Comprendre le flux de trafic non HTTP(S) du proxy de passerelle multicloud

Table des matières

Introduction

Ce document décrit comment la passerelle de défense multicloud Cisco gère le trafic TCP (autre que le Web) lorsqu'un proxy de transfert est configuré.

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

Un proxy sert d'intermédiaire pour deux points d'extrémité réseau. Il fonctionne comme une passerelle qui passe d'un réseau à un autre pour des applications spécifiques. Les proxys contrôlent et simplifient la complexité des demandes grâce à leur processus de demande et à leurs fonctionnalités de transfert. Ils offrent différents niveaux de fonctionnalité, de sécurité et de confidentialité, et s'avèrent utiles pour la navigation Web et la protection des données.

.

Proxy de transfert de passerelle multicloud

Ce schéma montre le flux réseau lorsque la passerelle multicloud est placée sur le chemin entre le client et le serveur et que la passerelle multicloud est configurée pour agir en tant que proxy de transfert.

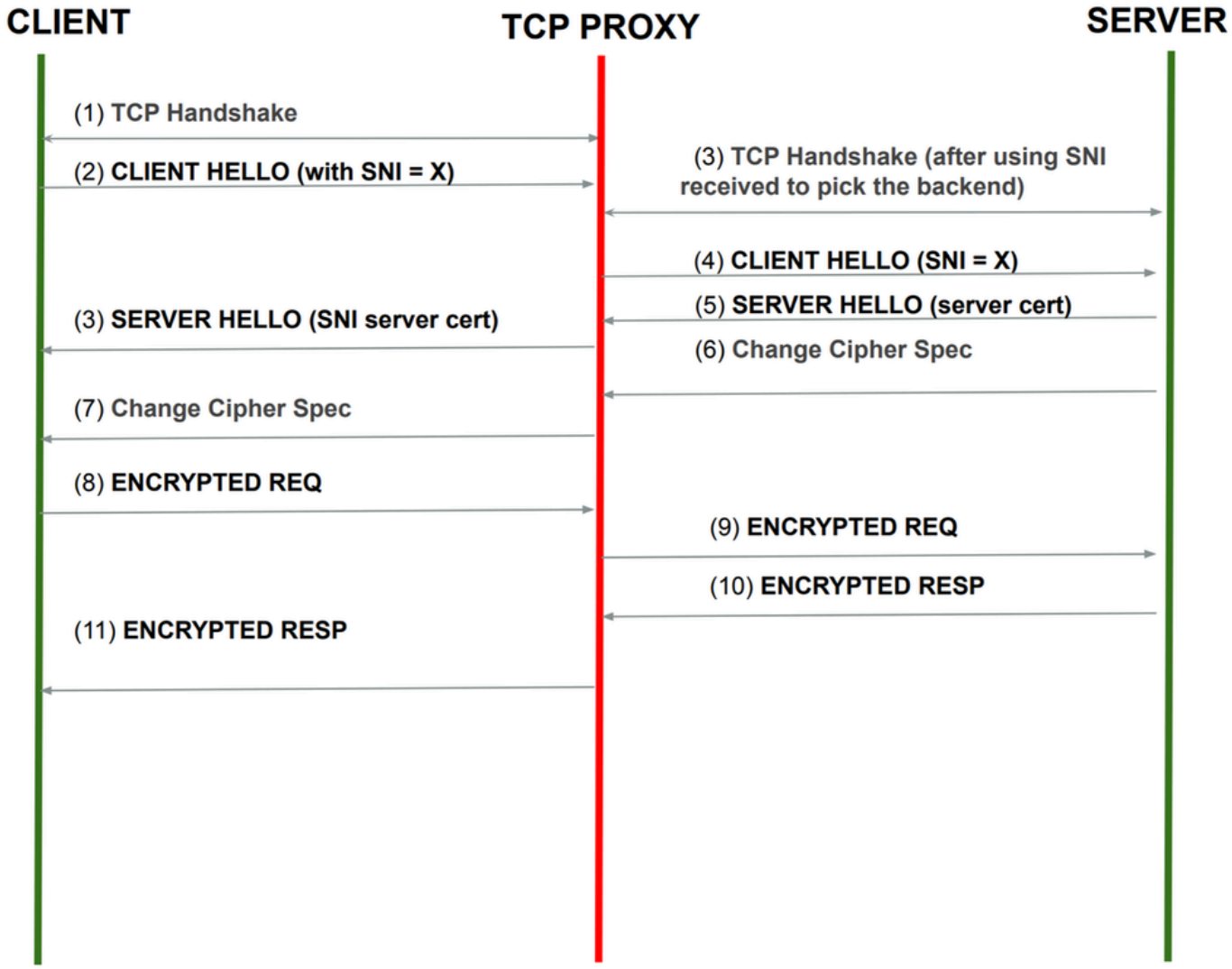
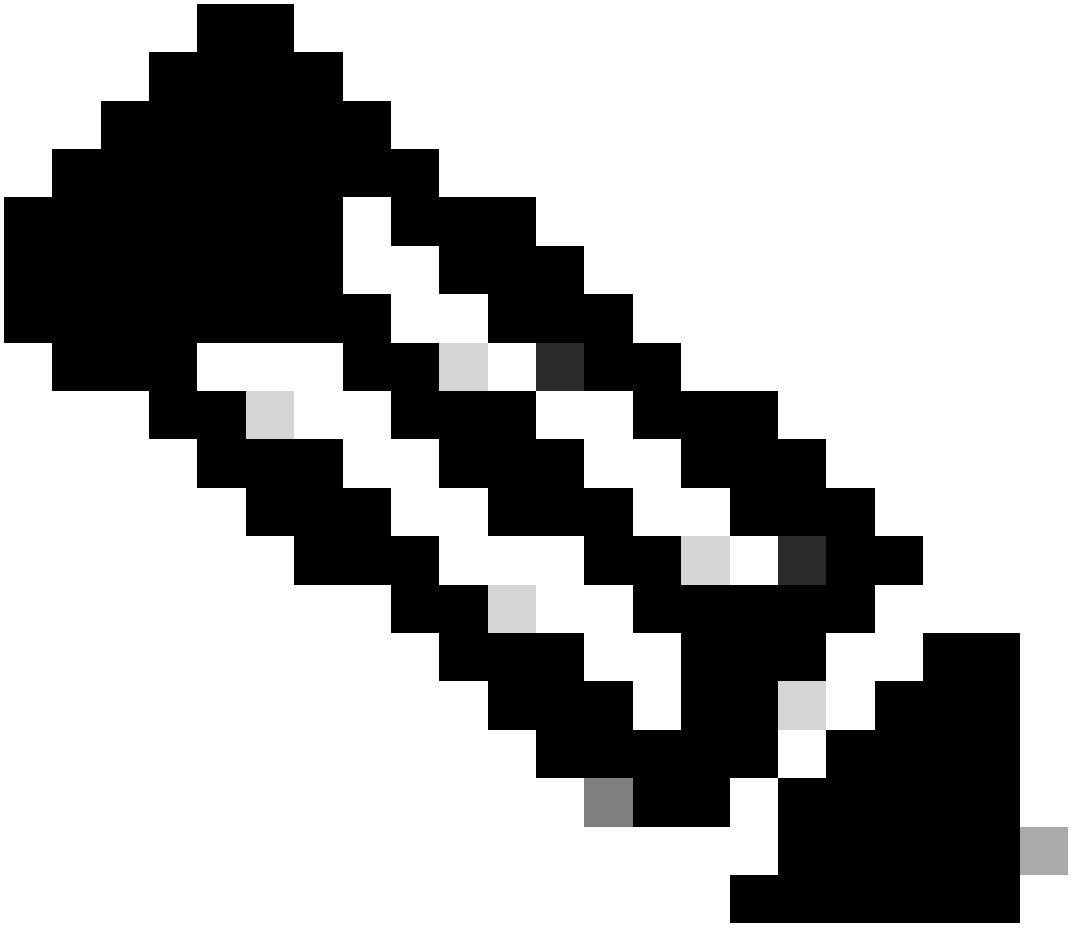
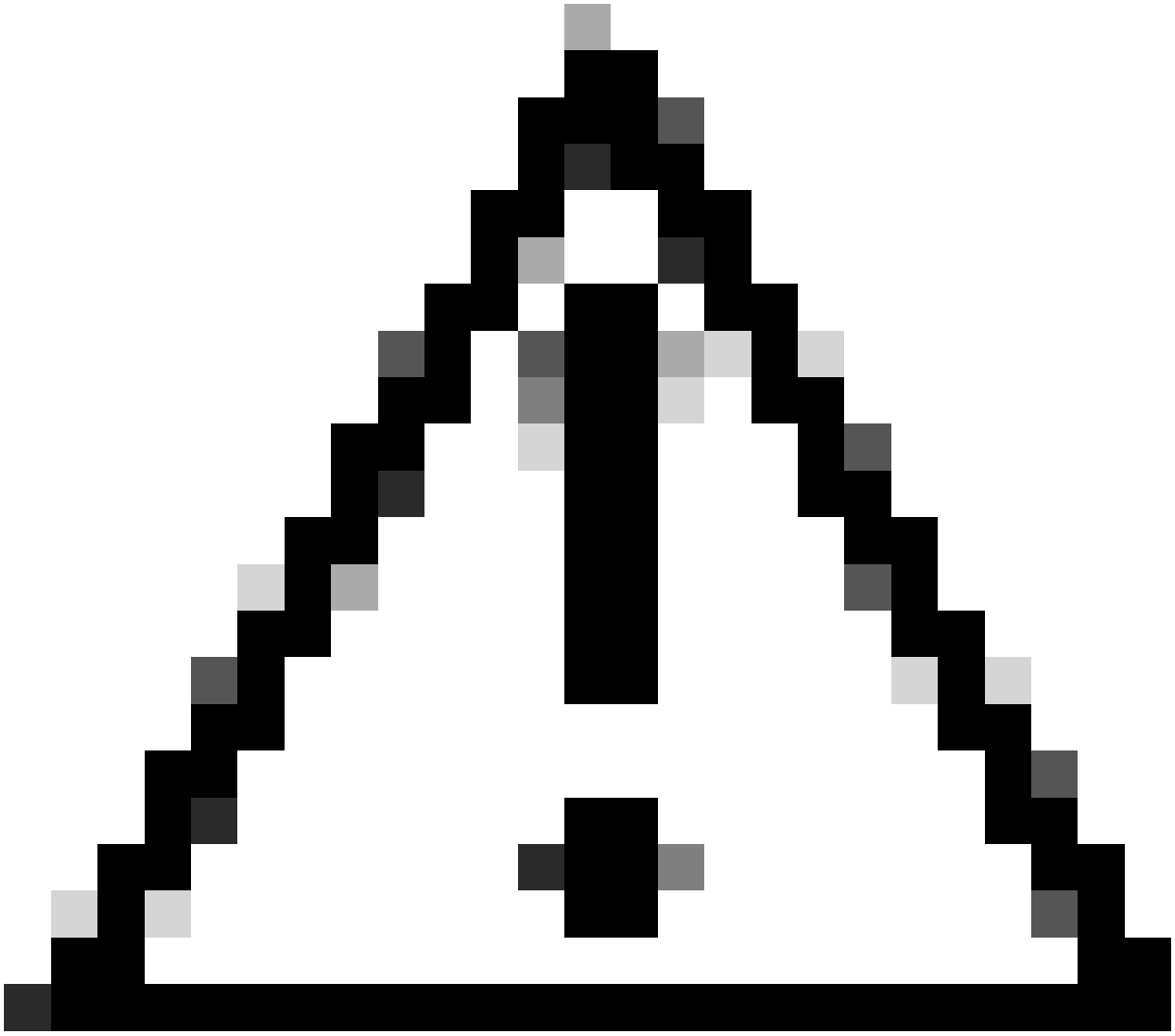


Image - Proxy de transfert MCD



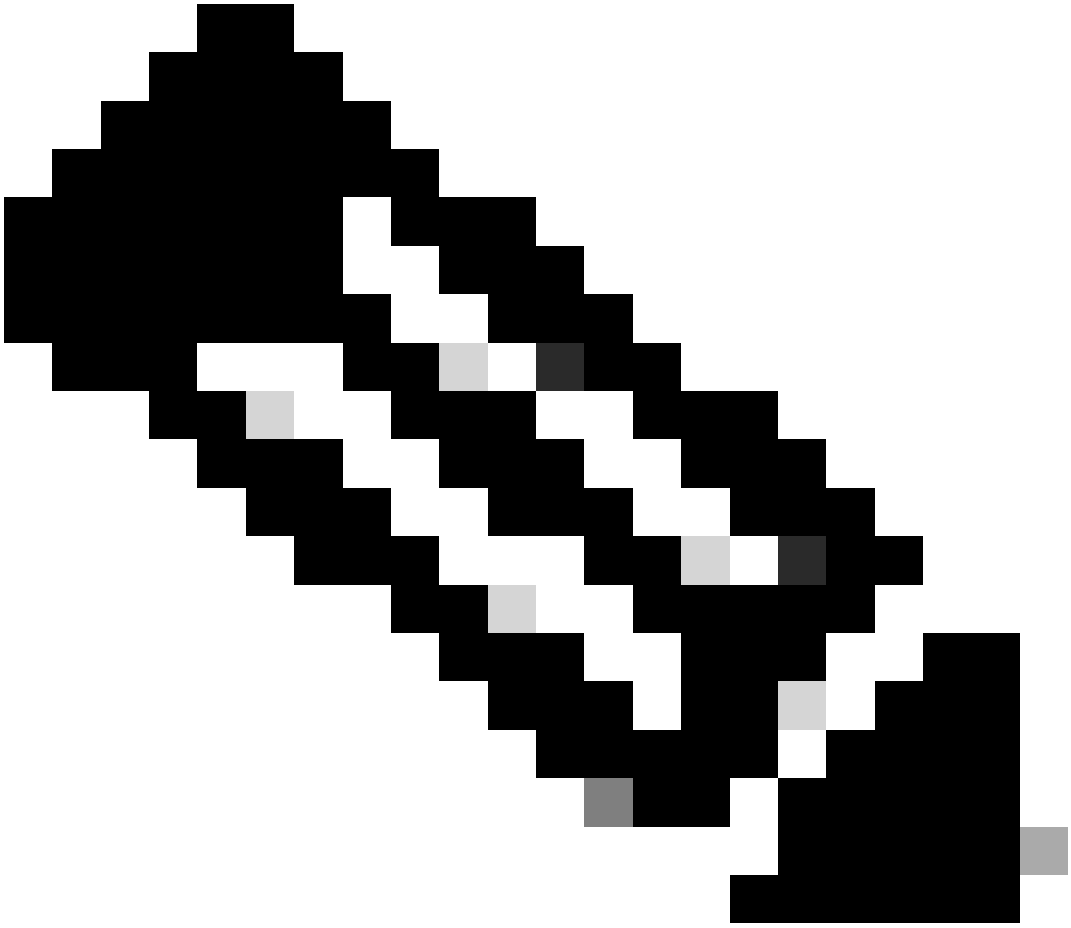
Remarque : ce processus s'applique au trafic SSH lorsque votre client est configuré pour utiliser la passerelle multicloud comme proxy pour se connecter au serveur SSH.

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



Attention : certaines applications configurées pour utiliser des protocoles de négociation automatique, telles que celles déterminant la version SSH, ne doivent pas transmettre le paquet Hello du client.

3. Si le trafic est autorisé, la passerelle initie une nouvelle requête d’échange TCP au serveur et transfère le paquet Hello du client. (tel que reçu du client)



Remarque : si le serveur n'a reçu aucun paquet de la passerelle multicloud, cela peut être dû au fait que le client n'a pas envoyé le paquet Hello du client.

4. La passerelle multicloud a transféré le paquet Hello du serveur au client.

5. Après l’échange de certificats, tous les paquets sont envoyés tels quels sans aucune action

Informations connexes

- Guide de l'utilisateur de Cisco Multicloud Defense - Profil de filtre FQDN [Cisco Defense Orchestrator] - Cisco
- FAQ - 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.