

Configuración de SWG para evitar conflictos con el tráfico VPN SSL

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe cómo resolver problemas de incompatibilidad entre Secure Web Gateway (SWG) y SSL VPNs mediante puertos interceptados.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

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.

Problema

Umbrella SWG para AnyConnect puede encontrar problemas de incompatibilidad con ciertas SSL VPN que utilizan puertos interceptados por el agente SWG, como TCP 443. AnyConnect SWG puede no activar y aplicar la cobertura de forma fiable. La fiabilidad de la red puede degradarse o dejar de estar disponible cuando SWG está activo y el tráfico VPN pasa a través de SWG. El tráfico que no es web se descarta en este escenario. Este problema afecta a todas las SSL VPN que utilizan los puertos 80 y 443.

Solución

Para evitar que SWG intercepte el tráfico VPN, configure una derivación para sus dominios VPN y direcciones IP:

1. En el panel de control de paraguas, navegue hasta Acceder a Despliegues > Gestión de Dominios > Dominios Externos.
2. Agregue el dominio y la dirección IP de sus servidores de cabecera VPN a la lista Dominios Externos. La entrada IP garantiza que el tráfico VPN nunca sea interceptado por el agente SWG debido al gran número de conexiones.
3. Deje que transcurra una hora para que el nuevo parámetro se propague.

Para utilizar SSL VPN con SWG:

1. Agregue el dominio VPN a la lista Dominios externos.
2. Si el dominio de cabecera VPN es un sufijo de búsqueda DNS, el cliente agrega automáticamente este dominio durante la conexión.
3. Agregue las direcciones IP o el rango de IP de la cabecera VPN a la lista Dominios Externos.

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).