Configuratie van ISE 2.2 IPSEC om NAD (IOS)-communicatie te beveiligen

Inhoud

Inleiding

Dit document beschrijft hoe u TACACS IPSEC kunt configureren en oplossen om de communicatie van Cisco Identity Services Engine (ISE) 2.2 - Network Access Devices (NAD) te beveiligen. TACACS-verkeer kan worden versleuteld met de site-to-site (LAN-to-LAN) IPSec Internet Key Exchange versie 2 (IKEv2) tussen router en ISE. Dit document heeft geen betrekking op het TACACS-configuratiegedeelte.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Cisco-router
- Algemene IPsec-concepten
- Algemene TACACS-concepten

Gebruikte componenten

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

- Cisco ISR 4451-X router met softwareversie 15.4(3)S2
- Cisco Identity Services Engine versie 2.2
- Windows 7 Service Pack 1

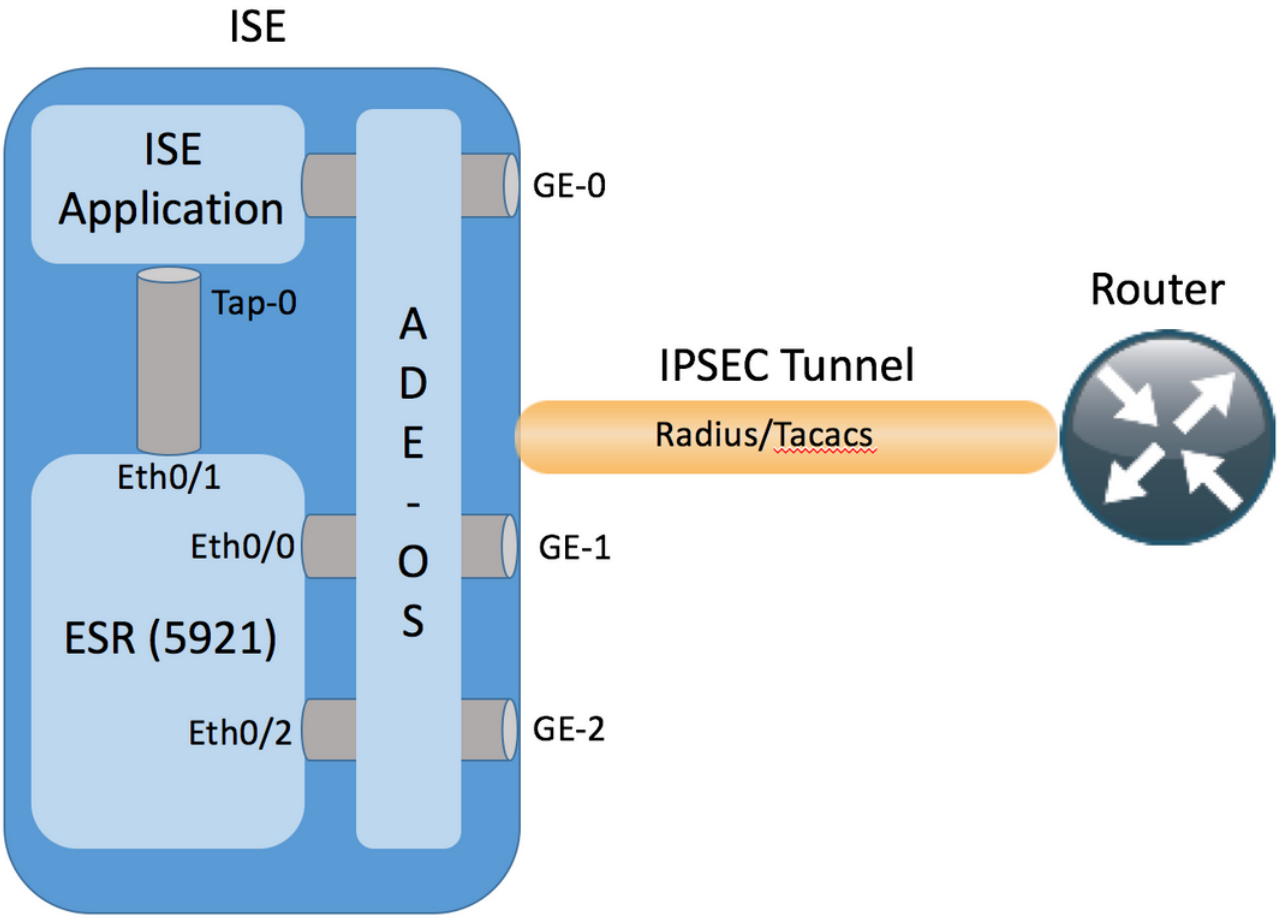
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Het doel is protocollen te beveiligen die gebruik maken van onveilige MD5-hash, RADIUS en TACACS met IPSec. Weinig feiten waarmee rekening moet worden gehouden:

- Cisco ISE ondersteunt IPSec in tunnels en transportmodi.
- Wanneer u IPSec op een interface van Cisco ISE toelaat, wordt een IPSec-tunnel gemaakt tussen Cisco ISE en NAD om de communicatie te verzekeren.
- U kunt een vooraf gedeelde toets definiëren of X.509-certificaten gebruiken voor IPSec-verificatie.
- IPsec kan op Eth1 door Eth5 interfaces worden ingeschakeld. U kunt IPSec op slechts één Cisco ISE-interface per PSN configureren.

ISE IPsec-architectuur



Nadat de versleutelde pakketten door GE-1 ISE-interface zijn ontvangen, onderbreekt de ingesloten services router (ESR) ze op Eth0/0-interface.

```
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 decrypteert ze en volgens vooraf gevormde NAT regels voert adresvertaling uit. Uitgaande (naar NAD) RADIUS/TACACS-pakketten worden vertaald naar Ethernet0/0 interfaceadres en versleuteld daarna.

```
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
```

Pakketten die bestemd zijn voor de Eth0/0-interface op RADIUS/TACACS-poorten moeten via Eth0/1-interface worden verstuurd naar 10.1.1.2 ip-adres, dat het interne adres van ISE is. ESR-configuratie van Eth0/1

```
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
```

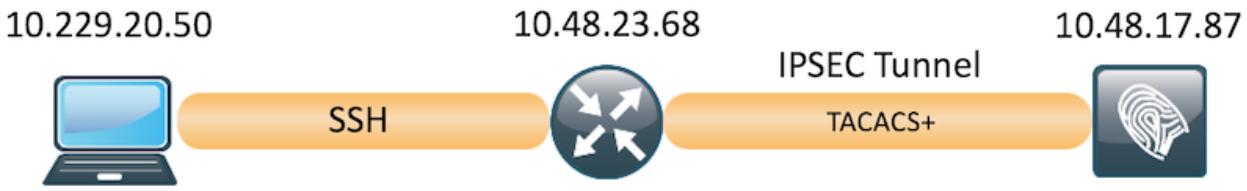
```
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
```

ISE-configuratie van interne Tap-0-interface:

```
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
```

Netwerkdiagram

De informatie in dit document gebruikt deze netwerkinstelling:



Configuratie van ikev1 ipsec VPN met behulp van vooraf gedeelde toets (uit het vakje)

In deze sectie worden beschreven hoe de IOS CLI en ISE configuraties moeten worden voltooid.

IOS-routerCLI-configuratie

Interfaces configureren

Als de IOS routerinterfaces nog niet zijn geconfigureerd, moet ten minste de WAN-interface worden geconfigureerd. Hierna volgt een voorbeeld:

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

Zorg ervoor dat er connectiviteit is aan de verre peer die zou moeten worden gebruikt om een site-to-site VPN-tunnel op te zetten. U kunt een ping gebruiken om basisconnectiviteit te verifiëren.

Het ISAKMP-beleid (IKEv1) configureren

Om het ISAKMP beleid voor de IKEv1-verbindingen te configureren voert u het **crypto-isakmp-**

beleid in **de** wereldwijde configuratie-modus. Hier is een voorbeeld:

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

> **Opmerking:** U kunt meerdere IKE-beleidsmaatregelen configureren op elk peer dat deelneemt aan IPSec. Wanneer de IKE-onderhandeling begint, probeert het een gemeenschappelijk beleid te vinden dat op beide peers is ingesteld en begint het met het hoogste prioriteitsbeleid dat op de afstandsbediening is gespecificeerd.

Een Cryptie ISAKMP-toets configureren

Om een *vooraf gedeelde* authenticatiesleutel te configureren voert u de opdracht **crypto**-*isakmp* in de wereldwijde configuratie-modus:

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

Configureer een ACL voor VPN-verkeer met belangstelling

Gebruik de uitgebreide of genoemde toegangslijst om het verkeer te specificeren dat door encryptie moet worden beschermd. Hierna volgt een voorbeeld:

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

> **Opmerking:** Een ACL voor VPN-verkeer gebruikt de bron- en doeladressen na NAT.

Instellen van transformatie

Om een IPSec transformatie set te definiëren (een aanvaardbare combinatie van veiligheidsprotocollen en algoritmen), **moet** u het **crypto ipsec transformatie-ingestelde** opdracht in mondiale configuratiemodus invoeren. Hierna volgt een voorbeeld:

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

Configuratie van een Crypto Kaart en pas het op een interface toe

Om een crypto kaartingang te maken of aan te passen en de configuratie van crypto in kaart te brengen, **moet** de **crypto kaart** mondiaal configuratie opdracht ingaan. Om de toegang tot crypto-plattegronden te kunnen voltooien, zijn er enkele aspecten die ten minste moeten worden gedefinieerd:

- De IPsec-peers waaraan het beschermde verkeer kan worden doorgestuurd, moeten worden gedefinieerd. Dit zijn de gelijken waarmee een SA kan worden opgericht. Om een IPSec peer in een crypto kaartingang te specificeren, voer de **vastgestelde peer** opdracht in.
- De transformatiesets die acceptabel zijn voor gebruik met het beschermde verkeer moeten

worden gedefinieerd. Om de transformatiesets te specificeren die gebruikt kunnen worden met de crypto map ingang, voer de **ingestelde transformatie-set** opdracht in.
- Het verkeer dat moet worden beschermd moet worden gedefinieerd. Om een uitgebreide toegangslijst voor een crypto map ingang te specificeren, voer de opdracht **matchadres** in.

Hierna volgt een voorbeeld:

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

De laatste stap is de eerder gedefinieerde crypto map toe te passen op een interface. Om dit toe te passen, voer de opdracht voor configuratie van de **crypto-kaart** in:

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

IOS-definitieve configuratie

Hier is de laatste IOS router CLI-configuratie:

```
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-configuratie

IP-adres configureren op ISE

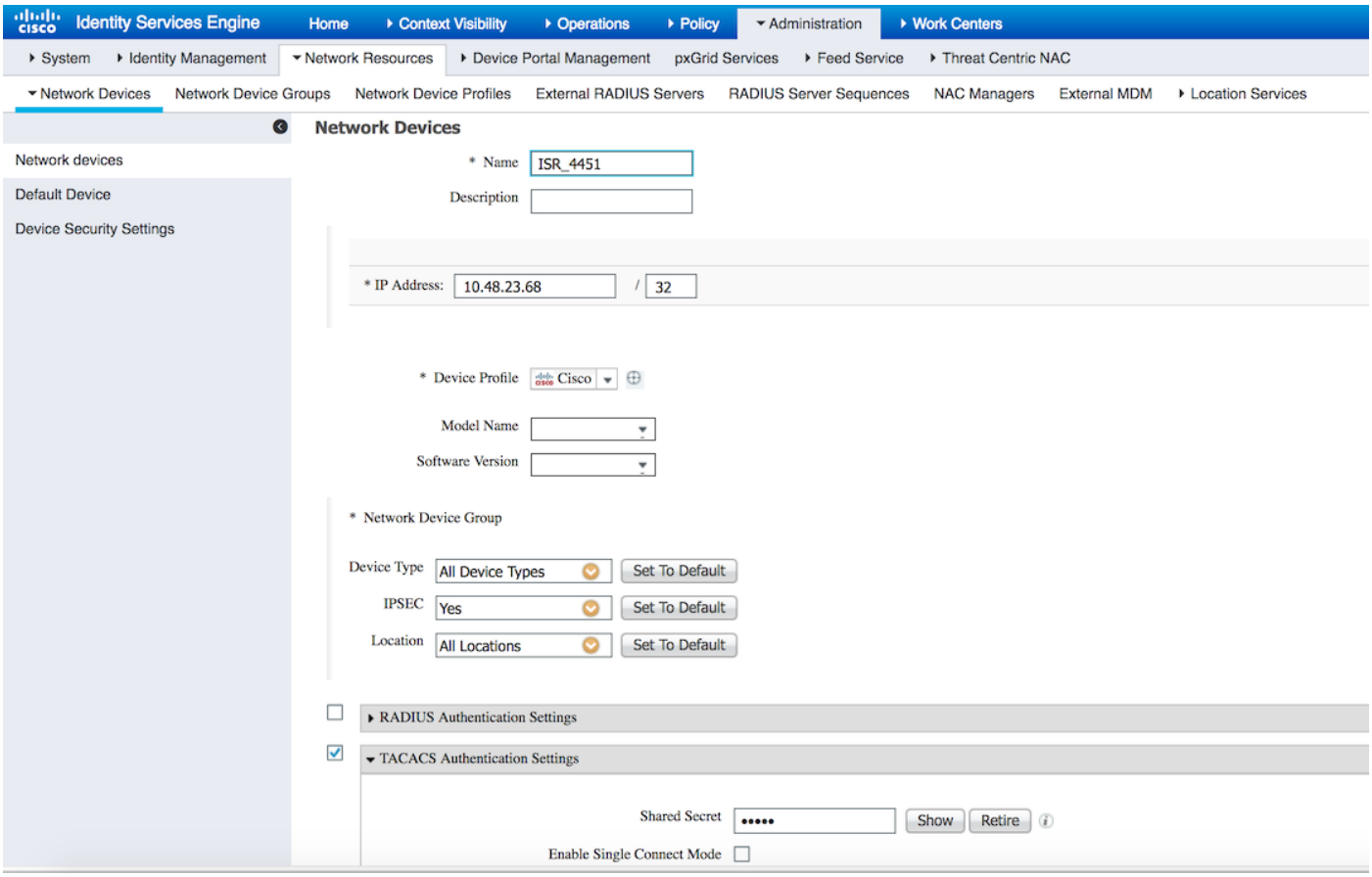
Het adres moet worden ingesteld op interface GE1-GE5 van de CLI, GE0 wordt niet ondersteund.

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

> Opmerking: Herstart van de toepassing nadat het IP-adres op de interface is ingesteld:
> % Een wijziging van het IP-adres kan ertoe leiden dat ISE-diensten opnieuw worden gestart
> Doorgaan met verandering van IP-adres? Y/N [N]: Y

NAD toevoegen aan IPSec-groep op ISE

Navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**. Klik op **Toevoegen**. Zorg ervoor dat u de naam, IP Adres, Gedeeld Geheime vormt. U kunt de IPSec-tunnel uit de NAD sluiten door JA tegen IPSEC-netwerkapparaatgroep te selecteren.

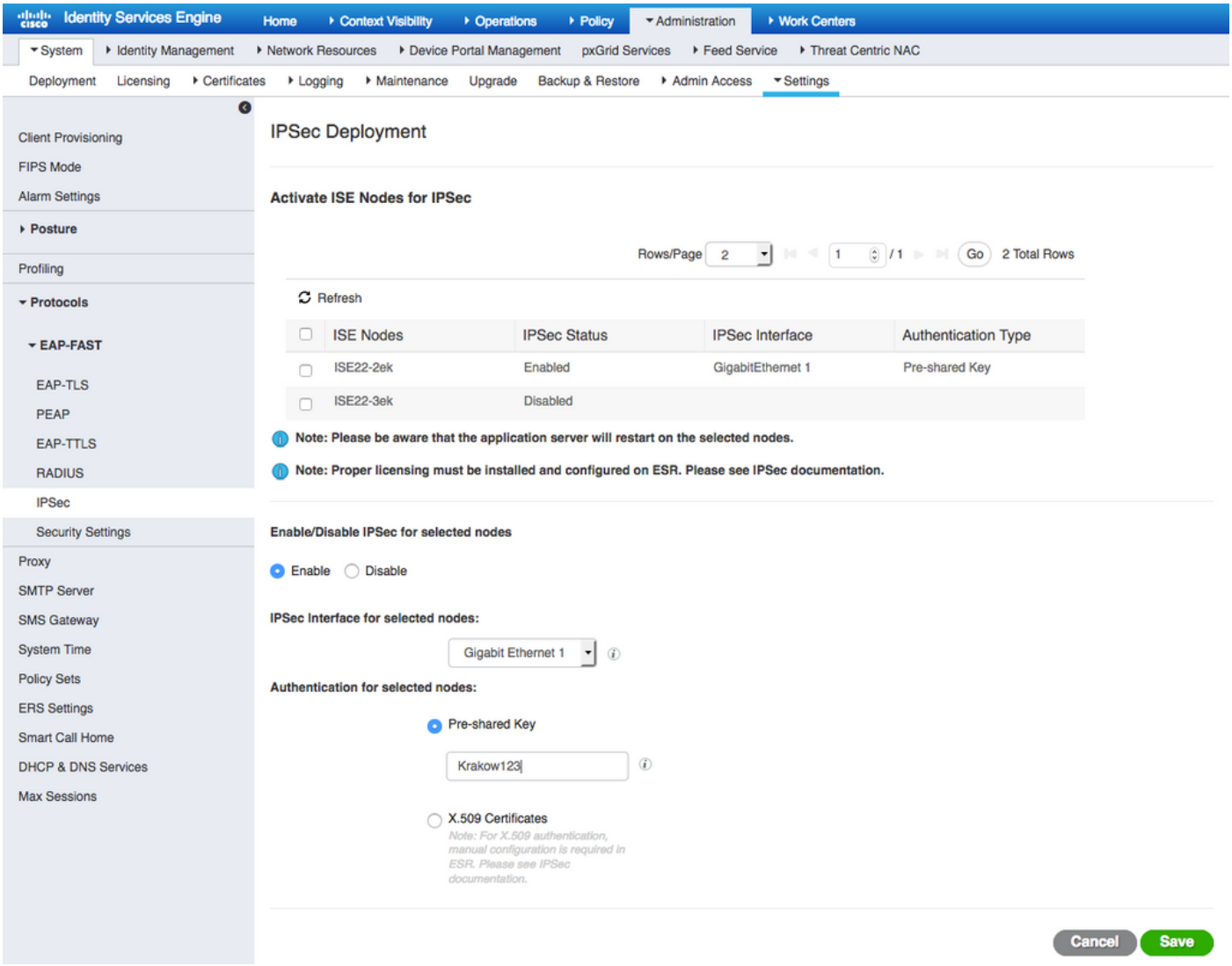


Zodra NAD is toegevoegd, moet er een extra route op ISE worden aangelegd om er zeker van te zijn dat RADIUS-verkeer via ESR verloopt en versleuteld wordt:

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

IPSEC op ISE inschakelen

Navigeer naar **Beheer > Systeem > Instellingen**. Klik op Radius en verder op IPSEC. Selecteer PSN (Single/Multiple/All) selecteer de optie Inschakelen, kies de interface en selecteer de verificatiemethode. Klik op **Opslaan**. Start de services opnieuw op het geselecteerde knooppunt op dit punt.



Merk op dat na het opnieuw opstarten van services ISE CLI configuratie de geconfigureerde interface zonder IP-adres en in shutdown-status toont, het verwacht wordt als ESR (Embedded Services router) controle over ISE-interface krijgt.

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

Wanneer de diensten opnieuw zijn opgestart, is ESR-functionaliteit ingeschakeld. U kunt als volgt inloggen op ESR-type of in de opdrachtregel:

```
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#
```

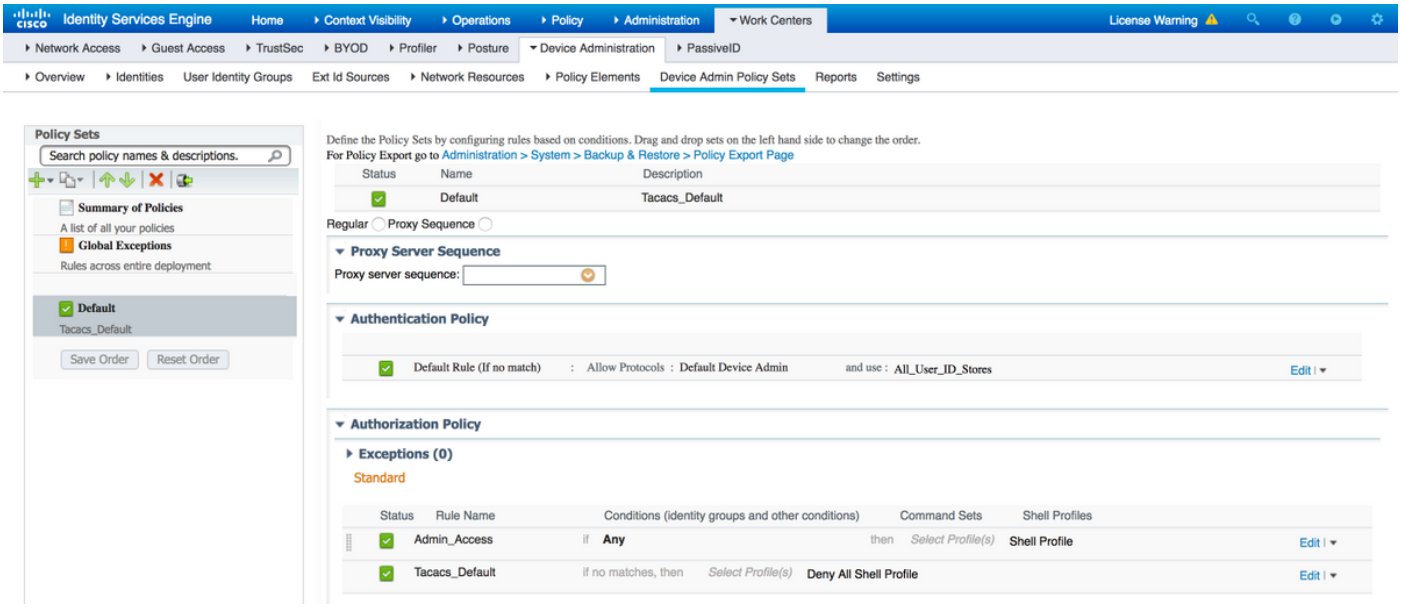
ESR wordt geleverd met deze crypto configuratie, die genoeg is om de ipsec-tunnel te laten sluiten met vooraf gedeelde toetsen:

```
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
```

Zorg ervoor dat ESR over een route beschikt om versleutelde pakketten te verzenden:

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

TACACS-beleid op ISE instellen



Verifiëren

IOS-router

Voordat de sessie wordt gestart op de router, zijn er geen actieve VPN-verbindingen:

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

IPv6 Crypto ISAKMP SA
```

Clientverbindingen met router, als een verificatiebron ISE 2.2 wordt gebruikt.

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

IOS verstuurt een TACACS Packet, dat de zittingstelling van VPN in werking stelt, wanneer de tunnel omhoog is de deze uitvoer op de router wordt gezien. Het bevestigt dat de eerste fase van de tunnel is opgebouwd:

```
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#
```

Fase 2 is omhoog, en de pakketten zijn versleuteld en gedecrypteerd:

```
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

Dezelfde uitgangen kunnen worden gecontroleerd op ESR, fase één is omhoog:

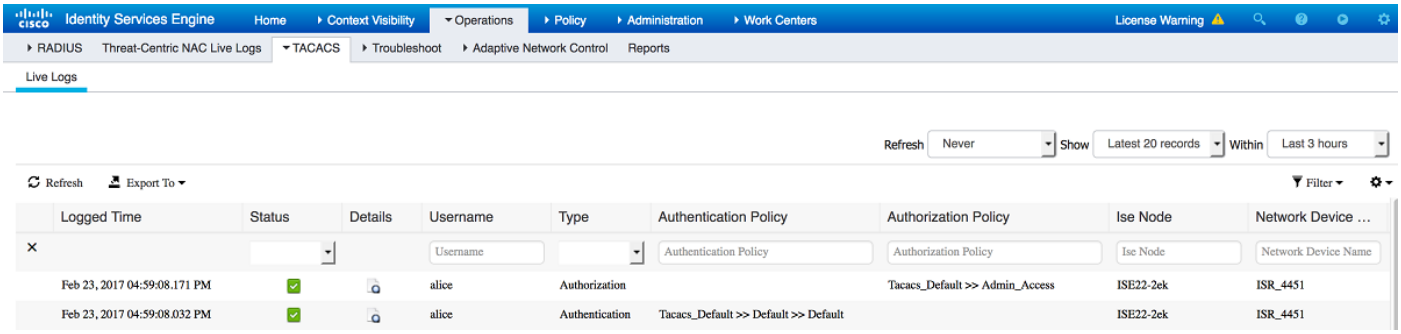
```
ise-esr5921#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.48.17.87     10.48.23.68     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

ise-esr5921#
```

Fase 2 is omhoog, pakketten worden versleuteld en gedecrypteerd met succes:

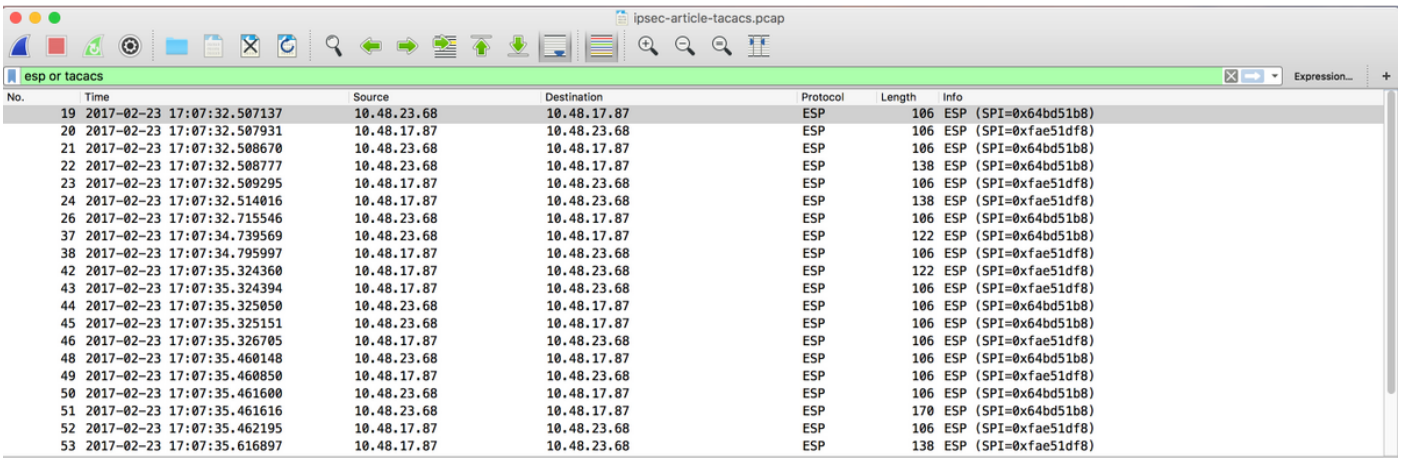
```
ise-esr5921#sh cry ipsec sa

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-verificatie duidt op regelmatige PAP_ASCII-verificatie:



Opname genomen op GE1 interface van ISE en gefilterd met ESP of TACACS, bevestig dat er geen Tacacs in duidelijke tekst zijn en al het verkeer is versleuteld:



Problemen oplossen

De gemeenschappelijke techniek van de Probleemoplossing van VPN kan worden toegepast op problemen van de probleemoplossing met betrekking tot IPSEC. U vindt de onderstaande nuttige documenten:

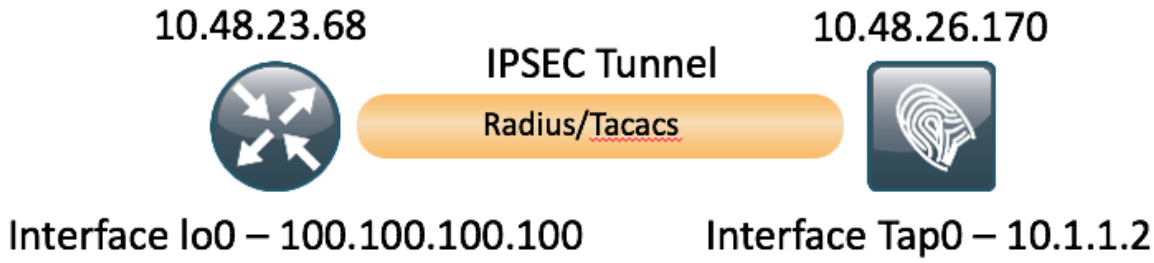
IOS IKEv2-apparaten voor Site-to-Site VPN met TechNotes voor probleemoplossing bij PSK's

ASA IKEv2-debugs voor Site-to-Site VPN met PSK's

IPsec-probleemoplossing: Opdrachten begrijpen en gebruiken

Configureer FlexVPN site-to-Site (DVTI-to-SVTI) tussen NAD en ISE 2.2

Het is ook mogelijk om RADIUS-verkeer met FlexVPN te beschermen. De volgende topologie wordt in het onderstaande voorbeeld gebruikt:



De configuratie van FlexVPN is eenvoudig. Zie voor meer informatie:

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

Voordelen van Flex VPN-ontwerp

- U kunt Flex langs al uw vorige IPsec VPN's uitvoeren. De meeste scenario's maken coëxistentie van vorige configuratie en flex mogelijk.
- Flex VPN is gebaseerd op IKEv2 en niet op IKEv1, wat vrijwel alle aspecten van onderhandeling en protocolstabiliteit verbetert.
- Meervoudige functies bereikbaar met één kader.
- Kunt u configuratie vereenvoudigen met behulp van standaardwaarden - u hoeft geen beleid te definiëren, sets enz. om te zetten, IKEv2 is ingebouwd op een waarde die logisch is en wordt bijgewerkt.

Routerconfiguratie

```
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#
```

ESR-configuratie op ISE

```
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-ontwerpoverwegingen

- In de meeste gevallen dient de Radius-verbinding te worden afgesloten op G0/1-interface van ISE, dat E0/0-interface van ESR is. Tijdens het gebruik van crypto kaarten zou interessant verkeer met toegangslijsten moeten worden gedefinieerd, met SVTI - het gebruik van routing. Het zal niet werken, als twee routers worden geconfigureerd voor ISE-interface, één via Tunnel (versleuteld) en één via interface (Tunnelinstelling). Het zelfde probleem is van toepassing op de routerconfiguratie.
- Om deze reden wordt interessant verkeer (Versleutelde straal) gecommuniceerd tussen Lo0-interface van de router en Tap0-interface van ISE (er is in dit geval geen NAT nodig op ESR). Daarom kan ip route worden geconfigureerd om Radius verkeer te dwingen door de tunnel te gaan en versleuteld te worden.
- Aangezien het IP-adres van de Tap0-interface van ISE is vastgesteld (10.1.1.2) kan deze op router in VRF worden geplaatst, zodat communicatie naar dit IP-adres alleen voor TACACS en alleen door de tunnel plaatsvindt.