Examinar el comportamiento de las consultas DNS y la resolución de nombres de dominio

Contenido

Introducción

Este documento describe cómo Cisco OS® maneja las consultas DNS y los efectos en la resolución de nombres de dominio con Cisco AnyConnect y tunelización dividida o completa.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

DNS dividido frente a DNS estándar

Cuando utiliza la tunelización split-include, estas son las tres opciones que tiene para el Sistema de nombres de dominio (DNS):

1. DNS dividido: las consultas de DNS que coinciden con los nombres de dominio se configuran en el dispositivo de seguridad adaptable de Cisco (ASA). Se mueven a través del túnel (a los servidores DNS que se definen en el ASA, por ejemplo) mientras que otros no lo hacen.

2. Tunnel-all-DNS - Solo se permite el tráfico DNS a los servidores DNS que son definidos por el ASA. Esta opción se configura en la directiva de grupo.

3. DNS estándar: todas las consultas DNS se mueven a través de los servidores DNS definidos por el ASA. En el caso de una respuesta negativa, las consultas DNS también pueden dirigirse a los servidores DNS que están configurados en el adaptador físico.

Nota: El comando split-tunnel-all-dns se implementó por primera vez en la versión 8.2(5) de ASA. Antes de esta versión, solo podía dividir DNS o DNS estándar.

En todos los casos, las consultas DNS que se definen para moverse a través del túnel, van a cualquier servidor DNS que sea definido por ASA. Si ASA no ha definido ningún servidor DNS, los parámetros de DNS del túnel estarán vacíos. Si no tiene DNS dividido definido, todas las consultas DNS se envían a los servidores DNS definidos por el ASA. Sin embargo, los comportamientos que se describen en este documento pueden ser diferentes, en función del sistema operativo (SO).

Nota: evite el uso de NSLookup cuando pruebe la resolución de nombres en el cliente. En su lugar, confíe en un navegador o utilice el comando ping. Esto se debe a que NSLookup no depende de la resolución DNS del sistema operativo. AnyConnect no fuerza la solicitud de DNS a través de una interfaz determinada, pero la permite o la rechaza en función de la configuración de DNS dividido. Para obligar a la resolución de DNS a probar un servidor DNS aceptable para una solicitud, es importante que la prueba de DNS dividido sólo se realice con aplicaciones que dependen de la resolución de DNS nativo para la resolución de

---

nombres de dominio (todas las aplicaciones excepto NSLookup, Dig y aplicaciones similares que controlan la resolución de DNS por sí mismas, por ejemplo).

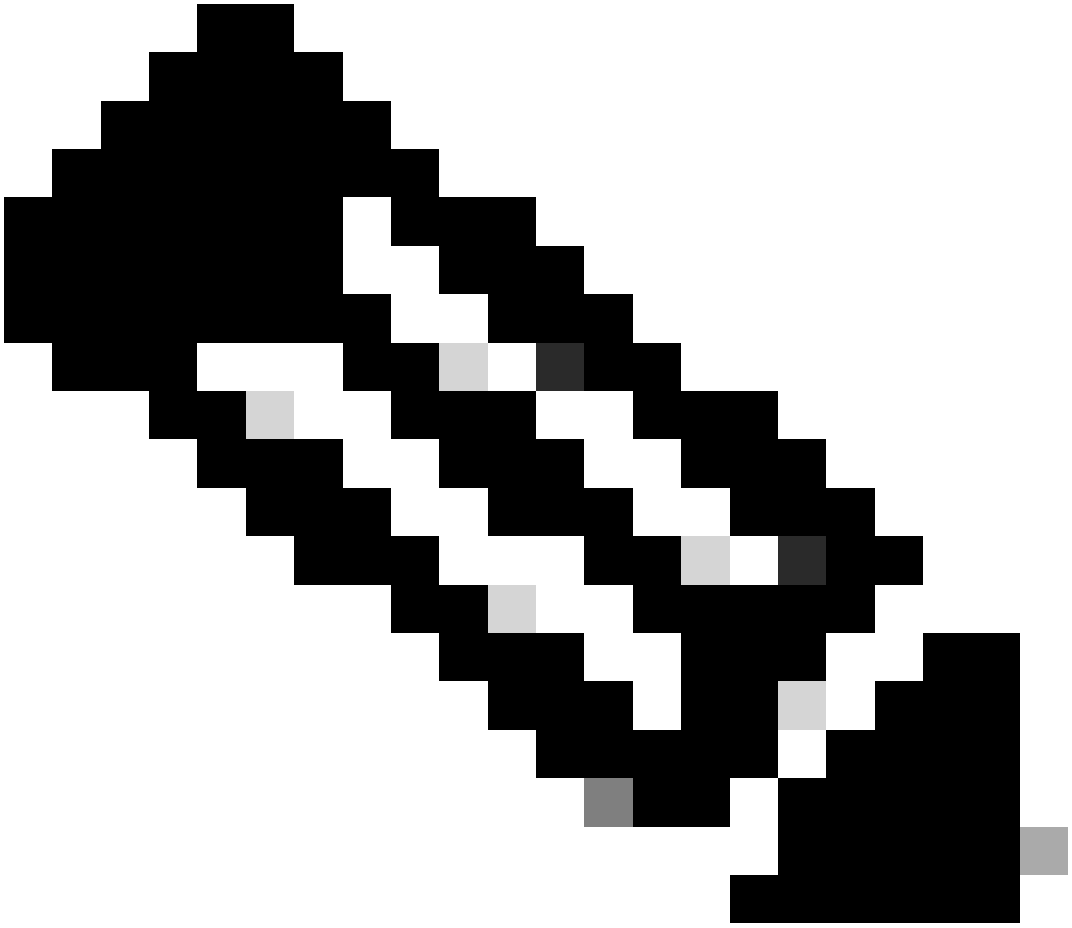
DNS dividido Verdadero frente a Mejor Esfuerzo

La versión 2.4 de AnyConnect admite la reserva de DNS dividido (DNS dividido según el mejor esfuerzo), que no es el verdadero DNS dividido y se encuentra en el cliente IPsec heredado. Si la solicitud coincide con un dominio DNS dividido, AnyConnect permite que la solicitud se tunelice en el ASA. Si el servidor no puede resolver el nombre de host, la resolución de DNS continúa y envía la misma consulta al servidor DNS asignado a la interfaz física.

Por otro lado, si la solicitud no coincide con ninguno de los dominios DNS divididos, AnyConnect no lo tuneliza en el ASA. En su lugar, genera una respuesta DNS para que la resolución de DNS retroceda y envíe la consulta al servidor DNS asignado a la interfaz física. Es por eso que esta función no se llama split DNS, sino DNS fallback para split tunneling. AnyConnect no solo garantiza que solo se tunelizan las solicitudes que tienen como destino dominios DNS divididos, sino que también se basa en el comportamiento de resolución de DNS del sistema operativo del cliente para la resolución de nombres de host.

Esto plantea problemas de seguridad debido a una posible filtración de nombres de dominio privado. Por ejemplo, el cliente DNS nativo puede enviar una consulta para un nombre de dominio privado a un servidor DNS público específicamente cuando el servidor de nombres DNS VPN no pudo resolver la consulta DNS.

Consulte Cisco bug ID CSCtn14578, actualmente resuelto en Microsoft Windows solamente, a partir de la versión 3.0(4235). La solución implementa un verdadero DNS dividido, consulta estrictamente los nombres de dominio configurados que coinciden y se les permite a los servidores DNS VPN. El resto de las consultas sólo se permiten a otros servidores DNS, como los configurados en los adaptadores físicos.



Nota: Solo los usuarios registrados de Cisco tienen acceso a la información y las herramientas internas de Cisco.

Tunnel-all y Tunnel-all DNS

Cuando se inhabilita la tunelización dividida (la configuración Tunnel-all), el tráfico DNS se permite estrictamente a través del túnel. La configuración Tunnel-all DNS (configurada en la política de grupo) envía todas las búsquedas de DNS a través del túnel, junto con algún tipo de tunelización dividida, y el tráfico DNS se permite estrictamente a través del túnel.

Esto es coherente en todas las plataformas con una advertencia en Microsoft Windows: cuando se configura cualquier DNS Tunnel-all o Tunnel-all, AnyConnect permite el tráfico DNS estrictamente a los servidores DNS que se configuran en el gateway seguro (aplicado al adaptador VPN). Se trata de una mejora de la seguridad implementada junto con la solución de DNS dividido verdadero mencionada anteriormente.

Si esto resulta problemático en ciertos escenarios (por ejemplo, las solicitudes de

actualización/registro de DNS se deben enviar a servidores DNS que no sean VPN), siga estos pasos:

1. Si la configuración actual es Tunnel-all, habilite split-exclude tunneling . Cualquier red de un solo host y excluida dividida es aceptable para su uso, como una dirección local de link.

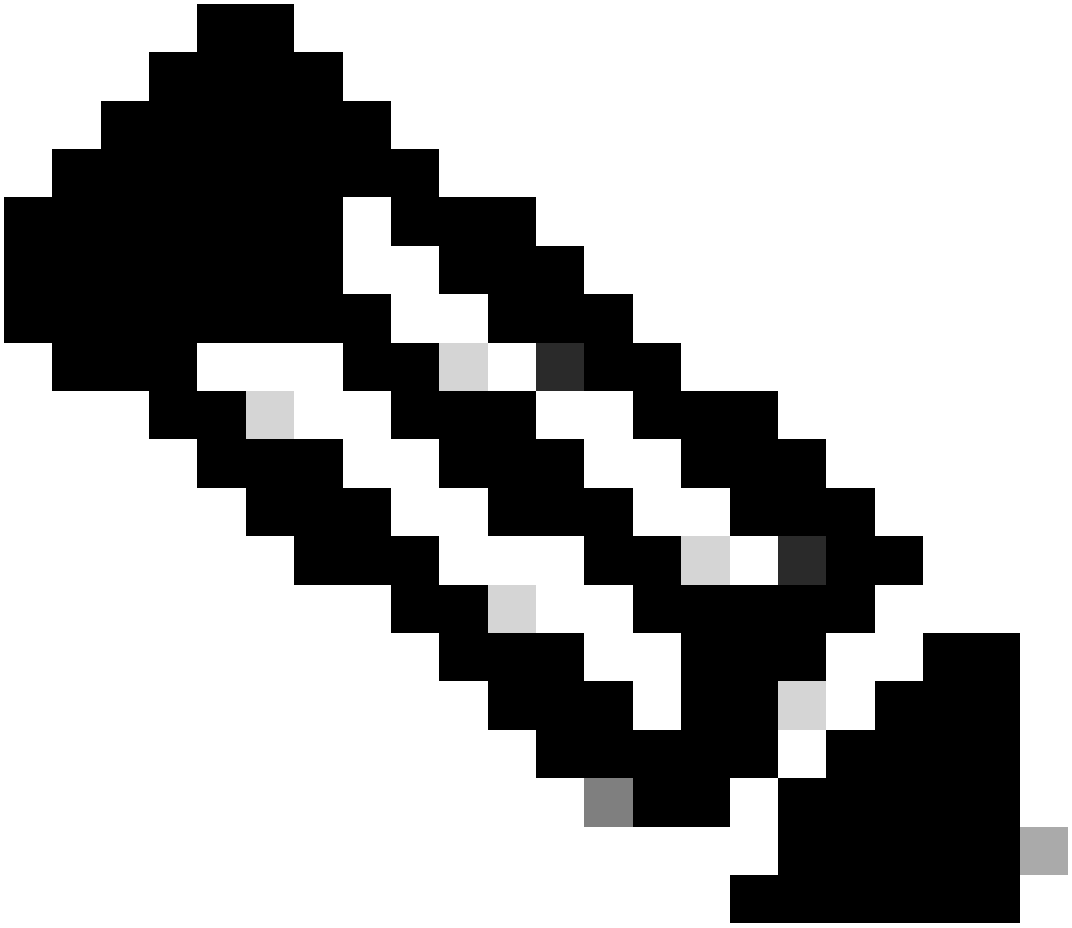
2. Asegúrese de que Tunnel-all DNS no esté configurado en la política de grupo.

Problema de rendimiento de DNS resuelto en AnyConnect versión 3.0(4235)

Este problema de Microsoft Windows es predominante en las siguientes condiciones:

- Con la configuración del router doméstico, a los servidores DNS y DHCP se les asigna la misma dirección IP (AnyConnect crea una ruta necesaria al servidor DHCP).
- Hay un gran número de dominios DNS en la directiva de grupo.
- Se utiliza una configuración Tunnel-all.
- La resolución de nombres la realiza un nombre de host no calificado, lo que implica que la resolución debe probar una serie de sufijos DNS en todos los servidores DNS disponibles hasta que se intente el correspondiente al nombre de host consultado. Este problema se debe al cliente DNS nativo que intenta enviar consultas DNS a través del adaptador físico, que AnyConnect bloquea (dada la configuración Tunnel-all). Esto provoca un retraso en la resolución de nombres que puede ser significativo, especialmente si el equipo de cabecera envía un gran número de sufijos DNS. El cliente DNS debe realizar todas las consultas y los servidores DNS disponibles hasta que reciba una respuesta positiva.

Este problema se resuelve en AnyConnect versión 3.0(4235). Consulte los ID de bug Cisco CSCtq02141 y el ID de bug Cisco CSCtn14578, junto con la introducción a la solución de DNS dividido verdadero mencionada anteriormente, para obtener más información.



Nota: Solo los usuarios registrados de Cisco tienen acceso a la información y las herramientas internas de Cisco.

Si no se puede implementar una actualización, estas son las soluciones alternativas posibles:

- Habilite split-exclude tunneling para una dirección IP, que permite que las solicitudes DNS locales fluyan a través del adaptador físico. Puede utilizar una dirección de la subred local del link 169.254.0.0/16 porque es poco probable que cualquier dispositivo envíe tráfico a una de esas direcciones IP a través de la VPN. Después de habilitar la tunelización split-exclude, habilite el acceso LAN local en el perfil del cliente o en el propio cliente y deshabilite Tunnel-all dDNS.

  En ASA, realice estos cambios de configuración:

```
access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
 group-policy gp_access-14 attributes
```

```
 split-tunnel-policy excludespecified
 split-tunnel-network-list value acl_linklocal_169.254.1.1
 split- Tunnel-all-dns disable
exit
```

En el perfil del cliente, debe agregar esta línea:

```
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
```

También puede habilitar esto para cada cliente en la GUI del cliente AnyConnect. Navegue hasta el menú AnyConnect Preference y marque la casilla de verificación Enable local LAN access.

- Utilice los nombres de dominio completos (FQDN) en lugar de los nombres de host no completos para las resoluciones de nombres.
- Utilice una dirección IP diferente para el servidor DNS en la interfaz física.

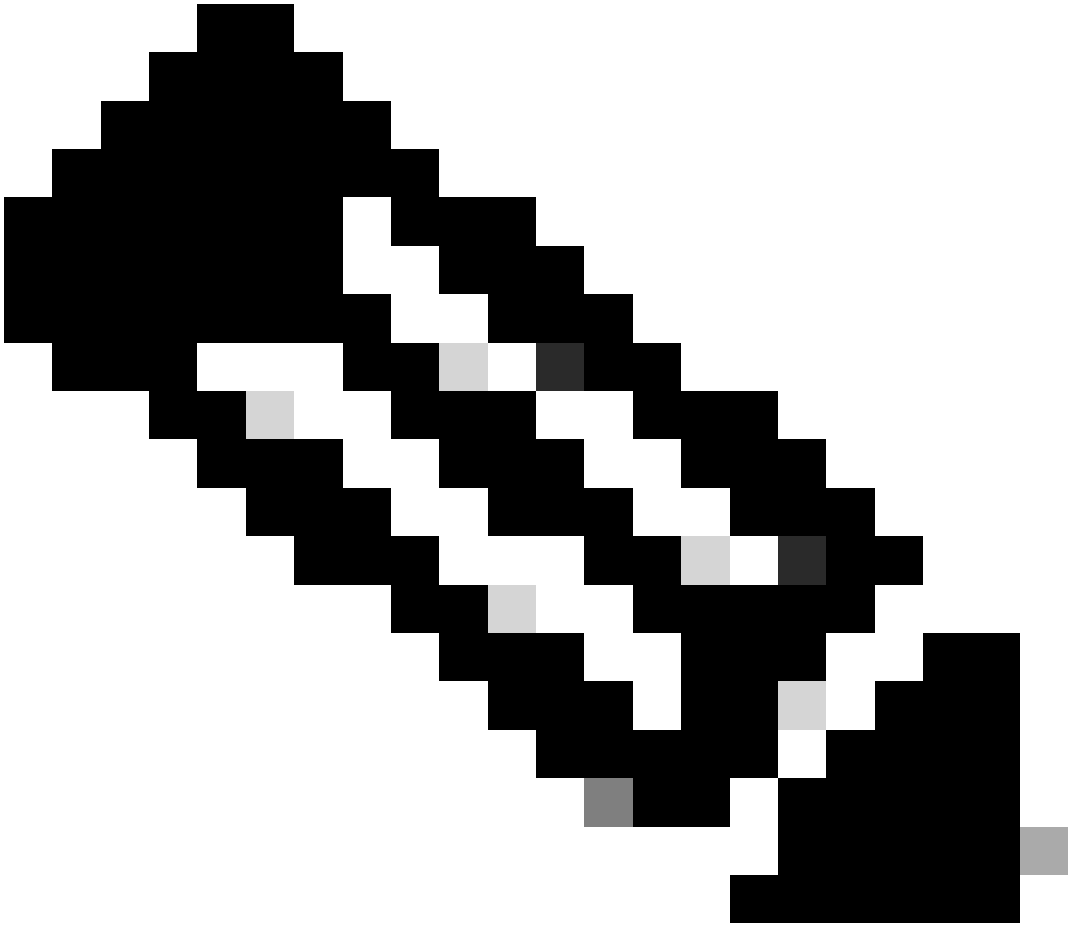
DNS con tunelación dividida en el sistema operativo de Cisco diferente

Los distintos sistemas operativos de Cisco gestionan las búsquedas de DNS de distintas formas cuando se utilizan con tunelación dividida (sin DNS dividido) para AnyConnect. Esta sección describe esas diferencias.

Microsoft Windows

En los sistemas Microsoft Windows, la configuración de DNS es por interfaz. Si se utiliza la tunelización dividida, las consultas DNS pueden recurrir a los servidores DNS del adaptador físico después de que fallan en el adaptador de túnel VPN. Si se define la tunelización dividida sin DNS dividido, la resolución de DNS interno y externo funciona porque recurre a los servidores DNS externos.

Se ha producido un cambio en el comportamiento del mecanismo DNS que gestiona esto en AnyConnect para Windows, en la versión 4.2 después de la corrección del error de Cisco con ID CSCuf07885.



Nota: Solo los usuarios registrados de Cisco tienen acceso a la información y las herramientas internas de Cisco.

Windows 7+

Configuración de túnel completo (y túnel dividido con DNS de túnel completo habilitado)

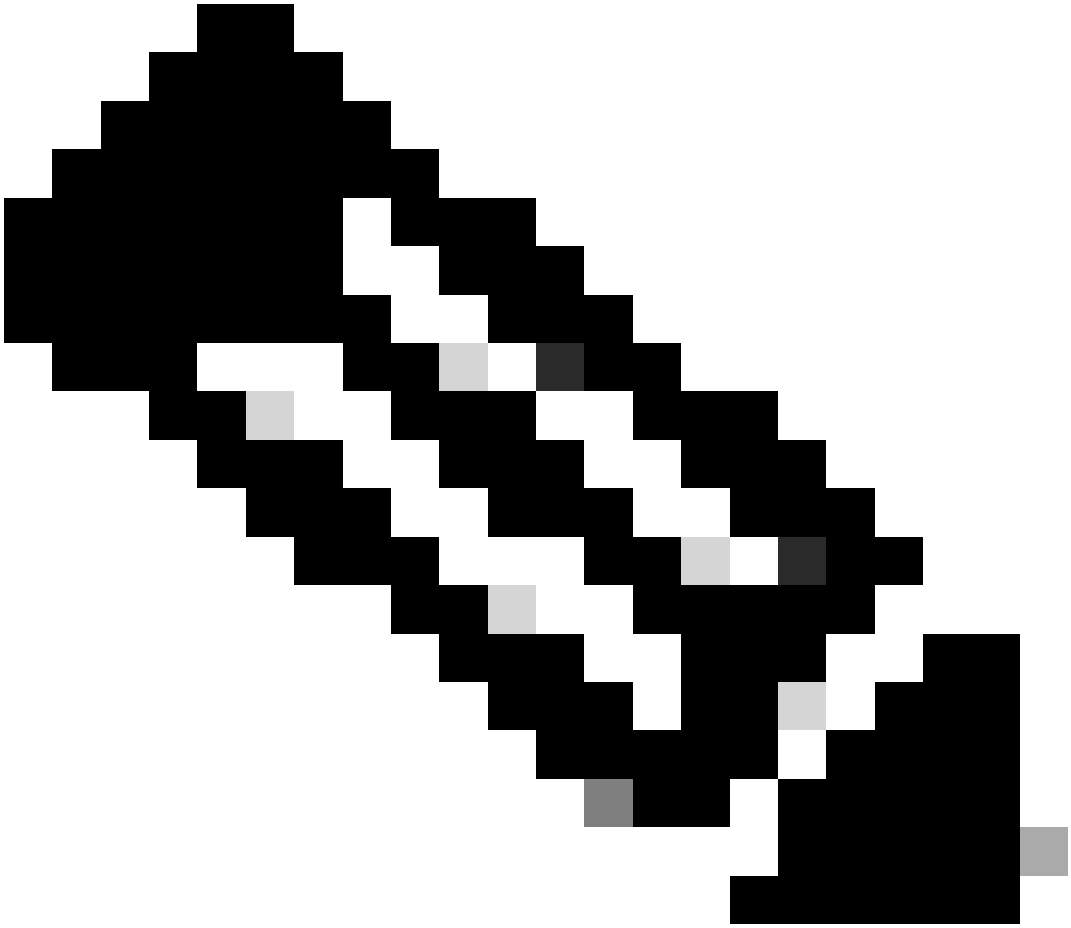
Antes de AnyConnect 4.2:

Sólo se permiten las solicitudes DNS a servidores DNS configurados en la directiva de grupo (servidores DNS de túnel). El controlador de AnyConnect responde a todas las demás solicitudes con una respuesta de "no existe tal nombre". Como resultado, la resolución de DNS solo se puede realizar con los servidores DNS de túnel.

AnyConnect 4.2+

Se permiten las solicitudes DNS a cualquier servidor DNS, siempre que se originen en el adaptador VPN y se envíen a través del túnel. El resto de las solicitudes se responden con ningún nombre , y la resolución de DNS solo se puede realizar a través del túnel VPN.

Antes de la corrección del Id. de error de Cisco CSCuf07885, AC restringía los servidores DNS de destino; sin embargo, con la corrección de este error, ahora restringe qué adaptadores de red pueden iniciar solicitudes DNS.



> Nota: Solo los usuarios registrados de Cisco tienen acceso a la información y las herramientas internas de Cisco.

Configuración de split-include (DNS de túnel completo deshabilitado y sin split-DNS)

El controlador de AnyConnect no interfiere con la resolución DNS nativa. Por lo tanto, la

resolución de DNS se realiza en función del orden de los adaptadores de red, donde AnyConnect es siempre el adaptador preferido cuando se conecta VPN. Además, una consulta de DNS se envía primero a través del túnel y, si no se resuelve, la resolución intenta resolverla a través de la interfaz pública. La lista de acceso split-include incluye la subred que cubre los servidores DNS del túnel. Para empezar con AnyConnect 4.2, el cliente AnyConnect agrega automáticamente las rutas de host para los servidores DNS del túnel como redes de inclusión dividida (rutas seguras) y, por lo tanto, la lista de acceso de inclusión dividida ya no requiere la adición explícita de la subred del servidor DNS del túnel.

Configuración de exclusión dividida (DNS de túnel completo deshabilitado y sin DNS dividido)

El controlador de AnyConnect no interfiere con la resolución DNS nativa. Por lo tanto, la resolución de DNS se realiza en función del orden de los adaptadores de red, donde AnyConnect es siempre el adaptador preferido cuando se conecta VPN. Además, una consulta de DNS se envía primero a través del túnel y, si no se resuelve, la resolución intenta resolverla a través de la interfaz pública. La lista de acceso split-exclude no debe incluir la subred que cubre los servidores DNS de túnel. Para empezar con AnyConnect 4.2, las rutas de host para los servidores DNS de túnel se agregan automáticamente como redes split-include (rutas seguras) por el cliente AnyConnect y, por lo tanto, evita el error de configuración en la lista de acceso split-exclude.

DNS dividido (DNS de túnel completo deshabilitado, split-include configurado)

Anterior a AnyConnect 4.2

Las solicitudes DNS, que coinciden con los dominios split-dns, pueden tunelizar servidores DNS, pero no se permiten a otros servidores DNS. Para evitar que estas consultas de DNS internas se filtren por el túnel, el controlador de AnyConnect responde con "no existe tal nombre" si la consulta se envía a otros servidores DNS. Por lo tanto, los dominios split-dns sólo se pueden resolver a través de servidores DNS de túnel.

Las solicitudes DNS, que no coinciden con los dominios split-dns, se permiten a otros servidores DNS, pero no a los servidores DNS de túnel. Incluso en este caso, el controlador de AnyConnect responde con "no existe tal nombre" si se intenta realizar una consulta de dominios no split-dns a través del túnel. Por lo tanto, los dominios sin split-dns sólo se pueden resolver a través de servidores DNS públicos fuera del túnel.

AnyConnect 4.2+

Las solicitudes DNS, que coinciden con los dominios split-dns, se permiten a cualquier servidor DNS, siempre que se originen desde el adaptador VPN. Si la consulta es originada por la interfaz pública, el controlador de AnyConnect responde con un "no tal nombre" para forzar a la resolución a utilizar siempre el túnel para la resolución de nombres. Por lo tanto, los dominios split-dns sólo se pueden resolver a través del túnel.

Las solicitudes DNS, que no coinciden con los dominios split-dns, se permiten en cualquier servidor DNS siempre que se originen en el adaptador físico. Si la consulta la origina el adaptador VPN, AnyConnect responde con "no existe tal nombre" para forzar a la resolución a intentar siempre la resolución del nombre a través de la interfaz pública. Por lo tanto, los dominios no split-dns sólo se pueden resolver a través de una interfaz pública.

Mac OSx

En los sistemas Macintosh, la configuración DNS es global. Si se utiliza la tunelización dividida, pero no se utiliza el DNS dividido, no es posible que las consultas DNS alcancen a los servidores DNS fuera del túnel. Sólo se puede resolver internamente, no externamente.

Esto se documenta en el ID de bug de Cisco CSCtf20226 y el ID de bug de Cisco CSCtz86314. En ambos casos, esta solución alternativa debe resolver el problema:

- Especifique una dirección IP de servidor DNS externo en la directiva de grupo y utilice un FQDN para las consultas DNS internas.

- Si los nombres externos se pueden resolver a través del túnel, navegue hasta Advanced > Split Tunneling y desactive split DNS mediante la eliminación de los nombres DNS que se configuran en la política de grupo. Esto requiere el uso de un FQDN para las consultas DNS internas.

El caso de DNS dividido se resuelve en AnyConnect versión 3.1. Sin embargo, debe asegurarse de que se cumple una de estas condiciones:

- El DNS dividido debe estar habilitado para ambos protocolos IP, lo que requiere Cisco ASA versión 9.0 o posterior.

- El DNS dividido debe estar habilitado para un protocolo IP. Si ejecuta Cisco ASA versión 9.0 o posterior, utilice el protocolo de omisión del cliente para el otro protocolo IP. Por ejemplo, asegúrese de que no haya un conjunto de direcciones y de que el Protocolo de omisión del cliente esté habilitado en la directiva de grupo. De manera alternativa, si ejecuta una versión de ASA anterior a la versión 9.0, asegúrese de que no haya un conjunto de direcciones configurado para el otro protocolo IP. Esto implica que el otro protocolo IP es IPv6.

Nota: AnyConnect no cambia el archivo resolv.conf en Macintosh OS X, sino que cambia la configuración DNS específica de OS X. Macintosh OS X mantiene actualizado el archivo resolv.conf por motivos de compatibilidad. Utilice el comando scutil —dns para ver la configuración de DNS en Macintosh OS X.

Configuración de túnel completo (y túnel dividido con DNS de túnel completo habilitado)

Cuando AnyConnect está conectado, solo los servidores DNS de túnel se mantienen en la configuración DNS del sistema y, por lo tanto, las solicitudes DNS solo se pueden enviar a los

servidores DNS de túnel.

Configuración de split-include (DNS de túnel completo deshabilitado y sin split-DNS)

AnyConnect no interfiere con la resolución DNS nativa. Los servidores DNS de túnel se configuran como resolvers preferidos, lo que tiene prioridad sobre los servidores DNS públicos, por lo que garantiza que la solicitud DNS inicial para una resolución de nombre se envíe a través del túnel. Dado que la configuración de DNS es global en Mac OS X, no es posible que las consultas DNS utilicen servidores DNS públicos fuera del túnel como se documenta en el ID de bug de Cisco CSCtf2026 . Para empezar con AnyConnect 4.2, el cliente AnyConnect agrega automáticamente las rutas de host para los servidores DNS del túnel como redes de inclusión dividida (rutas seguras) y, por lo tanto, la lista de acceso de inclusión dividida ya no requiere la adición explícita de la subred del servidor DNS del túnel.

Configuración de exclusión dividida (DNS de túnel completo deshabilitado y sin DNS dividido)

AnyConnect no interfiere con la resolución DNS nativa. Los servidores DNS de túnel se configuran como resolvers preferidos, tienen prioridad sobre los servidores DNS públicos, por lo que esto garantiza que la solicitud DNS inicial para una resolución de nombre se envíe a través del túnel. Dado que la configuración de DNS es global en Mac OS X, no es posible que las consultas DNS utilicen servidores DNS públicos fuera del túnel como se documenta en el ID de bug de Cisco CSCtf2026 . Para empezar con AnyConnect 4.2, el cliente AnyConnect agrega automáticamente las rutas de host para los servidores DNS del túnel como redes de inclusión dividida (rutas seguras) y, por lo tanto, la lista de acceso de inclusión dividida ya no requiere la adición explícita de la subred del servidor DNS del túnel.

DNS dividido (DNS de túnel completo deshabilitado, split-include configurado)

Si split-DNS está habilitado para ambos protocolos IP (IPv4 e IPv6) o sólo está habilitado para un protocolo y no hay ningún conjunto de direcciones configurado para el otro protocolo:
Se aplica un split-DNS real similar a Windows. True split-DNS significa que las solicitudes que coinciden con los dominios split-DNS sólo se resuelven a través del túnel, no se filtran a los servidores DNS fuera del túnel.

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 AC solo permite la solicitud DNS que coincide con los dominios split-DNS a través del túnel (otras solicitudes son contestadas por AC con respuesta "rechazada" para forzar la conmutación por fallas a los servidores DNS públicos), pero no puede hacer cumplir la solicitud que coincide con los dominios split-DNS que no se envían en forma clara, a través del adaptador público.

Linux

Configuración de túnel completo (y túnel dividido con DNS de túnel completo habilitado)

Cuando AnyConnect está conectado, solo los servidores DNS de túnel se mantienen en la configuración DNS del sistema y, por lo tanto, las solicitudes DNS solo se pueden enviar a los servidores DNS de túnel.

Configuración de split-include (DNS de túnel completo deshabilitado y sin split-DNS)

AnyConnect no interfiere con la resolución DNS nativa. Los servidores DNS de túnel se configuran como resolvers preferidos, lo que tiene prioridad sobre los servidores DNS públicos, por lo que garantiza que la solicitud DNS inicial para una resolución de nombre se envíe a través del túnel.

Configuración de exclusión dividida (DNS de túnel completo deshabilitado y sin DNS dividido)

AnyConnect no interfiere con la resolución DNS nativa. Los servidores DNS de túnel se configuran como resolvers preferidos, lo que tiene prioridad sobre los servidores DNS públicos, por lo que garantiza que la solicitud DNS inicial para una resolución de nombre se envíe a través del túnel.

DNS dividido (DNS de túnel completo deshabilitado, split-include configurado)

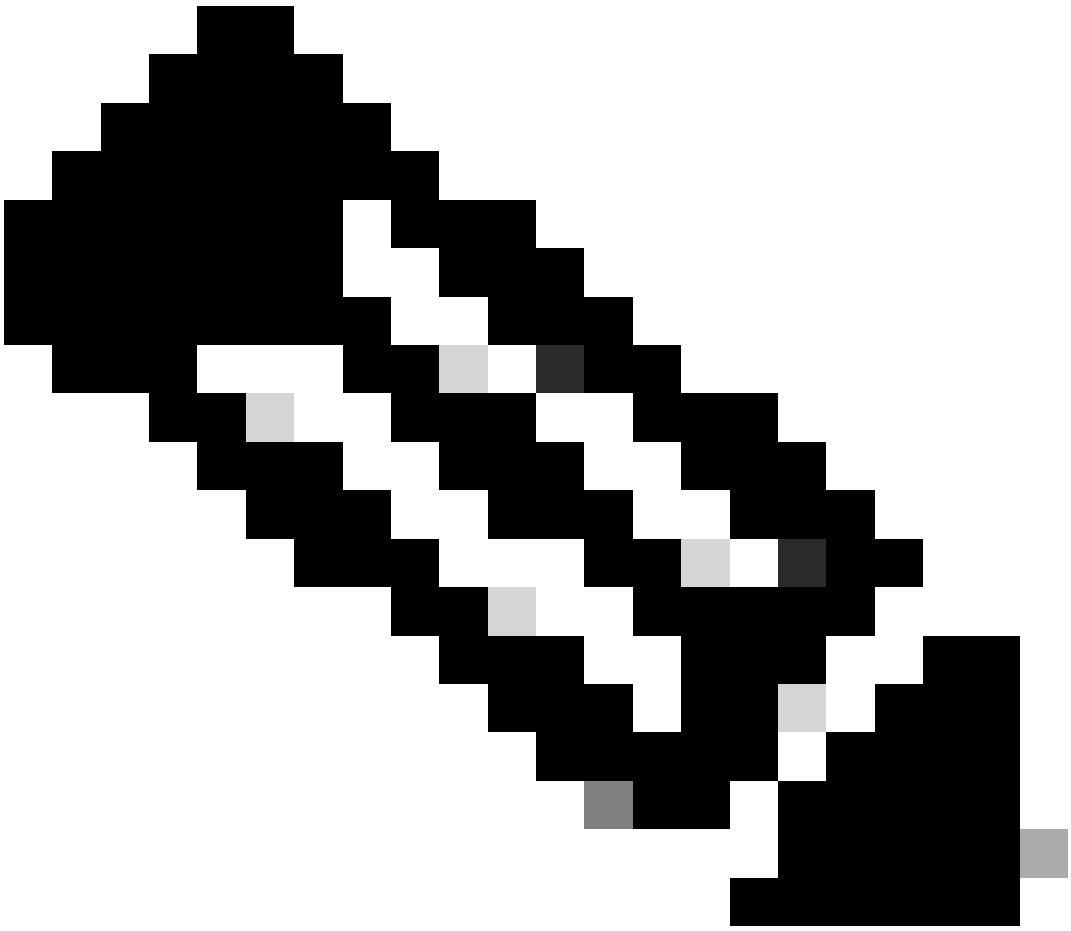
Si split-DNS está habilitado, solo se aplica el respaldo DNS para la tunelización dividida. Esto significa que AC solo permite la solicitud DNS que coincide con los dominios split-DNS a través del túnel (otras solicitudes son contestadas por AC con respuesta "rechazada" para forzar la conmutación por fallas a los servidores DNS públicos), pero no puede hacer cumplir esa solicitud que coincide con los dominios split-DNS que no se envían en forma clara, a través del adaptador público.

iPhone

El iPhone es el opuesto completo del sistema Macintosh y no es similar a Microsoft Windows. Si se define la tunelización dividida pero no se define el DNS dividido, las consultas DNS salen a través del servidor DNS global definido. Por ejemplo, las entradas de dominio DNS dividido son obligatorias para la resolución interna. Este comportamiento se documenta en el ID de bug de Cisco CSCtq09624 y se corrige en la versión 2.5.4038 para el cliente de Apple iOS AnyConnect.

Nota: Tenga en cuenta que las consultas de DNS del iPhone ignoran los dominios .locales. Esto se documenta con el ID de bug de Cisco CSCts89292. Los ingenieros de Apple confirman que el problema se debe a la funcionalidad del sistema operativo. Este es el comportamiento diseñado, y Apple confirma que no hay cambios para él.

Información de error relacionada



Nota: Solo los usuarios registrados de Cisco tienen acceso a la información y las herramientas internas de Cisco.

- Cisco bug ID CSCsv34395 - Agregar soporte en AnyConnect para que proxies el FQDN al servidor DHCP
- Id. de error de Cisco CSCtn14578: AnyConnect para admitir DNS dividido verdadero; no reserva
- Id. de error de Cisco CSCtq02141: problema de DNS de AnyConnect cuando el DNS del ISP está en la misma subred que la IP pública
- ID de bug de Cisco CSCtf20226 - Hacer que el DNS de AnyConnect con el comportamiento de túnel dividido para Mac sea igual que el de Windows
- ID de error de Cisco CSCtz86314 - Mac: las consultas de DNS no se enviaron

correctamente a través del túnel con DNS dividido

- ID de bug de Cisco CSCtq09624 - Hacer que el DNS de AnyConnect para iPhone con el comportamiento de tunelización dividida sea igual que el de Windows
- ID de bug de Cisco CSCts89292 - AC para consultas de DNS de iPhone ignorar dominios .locales

Información Relacionada

- Firewall Cisco IOS®
- Soporte técnico y descargas de Cisco

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).