配置ISE 2.2 IPSEC以保護NAD(ASA)通訊

目錄

簡介

本文描述如何配置RADIUS IPSEC並對其進行故障排除，以保護思科身份服務引擎(ISE)2.2 — 網路接入裝置(NAD)通訊。RADIUS流量應在自適應安全裝置(ASA)和ISE之間的站點到站點（LAN到LAN）IPSec網際網路金鑰交換版本1和2（IKEv1和IKEv2）隧道內加密。本文檔不涉及AnyConnect SSL VPN配置部分。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- Cisco ASA
- 一般IPSec概念
- 一般RADIUS概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5515-X系列ASA(運行軟體版本9.4(2)11)
- 思科身分識別服務引擎版本2.2
- Windows 7 Service Pack 1

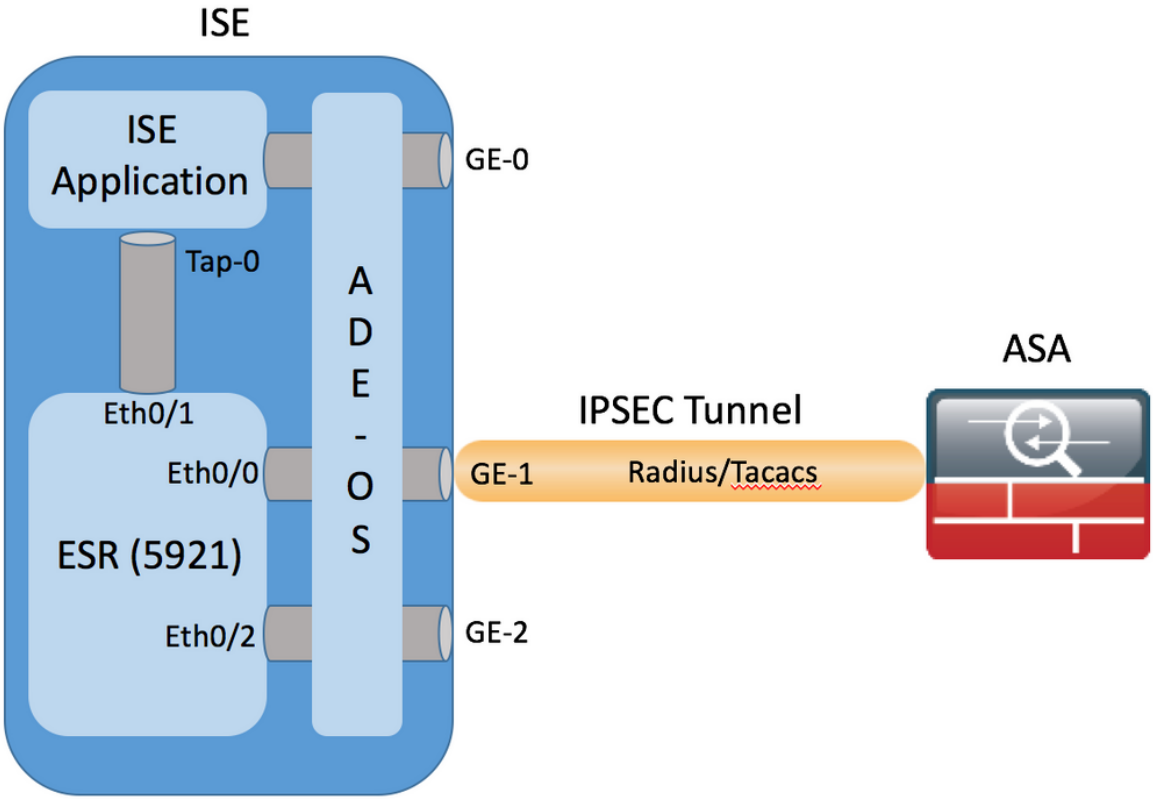
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

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。考慮到這一點：

- 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介面收到加密的資料包後，ESR會在Eth0/0介面上攔截這些資料包。

```
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.26.170 255.255.255.0
 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：

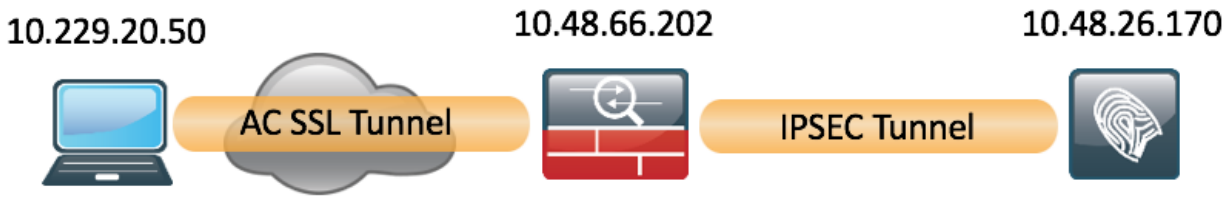
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)
       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
```

設定

本節介紹如何完成ASA CLI和ISE配置。

網路圖表

本檔案中的資訊使用以下網路設定：



ASA配置

配置ASA介面

如果未配置ASA介面/介面，請確保至少配置IP地址、介面名稱和安全級別：

```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
```

配置IKEv1策略並在外部介面上啟用IKEv1

要為IKEv1連線配置Internet安全關聯和金鑰管理協定(ISAKMP)策略，請輸入**crypto ikev1 policy <priority>**命令：

```
crypto ikev1 policy 20
 authentication pre-share
 encryption aes
 hash sha
 group 5
 lifetime 86400
```

注意：當來自兩個對等體的兩個策略包含相同的身份驗證、加密、雜湊和Diffie-Hellman引數值時，存在IKEv1策略匹配。對於IKEv1，遠端對等體策略還必須在發起方傳送的策略中指定小於或等於生存期的生存期。如果生存期不同，則ASA使用較短的生存期。

必須在終止VPN隧道的介面上啟用IKEv1。通常情況下，這是外部(或公共)介面。若要啟用IKEv1，請在全域性配置模式下輸入**crypto ikev1 enable <interface-name>**命令：

```
crypto ikev1 enable outside
```

配置隧道組（LAN到LAN連線配置檔案）

對於LAN到LAN隧道，連線配置檔案型別為**ipsec-l2l**。要配置IKEv1預共用金鑰，請進入*tunnel-group ipsec-attributes*配置模式：

```
tunnel-group 10.48.26.170 type ipsec-l2l
tunnel-group 10.48.26.170 ipsec-attributes
 ikev1 pre-shared-key Krakow123
```

為相關的VPN流量配置ACL

ASA使用訪問控制清單(ACL)來區分應使用IPSec加密保護的流量和不需要保護的流量。它保護與允許應用控制引擎(ACE)匹配的出站資料包，並確保與允許ACE匹配的入站資料包具有保護。

```
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

注意：用於VPN流量的ACL在網路地址轉換(NAT)之後使用源和目標IP地址。 在這種情況下，唯一加密的流量是ASA和ISE之間的流量。

配置IKEv1轉換集

IKEv1轉換集是安全協定和演算法的組合，用於定義ASA保護資料的方式。在IPSec安全關聯(SA)協商期間，對等體必須標識兩個對等體相同的轉換集或提議。然後，ASA應用匹配的轉換集或提議，以便建立一個SA，保護該加密對映的訪問清單中的資料流。

要配置IKEv1轉換集，請輸入**crypto ipsec ikev1 transform-set** 命令：

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

設定密碼編譯對應並將其套用到介面

加密對映定義要在IPSec SA中協商的IPSec策略，包括：

- 訪問清單，用於標識IPSec連線允許和保護的資料包
- 對等體識別
- IPSec流量的本地地址
- IKEv1轉換集

以下是範例：

```
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
```

接著您可以對介面套用密碼編譯對應：

```
crypto map MAP interface outside
```

ASA最終配置

以下是ASA上的最終配置：

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.48.66.202 255.255.254.0
!
!
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
!
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
crypto map MAP interface outside
```

ISE 組態

配置ISE上的IP地址

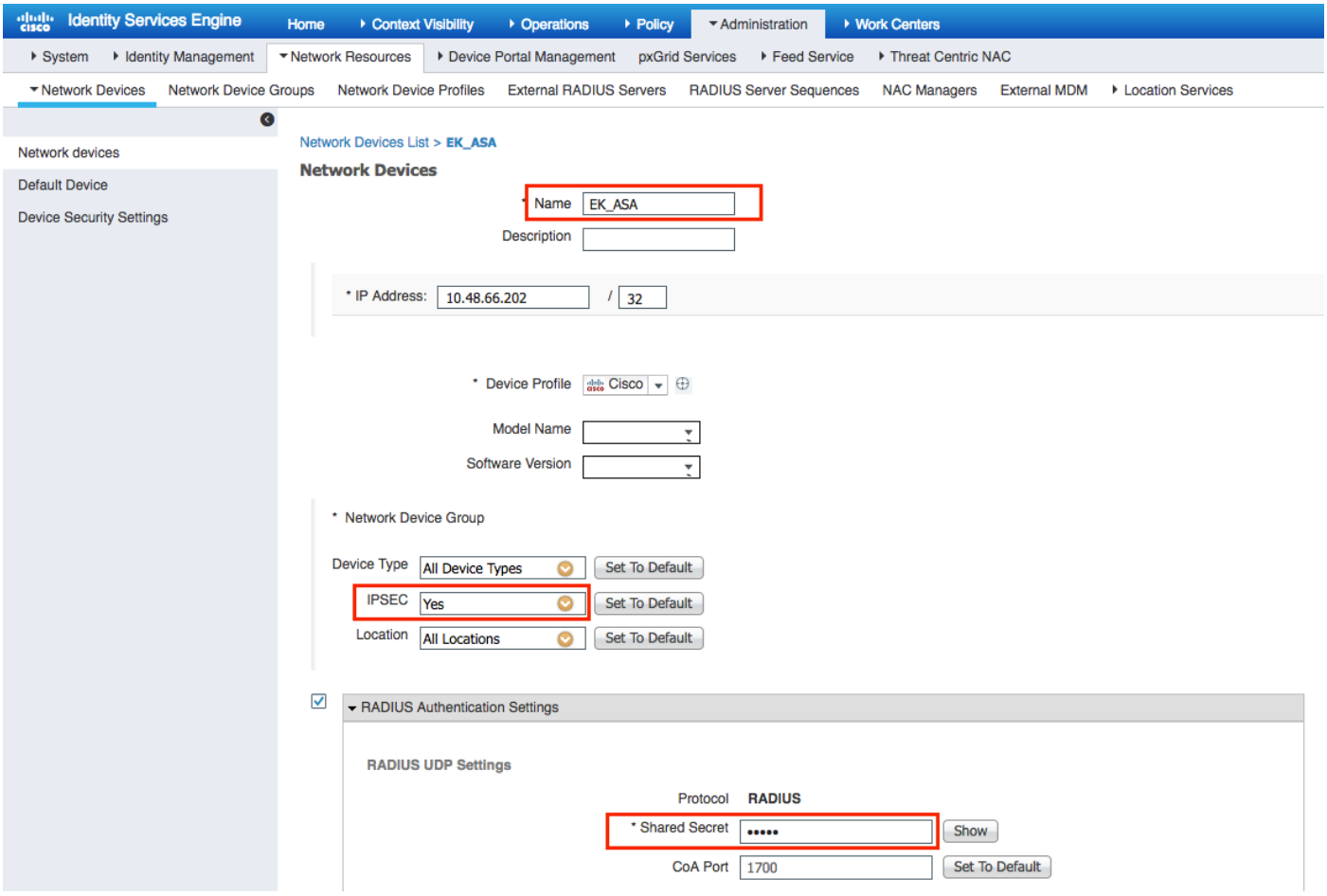
應該從CLI在介面GE1-GE5上配置地址，不支援GE0。

```
interface GigabitEthernet 1
 ip address 10.48.26.170 255.255.255.0
 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**。

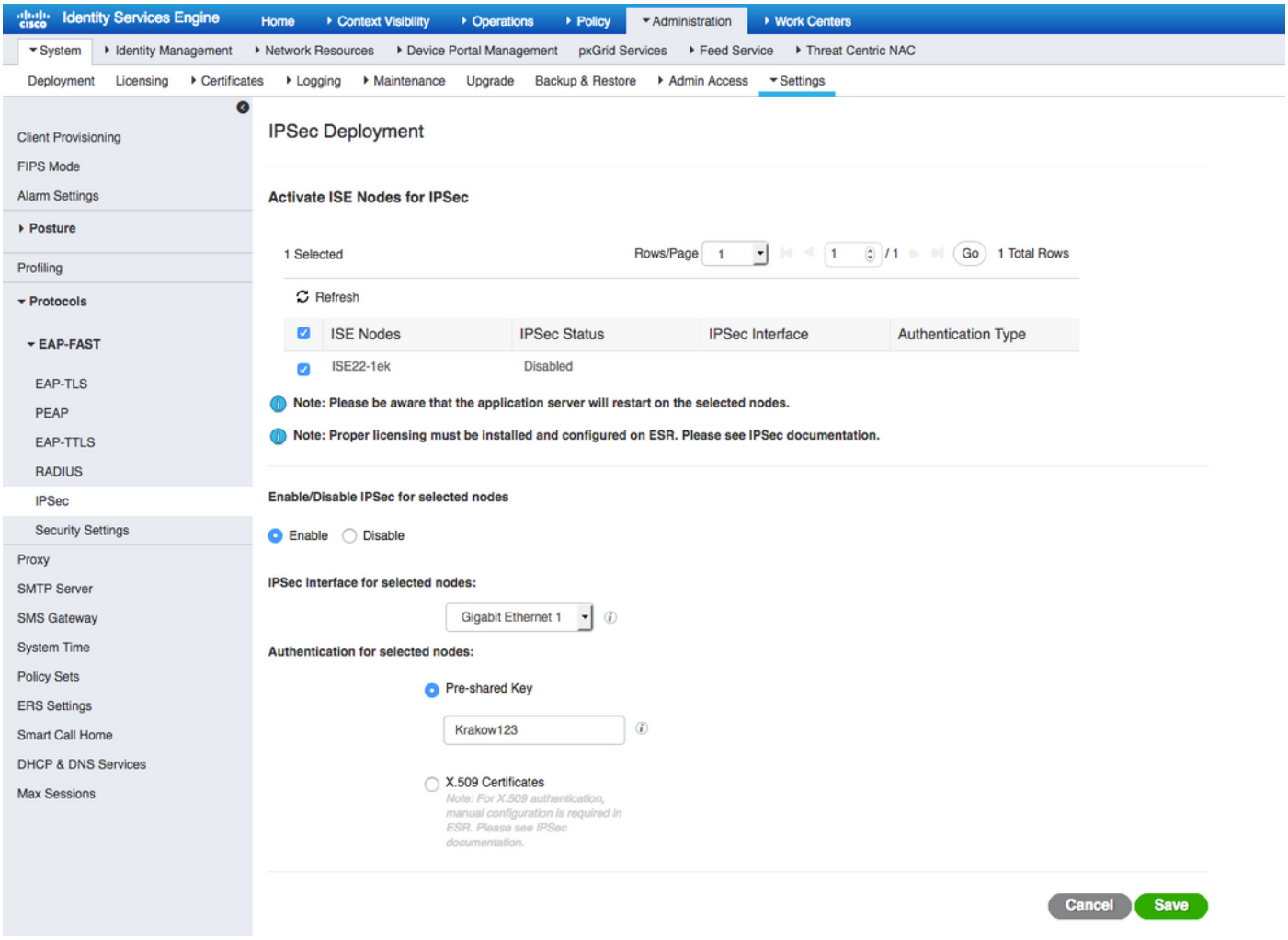


新增NAD後，應在ISE上建立其他路由，以確保RADIUS流量通過ESR並加密：

```
ip route 10.48.66.202 255.255.255.255 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。



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提供以下加密配置：

```
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
```

由於ASA不支援sha256雜湊演算法，因此ESR上需要額外的配置來匹配IPSEC第1階段和第2階段的IKEv1策略。配置isakmp策略和轉換集，以匹配ASA上配置的策略：

```
crypto isakmp policy 30
 encr aes
 authentication pre-share
 group 5
!
crypto ipsec transform-set radius-3 esp-aes esp-sha-hmac
 mode tunnel
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2 radius-3
```

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
```

驗證

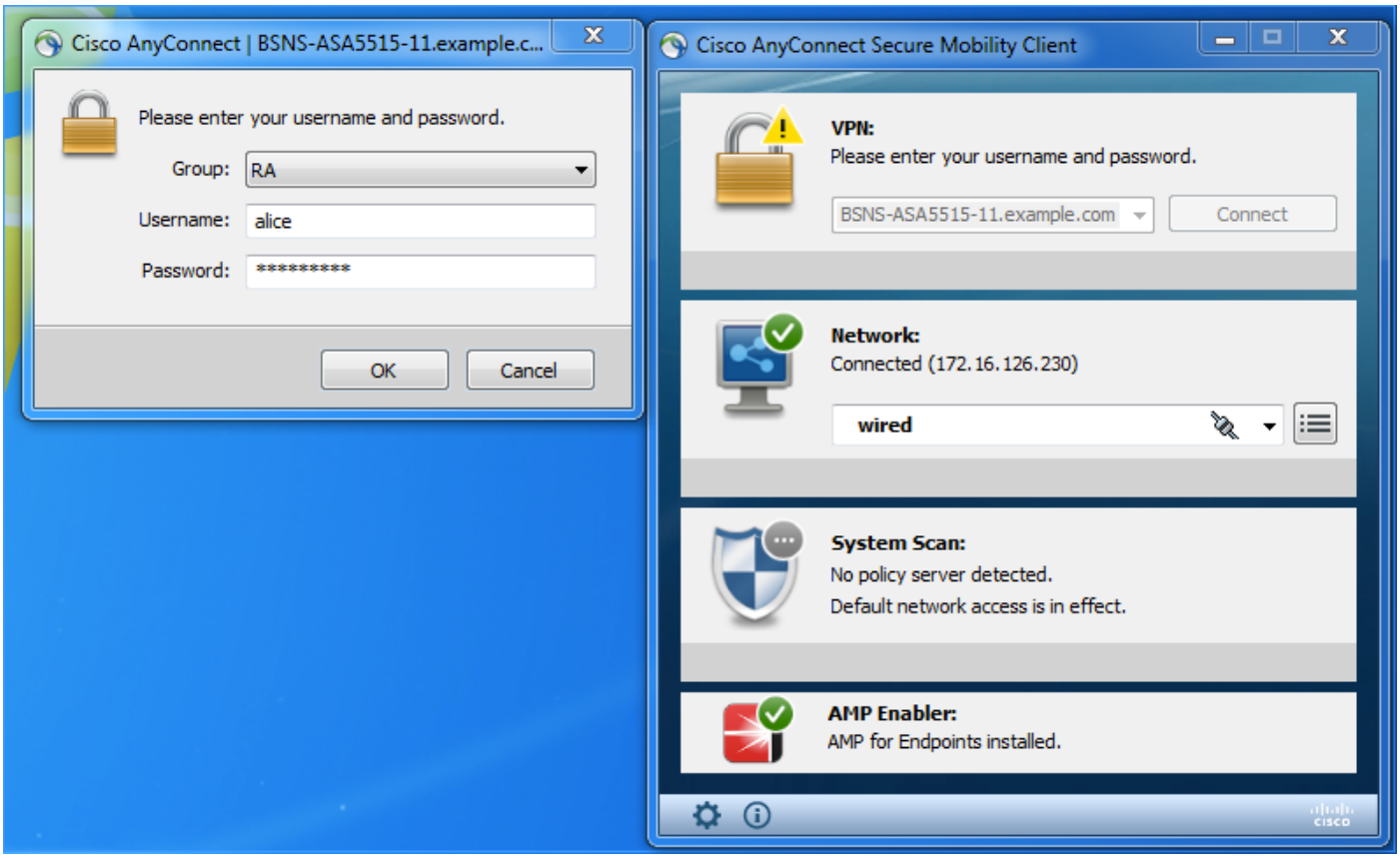
ASA

在Anyconnect客戶端連線之前，ASA沒有加密會話：

```
BSNS-ASA5515-11# sh cry isa sa

There are no IKEv1 SAs

There are no IKEv2 SAs
BSNS-ASA5515-11# sh cry ipsec sa
```

```
There are no ipsec sas
BSNS-ASA5515-11#
```

客戶端通過Anyconnect VPN客戶端連線，因為使用身份驗證源ISE 2.2。



隧道啟動後，ASA會傳送一個觸發VPN會話建立的RADIUS資料包，在ASA上看到以下輸出，並確認隧道的階段1已啟動：

```
BSNS-ASA5515-11# sh cry isa sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.48.26.170
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
BSNS-ASA5515-11#
```

階段2已啟動，封包已加密和解密：

```
BSNS-ASA5515-11# sh cry ipsec sa
interface: outside
   Crypto map tag: MAP, seq num: 20, local addr: 10.48.66.202

     access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
     local ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
     current_peer: 10.48.26.170
```

```
     #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
     #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 10.48.66.202/0, remote crypto endpt.: 10.48.26.170/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 5BBE9F07
     current inbound spi : 068C04D1

   inbound esp sas:
     spi: 0x068C04D1 (109839569)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 323584, crypto-map: MAP
        sa timing: remaining key lifetime (kB/sec): (4373999/3558)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000003F
   outbound esp sas:
     spi: 0x5BBE9F07 (1539219207)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 323584, crypto-map: MAP
        sa timing: remaining key lifetime (kB/sec): (4373999/3558)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

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
10.48.26.170    10.48.66.202    QM_IDLE           1012 ACTIVE MVPN-profile

IPv6 Crypto ISAKMP SA

ise-esr5921#
```

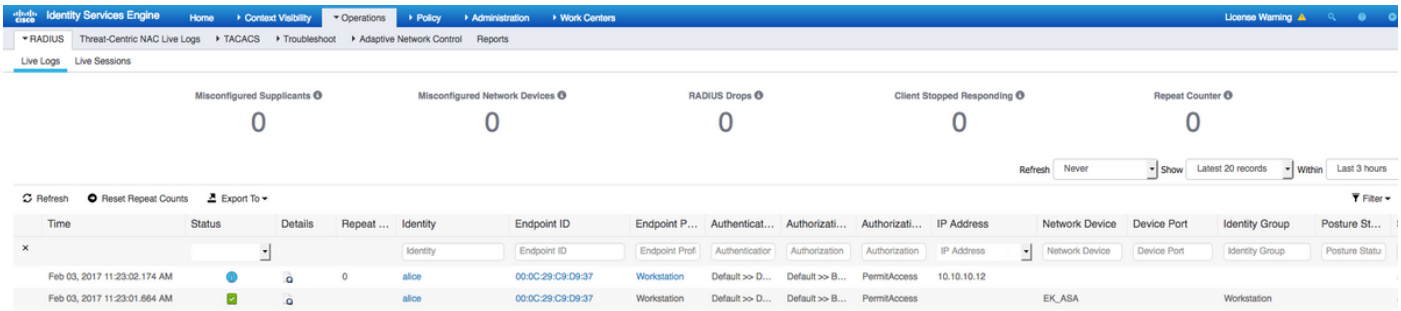
階段2已啟動，資料包已成功加密和解密：

```
ise-esr5921#sh cry ipsec sa

interface: Ethernet0/0
   Crypto map tag: radius, local addr 10.48.26.170

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
```

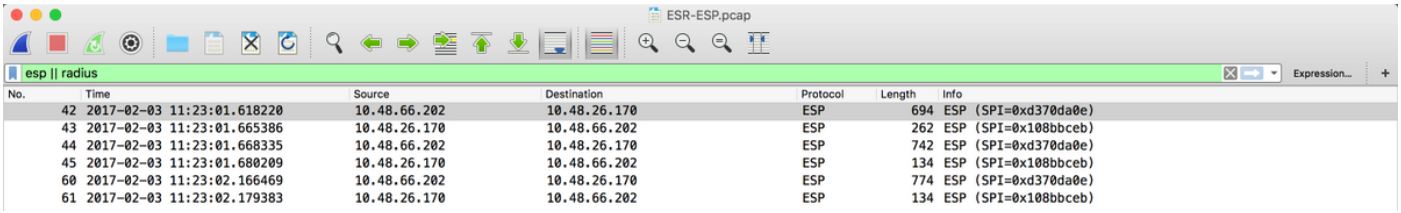
```
remote ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
current_peer 10.48.66.202 port 500
  PERMIT, flags={}
 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 10.48.26.170, remote crypto endpt.: 10.48.66.202
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
  current outbound spi: 0x68C04D1(109839569)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x5BBE9F07(1539219207)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 31, flow_id: SW:31, sibling_flags 80000040, crypto map: radius
     sa timing: remaining key lifetime (k/sec): (4259397/3508)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x68C04D1(109839569)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 32, flow_id: SW:32, sibling_flags 80000040, crypto map: radius
     sa timing: remaining key lifetime (k/sec): (4259397/3508)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```

ISE

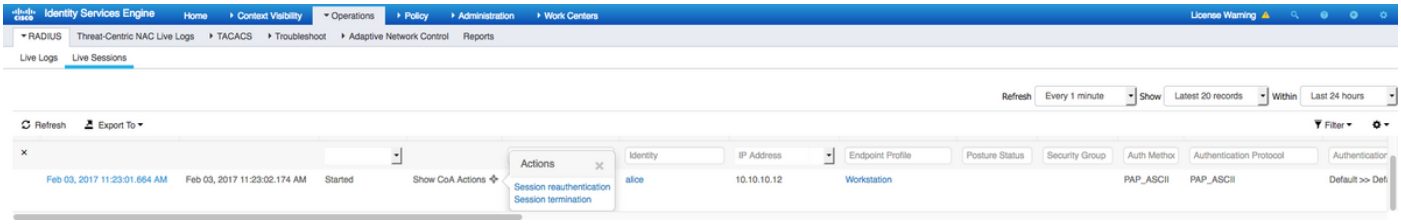
Live Authentication指示常規PAP_ASCII身份驗證：



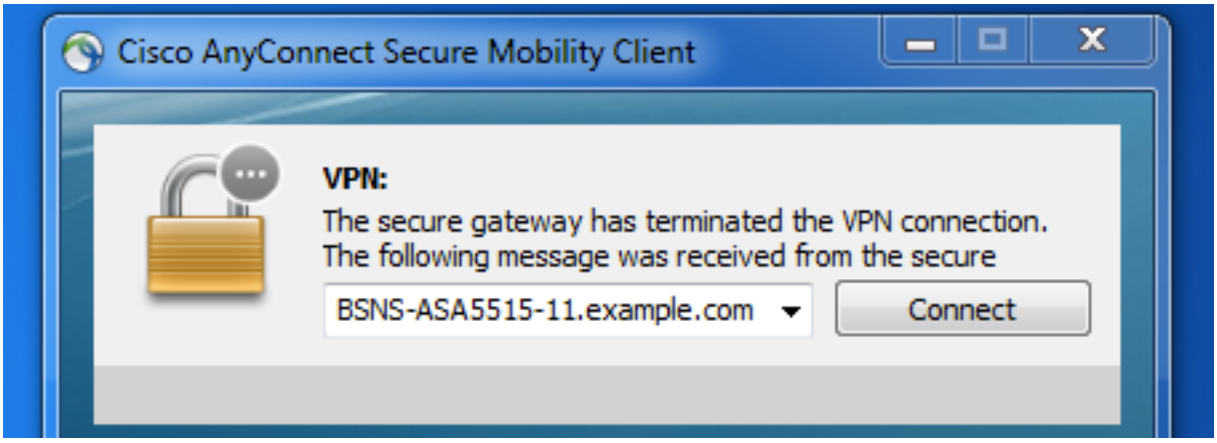
捕獲在ISE的GE1介面上捕獲並使用ESP或Radius過濾，確認明文中沒有Radius，並且所有流量都經過加密：



也可以從ISE傳送加密資料包 — 授權更改(CoA) — 隧道啟動並運行後：



在本示例中，已發出會話終止命令，因此VPN客戶端斷開連線：



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：

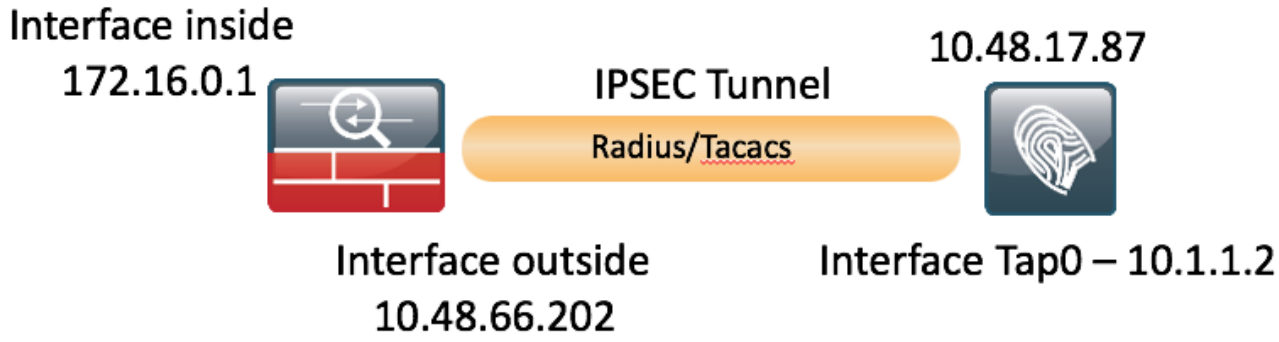
使用PSK的站點到站點VPN的IOS IKEv2調試故障排除技術說明

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

在NAD和ISE 2.2之間配置FlexVPN站點到站點（DVTI到加密對映）

也可以使用FlexVPN保護RADIUS流量。以下示例中使用了以下拓撲：



FlexVPN配置是直接向前進行的。更多詳情可參閱此處：

http://www.cisco.com/c/en/us/support/docs/security/flexvpn/116008-flexvpn-nge-config-00.html

ASA配置

```
hostname BSNS-ASA5515-11
domain-name example.com

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.0.1 255.255.255.0
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network POOL
 subnet 10.10.10.0 255.255.255.0
object network ISE
 host 10.48.17.86
object network ISE22
 host 10.1.1.2
object network INSIDE-NET
 subnet 172.16.0.0 255.255.0.0
access-list 101 extended permit ip host 172.16.0.1 host 10.1.1.2
access-list OUT extended permit ip any any
nat (inside,outside) source static INSIDE-NET INSIDE-NET destination static ISE22 ISE22
nat (outside,outside) source dynamic POOL interface
nat (inside,outside) source dynamic any interface
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.48.66.1 1

aaa-server ISE22 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE22 (inside) host 10.1.1.2
 key *****
```

```
crypto ipsec ikev2 ipsec-proposal SET
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map DMAP 1 set ikev1 transform-set SET
crypto map MAP 10 ipsec-isakmp dynamic DMAP
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.17.87
crypto map MAP 20 set ikev2 ipsec-proposal SET
crypto map MAP interface outside
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 2
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
management-access inside
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable
group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ssl-client
tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE22
 accounting-server-group ISE22
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
tunnel-group 10.48.17.87 type ipsec-l2l
tunnel-group 10.48.17.87 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

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

- VPN隧道是使用ESR端的DVTI和ASA端的Crypto Map構建的，ASA上的配置能夠生成源自內部介面的Radius資料包，這將確保加密的正確訪問清單可觸發VPN會話建立。
- 請注意，在這種情況下，ASA NAD應定義在具有內部介面IP地址的ISE上。