Guía de implementación del módulo Anyconnect OpenDNS Roaming Security

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Orginfo.json
Comportamiento de sondeo de DNS
Comportamiento de DNS con modos túnel AnyConnect
1. Tunnel-All (o tunnel-all-DNS habilitado)
2. Split-DNS (tunnel-all-DNS deshabilitado)
3. Tunelización con Split incluido y no incluido (no split-DNS y tunnel-all-DNS deshabilitados)
Instalar y configurar el Módulo Umbrella Roaming
Método antes de la implementación (manual)
Implementar el Módulo OpenDNS Roaming
Implementar Orginfo.json
Método de implementación web
Implementar el Módulo OpenDNS Roaming
Implementar Orginfo.json
Configurar
Verificación
Troubleshoot
Información Relacionada

Introducción

En este documento, se describen los pasos para instalar el módulo OpenDNS (Umbrella) Roaming, configurarlo y resolver sus problemas. En AnyConnect 4.3.X y posteriores, el cliente de roaming de OpenDNS está ahora disponible como módulo integrado. También se conoce como módulo de seguridad en la nube y puede preimplementarse en el terminal con el instalador AnyConnect o descargarse desde Adaptive Security Appliance (ASA) mediante la implementación web.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco AnyConnect Secure Mobility

- Módulo OpenDNS/Umbrella Roaming
- Cisco ASA

Componentes Utilizados

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

- Cisco ASA versión 9.3(3)7
- Cisco AnyConnect Secure Mobility Client 4.3.01095
- Módulo OpenDNS Roaming 4.3.01095
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 o posterior
- Microsoft Windows 8.1
- **Nota:** Los requisitos mínimos para implementar el módulo OpenDNS Umbrella son:
  - AnyConnect VPN Client Versión 4.3.01095 o posterior
  - Cisco ASDM 7.6.2 o posterior
  El módulo de roaming de OpenDNS actualmente no es compatible con las plataformas Linux.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red es en vivo, asegúrese de conocer el impacto potencial de todos los comandos o de todas las configuraciones.

Antecedentes

Orginfo.json

Para que el módulo de roaming de OpenDNS funcione correctamente, debe descargarse el archivo OrgInfo.json desde el tablero de OpenDNS o transmitirse desde ASA antes de utilizarse. Cuando se descarga primero el archivo, se guarda en una ruta específica que depende del sistema operativo.

Para Mac OS X, OrgInfo.json se descarga en /opt/cisco/anyconnect/Umbrella.
Para Microsoft Windows, OrgInfo.json se descarga en C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella.

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

Como se muestra, el archivo utiliza la codificación UTF-8 y contiene un Id. de organización, una huella digital y un Id. de usuario. El Id. de organización representa la información de la organización del usuario actualmente registrado en el tablero de OpenDNS. El Id. de organización es estático, único y se autogenera mediante OpenDNS para cada organización. La huella digital se utiliza para validar el archivo Orginfo.json durante el registro del dispositivo y la ID de usuario representa una ID única para el usuario que inició sesión.

Cuando el módulo de roaming se inicia en Windows, el archivo OrgInfo.json se copia en el directorio de datos, en el directorio Umbrella y se utiliza como copia en funcionamiento. En MAC

OS X, la información de este archivo se guarda en updater.plist en el directorio de datos dentro del directorio de Umbrella. Una vez que el módulo lee con éxito la información del archivo OrgInfo.json, intenta registrarse con OpenDNS mediante una API de nube. Este registro hará que OpenDNS asigne una ID de dispositivo única a la máquina que intentó realizar el registro. Si una ID de dispositivo de un registro previo ya está disponible, el dispositivo omitirá el registro.

Una vez que se completa el registro, el módulo de roaming realiza una operación de sincronización para recuperar la información de la política para el terminal. Se necesita una ID de dispositivo para la operación de sincronización. Los datos de sincronización incluyen syncInterval, dominios de omisión internos y direcciones IP, entre otras cosas. El intervalo de sincronización es la cantidad de minutos después de que el módulo intenta resincronizar.

Comportamiento de sondeo de DNS

Una vez que se registra y sincroniza correctamente, el módulo de roaming envía sondeos del sistema de nombres de dominio (DNS) a los resolutores locales. Estas solicitudes de DNS incluyen consultas TXT para debug.opendns.com. Según la respuesta, el cliente puede determinar si existe una máquina virtual (MV) OpenDNS en la instalación dentro de la red.

Si hay un dispositivo virtual (VA) presente, el cliente pasa al modo ‘detrás del VA’ y no se lleva a cabo la aplicación del DNS en el terminal. El cliente se basa en la MV para la aplicación de DNS a nivel de red.

Si no hay MV, el cliente envía una solicitud de DNS a los resolvers de OpenDNS públicos (208.67.222.222) a través de UDP/443.

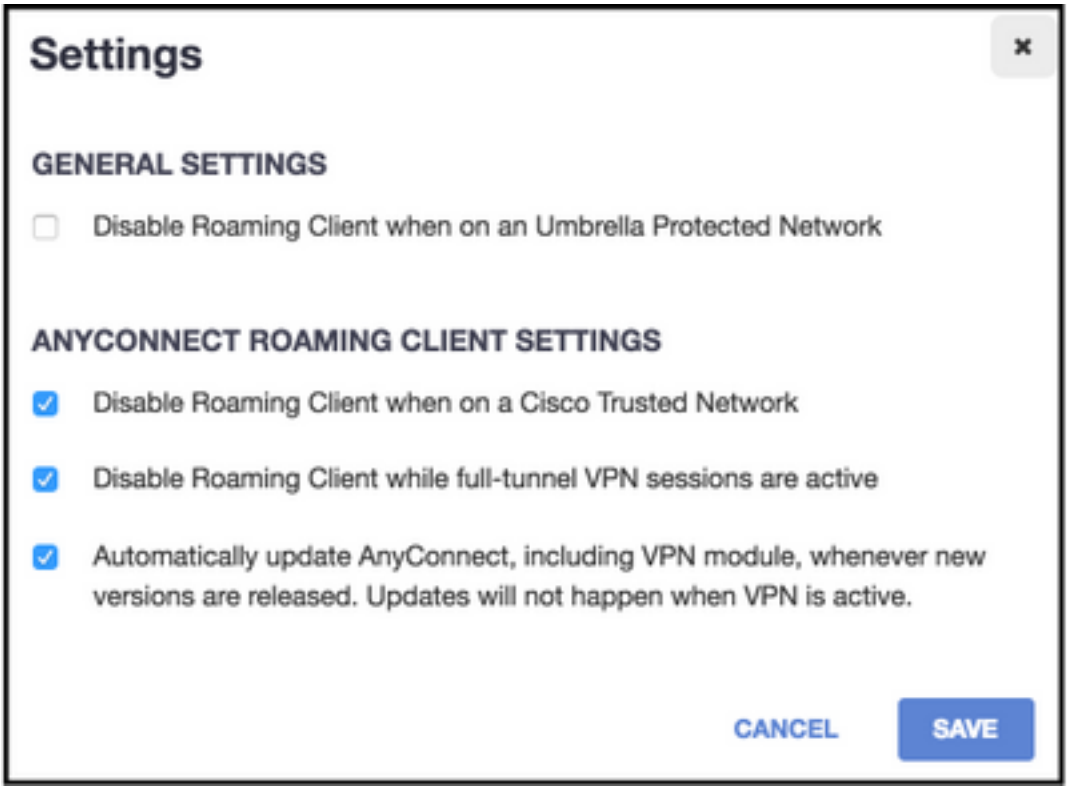
Una respuesta positiva indica que el cifrado de DNS es posible. Si se recibe una respuesta negativa, el cliente envía una solicitud de DNS a los resolvers OpenDNS públicos a través de UDP/53.

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

Cuando recibe un número determinado de respuestas negativas, el cliente pasa al estado de falla de apertura. Un estado falla-abierto indica que el cifrado o la protección de DNS no es posible. Una vez que el módulo Roaming se ha cambiado correctamente a un estado protegido y/o cifrado, todas las consultas DNS para dominios de búsqueda fuera de los dominios de búsqueda locales y dominios de omisión internos se envían a los resolvers OpenDNS para la resolución de nombres. Con el estado cifrado habilitado, todas las transacciones DNS son encriptadas por el proceso dnscrypt.

Comportamiento de DNS con modos túnel AnyConnect

1. Tunnel-All (o tunnel-all-DNS habilitado)



> **Nota:** Como se muestra, el comportamiento predeterminado del módulo de roaming es inhabilitar la protección del DNS mientras se activa un túnel de VPN con la configuración completa. Para que el módulo esté activo durante una configuración tunnel-all de AnyConnect, la **opción Disable roaming client while full-tunnel VPN sessions are active (Deshabilitar cliente roaming mientras haya sesiones VPN full-tunel activas) debe estar deshabilitada en el portal OpenDNS.** La posibilidad de habilitar esta función requiere un nivel de suscripción avanzado con OpenDNS. La siguiente información asume que la protección del DNS mediante el módulo de roaming está habilitada.

El dominio consultado forma parte de la lista de omisión interna

Las solicitudes de DNS que se originan en el adaptador de túnel están permitidas y se envían a los servidores DNS de túnel a través del túnel VPN. La consulta permanecerá sin resolver si los servidores DNS de túnel no la pueden resolver.

El dominio consultado no forma parte de la lista de omisión interna

Las solicitudes de DNS que se originan desde el adaptador de túnel están permitidas y serán procesadas a los resolvers OpenDNS públicos a través del módulo de Roaming y se enviarán a través del túnel VPN. Para el cliente DNS parecerá que la resolución del nombre se realizó a través del servidor DNS del VPN. Si la resolución del nombre mediante los resolutores de OpenDNS no es exitosa, el módulo de roaming conmuta por error a los servidores del DNS localmente configurados, comenzando por el adaptador de VPN (que es el adaptador preferido cuando el túnel está activado).

2. Split-DNS (tunnel-all-DNS deshabilitado)

> **Nota:** Todos los dominios split-DNS se agregan automáticamente a la lista de omisión interna del módulo Roaming cuando se establece el túnel. Esto se hace para proporcionar un mecanismo de manejo constante del DNS entre AnyConnect y el módulo de roaming.

Asegúrese de que en una configuración split-DNS (con tunelización split-include) los resolvers OpenDNS públicos no estén incluidos en las redes split-include.

Nota: En Mac OS X, si el DNS dividido se habilita para ambos protocolos IP (IPv4 e IPv6) o se habilita solamente para un protocolo y no se configura ningún grupo de direcciones para el otro protocolo, se aplica el verdadero DNS dividido, similar a Windows.
Si split-DNS está habilitado solo para un protocolo y se asigna una dirección de cliente para el otro protocolo, solo se aplica el último recurso de DNS para la tunelización dividida. Esto significa que AnyConnect solo permite las solicitudes del DNS que coinciden con los dominios del DNS dividido a través del túnel (AC responde otras solicitudes negándose a aplicar la conmutación por error a los servidores de DNS públicos), pero no puede impedir el envío sin cifrar de las solicitudes que coinciden con los dominios del DNS dividido a través del adaptador público.

El dominio consultado forma parte de la lista de omisión interna y también forma parte de los dominios split-DNS

Las solicitudes de DNS que se originan en el adaptador de túnel están permitidas y se envían a los servidores DNS de túnel a través del túnel VPN. El controlador de AnyConnect responde el resto de las solicitudes de coincidencia de los dominios de otros adaptadores con ‘no existe dicha denominación’ para lograr un verdadero DNS dividido (evitando la demora del DNS). Por lo tanto, sólo el tráfico de DNS sin túnel está protegido por el módulo Roaming.

El dominio consultado forma parte de la lista de omisión interna, pero no forma parte de los dominios de DNS dividido

Las solicitudes de DNS que se originan en el adaptador físico están permitidas y se envían a los servidores DNS públicos, fuera del túnel VPN. El controlador de AnyConnect responde el resto de las solicitudes de coincidencia de los dominios del adaptador del túnel con ‘no existe dicha denominación’ para evitar el envío de la consulta a través del túnel de VPN.

El dominio consultado no forma parte de la lista de omisión interna ni de los dominios DNS divididos

Las solicitudes de DNS que se originan en el adaptador físico están permitidas y serán procesadas a los resolvers OpenDNS públicos y se enviarán fuera el túnel VPN. Para el cliente DNS parecerá que la resolución del nombre se realizó a través del servidor DNS. Si la resolución del nombre mediante los resolutores de OpenDNS no es exitosa, el módulo de roaming conmuta por error a los servidores del DNS localmente configurados, excepto los que están configurados en el adaptador de VPN. El controlador de AnyConnect responde el resto de las solicitudes de coincidencia de los dominios del adaptador del túnel con ‘no existe dicha denominación’ para evitar el envío de la consulta a través del túnel de VPN.

3. Tunelización con Split incluido y no incluido (no split-DNS y tunnel-all-DNS deshabilitados)

El dominio consultado forma parte de la lista de omisión interna

El resolver nativo del SO realiza una resolución de DNS según el orden de los adaptadores de red, y AnyConnect es el adaptador preferido cuando el VPN está activo. Las solicitudes de DNS se originan primero en el adaptador del túnel y se envían a los servidores DNS de túnel a través del túnel VPN. Si la consulta no puede se resuelta por los servidores DNS de túnel, el resolver del

SO intentará resolverla a través de los servidores DNS públicos.

El dominio consultado no forma parte de la lista de omisión interna

El resolver nativo del SO realiza una resolución de DNS según el orden de los adaptadores de red, y AnyConnect es el adaptador preferido cuando el VPN está activo. Las solicitudes de DNS se originan primero en el adaptador del túnel y se envían a los servidores DNS de túnel a través del túnel VPN. Si la consulta no puede se resuelta por los servidores DNS de túnel, el resolver del SO intentará resolverla a través de los servidores DNS públicos.

Si los resolutores públicos de OpenDNS son parte de la lista dividida incluida o no forman parte de la lista dividida excluida, la solicitud con proxys se envía a través del túnel de VPN.

Si los resolutores públicos de OpenDNS no son parte de la lista dividida incluida o forman parte de la lista dividida excluida, la solicitud con proxys se envía por fuera del túnel de VPN.

Si la resolución del nombre mediante los resolutores de OpenDNS no es exitosa, el módulo de roaming conmuta por error a los servidores del DNS localmente configurados, comenzando por el adaptador de VPN (que es el adaptador preferido cuando el túnel está activado). Si la respuesta final devuelta por el módulo de roaming (enviada por proxy al cliente DNS nativo) no es exitosa, el cliente nativo probará otros servidores del DNS, si están disponibles.

Instalar y configurar el Módulo Umbrella Roaming

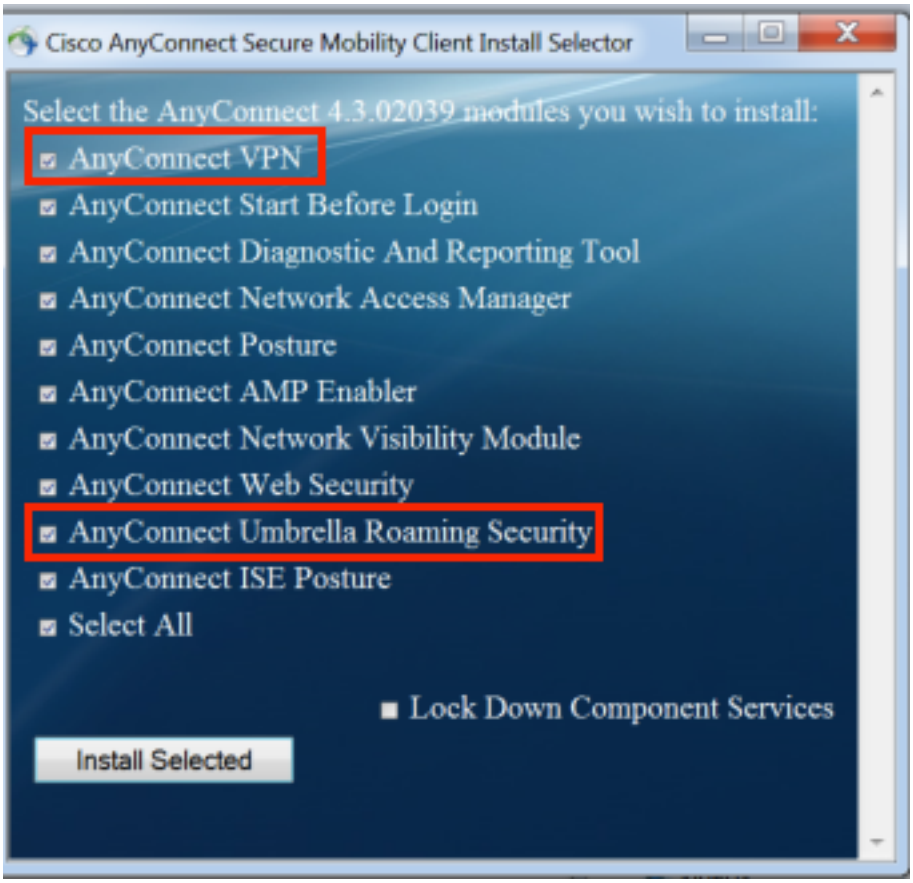
Con el fin de integrar el módulo OpenDNS Roaming con el cliente AnyConnect del VPN, el módulo se debe instalar ya sea por el método de implementación previa o implementación web:

Método antes de la implementación (manual)

La preimplementación requiere la instalación manual del módulo de roaming de OpenDNS y el copiado del archivo OrgInfo.json en la máquina del usuario. Las implementaciones a gran escala generalmente se logran con los sistemas de administración de software (SMS) empresariales.

Implementar el Módulo OpenDNS Roaming

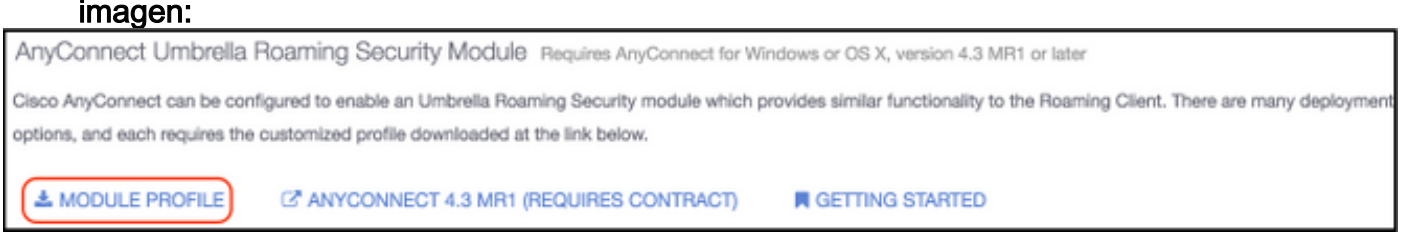
Durante la instalación del paquete de AnyConnect, elija los módulos **VPN de AnyConnect y Seguridad de roaming de AnyConnect Umbrella:**



Implementar Orginfo.json

Para descargar el archivo OrgInfo.json, complete los siguientes pasos:

1. Inicie sesión en el tablero de OpenDNS.
2. Seleccione **Configuration > Identities > Roaming Computers (Configuración > Identidades > Computadoras en roaming).**
3. Haga clic en el signo +.
4. Desplácese hacia abajo y seleccione **Module Profile (Perfil del módulo) en la sección Módulos de seguridad de roaming de Anyconnect Umbrella, como se muestra en esta imagen:**



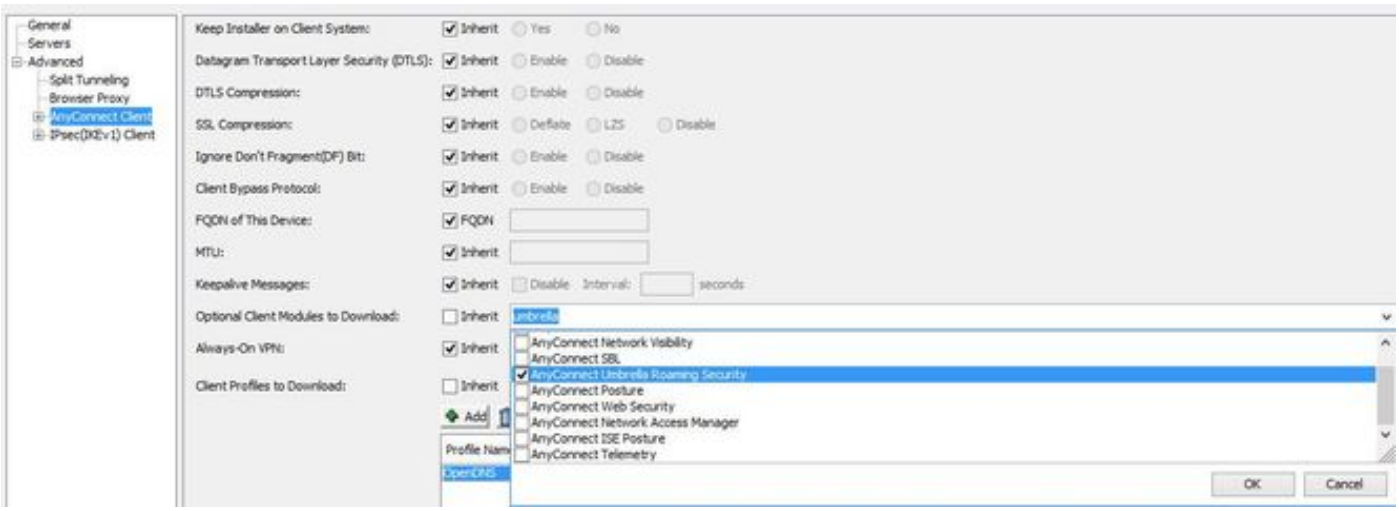
Una vez que el archivo se descarga, debe guardarse en una de estas rutas, que dependen del sistema operativo.

Para Mac OS X: /opt/cisco/anyconnect/Umbrella
Para Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

Método de implementación web

Implementar el Módulo OpenDNS Roaming

Descargue el paquete de cliente de Anyconnect Security Mobility (es decir, anyconnect-win-4.3.02039-k9.pkg) del sitio web de Cisco y cárguelo en la memoria flash de ASA. Una vez cargado, en ASDM, elija **Group Policy > Advanced > AnyConnect Client > Optional Client Modules to Download (Política de grupo > Avanzada > Cliente AnyConnect > Módulos de clientes opcionales para descargar) y seleccione Umbrella Roaming Security (Seguridad de roaming de Umbrella).**

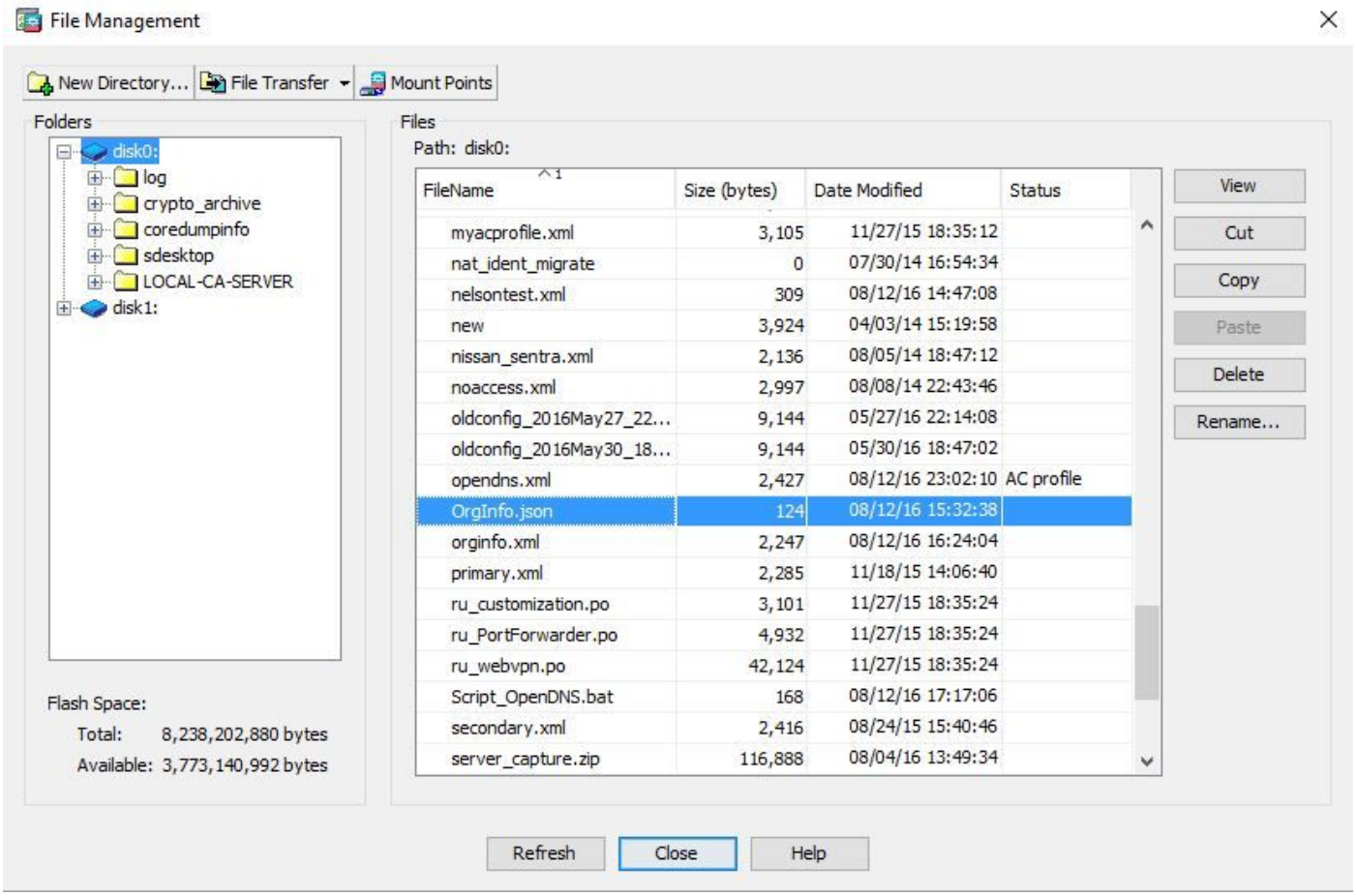


CLI equivalente

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

Implementar Orginfo.json

1. Descargue el archivo OrgInfo.json del tablero de OpenDNS y cárguelo en la memoria flash de ASA.



2. Configurar ASA para trasladar el archivo OrgInfo.json a terminales remotas.

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

> **Nota:** Esta configuración solo puede realizarse con la CLI. Para poder utilizar ASDM para esta tarea, se debe reinstalar la versión 7.6.2 o posterior de ASDM en ASA.

Una vez que el cliente de roaming de Umbrella está instalado a través de uno de los métodos analizados, debe aparecer como módulo integrado dentro de la GUI de AnyConnect tal y como se muestra en esta imagen:

Hasta que no se implemente el archivo Orginfo.json en la terminal y en la ubicación correcta, el módulo Umbrella Roaming no se iniciará.

Configurar

La sección muestra ejemplos de los fragmentos de configuración de CLI necesarios para operar el módulo OpenDNS Roaming con los diferentes módulos de 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




        (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.

Troubleshoot

Los pasos para solucionar los problemas asociados a AnyConnect con OpenDNS son:

1. Asegúrese de que el módulo de seguridad de roaming de Umbrella esté instalado junto con el cliente de movilidad segura de Anyconnect.
2. Asegúrese de que OrgInfo.json esté presente en el terminal en la ruta correcta en función del sistema operativo y de que tenga el formato especificado en este documento.
3. Si las consultas del DNS para los resolutores de OpenDNS deben pasar por el túnel de VPN de AnyConnect, asegúrese de configurar la horquilla en ASA para permitir la accesibilidad a los resolutores de OpenDNS.
4. Recopile las capturas de paquetes (sin filtros) en el adaptador virtual y el adaptador físico de AnyConnect simultáneamente y anote los dominios que no se pueden resolver.
5. Si el módulo de roaming actúa en estado cifrado, recopile las capturas de paquetes después de bloquear el UDP 443 localmente (solo a fines de solucionar los problemas). De esta manera podrá ver las transacciones del DNS.
6. Ejecute DART en AnyConnect y los diagnósticos de Umbrella y anote el momento en que falla el DNS. Vea Cómo recopilar el paquete DART para Anyconnect a fin de obtener más información.
7. Recopile registros de diagnóstico de Umbrella y envíe la URL resultante a su administrador de OpenDNS. Solo usted y el administrador de OpenDNS tienen acceso a esta información.
   Para Windows: C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   Para Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Información Relacionada

- **Id. de errorCSCvb34863 de Cisco: Latencia en la resolución de DNS cuando AnyConnect está configurado para la tunelización split-include.**
- Soporte Técnico y Documentación - Cisco Systems