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

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
Architecture ISE IPSec
Configurer
Diagramme du réseau
Configuration ASA
Configurez les interfaces ASA
Configurez la stratégie IKEv1 et activez IKEv1 sur l'interface extérieure
Configurez le groupe de tunnel (le profil de connexion entre réseaux locaux)
Configurez l'ACL pour le trafic VPN d'intérêt
Configurez le jeu de transformations IKEv1
Configurez un crypto map et appliquez-le à une interface
Configuration finale ASA
Configuration ISE
Configurez l'adresse IP sur ISE
Ajoutez le NAD au groupe IPSec sur ISE
Enable IPSEC sur ISE
Vérifier
ASA
ESR
ISE
Dépanner
Configurez le site à site de FlexVPN (DVTI au crypto map) entre NAD et ISE 2.2
Configuration ASA
Configuration ESR sur ISE
Considérations de conception de FlexVPN

Introduction

Ce document décrit comment configurer et dépanner RADIUS 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 RADIUS 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

Exigences

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

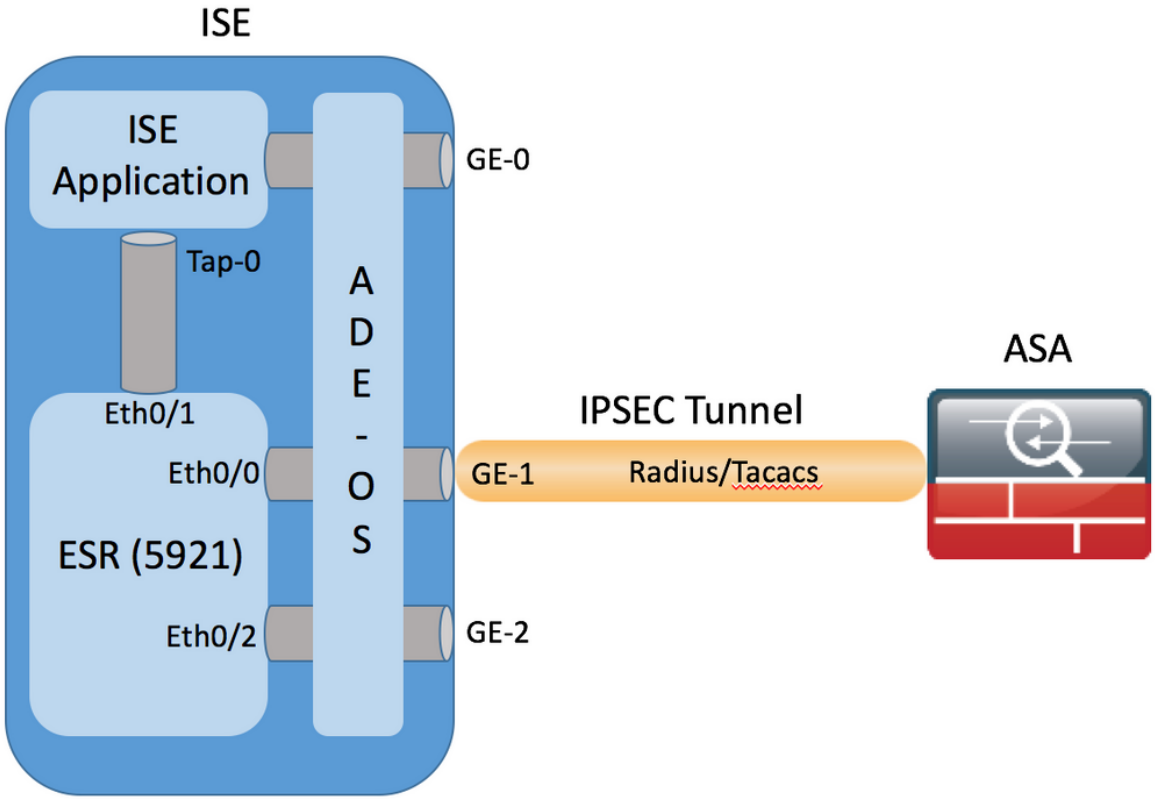
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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

Informations générales

L'objectif est aux protocoles sécurisés qui utilisent les informations parasites non sécurisées, le Radius 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 :

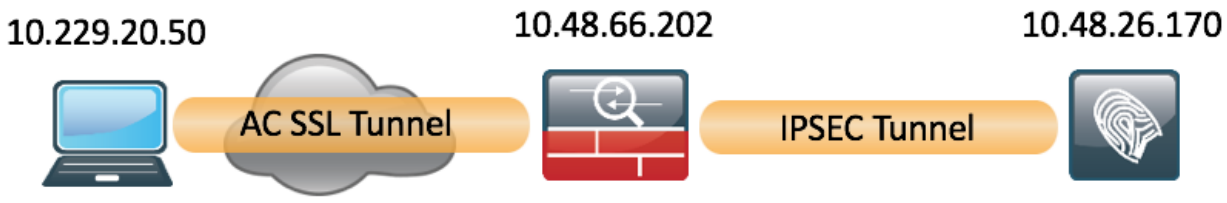
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)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

Configurer

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* :

```
crypto ikev1 enable outside
```

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

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 :

```
crypto map MAP interface outside
```

Configuration ISE

Configurez l'adresse IP sur ISE

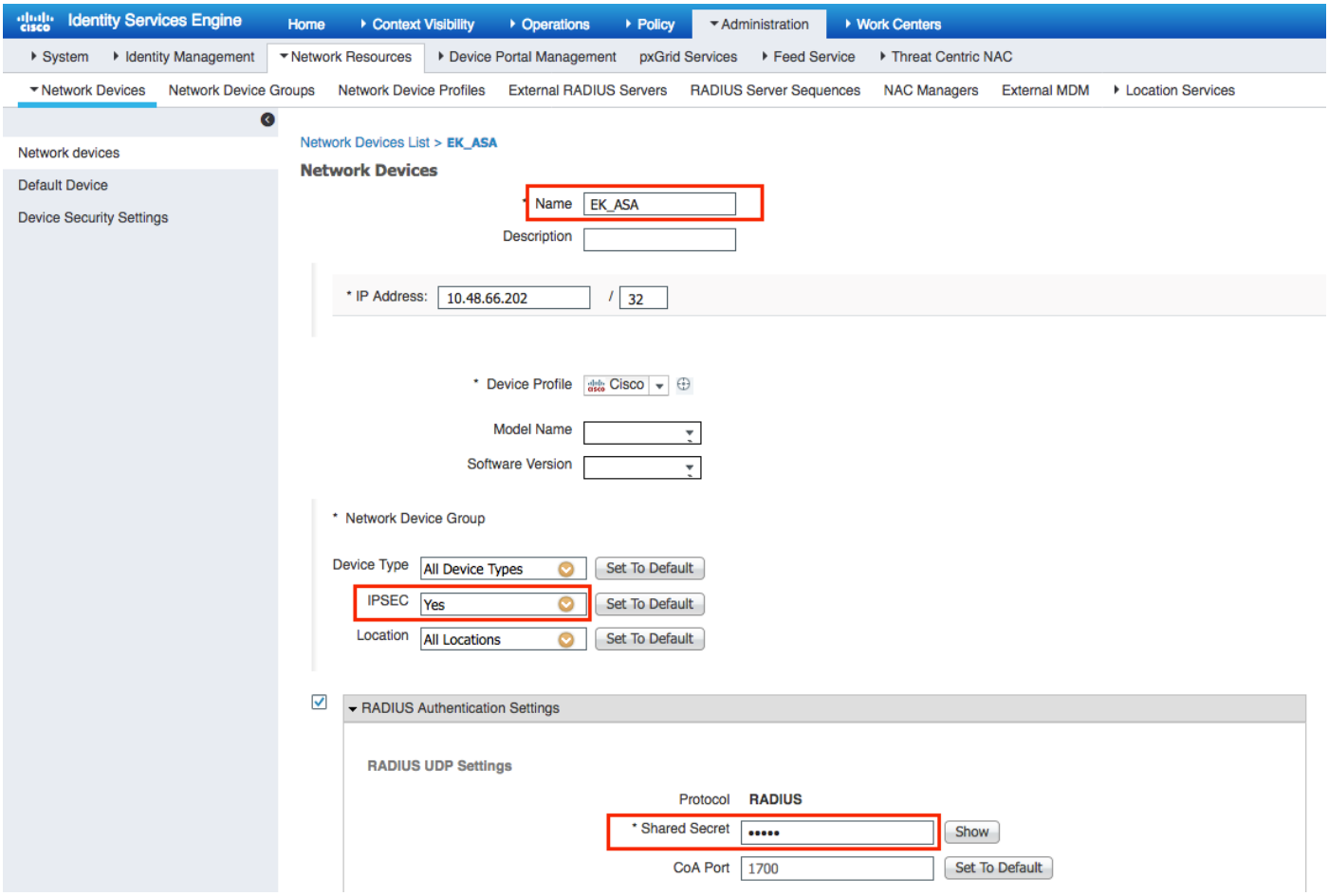
L'adresse devrait être configurée sur l'interface GE1-GE5 du CLI, GE0 n'est pas prise en charge.

```
crypto map MAP interface outside
```

> **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] : O

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.

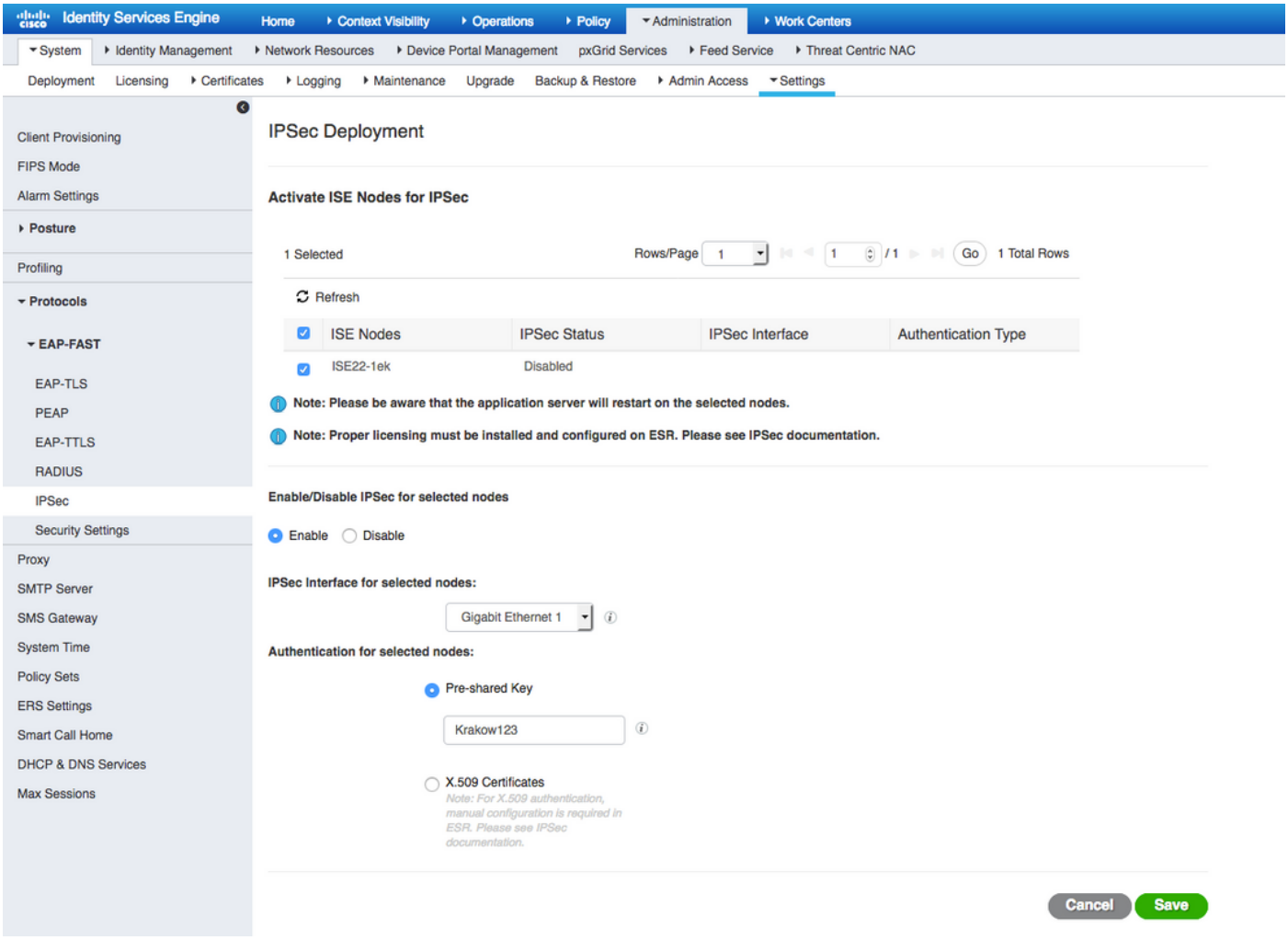


Une fois que le NAD est ajouté, l'artère supplémentaire devrait être créée sur ISE, pour s'assurer que le trafic de RADIUS passe par l'ESR et obtient chiffré :

```
crypto map MAP interface outside
```

Enable IPSEC sur ISE

Naviguez vers la **gestion > le système > les configurations**. Cliquez sur en fonction **Radius** 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.

```
crypto map MAP interface outside
```

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 :

```
crypto map MAP interface outside
```

L'ESR est propose la crypto configuration suivante :

```
crypto map MAP interface outside
```

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 map MAP interface outside
```

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

```
crypto map MAP interface outside
```

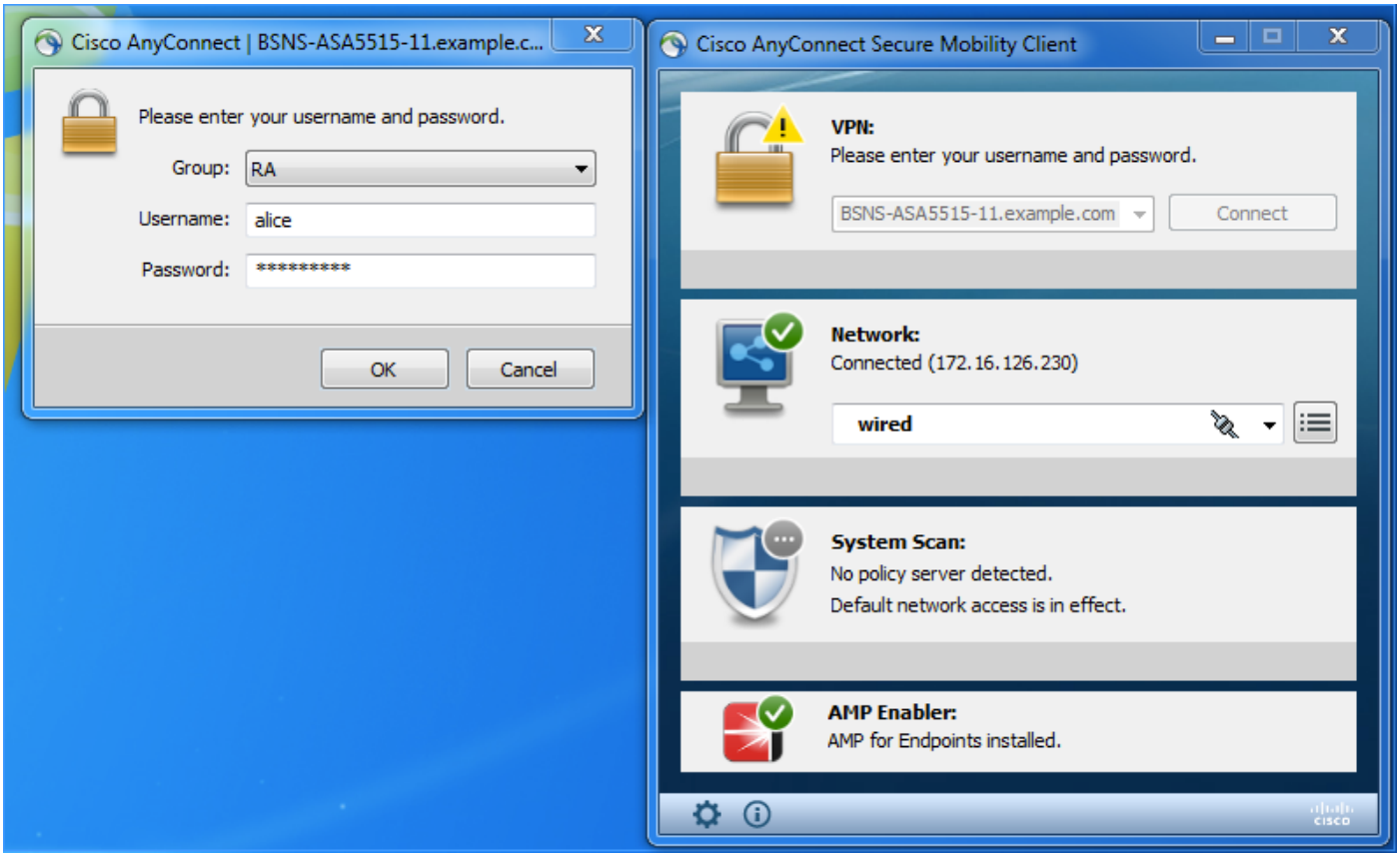
Vérifiez

ASA

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

```
crypto map MAP interface outside
```

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 :

```
crypto map MAP interface outside
```

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

```
crypto map MAP interface outside
```

ESR

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

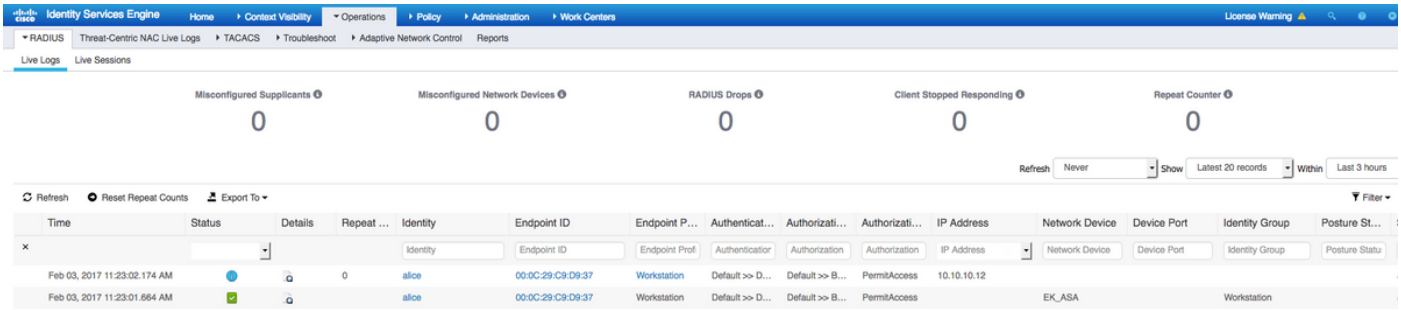
```
crypto map MAP interface outside
```

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

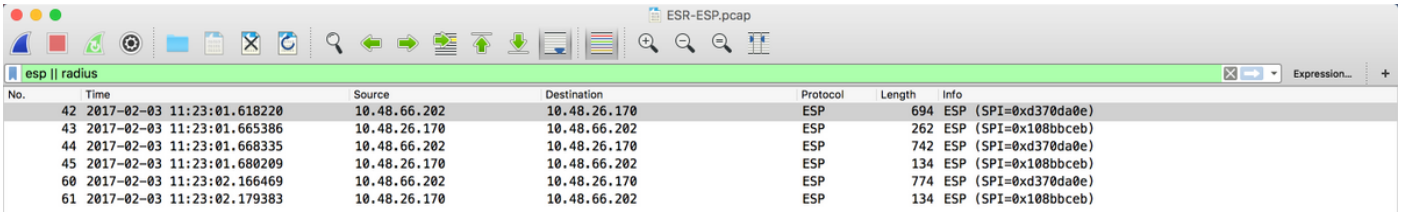
```
crypto map MAP interface outside
```

ISE

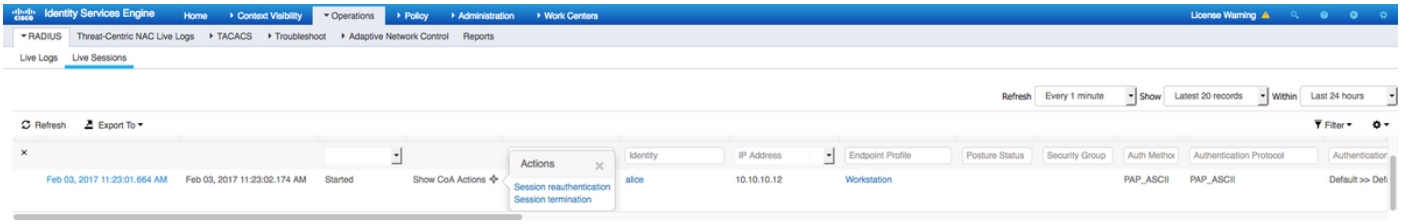
L'authentification vivante indique l'authentification régulière PAP_ASCII :



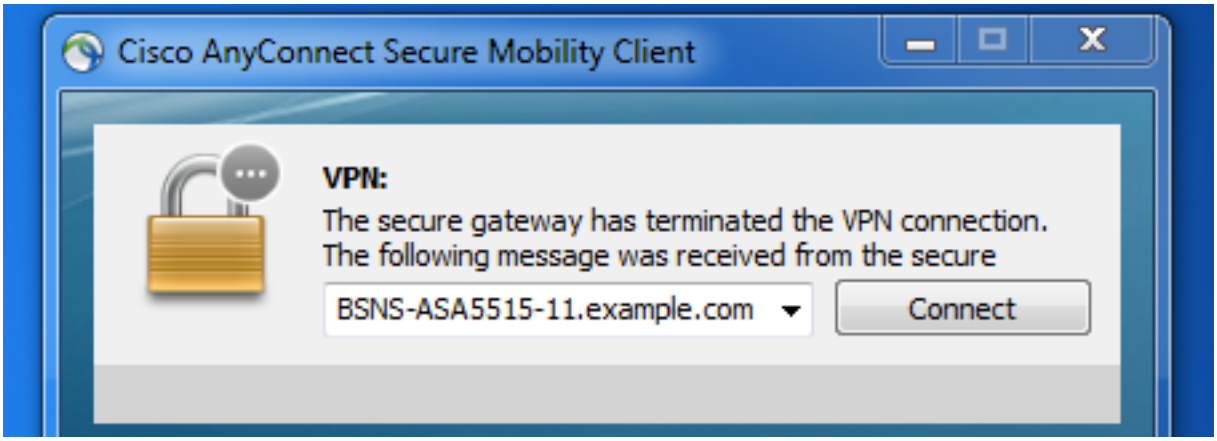
Les captures prises sur l'interface GE1 d'ISE et filtrées avec l'ESP ou le Radius, confirment qu'il n'y a aucun Radius en texte clair, et tout le trafic est chiffré :



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 :



Dépanner

La technique commune de dépannage VPN peut être appliquée pour dépanner le problème lié à

IPSEC. Vous pouvez trouver les documents utiles ci-dessous :

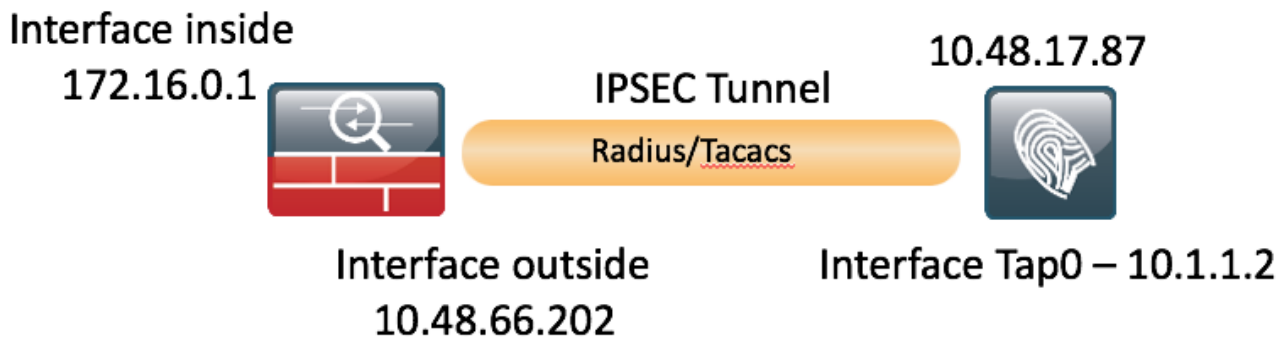
Debugs IOS IKEv2 pour le site à site VPN avec PSKs dépannant TechNote

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 RADIUS 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

```
crypto map MAP interface outside
```

Configuration ESR sur ISE

```
crypto map MAP interface outside
```

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.