Interop entre AnyConnect y el cliente de itinerancia de OpenDNS

Contenido

Introducción

Este documento describe algunas de las limitaciones actuales y las soluciones alternativas disponibles para hacer AnyConnect y al cliente de itinerancia de OpenDNS trabajan juntas. Los clientes de Cisco confían en el cliente VPN de AnyConnect para seguro y la comunicación encriptada a sus redes corporativas. Semejantemente, el cliente de itinerancia de OpenDNS da a usuarios la capacidad de utilizar con seguridad los servicios DNS con la ayuda de los servidores del público de OpenDNS. Ambos estos clientes agregan a un conjunto mejorado de funciones de seguridad en el punto final, y por lo tanto es importante que interoperen con uno a.

Prerequisites

Conocimiento sobre el funcionamiento del cliente de itinerancia de AnyConnect y de OpenDNS.

Familiaridad con la configuración del headend ASA o IOS/IOS-XE (grupo de túnel/grupo-directiva) para AnyConnect VPN.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Headend ASA o IOS/IOS-XE
- Punto final que funciona con al cliente de itinerancia del cliente VPN y de OpenDNS de AnyConnect

Componentes Utilizados

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

- Headend ASA que funciona con la versión 9.4
- Windows 7
- Cliente 4.2.00096 de AnyConnect
- Cliente de itinerancia 2.0.154 de OpenDNS

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

OpenDNS está desarrollando un AnyConnect plug-in con el equipo de Cisco AnyConnect para estar disponible en el futuro. Mientras que no se ha fijado ningunas fechas, esta integración permitirá que el cliente de itinerancia trabaje con el cliente de AnyConnect sin las soluciones alternativas dirigidas. Esto también permitirá a AnyConnect para ser un mecanismo de entrega para el cliente de itinerancia.

Funcionalidad

Dirección de AnyConnect DNS

La cabecera VPN se puede configurar en las maneras diferentes de un par de manejar el tráfico del cliente de AnyConnect.

1. Configuración del túnel completa (túnel-toda): Esto fuerza todo el tráfico del punto final para ser enviada a través del túnel VPN cifrado, y por lo tanto el tráfico nunca deja el adaptador

de interfaz pública en el texto claro

2. Configuración del túnel dividido:

a. Fractura-incluya el Tunelización: Trafique destinado solamente a las subredes específicas o los host definidos en la cabecera VPN se envían a través del túnel, el resto del tráfico se envían fuera del túnel en el texto claro

b. Fractura-excluya el Tunelización: Trafique destinado solamente a las subredes específicas o los host definidos en la cabecera VPN se excluyen del cifrado y dejan la interfaz pública en el texto claro, el resto del tráfico se cifra y se envía solamente a través del túnel

Cada uno de estas configuraciones determina cómo la resolución de DNS es manejada por el cliente de AnyConnect, dependiendo del sistema operativo en el punto final. 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, y AnyConnect es siempre el adaptador preferido cuando el VPN está conectado. Una interrogación DNS primero será enviada tan vía el túnel y si no consigue resuelto, el software de resolución de nombres intentará resolverlo vía la interfaz pública. La lista de acceso del fractura-incluido tendrá que incluir la subred que cubre los servidores DNS del túnel. Comenzando 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, y AnyConnect es siempre el adaptador preferido cuando el VPN está conectado. Una interrogación DNS primero será enviada tan vía el túnel y si no consigue resuelto, el software de resolución de nombres intentará 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. Comenzando 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 que prevendrá 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 corresponden 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. Los dominios del DNS dividido se pueden resolver tan solamente vía los servidores DNS del túnel.

El DNS pide no corresponder con el DNS dividido que los dominios se permiten a otros servidores DNS, pero no permitido 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. Tan 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 corresponden 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. Los dominios del DNS dividido se pueden resolver tan solamente vía el túnel.

El DNS pide no corresponder con el DNS dividido que los dominios 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. Tan no los dominios del DNS dividido se pueden resolver solamente vía la interfaz pública.

Mac 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, tomando la precedencia sobre los servidores DNS públicos, así asegurándose de que la petición inicial DNS una resolución de nombre está 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. Comenzando 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 como softwares de resolución de nombres preferidos, tomando la precedencia sobre los servidores DNS públicos, así asegurándose de que la petición inicial DNS una resolución de nombre está 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. Comenzando 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 que las peticiones que corresponden con los dominios del DNS dividido están resueltas 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 las peticiones DNS que corresponden 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 que las peticiones que corresponden con los dominios del DNS dividido no están enviadas 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, tomando la precedencia sobre los servidores DNS públicos, así asegurándose de que la petición inicial DNS una resolución de nombre está 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, tomando la precedencia sobre los servidores DNS públicos, así asegurándose de que la petición inicial DNS una resolución de nombre está 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 las peticiones DNS que corresponden 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 que las peticiones que corresponden con los dominios del DNS dividido no están enviadas en el claro, vía el adaptador público.

Cliente de itinerancia de OpenDNS

El cliente de itinerancia es un software que maneja los servicios DNS en el punto final, y utiliza a los servidores DNS públicos de OpenDNS para asegurar y para cifrar el tráfico DNS.

Idealmente, el cliente debe estar en un estado protegido y cifrado. Sin embargo, si el cliente no puede establecer una sesión de TLS con el servidor público del software de resolución de nombres de OpenDNS (208.67.222.222), intenta enviar el tráfico DNS unencrypted en el puerto 53 UDP a 208.67.222.222. El cliente de itinerancia utiliza exclusivamente a la dirección IP 208.67.222.222 pública del software de resolución de nombres de OpenDNS (hay algunos otros tales como 208.67.220.220, 208.67.222.220, y 208.67.220.222). El cliente de itinerancia instalado una vez, fija 127.0.0.1 (localhost) como el servidor DNS local y reemplaza las configuraciones actuales del por interface DNS. Las configuraciones actuales DNS se salvan en los archivos locales resolv.conf (incluso en Windows) dentro de la carpeta de itinerancia de la configuración del cliente. OpenDNS de reserva incluso esos servidores DNS que sean doctos vía el adaptador

de AnyConnect. Por ejemplo, si 192.168.92.2 es el servidor DNS en el adaptador público, OpenDNS creará el resolv.conf en la siguiente ubicación:

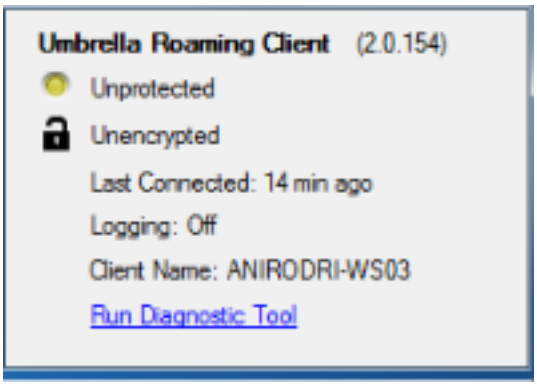
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2

El cliente de itinerancia cifrará cada paquete fijado a OpenDNS; sin embargo, no enciende ni utiliza un túnel de encripción a 208.67.222.222. El cliente de itinerancia tiene una característica opcional de la aplicación de la capa IP que abra conexión IPSec para que los propósitos del no DNS bloqueen los IP Addresses. Esto inhabilitará automáticamente en presencia de una conexión activa de AnyConnect. También ata a 127.0.0.1:53 para recibir las interrogaciones localmente generadas en el ordenador. Cuando el punto final necesita resolver un nombre, las interrogaciones locales se dirigen a 127.0.0.1 debido a la invalidación, y entonces al proceso subyacente del dnscrypt-proxy del cliente de itinerancia adelante ellos a los servidores públicos de OpenDNS sobre el canal cifrado.

Si el DNS no se permite para fluir a 127.0.0.1:53, después el cliente de itinerancia no podrá funcionar y lo que sigue ocurrirá. Si el cliente no puede alcanzar los servidores DNS públicos o el direccionamiento encuadernado de 127.0.0.1:53, transición a un estado fracaso-abierto y restablecer las configuraciones DNS en los adaptadores locales. En el fondo, continúa enviando las sondas a 208.67.222.222 y puede transición al modo activo si se restablece la conexión segura.

Limitaciones

Mirando las funciones de alto nivel de ambos clientes, es evidente que el cliente de itinerancia necesita tener la capacidad de cambiar las configuraciones del DNS local y de atar a 127.0.0.1:53 para remitir las interrogaciones a través del canal seguro. Cuando el VPN está conectado, las únicas configuraciones donde AnyConnect no interfiere con el solucionador de DNS nativo son el fractura-incluir y fractura-excluir (con fractura-túnel-todo DNS inhabilitado). Por lo tanto, se recomienda actualmente para utilizar una de esas configuraciones, cuando el cliente de itinerancia es también funcionando. El cliente de itinerancia permanecerá en un estado desprotegido/unencrypted si se utiliza túnel-toda configuración, o fractura-túnel-todo DNS se habilita, tal y como se muestra en de la imagen.



Solución Aternativa

Si el intento es proteger la comunicación entre el cliente de itinerancia y los servidores de OpenDNS usando el VPN hace un túnel, después un maniquí fractura-excluye la lista de acceso se puede utilizar en la cabecera VPN. Ésta será la cosa más cercana a una configuración del túnel completa. Si no hay tal requisito, después fractura-incluya puede ser utilizado donde la lista de acceso no incluye los servidores públicos de OpenDNS, o fractura-excluyen puede ser utilizado donde la lista de acceso incluye los servidores del público de OpenDNS.

Además, al usar al cliente de itinerancia, los modos del DNS dividido no pueden ser utilizados pues éste dará lugar a una pérdida de resolución del DNS local. Fractura-túnel-todo DNS debe también seguir siendo discapacitado; sin embargo, se soporta y debe parcialmente permitir que el cliente de itinerancia haga poste-Conmutación por falla cifrada.

Configuraciones

Tráfico de OpenDNS del túnel

Este ejemplo utiliza una dirección IP simulada en la lista de acceso de la fractura-exclusión. Con esta configuración, toda la comunicación con 208.67.222.222 sucede a través del túnel VPN, y el cliente de itinerancia actúa en un estado cifrado y protegido.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Excluya el tráfico de OpenDNS del túnel VPN

Este ejemplo utiliza el direccionamiento del software de resolución de nombres de OpenDNS en la lista de acceso de la fractura-exclusión. Con esta configuración, toda la comunicación con 208.67.222.222 sucede fuera del túnel VPN, y el cliente de itinerancia actúa en un estado cifrado y protegido.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
```

```
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Este ejemplo muestra una configuración del fractura-incluido para una subred interna 192.168.1.0/24. Con esta configuración, el cliente de itinerancia todavía actuará en un estado cifrado y protegido puesto que el tráfico a 208.67.222.222 no se envía vía el túnel.

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#

Note: Split-tunnel-all-dns must be disabled in all of the  scenarios
```

Verificación

Cuando el VPN está conectado, el cliente de itinerancia debe mostrar protegido y cifrado tal y como se muestra en de esta imagen: