Configurez ISE 2.2 IPSEC pour sécuriser la transmission NAD (ASA)

Contenu

Introduction

Ce document décrit comment configurer et dépanner le RAYON IPSEC pour sécuriser l'engine de gestion d'identité de Cisco (ISE) 2.2 - transmission du périphérique d'accès au réseau (NAD). Le trafic de RAYON devrait être chiffré dans la version 1 d'échange de clés Internet (IKE) d'IPSec de site à site (entre réseaux locaux) et (IKEv1 et IKEv2) le tunnel 2 entre l'appliance de sécurité adaptable (ASA) et l'ISE. Ce document ne couvre pas la cloison de configuration de VPN SSL d'AnyConnect.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Cisco ASA
- Concepts du Général IPSec
- Concepts de général RADIUS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme Cisco 5515-X ASA qui exécute la version de logiciel 9.4(2)11
- Version 2.2 d'engine de gestion d'identité de Cisco
- Service Pack 1 de Windows 7

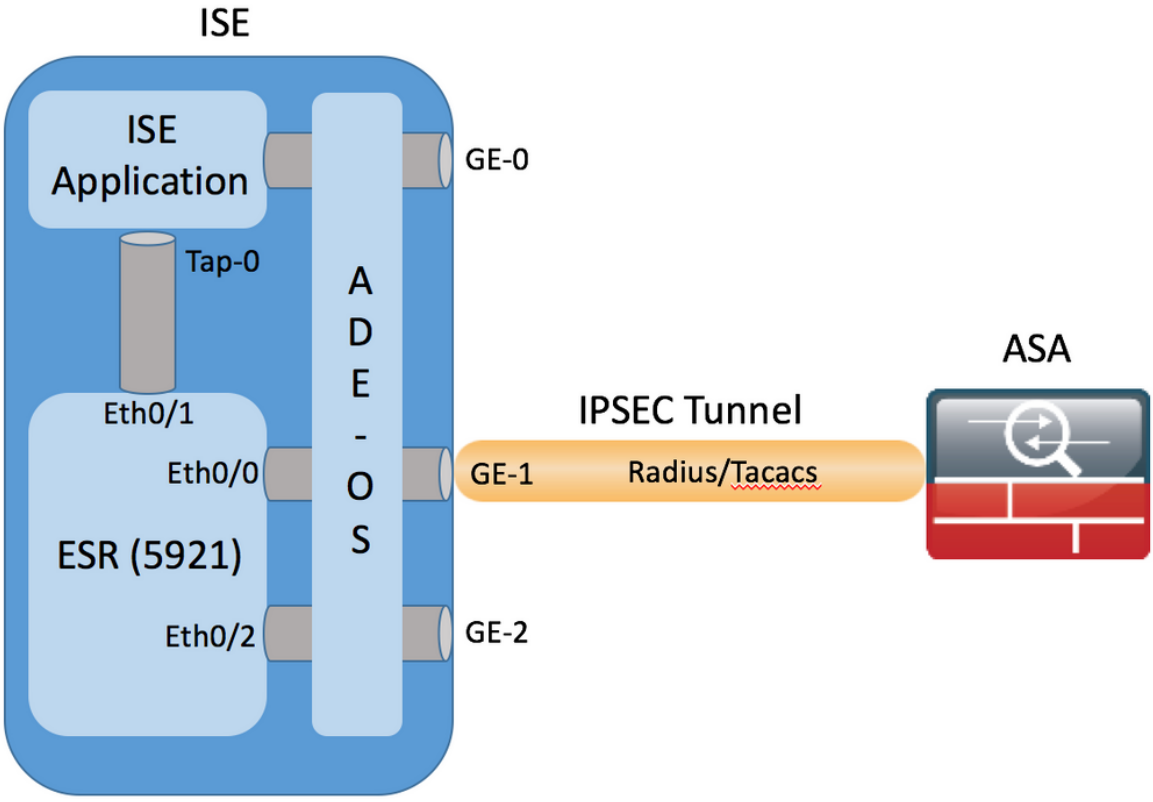
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'objectif est aux protocoles sécurisés qui utilisent les informations parasites non sécurisées, le rayon et le TACACS de MD5 avec IPSec. Prenez en compte ceci :

- Cisco ISE prend en charge IPSec en modes de tunnel et de transport.
- Quand vous activez IPSec sur une interface de Cisco ISE, un tunnel d'IPSec est créé entre Cisco ISE et le NAD pour sécuriser la transmission.
- Vous pouvez définir des Certificats pré-partagés principaux ou de l'utilisation X.509 pour l'authentification d'IPSec.
- IPSec peut être activé sur Eth1 par les interfaces Eth5. Vous pouvez configurer IPSec sur seulement une interface de Cisco ISE par RPC.

Architecture ISE IPSec



Une fois que des paquets chiffrés sont reçus par l'interface ESR GE-1 ISE les intercepte sur l'interface Eth0/0.

```
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
```

L'ESR les déchiffre et selon des règles NAT préconfigurées exécute la traduction d'adresses. (Vers le NAD) des paquets sortants RADIUS/TACACS sont traduits à l'adresse de l'interface Ethernet0/0 et après chiffrés.

```
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
```

Des paquets qui sont destinés à l'interface Eth0/0 sur des ports RADIUS/TACACS devraient forwared par l'intermédiaire de l'interface Eth0/1 à l'IP address de 10.1.1.2, qui est adresse interne d'ISE. Configuration ESR d'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
```

Configuration ISE de l'interface Tap-0 interne :

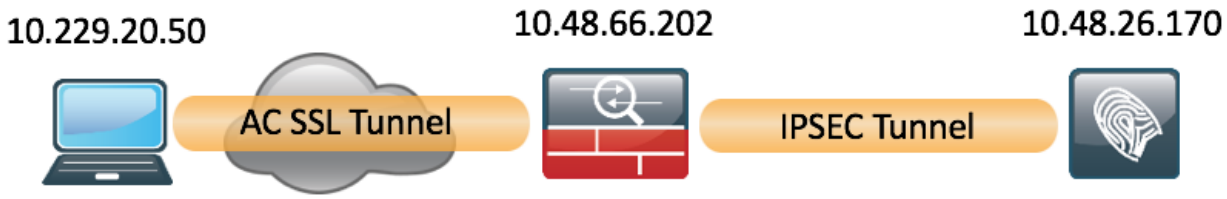
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)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

Configurez

Cette section décrit comment se terminer les configurations ASA CLI et ISE.

Diagramme du réseau

Les informations dans ce document utilisent cette configuration réseau :



Configuration ASA

Configurez les interfaces ASA

Si l'interface/interfaces ASA ne sont pas configurées, assurez-vous que vous configurez au moins l'adresse IP, reliez le nom, et niveau de la Sécurité :

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

Configurez la stratégie IKEv1 et activez IKEv1 sur l'interface extérieure

Afin de configurer les stratégies de Protocole ISAKMP (Internet Security Association and Key Management Protocol) pour les connexions IKEv1, sélectionnez la **crypto** commande de **<priority> de la stratégie ikev1** :

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

> **Remarque:** Une correspondance de la stratégie IKEv1 existe quand chacun des deux stratégies des deux pairs des valeurs contiennent la mêmes authentification, cryptage, informations parasites, et de Diffie-Hellman paramètre. Pour IKEv1, la stratégie distante de pair doit également spécifier une vie inférieur ou égal à la vie dans la stratégie que le demandeur envoie. Si les vies ne sont pas identiques, alors l'ASA utilise la vie plus courte.

Vous devez activer IKEv1 sur l'interface qui termine le tunnel VPN. Typiquement, c'est l'interface extérieure (ou *public*). Afin d'activer IKEv1, sélectionnez la **crypto** commande de **<interface-name> de l'enable ikev1** en mode de configuration globale :

```
crypto ikev1 enable outside
```

Configurez le groupe de tunnel (le profil de connexion entre réseaux locaux)

Pour un tunnel entre réseaux locaux, le type de profil de connexion est **ipsec-l2l**. Afin de configurer la clé pré-partagée IKEv1, écrivez le mode de configuration d'ipsec-*attributs de groupe de tunnels* :

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

Configurez l'ACL pour le trafic VPN d'intérêt

L'ASA emploie le Listes de contrôle d'accès (ACL) afin de différencier le trafic qui devrait être protégé avec le chiffrement IPSec contre le trafic qui n'exige pas la protection. Il protège les paquets sortants qui apparient une engine de contrôle d'application d'autorisation (ACE) et s'assure que les paquets entrant qui apparient une autorisation ACE ayez la protection.

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

> **Remarque:** Un ACL pour le trafic VPN utilise la source et les adresses IP de destination après Traduction d'adresses de réseau (NAT). Le seul trafic chiffré dans ce cas est le trafic entre l'ASA et l'ISE.

Configurez le jeu de transformations IKEv1

Un jeu de transformations IKEv1 est une combinaison des protocoles de Sécurité et des algorithmes qui définissent la manière dont l'ASA protège des données. Pendant les négociations de l'association de sécurité IPSec (SA), les pairs doivent identifier un jeu de transformations ou une proposition qui est identiques pour chacun des deux pairs. L'ASA applique alors le jeu de transformations ou la proposition apparié afin de créer SA qui protège des flux de données dans la liste d'accès pour ce crypto map.

Afin de configurer le jeu de transformations IKEv1, sélectionnez la **crypto** commande de **transform-set de l'ipsec ikev1** :

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

Configurez un crypto map et appliquez-le à une interface

Un crypto map définit une stratégie IPSec à négocier à IPSec SA et l'inclut :

- Une liste d'accès afin d'identifier les paquets que la connexion d'IPSec permet et protège

- Identification de pair
- Une adresse locale pour le trafic d'IPSec
- Les jeux de transformations IKEv1

Voici un exemple :

```
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
```

Vous pouvez alors appliquer le crypto map à l'interface :

```
crypto map MAP interface outside
```

Configuration finale ASA

Voici la configuration finale sur l'ASA :

```
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
```

Configuration ISE

Configurez l'adresse IP sur ISE

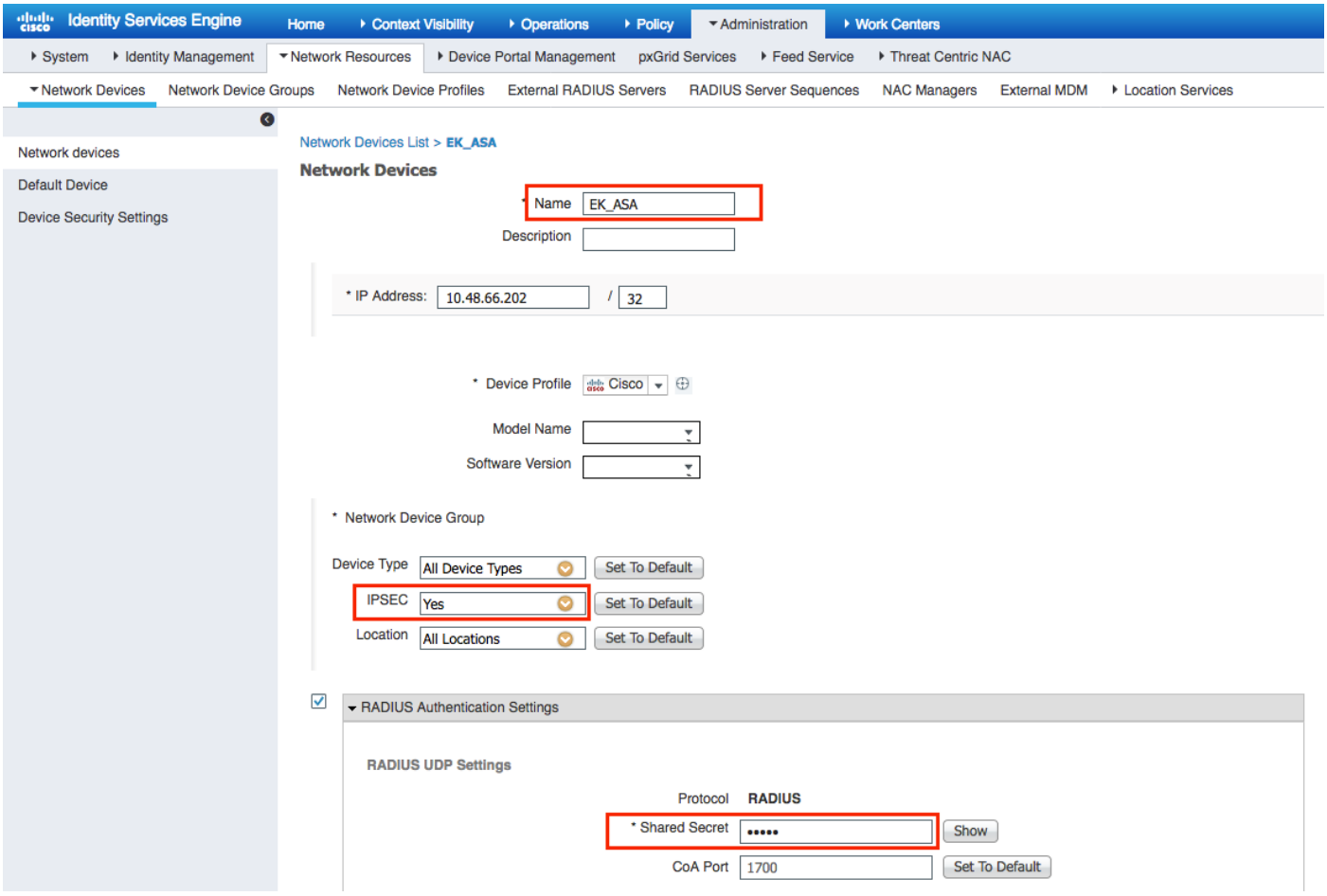
L'adresse devrait être configurée sur l'interface GE1-GE5 du CLI, GE0 n'est pas prise en charge.

```
interface GigabitEthernet 1
 ip address 10.48.26.170 255.255.255.0
 ipv6 address autoconfig
 ipv6 enable
```

> **Remarque:** Des reprises d'application après l'adresse IP est configurées sur l'interface :
> % changeant l'adresse IP pourraient faire redémarrer des services ISE
> Continuez la modification d'adresse IP ? Y/N [N] : Y

Ajoutez le NAD au groupe IPSec sur ISE

Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau**. Cliquez sur **ajoutent** en fonction. Assurez que vous configurez le nom, adresse IP, secret partagé. Pour terminer le tunnel d'IPSec de l'**OUI** choisi NAD contre le groupe de périphériques réseau IPSEC.

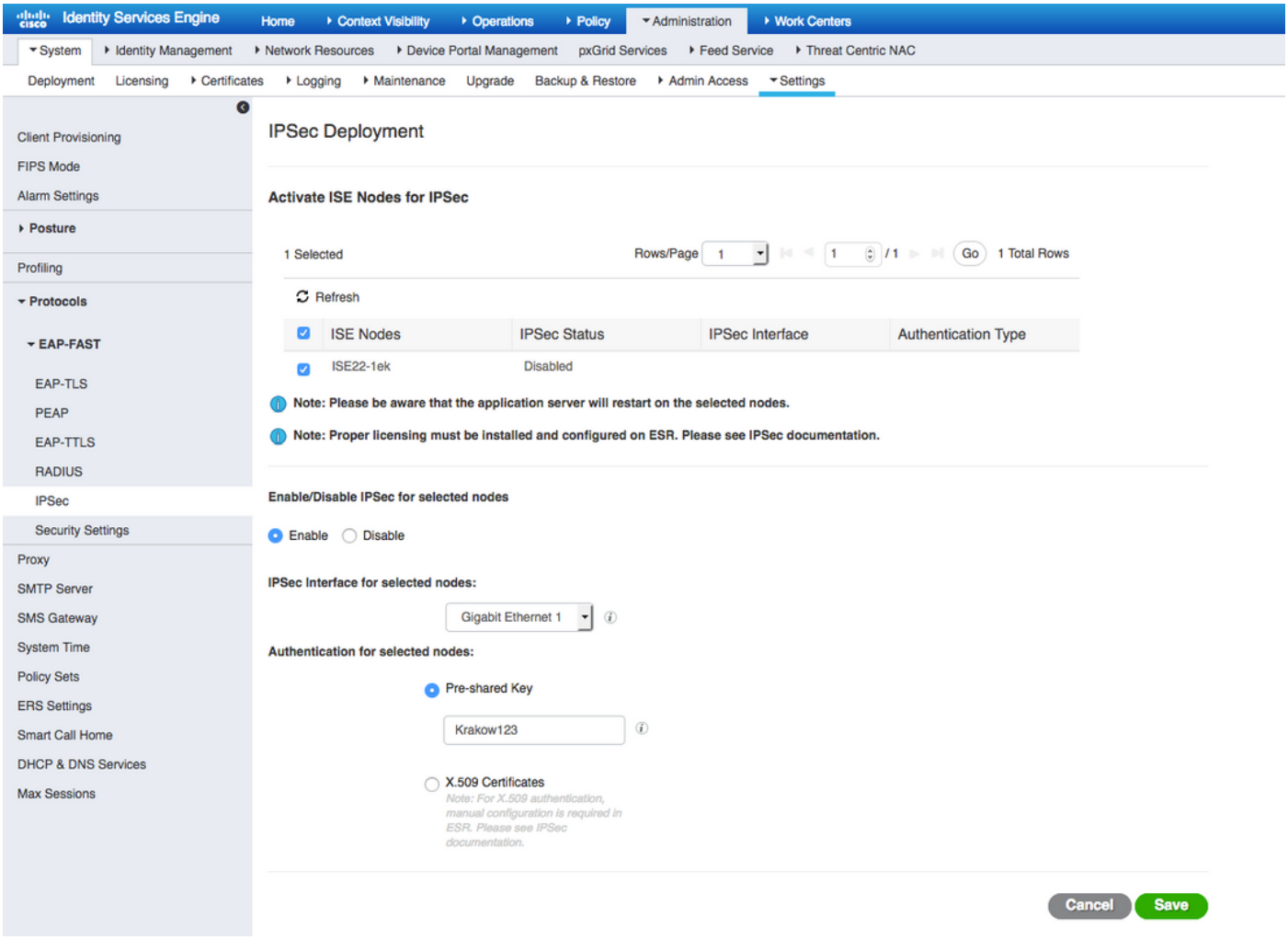


Une fois que le NAD est ajouté, l'artère supplémentaire devrait être créée sur ISE, pour s'assurer que le trafic de RAYON passe par l'ESR et obtient chiffré :

```
ip route 10.48.66.202 255.255.255.255 gateway 10.1.1.1
```

Enable IPSEC sur ISE

Naviguez vers la **gestion > le système > les configurations**. Cliquez sur en fonction le **rayon** et le furhter sur **IPSEC**. L'option choisie choisie d'enable RPC (simple/multiple/tous), sélectionnent l'interface et sélectionnent la méthode d'authentification. Cliquez sur **Save**. Reprise de services sur le noeud sélectionné en ce moment.



Note, cela après que la configuration de la reprise ISE CLI de services affiche l'interface configurée sans adresse IP et dans l'état d'arrêt, il est prévu pendant qu'ESR (routeur encastré de services) prend le contrôle de l'interface ISE.

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

Une fois que des services sont redémarrés, la fonctionnalité ESR est activée. Pour ouvrir une session à l'ESR tapez l'esr dans la ligne de commande :

```
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#
```

L'ESR est propose la crypto configuration suivante :

```
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
```

En raison de l'ASA ne prend en charge pas l'algorith du hachage sha256, la configuration supplémentaire est exigée sur l'ESR pour apparier les stratégies IKEv1 pour la 1ère et 2ème phase d'IPSEC. Configurez la stratégie et le jeu de transformations d'ISAKMP, pour apparier ceux configurés sur l'ASA :

```
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
```

Assurez-vous que l'ESR a une artère pour envoyer les paquets chiffrés :

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

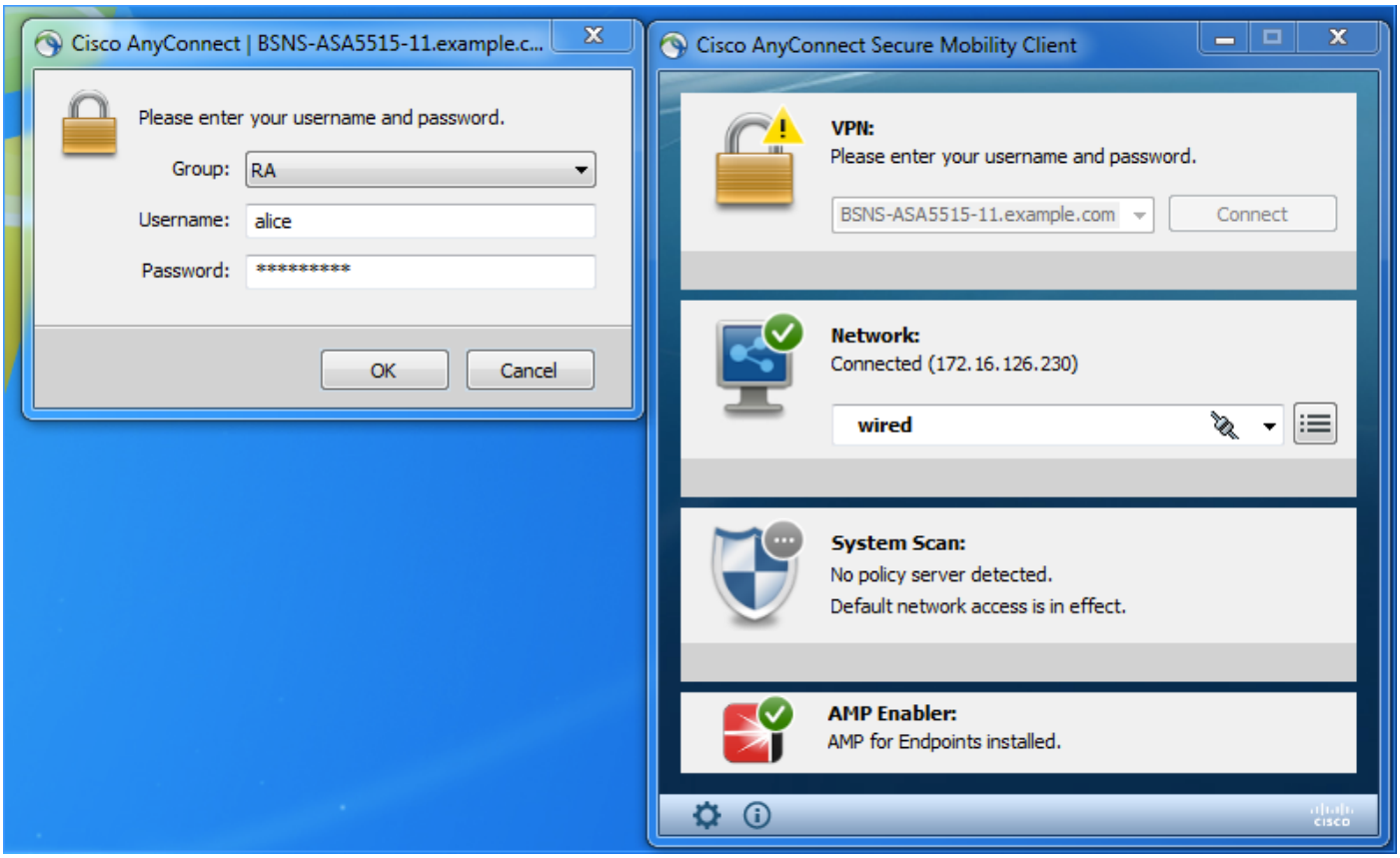
Vérifiez

ASA

Avant que les clients d'Anyconnect se connectent, l'ASA n'a aucune crypto session :

```
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#
```

Le client se connecte par l'intermédiaire du client d'Anyconnect VPN, car une source ISE 2.2 d'authentification est utilisée.



L'ASA envoie un paquet RADIUS, qui déclenche l'établissement de session VPN, une fois que le tunnel est vers le haut de la sortie suivante est vu sur l'ASA et il confirme que la phase 1 du tunnel est en hausse :

```
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#
```

Le Phase 2 est en hausse, et des paquets sont chiffrés et déchiffrés :

```
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

Les mêmes sorties peuvent être vérifiées l'ESR, la phase une est en hausse :

```
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#
```

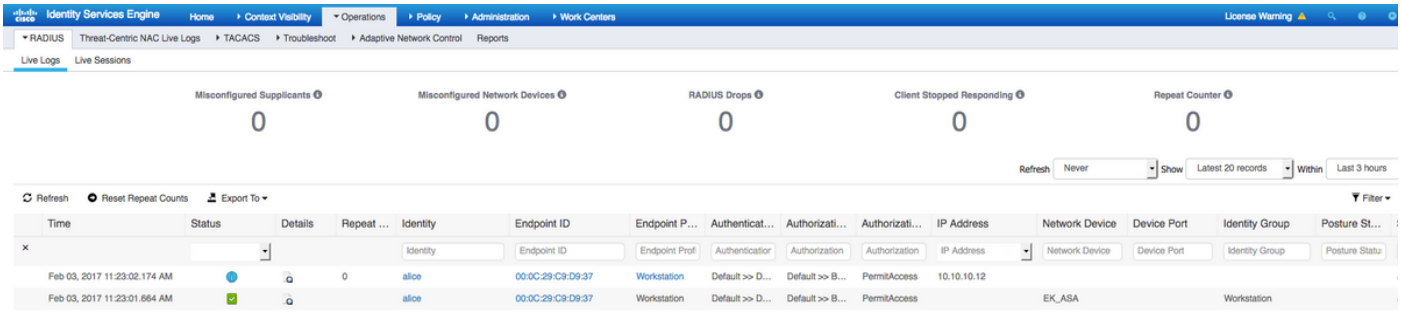
Le Phase 2 est en hausse, des paquets sont chiffrés et déchiffrés avec succès :

```
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
```

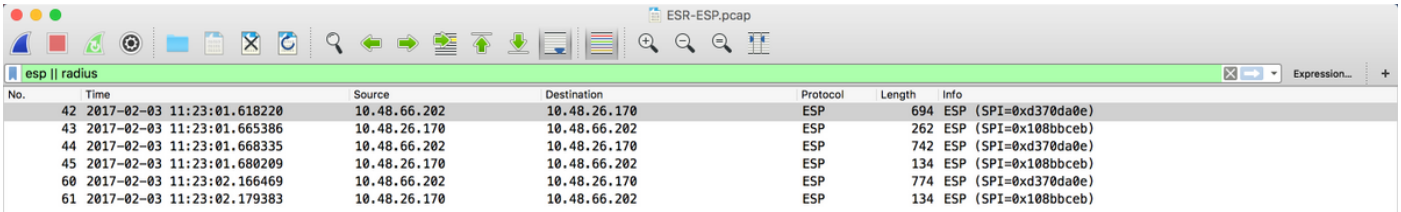
```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

 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

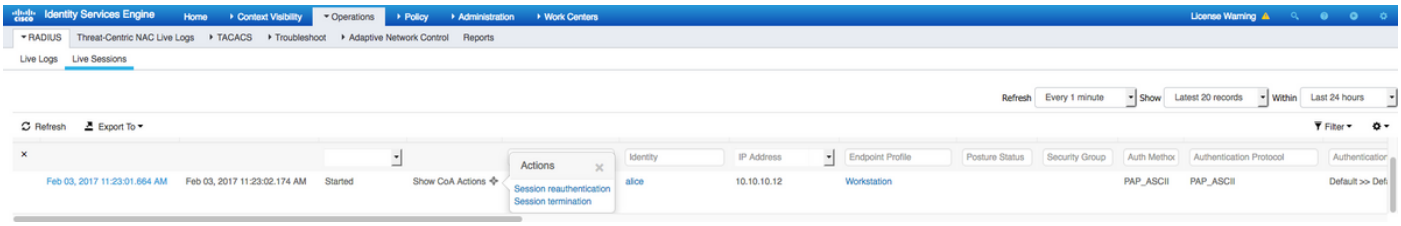
L'authentification vivante indique l'authentification régulière PAP_ASCII :



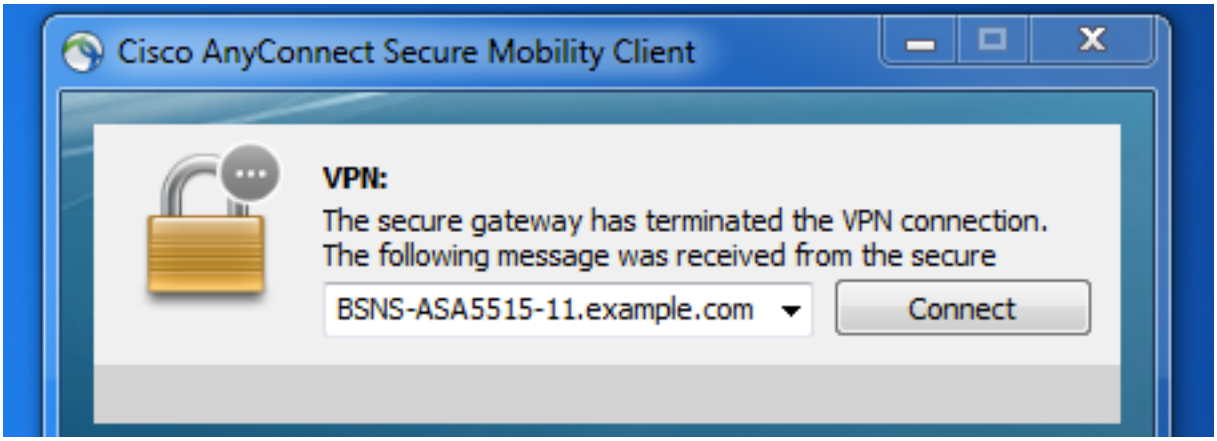
Les captures prises sur l'interface GE1 d'ISE et filtrées avec l'ESP ou le rayon, confirment qu'il n'y a aucun rayon en texte clair, et tout le trafic est chiffré :



Il est également possible d'envoyer les paquets chiffrés d'ISE - modification de l'autorisation (CoA) - une fois que le tunnel est en service :



En cet exemple de session l'arrêt a été émis, et le client vpn a obtenu déconnecté en conséquence :



Dépannez

La technique commune de dépannage VPN peut être appliquée pour dépanner le problème lié à IPSEC. Vous pouvez trouver les documents utiles ci-dessous :

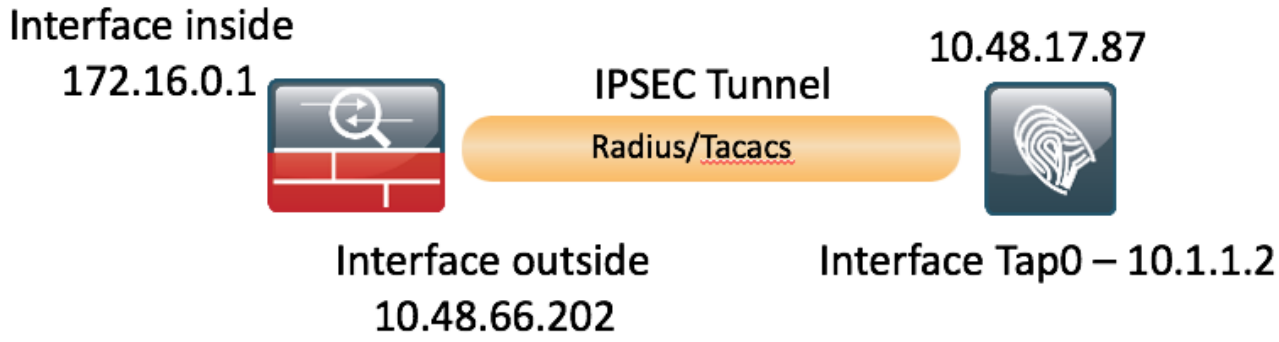
Debugs IOS IKEv2 pour le site à site VPN avec PSKs dépannant TechNote

Debugs ASA IKEv2 pour le site à site VPN avec PSKs

Dépannage IPsec : Présentation et utilisation des commandes de débogage

Configurez le site à site de FlexVPN (DVTI au crypto map) entre NAD et ISE 2.2

Il est également possible de protéger le trafic de RAYON avec FlexVPN. La topologie suivante est utilisée dans l'exemple ci-dessous :



La configuration de FlexVPN est simple. Plus de détails peuvent être trouvés ici :

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

Configuration ASA

```
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 *****
```

Configuration ESR sur 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
```

Considérations de conception de FlexVPN

- Le tunnel VPN est établi utilisant DVTI de côté ESR et le crypto map du côté ASA, avec la configuration au-dessus de l'ASA peut générer le paquet RADIUS provenu de l'interface interne, qui assurera la liste d'accès correcte pour que le cryptage déclenche l'établissement de session VPN.
- La note, cette dans ce cas ASA NAD devrait être définie sur ISE avec l'IP address d'interface interne.