Comprensión del flujo de tráfico HTTPS de Proxy de Multicloud Defense Gateway

Contenido

Introducción

Este documento describe cómo Cisco Multicloud Defense Gateway maneja el tráfico HTTPS cuando se configura la acción de proxy de reenvío o reverso.

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.

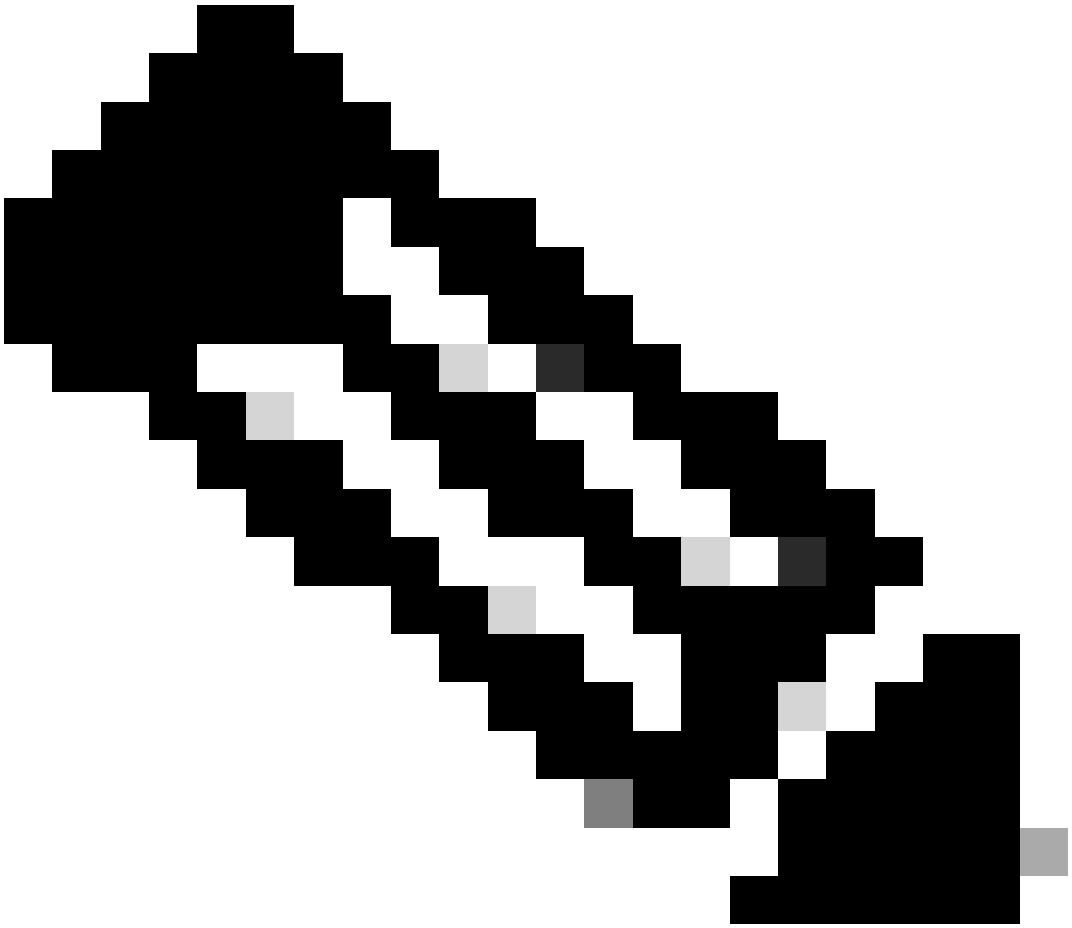
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Proxy de reenvío explícito

Proxy de reenvío explícito significa que la configuración de red del equipo está configurada para utilizar explícitamente el proxy. El tráfico del cliente está destinado al servidor proxy y el servidor proxy lo examina antes de reenviar el tráfico al destino real.

Proxy de reenvío explícito (con excepción de descifrado)

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



Nota: Las excepciones de descifrado hacen referencia a situaciones en las que prefiere que Multicloud Gateway no descifre ni inspeccione el tráfico, que a menudo se aplica a sitios web financieros, sanitarios y gubernamentales. En estas situaciones, puede activar excepciones de descifrado para FQDN específicos.

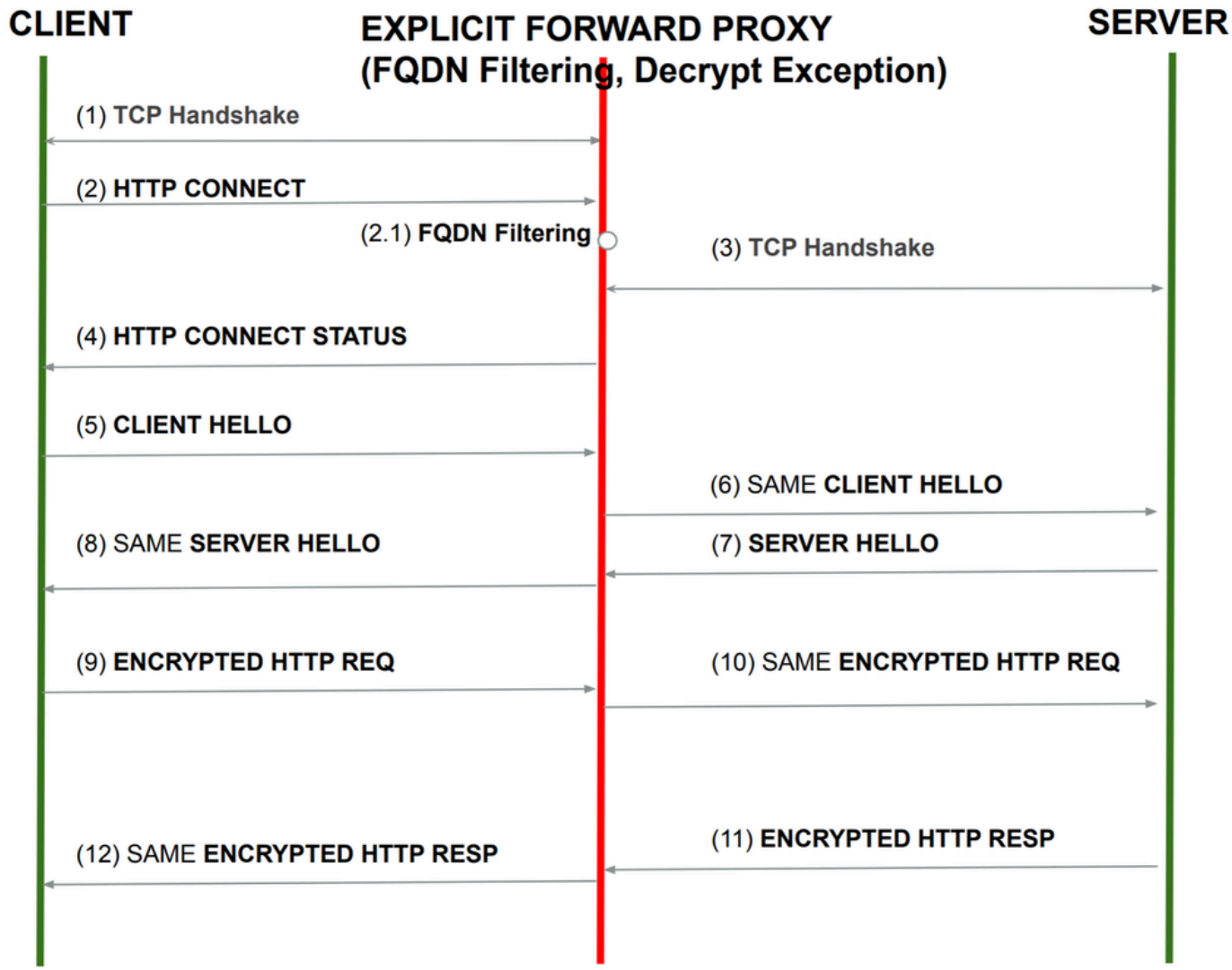


Imagen: flujo de proxy de reenvío explícito (con excepción de descifrado)

[1] El protocolo de enlace TCP de 3 vías se inicia entre el cliente y el gateway de nube múltiple.

[2] Una vez finalizado el protocolo de enlace, el cliente envía HTTP CONNECT.

[3] En el encabezado CONNECT, el gateway en varias nubes identifica el FQDN y aplica la política de filtrado de FQDN.

[4] Si se permite el tráfico, el gateway inicia una nueva solicitud de protocolo de enlace TCP al servidor y reenvía HTTP CONNECT.

[5] El mensaje de respuesta HTTP STATUS se reenvía de forma transparente al cliente.

[6] A partir de este momento, todos los mensajes se envían directamente sin ninguna interceptación

Proxy de reenvío explícito (con descifrado)

Este es el flujo de tráfico, mientras que el proxy de reenvío explícito se configura para descifrar el tráfico.

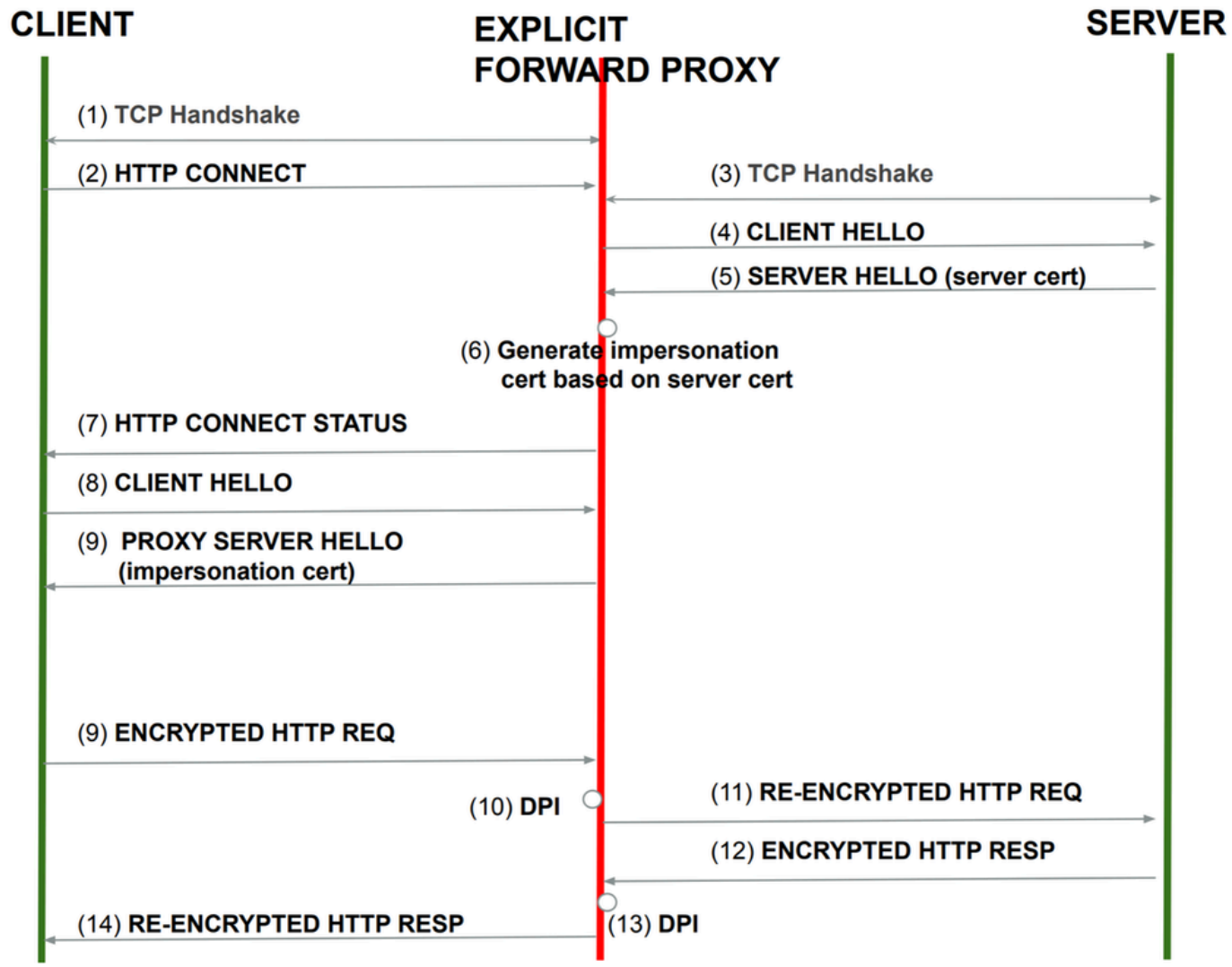


Imagen - Proxy de reenvío explícito (con descifrado)

[1] El protocolo de enlace TCP de 3 vías se inicia entre el cliente y el gateway de nube múltiple.

[2] Una vez finalizado el protocolo de enlace, el cliente envía HTTP CONNECT.

[3] En el encabezado CONNECT, el gateway en varias nubes identifica el FQDN y aplica la política de filtrado de FQDN.

[4] La puerta de enlace de nube múltiple inicia el protocolo de enlace TCP con el servidor.

[5] Después de que el intercambio de señales TLS finalizara correctamente entre la puerta de enlace de nube múltiple y el servidor, la puerta de enlace de nube múltiple emitió un certificado para el tráfico descifrado entre el cliente y la puerta de enlace de nube múltiple.

[6] A partir de este momento, todo el tráfico entre el cliente y el servidor se descifra y se cifra de nuevo.

Proxy de reenvío transparente

Proxy de reenvío transparente (con excepción de descifrado)

El siguiente escenario describe el proceso cuando el tráfico tiene como destino un servidor público y el gateway tiene una configuración para el proxy de reenvío con una excepción de descifrado.

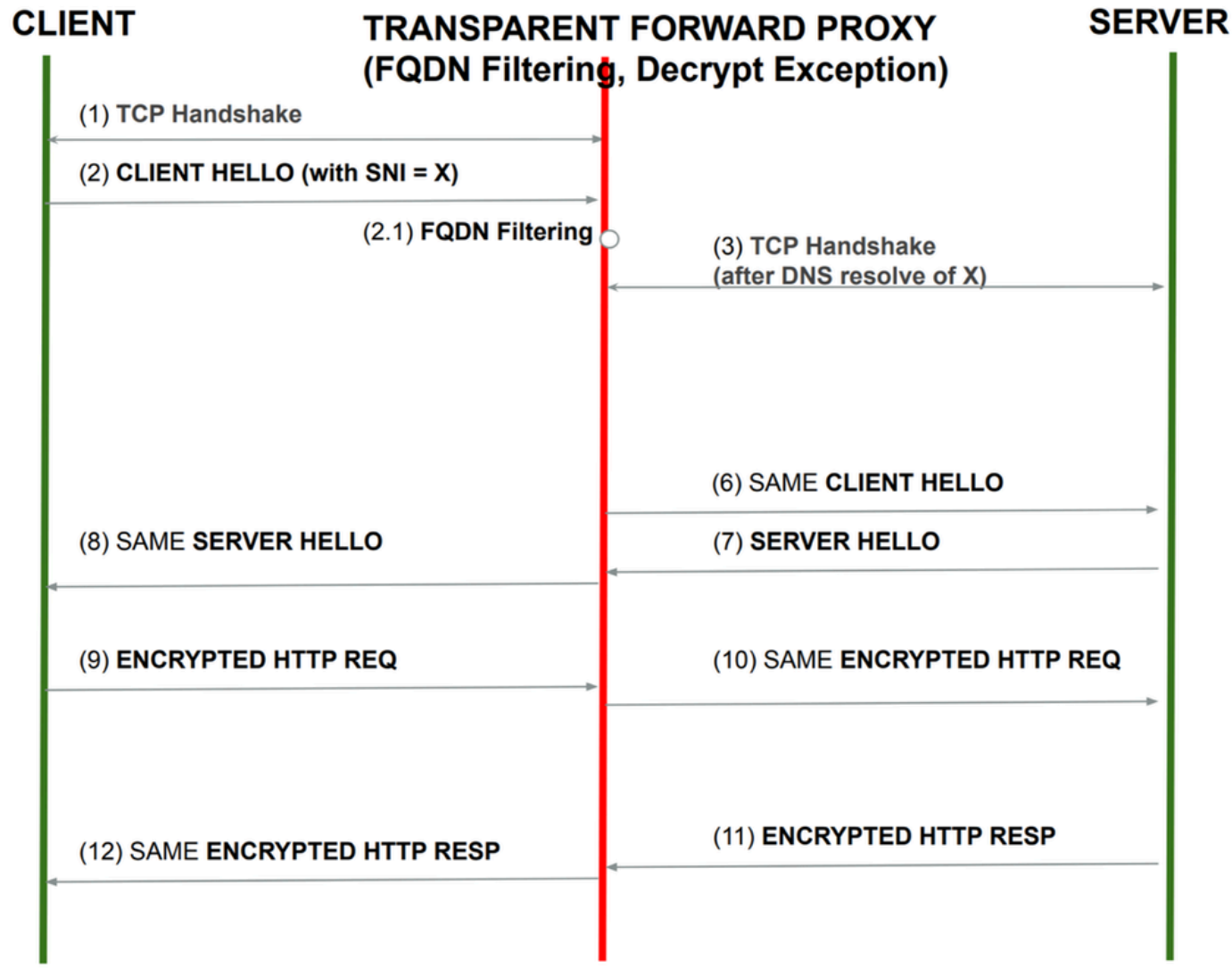


Imagen: proxy de reenvío transparente (con excepción de descifrado)

[1] El gateway de nube múltiple responde al protocolo de enlace TCP.

[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). El gateway intercepta este paquete y ejecuta la política de filtrado de FQDN.

[3] Si se permite el tráfico y se configura la excepción de descifrado para la URL, el gateway de nube múltiple realiza otra resolución DNS para el SNI.

[4] La puerta de enlace de nube múltiple inicia un protocolo de enlace TCP con el servidor.

[5] La puerta de enlace de nube múltiple reenvía el mismo SALUDO DE CLIENTE al servidor (tal y como lo recibió del cliente).

[6] El SALUDO DEL SERVIDOR recibido del servidor se reenvía tal cual sin ninguna modificación.

[7] A partir de este punto, todos los paquetes se envían tal cual sin ninguna acción

Proxy de reenvío transparente (con descifrado)

El siguiente escenario describe el proceso cuando el tráfico tiene como destino un servidor público y el gateway tiene una configuración para que el proxy de reenvío descifre el tráfico.

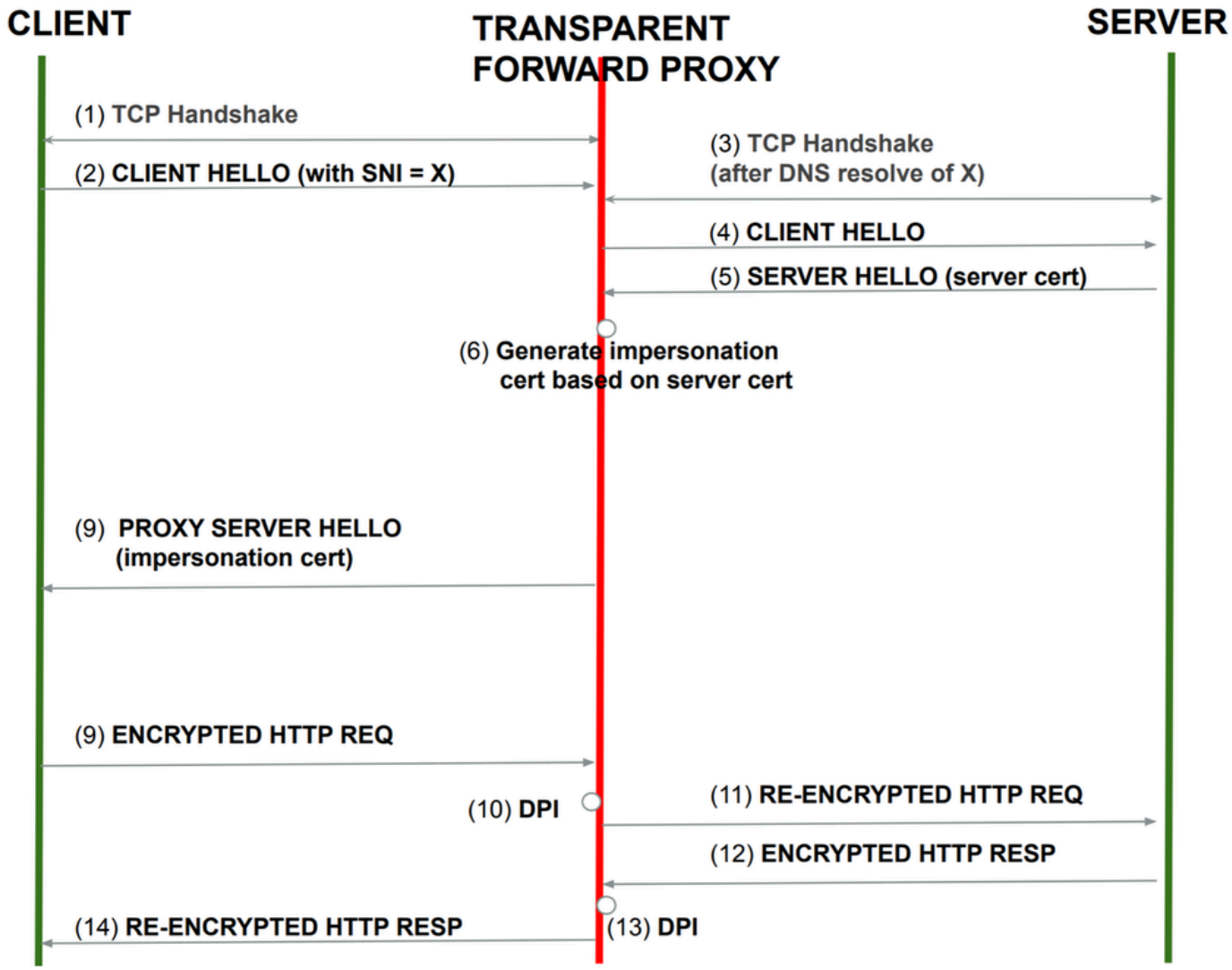


Imagen - Proxy de reenvío transparente (con descifrado)

[1] El gateway de nube múltiple responde al protocolo de enlace TCP.

[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). El gateway intercepta este paquete y ejecuta la política de filtrado de FQDN.

[3] Si se permite el tráfico y se configura el descifrado para la URL, el gateway de nube múltiple realiza otra resolución DNS para el SNI.

[4] La puerta de enlace de nube múltiple comienza a iniciar un protocolo de enlace TCP con el servidor.

[5] Después de que el intercambio de señales TLS finalizara correctamente entre la puerta de enlace de nube múltiple y el servidor, la puerta de enlace de nube múltiple emitió un certificado para el tráfico descifrado entre el cliente y la puerta de enlace de nube múltiple.

[6] A partir de este momento, todo el tráfico entre el cliente y el servidor se descifra y se cifra de nuevo.

Información Relacionada

- Guía del usuario de Cisco Multicloud Defense - Perfil de filtro de FQDN [Cisco Defense Orchestrator] - Cisco
- Guía del usuario de Cisco Multicloud Defense - Gestionar gateways [Cisco Defense Orchestrator] - 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).