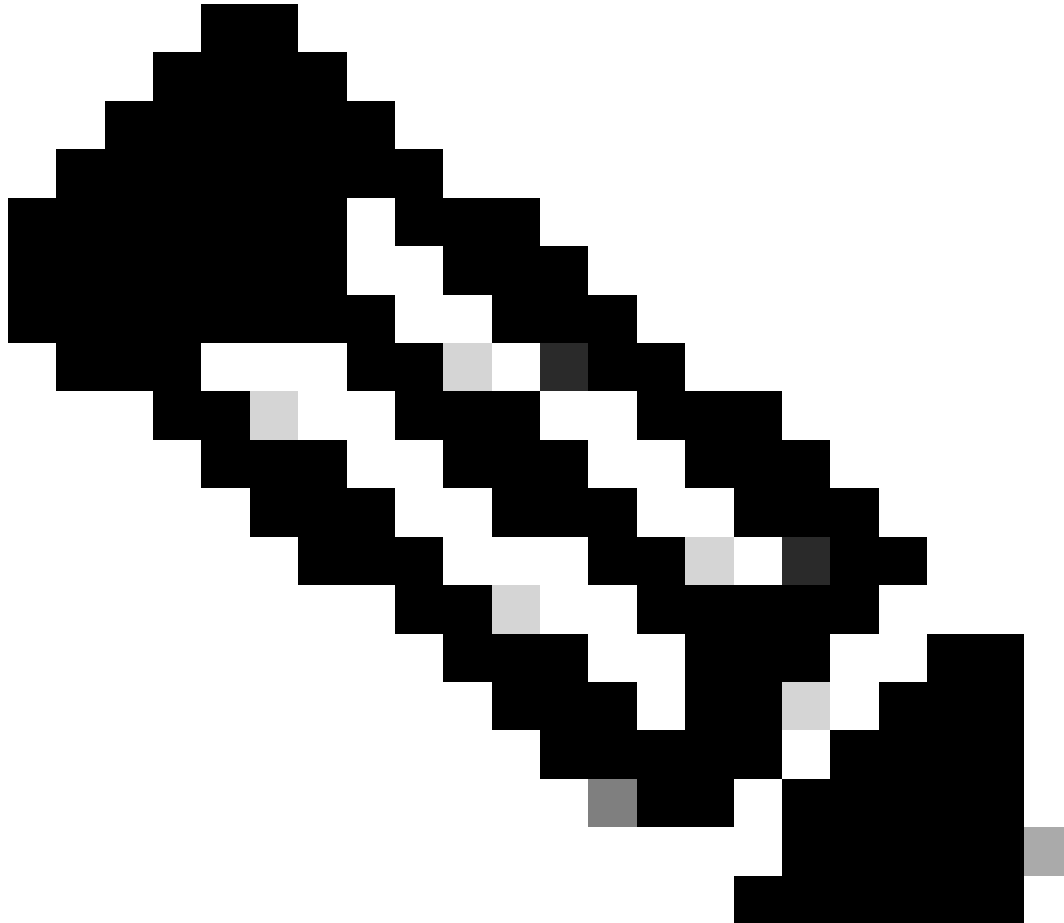
```
crypto ikev2 policy POLICY
 proposal PROPOSAL
```

Configurare un profilo Crypto IKEv2

Per configurare il profilo IKEv2, immettere il comando `crypto ikev2 profile<name>` in modalità di configurazione globale.

```
crypto ikev2 profile PROFILE
```

```
match address local 10.62.148.79
match identity remote address 10.48.23.85 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
```



Nota: per impostazione predefinita, ISE utilizza il campo CN del proprio certificato di identità come identità IKE nella negoziazione IKEv2. Per questo motivo, nella sezione "match identity remote" del profilo IKEv2, è necessario specificare il tipo di FQDN e il valore corretto di dominio o FQDN di ISE.

Configurazione di un ACL per il traffico VPN di interesse

Utilizzare l'elenco degli accessi esteso o con nome per specificare il traffico che deve essere protetto dalla crittografia. Di seguito è riportato un esempio:

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

 Nota: un ACL per il traffico VPN usa gli indirizzi IP di origine e destinazione dopo NAT.

Configurare un set di trasformazioni

Per definire un set di trasformazioni IPsec (una combinazione accettabile di protocolli e algoritmi di sicurezza), immettere il comando `crypto ipsec transform-set` in modalità di configurazione globale. Di seguito è riportato un esempio:

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

Configurazione di una mappa crittografica e applicazione a un'interfaccia

Per creare o modificare una voce della mappa crittografica e accedere alla modalità di configurazione della mappa crittografica, immettere il comando di configurazione globale `crypto map`. Affinché la voce della mappa crittografica sia completa, è necessario definire almeno alcuni aspetti:

- È necessario definire i peer IPsec a cui è possibile inoltrare il traffico protetto. Si tratta dei peer con cui è possibile stabilire un'associazione di protezione. Per specificare un peer IPsec in una voce della mappa crittografica, immettere il comando `set peer`.
- È necessario definire i set di trasformazioni che possono essere utilizzati con il traffico protetto. Per specificare i set di trasformazioni che possono essere utilizzati con la voce della mappa crittografica, immettere il comando `set transform-set`.
- È necessario definire il traffico da proteggere. Per specificare un elenco degli accessi estesi per una voce della mappa crittografica, immettere il comando `match address`.

Di seguito è riportato un esempio:

```
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
```

Il passaggio finale è l'applicazione a un'interfaccia della mappa crittografica definita in precedenza. Per applicare questa condizione, immettere il comando di configurazione dell'interfaccia `crypto map`:


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

Configurazione finale di IOS-XE

Di seguito è riportata la configurazione finale della CLI dello switch IOS-XE:

```
aaa new-model
!
aaa group server radius ISE
  server name ISE33-2
!
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting network default start-stop group ISE
!
aaa server radius dynamic-author
  client 10.48.23.85
  server-key cisco
!
dot1x system-auth-control
!
crypto ikev2 proposal PROPOSAL
  encryption aes-cbc-256
  integrity sha512
  group 16
!
crypto ikev2 policy POLICY
  proposal PROPOSAL
!
crypto ikev2 profile PROFILE
  match address local 10.62.148.79
  match identity remote address 10.48.23.85 255.255.255.255
  authentication remote pre-share key cisco123
  authentication local pre-share key cisco123
!
crypto ipsec transform-set SET esp-aes 256 esp-sha512-hmac
  mode tunnel
!
crypto map MAP-IKEV2 10 ipsec-isakmp
  set peer 10.48.23.85
  set transform-set SET
  set pfs group16
  set ikev2-profile PROFILE
  match address 100
!
interface GigabitEthernet1/0/23
  switchport trunk allowed vlan 1,480
  switchport mode trunk
!
interface Vlan480
  ip address 10.62.148.79 255.255.255.128
  crypto map MAP-IKEV2
!
```


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

Configurazione di ISE

Configurazione dell'indirizzo IP in ISE

L'indirizzo deve essere configurato sull'interfaccia GE1-GE5 dalla CLI. GE0 non è supportato.

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

 Nota: l'applicazione viene riavviata dopo che l'indirizzo IP è stato configurato sull'interfaccia:
% La modifica dell'indirizzo IP potrebbe causare il riavvio dei servizi ISE
Continuare con la modifica dell'indirizzo IP? Y/N [N]: Y

Configura tunnel IPsec

Selezionare Amministrazione > Sistema > Impostazioni > Protocolli > IPsec > IPsec nativo. Fare clic su Add. Selezionare Nodo, che termina il tunnel IPsec, configura e indirizzo IP con maschera, gateway predefinito e interfaccia IPsec. Selezionare Authentication Setting (Impostazione autenticazione) come X.509 Certificate (Certificato X.509 certificato) e Choose Certificate System Certificate Installed (Scegli certificato di sistema certificato installato).

Il gateway predefinito è una configurazione facoltativa. In effetti, sono disponibili due opzioni: è possibile configurare un gateway predefinito nell'interfaccia utente IPsec nativa, che installa una route nel sistema operativo sottostante. Questa route non è esposta in show running-config:

```
ise332/admin#show running-config | include route
ise332/admin#
```

```
<#root>
```

```
ise332/admin#show ip route
```

```
Destination Gateway Iface
```

```
-----
```

```
10.48.23.0/24 0.0.0.0 eth1
```

```
default 10.48.60.1 eth0
```

```
10.48.60.0/24 0.0.0.0 eth0
```

```
10.62.148.79 10.48.23.1 eth1
```

```
169.254.2.0/24 0.0.0.0 cni-podman1
```

```
169.254.4.0/24 0.0.0.0 cni-podman2
```

```
ise332/admin#
```

In alternativa, è possibile lasciare vuoto il gateway predefinito e configurare il percorso

manualmente su ISE, in modo da ottenere lo stesso effetto:

```
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#
```

Configurare le impostazioni generali per il tunnel IPsec. Configurare le impostazioni della fase uno. Le impostazioni generali, le impostazioni della fase uno e le impostazioni della fase due devono corrispondere alle impostazioni configurate sull'altro lato del tunnel IPsec.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine" on the left, and "Administration / System" on the right. Below the navigation bar, there are several tabs: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, and Backup & Restore. The main content area is divided into a left sidebar and a right main panel. The sidebar contains a list of settings categories: 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 (Legacy IPsec (ESR), Native IPsec), and Endpoint Scripts. The main panel is titled "General Settings" and contains several configuration fields, each with a red box around it and a help icon (i):

- 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

Configurare Impostazioni fase due e fare clic su Salva.

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

Verifica

Per verificare che RADIUS funzioni sul tunnel IPsec, usare il comando test aaa o eseguire l'autenticazione MAB o 802.1X

```
KSEC-9248L-1#test aaa group ISE alice Krakow123 new-code
User successfully authenticated
```

USER ATTRIBUTES

```
username 0 "alice"
vn 0 "vn1"
security-group-tag 0 "000f-00"
KSEC-9248L-1#
```

Verifica su 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#

Verifica all'ISE

È possibile verificare lo stato del tunnel dalla GUI

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

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

Usare il comando application configure ise per verificare lo stato del tunnel dalla CLI

<#root>

ise332/admin#application configure ise

Selection configuration option

- [1]Reset M&T Session Database
- [2]Rebuild M&T Unusable Indexes
- [3]Purge M&T Operational Data
- [4]Reset M&T Database
- [5]Refresh Database Statistics
- [6]Display Profiler Statistics
- [7]Export Internal CA Store
- [8]Import Internal CA Store
- [9]Create Missing Config Indexes
- [10]Create Missing M&T Indexes
- [12]Generate Daily KPM Stats
- [13]Generate KPM Stats for last 8 Weeks
- [14]Enable/Disable Counter Attribute Collection
- [15]View Admin Users
- [16]Get all Endpoints
- [19]Establish Trust with controller
- [20]Reset Context Visibility
- [21]Synchronize Context Visibility With Database
- [22]Generate Heap Dump
- [23]Generate Thread Dump
- [24]Force Backup Cancellation
- [25]CleanUp ESR 5921 IOS Crash Info Files
- [26]Recreate undotablespace
- [27]Reset Upgrade Tables
- [28]Recreate Temp tablespace
- [29]Clear Sysaux tablespace
- [30]Fetch SGA/PGA Memory usage
- [31]Generate Self-Signed Admin Certificate
- [32]View Certificates in NSSDB or CA_NSSDB
- [33]Recreate REPLUGINS tablespace
- [34]View Native IPsec status
- [0]Exit

34

7212b70a-1405-429a-94b8-71a5d4beb1e5: #114,

ESTABLISHED

, IKEv2, 0ca3c29e36290185_i 08c7fb6db177da84_r*

local 'CN=ise332.example.com' @ 10.48.23.85[500]

remote '10.62.148.79' @ 10.62.148.79[500]

AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096

established 984s ago, rekeying in 10283s, reauth in 78609s

net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5: #58, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-256/HMAC_S

installed 984s ago, rekeying in 12296s, expires in 14856s

in c17542e9, 100 bytes,

1 packets

, 983s ago

out f7a68f69, 100 bytes,

1 packets

, 983s ago


```
local 10.48.23.85/32
remote 10.62.148.79/32
```

Risoluzione dei problemi

Risoluzione dei problemi su IOS-XE

Debug da abilitare

```
<#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#
```

Serie completa dei debug operativi su IOS-XE

```
Apr 25 18:57:36.572: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 10.62.148.79:500, remote= 10.48.23.85:500,
local_proxy= 10.62.148.79/255.255.255.255/256/0,
remote_proxy= 10.48.23.85/255.255.255.255/256/0,
protocol= ESP, transform= esp-aes 256 esp-sha512-hmac (Tunnel), esn= FALSE,
lifedur= 86400s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Searching Policy with fvrf 0, local address 10.62.148.79
Apr 25 18:57:36.573: IKEv2:(SESSION ID = 0,SA ID = 0):Found Policy 'POLICY'
Apr 25 18:57:36.573: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Start PKI Session
Apr 25 18:57:36.574: IKEv2:(SA ID = 1):[PKI -> IKEv2] Starting of PKI Session PASSED
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public key,
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Compu
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH key
```

Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKEv2 initiator - no config data to send in IKE_SA_INIT message
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_SA_INIT message
Apr 25 18:57:36.574: IKEv2:(SESSION ID = 5,SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial negotiation)
Num. transforms: 4
AES-CBC SHA512 SHA512 DH_GROUP_4096_MODP/Group 16

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)

Apr 25 18:57:36.575: IKEv2:(SESSION ID = 5,SA ID = 1):Insert SA

Apr 25 18:57:36.640: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(Unknown -)

Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Verify SA init message
Apr 25 18:57:36.641: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_SA_INIT message
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificate
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.641: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the trustpoint KrakowCA
Apr 25 18:57:36.643: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the trustpoint PASSED
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):Checking NAT discovery
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):NAT not found
Apr 25 18:57:36.643: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret key,
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computed
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Request queued for computation of DH secret
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKD
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculated
Apr 25 18:57:36.874: IKEv2:(SESSION ID = 5,SA ID = 1):Completed SA init exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Generate my authentication data
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication data generated
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Get my authentication method
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):My authentication method is 'RSA'
Apr 25 18:57:36.876: IKEv2:(SESSION ID = 5,SA ID = 1):Sign authentication data
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting private key
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of private key PASSED
Apr 25 18:57:36.877: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Sign authentication data
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Signing of authentication data PASSED
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Authentication material has been successfully signed
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Generating IKE_AUTH message
Apr 25 18:57:36.945: IKEv2:(SESSION ID = 5,SA ID = 1):Constructing IDi payload: '10.62.148.79' of type ID_IPV4_ADDR
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured trustpoint(s)
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'KrakowCA'
Apr 25 18:57:36.945: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Get Public Key Hashes of trustpoints
Apr 25 18:57:36.946: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of Public Key Hashes of trustpoints PASSED
Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotiation)
Num. transforms: 3
AES-CBC SHA512 Don't use ESN

Apr 25 18:57:36.946: IKEv2:(SESSION ID = 5,SA ID = 1):Building packet for encryption.
Payload contents:
VID IDi CERT CERTREQ AUTH SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO)

Apr 25 18:57:36.947: IKEv2:(SESSION ID = 5,SA ID = 1):Sending Packet [To 10.48.23.85:500/From 10.62.148.79:500]

Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Apr 25 18:57:37.027: IKEv2:(SESSION ID = 5,SA ID = 1):Received Packet [From 10.48.23.85:500/To 10.62.148.79:500]
Initiator SPI : OCA3C29E36290185 - Responder SPI : 08C7FB6DB177DA84 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
IDr CERT AUTH SA TSi TSr

Apr 25 18:57:37.029: IKEv2:(SESSION ID = 5,SA ID = 1):Process auth response notify
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching policy based on peer's identity 'cn=ise332.example.com'
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Searching Policy with fvrf 0, local address 10.62.148.79
Apr 25 18:57:37.031: IKEv2:(SESSION ID = 5,SA ID = 1):Found Policy 'POLICY'
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's policy
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's policy verified
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Get peer's authentication method
Apr 25 18:57:37.032: IKEv2:(SESSION ID = 5,SA ID = 1):Peer's authentication method is 'RSA'
Apr 25 18:57:37.033: IKEv2:Validation list created with 1 trustpoints
Apr 25 18:57:37.033: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating certificate chain
Apr 25 18:57:37.043: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain PASSED
Apr 25 18:57:37.043: IKEv2:(SESSION ID = 5,SA ID = 1):Save pubkey
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):Verify peer's authentication data
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Apr 25 18:57:37.045: IKEv2:(SESSION ID = 5,SA ID = 1):[Crypto Engine -> IKEv2] IKEv2 authentication data
Apr 25 18:57:37.045: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Verify signed authentication data
Apr 25 18:57:37.047: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of signed authentication data
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Check for EAP exchange
Apr 25 18:57:37.048: IKEv2:(SESSION ID = 5,SA ID = 1):Processing IKE_AUTH message
Apr 25 18:57:37.050: IKEv2:(SESSION ID = 5,SA ID = 1):IPSec policy validate request sent for profile 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...

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= 1000000000
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

```

Risoluzione dei problemi con ISE

Debug da abilitare

Non ci sono debug specifici da abilitare su ISE, per stampare i debug sulla console, usare il comando:

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

Serie completa dei debug operativi su ISE

```

Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 13[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 0000000000000000_r
Apr 26 00:57:36 13[MGR] created IKE_SA (unnamed)[114]
Apr 26 00:57:36 13[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (774 bytes)
Apr 26 00:57:36 13[ENC] <114> parsed IKE_SA_INIT request 0 [ SA KE No V V V N(NATD_S_IP) N(NATD_D_IP)
Apr 26 00:57:36 13[CFG] <114> looking for an IKEv2 config for 10.48.23.85...10.62.148.79
Apr 26 00:57:36 13[CFG] <114> candidate: 10.48.23.85...10.62.148.79, prio 3100
Apr 26 00:57:36 13[CFG] <114> found matching ike config: 10.48.23.85...10.62.148.79 with prio 3100
Apr 26 00:57:36 13[IKE] <114> local endpoint changed from 0.0.0.0[500] to 10.48.23.85[500]
Apr 26 00:57:36 13[IKE] <114> remote endpoint changed from 0.0.0.0 to 10.62.148.79[500]
Apr 26 00:57:36 13[IKE] <114> received Cisco Delete Reason vendor ID

```

Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:2d:30:32
Apr 26 00:57:36 13[ENC] <114> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:43:2d:52:
Apr 26 00:57:36 13[IKE] <114> received Cisco FlexVPN Supported vendor ID
Apr 26 00:57:36 13[IKE] <114> 10.62.148.79 is initiating an IKE_SA
Apr 26 00:57:36 13[IKE] <114> IKE_SA (unnamed)[114] state change: CREATED => CONNECTING
Apr 26 00:57:36 13[CFG] <114> selecting proposal:
Apr 26 00:57:36 13[CFG] <114> proposal matches
Apr 26 00:57:36 13[CFG] <114> received proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MO
Apr 26 00:57:36 13[CFG] <114> configured proposals: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512
Apr 26 00:57:36 13[CFG] <114> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MO
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=KrakowCA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "DC=com, DC=example, CN=LAB CA"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Endpoint Sub CA - ise33
Apr 26 00:57:36 13[IKE] <114> sending cert request for "CN=Certificate Services Node CA - ise332"
Apr 26 00:57:36 13[IKE] <114> sending cert request for "O=Cisco, CN=Cisco Manufacturing CA SHA2"
Apr 26 00:57:36 13[ENC] <114> generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) CE
Apr 26 00:57:36 13[NET] <114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500] (809 bytes)
Apr 26 00:57:36 13[MGR] <114> checkin IKEv2 SA (unnamed)[114] with SPIs 0ca3c29e36290185_i 08c7fb6db177
Apr 26 00:57:36 13[MGR] <114> checkin of IKE_SA successful
Apr 26 00:57:36 04[NET] sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
Apr 26 00:57:36 03[NET] received packet: from 10.62.148.79[500] to 10.48.23.85[500]
Apr 26 00:57:36 03[NET] waiting for data on sockets
Apr 26 00:57:36 09[MGR] checkout IKEv2 SA by message with SPIs 0ca3c29e36290185_i 08c7fb6db177da84_r
Apr 26 00:57:36 09[MGR] IKE_SA (unnamed)[114] successfully checked out
Apr 26 00:57:36 09[NET] <114> received packet: from 10.62.148.79[500] to 10.48.23.85[500] (1488 bytes)
Apr 26 00:57:37 09[ENC] <114> parsed IKE_AUTH request 1 [V IDi CERT CERTREQ AUTH SA TSi TSr N(INIT_CON
Apr 26 00:57:37 09[IKE] <114> received cert request for "CN=KrakowCA"
Apr 26 00:57:37 09[IKE] <114> received end entity cert "CN=KSEC-9248L-1.example.com"
Apr 26 00:57:37 09[CFG] <114> looking for peer configs matching 10.48.23.85[%any]...10.62.148.79[10.62.
Apr 26 00:57:37 09[CFG] <114> candidate "7212b70a-1405-429a-94b8-71a5d4beb1e5", match: 1/1/3100 (me/oth
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected peer config '7212b70a-1405-
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using certificate "CN=KSEC-9248L-1.e
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KSEC-9248L-1.example
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using trusted ca certificate "CN=Kra
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate "CN=KrakowCA" key: 2048
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> reached self-signed root ca with a p
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checking certificate status of "CN=K
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> ocsf check skipped, no ocsf found
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> certificate status is not available
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of '10.62.148.79' wit
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received ESP_TFC_PADDING_NOT_SUPPORT
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> authentication of 'CN=ise332.example
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending end entity cert "CN=ise332.e
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> IKE_SA 7212b70a-1405-429a-94b8-71a5d
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling rekeying in 11267s
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> scheduling reauthentication in 79593
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> maximum IKE_SA lifetime 19807s
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> looking for a child config for 10.48
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for us:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.48.23.85/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposing traffic selectors for othe
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> 10.62.148.79/32
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> candidate "net-net-7212b70a-1405-429
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> found matching child config "net-net
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selecting proposal:
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> proposal matches
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> received proposals: ESP:AES_CBC_256/
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> configured proposals: ESP:AES_CBC_25
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> selected proposal: ESP:AES_CBC_256/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 other
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 10
Apr 26 00:57:37 09[CFG] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> config: 10.62.148.79/32, received: 10
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using AES_CBC for encryption
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using HMAC_SHA2_512_256 for integrity
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding inbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xc17542e9, src 10.62.148.79 dst 10.48.23.85
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI c17542e9 and SPI f7a68f69
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC with integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 32 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding outbound ESP SA
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> SPI 0xf7a68f69, src 10.48.23.85 dst 10.62.148.79
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding SAD entry with SPI f7a68f69 and SPI c17542e9
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using encryption algorithm AES_CBC with integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using integrity algorithm HMAC_SHA2_512_256
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using replay window of 0 packets
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> HW offload: no
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10.62.148.79/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.62.148.79/32 === 10.62.148.79/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> adding policy 10.48.23.85/32 === 10.48.23.85/32
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting a local address in traffic selector
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using host 10.48.23.85
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface name for index 22
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> using 10.48.23.1 as nexthop and eth1 as interface
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> installing route: 10.62.148.79/32 via 10.48.23.1
Apr 26 00:57:37 09[KNL] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> getting iface index for eth1
Apr 26 00:57:37 09[IKE] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[CHD] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> CHILD_SA net-net-7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[ENC] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> generating IKE_AUTH response 1 [IDr=0, SA=7212b70a-1405-429a-94b8-71a5d4beb1e5, SPI=0xc17542e9, src=10.48.23.85, dst=10.62.148.79]
Apr 26 00:57:37 09[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500]
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin IKEv2 SA 7212b70a-1405-429a-94b8-71a5d4beb1e5
Apr 26 00:57:37 09[MGR] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> checkin of IKE_SA successful
Apr 26 00:57:37 04[NET] <7212b70a-1405-429a-94b8-71a5d4beb1e5|114> sending packet: from 10.48.23.85[500] to 10.62.148.79[500]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).