Comprensión de la configuración de respaldo de DNS y SWG para CSC

Contenido

Introducción

Este documento describe la configuración de respaldo de DNS y gateway web seguro (SWG) para Cisco Secure Client (CSC).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Secure 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.

Overview

Hasta aproximadamente el 25 de abril de 2024, el comportamiento de la interrupción del módulo SWG de Cisco Secure Client no podía controlarse independientemente del estado del módulo DNS y dependía de la configuración de la interrupción DNS para habilitar/deshabilitar la protección SWG. Para solucionar este problema, Umbrella ha separado el comportamiento del módulo DNS y el módulo SWG, lo que permite una gestión independiente según sea necesario. Está disponible para Cisco Secure Clients en la versión 5.1.3.62 y posteriores donde Umbrella

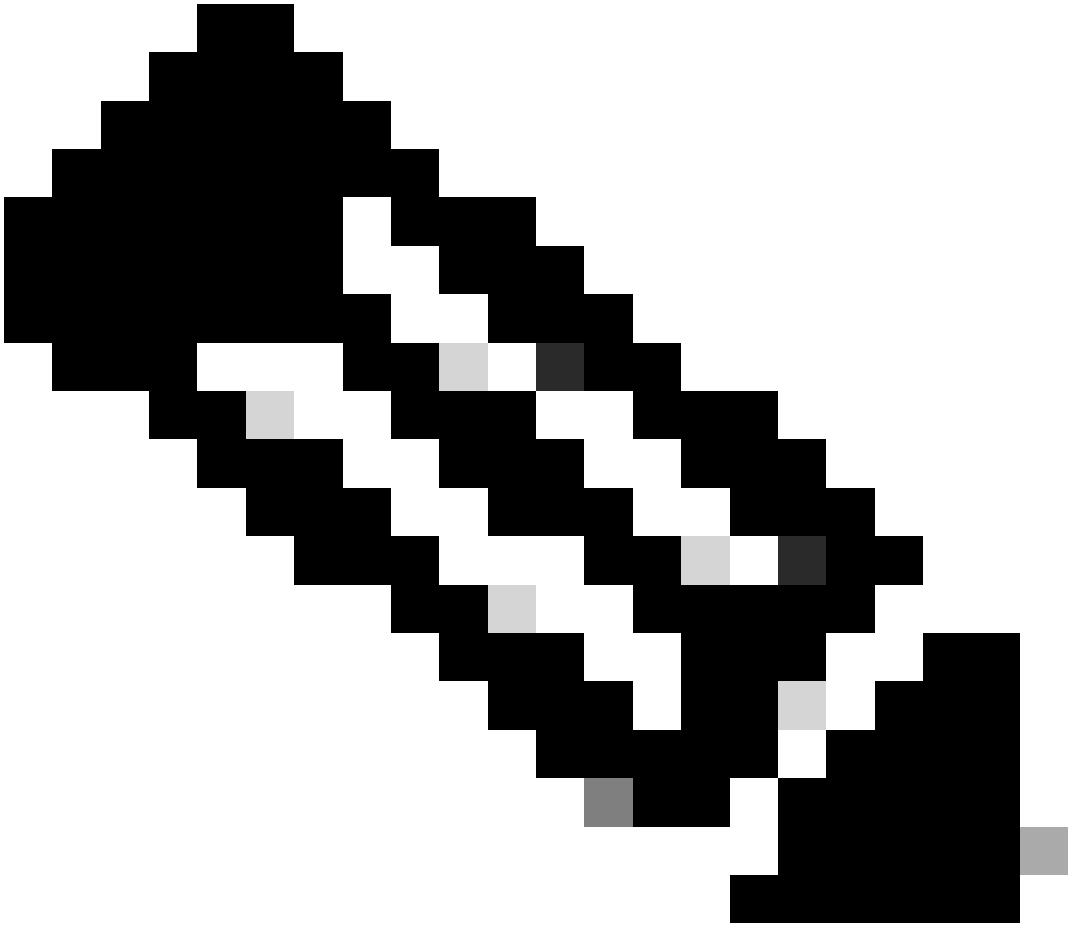
desacopló la configuración de respaldo de DNS y SWG para permitir un control granular mejorado. Los clientes de versiones anteriores no siguieron la desconexión del módulo SWG independiente.

Cuando se habilita la función Secure Web Gateway backoff follow DNS backoff, el módulo SWG de CSC sigue el comportamiento del módulo DNS. Sin embargo, esto no ocurre con todos los valores de configuración de la desconexión de DNS. En la siguiente sección, se detallan las configuraciones de respaldo de DNS que el módulo SWG sigue o no.

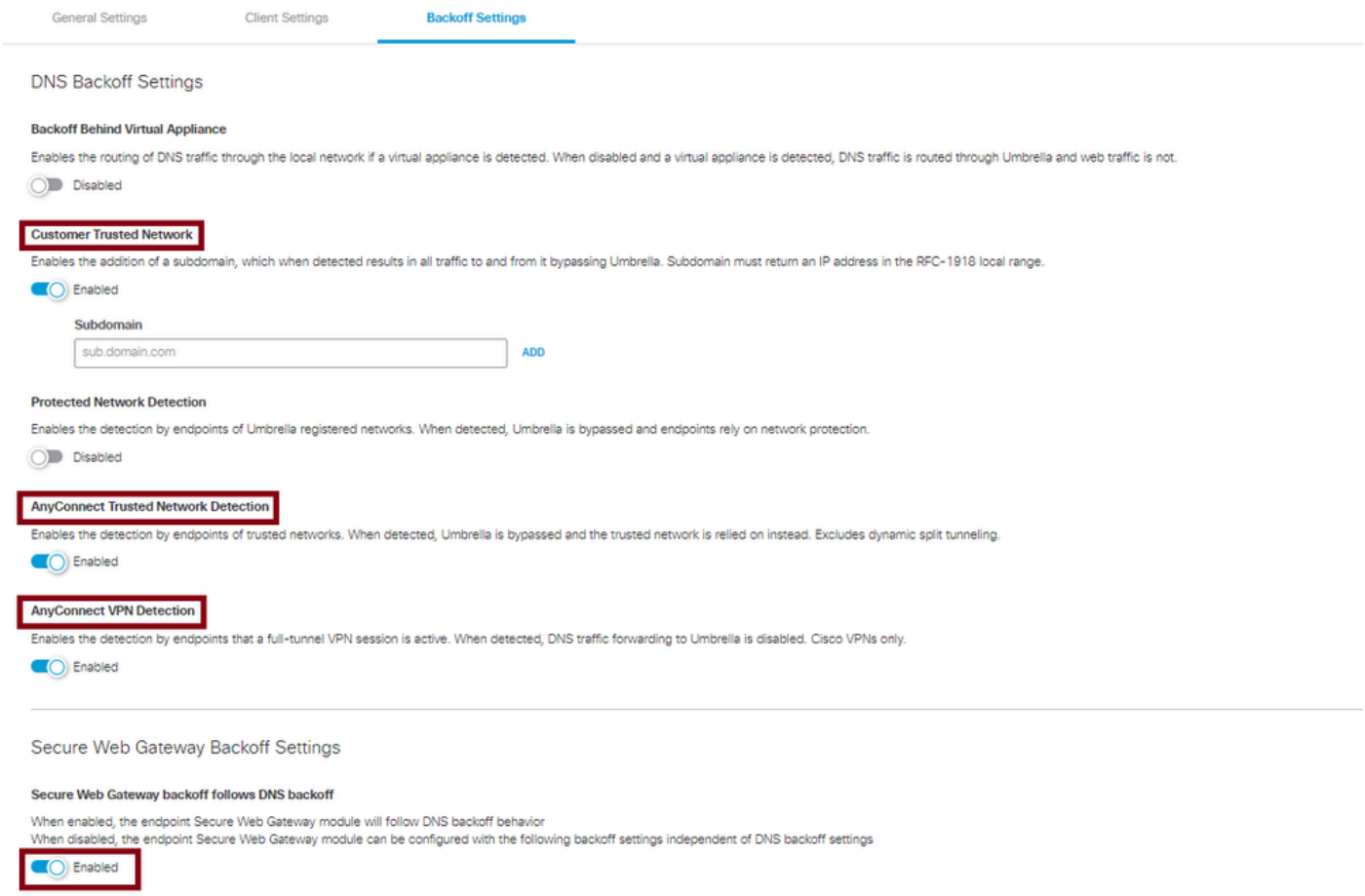
¿Qué configuración de desconexión de DNS hace que SWG se desconecte?

Estos ajustes de respaldo de DNS hacen que SWG se apague:

- Red de confianza del cliente: Uno de los métodos más sencillos consiste en configurar un dominio Customer Trusted Network en la configuración de respaldo de DNS. Al alojar un dominio interno que se resuelve en una dirección RFC1918, tanto DNS como SWG pueden retroceder simultáneamente. El cliente de Umbrella está codificado para consultar ese dominio. Si resuelve correctamente el dominio en una dirección IP privada, identifica que el dispositivo se encuentra en una red privada y protegida, lo que hace que el módulo DNS se desactive. Este mecanismo de respaldo también es respetado por el módulo Web, que puede retroceder de manera similar cuando el módulo DNS resuelve correctamente el dominio.
- Detección de redes de confianza AnyConnect
- Detección de VPN AnyConnect



Nota: La configuración de respaldo de DNS sigue funcionando en Cisco Secure Clients que ejecutan versiones anteriores a la 5.1.3.62, ya que se implementó antes de la separación de la configuración de respaldo de DNS y SWG.

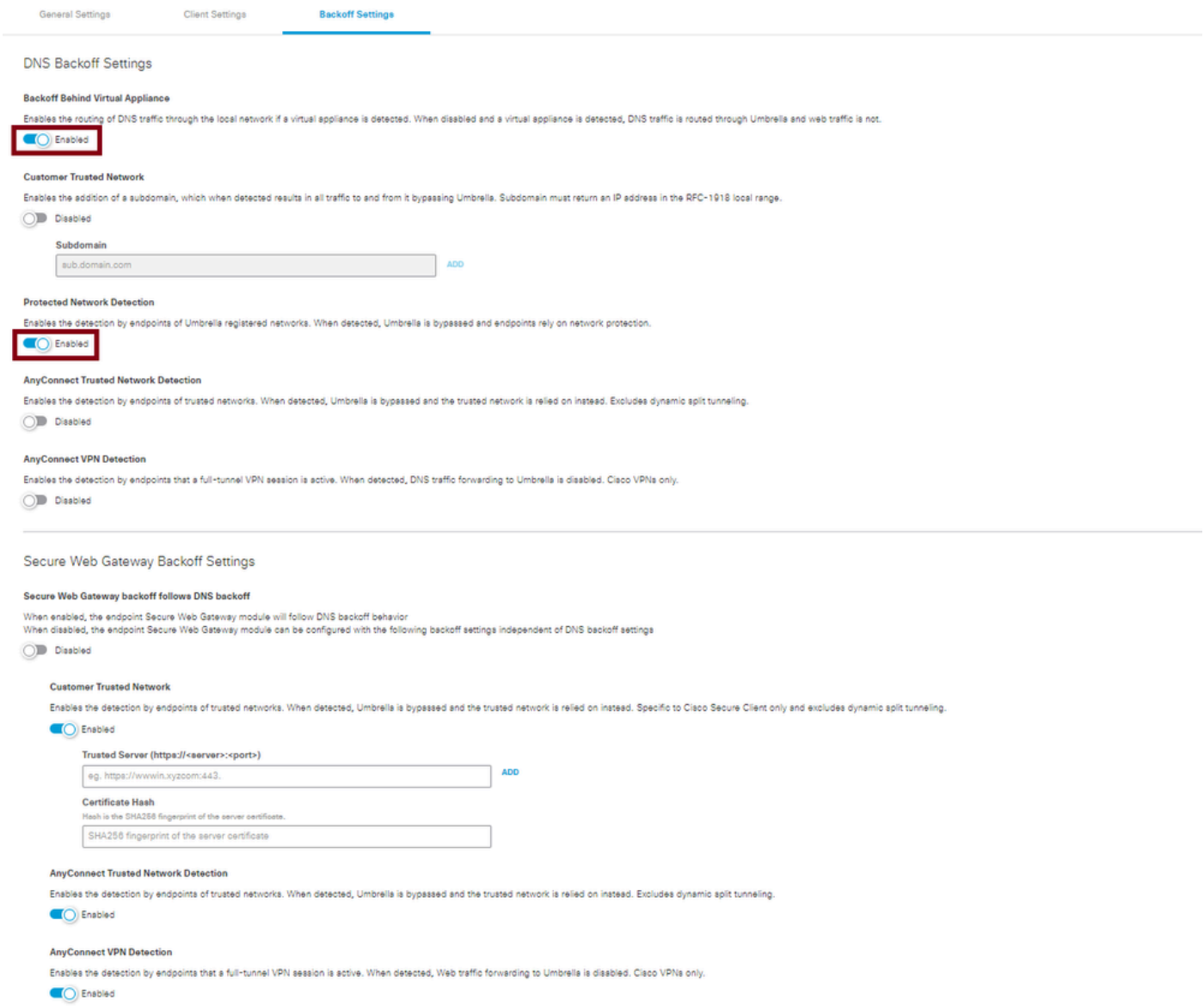


27885424859028

¿Qué parámetros de desconexión de DNS no provocan que SWG se desconecte?

La configuración de estas dos funciones de respaldo de DNS no hace que SWG se apague. Por lo tanto, debe configurar los ajustes de respaldo SWG de forma selectiva, independientemente del estado de configuración de DNS. Esto se trata con más detalle en la siguiente sección.

- Retroceso detrás del dispositivo virtual: A partir de AnyConnect 4.10.07061 (MR7) y Secure Client 5.0.02075 (MR2), el módulo SWG puede permanecer activado en las redes en las que haya un dispositivo virtual Umbrella. Si anteriormente confiaba en la presencia de un dispositivo virtual para desactivar el módulo SWG y la redirección web en una red determinada, puede utilizar en su lugar Trusted Network Domain o AnyConnect Trusted Network Detection.
- Detección de red protegida



27885587178772

Configuración independiente de retroceso SWG

Si estas funciones de respaldo de DNS no están habilitadas en su entorno, puede utilizar exclusivamente una de las configuraciones de respaldo de SWG descritas aquí para asegurarse de que SWG permanezca deshabilitado:

- Red de confianza del cliente
- Detección de redes de confianza AnyConnect
- Detección de VPN AnyConnect

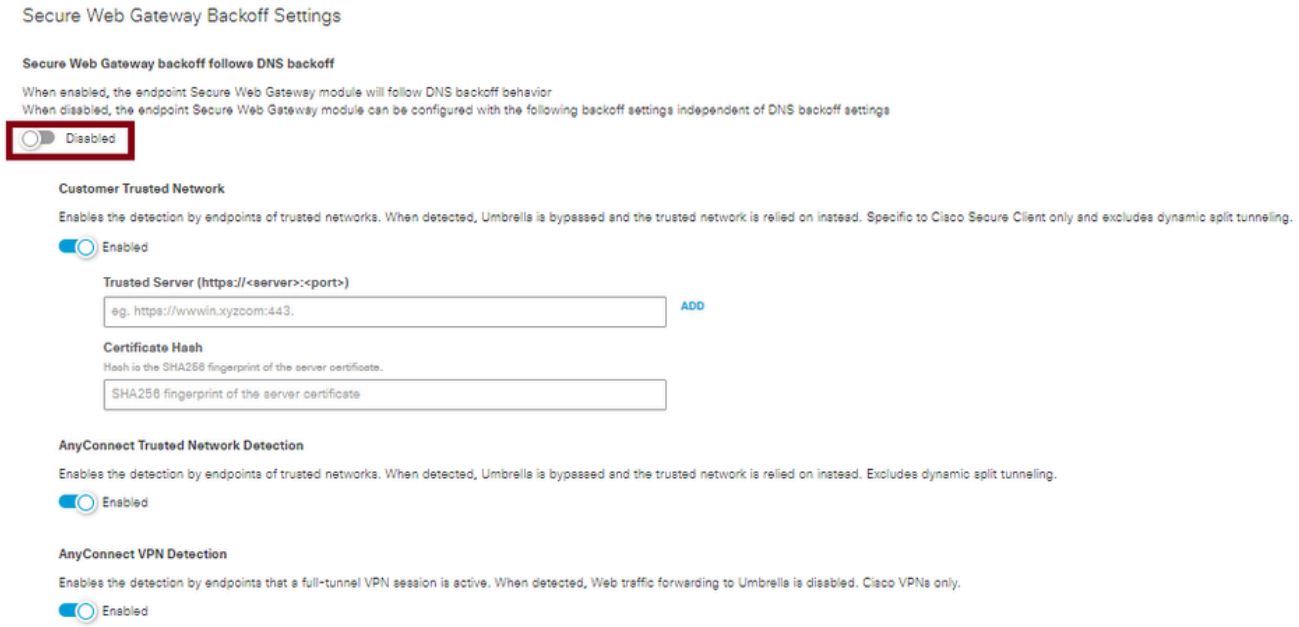
Esta nueva capacidad permite que el módulo SWG funcione independientemente del módulo DNS. Esta función está disponible para Cisco Secure Clients con la versión 5.1.3.62 y posteriores. Configure uno de los interruptores de retroceso SWG explícitos en el panel:

- Red de confianza del cliente: Una opción es utilizar la opción Customer Trusted Network en la configuración de respaldo SWG donde puede configurar un servidor interno que el cliente

pueda alcanzar para confirmar que está en la red protegida. Debe asegurarse de que el cliente puede acceder al servidor web, obtener un certificado en ese servidor y copiar el hash del certificado en el panel de Umbrella.

Las otras dos opciones se aplican exclusivamente a las conexiones VPN:

- Detección de redes de confianza AnyConnect
- Detección de VPN AnyConnect



27886005743764

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).