Comprender la compatibilidad de Umbrella Roaming Client y F5 VPN

Contenido

Introducción

Este documento describe la compatibilidad entre Cisco Umbrella Roaming Client y F5 VPN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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.

Introducción

El cliente de roaming de Umbrella se puede utilizar en una amplia variedad de configuraciones de red y software. Este artículo documenta todos los temas de compatibilidad conocidos con el cliente F5 VPN. Este artículo comienza con los comportamientos de detección esperados actuales y, a continuación, analiza las notas de compatibilidad específicas de F5 VPN.

El cliente Umbrella ha implementado mecanismos de detección automatizados para reaccionar a los cambios de VPN con el fin de garantizar que se mantenga la funcionalidad de DNS. Esto puede hacer que el cliente permanezca temporalmente desprotegido mientras la VPN está conectada. Consulte el artículo Heurística de detección de VPN de terceros con el cliente de roaming de Umbrella para obtener más detalles.

Compatibilidad con VPN F5

En muchas configuraciones, la VPN F5 funciona insertando las direcciones DNS de VPN en las NIC que no son VPN, prependientes de los servidores VPN en el DNS de la NIC. Por lo tanto, para una configuración DNS local de x.x.x.x y una configuración VPN de y.y.y.y.y, el resultado es y.y.y.y, x.x.x.x.

Con el cliente de roaming de Umbrella, esto invalida el 127.0.0.1 colocado. Para asegurarse de que la VPN F5 no se vea afectada por un bucle de cambio sin fin, Umbrella deja de redirigir si 127.0.0.1 se coloca al final de la lista DNS o se cambia rápidamente de nuevo de 127.0.0.1.

En la mayoría de los casos, Umbrella recomienda el uso del módulo de seguridad de roaming de Umbrella que forma parte del cliente de seguridad de roaming de AnyConnect. No es necesario implementar la VPN (se puede quitar de la visualización para el usuario en el momento de la instalación).

La compatibilidad con F5 en este momento se define como una conexión VPN F5 correcta con DNS público y local totalmente funcional. Esto puede ser el resultado de un retraso sin errores por parte del cliente de roaming a un estado sin protección. Asegúrese de que dispone de la cobertura en la red mientras utiliza F5 configurando la red para Cisco Umbrella.

Cliente VPN BigIP F5

El cliente de borde F5 de BigIP es el cliente VPN F5 más común en este momento. Sin embargo, en muchas implementaciones se está sustituyendo por el nuevo cliente F5. Este artículo trata todos los problemas de interoperabilidad conocidos con el cliente F5 BigIP.

Proxy de retransmisión de DNS F5

El cliente de itinerancia no es compatible con el cliente VPN 2.2+ en las configuraciones que activan el servicio F5 DNS Relay Proxy. Se sabe que este proxy de retransmisión se activa en el modo split-dns y en los modos de tunelización split basados en DNS. F5 no se puede utilizar con nombres DNS definidos con el cliente de itinerancia. Para utilizar la tunelización dividida con F5 y el cliente de itinerancia en este momento, utilice la tunelización dividida basada en IP en lugar de la tunelización dividida basada en DNS. Además, algunas configuraciones y versiones pueden hacer que Umbrella se anule a pesar de que se muestre en verde cuando se active el proxy de retransmisión DNS.

Busque la configuración de split-dns o de túnel dividido basado en DNS

La tunelización dividida F5 VPN con split-dns aparece en forma de la configuración "Espacio de direcciones DNS". Cuando está activo, esto activa el proxy DNS propio de F5 que entra en conflicto con el cliente de roaming. El síntoma es una falla al resolver los registros A mientras el cliente de roaming y la VPN están activos. Vea esta captura de pantalla para ver una configuración en funcionamiento:

Client Settings: Advanced ▼

Traffic Options	○ Force all traffic through tunnel ◉ Use split tunneling for traffic
IPV4 LAN Address Space	IP Address Mask Add 0.0.0.0/0.0.0.0 Edit Delete
DNS Address Space	DNS Add Edit Delete
IPV4 Exclude Address Space	IP Address Mask Add Edit Delete
DNS Exclude Address Space	DNS Add

Ensure this is empty!

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).