IPSEC de la configuración ISE 2.2 para asegurar la comunicación NAD (ASA)

Contenido

Introducción

Este documento describe cómo configurar y resolver problemas el IPSEC RADIUS para asegurar el motor del servicio de la identidad de Cisco (ISE) 2.2 - comunicación del dispositivo de acceso a la red (NAD). El tráfico de RADIUS se debe cifrar dentro de la versión 1 del intercambio de claves de Internet del IPSec del sitio a localizar (LAN a LAN) y (IKEv1 e IKEv2) del túnel 2 entre el dispositivo de seguridad adaptante (ASA) y el ISE. Este documento no cubre la partición de la configuración VPN de AnyConnect SSL.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Cisco ASA
- Conceptos generales del IPSec
- Conceptos generales RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5515-X Series ASA que funcionan con la versión de software 9.4(2)11
- Versión 2.2 del motor del servicio de la identidad de Cisco
- Service Pack 1 de Windows 7

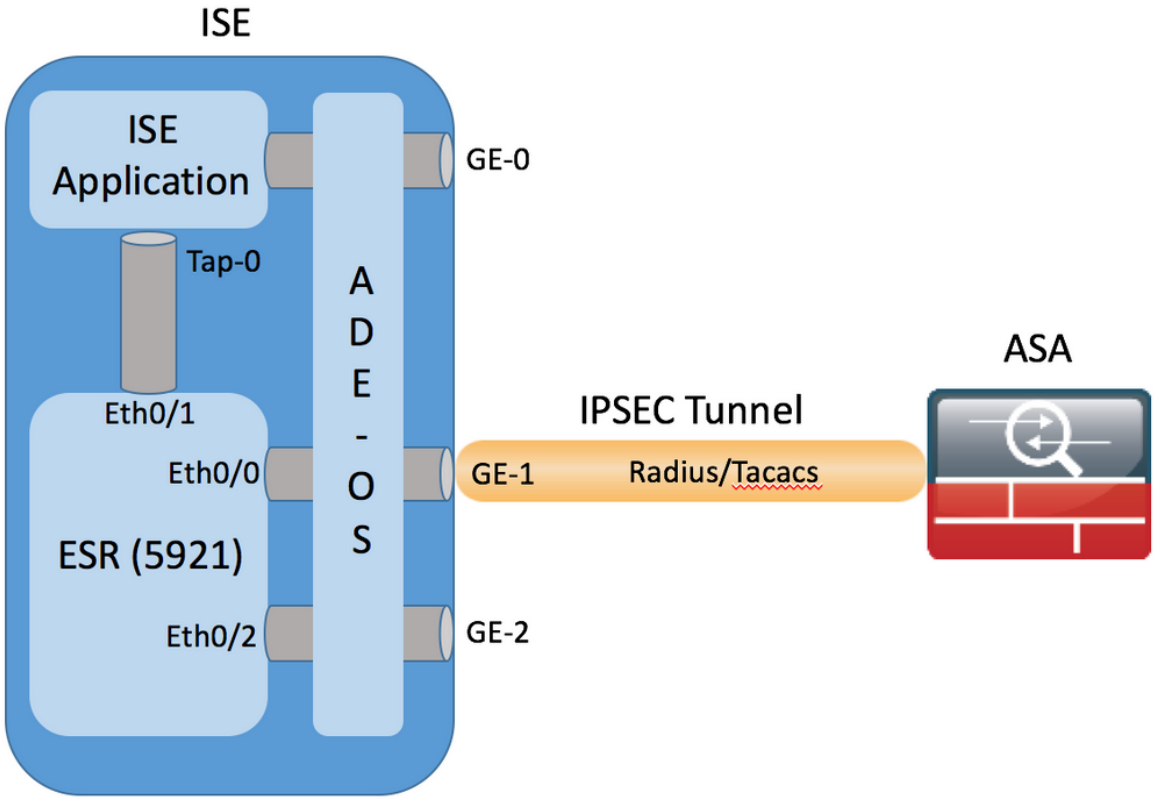
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El objetivo es asegurar los protocolos que utilizan el hash MD5, el radio y el TACACS inseguros con el IPSec. Tome esto en la consideración:

- Cisco ISE soporta el IPSec en los modos del túnel y de transporte.
- Cuando usted habilita el IPSec en una interfaz de Cisco ISE, un túnel IPsec se crea entre Cisco ISE y el NAD para asegurar la comunicación.
- Usted puede definir una clave previamente compartida o utilizar los Certificados X.509 para la Autenticación IPSec.
- El IPSec se puede habilitar en el eth1 a través de las interfaces Eth5. Usted puede configurar el IPSec en solamente una interfaz de Cisco ISE por el PSN.

Arquitectura del IPSec ISE



Una vez que los paquetes encriptados son recibidos por la interfaz ESR GE-1 ISE los interceptan en la interfaz 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
```

El ESR los desencripta y según el NAT preconfigurado las reglas realizan la traducción de la dirección. (Hacia el NAD) los paquetes salientes RADIUS/TACACS se traducen al direccionamiento de la interfaz del Ethernet0/0 y se cifran luego.

```
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
```

Los paquetes que se destinan a la interfaz Eth0/0 en los puertos RADIUS/TACACS se deben forwared vía la interfaz Eth0/1 a la dirección IP 10.1.1.2, que es dirección interna del ISE.
Configuración ESR de 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
```

Configuración ISE de la interfaz interna Tap-0:

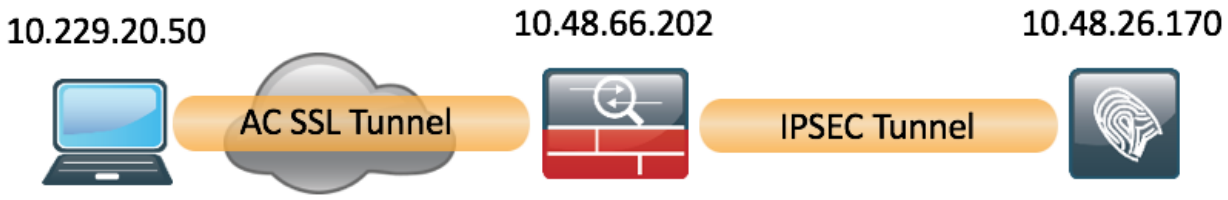
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)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

Configurar

Esta sección describe cómo completar las configuraciones ASA CLI y ISE.

Diagrama de la red

La información en este documento utiliza esta configuración de la red:



Configuración ASA

Configure las interfaces ASA

Si la interfaz/las interfaces ASA no se configura, asegúrese de que usted configure por lo menos la dirección IP, interconecte el nombre, y el nivel de seguridad:

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

Configure la directiva IKEv1 y habilite IKEv1 en la interfaz exterior

Para configurar las directivas del Internet Security Association and Key Management Protocol (ISAKMP) para las conexiones IKEv1, ingrese el comando **crypto del <priority> de la directiva ikev1**:

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

> **Nota:** Una coincidencia de la directiva IKEv1 existe cuando ambas directivas de los dos pares contienen la misma autenticación, cifrado, hash, y Valores de parámetro de Diffie Hellman. Para IKEv1, la directiva del peer remoto debe también especificar un curso de la vida inferior o igual el curso de la vida en la directiva que el iniciador envía. Si los cursos de la vida no son idénticos, después el ASA utiliza el curso de la vida más corto.

Usted debe habilitar IKEv1 en la interfaz que termina el túnel VPN. Típicamente, ésta es la interfaz del exterior (o *público*). Para habilitar IKEv1, ingrese el **ikev1 crypto habilitan <interface name> el** comando en el modo de configuración global:

```
crypto ikev1 enable outside
```

Configure el grupo de túnel (el perfil de la conexión de LAN a LAN)

Para un túnel de LAN a LAN, el tipo del perfil de la conexión es **ipsec-l2l**. Para configurar la clave del preshared IKEv1, ingrese al modo de configuración de los IPSec-*atributos del grupo de túnel*:

```
crypto ikev1 enable outside
```

Configure el ACL para el tráfico VPN del interés

El ASA utiliza el Listas de control de acceso (ACL) para distinguir el tráfico que se debe proteger con la encripción de IPSec contra el tráfico que no requiere la protección. Protege los paquetes salientes que hacen juego un motor del control de la aplicación del permiso (ACE) y se asegura de que los paquetes de entrada que hacen juego un permiso ACE tenga protección.

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

> **Nota:** Un ACL para el tráfico VPN utiliza los IP Address de origen y de destino después del Network Address Translation (NAT). El único tráfico cifrado en este caso es tráfico entre el ASA y el ISE.

Configure el IKEv1 transforman el conjunto

Un IKEv1 transforma el conjunto es una combinación de protocolos de Seguridad y los algoritmos que define la manera que el ASA protege los datos. Durante las negociaciones de la asociación de seguridad IPSec (SA), los pares deben identificar una transformación fijada o la oferta que sean lo mismo para ambos pares. El ASA entonces aplica correspondido con transforma el conjunto o la oferta para crear un SA que proteja los flujos de datos en la lista de acceso para esa correspondencia de criptografía.

Para configurar el IKEv1 transforme el conjunto, ingresan el comando **crypto del transforme el conjunto del IPSec ikev1**:

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

Configure una correspondencia de criptografía y apliqúela a una interfaz

Una correspondencia de criptografía define una política IPSec que se negociará en IPSec SA y la incluye:

- Una lista de acceso para identificar los paquetes que conexión IPSec los permisos y protege
- Identificación del par

- Una dirección local para el tráfico IPSec
- Los IKEv1 transforman los conjuntos

Aquí tiene un ejemplo:

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

Usted puede entonces aplicar la correspondencia de criptografía a la interfaz:

```
crypto map MAP interface outside
```

Configuración final ASA

Aquí está la configuración final en el ASA:

```
crypto map MAP interface outside
```

Configuración ISE

Dirección IP de la configuración en el ISE

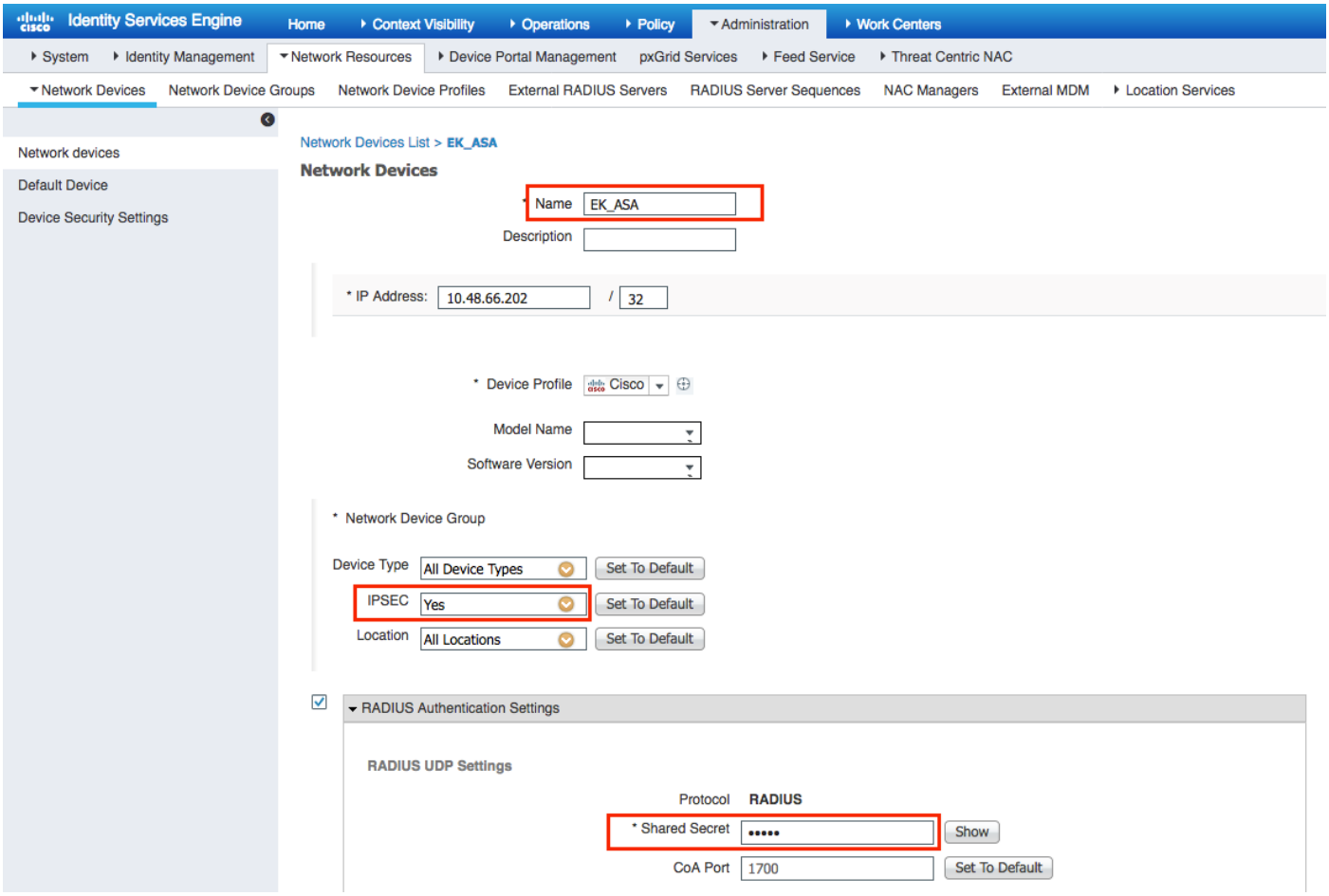
El direccionamiento se debe configurar en el GE1-GE5 de la interfaz del CLI, GE0 no se soporta.

```
crypto map MAP interface outside
```

> **Nota:** La aplicación recomienza después de que la dirección IP se configure en la interfaz:
> % que cambiaban la dirección IP pudieron hacer los servicios ISE recomenzar
> ¿Continúe con el cambio de la dirección IP? Y/N [n]: S

Agregue el NAD al grupo IPSec en el ISE

Navegue a la **administración > a los recursos de red > a los dispositivos de red**. Haga clic en **agregan**. Asegúrele la configuración el nombre, dirección IP, secreto compartido. Para terminar el túnel IPsec del NAD seleccione los **YE** contra el grupo de dispositivos de la red IPsec.

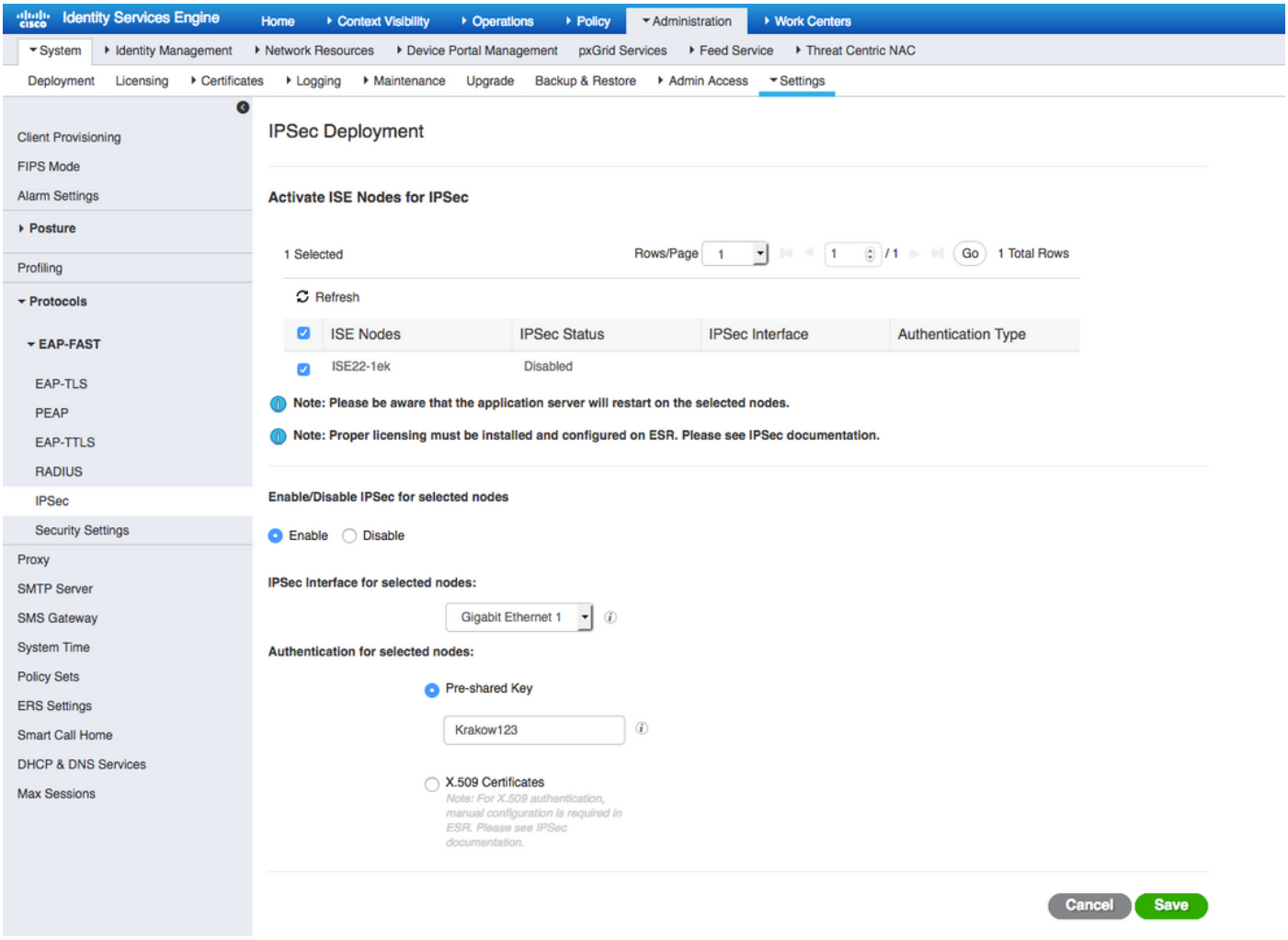


Una vez que se agrega el NAD, la ruta adicional se debe crear en el ISE, para asegurarse de que el tráfico de RADIUS pasa con el ESR y consigue cifrado:

```
crypto map MAP interface outside
```

IPSEC del permiso en el ISE

Navegue a la **administración > al sistema > a las configuraciones**. Haga clic en el **radio** y el furhter en el **IPSEC**. Seleccione la opción selecta del permiso PSN (solo/múltiplo/todo), escoja la interfaz y seleccione el método de autentificación. Haga clic en Save (Guardar). Los servicios recomienzan en el nodo seleccionado en este momento.



Observe, eso después de que la configuración CLI del reinicio ISE de los servicios muestre la interfaz configurada sin el IP Address y en el estado de cierre normal, él se espera como el ESR (router integrado de los servicios) toma el control de la interfaz ISE.

```
crypto map MAP interface outside
```

Una vez que recomienzan a los servicios, se habilitan las funciones ESR. Para iniciar sesión al ESR teclee el esr en la línea de comando:

```
crypto map MAP interface outside
```

El ESR es sube con la configuración de criptografía siguiente:

```
crypto map MAP interface outside
```

Debido al ASA no soporta el algorith del picado sha256, la configuración adicional se requiere en el ESR hacer juego las directivas IKEv1 para la 1ra y 2da fase de IPSEC. Configure la política isakmp y transforme el conjunto, para hacer juego ésos configurados en el ASA:

```
crypto map MAP interface outside
```

Aseegurese el ESR tiene una ruta para mandar los paquetes encriptados:

```
crypto map MAP interface outside
```

Verificación

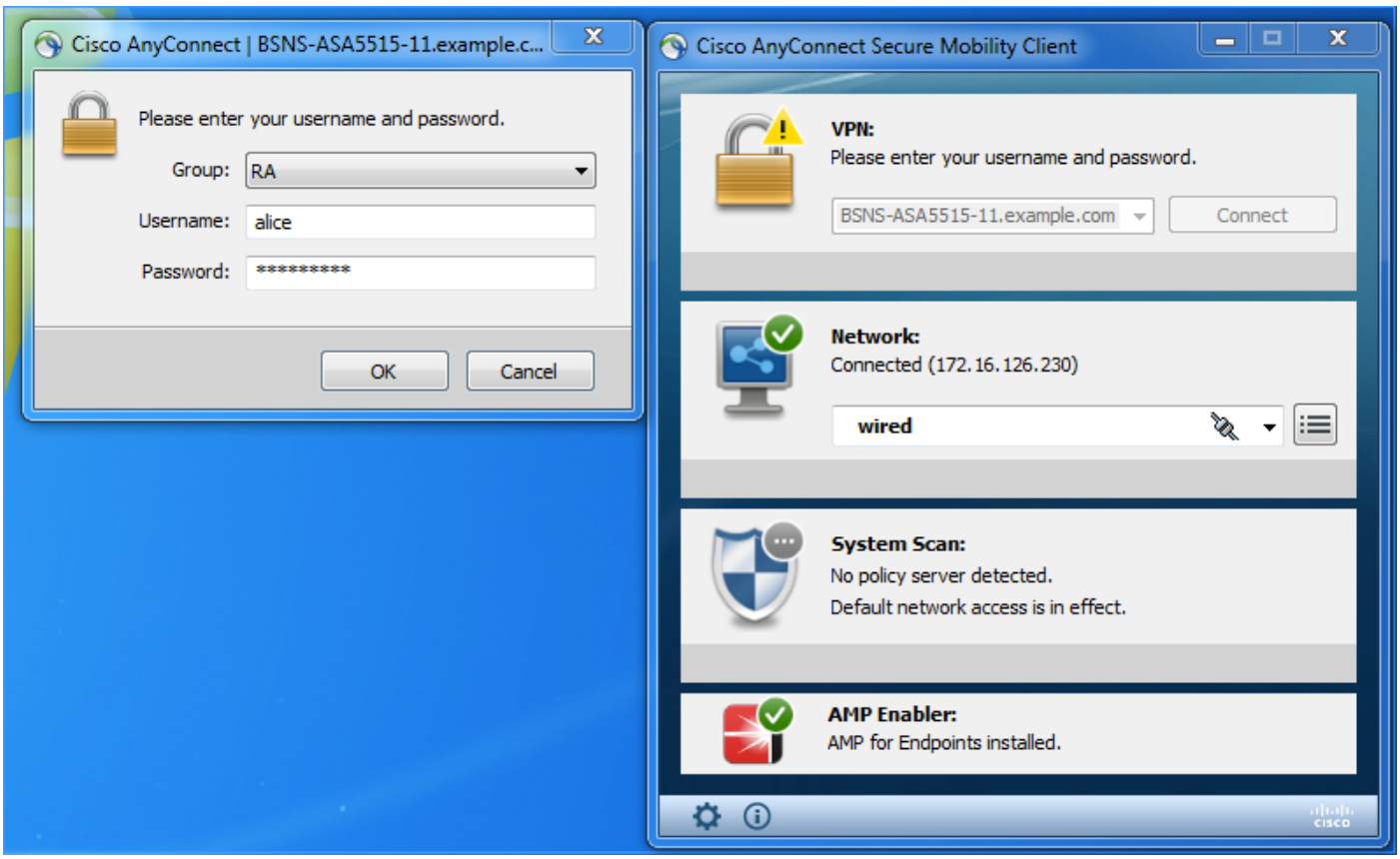
ASA

Antes de que los clientes de Anyconnect conecten, el ASA no tiene ninguna sesión de

criptografía:

```
crypto map MAP interface outside
```

El cliente conecta vía el cliente VPN de Anyconnect, pues se utiliza una fuente ISE 2.2 de la autenticación.



El ASA envía un paquete RADIUS, que acciona el establecimiento de la sesión de VPN, una vez que el túnel está encima del producto siguiente se ve en el ASA y confirma que la fase 1 del túnel está para arriba:

```
crypto map MAP interface outside
```

La fase 2 está para arriba, y se cifran y se desencriptan los paquetes:

```
crypto map MAP interface outside
```

ESR

Las mismas salidas se pueden comprobar el ESR, fase uno están para arriba:

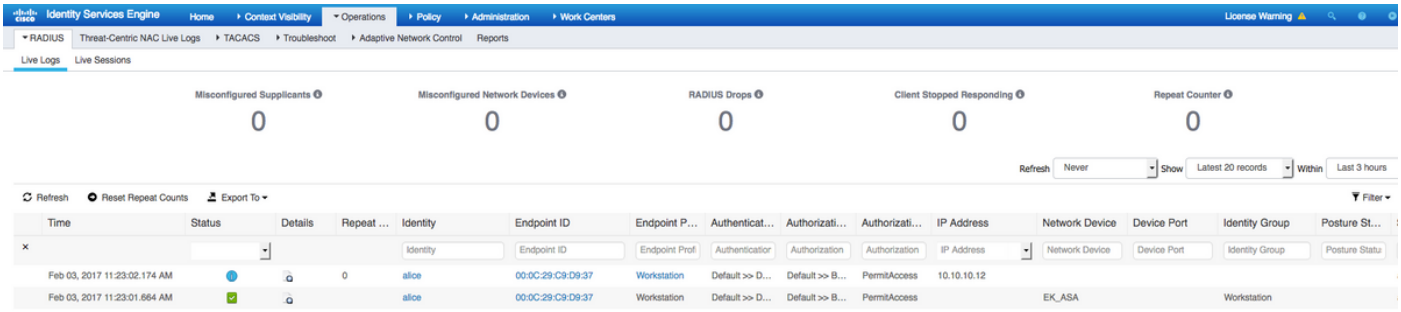
```
crypto map MAP interface outside
```

La fase 2 está para arriba, los paquetes se cifran y se desencriptan con éxito:

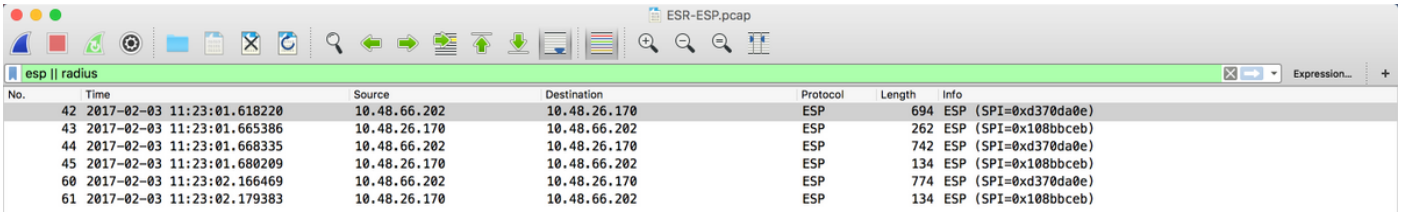
```
crypto map MAP interface outside
```

ISE

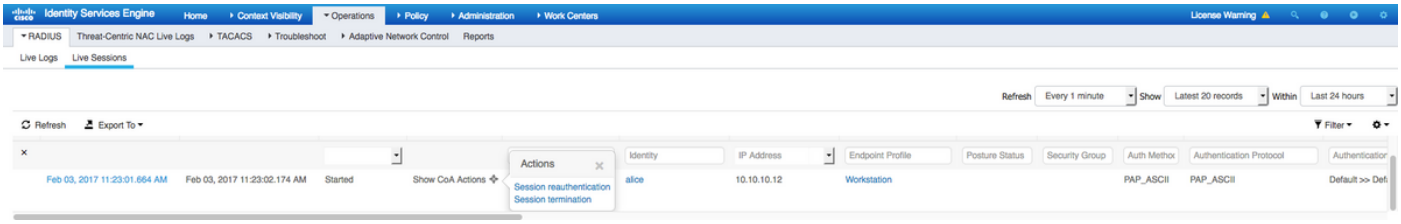
La autenticación viva indica la autenticación regular PAP_ASCII:



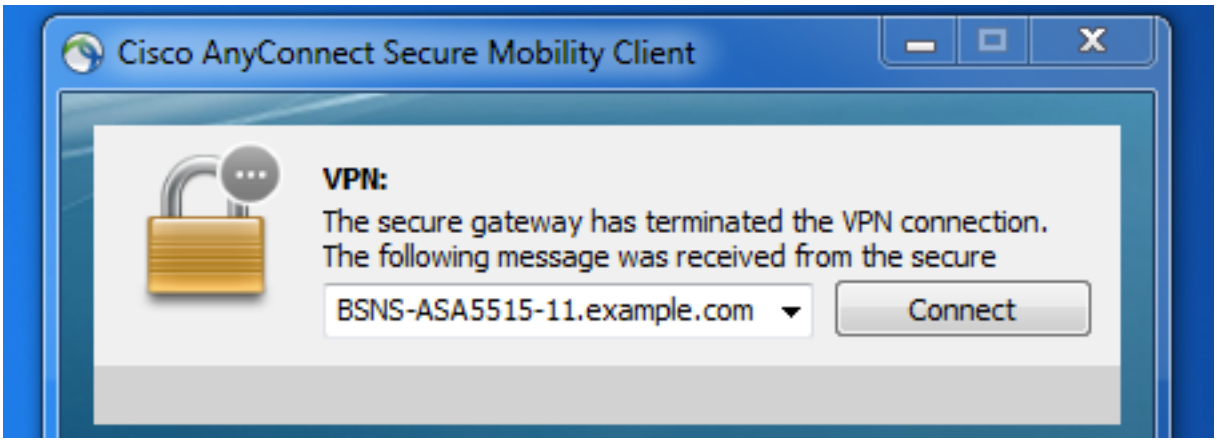
Las capturas adquiridas la interfaz GE1 del ISE y filtradas con el ESP o el radio, confirman que no hay radio en el texto claro, y se cifra todo el tráfico:



Es también posible enviar los paquetes encriptados del ISE - cambio de la autorización (CoA) - una vez que el túnel es en servicio:



En esta sesión de ejemplo la terminación fue publicada, y el cliente VPN consiguió disconnected como consecuencia:



Troubleshooting

Las técnicas de Troubleshooting comunes VPN se pueden aplicar para resolver problemas los problemas relacionados con el IPSEC. Usted puede encontrar los documentos útiles abajo:

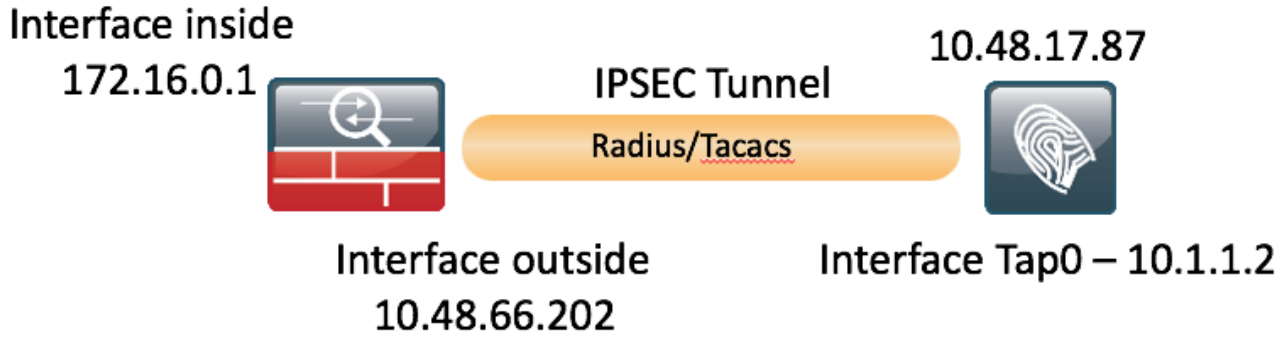
Debugs IOS IKEv2 para el VPN de sitio a sitio con la Nota Técnica del troubleshooting de PSKs

Debugs ASA IKEv2 para el VPN de sitio a sitio con PSKs

[Troubleshooting de IPSec: Entendiendo y con los comandos debug]

Sitio a localizar de FlexVPN de la configuración (DVTI a la correspondencia de criptografía) entre NAD y ISE 2.2

Es también posible proteger el tráfico de RADIUS con FlexVPN. La topología siguiente se utiliza en el ejemplo abajo:



La configuración de FlexVPN es directa. Más detalles se pueden encontrar aquí:

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

Configuración ASA

```
crypto map MAP interface outside
```

Configuración ESR en el ISE

```
crypto map MAP interface outside
```

Aspectos del diseño de FlexVPN

- El túnel VPN se construye usando DVTI en el lado ESR y la correspondencia de criptografía en el lado ASA, con la configuración sobre el ASA puede generar el paquete RADIUS originado de la interfaz interior, que asegurará la lista de acceso correcta para que el cifrado accione el establecimiento de la sesión de VPN.
- Observe, ese en este caso ASA NAD debe ser definido en el ISE con el IP Address de la interfaz interior.