Instale y configure el módulo de la visibilidad de la red de Cisco con AnyConnect 4.2.x y Splunk

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Cliente de movilidad Cisco AnyConnect Secure
Exportación de la información de flujo del protocolo de Internet (IPFIX)
Colector IPFIX
Splunk
Topología
Configurar
Perfil del cliente de Anyconnect MNV
Perfil del cliente de la configuración MNV vía el ASDM
Configure el perfil del cliente MNV vía el editor del perfil de Anyconnect
Configure el Red-despliegue en Cisco ASA
Configure el Red-despliegue en Cisco ISE
Detección de la red de confianza
Despliegue
Paso 1. Configuración Anyconnect MNV en Cisco ASA/ISE
Paso 2. Componente del colector de la configuración IPFIX
Paso 3. Configuración Splunk con el App de Cisco MNV
Verificación
Valide la instalación de Anyconnect MNV
Valide el estado del colector como funcionamiento
Valide Splunk
Troubleshooting
Flujo de paquetes
Pasos básicos del Troubleshooting
Detección de la red de confianza (TND)
Plantillas del flujo
Versión recomendada
Defectos relacionados
Links relacionados

Introducción

Este documento describe el método para instalar y para configurar el módulo de la visibilidad de la red de Cisco AnyConnect (MNV) en un sistema del usuario final usando AnyConnect 4.2.x o

más arriba.

Cisco AnyConnect MNV se utiliza como media para el analytics de la Seguridad que despliega. La MNV autoriza las organizaciones para considerar el punto final y el comportamiento del usuario en su red, recoge los flujos de los puntos finales encendido y de la apagado-premisa junto con el contexto adicional como los usuarios, las aplicaciones, los dispositivos, las ubicaciones y los destinos.

Esta Nota Técnica es un ejemplo de configuración usando AnyConnect MNV con Splunk.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- AnyConnect 4.2.01022 o más alto con la MNV
- Licencia de AnyConnect APEX
- ASDM 7.5.1 o más alto

Componentes Utilizados

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

- Cliente 4.2 de la movilidad de la Seguridad de Cisco AnyConnect o más adelante
- Editor del perfil de Cisco AnyConnect
- Dispositivo de seguridad adaptante de Cisco (ASA), versión 9.5.2
- Cisco Adaptive Security Device Manager (ASDM), versión 7.5.1
- Empresa 6.3 de Splunk
- Ubuntu 14.04.3 LT como dispositivo del colector

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

Cliente de movilidad Cisco AnyConnect Secure

Cisco Anyconnect es un agente unificado que entrega los Servicios de seguridad múltiples para proteger la empresa. Anyconnect es el más de uso general como cliente VPN de la empresa, pero también soporta los módulos adicionales que abastecen a diversos aspectos de la Seguridad de la empresa. Los módulos adicionales habilitan las funciones de seguridad como la evaluación de la postura, la Seguridad de la red, la protección del malware, la visibilidad de la red y más.

Esta Nota Técnica está sobre el módulo de la visibilidad de la red (MNV), que integra con Cisco Anyconnect para proporcionar a los administradores la capacidad de monitorear el uso de la aplicación del punto final.

Para más información con respecto a Cisco Anyconnect, refiérase:

Guía del administrador del Cliente de movilidad Cisco AnyConnect Secure, versión 4.3

Exportación de la información de flujo del protocolo de Internet (IPFIX)

IPFIX es un protocolo IETF para definir un estándar para exportar la información de flujo IP para los diversos propósitos como las estadísticas/la auditoría/Seguridad. IPFIX se basa en NetFlow de Cisco el protocolo v9, aunque no no directamente compatible.

El vzFlow de Cisco es una especificación del protocolo ampliada sobre la base del protocolo IPFIX. IPFIX no tiene bastantes elementos de información estándar para soportar todos los parámetros se puede recoger como parte de AC MNV. El protocolo del vzFlow de Cisco amplía el IPFIX estándar y define los nuevos elementos de información así como define a un conjunto estándar de plantillas IPFIX que sean utilizadas por AC MNV para exportar los datos IPFIX.

Para más información sobre IPFIX, refiera al rfc5101, rfc7011, rfc7012, rfc7013, rfc7014, rfc7015.

Colector IPFIX

Un colector es un servidor que recibe y salva los datos IPFIX. Puede entonces alimentar estos datos a Splunk. Eg. Lancope.

Cisco también proporciona su colector de cosecha propia IPFIX.

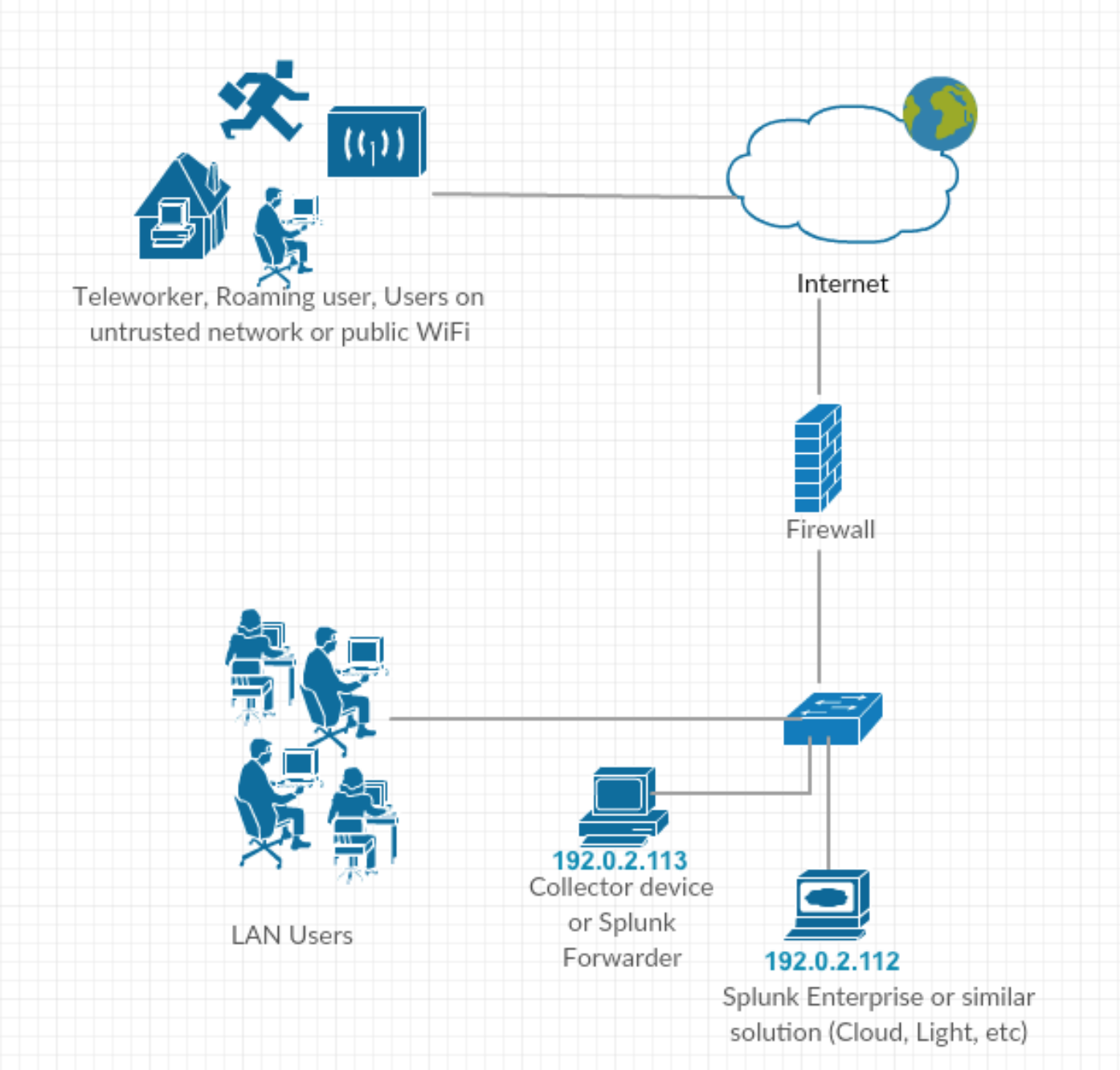
Splunk

Splunk es una herramienta potente que recoge y analiza los datos diagnósticos para dar la información significativa sobre la infraestructura informática. Proporciona una ubicación todo en uno para que los administradores recojan los datos que son cruciales en la comprensión de la salud de la red.

Splunk no es poseído ni es mantenido por Cisco Systems, no obstante Cisco proporciona el App de Cisco AnyConnect MNV para Splunk.

Para más información con respecto al arrojo, visite por favor su sitio web.

Topología



Convenios de la dirección IP en esta Nota Técnica:

Dirección IP del colector: 192.0.2.123

Dirección IP de Splunk: 192.0.2.113

Configurar

Esta sección cubre la configuración de los componentes de Cisco MNV.

Perfil del cliente de Anyconnect MNV

La configuración de Anyconnect MNV se guarda en un archivo XML que contenga la información sobre la dirección IP y el número del puerto del colector, junto con la otra información. La dirección IP y el número del puerto del colector necesitan ser configurados correctamente en el perfil del cliente MNV.

Para la operación correcta del módulo MNV, el archivo XML se requiere para ser puesto en este directorio:

- Para Windows 7 y posterior: **El %ALLUSERSPROFILE% \ Cisco \ Cliente de movilidad Cisco AnyConnect Secure \ MNV**
- Para el mac OSX: **/opt/cisco/anyconnect/nvm**

Si el perfil está presente en Cisco ASA/Identity mantiene el motor (ISE), después auto-se despliega junto con el despliegue de Anyconnect MNV.

Ejemplo del perfil XML:

```
<?xml version="1.0" encoding="UTF-8"?>
-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="NVMProfile.xsd">
-<CollectorConfiguration>
<CollectorIP>192.0.2.123</CollectorIP>
<Port>2055</Port>
</CollectorConfiguration>
<Anonymize>false</Anonymize>
<CollectionMode>all</CollectionMode>
</NVMProfile>
```

El perfil MNV se puede crear usando dos diversas herramientas:

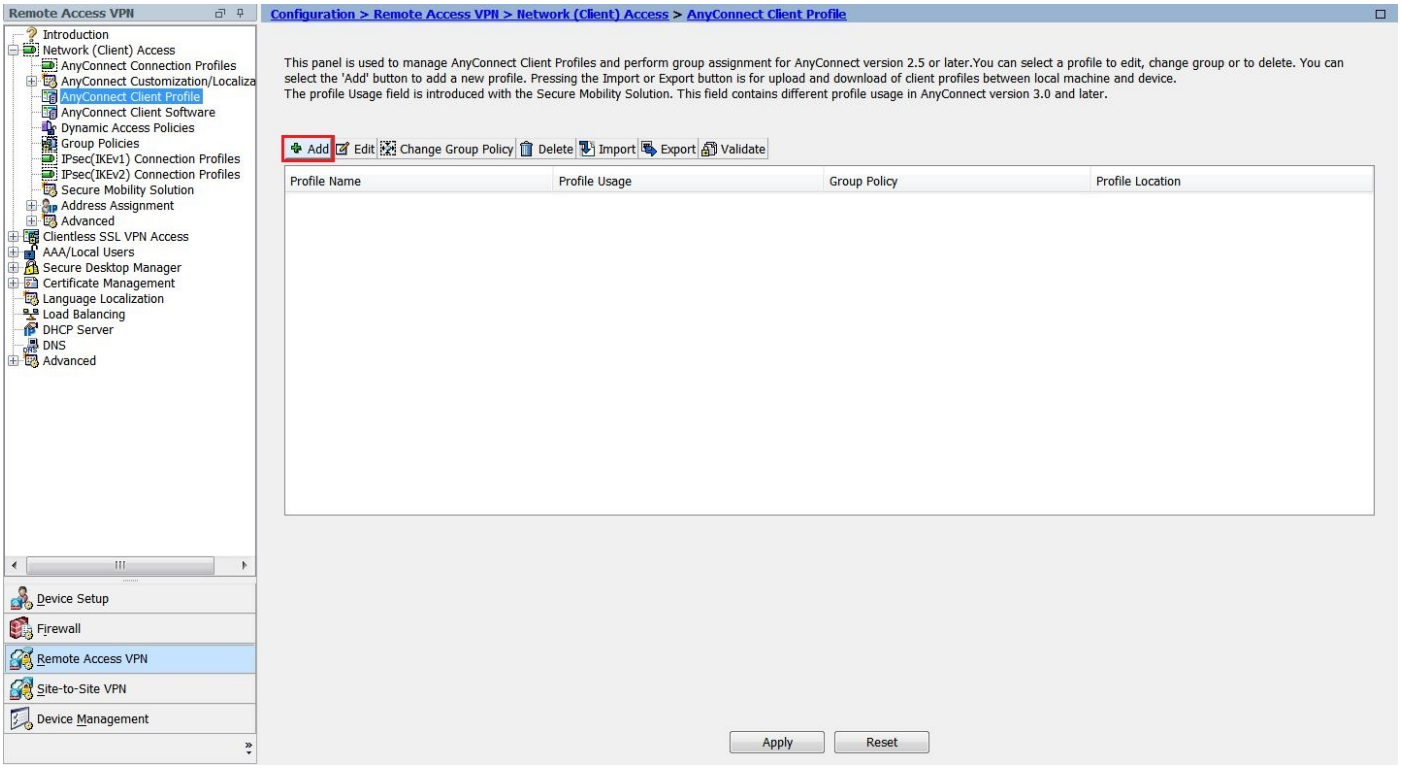
- ASDM de Cisco
- Editor del perfil de Anyconnect

Perfil del cliente de la configuración MNV vía el ASDM

Este método es preferible si Anyconnect MNV se está desplegando vía Cisco ASA.

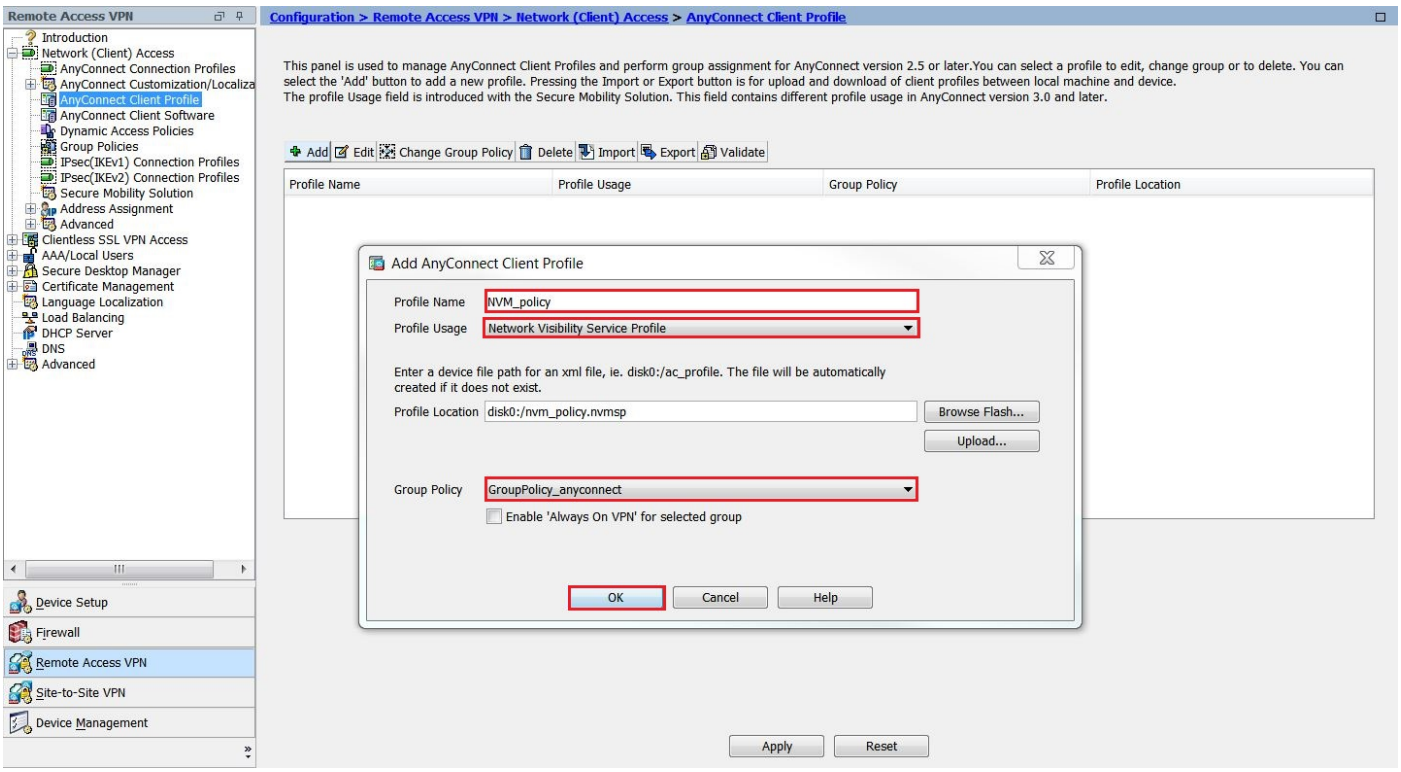
1. Navegue a la **configuración > quitan el acceso del VPN de acceso > de la red (cliente) > el perfil del cliente de Anyconnect**

2. El tecleo **agrega**

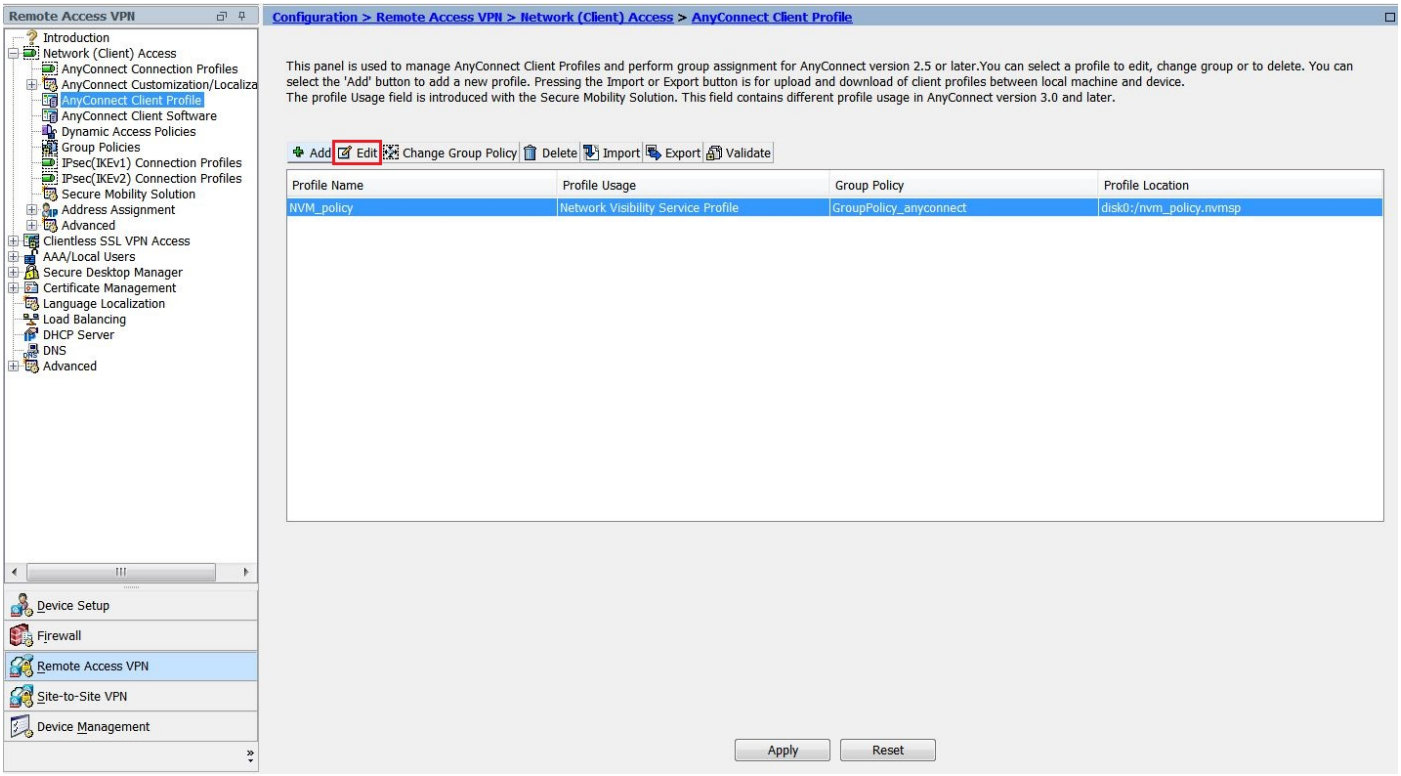


3. Dé a perfil un nombre. En el **uso del perfil**, seleccione el **perfil del servicio de la visibilidad de la red**

4. Asígnelo a la grupo-directiva que es utilizada por los usuarios de Anyconnect. Click OK.

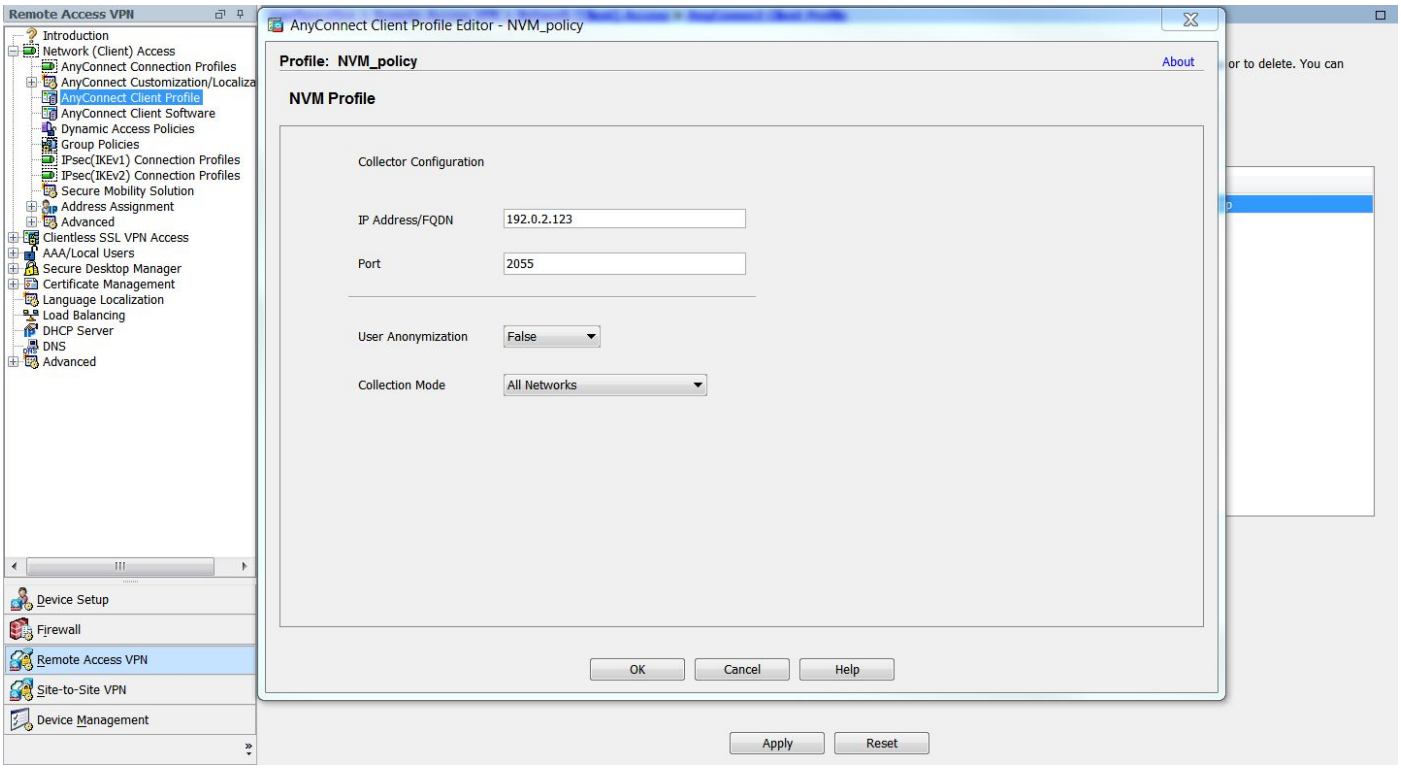


5. Se crea la nueva directiva. El tecleo **edita**



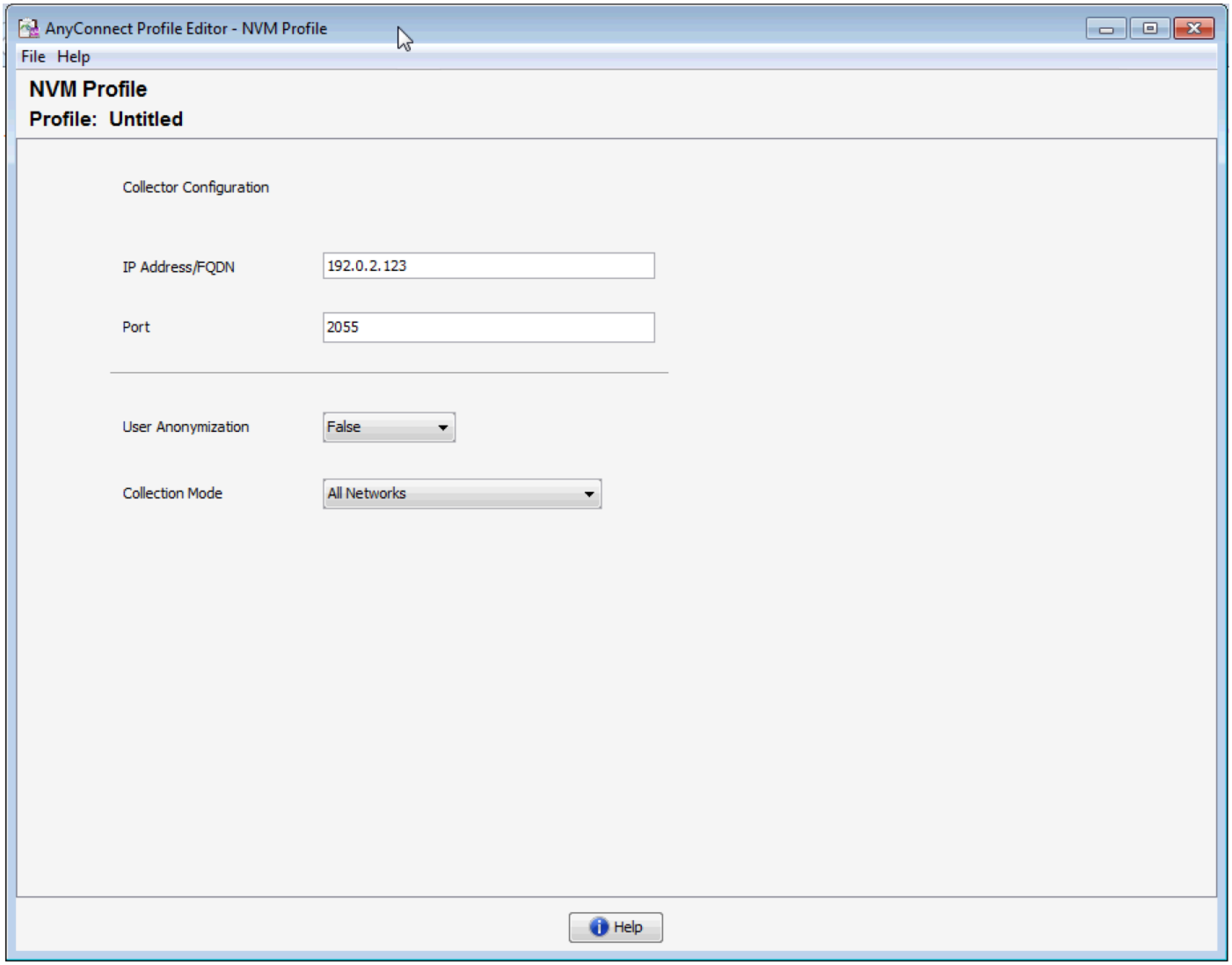
6. Llene la información con respecto la dirección IP y al número del puerto del colector. Click OK.

7. Haga clic en Apply (Aplicar).



Configure el perfil del cliente MNV vía el editor del perfil de Anyconnect

Esto es una herramienta independiente disponible en el cisco.com. Este método es preferible si Anyconnect MNV se está desplegando vía Cisco ISE. El perfil MNV creado usando esta herramienta se puede cargar a Cisco ISE, o copiar directamente a los puntos finales.



Para información detallada sobre el editor del perfil de Anyconnect, refiérase:

El editor del perfil de AnyConnect

Red-despliegue de la configuración en Cisco ASA

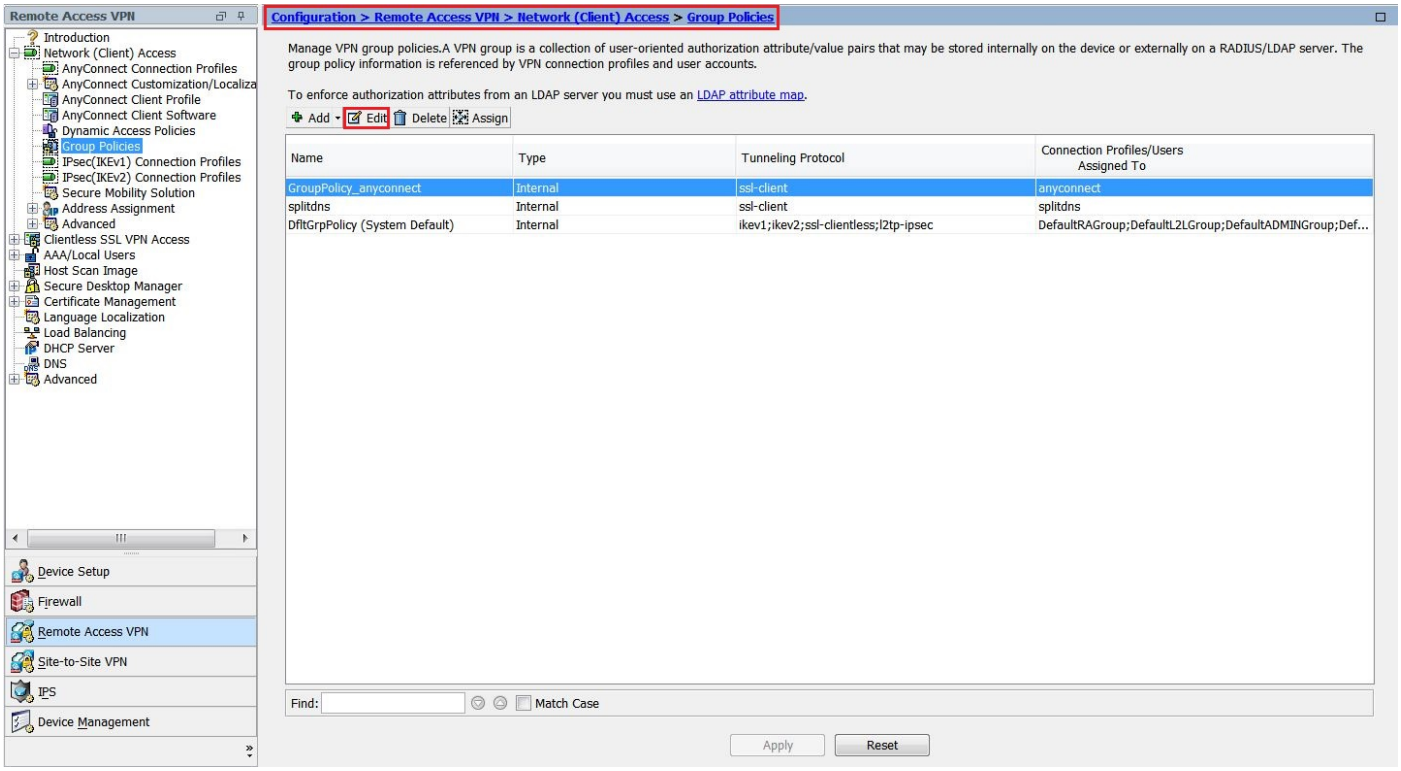
Esta Nota Técnica asume que Anyconnect está configurado ya en el ASA, y solamente la configuración de módulos MNV necesita ser agregada. Para información detallada sobre la configuración ASA Anyconnect, refiérase:

Libro 3 del ASDM: Guía de Configuración de ASDM de la serie VPN de Cisco ASA, 7.5

Para habilitar el módulo de Anyconnect MNV en Cisco ASA, realice estos pasos:

1. Navegue a la **configuración > al VPN de acceso remoto > las directivas al acceso > al grupo de la red (cliente)**

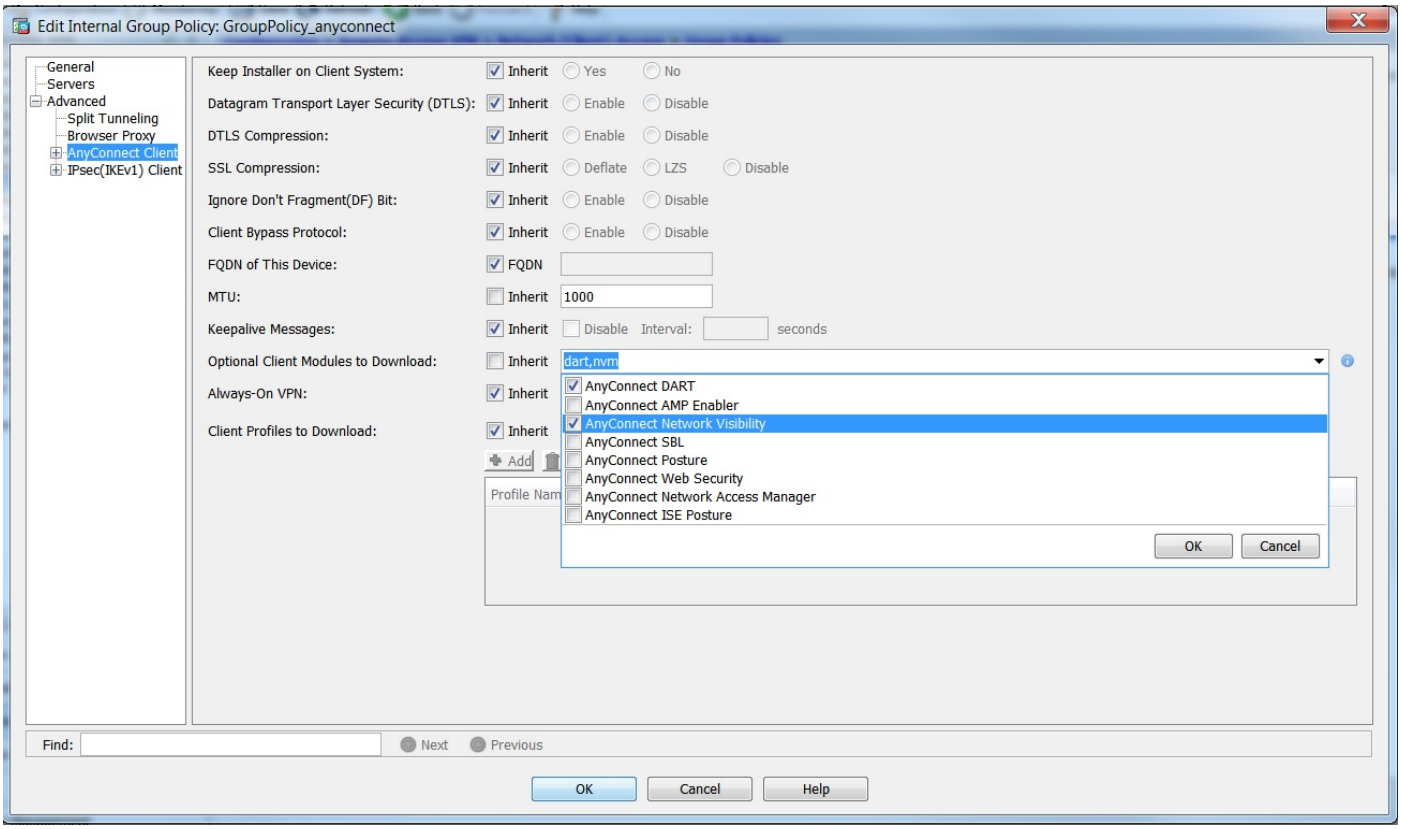
2. Seleccione la grupo-directiva relevante y el tecleo **edita**



3. Dentro de la grupo-directiva móvil, navegue a **avanzado > cliente de Anyconnect.**

4. Amplíe los **módulos cliente opcionales para descargar** y para seleccionar la **visibilidad de la red de Anyconnect.**

5. El Haga Click en OK y aplica los cambios.



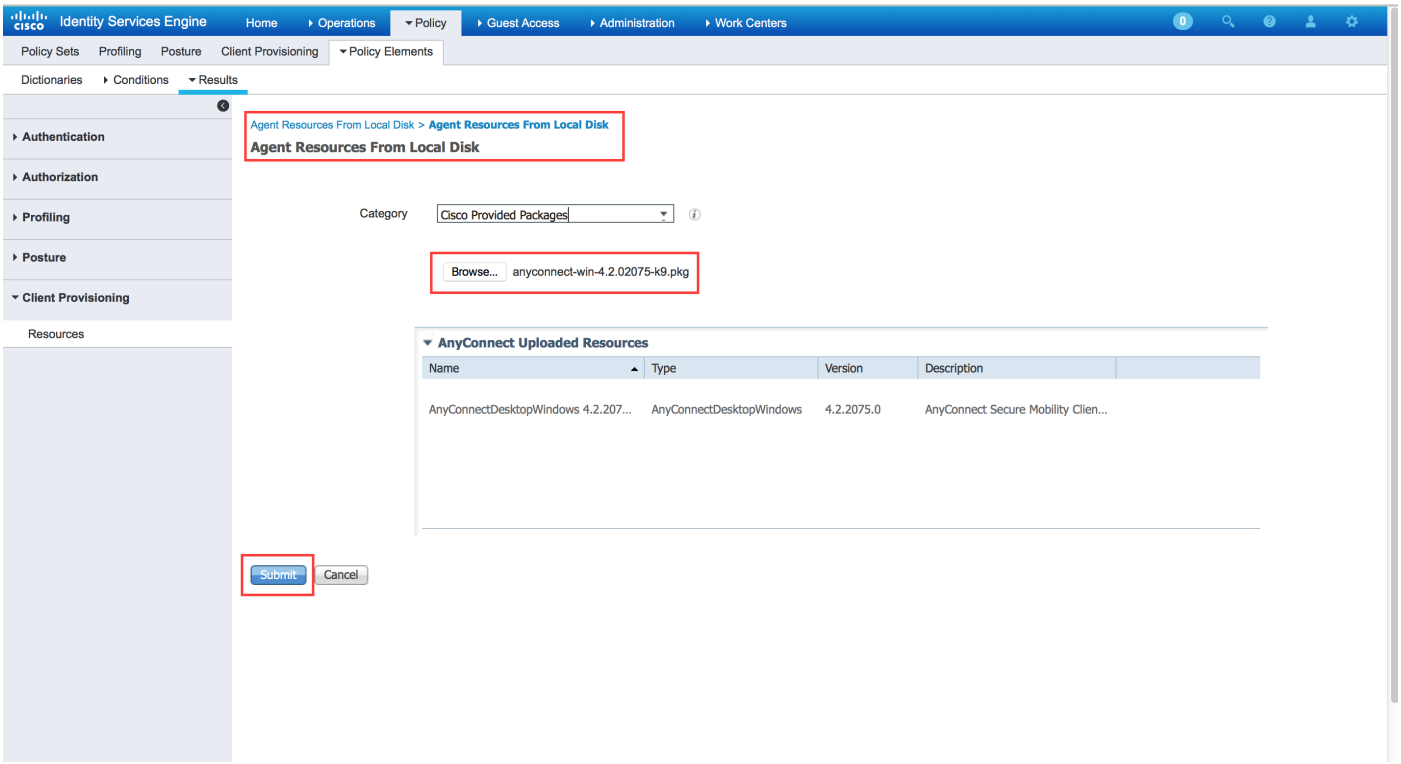
Red-despliegue de la configuración en Cisco ISE

- Para configurar Cisco ISE para el Red-despliegue de Anyconnect, realice estos pasos:

- En Cisco ISE GUI, navegue a la **directiva > a los elementos > a los resultados de la directiva**
- Amplíe el **aprovisionamiento del cliente** para mostrar los **recursos,** y para seleccionar los **recursos**

Agregar la imagen de Anyconnect

Selecto **agregue > los recursos del agente,** y cargue el archivo de paquete de Anyconnect.



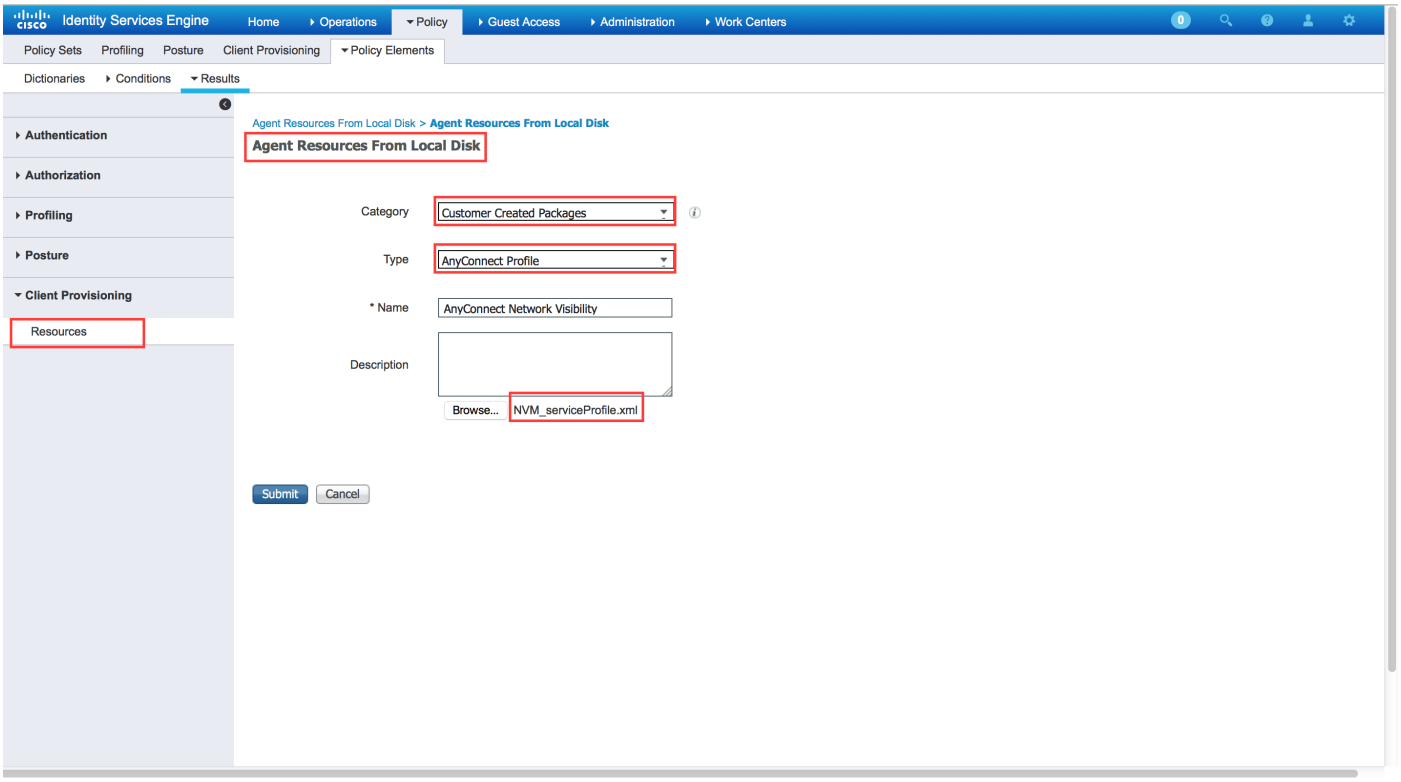
Confirme el hash del paquete en el móvil.

El archivo-hash se puede verificar contra la página de la descarga del cisco.com o usar la herramienta de tercera persona.

Este paso se puede relanzar para agregar las imágenes múltiples de Anyconnect. (para el mac OSX y el Linux OS)

Agregar el perfil de Anyconnect MNV:

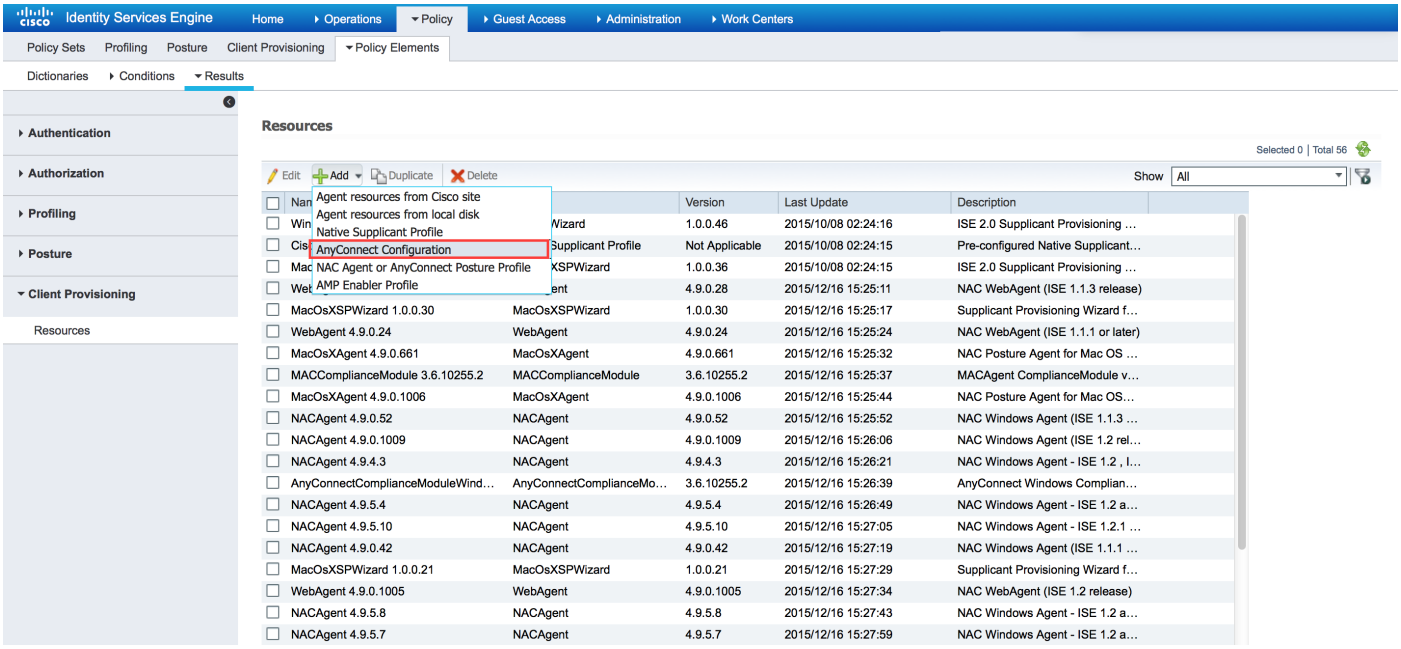
Selecto agregue > los recursos del agente, y cargue el perfil del cliente MNV.



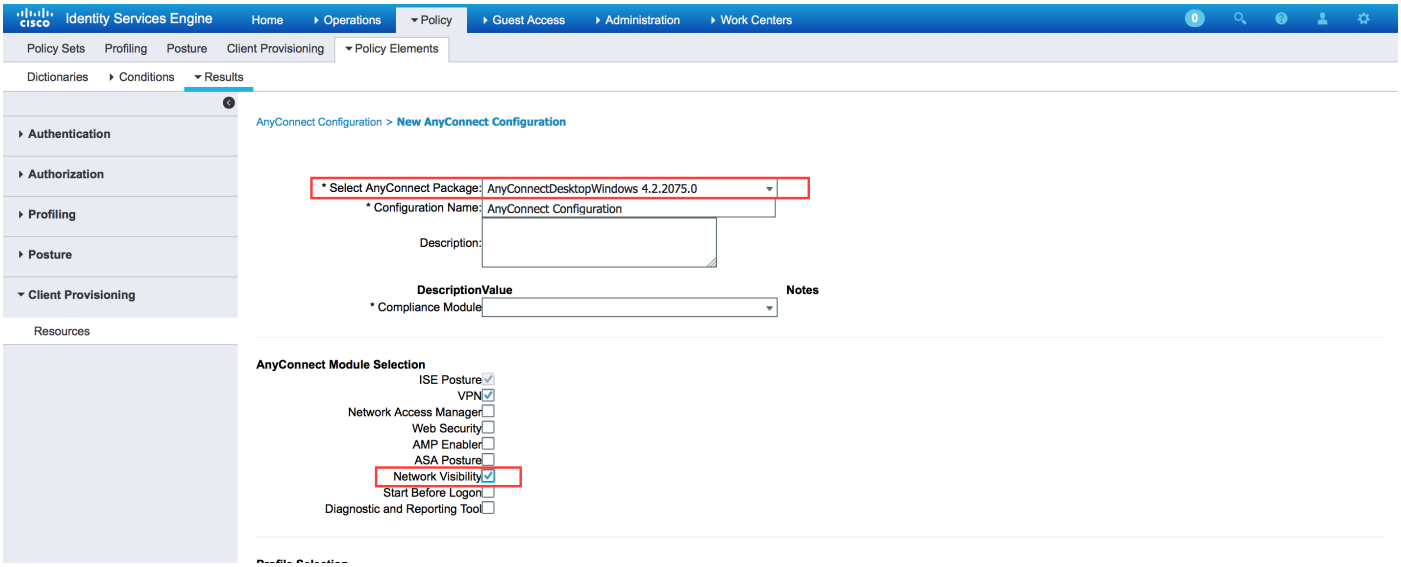
Agregue el archivo de configuración de Anyconnect:

Selecto agregue > configuración de AnyConnect

Elija el paquete cargado en el paso anterior.



Habilite la **MNV** en la **selección del módulo de AnyConnect** junto con la directiva requerida.



En la sección antedicha, habilitamos los módulos cliente de AnyConnect, los perfiles, los paquetes del arreglo para requisitos particulares/del lenguaje, y los paquetes de Opswat.

Para información detallada sobre la configuración del red-despliegue en Cisco ISE, refiérase:

AnyConnect Red-que despliega

Detección de la red de confianza

La MNV envía la información de flujo solamente cuando está en una red de confianza. Utiliza la característica TND del cliente de Anyconnect para aprender si el punto final está en una red de confianza. El TND utiliza la información DNS/domain para determinar si el punto final está en una red de confianza. Cuando el VPN está conectado, se considera estar en una red de confianza, y la información de flujo se envía al colector.

El TND necesita ser configurado correctamente para el funcionamiento correcto de la MNV. Para los detalles en la configuración TND, refiérase:

Configure la detección de la red de confianza

Despliegue

La solución de Anyconnect que despliega MNV implica estos pasos:

1. Configuración Anyconnect MNV en Cisco ASA/ISE

2. Componente del colector de la configuración IPFIX

3. Configuración Splunk con el App de Cisco MNV

Paso 1. Configuración Anyconnect MNV en Cisco ASA/ISE

Este paso se ha cubierto detalladamente en la sección de la configuración.

Una vez que la MNV se configura en Cisco ISE/ASA, puede auto-ser desplegada a los puntos finales del cliente.

Paso 2. Componente del colector de la configuración IPFIX

El componente del colector es responsable de recoger y de traducir todos los datos IPFIX de los puntos finales y de remitirlos al App de Splunk. Hay diversas herramientas de tercera persona del colector disponibles, y Cisco MNV es compatible con cualquier colector que entienda IPFIX. Esta Nota Técnica utiliza la herramienta de cosecha propia del colector de Cisco que se ejecuta en Linux 64-bit. Las secuencias de comandos de configuración de CentOS y de Ubuntu se incluyen adentro con la aplicación del splunk. El CentOS instala los scripts y los archivos de configuración se pueden también utilizar en las distribuciones de Fedora y de Redhat también. El colector se debe funcionar con en un sistema Linux 64-bit independiente o un promotor de Splunk que se ejecuta en Linux 64-bit.

Para instalar el colector que usted necesitará copiar la aplicación en el archivo de CiscoNVMCollector_TA.tar, situado en el directorio APP_DIR/appserver/addon/al sistema usted planea instalarlo encendido.

Splunk, para esta Nota Técnica, está instalado en la estación de trabajo con Windows en la E: conduzca.

El archivo de CiscoNVMCollector_TA.tar se puede situar en el directorio siguiente:

```
E:\Program Files\Splunk\etc\apps\CiscoNVM\appserver\addon\
```

Extraiga el **archivo TAR** en el sistema donde usted planea instalar el colector y ejecutar el script de **install.sh** con los privilegios del superusuario. Se recomienda para leer el archivo **$PLATFORM$_README** en el conjunto de .tar antes de ejecutar el script de install.sh. El archivo **$PLATFORM$_README** proporciona la información sobre las configuraciones de la configuración pertinente que necesitan ser verificadas y ser modificadas (en caso necesario) antes de que se ejecute el script de **install.sh**.

Directorio del colector en el servidor de Ubuntu:

```
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$ ls
acnvmcollector   CENTOS_README                  libboost_log.so.1.57.0
acnvmcollectord  install_centos.sh              libboost_system.so.1.57.0
acnvm.conf       install.sh                     libboost_thread.so.1.57.0
acnvm.conf~      install_ubuntu.sh              UBUNTU_README
acnvm.service    libboost_filesystem.so.1.57.0
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$
```

Las informaciones necesitas de ser configurado en el archivo de configuración (**acnvm.conf):**

1. Dirección IP y puerto de escucha de caso de Splunk.

2. Puerto de escucha para el colector (datos entrantes IPFIX).

Por el puerto de los datos de flujo, el puerto de los datos de la identidad del punto final y el puerto del colector se preconfiguran a las configuraciones predeterminadas en el archivo de configuración. Asegúrese de que estos valores estén cambiados si se están utilizando los puertos no valor por defecto.

Esta información se agrega en el archivo de configuración (**acnvm.conf):**

```
  GNU nano 2.2.6                                File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

Para obtener más información, consulte:

https://splunkbase.splunk.com/app/2992/#/documentation

Paso 3. Configuración Splunk con el App de Cisco MNV

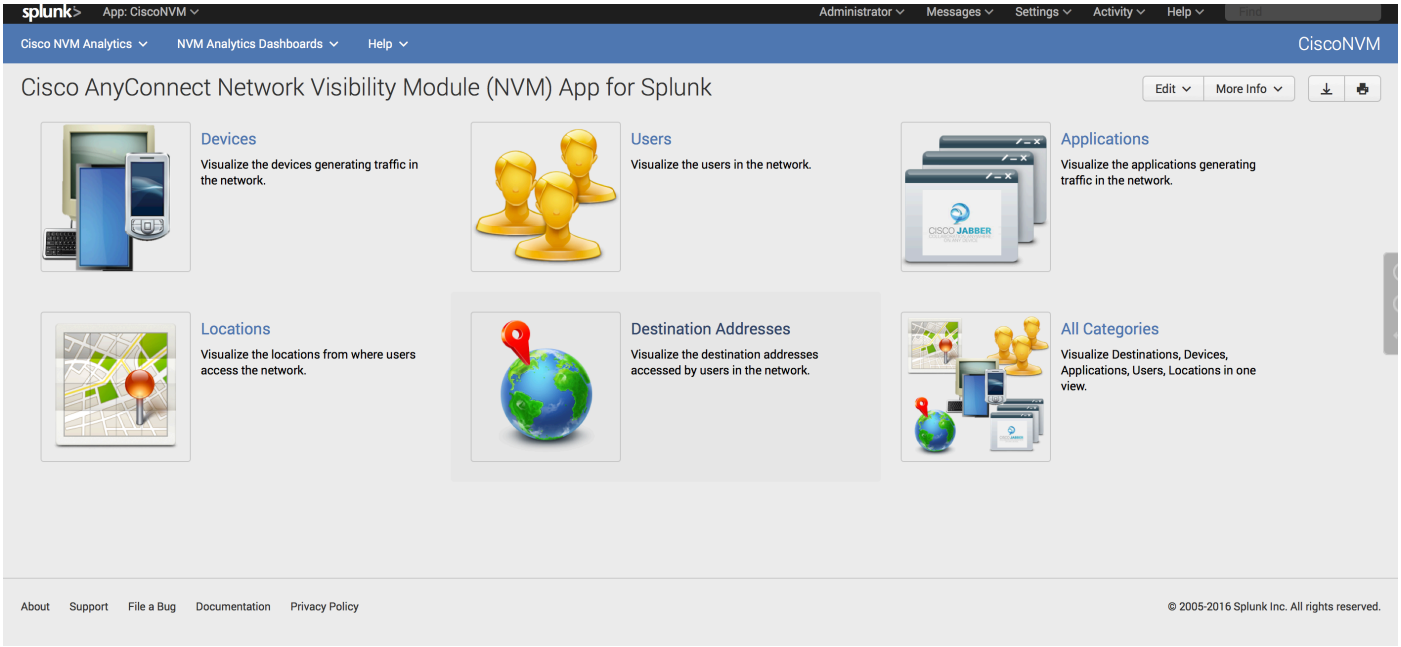
El App de Cisco AnyConnect MNV para Splunk está disponible en Splunkbase. Este app ayuda con los informes predefinidos y los paneles a utilizar los datos IPFIX (nvzFlow) de los puntos extremos en los informes usables, y correlaciona el comportamiento del usuario y del punto final.

Link para el App de Cisco MNV en Splunkbase:

https://splunkbase.splunk.com/app/2992/

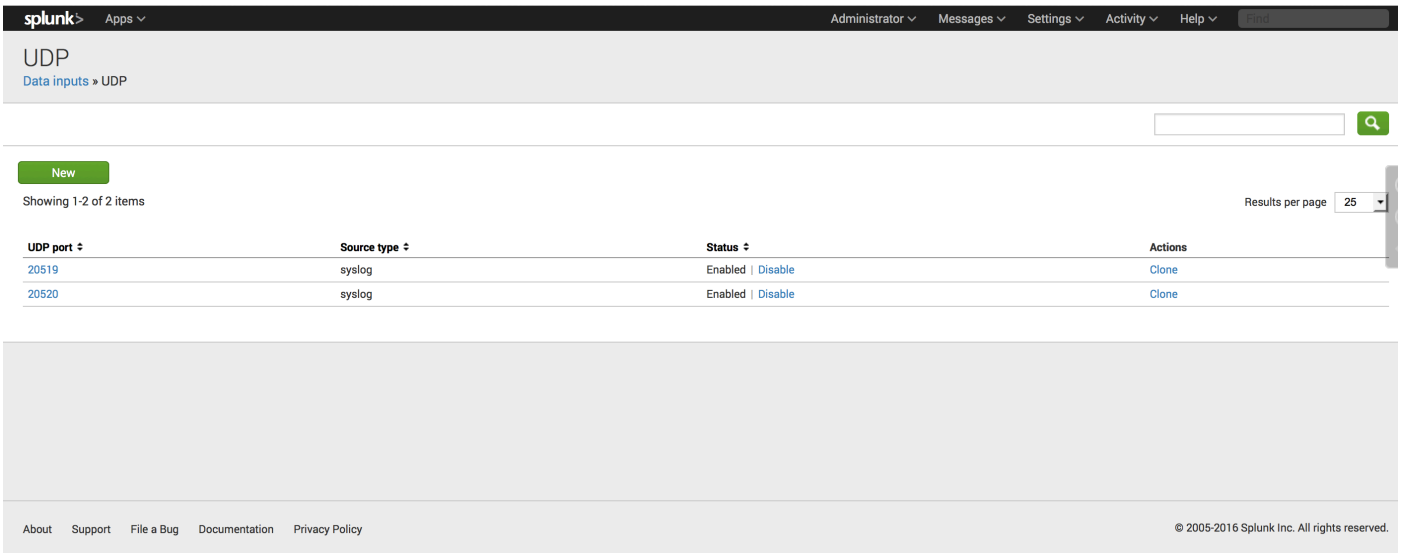
Instale:

Navegue a **Splunk > al Apps** y instale el archivo de **tar.gz** descargado del Splunkbase o busque dentro de la sección del Apps.



Por abandono, Splunk recibe dos alimentaciones de la entrada de datos para por los datos de flujo y los datos de la identidad del punto final, sobre los puertos 20519 y 20520 UDP respectivamente. El componente del colector envía estas alimentaciones en estos puertos por abandono. Los puertos predeterminados se pueden cambiar en el splunk, pero los mismos puertos también necesitan ser especificados en la configuración del colector (véase el paso 2)

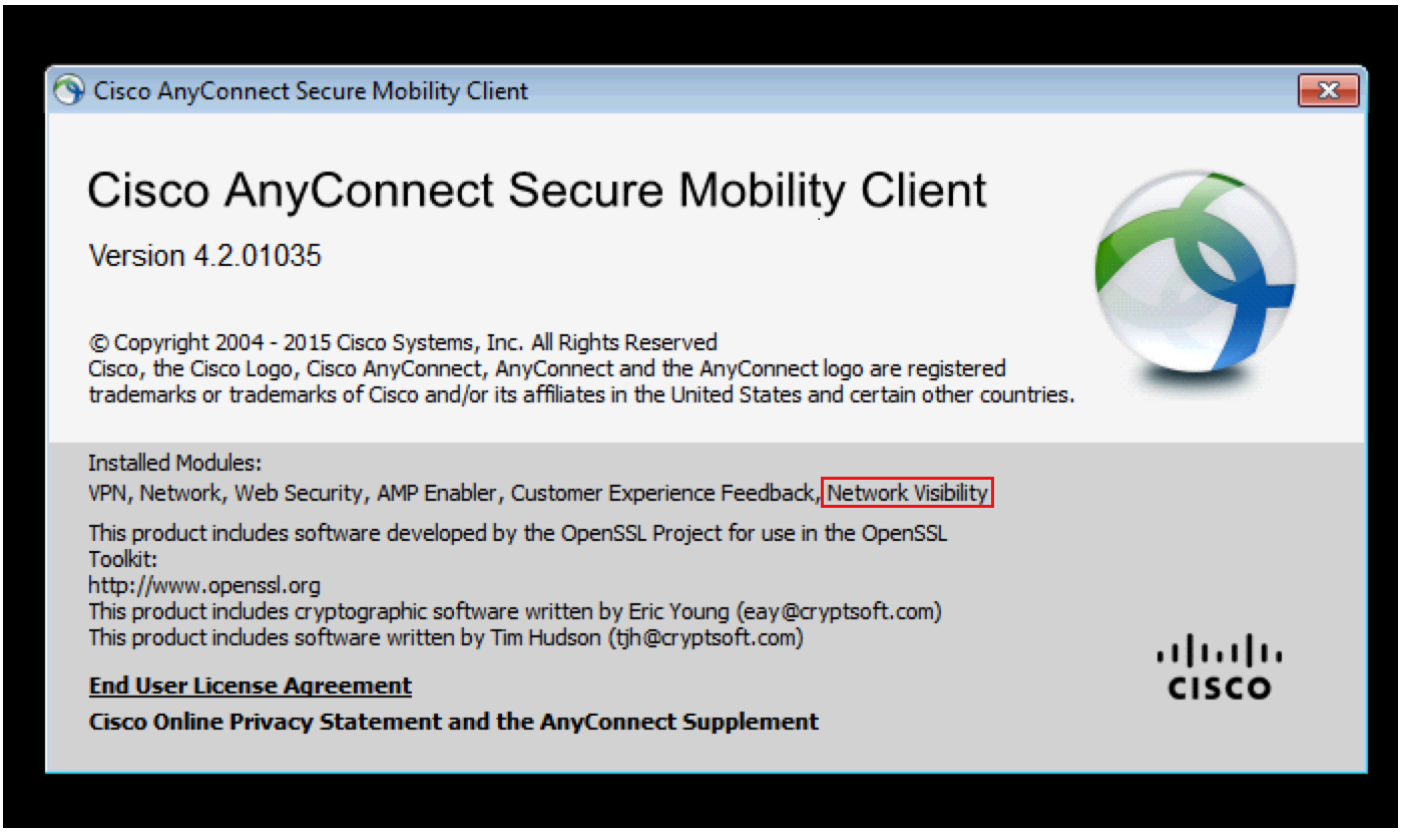
Para cambiar los puertos predeterminados, navegue a **Splunk > a las configuraciones > a la entrada de datos > al UDP**



Verificación

Valide la instalación de Anyconnect MNV

Después de la instalación exitosa, el módulo de la visibilidad de la red se debe enumerar en los **módulos instalados,** dentro en la **sección de información del** cliente seguro de la movilidad de Anyconnect.



También, verifique si el servicio MNV se está ejecutando en el punto extremo y el perfil está en el directorio requerido.

Valide el estado del colector como funcionamiento

Asegúrese de que el estado del colector se esté ejecutando. Esto se asegura de que el colector esté recibiendo IPFIX/cflow de los puntos finales siempre.

```
  GNU nano 2.2.6                                File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

Valide Splunk

Asegúrese de que Splunk y sus servicios relevantes se estén ejecutando. Para la documentación en resolver problemas Splunk, refiera por favor a su sitio web.

Troubleshooting

Flujo de paquetes

1. Los paquetes IPFIX son generados en los puntos finales del cliente por el módulo de Anyconnect MNV.

2. Los puntos finales del cliente remiten los paquetes IPFIX a la dirección IP del colector

3. El colector recoge la información y adelante la a Splunk

4. El colector envía el tráfico a Splunk en dos diversas secuencias: Por los datos de flujo y los datos de la identidad del punto final

Todo el tráfico es UDP basado encendido allí no es ningún acuse de recibo del tráfico.

Puerto predeterminado para el tráfico:

Datos 2055 IPFIX

Por los datos de flujo 20519

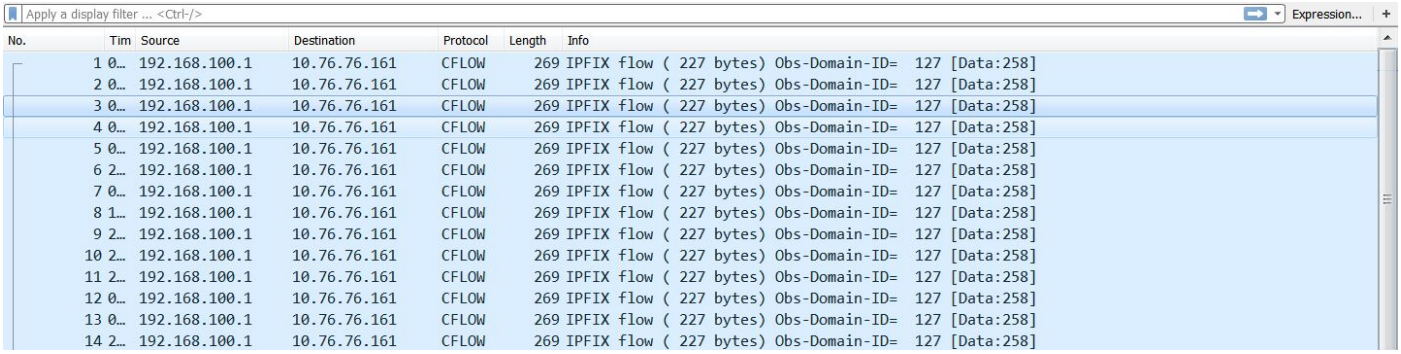
Por los datos de flujo 20520

El módulo MNV oculta los datos IPFIX y los envía al colector cuando está en la red de confianza. Esto puede cualquiera ser cuando la laptop está conectada con la red corporativa (en-prem) o cuando está conectada vía el VPN.

Pasos básicos del Troubleshooting

- Asegure la conectividad de red entre el punto final del cliente y el colector.
- Asegure la conectividad de red entre el colector y el splunk.
- Asegúrese de que la MNV esté instalada correctamente en el punto final del cliente.
- Aplique las capturas en el punto final para ver si se está generando el tráfico IPFIX.
- Aplique las capturas en el colector para ver si está recibiendo el tráfico IPFIX, y si es tráfico de reenvío a Splunk.
- Aplique las capturas en Splunk para ver si está recibiendo el tráfico.

Tráfico IPFIX como se ve en Wireshark:



Detección de la red de confianza (TND)

La MNV confía en el TND para detectar cuando el punto final está dentro de red de confianza. Si la configuración TND es incorrecta, ésta causará los problemas con la MNV.

Trabajos TND basados en la información recibida vía el DHCP: Domain Name y servidor DNS. Si el servidor DNS y/o el Domain Name hacen juego los valores configurados, después la red se juzga ser confiada en.

Si la MNV no es tráfico de reenvío al colector, después podría ser un problema con el TND.

Plantillas del flujo

IPFIX fluyen las plantillas se envían al colector al inicio de la comunicación IPFIX. Estas plantillas ayudan al colector a tener sentido de los datos IPFIX. Si esta información no se envía al colector, después el colector no puede recoger los datos IPFIX. Esto causa los problemas con la obtención de datos.

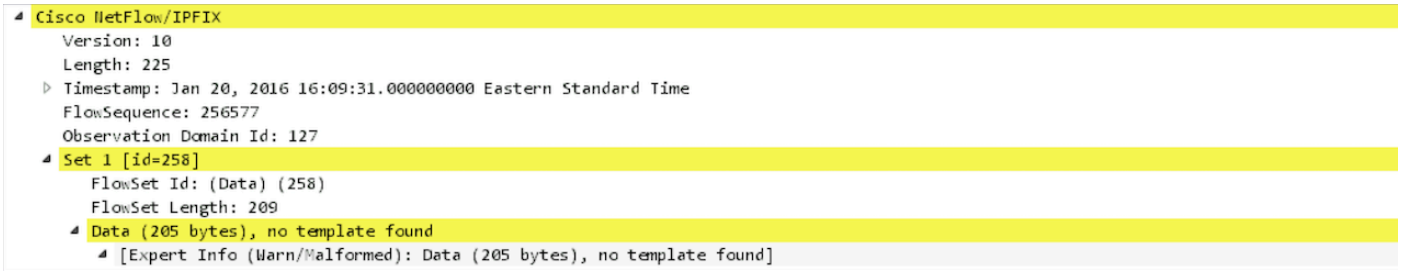
Se consideran tales problemas si el colector se configura más adelante, o si los primeros paquetes IPFIX se caen en la red (VPN excesivo común). Para atenuar esto, uno de los eventos abajo debe ocurrir:

1. Hay un cambio en el perfil del cliente MNV.
2. Hay un evento del cambio de la red.
3. Se recomienza el servicio nvmagent.
4. Se reinicia/se recomienza el punto extremo.

Este problema puede ser recuperado reiniciando el punto final, o volviendo a conectar el VPN.

El problema se puede identificar no observando **ninguna plantilla encontrada** en una captura de paquetes en el punto extremo, o **ningunas plantillas para el flowset** en los registros del colector.

Captura de paquetes



Registros del colector:

```
  GNU nano 2.2.6                                File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

Versión recomendada

Cisco recomienda siempre la versión del último software de AnyConnect a la hora del uso o de la puesta al día. Mientras que elige la versión de AnyConnect, utilice por favor al último cliente 4.2.x o 4.3.x. Esto dará las últimas mejoras con el resepect MNV, las correcciones de defectos y atenuar los cambios recientes con Microsoft cifre las aplicaciones de firma de los Certificados. Más detalles aquí.

Defectos relacionados

1. CSCva21660 - Manijas/escape de Anyconnect MNV para el proceso acnvmagent.exe*32

Links relacionados

1. App de la visibilidad de la red de Cisco AnyConnect (MNV) para Splunk: https://splunkbase.splunk.com/app/2992/
2. Documentación de Splunk en la configuración y instalar del colector de Splunk los scripts del colector: https://splunkbase.splunk.com/app/2992/#/documentation
3. Guía del administrador del Cliente de movilidad Cisco AnyConnect Secure, versión 4.3
4. Release Note de AnyConnect 4.3