# 配置ISE 2.2 IPSEC以保護NAD(IOS)通訊

## 目錄

## 簡介

本檔案介紹如何設定TACACS IPSEC並疑難排解，以確保思科身分識別服務引擎(ISE)2.2 — 網路存取裝置(NAD)通訊的安全。TACACS流量可以使用路由器和ISE之間的站點到站點（LAN到LAN）IPSec網際網路金鑰交換版本2(IKEv2)隧道進行加密。本文檔不涉及TACACS配置部分。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ISE
- 思科路由器
- 一般IPSec概念
- 一般TACACS概念

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本15.4(3)S2的Cisco ISR4451-X路由器
- 思科身分識別服務引擎版本2.2
- Windows 7 Service Pack 1

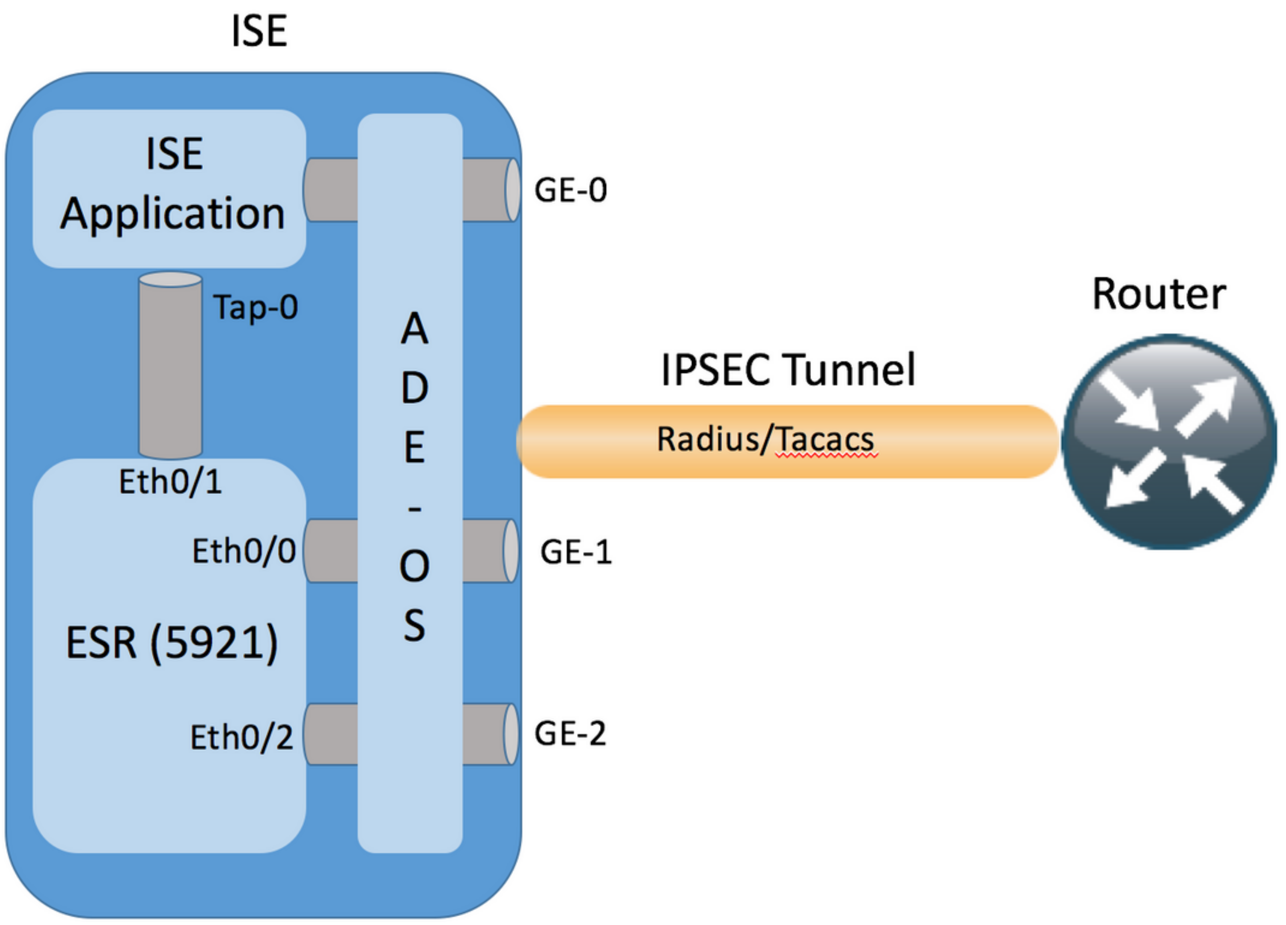
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

目標是保護使用不安全的MD5雜湊、Radius和具有IPSec的TACACS的協定。需要考慮的事實很少：

- 思科ISE在隧道和傳輸模式下支援IPSec。
- 當您在Cisco ISE介面上啟用IPSec時，會在Cisco ISE和NAD之間建立IPSec隧道以保護通訊。
- 您可以定義預共用金鑰或使用X.509證書進行IPSec身份驗證。
- 可以在Eth1到Eth5介面上啟用IPSec。每個PSN只能在一個思科ISE介面上配置IPSec。

### ISE IPSec架構



GE-1 ISE介面收到加密資料包後，嵌入式服務路由器(ESR)會攔截其Eth0/0介面。

```
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.17.87 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
```

ESR會解密它們，並根據預配置的NAT規則執行地址轉換。傳出（傳向NAD）RADIUS/TACACS資料包被轉換為Ethernet0/0介面地址，然後進行加密。

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

目的地為RADIUS/TACACS埠上Eth0/0介面的資料包應該通過Eth0/1介面轉發到10.1.1.2 ip address（ISE的內部地址）。Eth0/1的ESR配置

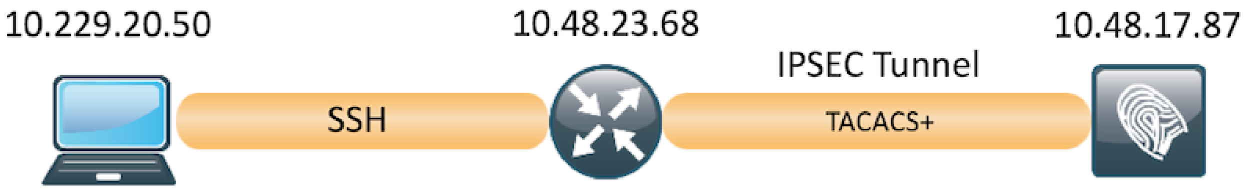
```
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
```

內部Tap-0介面的ISE配置：

```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)
       RX packets 81462  bytes 8927953 (8.5 MiB)
       RX errors 0  dropped 68798  overruns 0  frame 0
       TX packets 105  bytes 8405 (8.2 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

## 網路圖表

本檔案中的資訊使用以下網路設定：



# 使用預共用金鑰配置ikev1 ipsec vpn（開箱即用）

本節介紹如何完成IOS CLI和ISE配置。

## IOS路由器CLI配置

### 配置介面

如果尚未配置IOS路由器介面，則至少應配置WAN介面。以下是範例：

```
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
no shutdown
!
```

確儲存在與遠端對等點的連線，該連線應用於建立站點到站點VPN隧道。您可以使用ping驗證基本連線。

### 配置ISAKMP(IKEv1)策略

若要為IKEv1連線配置ISAKMP策略，請在全域性配置模式下輸入**crypto isakmp policy <priority>**命令。下面是一個示例：

```
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
```

> **注意：**可以在參與IPSec的每個對等體上配置多個IKE策略。當IKE協商開始時，它會嘗試查詢在兩個對等體上配置的公共策略，並且從遠端對等體上指定的最高優先順序策略開始。

### 配置加密ISAKMP金鑰

若要設定預先共用的*驗證*金鑰，請在全域組態模式下輸入**crypto isakmp key**指令：

```
crypto isakmp key Krakow123 address 10.48.17.87
```

### 為相關的VPN流量配置ACL

使用擴充或命名存取清單來指定應受加密保護的流量。以下是範例：

```
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
```

> **注意：**用於VPN流量的ACL在NAT之後使用源和目標IP地址。

### 配置轉換集

要定義IPSec轉換集（安全協定和演算法的可接受組合），請在全域性配置模式下輸入**crypto ipsec transform-set**命令。以下是範例：

```
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
 mode transport
```

### 設定密碼編譯對應並將其套用到介面

若要建立或修改加密對映條目並進入加密對映配置模式，請輸入**crypto map** global configuration命令。為了完成加密對映條目，必須至少定義以下幾個方面：

- 必須定義可將受保護流量轉發到的IPsec對等路由器。以下是可以建立SA的對等路由器。要在加密對映條目中指定IPSec對等體，請輸入**set peer**命令。
- 必須定義可接受用於受保護流量的轉換集。若要指定可與加密對映條目一起使用的轉換集，請輸入**set transform-set**命令。
- 必須定義應保護的流量。要為加密對映條目指定擴展訪問清單，請輸入**match address**命令。

以下是範例：

```
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
```

最後一步是將之前定義的加密對映集應用到介面。若要套用此功能，請輸入**crypto map** interface configuration指令：

```
interface GigabitEthernet0/0
crypto map MAP
```

### IOS最終配置

下面是最終的IOS路由器CLI配置：

```
aaa group server tacacs+ ISE_TACACS
 server name ISE22
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp key Krakow123 address 10.48.17.87
!
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
 mode transport
!
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
!
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
 no shutdown
!
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
!
tacacs server ISE22
 address ipv4 10.48.17.87
 key cisco
```

## ISE 組態

### 配置ISE上的IP地址

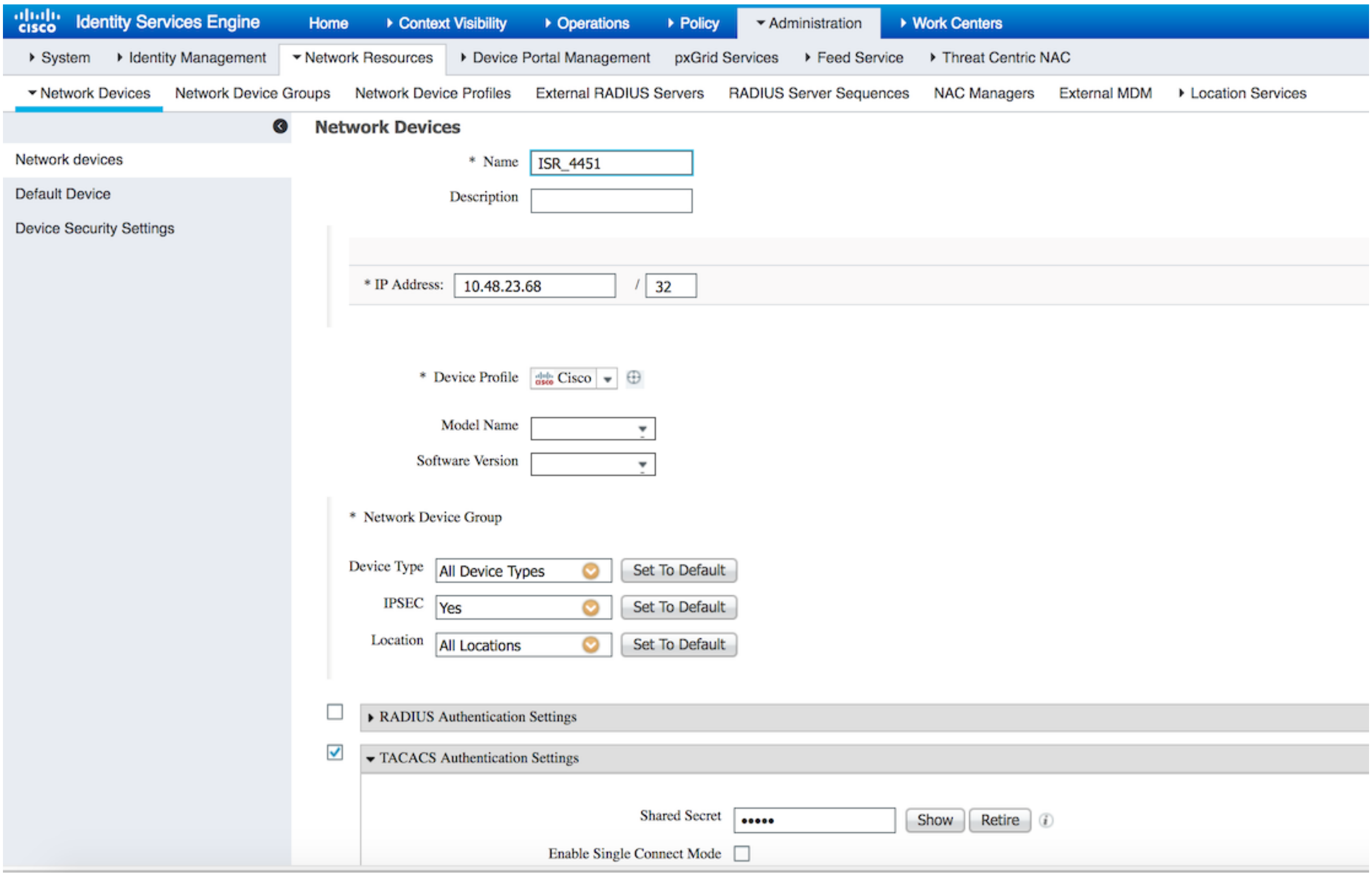
應該從CLI在介面GE1-GE5上配置地址，不支援GE0。

```
interface GigabitEthernet 1
 ip address 10.48.17.87 255.255.255.0
 ipv6 address autoconfig
 ipv6 enable
```

> **附註：**在介面上配置IP地址後，應用程式重新啟動：
> %更改IP地址可能導致ISE服務重新啟動
> 是否繼續更改IP地址？ Y/N [N]:Y

## 向ISE上的IPSec組新增NAD

導覽至**Administration > Network Resources > Network Devices**。按一下「**Add**」。確保配置名稱、IP地址和共用金鑰。要從NAD終止IPSec隧道，請針對IPSEC網路裝置組選擇YES。



Network Devices

* Name: ISR_4451

Description:

* IP Address: 10.48.23.68 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Device Type: All Device Types

IPSEC: Yes

Location: All Locations

□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: •••••

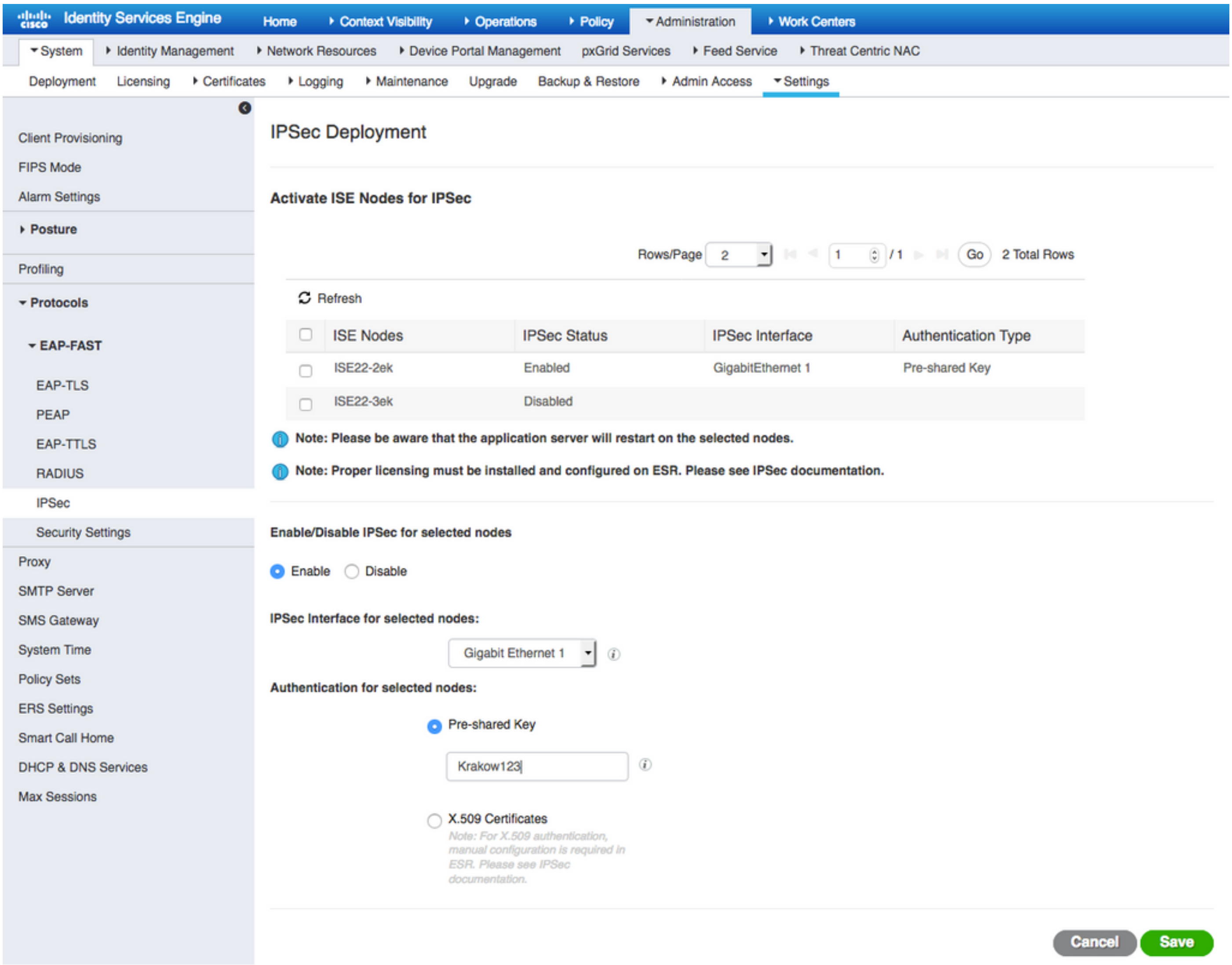
Enable Single Connect Mode □

新增NAD後，應在ISE上建立其他路由，以確保RADIUS流量通過ESR並加密：

```
ip route 10.48.23.68 255.255.255.255 gateway 10.1.1.1
```

## 在ISE上啟用IPSEC

導覽至**Administration > System > Settings**。按一下Radius，然後進一步按一下IPSEC。選擇PSN（單一/多重/全部）選擇啟用選項，選擇介面並選擇身份驗證方法。按一下「**Save**」。此時服務將在所選節點上重新啟動。



IPSec Deployment

Activate ISE Nodes for IPSec

Rows/Page 2 | 1 /1 Go 2 Total Rows

Refresh

| □ | ISE Nodes | IPSec Status | IPSec Interface | Authentication Type |
|---|---|---|---|---|
| □ | ISE22-2ek | Enabled | GigabitEthernet 1 | Pre-shared Key |
| □ | ISE22-3ek | Disabled | | |

Note: Please be aware that the application server will restart on the selected nodes.

Note: Proper licensing must be installed and configured on ESR. Please see IPSec documentation.

Enable/Disable IPSec for selected nodes

● Enable ○ Disable

IPSec Interface for selected nodes:

Gigabit Ethernet 1

Authentication for selected nodes:

● Pre-shared Key

Krakow123

○ X.509 Certificates

Note: For X.509 authentication, manual configuration is required in ESR. Please see IPSec documentation.

請注意，服務重新啟動後，ISE CLI配置顯示配置介面沒有IP地址且處於關閉狀態，預期由ESR（嵌入式服務路由器）控制ISE介面。

```
interface GigabitEthernet 1
 shutdown
 ipv6 address autoconfig
 ipv6 enable
```

服務重新啟動後，ESR功能將啟用。要登入到ESR，請在命令列中鍵入esr:

```
ISE22-1ek/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE
SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, <CTRL-C> to exit

ise-esr5921>en
ise-esr5921#
```

ESR隨附此加密配置，足以使ipsec隧道以預共用金鑰終止：

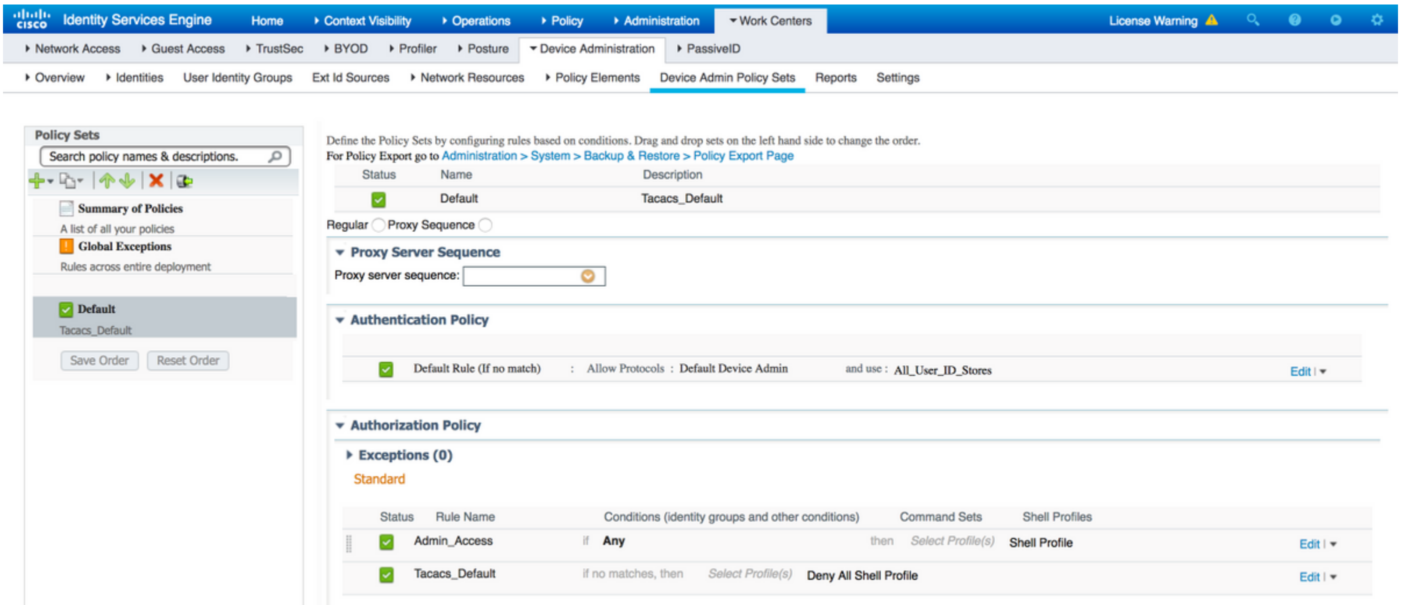
```
crypto keyring MVPN-spokes
```

```
 pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp policy 20
 encr aes
 hash sha256
 authentication pre-share
 group 14
!
crypto isakmp key Krakow123 address 0.0.0.0
!
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
 mode transport
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
```

確保ESR具有傳送加密資料包的路由：

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

### 在ISE上設定Tacacs策略



Summary of Policies

A list of all your policies

Global Exceptions

Rules across entire deployment

☑ Default

Tacacs_Default

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

| Status | Name | Description |
|---|---|---|
| ☑ | Default | Tacacs_Default |

Regular ○ Proxy Sequence ○

Proxy Server Sequence

Proxy server sequence:

Authentication Policy

☑ Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores

Authorization Policy

Exceptions (0)

Standard

| Status | Rule Name | Conditions (identity groups and other conditions) | Command Sets | Shell Profiles |
|---|---|---|---|---|
| ☑ | Admin_Access | if Any | then Select Profile(s) | Shell Profile |
| ☑ | Tacacs_Default | if no matches, then | Select Profile(s) | Deny All Shell Profile |

# 驗證

## IOS路由器

在啟動到路由器的ssh會話之前，沒有活動的VPN連線：

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

由於使用身份驗證源ISE 2.2，因此客戶端連線到路由器。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh alice@10.48.23.68
Password:
ISR4451#
```

一旦通道開啟，IOS會傳送一個TACACS封包，其會觸發VPN作業階段的建立，但路由器上會顯示此輸出。這確認通道的第一階段已啟動：

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.48.17.87     10.48.23.68     QM_IDLE           1962 ACTIVE

IPv6 Crypto ISAKMP SA

ISR4451#
```

階段2已啟動，封包已加密和解密：

```
ISR4451#sh cry ipsec sa

interface: GigabitEthernet0/0/0
   Crypto map tag: MAP, local addr 10.48.23.68

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
  current_peer 10.48.17.87 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
   #pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
   #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.: 10.48.23.68, remote crypto endpt.: 10.48.17.87
    plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
    current outbound spi: 0x64BD51B8(1690128824)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xFAE51DF8(4209319416)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 2681, flow_id: ESG:681, sibling_flags FFFFFFFF80004008, crypto map: MAP
       sa timing: remaining key lifetime (k/sec): (4607998/3127)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x64BD51B8(1690128824)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 2682, flow_id: ESG:682, sibling_flags FFFFFFFF80004008, crypto map: MAP
       sa timing: remaining key lifetime (k/sec): (4607997/3127)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
ISR4451#
```

## ESR

在ESR上可以檢查相同的輸出，第一階段為up:

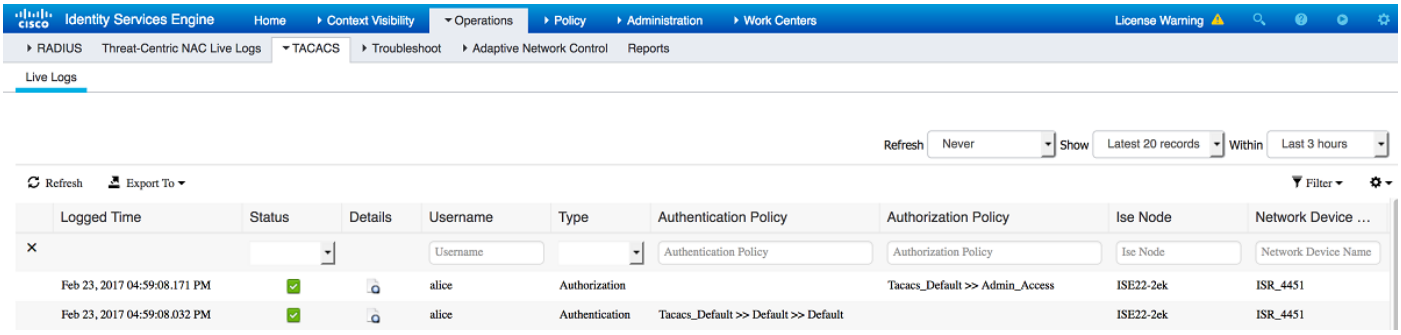
```
ise-esr5921#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.48.17.87     10.48.23.68     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

ise-esr5921#
```

階段2已啟動，資料包已成功加密和解密：

```
ise-esr5921#sh cry ipsec sa

interface: Ethernet0/0
   Crypto map tag: radius, local addr 10.48.17.87

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
  current_peer 10.48.23.68 port 500
    PERMIT, flags={}
   #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
   #pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
   #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.: 10.48.17.87, remote crypto endpt.: 10.48.23.68
    plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xFAE51DF8(4209319416)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x64BD51B8(1690128824)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: radius
       sa timing: remaining key lifetime (k/sec): (4242722/3056)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xFAE51DF8(4209319416)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: radius
       sa timing: remaining key lifetime (k/sec): (4242722/3056)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
ise-esr5921#
```

## ISE

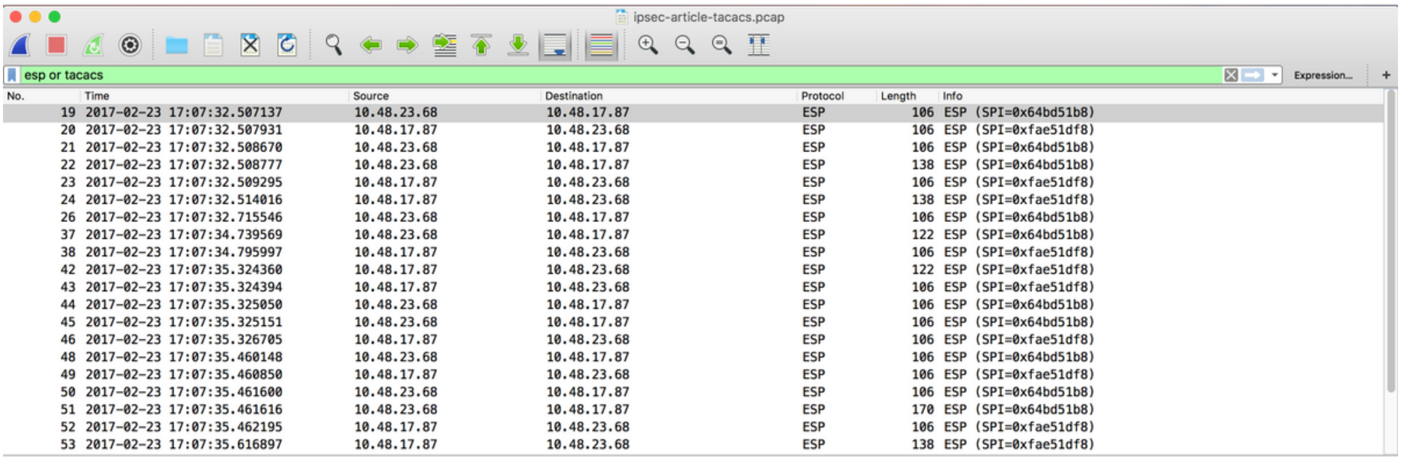
Live Authentication指示常規PAP_ASCII身份驗證：



Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

| Logged Time | Status | Details | Username | Type | Authentication Policy | Authorization Policy | Ise Node | Network Device ... |
|---|---|---|---|---|---|---|---|---|
| Feb 23, 2017 04:59:08.171 PM | ✓ | | alice | Authorization | | Tacacs_Default >> Admin_Access | ISE22-2ek | ISR_4451 |
| Feb 23, 2017 04:59:08.032 PM | ✓ | | alice | Authentication | Tacacs_Default >> Default >> Default | | ISE22-2ek | ISR_4451 |

捕獲在ISE的GE1介面上捕獲並使用ESP或Tacacs過濾，確認明文中沒有Tacacs，並且所有流量都加密：



esp or tacacs

```
No.   Time                        Source          Destination      Protocol  Length  Info
   19 2017-02-23 17:07:32.507137  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   20 2017-02-23 17:07:32.507931  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   21 2017-02-23 17:07:32.508670  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   22 2017-02-23 17:07:32.508777  10.48.23.68     10.48.17.87      ESP          138  ESP (SPI=0x64bd51b8)
   23 2017-02-23 17:07:32.509295  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   24 2017-02-23 17:07:32.514016  10.48.17.87     10.48.23.68      ESP          138  ESP (SPI=0xfae51df8)
   26 2017-02-23 17:07:32.715546  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   37 2017-02-23 17:07:34.739569  10.48.23.68     10.48.17.87      ESP          122  ESP (SPI=0x64bd51b8)
   38 2017-02-23 17:07:34.795997  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   42 2017-02-23 17:07:35.324360  10.48.17.87     10.48.23.68      ESP          122  ESP (SPI=0xfae51df8)
   43 2017-02-23 17:07:35.324394  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   44 2017-02-23 17:07:35.325050  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   45 2017-02-23 17:07:35.325151  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   46 2017-02-23 17:07:35.326705  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   48 2017-02-23 17:07:35.460148  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   49 2017-02-23 17:07:35.460850  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   50 2017-02-23 17:07:35.461600  10.48.23.68     10.48.17.87      ESP          106  ESP (SPI=0x64bd51b8)
   51 2017-02-23 17:07:35.461616  10.48.23.68     10.48.17.87      ESP          170  ESP (SPI=0x64bd51b8)
   52 2017-02-23 17:07:35.462195  10.48.17.87     10.48.23.68      ESP          106  ESP (SPI=0xfae51df8)
   53 2017-02-23 17:07:35.616897  10.48.17.87     10.48.23.68      ESP          138  ESP (SPI=0xfae51df8)
```

# 疑難排解

常見VPN故障排除技術可用於排除與IPSEC相關的問題。您可以在下面找到有用的文檔：

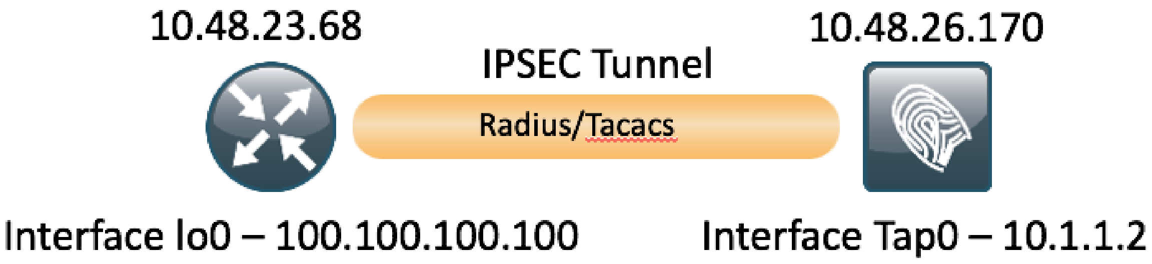
[使用PSK的站點到站點VPN的IOS IKEv2調試故障排除技術說明]

[適用於採用PSK的站點到站點VPN的ASA IKEv2調試]

[IPsec 疑難排解：瞭解和使用偵錯指令]

# 配置NAD和ISE 2.2之間的FlexVPN站點到站點（DVTI到SVTI）

也可以使用FlexVPN保護RADIUS流量。以下示例中使用了以下拓撲：



FlexVPN的配置非常簡單。更多詳情可參閱此處：

http://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html

## Flex VPN設計的優勢

- 您可以在所有先前的IPsec VPN上運行Flex。大多數方案都允許以前的配置和彈性並存。
- Flex VPN基於IKEv2而不是IKEv1，這幾乎改進了協商和協定穩定性的所有方面。
- 用一個框架可以實現多種功能。
- 使用明智的預設值易於配置 — 您不需要定義策略、轉換集等，IKEv2內建的預設值合理且已更新。

## 路由器配置

```
aaa new-model
!
!
aaa group server tacacs+ ISE_TACACS
 server name ISE22_VRF
ip vrf forwarding TACACS
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
aaa authorization network default local
!
crypto ikev2 authorization policy default
 route set interface Loopback0
 no route set interface
!
!
crypto ikev2 keyring mykeys
 peer ISE22
 address 10.48.17.87
 pre-shared-key Krakow123
 !
!
!
crypto ikev2 profile default
 match identity remote address 10.48.17.87 255.255.255.255
 authentication remote pre-share (with the command authentication remote pre-share key in place
keyring is not required)
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list default default
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
crypto ipsec profile default
 set ikev2-profile default (it is default configuration)
!
!
!
interface Loopback0
ip vrf forwarding TACACS
 ip address 100.100.100.100 255.255.255.0
!
interface Tunnel0
ip vrf forwarding TACACS
 ip address 10.1.12.1 255.255.255.0
 tunnel source GigabitEthernet0/0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.48.17.87
 tunnel protection ipsec profile default
!
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
!
!
ip route 0.0.0.0 0.0.0.0 10.48.23.1
ip tacacs source-interface Loopback0
!
!
tacacs server ISE22_VRF
 address ipv4 10.1.1.2
 key cisco
!
ISR4451#
```

## ISE上的ESR配置

```
ise-esr5921#sh run
Building configuration...

Current configuration : 5778 bytes
!
! Last configuration change at 17:32:58 CET Thu Feb 23 2017
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
service call-home
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
!
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone CET 1 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
 active
 destination transport-method http
 no destination transport-method email
!
!
!
!
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
 30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
 6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
 3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
 526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
 82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
 CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
 4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
 7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
 68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
 C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
 DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
 06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
 4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
 03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
 604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
 D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
 467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
 7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
 80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
 418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
 D697DF7F 28
       quit
license udi pid CISCO5921-K9 sn 98492083R3X
username lab password 0 lab
!
redundancy
!
!
!
crypto keyring MVPN-spokes
 pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
crypto ikev2 authorization policy default
 route set interface
 route set remote ipv4 10.1.1.0 255.255.255.0
!
!
!
crypto ikev2 keyring mykeys
 peer ISR4451
 address 10.48.23.68
 pre-shared-key Krakow123
  !
!
!
crypto ikev2 profile default
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list default default local
 virtual-template 1
!
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp policy 20
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key Krakow123 address 0.0.0.0
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
 mode transport
!
!
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2
!
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
!
!
!
!
interface Loopback0
 ip address 10.1.12.2 255.255.255.0
!
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.17.87 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
!
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/2
 description e0/2->connection to CSSM backend license server
 no ip address
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
```

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
ip route 0.0.0.0 0.0.0.0 10.48.17.1
!
!
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
!
!
end
```

## FlexVPN設計注意事項

- 在大多數情況下，應該在ISE的G0/1介面（即ESR的E0/0介面）上終止Radius連線。使用加密對映時，應該使用訪問清單定義相關流量，並使用SVTI — 使用路由。如果兩個路由器配置為通過Tunnel（加密）的ISE介面1和通過interface(Tunnel establishment)的ISE介面，則它將不起作用。 路由器配置也存在同樣的問題。
- 因此，相關流量（加密Radius）在路由器的Lo0介面與ISE的Tap0介面之間通訊（在這種情況下，在ESR上不需要nat）。 因此，可以設定ip route，迫使Radius流量通過通道並進行加密。
- 由於ISE的Tap0介面的IP地址是固定的(10.1.1.2)，因此可以將其置於路由器的VRF中，以確保只在TACACS中通過隧道與此IP地址進行通訊。