Guía de despliegue de itinerancia del módulo de la Seguridad de AnyConnect OpenDNS

Contenido

Introducción

Este documento describe la instalación, la configuración, y los pasos de Troubleshooting para el módulo de itinerancia de OpenDNS (paraguas). En AnyConnect 4.3.X y posterior, el cliente de itinerancia de OpenDNS está disponible ahora como módulo integrado. También se conoce como el módulo de la Seguridad de la nube y puede ser predesplegado al punto final con el instalador de AnyConnect, o puede ser descargado del dispositivo de seguridad adaptante (ASA) vía red-despliega.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Movilidad segura de Cisco AnyConnect
- OpenDNS/módulo de itinerancia del paraguas
- Cisco ASA

Componentes Utilizados

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

- Versión de ASA 9.3(3)7 de Cisco
- Cliente de movilidad Cisco AnyConnect Secure 4.3.01095
- Módulo de itinerancia 4.3.01095 de OpenDNS
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 o más adelante
- Microsoft Windows 8.1
- **Note**: Los requerimientos mínimos de desplegar el módulo del paraguas de OpenDNS son:
  - Versión 4.3.01095 o posterior del cliente VPN de AnyConnect
  - ASDM 7.6.2 de Cisco o más adelante
  El módulo de itinerancia de OpenDNS no se soporta actualmente en las plataformas Linux.

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 su red está viva, aseegurese que usted entiende el impacto potencial de los comandos any o de la configuración.

Antecedentes

OrgInfo.json

Para que el módulo de itinerancia de OpenDNS funcione correctamente, un archivo OrgInfo.json se debe descargar del panel de OpenDNS o avanzar del ASA antes de que se utilice el módulo. Cuando el archivo primero se descarga, se guarda en una trayectoria específica que dependa del sistema operativo.

Para Mac OS X, OrgInfo.json se descarga a /opt/cisco/anyconnect/Umbrella.
Para Microsoft Windows, OrgInfo.json se descarga al cliente \ al paraguas seguros de la movilidad de C:\ProgramData\Cisco\Cisco AnyConnect.

```
{
"organizationId" : "XXXXXXX",
"fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
"userId" : "XXXXXXX"
}
```

Como se muestra, el archivo utiliza UTF-8 que codifica y contiene un organizationId, una huella dactilar, y un userId. El ID de la organización representa la información de la organización para el usuario que se registra actualmente en el panel de OpenDNS. El ID de la organización es estático, único, y auto-generado por OpenDNS para cada organización. La huella dactilar se utiliza para validar el archivo OrgInfo.json durante el registro del dispositivo y la identificación del usuario representa un ID único para el usuario autenticado.

Cuando el módulo de itinerancia comienza en Windows, el archivo OrgInfo.json se copia al

directorio de datos bajo directorio del paraguas y se utiliza como la copia de funcionamiento. En MAC OS X, la información de este archivo se guarda a updater.plist en el directorio de datos bajo directorio del paraguas. Una vez que el módulo ha leído con éxito la información del archivo OrgInfo.json, intenta registrarse con OpenDNS con una nube API. Este registro da lugar a OpenDNS que asigna a un dispositivo único ID a la máquina ese registro frustrado. Si un ID del dispositivo del registro anterior está ya disponible, el dispositivo salta el registro.

Después de que el registro sea completo, el módulo de itinerancia realiza una operación de sincronización para extraer la información de política para el punto final. Un ID del dispositivo es necesario para que la operación de sincronización trabaje. Sincronice los datos incluye los dominios syncInterval, whitelisted, y los IP Addresses entre otras cosas. El intervalo del sincronizar es el número de minutos después de lo cual el módulo debe intentar a la RESYNC.

Comportamiento que sonda DNS

Sobre el registro exitoso y sincronice, el módulo de itinerancia envía las sondas del Domain Name System (DNS) a sus softwares de resolución de nombres locales. Estas peticiones DNS incluyen las interrogaciones de TXT para debug.opendns.com. De acuerdo con la respuesta, el cliente puede determinar si una aplicación virtual de OpenDNS de la en-premisa (VA) existe en la red.

Si un dispositivo virtual (VA) está presente, las transiciones del cliente a un modo “detrás-VA”, y la aplicación DNS no se realiza en el punto final. El cliente confía en el VA para la aplicación DNS en el nivel de red.

Si un VA no está presente, el cliente envía una petición DNS a los softwares de resolución de nombres públicos de OpenDNS (208.67.222.222) usando UDP/443.

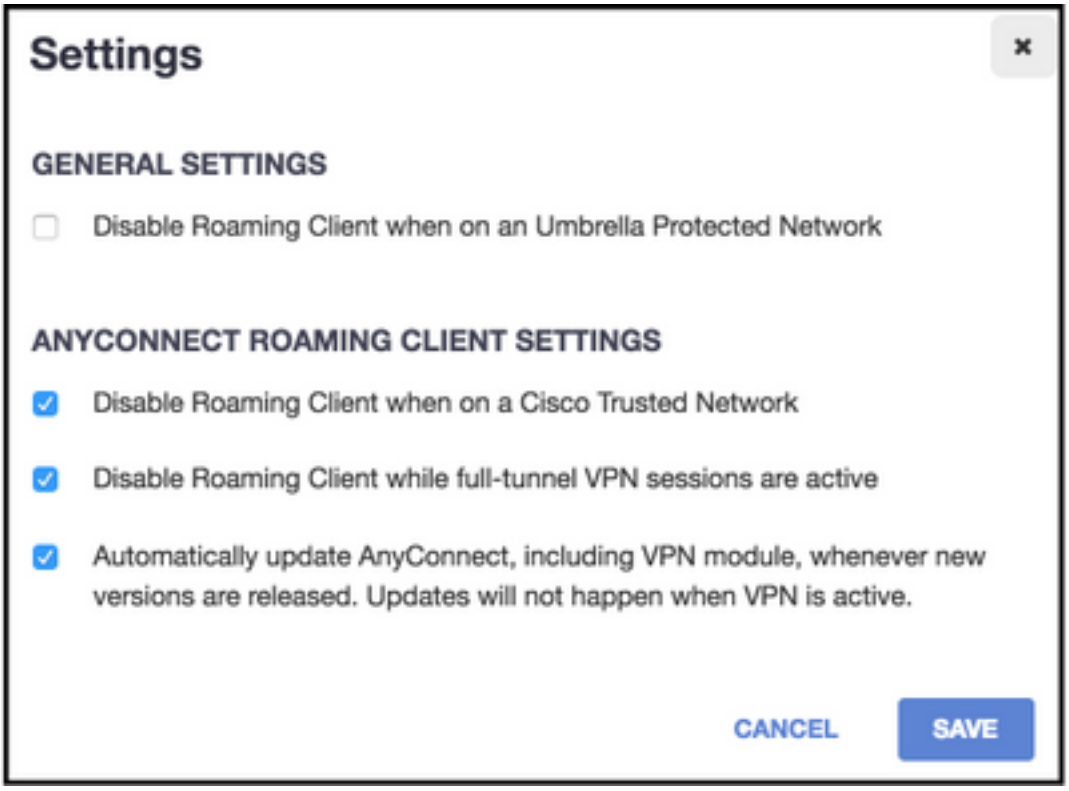
Una respuesta positiva indica que el cifrado DNS es posible. Si se recibe una respuesta negativa, el cliente envía una petición DNS a los softwares de resolución de nombres públicos de OpenDNS usando UDP/53.

Una respuesta positiva a esta interrogación indica que la protección DNS es posible. Si se recibe una respuesta negativa, el cliente revisa la interrogación en unos segundos.

Tras el recibo de un determinado número de respuestas negativas, las transiciones del cliente al estado fracaso-abierto. Un estado fracaso-abierto significa que el cifrado y/o la protección DNS no es posibles. Una vez que el módulo de itinerancia tiene con éxito transitioned a un estado protegido y/o cifrado, todas las interrogaciones DNS para los dominios de la búsqueda fuera de los dominios locales de la búsqueda y de los dominios del whitelist se envían a los discernidores de imágenes de OpenDNS para la resolución de nombre. Con el estado cifrado habilitado, todas las transacciones DNS son cifradas por el proceso del dnscrypt.

Comportamiento DNS con los modos del Tunelización de AnyConnect

1. Túnel-todo (o túnel-todo-DNS habilitado)



> **Note**: Como se muestra, el comportamiento predeterminado está para que el módulo de itinerancia inhabilite la protección DNS mientras que un túnel VPN con túnel-toda configuración es activo. Para que el módulo sea activo durante un AnyConnect túnel-toda configuración, el **cliente de itinerancia de la neutralización mientras que las sesiones de VPN del FULL-túnel son opción activa** debe ser desmarcado en el portal de OpenDNS. La capacidad de habilitar esta característica requiere una suscripción avanzada llana con OpenDNS. La información abajo asume que la protección DNS vía el módulo de itinerancia está habilitada.

Lista blanca preguntada de la parte del dominio

Las peticiones DNS que originan del adaptador del túnel se permiten y se envían a los servidores DNS del túnel, a través del túnel VPN. La interrogación seguirá siendo sin resolver si no puede ser resuelta por los servidores DNS del túnel.

Lista blanca preguntada de la parte del dominio no

Las peticiones DNS que originan del adaptador del túnel se permiten, y proxied a los softwares de resolución de nombres públicos de OpenDNS vía el módulo de itinerancia y serán enviadas a través del túnel VPN. Al cliente DNS aparecerá como si la resolución de nombre hubiera ocurrido vía el servidor DNS VPN. Si la resolución de nombre vía los softwares de resolución de nombres de OpenDNS no es acertada, el módulo de itinerancia falla encima a los servidores DNS localmente configurados, empezando por el adaptador VPN (que es el adaptador preferido mientras que el túnel está para arriba).

2. DNS dividido (túnel-todo-DNS inhabilitado)

> **Note**: Todos los dominios del DNS dividido se agregan automáticamente a la lista blanca de itinerancia del módulo sobre el establecimiento del túnel. Esto se hace para proporcionar un mecanismo de dirección constante DNS entre AnyConnect y el módulo de itinerancia.

Asegúrese de que en una configuración del DNS dividido (con fractura-incluya el Tunelización) los softwares de resolución de nombres públicos de OpenDNS no estén incluidos en las redes del fractura-incluido.

Note: En Mac OS X, si el DNS dividido se habilita para ambo IPv4 y IPv6) de los protocolos IP (o se habilita solamente para un protocolo y no hay agrupación de direcciones configurada para el otro protocolo, el DNS dividido verdadero similar a Windows se aplica. Si el DNS dividido se habilita para solamente un protocolo y asignan una dirección cliente para el otro protocolo, sólo el retraso DNS para el Túnel dividido se aplica. Esto significa que AnyConnect permite solamente las peticiones DNS que hacen juego los dominios del DNS dividido vía el túnel (otras peticiones son contestadas por el AC con la respuesta rechazada de forzar la Conmutación por falla a los servidores DNS públicos), pero que no puede aplicar que las peticiones que hacen juego los dominios del DNS dividido no estén enviadas en el claro vía el adaptador público.

Lista blanca de la parte del dominio y también dominios preguntados del DNS dividido de la parte de

Las peticiones DNS que originan del adaptador del túnel se permiten y se envían a los servidores DNS del túnel, a través del túnel VPN. El resto de los pedidos los dominios que corresponden con de otros adaptadores serán respondidos por el driver de AnyConnect con “ningún tal nombre” para alcanzar el DNS dividido verdadero (prevenga el retraso DNS). Por lo tanto, solamente el tráfico del NON-túnel DNS es protegido por el módulo de itinerancia.

Lista blanca preguntada de la parte del dominio, pero no dominios del DNS dividido de la parte de

Las peticiones DNS que originan del adaptador físico se permiten y se envían a los servidores DNS públicos, fuera del túnel VPN. El resto de los pedidos los dominios que corresponden con del adaptador del túnel serán respondidos por el driver de AnyConnect con “ningún tal nombre” para evitar que la interrogación sea enviada a través del túnel VPN.

Lista blanca de la parte del dominio no o dominios preguntados del DNS dividido

Las peticiones DNS que originan del adaptador físico se permiten y proxied a los softwares de resolución de nombres públicos de OpenDNS, y se envían fuera del túnel VPN. Al cliente DNS aparecerá como si la resolución de nombre hubiera ocurrido vía el servidor DNS público. Si la resolución de nombre vía los softwares de resolución de nombres de OpenDNS es fracasada, el módulo de itinerancia falla encima a los servidores DNS localmente configurados, excepto los que está configurados en el adaptador VPN. El resto de los pedidos los dominios que corresponden con del adaptador del túnel serán respondidos por el driver de AnyConnect sin tal nombre para evitar que la interrogación sea enviada a través del túnel VPN.

3. Fractura-incluya o Fractura-excluya el Tunelización (ningún DNS dividido y túnel-todo-DNS inhabilitados)

Lista blanca preguntada de la parte del dominio

El software de resolución de nombres nativo OS realiza la resolución de DNS basada por orden de los adaptadores de red, y AnyConnect es el adaptador preferido cuando el VPN es activo. Las peticiones DNS primero originarán del adaptador del túnel y serán enviadas a los servidores DNS del túnel, a través del túnel VPN. Si la interrogación no se puede resolver por los servidores DNS

del túnel, el software de resolución de nombres OS intentará resolverla vía los servidores DNS públicos.

Lista blanca preguntada de la parte del dominio no

El software de resolución de nombres nativo OS realiza la resolución de DNS basada por orden de los adaptadores de red, y AnyConnect es el adaptador preferido cuando el VPN es activo. Las peticiones DNS primero originarán del adaptador del túnel y serán enviadas a los servidores DNS del túnel, a través del túnel VPN. Si la interrogación no se puede resolver por los servidores DNS del túnel, el software de resolución de nombres OS intentará resolverla vía los servidores DNS públicos.

Si los softwares de resolución de nombres públicos de OpenDNS son parte de la lista del fractura-incluido o no parte de la lista de la fractura-exclusión, la petición proxied se envía a través del túnel VPN.

Si los softwares de resolución de nombres públicos de OpenDNS no son parte de la lista del fractura-incluido o parte de la lista de la fractura-exclusión, la petición proxied se envía fuera del túnel VPN.

Si la resolución de nombre vía los softwares de resolución de nombres de OpenDNS no es acertada, el módulo de itinerancia falla encima a los servidores DNS localmente configurados, empezando por el adaptador VPN (que es el adaptador preferido mientras que el túnel está para arriba). Si la respuesta final devuelta por el módulo de itinerancia (y proxied de nuevo al cliente DNS nativo) no es acertada, el cliente original intentará a otros servidores DNS, si está disponible.

Instale y configure el módulo de itinerancia del paraguas

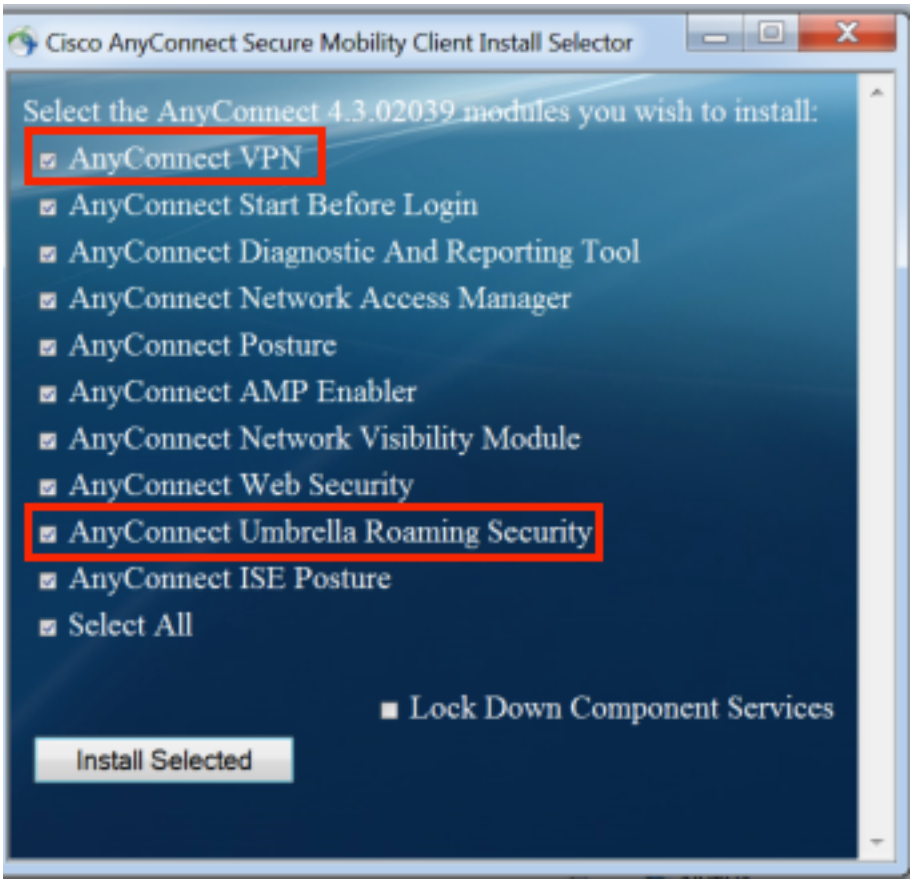
Para integrar el módulo de itinerancia de OpenDNS con el cliente VPN de AnyConnect, el módulo necesita ser instalado vía el PRE-deploment o el método de implementación de la red:

método (manual) del PRE-despliegue

el PRE-despliegue requiere la instalación manual del módulo de itinerancia de OpenDNS y el copiado del archivo OrgInfo.json en la máquina del usuario. Los despliegues a grandes escala se alcanzan típicamente con los sistemas de administración del software para empresas (SMS).

Despliegue el módulo de itinerancia de OpenDNS

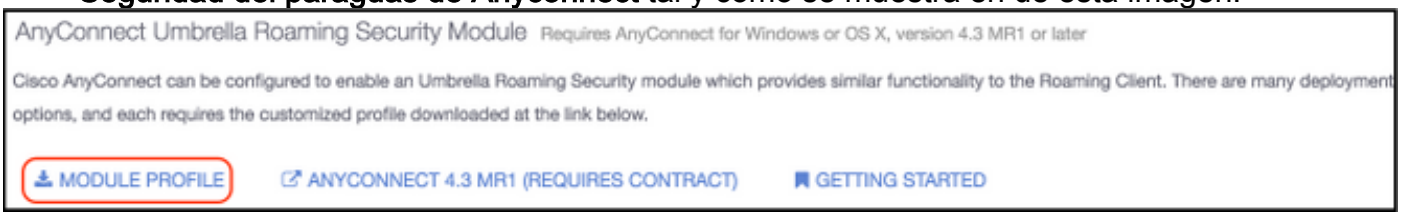
Durante la instalación del paquete de AnyConnect, elija el **AnyConnect VPN** y los módulos de **itinerancia de la Seguridad del paraguas de AnyConnect**:



Despliegue OrgInfo.json

Para descargar el archivo OrgInfo.json, complete estos pasos:

1. Registro en el panel de OpenDNS.
2. Elija la **configuración > las identidades > las Computadoras de itinerancia.**
3. Haga clic **+** muestra.
4. Navegue hacia abajo y elija el **perfil del módulo** en la **sección del módulo de itinerancia de la Seguridad del paraguas de Anyconnect** tal y como se muestra en de esta imagen:



Una vez el archivo se descarga le se debe guardar a la una de estas trayectorias, que depende del sistema operativo.

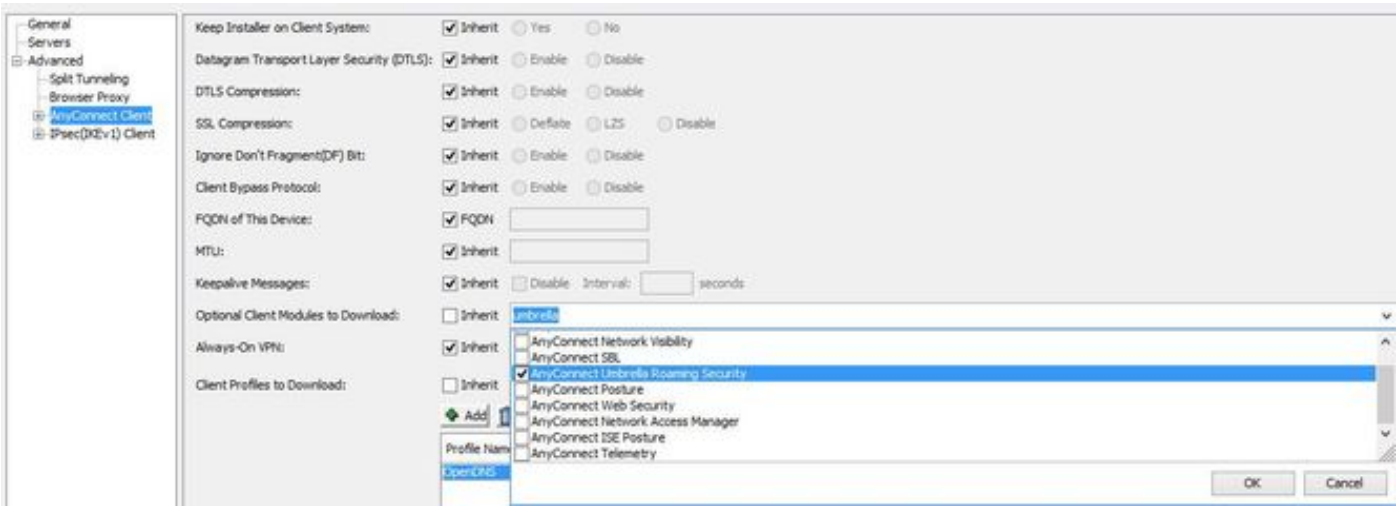
Para Mac OS X: /opt/cisco/anyconnect/Umbrella
Para Windows: Cliente \ paraguas seguros de la movilidad de C:\ProgramData\Cisco\Cisco AnyConnect

Método del Red-despliegue

Despliegue el módulo de itinerancia de OpenDNS

Descargue el paquete del cliente de la movilidad de la Seguridad de Anyconnect (es decir,

anyconnect-win-4.3.02039-k9.pkg) del sitio Web de Cisco y carguelo al flash ASA. Una vez que está cargado, en el ASDM, elija la **directiva del grupo > avanzó > cliente de AnyConnect > los módulos cliente opcionales para descargar** y después para elegir la **Seguridad de itinerancia del paraguas.**

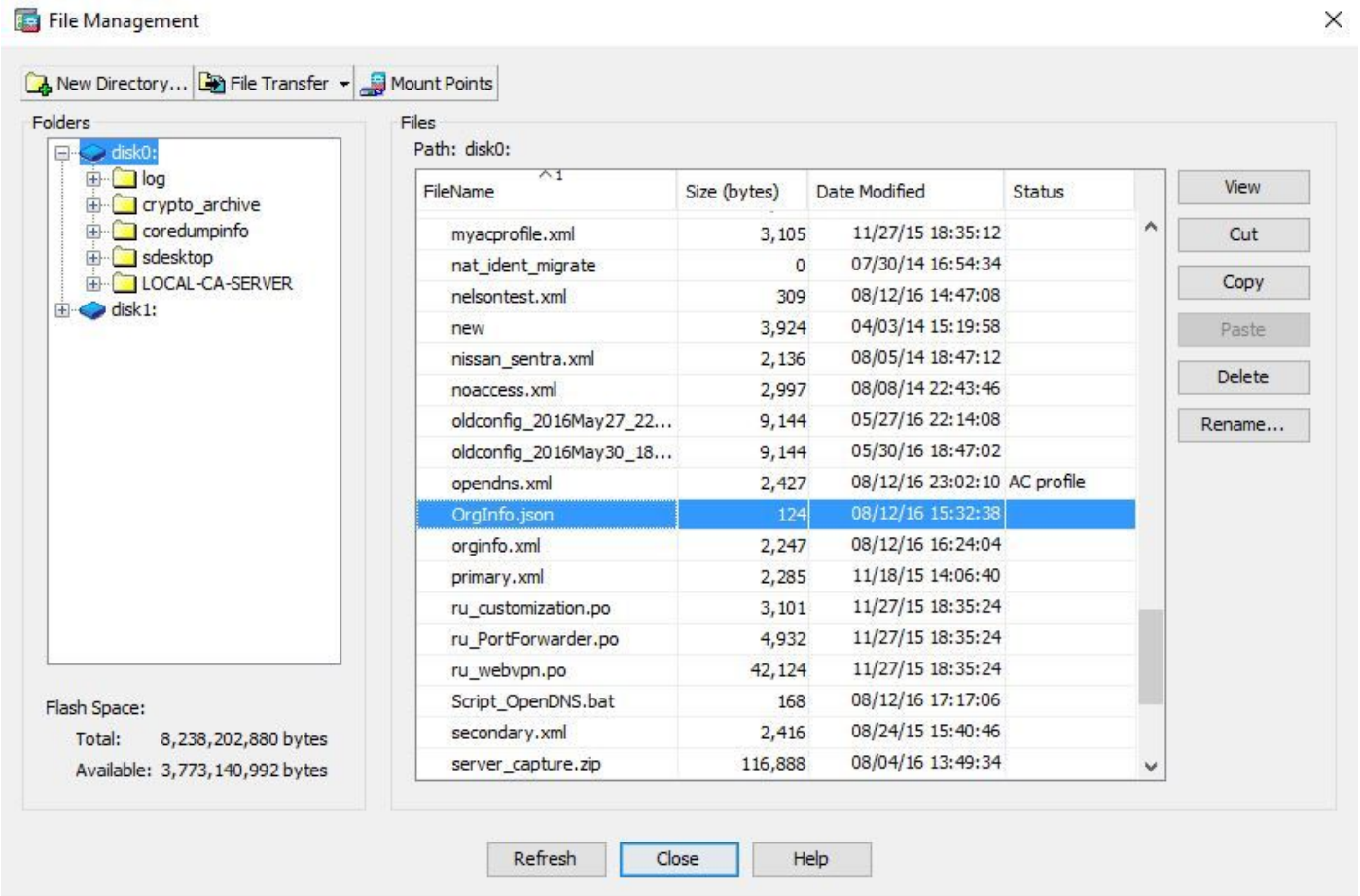


Equivalente CLI

```
group-policy <Group_Policy_Name> attributes
webvpn
anyconnect modules value umbrella
```

Despliegue OrgInfo.json

1. Descargue el archivo OrgInfo.json del panel de OpenDNS y carguelo al flash ASA.



2. Configure el ASA para avanzar el archivo OrgInfo.json a los puntos finales remotos.

```
webvpn
anyconnect profiles OpenDNS disk0:/OrgInfo.json
!
!
group-policy <Group_Policy_Name> attribute
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **Note**: Esta configuración se puede realizar solamente con el CLI. Para utilizar el ASDM para esta tarea, la versión 7.6.2 o posterior del ASDM necesita ser instalada en el ASA.

Una vez que el cliente de itinerancia del paraguas está instalado vía uno de los métodos discutidos, debe aparecer como módulo integrado dentro del AnyConnect GUI tal y como se muestra en de esta imagen:

Hasta que el OrgInfo.json se despliegue en el punto final en la ubicación correcta, el módulo de itinerancia del paraguas no será inicializado.

Configurar

La sección muestra el snippets de la configuración CLI de la muestra necesario actuar el módulo de itinerancia de OpenDNS con los diversos modos del Tunelización de AnyConnect.

```
!--- ip local pool for vpn
ip local pool vpn_pool 198.51.100.1-198.51.100.9 mask 255.255.255.224

!--- Optional NAT Hairpin configuration to reach OpenDNS servers through VPN tunnel
object network OpenDNS
subnet 198.51.100.0 255.255.255.0
```

```
nat (outside,outside) source dynamic OpenDNS interface
!
same-security-traffic permit intra-interface

!--- Global Webvpn Configuration
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.01095-k9.pkg 1
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect profiles OpenDNS disk0:/OrgInfo.json
anyconnect enable
tunnel-group-list enable

!--- split-include Configuration
access-list Split_Include standard permit <host/subnet>

group-policy OpenDNS_Split_Include internal
group-policy OpenDNS_Split_Include attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Include
split-dns value <internal domains> (Optional Split-DNS Configuration)
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Include type remote-access
tunnel-group OpenDNS_Split_Include general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Include
tunnel-group OpenDNS_Split_Include webvpn-attributes
group-alias OpenDNS_Split_Include enable


!--- Split-exclude Configuration
access-list Split_Exclude standard permit <host/subnet>

group-policy OpenDNS_Split_Exclude internal
group-policy OpenDNS_Split_Exclude attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Exclude
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Exclude type remote-access
tunnel-group OpenDNS_Split_Exclude general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Exclude
tunnel-group OpenDNS_Split_Exclude webvpn-attributes
group-alias OpenDNS_Split_Exclude enable


!--- Tunnelall Configuration
group-policy OpenDNS_Tunnel_All internal
group-policy OpenDNS_Tunnel_All attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
```

```
 split-tunnel-policy tunnelall
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Tunnel_All type remote-access
tunnel-group OpenDNS_Tunnel_All general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Tunnel_All
tunnel-group OpenDNS_Tunnel_All webvpn-attributes
group-alias OpenDNS_Tunnel_All enable
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Los pasos para resolver problemas los asuntos relacionados de AnyConnect OpenDNS son:

1. Asegúrese de que el módulo de itinerancia de la Seguridad del paraguas esté instalado junto con el cliente seguro de la movilidad de Anyconnect.
2. Asegúrese que OrgInfo.json esté presente en el punto final en la trayectoria correcta basada en el sistema operativo y que esté en el formato especificado en este documento.
3. Si las interrogaciones DNS a los softwares de resolución de nombres de OpenDNS se piensan para pasar el túnel de AnyConnect VPN, asegúrese de que la horquilla esté configurada en el ASA para permitir el accesibilidad a los softwares de resolución de nombres de OpenDNS.
4. Recoja a las capturas de paquetes (sin cualquier filtros) en el adaptador virtual y el adaptador físico de AnyConnect simultáneamente y obsérvelas abajo de los dominios que no pueden resolver.
5. Si el módulo de itinerancia actúa en un estado cifrado, recoja a las capturas de paquetes después de bloquear UDP 443 localmente, para los propósitos de Troubleshooting solamente. Esa manera allí es visibilidad en las transacciones DNS.
6. Ejecute el DARDO de AnyConnect, los diagnósticos del paraguas y obsérvelo abajo de la época del error de DNS. Vea cómo recoger al conjunto del DARDO para Anyconnect para más información.
7. Recoja los registros de diagnóstico del paraguas y envíe el URL resultante a su administrador de OpenDNS. Solamente usted y el administrador de OpenDNS tienen acceso a esta información. Para Windows: C:\Program clasifía (el cliente seguro \ UmbrellaDiagnostic.exe de la movilidad x86)\Cisco\Cisco AnyConnect
   Para el mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Información Relacionada

- **Id. de bug Cisco CSCvb34863: El tiempo de espera en la resolución del DNS cuando AnyConnect configuró para fractura-incluye el Tunelización**
- **Soporte Técnico y Documentación - Cisco Systems**