Comprensión del flujo de tráfico proxy no HTTP(S) de gateway en varias nubes

Contenido

Introducción

Este documento describe cómo Cisco Multicloud Defense Gateway maneja el tráfico TCP (que no sea la web), cuando se configura un proxy de reenvío.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Conocimientos básicos de cloud computing
- Conocimiento básico de redes informáticas

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Proxy

Un proxy actúa como intermediario para dos terminales de red. Funciona como un gateway que realiza la transición de una red a otra para aplicaciones específicas. Los proxies controlan y simplifican la complejidad de las solicitudes a través del proceso de solicitud y las capacidades de

reenvío. Proporcionan diferentes niveles de funcionalidad, seguridad y privacidad, y resultan beneficiosos para la navegación web y la protección de datos.

.

Multicloud Gateway Forward Proxy

Este diagrama muestra el flujo de red cuando el gateway de nube múltiple se coloca en la ruta entre el cliente y el servidor y el gateway de nube múltiple se configura para actuar como proxy de reenvío.

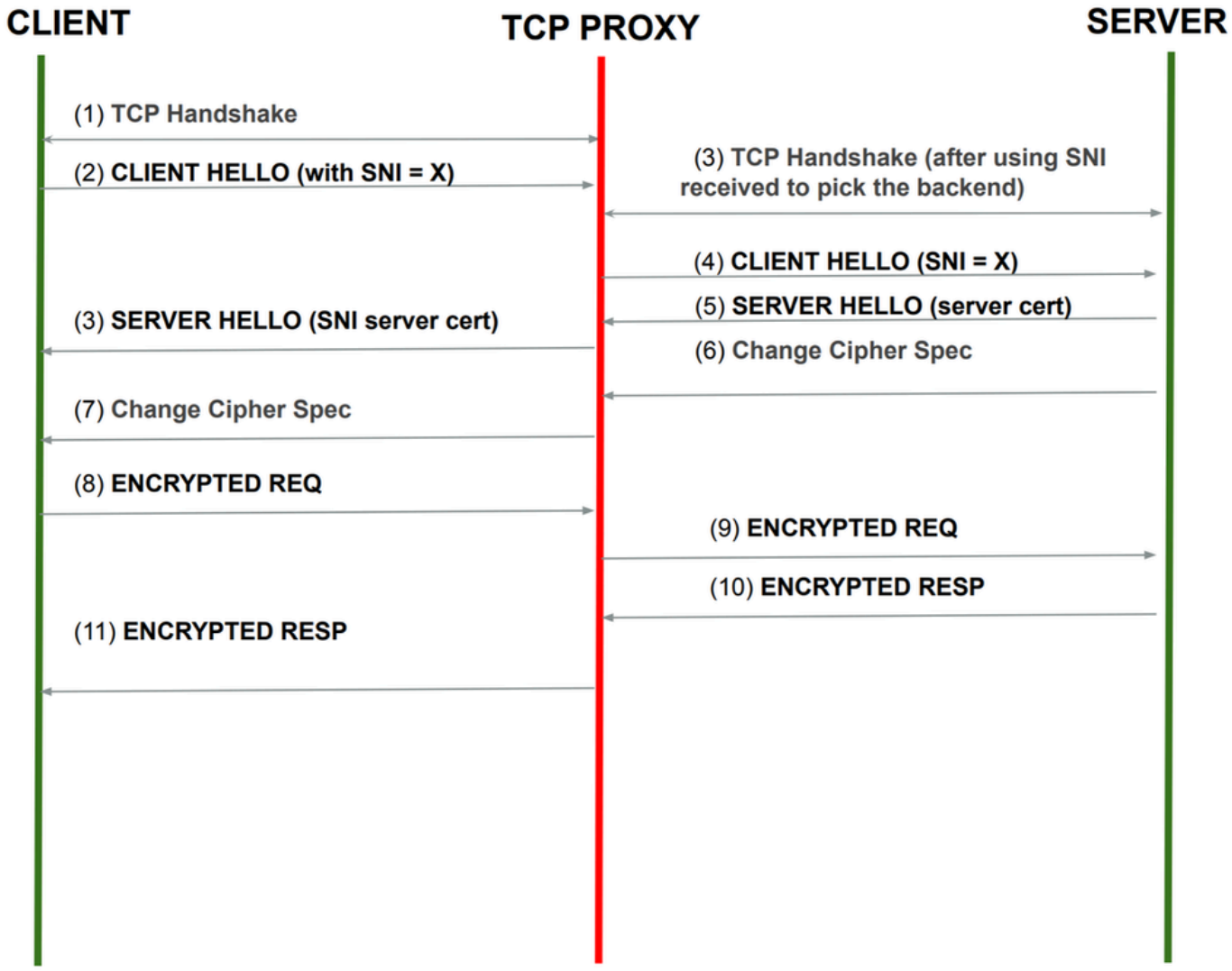
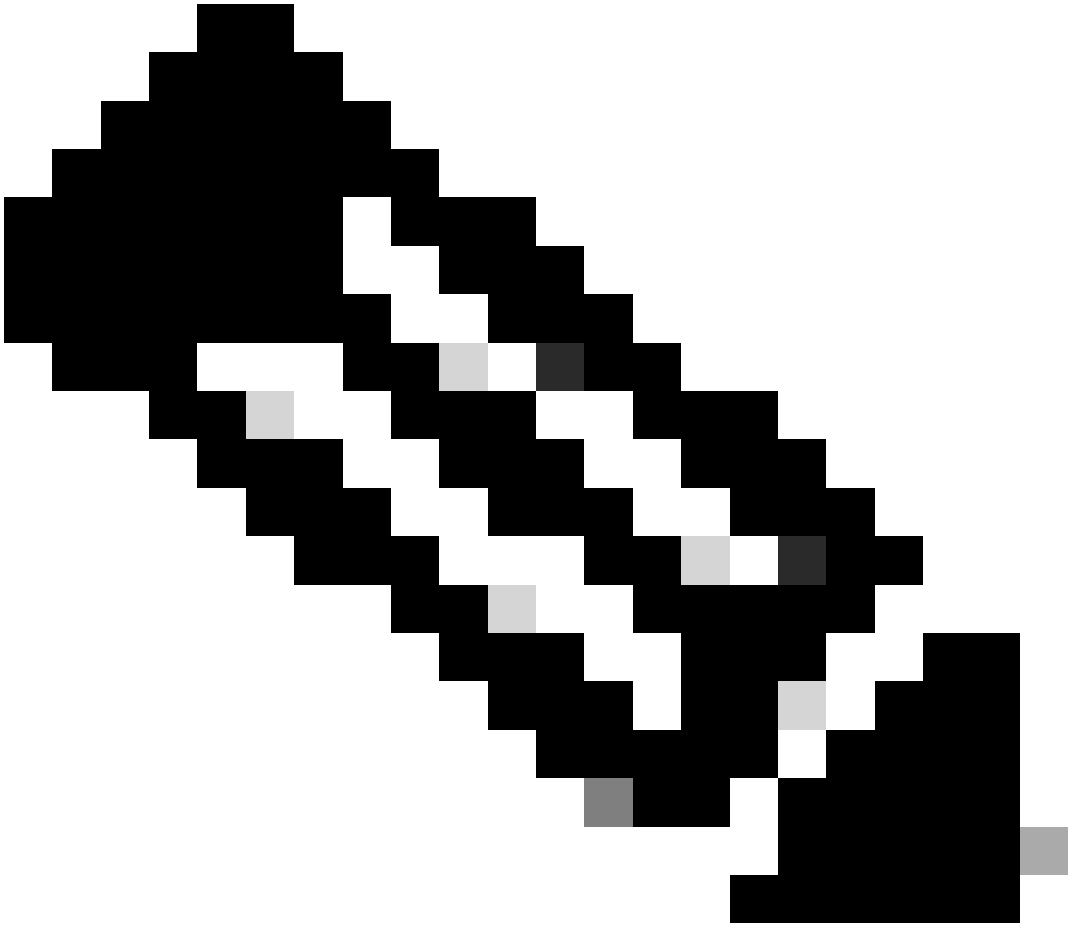
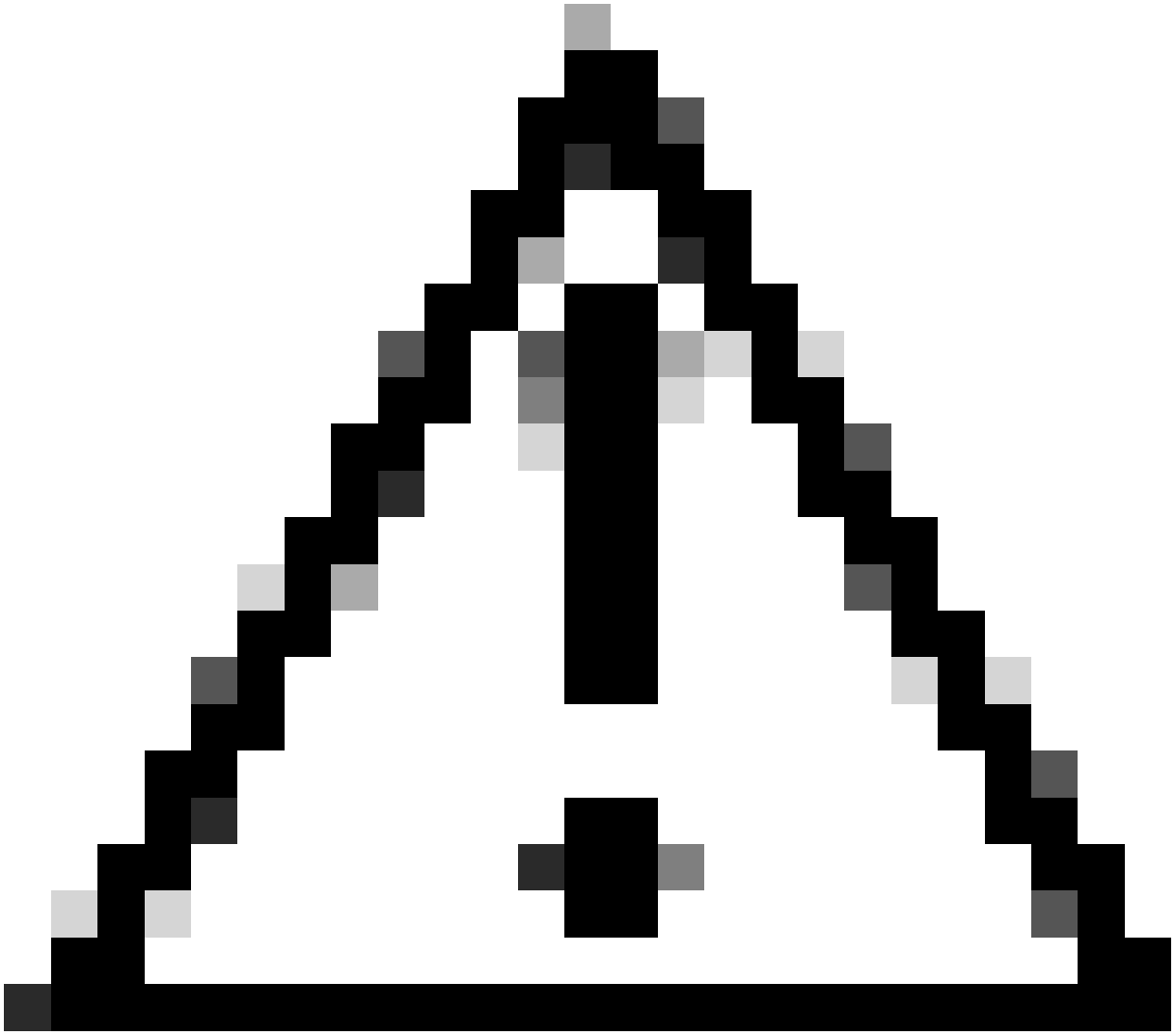


Imagen: proxy de reenvío MCD



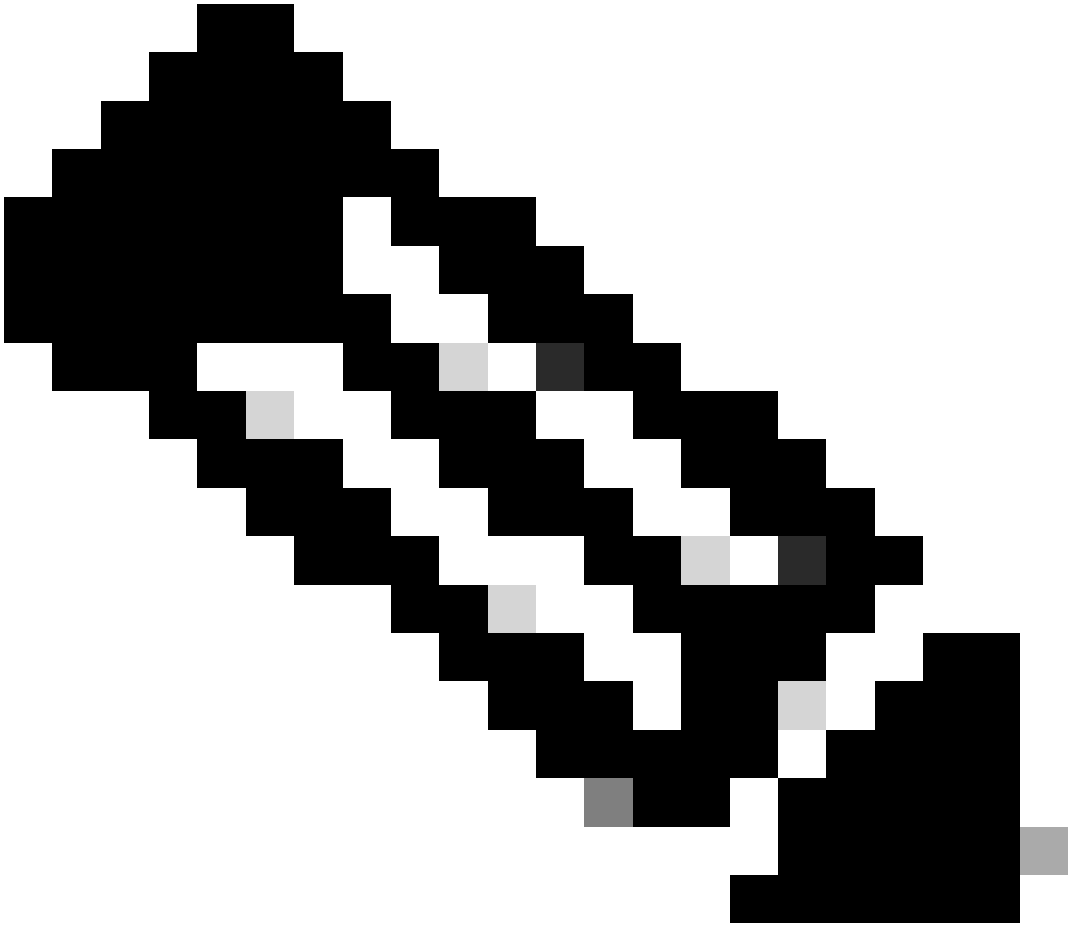
Nota: Este proceso se aplica al tráfico SSH cuando el cliente está configurado para utilizar el gateway de nube múltiple como proxy para conectarse al servidor SSH.

1. El protocolo de enlace de 3 vías TCP se inicia entre el cliente y el gateway de nube múltiple.
2. El cliente envía un mensaje de SALUDO DE CLIENTE al servidor. Este mensaje de SALUDO DE CLIENTE contiene el identificador de nombre de servidor (SNI). La puerta de enlace intercepta este paquete y ejecuta la política de filtrado de FQDN.



Precaución: Ciertas aplicaciones configuradas para utilizar protocolos de negociación automática, como las que determinan la versión de SSH, no deben transmitir el mensaje de saludo del cliente.

3. Si se permite el tráfico, el gateway inicia una nueva solicitud de protocolo de enlace TCP al servidor y reenvía el saludo del cliente. (según lo recibido del cliente)



Nota: Si el servidor no ha recibido ningún paquete del gateway de la nube múltiple, podría deberse a que el cliente no envió el saludo del cliente.

4. El gateway multicloud reenvió el saludo del servidor al cliente.

5. Después del intercambio de certificados, todos los paquetes se envían como están sin ninguna acción

Información Relacionada

- Guía del usuario de Cisco Multicloud Defense - Perfil de filtro de FQDN [Cisco Defense Orchestrator] - Cisco
- Preguntas frecuentes - Cisco

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).