Gestionar la compatibilidad de VPN y Umbrella Roaming Client

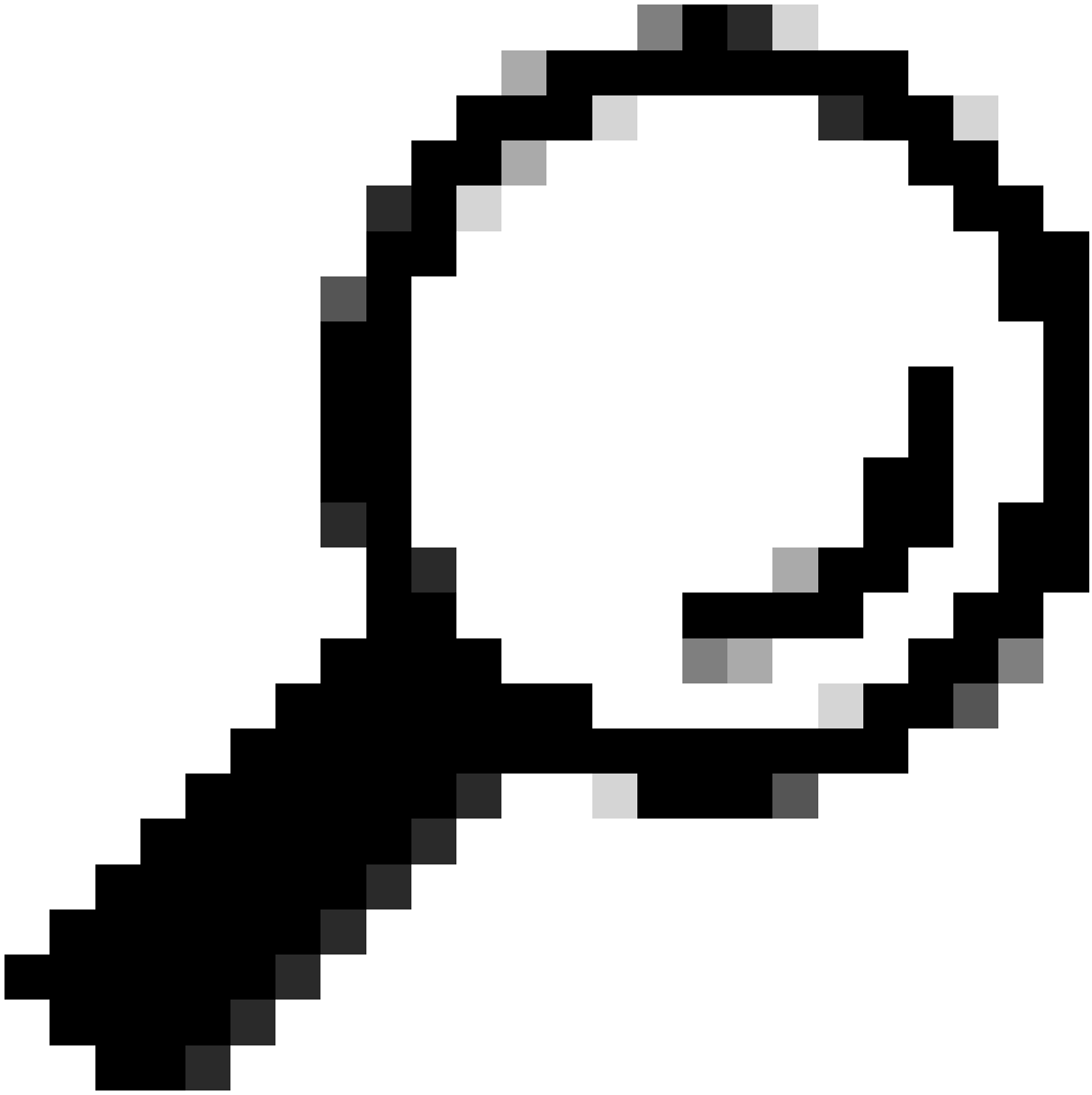
Contenido

Introducción

Este documento describe la interacción y compatibilidad de Cisco Umbrella Roaming Client con varios programas de VPN.

Overview

Cisco Umbrella Roaming Client funciona con la mayoría del software VPN, pero se pueden requerir pasos adicionales para el funcionamiento esperado. Cisco Umbrella recomienda implementar el módulo Cisco Secure Client y Roaming Security para obtener la máxima compatibilidad. Este módulo se puede implementar sin los componentes VPN.



Consejo: Este documento sirve como guía general y no sirve como una lista oficial de software soportado. Cisco Umbrella no prueba, valida ni certifica la funcionalidad con ningún software de terceros o cliente VPN.

Este documento proporciona información técnica y contexto adicional para clientes VPN específicos que pueden requerir configuraciones adicionales. Para obtener una lista de software de VPN incompatible conocido, consulte la sección Incompatibilidades de Umbrella Roaming Client. La incompatibilidad de DNS con el cliente de roaming también puede hacer que el módulo Cisco Secure Client + Roaming Security con SWG falle, ya que el cliente SWG también depende del establecimiento correcto de una conexión DNS.

Cómo Umbrella Roaming Client Funciona con los Clientes VPN

El cliente de roaming de Umbrella se enlaza a todos los adaptadores de red y cambia la configuración DNS del equipo a 127.0.0.1 (localhost). Esto permite que el cliente de roaming de Umbrella reenvíe todas las consultas DNS directamente a Umbrella, a la vez que permite la resolución de dominios locales a través de la función Dominios internos. Al establecer una conexión con un servidor VPN, el cliente de roaming de Umbrella detecta una nueva conexión de red en el sistema y cambia la configuración de DNS de la conexión para que apunte al cliente de roaming de Umbrella. El cliente de roaming de Umbrella se basa en realizar búsquedas de DNS en direcciones IP de Umbrella AnyCast DNS (208.67.222.222/208.67.220.220).

Si un usuario se conecta a una VPN, el firewall asociado a la VPN debe permitir el acceso a Umbrella.

Incompatibilidades de Umbrella Roaming Client

Actualmente, el cliente de roaming de Umbrella ofrece aplicación de capa DNS. La capa DNS es la función principal del cliente de roaming, ya que aplica políticas de seguridad basadas en DNS en cualquier red. Esta función del cliente de roaming puede experimentar incompatibilidades de software conocidas. La capa DNS del cliente de roaming de Umbrella no es compatible con los clientes enumerados a continuación, según las pruebas del equipo de soporte. Cisco Umbrella Engineering no verifica ni prueba estos clientes, y todas las entradas están sujetas a revisión. Este artículo hace referencia al cliente de roaming independiente de Umbrella. Para ver un artículo adicional sobre el módulo de seguridad Umbrella Roaming Security Module para Cisco Secure Client (y productos antiguos), consulte la documentación pertinente.

Cliente VPN	Problema/Incompatibilidad	Resolución
Pulso seguro	Al desconectarse, el DNS local guardado puede seguir siendo valores de VPN en lugar de valores WiFi/Ethernet debido a la modificación de impulsos durante la conexión VPN.	Se resuelve con el módulo Umbrella, incluido en la mayoría de las licencias.
VPN de Avaya	Incompatible.	Se resuelve con el módulo Umbrella, incluido en la mayoría de las licencias.
VPN con Windows (especialmente VPN siempre activa)	Puede dar lugar a que el DNS local no pueda resolver la respuesta interna a pesar de que los nombres de host DNS estén en la lista de dominios internos.	Se resuelve con el módulo Umbrella, incluido en la mayoría de las licencias.
"Aplicaciones" de VPN integradas en la plataforma	Estas aplicaciones deben utilizar una API de conexión de Microsoft que requiera que se envíe DNS a la NIC local, no a	Se resuelve con el módulo Umbrella, incluido en la mayoría de las licencias.

Cliente VPN	Problema/Incompatibilidad	Resolución
universal de Windows	127.0.0.1. Por lo tanto, la aplicación muestra un error que indica que no se puede conectar.	
OpenVPN	Incompatible.	No hay soluciones disponibles.
GlobalProtect VPN de Palo Alto	No funciona con ninguna versión de cliente de roaming independiente después de 3.0.110.	Se corrige mediante el módulo Umbrella, incluido en la mayoría de las licencias.
VPN F5	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.
VPN de punto de control	solo macOS, solo modo de túnel dividido.	Inhabilite split-tunnel en macOS.
NetExtender de SonicWall	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.
VPN Zscaler	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.
Protección de terminales de Akamai (ETPclient)	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.
NordVPN	Utilice una solución alternativa.	Existen dos opciones para agregar compatibilidad: 1. Utilice el método de conexión OpenVPN como se describe en Cómo configurar una conexión manual en Windows con OpenVPN 2. Permitir DNS

Cliente VPN	Problema/Incompatibilidad	Resolución
		personalizado en configuración avanzada. Establezca DNS en 208.67.220.220 y 208.67.222.222.
VPN de Azure	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.
VPN AWS	Utilice una solución alternativa.	Edite el archivo de configuración (descargado de AWS manualmente) para tener una segunda línea de`pull-filter ignore "block-outside-dns"`.
VPN Pritunl	Incompatible.	Corregido por el módulo Umbrella, incluido en la mayoría de las licencias.

Razones de incompatibilidad para clientes VPN

Algunos clientes VPN tienen un comportamiento DNS similar al del cliente de roaming de Umbrella. Si el servidor DNS de la conexión VPN cambia a un valor inesperado, el software VPN cambia la configuración DNS del sistema al valor establecido por la VPN cuando se conectó inicialmente. El cliente de roaming de Umbrella también realiza la misma operación, cambiando cualquier servidor DNS de nuevo a 127.0.0.1. Este comportamiento de ida y vuelta crea un conflicto entre la VPN y el cliente de roaming de Umbrella. Este conflicto provoca un ciclo interminable de los servidores DNS para el restablecimiento de la conexión VPN. El cliente de roaming detecta esto y se inhabilita para mantener la conexión VPN si es posible.

Dispositivos virtuales y redes protegidas

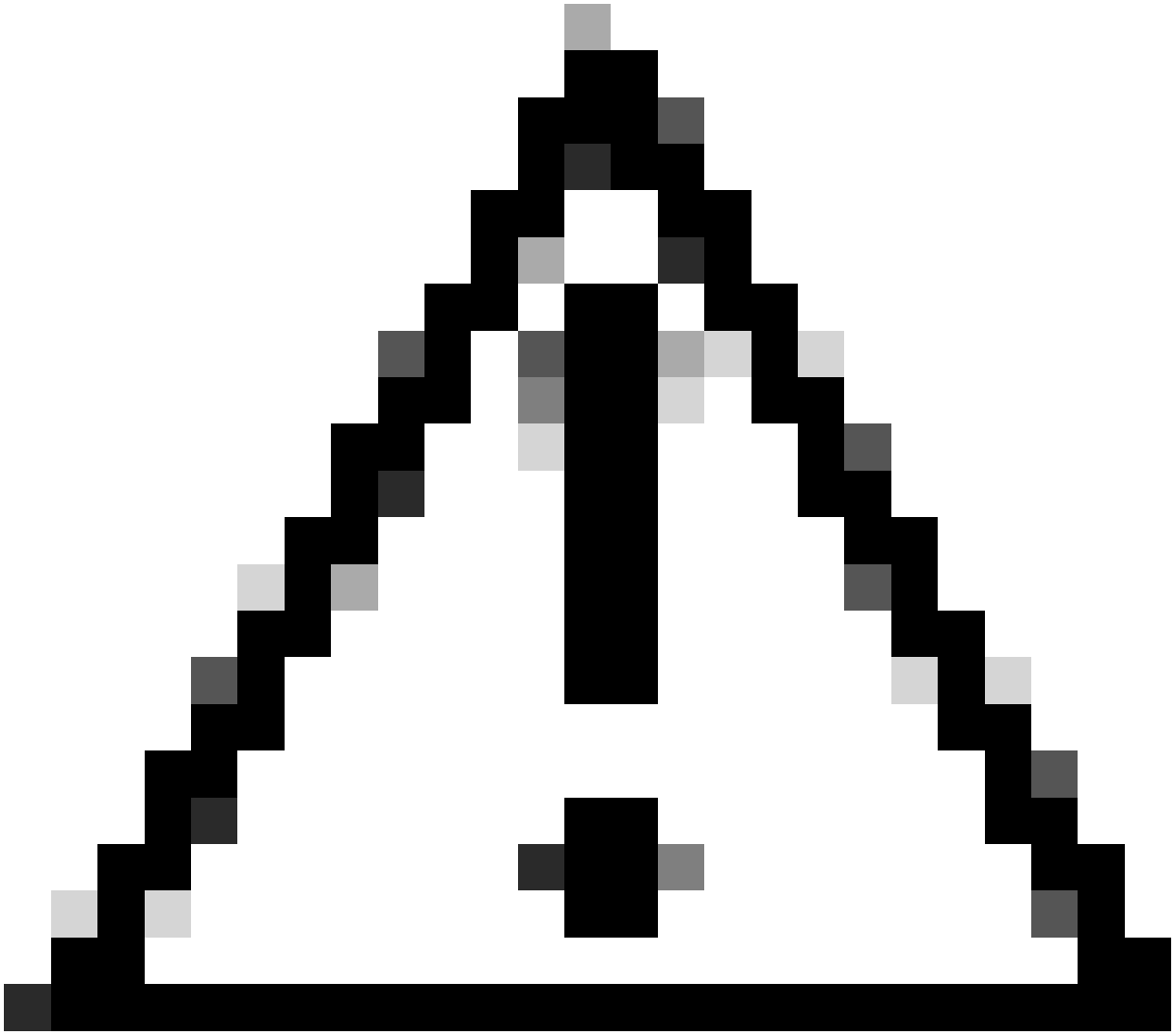
El cliente de roaming de Umbrella se comporta de forma diferente cuando se conecta a una red que utiliza la función de dispositivos virtuales de Umbrella (VA) o redes protegidas. Esto se aplica tanto si un usuario se conecta a la red localmente como a través de una VPN. Para obtener más información, consulte la documentación de Roaming Client and Virtual Appliances o Redes protegidas.

Consideraciones especiales para el módulo de seguridad de

roaming + cliente seguro de Cisco e independiente

La información proporcionada aquí es específica para el cliente de roaming independiente de Umbrella y no se extiende al módulo Cisco Secure Client (CSC) + Roaming Security. Los usuarios que busquen una instalación sencilla de complementos pueden utilizar Umbrella Roaming integrado en CSC. Los usuarios de Cisco Secure Client VPN deben migrar al módulo CSC + Roaming Security si se produce un problema funcional con la VPN. Cisco Umbrella requiere validación en el módulo de seguridad CSC + Roaming y recomienda una migración completa.

El software Cisco Secure Client VPN proporciona opciones sobre cómo el sistema maneja DNS cuando se establece una conexión VPN. Consulte el artículo Diferencias de comportamiento con respecto a las consultas DNS y la resolución de nombres de dominio en diferentes sistemas operativos para obtener detalles adicionales. Esta información se basa en la experiencia con Cisco Secure Client y Umbrella Roaming Client. Se recomienda probar el cliente de roaming de Umbrella con Cisco Secure Client VPN habilitado para garantizar las funciones de resolución de DNS internas y externas según lo esperado.



Precaución: Cisco requiere que utilice el módulo CSC + Roaming Security si también utiliza Cisco Secure Client para la compatibilidad del servicio DNS. Los pasos proporcionados son para el cliente de roaming no integrado sólo si es necesario. Estos pasos no son necesarios para el módulo CSC + Roaming Security.

Tanto en el modo de túnel completo como en el modo de túnel dividido, se requieren instrucciones especiales para permitir que el cliente de roaming funcione mientras Cisco Secure Client está conectado. Esto es necesario para permitir que DNS fluya al cliente de roaming en lugar de ser reemplazado por el controlador del núcleo. Para el túnel completo, el síntoma es que el cliente se ve obligado a inhabilitar. Para la tunelización dividida, el síntoma es una pérdida de DNS interno mientras está conectado a la VPN.

Orden de vinculación de DNS Modo de compatibilidad de VPN para Windows 10 y 11

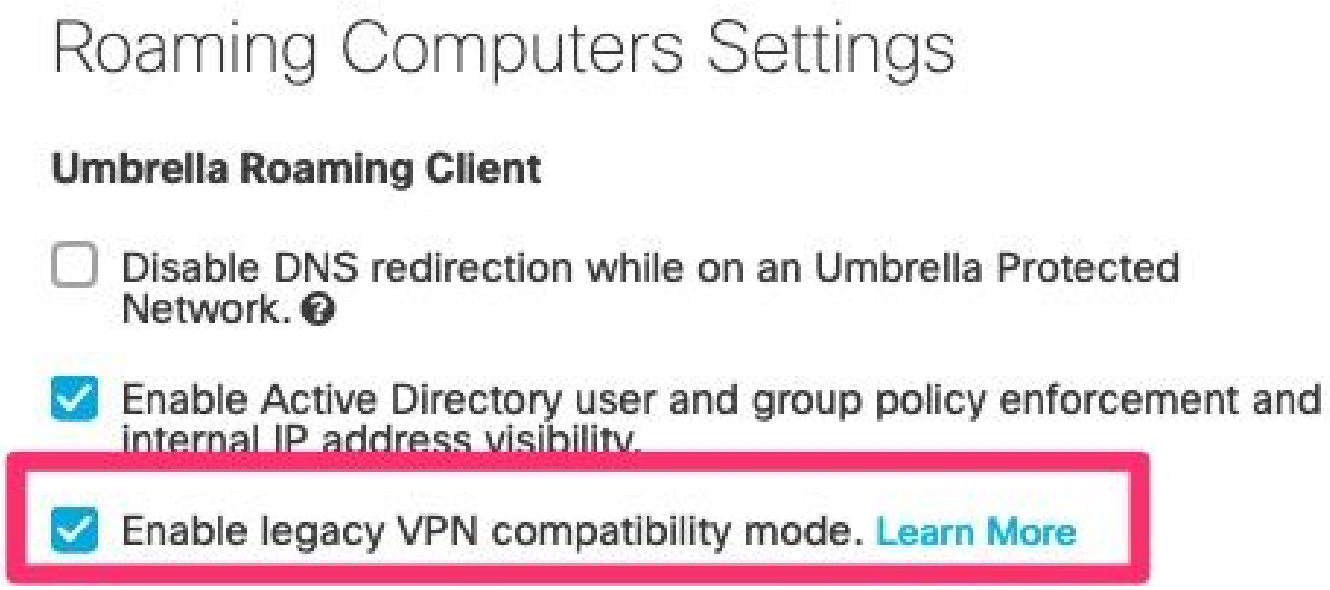
Un conjunto limitado de usuarios de Windows 10 encuentra un problema específico en el que se da prioridad a la LAN local en lugar de a la NIC VPN para DNS. En este caso, el DNS local en la

lista de dominios internos para el cliente de roaming no se puede resolver mientras el DNS público funciona sin problemas. Esto afecta a las versiones 2.0.338 y 2.0.341 (de forma predeterminada) y a todas las versiones posteriores. El problema no ocurrió en la versión 2.0.255.

Los clientes VPN anteriormente afectados incluyen:

- AnyConnect 3.x
- AnyConnect 4.x (AnyConnect Umbrella o CSC + módulo de roaming no se ve afectado)
- VPN de Sophos
- Algunas configuraciones de Palo Alto GlobalProtect en versiones anteriores
- VPN móvil WatchGuard
- Shrew Soft VPN
- VPN Barracuda

Resolución
Cambie la configuración del cliente de roaming Habilitar el modo de compatibilidad VPN heredado a habilitado.



360027547111

Para confirmar si éste es el problema, ejecute la prueba de diagnóstico y haga clic en los resultados de`resolv.confs`. Si el adaptador VPN aparece primero, el problema no afecta al usuario. Si el adaptador VPN aparece en segundo lugar, el problema puede afectar al usuario.

Ejemplo de resultado resolv.confs

```
Results for: resolv.confs
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1
```

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

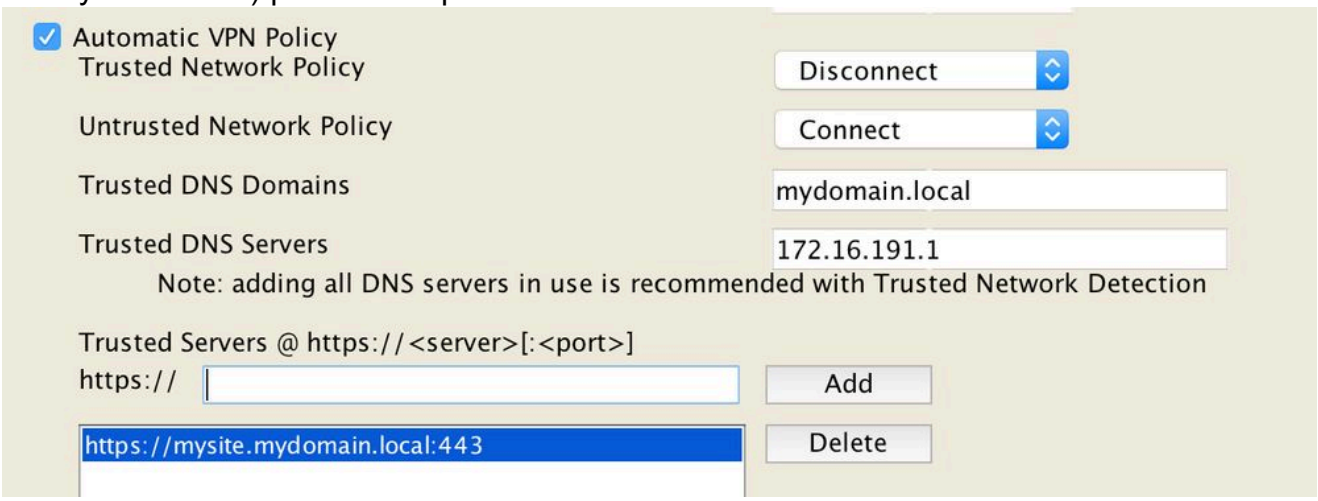
Consideraciones especiales para VPN de terceros

VPN siempre activa

El cliente de roaming independiente no es compatible con la configuración VPN Always On de Cisco Secure Client cuando se definen los servidores DNS de confianza. Cuando está activo, el cliente de roaming independiente siempre establece DNS en 127.0.0.1, lo que elimina todos los servidores DNS de confianza de la configuración NIC. El cliente de roaming se puede inhabilitar en la red para restaurar la configuración DHCP; sin embargo, todas las protecciones relacionadas con el cliente de roaming cesan cuando se configuran. Póngase en contacto con el servicio de asistencia de Umbrella para obtener más información sobre cómo desactivar el cliente en una red de confianza.

Soluciones

- El módulo de seguridad CSC + Roaming (cliente de roaming para Cisco Secure Client) no se ve afectado y funciona de manera eficaz con una política de VPN automática.
- Agregue 127.0.0.1 a la lista de servidores DNS de confianza.
- Asegúrese de que se han definido métodos alternativos de detección de confianza (nombres DNS y servidores) para evitar que todas las redes se declaren de confianza.



360031250911

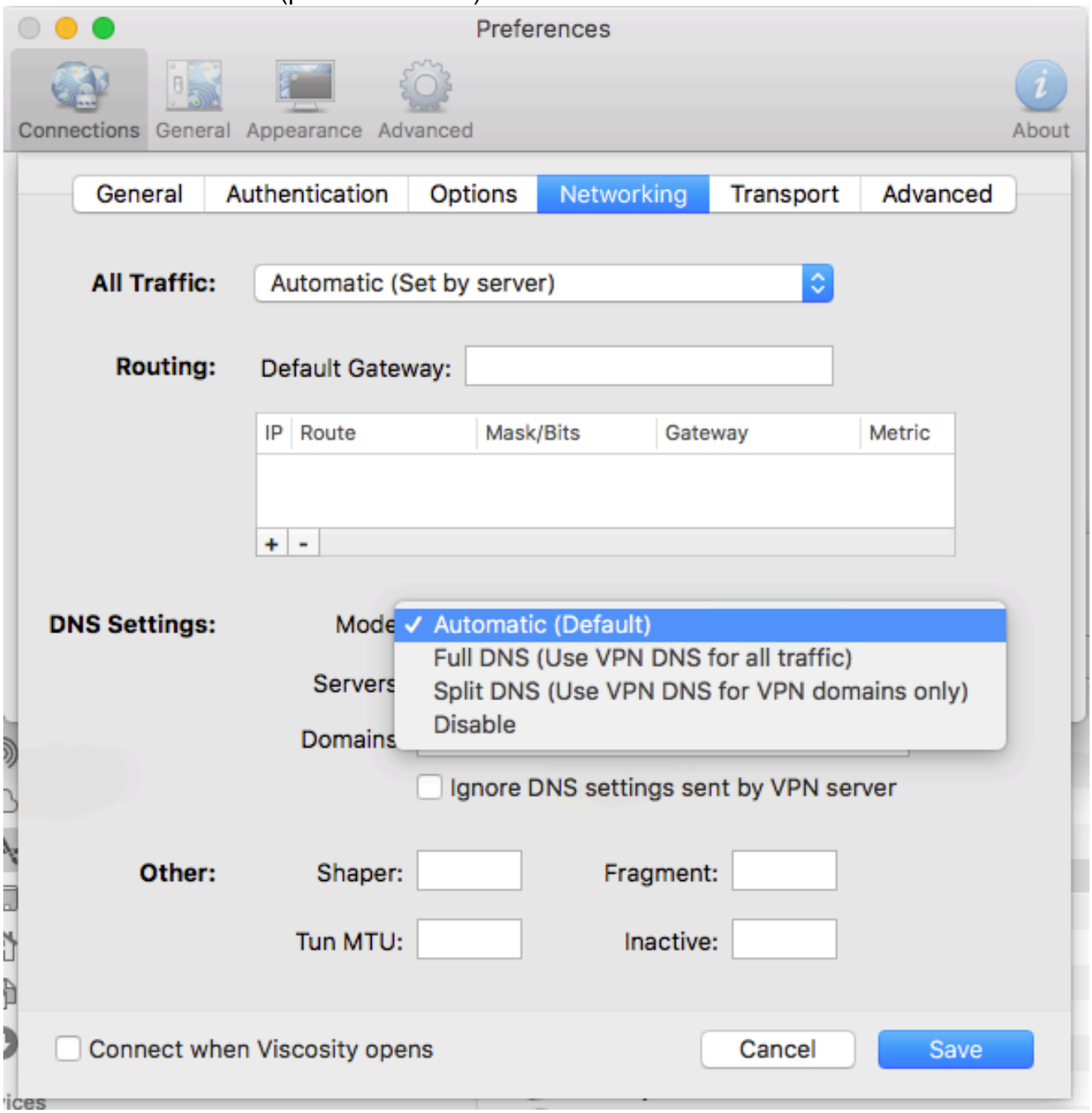
VPN de viscosidad

Viscosity VPN requiere un cambio en la configuración para funcionar con el cliente de roaming de Umbrella. Si no se realiza este cambio, el comportamiento predeterminado de Viscosity imita el de

otras VPN incompatibles. Este cambio indica a Viscosity que utilice la configuración de DNS enviada a través del servidor Umbrella para todos los dominios en el dominio de búsqueda, y 127.0.0.1 se sigue utilizando para cualquier otra solicitud.

Configurar viscosidad

1. En Viscosidad, navegue hasta Preferencias > Conexiones > <su conexión> (específica del sitio) > Redes > Configuración de DNS.
2. Seleccione Automático (predeterminado).



115013433283

Cuando utilice un servidor OpenVPN, asegúrese de que persist-tun no esté habilitado en el lado del servidor para garantizar que los cambios en la red se activan al desconectarse o

reconectarse.

Tunnelblick

Tunnelblick requiere dos cambios para:

- Permite cambiar los servidores DNS del adaptador.
- Aplique la configuración de DNS después de establecer el túnel.

Al garantizar la configuración proporcionada en el menú Advanced, Tunnelblick funciona con Umbrella Roaming Client:

En la ficha Conexión y desconexión, habilite estas dos opciones:

- Vaciar la caché DNS después de conectar o desconectar (predeterminado)
- Establecer DNS después de establecer rutas en lugar de antes de establecer rutas

En la pestaña Mientras esté conectado, cambie esta configuración a Ignorar:

- DNS: Servers > Cuando cambia al valor anterior a la VPN, Cuando cambia a cualquier otra cosa.

Cuando utilice un servidor OpenVPN, asegúrese de que persist-tun no esté habilitado en el lado del servidor para asegurarse de que los cambios en la red se activan al desconectarse o reconectarse.

Problemas de desconexión de Tunnelblick VPN

Con algunas versiones de Tunnelblick, el cliente de roaming no puede identificar correctamente los servidores DNS internos correctos después de una desconexión de VPN. Si se producen problemas con Dominios internos después de una desconexión de VPN, Umbrella recomienda estos pasos:

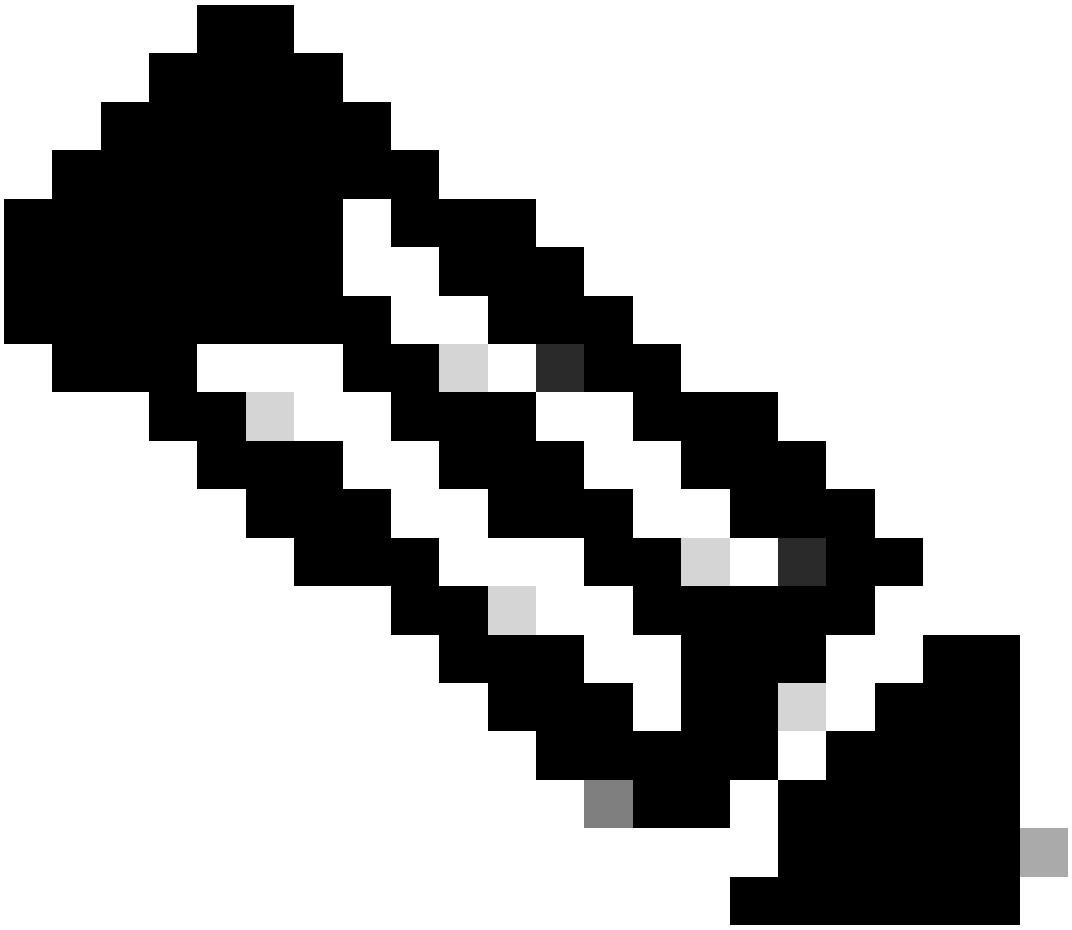
Este cambio hace que Tunnelblick desactive y active la interfaz de red principal después de la desconexión de VPN. Esto se administra en la pestaña Settings del panel de configuración de Tunnelblick:

- En versiones anteriores de Tunnelblick (anteriores a 3.7.5beta03), utilice la casilla de verificación Restablecer la interfaz principal después de desconectar.
- En las versiones más recientes de Tunnelblick (3.7.5beta03 y superiores), establezca los valores de Desconexión esperada On y Desconexión inesperada On en Restablecer interfaz principal.

Cohete Lightspeed

Lightspeed Rocket tiene características seleccionadas que no son compatibles con el cliente de roaming. Específicamente, la modificación de DNS para No SSL Search y la redirección SafeSearch CNAME de `www.google.com` nosslsearch.google.com y forcesafesearch.com respectivamente hace

que toda la resolución www.google.com de DNS falle mientras esté habilitada la redirección de Lightspeed Rocket DNS.



Nota: Este artículo hace referencia al cliente de roaming independiente de Umbrella. Para ver un artículo adicional sobre el módulo de seguridad Umbrella Roaming Security Module para Cisco Secure Client y el software heredado, consulte la documentación pertinente.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).