Diferencias del comportamiento con respecto a las interrogaciones DNS y resolución del Domain Name en diversos OS

Contenido

Introducción

Este documento describe cómo diversas interrogaciones del Domain Name System (DNS) de la manija de los sistemas operativos (OS) y las influencias en la resolución del Domain Name con Cisco AnyConnect y fractura o Tunelización lleno.

Fractura contra el DNS estándar

Cuando usted utiliza fractura-incluya el Tunelización, allí son tres opciones para el DNS:

1. **DNS dividido** - El DNS pregunta que hace juego los Domain Name, se configura en el dispositivo de seguridad adaptante de Cisco (ASA). Se mueven a través del túnel (a los servidores DNS que se definen en el ASA, por ejemplo) mientras que no lo hacen otros.

2. **TÚNEL-TODO-DNS** - Solamente el tráfico DNS a los servidores DNS que son definidos por el ASA se permite. Esta configuración se configura en la directiva del grupo.

3. **DNS estándar** - Todas las interrogaciones DNS se mueven a través de los servidores DNS que son definidos por el ASA. En el caso de una respuesta negativa, las interrogaciones DNS pudieron también ir a los servidores DNS que se configuran en el adaptador físico.

Nota: El comando fractura-túnel-todo-**dns** primero fue implementado en la Versión de ASA 8.2(5). Antes de esta versión, usted podría hacer solamente el DNS dividido o el DNS estándar.

En todos los casos, las interrogaciones DNS que se definen para moverse a través del túnel, van a cualquier servidor DNS que sean definidos por el ASA. Si no hay servidores DNS definidos por el ASA, después las configuraciones DNS son en blanco para el túnel. Si usted no hace el DNS dividido definir, después todas las interrogaciones DNS se envían a los servidores DNS que son definidos por el ASA. Sin embargo, los comportamientos que se describen en este documento pueden ser diferentes, dependiendo del operating system (OS).

Nota: Evite el uso del NSLookup cuando usted prueba la resolución de nombre en el cliente. En lugar, confíe en un navegador o utilice el **comando ping**. Esto es porque NSLookup no confía en el solucionador de DNS OS. AnyConnect no fuerza la petición DNS vía una cierta interfaz sino la permite o la rechaza dependiente sobre la configuración del DNS dividido. Para forzar el solucionador de DNS para intentar a un servidor DNS aceptable para una petición, es importante que la prueba del DNS dividido está realizada solamente con las aplicaciones que confían en el solucionador de DNS nativo para la resolución del Domain Name (todas las aplicaciones excepto NSLookup, el empuje, y las aplicaciones similares que manejan la resolución de DNS solo, por ejemplo).

Verdad contra el mejor DNS dividido de esfuerzo

La versión 2.4 de AnyConnect soporta el retraso del DNS dividido (el mejor DNS dividido de esfuerzo), que no es el DNS dividido verdadero y se encuentra en el cliente IPSec de la herencia. Si la petición corresponde con un dominio del DNS dividido, AnyConnect permite la petición de ser tunneled en el ASA. Si el servidor no puede resolver el nombre del host, el solucionador de DNS continúa y envía la misma interrogación al servidor DNS que se asocia a la interfaz física.

Por otra parte, si la petición no hace juego los dominios uces de los del DNS dividido, AnyConnect no la hace un túnel en el ASA. En lugar, construye una respuesta de DNS de modo que el solucionador de DNS baje y envíe la interrogación al servidor DNS que se asocia a la interfaz física. Por eso esta característica no se llama DNS dividido, sino retraso DNS para el Túnel dividido. No sólo AnyConnect asegura que solamente las peticiones que apuntan los dominios del DNS dividido son tunneled adentro, él también confía en el comportamiento del solucionador de DNS del OS cliente para la resolución de nombre del host.

Esto despierta los problemas de seguridad debido a un escape privado potencial del Domain Name. Por ejemplo, el cliente DNS nativo puede enviar una interrogación para un Domain Name privado a un servidor DNS público específicamente cuando el servidor del nombre DNS VPN no podría resolver la interrogación DNS.

Refiera al Id. de bug Cisco CSCtn14578, resuelto actualmente en Microsoft Windows solamente, a partir de la versión 3.0(4235). La solución implementa el DNS dividido verdadero, pregunta estrictamente los Domain Name configurados que los emparejamientos y no se prohiben a los servidores DNS VPN. El resto de las interrogaciones se permiten solamente a otros servidores DNS, tales como ésos configurados en el adaptador físico.

Haga un túnel todos y haga un túnel todo el DNS

Cuando se inhabilita el Túnel dividido (el **túnel toda la** configuración), el tráfico DNS se permite estrictamente vía el túnel. **El túnel toda la Configuración de DNS** (configurada en la directiva del grupo) envía todas las búsquedas de DNS a través del túnel, junto con algún tipo de Túnel dividido, y el tráfico DNS se permite estrictamente vía el túnel.

Esto es constante a través de las Plataformas con una advertencia en Microsoft Windows: cuando se configura cualquier **túnel todo** o **hace un túnel todo el DNS**, AnyConnect permite el tráfico DNS estrictamente a los servidores DNS que se configuran en el gateway seguro (aplicado al adaptador VPN). Esto es una mejora de la seguridad implementada junto con la solución verdadera previamente mencionada del DNS dividido.

Si esto prueba problemático en ciertos escenarios (por ejemplo, la actualización DNS/los pedidos de inscripción se debe enviar a los servidores DNS NON-VPN), después complete estos pasos:

1. Si la configuración actual es **túnel todo**, después el permiso fractura-**excluye el Tunelización**. Cualquier solo host, fractura-excluye la red es aceptable para el uso, tal como una dirección local del link.

2. Asegúrese de que el **túnel todo el DNS** no esté configurado en la directiva del grupo.

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

Este problema de Microsoft Windows es sobre todo inferior frecuente estas condiciones:

- Con la configuración casera del router, asignan el DNS y los servidores DHCP la misma dirección IP (AnyConnect crea una ruta necesario al servidor DHCP).

- Un gran número de dominios DNS están en la directiva del grupo.

- Se utiliza una Túnel-**toda** configuración.

- La resolución de nombre es realizada por un nombre del host NON-calificado, que implica que el software de resolución de nombres debe intentar varios sufijos DNS en todos los servidores DNS disponibles hasta que intenten el que está relevante al nombre del host preguntado.

Este problema es debido al cliente DNS nativo que intenta enviar las interrogaciones DNS vía el adaptador físico, que AnyConnect bloquea (dado la túnel-**toda** configuración). Esto lleva a un retardo de la resolución de nombre que pueda ser significativo, especialmente si un gran número de sufijos DNS son avanzados por el headend. El cliente DNS debe recorrer a través de todas las

interrogaciones y servidores DNS disponibles hasta que reciba una respuesta positiva.

Este problema se resuelve en la versión 3.0(4235) de AnyConnect. Refiérase al bug Cisco ID CSCtq02141 y CSCtn14578, junto con la introducción a la solución verdadera anterior-mencionada del DNS dividido, para más información.

Si una actualización no puede ser implementada, después éstas son las soluciones alternativas posibles:

- El permiso fractura-**excluye el Tunelización** para una dirección IP, que permite las peticiones del DNS local de atravesar el adaptador físico. Usted puede utilizar un direccionamiento de la subred linklocal **169.254.0.0/16** porque es inverosímil que cualquier dispositivo envía el tráfico a uno de esos IP Addresses sobre el VPN. Después de que usted habilite el **Tunelización de la fractura-exclusión**, habilite el acceso en el perfil del cliente o en el cliente sí mismo del LAN local, y inhabilite el **túnel todo el DNS**.

  En el 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, usted debe agregar esta línea:

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

  Usted puede también habilitar esto sobre una base del por-cliente en el cliente GUI de AnyConnect. Navegue al menú de la **preferencia de AnyConnect**, y marque la casilla de verificación del **acceso del LAN local del permiso**.

- Utilice los nombres de dominio completamente calificado (FQDN) en vez de los nombres del host incompetentes para las resoluciones de nombre.

- Utilice una diversa dirección IP para el servidor DNS en la interfaz física.

DNS con el Túnel dividido en diversos OS

Diversa manija DNS OS busca en las maneras diferentes cuando está utilizada con el Túnel dividido (sin el DNS dividido) para AnyConnect. Esta sección describe esas diferencias.

Microsoft Windows

En los sistemas de Microsoft Windows, las configuraciones DNS son por interface. Si se utiliza el Túnel dividido, las interrogaciones DNS pueden recurrir a los servidores DNS físicos del adaptador después de que fallen en el adaptador del túnel VPN. Si el Túnel dividido sin el DNS dividido se define, después la resolución de DNS interna y externa trabaja porque recurre a los servidores DNS externos.

Ha habido un cambio en el comportamiento en el mecanismo de dirección DNS en AnyConnect

para Windows, en la versión 4.2 después del arreglo para CSCuf07885.

Windows 7+

Túnel-toda configuración (y Túnel dividido con túnel-todo DNS habilitado)

Pre AnyConnect 4.2:

Solamente las peticiones DNS a los servidores DNS configurados bajo grupo-directiva (servidores DNS del túnel) se permiten. El driver de AnyConnect responde al resto de las peticiones con una respuesta de “ningún tal nombre”. Como consecuencia, la resolución de DNS se puede realizar solamente usando los servidores DNS del túnel.

AnyConnect 4.2 +

Las peticiones DNS a cualquier servidor DNS se permiten, mientras se originen del adaptador VPN y se envíen a través del túnel. El resto de las peticiones se responden con la respuesta de “ningún tal nombre”, y la resolución de DNS se puede realizar solamente vía el túnel VPN

Antes del arreglo CSCuf07885, el AC restringe a los servidores DNS de la blanco, no obstante con el arreglo para CSCuf07885, restringe qué adaptadores de red pueden iniciar las peticiones DNS.

Fractura-incluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

El driver de AnyConnect no interfiere con el solucionador de DNS nativo. Por lo tanto, se realiza la resolución de DNS basó por orden de los adaptadores de red donde está siempre el adaptador AnyConnect preferido cuando el VPN está conectado. Por otra parte, una interrogación DNS primero se envía vía el túnel y si no consigue resuelto, el software de resolución de nombres intenta resolverlo vía la interfaz pública. La lista de acceso del fractura-incluido incluye la subred que cubre los servidores DNS del túnel. Para comenzar con AnyConnect 4.2, las rutas del host para los servidores DNS del túnel son agregadas automáticamente como fractura-incluyen las redes (asegure las rutas) por el cliente de AnyConnect, y por lo tanto la lista de acceso del fractura-incluido requiere no más la adición explícita de la subred del servidor DNS del túnel.

Fractura-excluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

El driver de AnyConnect no interfiere con el solucionador de DNS nativo. Por lo tanto, se realiza la resolución de DNS basó por orden de los adaptadores de red donde está siempre el adaptador AnyConnect preferido cuando el VPN está conectado. Por otra parte, una interrogación DNS primero se envía vía el túnel y si no consigue resuelto, el software de resolución de nombres intenta resolverlo vía la interfaz pública. La lista de acceso de la fractura-exclusión no debe incluir la subred que cubre los servidores DNS del túnel. Para comenzar con AnyConnect 4.2, las rutas del host para los servidores DNS del túnel son agregadas automáticamente como fractura-incluyen las redes (asegure las rutas) por el cliente de AnyConnect, y por lo tanto previenen el misconfiguration en la lista de acceso de la fractura-exclusión.

DNS dividido (túnel-todo DNS inhabilitado, fractura-incluye configurado)

Pre AnyConnect 4.2

Las peticiones DNS, que hace juego con los dominios del DNS dividido se permiten hacer un túnel a los servidores DNS, pero no se permiten a otros servidores DNS. Para evitar que tales interrogaciones de los DN internos se escapen hacia fuera el túnel, el driver de AnyConnect responde con “ningún tal nombre” si la interrogación se envía a otros servidores DNS. Por lo tanto, los dominios del DNS dividido se pueden resolver solamente vía los servidores DNS del túnel.

Las peticiones DNS, que no hace juego con los dominios del DNS dividido se permiten a otros servidores DNS, pero no se permiten hacer un túnel a los servidores DNS. Incluso en este caso, el driver de AnyConnect responde con “ningún tal nombre” si una interrogación para no los dominios del DNS dividido se intenta vía el túnel. Por lo tanto, no los dominios del DNS dividido se pueden resolver solamente vía los servidores DNS públicos fuera del túnel.

AnyConnect 4.2 +

Las peticiones DNS, que hace juego con los dominios del DNS dividido se permiten a cualquier servidor DNS, mientras originen del adaptador VPN. Si la interrogación es originada por la interfaz pública, el driver de AnyConnect responde con un “ningún tal nombre” para forzar el software de resolución de nombres para utilizar siempre el túnel para la resolución de nombre. Por lo tanto, los dominios del DNS dividido se pueden resolver solamente vía el túnel.

Las peticiones DNS, que no hace juego con los dominios del DNS dividido se permiten a cualquier servidor DNS mientras originen del adaptador físico. Si la interrogación es originada por el adaptador VPN, AnyConnect responde con “ningún tal nombre” para forzar el software de resolución de nombres para intentar siempre la resolución de nombre vía la interfaz pública. Por lo tanto, no los dominios del DNS dividido se pueden resolver solamente vía la interfaz pública.

Mac OSx

En los sistemas Macintosh, las configuraciones DNS son globales. Si se utiliza el Túnel dividido, pero el DNS dividido no se utiliza, no es posible que las interrogaciones DNS alcancen a los servidores DNS fuera del túnel. Usted puede resolver solamente internamente, no externamente.

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

- Especifique una dirección IP externa del servidor DNS bajo directiva del grupo y utilice un FQDN para las interrogaciones de los DN internos.

- Si los nombres externos son resolvable a través del túnel, después navegue a **avanzado > Túnel dividido** y inhabilite el DNS dividido vía el retiro de los nombres DNS que se configuran en la directiva del grupo. Esto requiere el uso de un FQDN para las interrogaciones de los DN internos.

El caso del DNS dividido se resuelve en la versión 3.1 de AnyConnect. Sin embargo, usted debe

asegurarse de que una de estas condiciones esté cumplido:

- El DNS dividido se debe habilitar para ambos protocolos IP, que requiere la Versión de ASA 9.0 de Cisco o más adelante.

- El DNS dividido se debe habilitar para uno protocolo IP. Si usted ejecuta la Versión de ASA 9.0 de Cisco o más adelante, después utilice el protocolo de puente del cliente para el otro protocolo IP. Por ejemplo, asegúrese de que no haya agrupación de direcciones y de que el **protocolo de puente del cliente** está habilitado en la directiva del grupo. Alternativamente, si usted funciona con una Versión de ASA que sea anterior que la versión 9.0, asegúrese de que no haya agrupación de direcciones configurada para la otra protocolo IP. Esto implica que el otro protocolo IP es IPv6.

Nota: AnyConnect no cambia el **archivo resolv.conf** en el Macintosh OS X, sino cambia bastante las configuraciones X-específicas OS DNS. El Macintosh OS X mantiene el resolv.conffile actual por los motivos de compatibilidad. Utilice el scutil**--comando dns** para ver las configuraciones DNS en el Macintosh OS X.

Túnel-toda configuración (y Túnel dividido con túnel-todo DNS habilitado)

Cuando AnyConnect está conectado, sólo mantienen a los servidores DNS del túnel en la Configuración de DNS del sistema, y por lo tanto las peticiones DNS puede ser enviado solamente a los servidores DNS del túnel.

Fractura-incluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

AnyConnect no interfiere con el solucionador de DNS nativo. Configuran a los servidores DNS del túnel como softwares de resolución de nombres preferidos, que toma la precedencia sobre los servidores DNS públicos, así se asegura de que la petición inicial DNS una resolución de nombre esté enviada sobre el túnel. Puesto que las configuraciones DNS son globales en Mac OS X, no es posible que las interrogaciones DNS utilicen a los servidores DNS públicos fuera del túnel como se documenta en CSCtf20226. Para comenzar con AnyConnect 4.2, las rutas del host para los servidores DNS del túnel son agregadas automáticamente como fractura-incluyen las redes (asegure las rutas) por el cliente de AnyConnect, y por lo tanto la lista de acceso del fractura-incluido requiere no más la adición explícita de la subred del servidor DNS del túnel.

Fractura-excluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

AnyConnect no interfiere con el solucionador de DNS nativo. Configuran a los servidores DNS del túnel mientras que los softwares de resolución de nombres preferidos, tomando la precedencia sobre los servidores DNS públicos, así se asegura de que la petición inicial DNS una resolución de nombre esté enviada sobre el túnel. Puesto que las configuraciones DNS son globales en Mac OS X, no es posible que las interrogaciones DNS utilicen a los servidores DNS públicos fuera del túnel como se documenta en CSCtf20226. Para comenzar con AnyConnect 4.2, las rutas del host para los servidores DNS del túnel son agregadas automáticamente como fractura-incluyen las redes (asegure las rutas) por el cliente de AnyConnect, y por lo tanto la lista de acceso del fractura-incluido requiere no más la adición explícita de la subred del servidor DNS del túnel.

DNS dividido (túnel-todo DNS inhabilitado, fractura-incluye configurado)

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. El DNS dividido verdadero significa esa petición que las coincidencias con los dominios del DNS dividido se resuelvan solamente vía el túnel, él no se escapa a los servidores DNS fuera del túnel.

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 el AC permite solamente la petición DNS que hace 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 la petición que hace juego con los dominios del DNS dividido que no se envían en el claro, vía el adaptador público.

Linux

Túnel-toda configuración (y Túnel dividido con túnel-todo DNS habilitado)

Cuando AnyConnect está conectado, sólo mantienen a los servidores DNS del túnel en la Configuración de DNS del sistema, y por lo tanto las peticiones DNS puede ser enviado solamente a los servidores DNS del túnel.

Fractura-incluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

AnyConnect no interfiere con el solucionador de DNS nativo. Configuran a los servidores DNS del túnel como softwares de resolución de nombres preferidos, que toma la precedencia sobre los servidores DNS públicos, así se asegura de que la petición inicial DNS una resolución de nombre esté enviada sobre el túnel.

Fractura-excluya la configuración (túnel-todo DNS inhabilitado y ningún DNS dividido)

AnyConnect no interfiere con el solucionador de DNS nativo. Configuran a los servidores DNS del túnel como softwares de resolución de nombres preferidos, que toma la precedencia sobre los servidores DNS públicos, así se asegura de que la petición inicial DNS una resolución de nombre esté enviada sobre el túnel.

DNS dividido (túnel-todo DNS inhabilitado, fractura-incluye configurado)

Si se habilita el DNS dividido, sólo el **retraso DNS para el Túnel dividido** se aplica. Esto significa que el AC permite solamente la petición DNS que hace juego con 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 esa petición que

haga juego con los dominios del DNS dividido que no se envían en el claro, vía el adaptador público.

iPhone

El iPhone es el contrario completo del sistema Macintosh y no es similar al Microsoft Windows. Si se define el Túnel dividido pero el DNS dividido no se define, después el DNS pregunta la salida a través del servidor DNS global se define que. Por ejemplo, las entradas de dominio del DNS dividido son obligatorias para la resolución interna. Este comportamiento se documenta en el Id. de bug Cisco CSCtq09624 y se repara en la versión 2.5.4038 para el cliente IOS AnyConnect de Apple.

> Nota: Sea consciente que las interrogaciones del iPhone DNS ignoran los **dominios .local**. Esto se documenta en el Id. de bug Cisco CSCts89292. Los ingenieros de Apple confirman que el problema es causado por las funciones del OS. Éste es el comportamiento diseñado, y Apple confirma allí no es ningún cambio para él.

Información Relacionada

- CSCsv34395 - Agregue el soporte en AnyConnect para el envío a través de proxy el FQDN al servidor DHCP
- CSCtn14578 - AnyConnect para soportar el DNS dividido verdadero; no retraso
- CSCtq02141 - Problema de AnyConnect DNS cuando el ISP DNS está en la misma subred como IP del público
- CSCtn14578 - AnyConnect para soportar el DNS dividido verdadero; no retraso
- CSCtf20226 - Haga AnyConnect DNS con el comportamiento del túnel dividido para el mac lo mismo que las ventanas
- CSCtz86314 - Mac: Interrogaciones DNS no enviadas incorrectamente vía el túnel con el DNS dividido
- CSCtq09624 - Haga el iPhone DNS de AnyConnect con el comportamiento del Túnel dividido lo mismo que Windows
- CSCts89292 - El AC para las interrogaciones del iPhone DNS ignora los dominios .local
- Cisco IOS Firewall
- Soporte Técnico y Documentación - Cisco Systems