Uso de la compatibilidad con CSC para la protección de Umbrella DNS en IPv6 de una sola pila

Contenido

Introducción

Este documento describe cómo habilitar Cisco Secure Client (CSC) para admitir la protección Umbrella DNS en redes IPv6 de pila única.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Secure Client en Umbrella Roaming Security.

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.

Overview

En el pasado, Cisco Secure Client admitía configuraciones de red de pila dual y solo IPv4. En este artículo se describe la compatibilidad con redes sólo IPv6 a partir de Cisco Secure Client 5.1.4.74 (MR4). La función debe estar habilitada mediante un archivo de indicador.

Background

Con la proliferación generalizada de IPv6, los ISP de todo el mundo asignan cada vez más direcciones IPv6 únicamente. Sin embargo, muchos recursos de servidor siguen estando en redes IPv4 solamente. DNS64, combinado con NAT64, son capacidades de transición que permiten una comunicación fluida entre los clientes solo de IPv6 y los servidores solo de IPv4 sin que sea necesario que los clientes conozcan la infraestructura IPv4 subyacente.

Los registros AAAA se utilizan exclusivamente con IPv6, mientras que los registros A se utilizan exclusivamente con IPv4. DNS64 funciona sintetizando registros AAAA (IPv6) para servidores que sólo tienen registros A en su DNS, lo que permite que los clientes sólo de IPv6 lleguen a servidores sólo de IPv4. DNS64 crea estos registros AAAA combinando un prefijo IPv6 configurable con la dirección IPv4 de una búsqueda de registros A. La dirección IPv4 está integrada en los últimos 32 bits de la dirección IPv6.

Cisco Secure Client 5.1.4.74 (MR4) ahora es compatible con la protección Umbrella para redes que solo admiten IPv6. El módulo Umbrella detecta el prefijo NAT64 que está empleando el gateway de red consultando los resolvers DNS LAN. A continuación, realiza la síntesis de la dirección IPv6 de DNS64 mediante el prefijo NAT64 detectado cuando la resolución de DNS de Umbrella participa en la resolución de nombres para la aplicación de políticas.

Activar la función

Windows:

Cree un archivo denominado `single_stack_ipv6.flag` y colóquelo en este directorio:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data
```

Una vez que el archivo de indicador se haya colocado en el directorio, reinicie Cisco Secure Client para que la función surta efecto.

macOS

Cree un archivo denominado `single_stack_ipv6.flag` y colóquelo en este directorio:

```
/opt/cisco/secureclient/umbrella/data
```

Una vez que el archivo de indicador se haya colocado en el directorio, reinicie Cisco Secure Client para que la función surta efecto.

Limitaciones

En la versión 5.1.4 de CSC, DNS64 sólo se admite para el tráfico DNS cifrado que va a los resolvers de Umbrella DNS. No es compatible con el tráfico DNS no cifrado, incluso si se aplica protección.

Preguntas frecuentes

¿Cómo sé si DNS64/NAT64 es compatible con mi red (macOS)?

Puede utilizar la prueba de excavación de DNS64/NAT64.

Estas pruebas están diseñadas para calificar una red en la que el host solo se configura con una dirección IPv6. Para alcanzar los servicios IPv4 existentes en Internet, el host debe utilizar DNS64 de la resolución configurada para recibir la dirección IPv6 sintetizada de la dirección IPv4. Una vez que Umbrella tiene la dirección sintetizada, se asegura de que sea accesible. Solo puede ser alcanzable si NAT64 está habilitado en el gateway. Umbrella utiliza el dominio "api-ipv4.opendns.com" porque solo hay direcciones v4 configuradas. Por lo tanto, si Umbrella obtiene una dirección v6 en el registro de respuesta, Umbrella sabe que se ha sintetizado. Cuando hace `ping6` en la dirección devuelta por el comando `dig`, sabe que la dirección sintetizada se traduce correctamente a una dirección v4 en Internet y la respuesta se traduce de vuelta al host.

DNS64

Lo primero que desea probar es:

```
➜ osx dig AAAA api-ipv4.opendns.com

; <<>> DiG 9.10.6 <<>> AAAA api-ipv4.opendns.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31228
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;api-ipv4.opendns.com. IN AAAA

;; ANSWER SECTION:
api-ipv4.opendns.com. 60 IN AAAA 64:ff9b::9270:ff9b <-synthesized address

;; Query time: 921 msec
;; SERVER: 2001:4860:4860::6464#53(2001:4860:4860::6464)
```

```
;; WHEN: Thu Jun 20 17:28:12 PDT 2024
;; MSG SIZE rcvd: 77
```

NAT64

Ahora, puede hacer ping a la dirección sintetizada:

```
➜ osx ping6 64:ff9b::9270:ff9b
PING6(56=40+8+8 bytes) 2001:db8:1:0:785e:e00f:f8fe:9f7b --> 64:ff9b::9270:ff9b
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=0 hlim=54 time=103.653 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=1 hlim=54 time=51.491 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=2 hlim=54 time=54.278 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=3 hlim=54 time=78.153 ms
```

¿Cómo sé si DNS64/NAT64 es compatible con mi red (Windows)?

DNS64

Lo primero que desea probar es:

```
C:\>nslookup -type=AAAA api-ipv4.opendns.com.
Server: UnKnown
Address: 2600:1f14:1799:7000:d2b9:d714:e957:6d4
```

Respuesta no autoritativa:

```
Name: api-ipv4.opendns.com
Address: 64:ff9b::9270:ff9b <-synthesized address
```

NAT64

Ahora, puede hacer ping a la dirección sintetizada:

```
C:\>ping 64:ff9b::9270:ff9b

Pinging 64:ff9b::9270:ff9b with 32 bytes of data:
Reply from 64:ff9b::9270:ff9b: time=18ms
Reply from 64:ff9b::9270:ff9b: time=22ms
Reply from 64:ff9b::9270:ff9b: time=21ms
Reply from 64:ff9b::9270:ff9b: time=19ms

Ping statistics for 64:ff9b::9270:ff9b:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 18ms, Maximum = 22ms, Average = 20ms
```

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).