Comprendre le flux de trafic HTTPS du proxy Multicloud Defense Gateway

Table des matières

Introduction

Ce document décrit comment la passerelle de défense multicloud Cisco gère le trafic HTTPS lorsque l'action de transfert ou de proxy inverse est configurée.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Connaissance de base du cloud computing
- Connaissances de base des réseaux informatiques

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

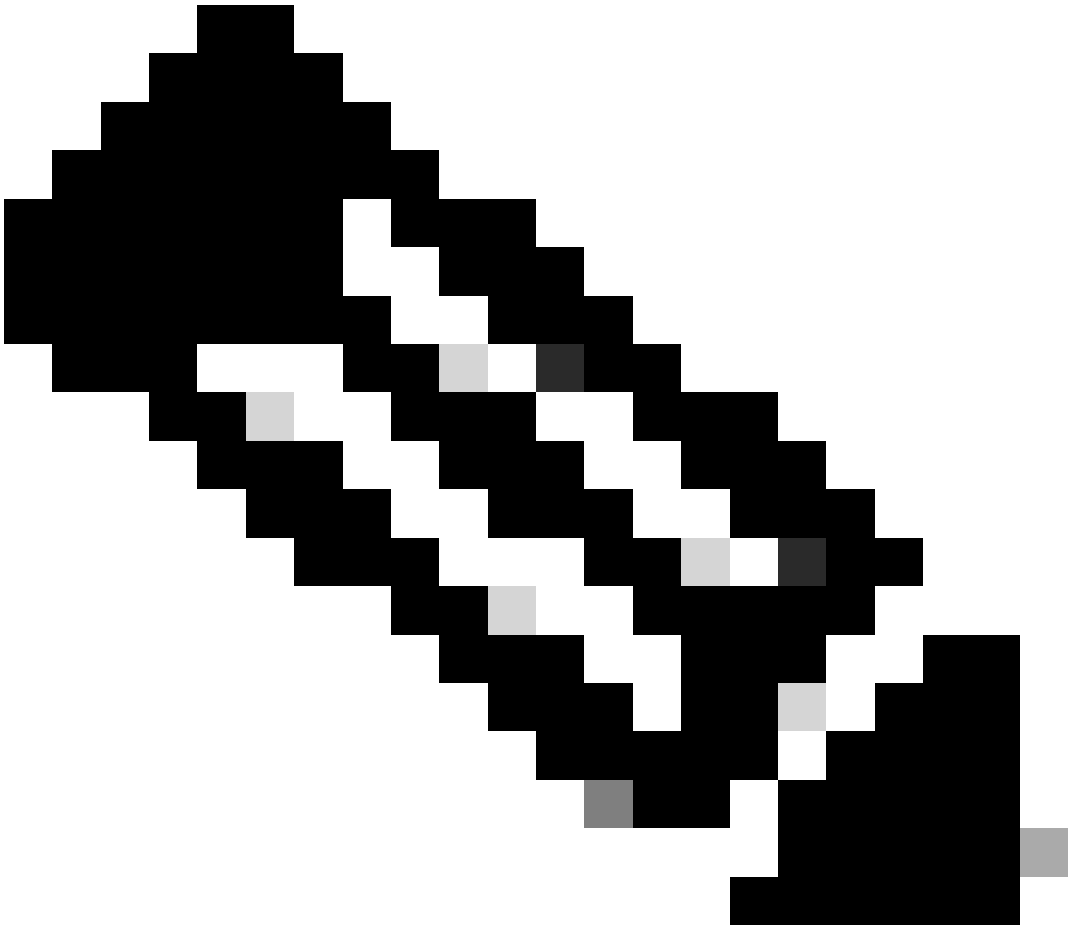
Proxy de transfert explicite

Un proxy de transfert explicite signifie que les paramètres réseau de votre ordinateur sont

configurés pour utiliser explicitement le proxy. Le trafic provenant du client est destiné au serveur proxy et le serveur proxy l'examine avant de le transférer à la destination réelle.

Proxy de transfert explicite (avec exception de déchiffrement)

Ce schéma montre le flux réseau lorsque la passerelle Multicloud est placée sur le chemin entre le client et le serveur Web et que la passerelle Multicloud est configurée pour agir en tant que proxy de transfert avec une exception de déchiffrement.



Remarque : les exceptions de déchiffrement concernent les scénarios dans lesquels vous préférez que la passerelle multicloud ne déchiffre pas et n'inspecte pas le trafic, souvent applicable aux sites Web des services financiers, de santé et gouvernementaux. Dans ces situations, vous activez des exceptions de déchiffrement pour des FQDN spécifiques.

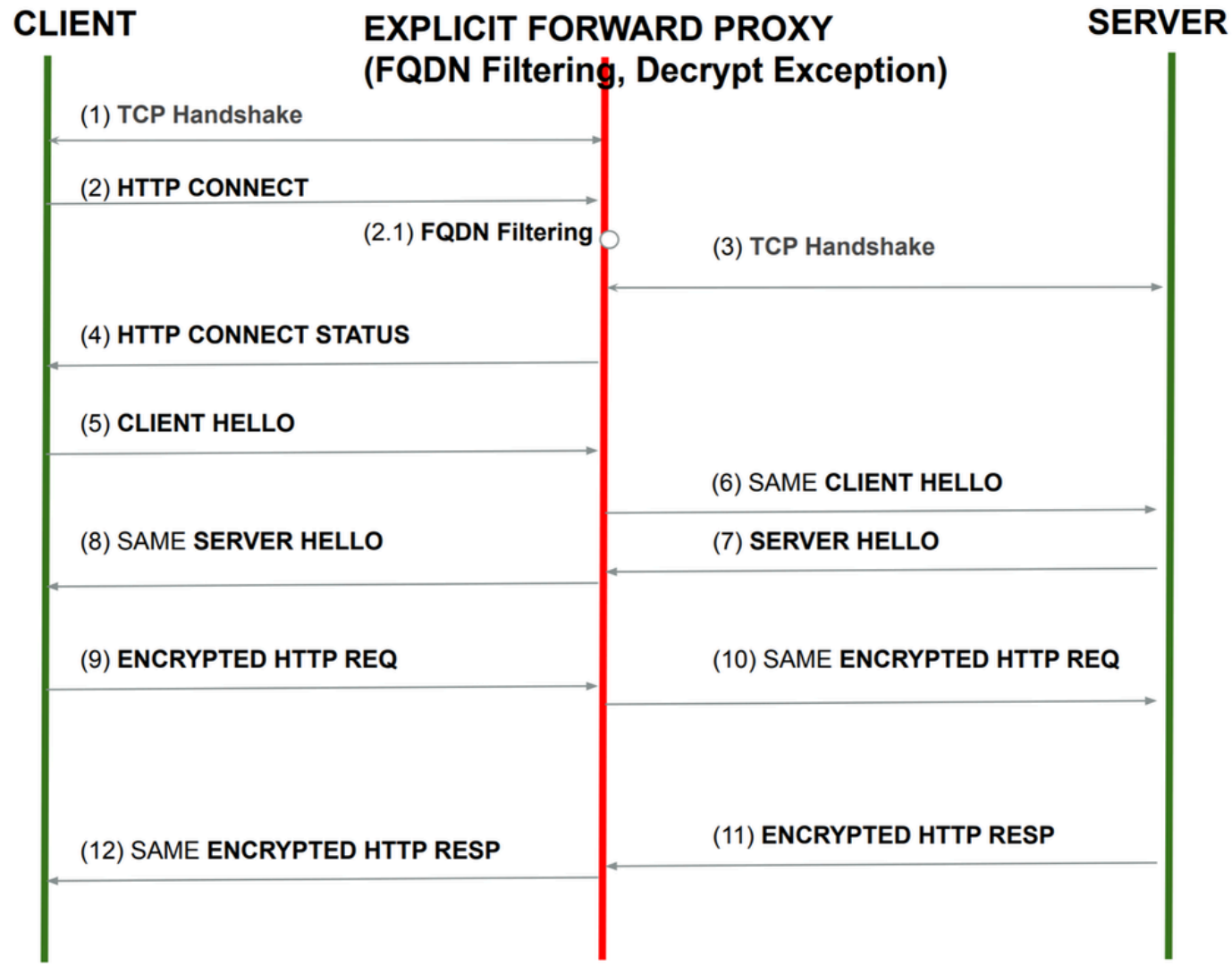


Image - Flux du proxy de transfert explicite (avec exception de déchiffrement)

[1] La connexion TCP en trois étapes est initiée entre le client et la passerelle Multicloud.

[2] Une fois la connexion établie, le client envoie HTTP CONNECT.

[3] À partir de l'en-tête CONNECT, la passerelle multicloud identifie le nom de domaine complet et applique la stratégie de filtrage du nom de domaine complet.

[4] Si le trafic est autorisé, la passerelle initie une nouvelle requête d'échange TCP au serveur et transfère la requête HTTP CONNECT.

[5] Le message de réponse HTTP STATUS est transmis de manière transparente au client.

[6] À partir de ce moment, tous les messages sont envoyés directement sans aucune interception

Proxy de transfert explicite (avec déchiffrement)

Voici le flux de trafic, tandis que le proxy de transfert explicite est configuré pour déchiffrer le trafic.

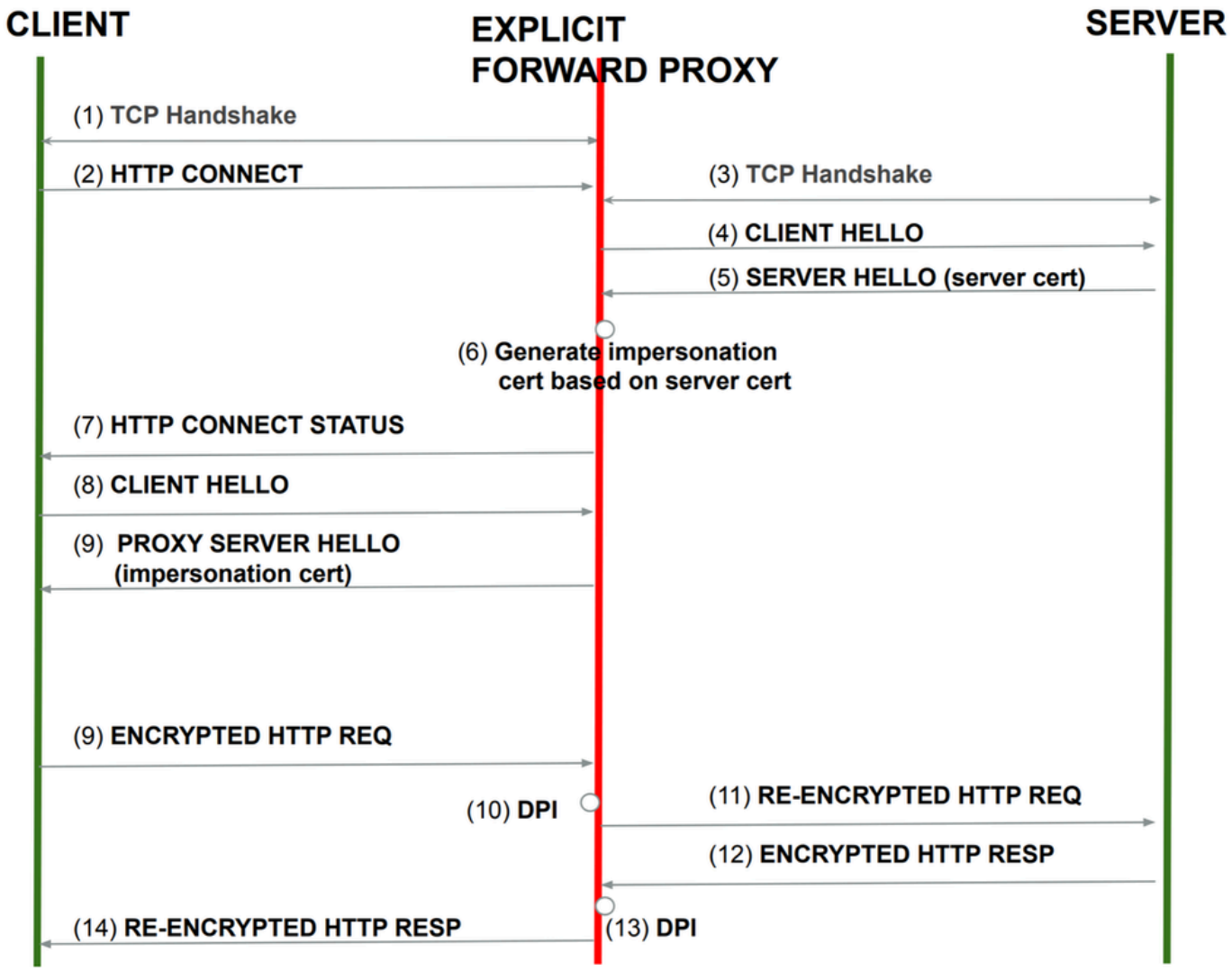


Image - Proxy de transfert explicite (avec décryptage)

[1] La connexion TCP en trois étapes est initiée entre le client et la passerelle Multicloud.

[2] Une fois la connexion établie, le client envoie HTTP CONNECT.

[3] À partir de l'en-tête CONNECT, la passerelle multicloud identifie le nom de domaine complet et applique la stratégie de filtrage du nom de domaine complet.

[4] La passerelle multicloud démarre la connexion TCP avec le serveur.

[5] Une fois la connexion TLS établie avec succès entre la passerelle multicloud et le serveur, la passerelle multicloud a émis un certificat pour le trafic déchiffré entre le client et la passerelle multicloud.

[6] À partir de ce moment, tout le trafic entre le client et le serveur est déchiffré et chiffré à nouveau.

Proxy de transfert transparent

Proxy de transfert transparent (avec exception de déchiffrement)

Le scénario suivant décrit le processus lorsque le trafic cible un serveur public et que la passerelle a une configuration pour le proxy de transfert avec une exception de déchiffrement.

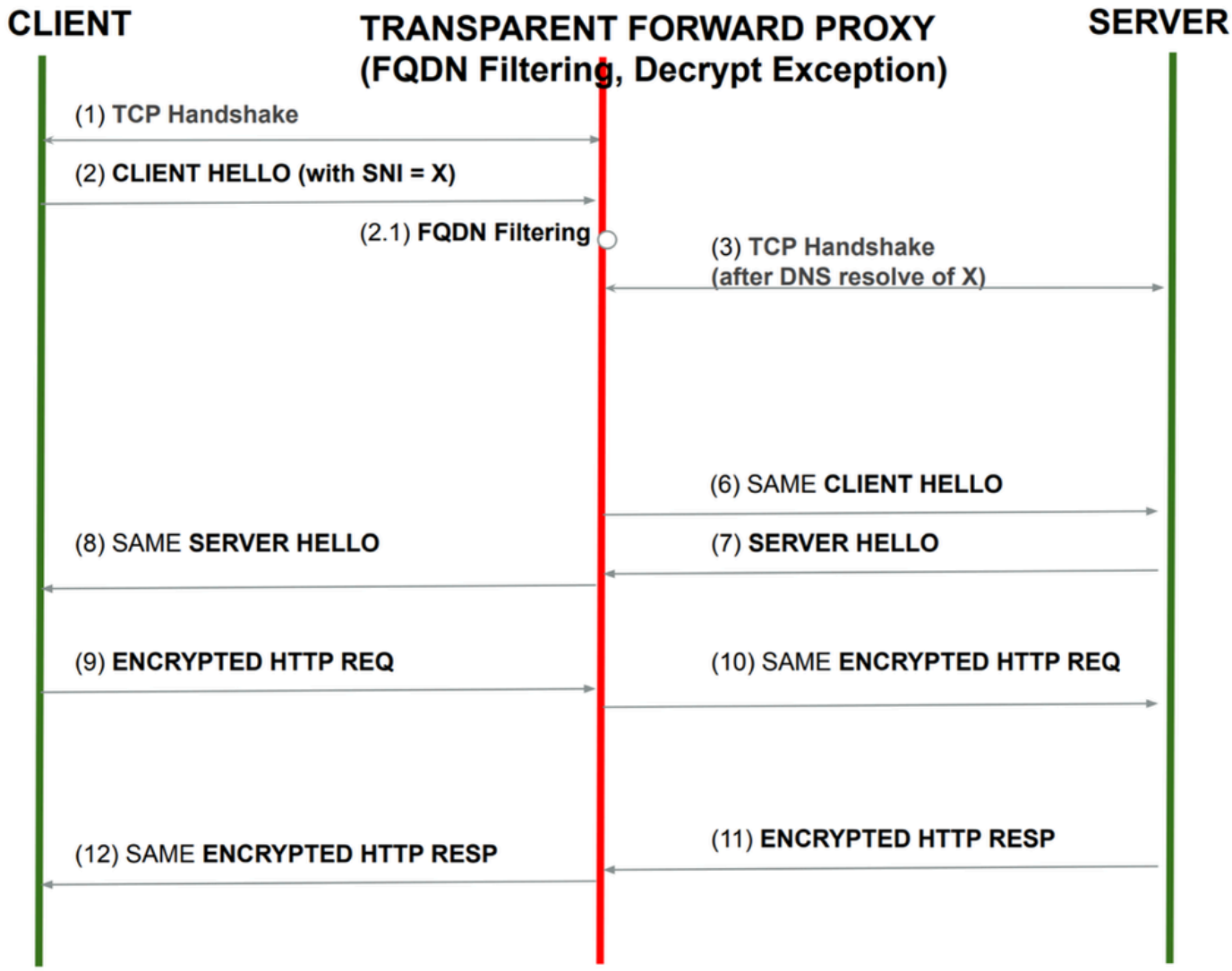


Image - Proxy de transfert transparent (avec exception de décryptage)

[1] La passerelle multicloud répond à la connexion TCP.

[2] Le client envoie un HELLO CLIENT au serveur. Ce HELLO CLIENT contient l'identifiant de nom de serveur (SNI). La passerelle intercepte ce paquet et exécute la stratégie de filtrage FQDN.

[3] Si le trafic est autorisé et que l'exception de déchiffrement est configurée pour l'URL, la passerelle Multicloud effectue une autre résolution DNS pour le SNI.

[4] La passerelle multicloud initie une connexion TCP avec le serveur.

[5] La passerelle multicloud transfère le même HELLO CLIENT au serveur (tel qu'il a été reçu du client).

[6] Le HELLO du SERVEUR reçu du serveur est transféré tel quel sans aucune modification.

[7] À partir de ce moment, tous les paquets sont envoyés tels quels sans aucune action

Proxy de transfert transparent (avec déchiffrement)

Le scénario suivant décrit le processus lorsque le trafic cible un serveur public et que la passerelle dispose d'une configuration permettant au proxy de transfert de déchiffrer le trafic.

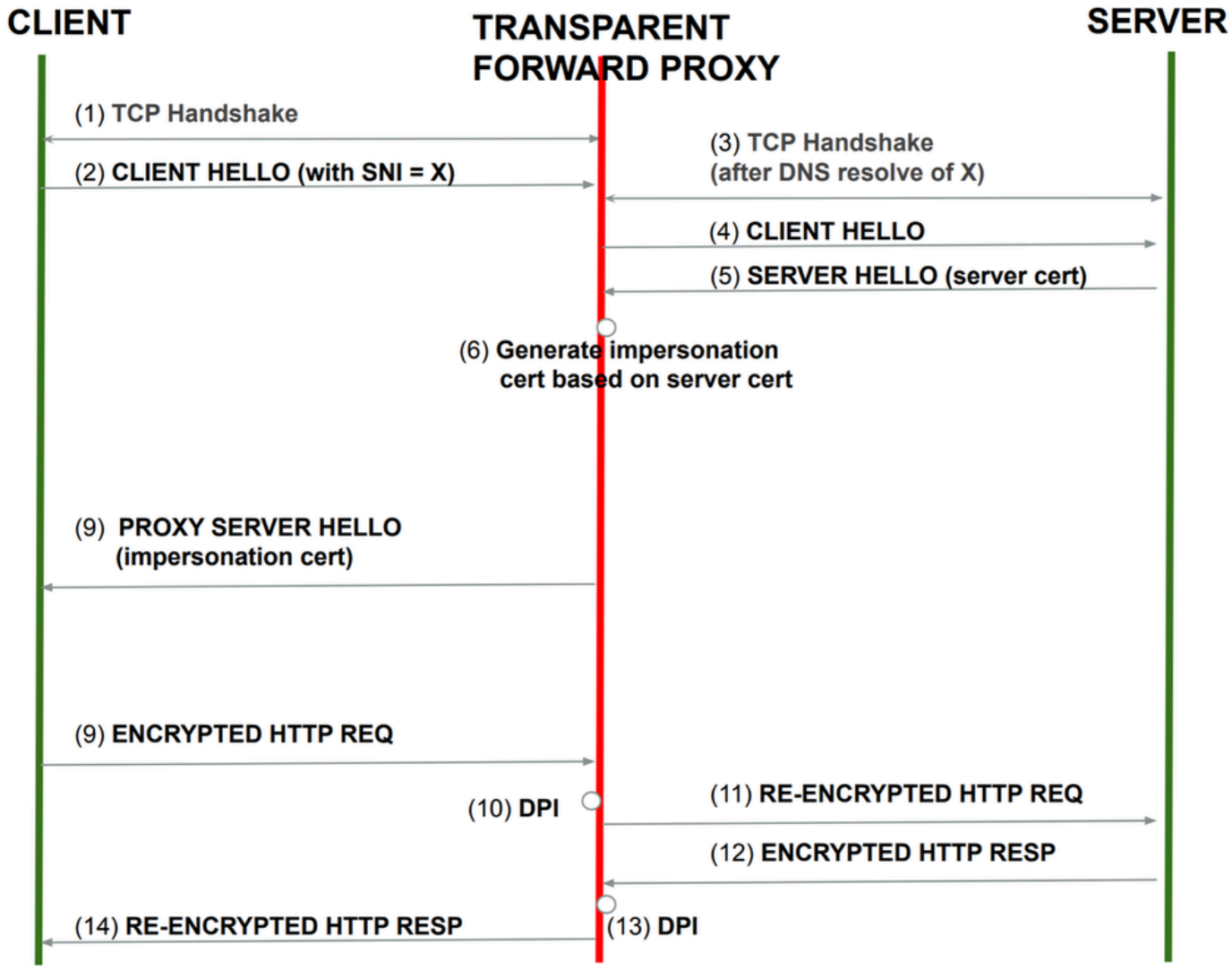


Image - Transparent Forward Proxy (avec déchiffrement)

[1] La passerelle multicloud répond à la connexion TCP.

[2] Le client envoie un HELLO CLIENT au serveur. Ce HELLO CLIENT contient l'identifiant de nom de serveur (SNI). La passerelle intercepte ce paquet et exécute la stratégie de filtrage FQDN.

[3] Si le trafic est autorisé et que le décodage est configuré pour l'URL, la passerelle Multicloud effectue une autre résolution DNS pour le SNI.

[4] La passerelle multicloud commence à établir une connexion TCP avec le serveur.

[5] Une fois la connexion TLS établie avec succès entre la passerelle multicloud et le serveur, la passerelle multicloud a émis un certificat pour le trafic déchiffré entre le client et la passerelle multicloud.

[6] À partir de ce moment, tout le trafic entre le client et le serveur est déchiffré et chiffré à nouveau.

Informations connexes

- Guide de l'utilisateur de Cisco Multicloud Defense - Profil de filtre FQDN [Cisco Defense Orchestrator] - Cisco
- Guide de l'utilisateur de Cisco Multicloud Defense - Gestion des passerelles [Cisco Defense Orchestrator] - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.