Multicloud Defense Gateway Proxy HTTPS-Datenverkehrsfluss verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie das Cisco Multicloud Defense Gateway den HTTPS-Datenverkehr behandelt, wenn die Vorwärts- oder Rückwärts-Proxy-Aktion konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Grundkenntnisse des Cloud Computing
- Grundkenntnisse der Computernetzwerke

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

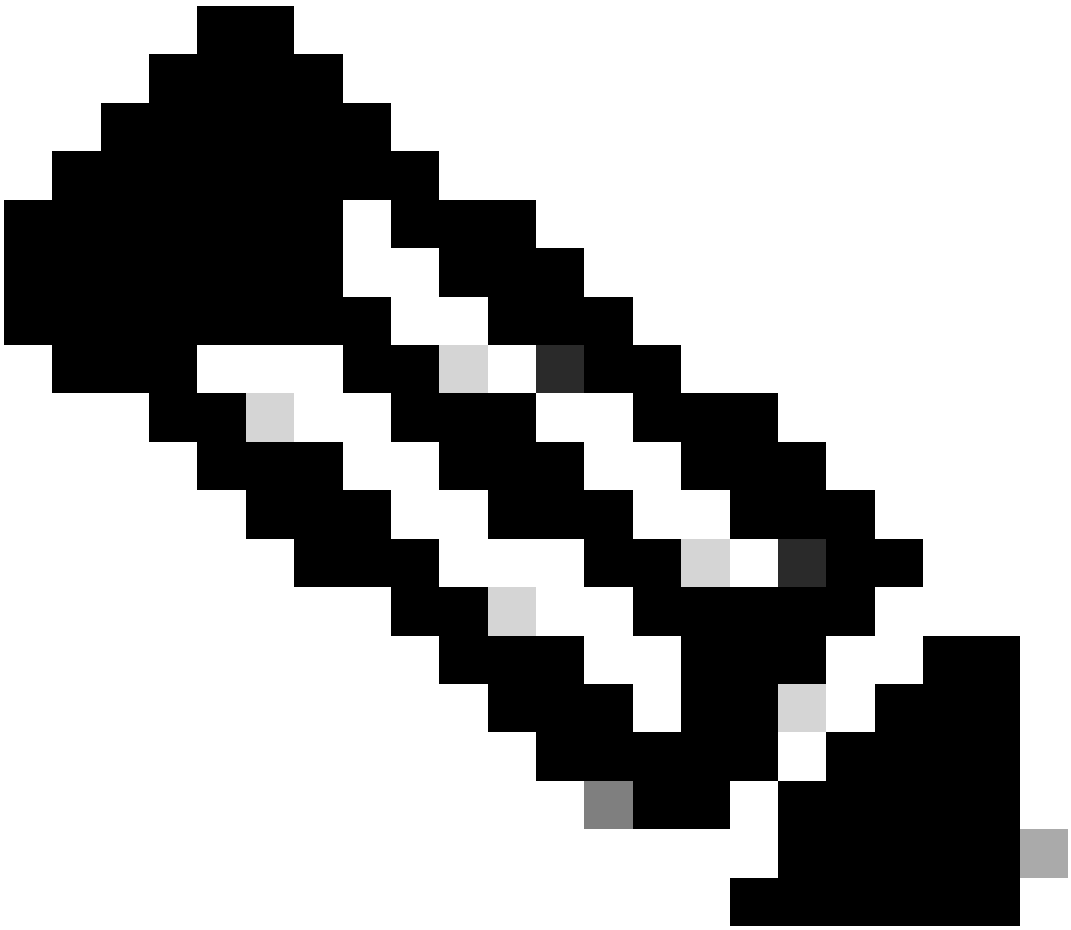
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Expliziter Weiterleitungsproxy

Ein expliziter Weiterleitungsproxy bedeutet, dass die Netzwerkeinstellungen Ihres Computers so konfiguriert sind, dass sie den Proxy explizit verwenden. Der Datenverkehr vom Client wird an den Proxyserver weitergeleitet, der ihn daraufhin überprüft, bevor er an das eigentliche Ziel weitergeleitet wird.

Expliziter Weiterleitungsproxy (mit Entschlüsselungsausnahme)

Dieses Diagramm zeigt den Netzwerkfluss, wenn das Multicloud-Gateway im Pfad zwischen dem Client und dem Webserver platziert wird und das Multicloud-Gateway so konfiguriert ist, dass es als Forward-Proxy mit einer Entschlüsselungsausnahme fungiert.



> Hinweis: Entschlüsselungsausnahmen beziehen sich auf Szenarien, in denen Sie es vorziehen, dass Multicloud Gateway den Datenverkehr nicht entschlüsselt und nicht untersucht. Diese Ausnahmen gelten häufig für Websites in den Bereichen Finanzen, Gesundheitswesen und öffentliche Einrichtungen. In diesen Situationen aktivieren Sie Entschlüsselungsausnahmen für bestimmte FQDNs.

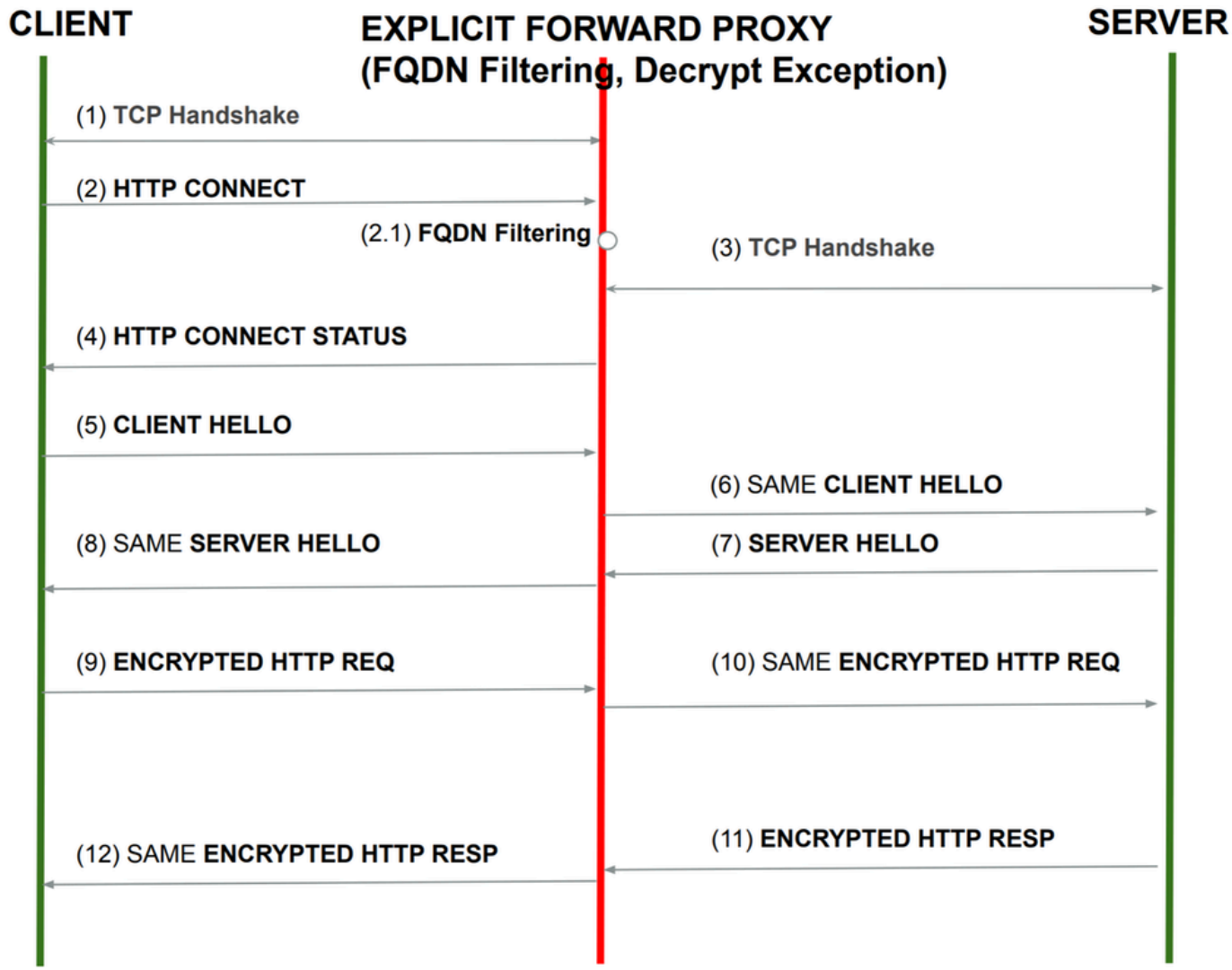


Image - Expliziter Weiterleitungsproxy-Fluss (mit Entschlüsselungsausnahme)

[1] Der TCP-3-Wege-Handshake wird zwischen dem Client und dem Multicloud-Gateway initiiert.

[2] Sobald der Handshake abgeschlossen ist, sendet der Client HTTP CONNECT.

[3] Über den CONNECT-Header identifiziert das Multicloud-Gateway den FQDN und wendet eine FQDN-Filterrichtlinie an.

[4] Wenn der Datenverkehr zulässig ist, initiiert das Gateway eine neue TCP-Handshake-Anforderung an den Server und leitet die HTTP-VERBINDUNG weiter.

[5] HTTP STATUS-Antwortnachricht wird transparent an den Client weitergeleitet.

[6] Ab diesem Zeitpunkt werden alle Nachrichten ohne Unterbrechung direkt gesendet

Expliziter Weiterleitungsproxy (mit Entschlüsselung)

Hier sehen Sie den Datenverkehrsfluss, während der Explicit Forward-Proxy für die Entschlüsselung des Datenverkehrs konfiguriert ist.

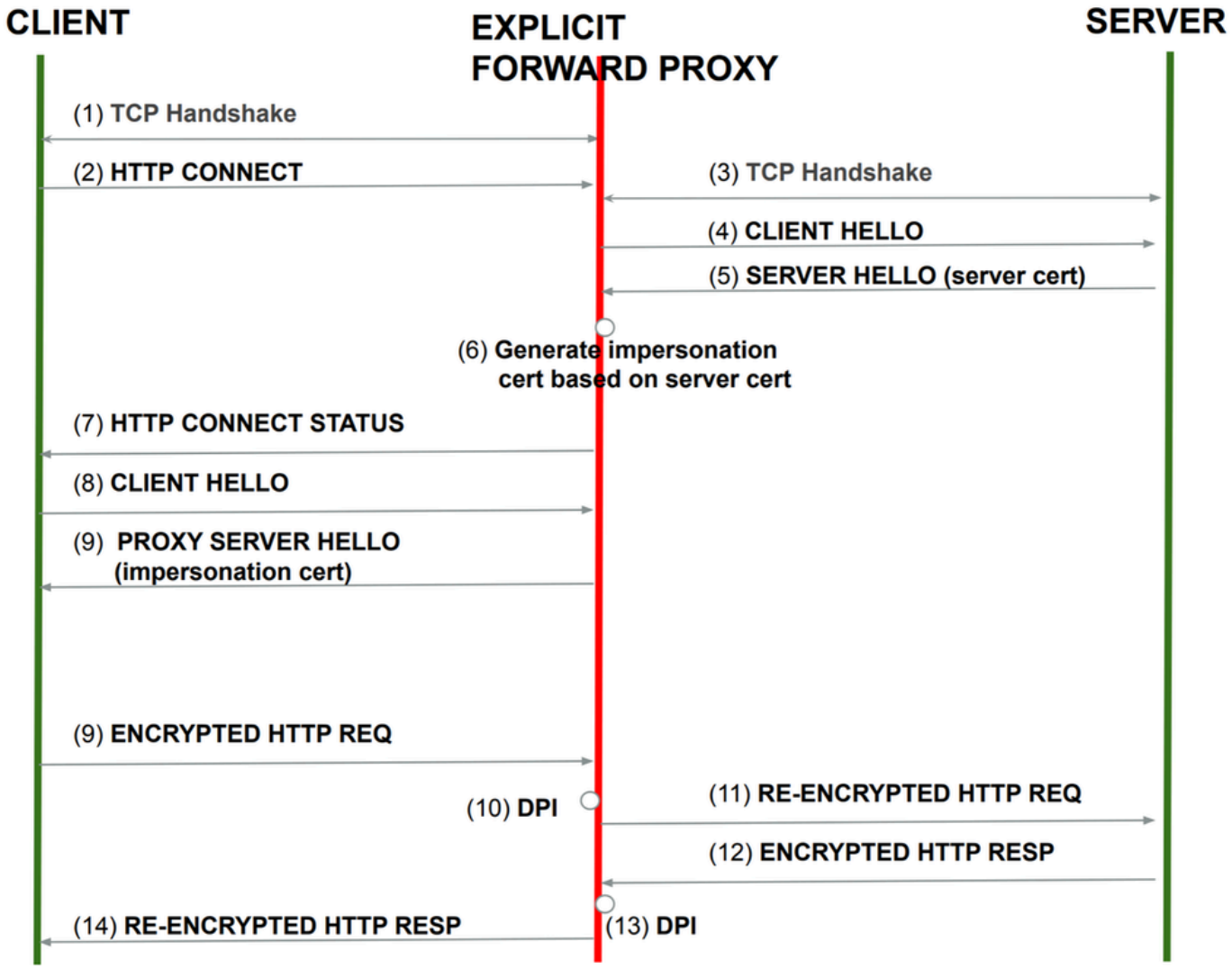


Bild - Expliziter Weiterleitungsproxy (mit Entschlüsselung)

[1] Der TCP-3-Wege-Handshake wird zwischen dem Client und dem Multicloud-Gateway initiiert.

[2] Sobald der Handshake abgeschlossen ist, sendet der Client HTTP CONNECT.

[3] Über den CONNECT-Header identifiziert das Multicloud-Gateway den FQDN und wendet die FQDN-Filterrichtlinie an.

[4] Multicloud Gateway startet den TCP-Handshake mit dem Server.

[5] Nachdem der TLS-Handshake zwischen dem Multicloud-Gateway und dem Server erfolgreich abgeschlossen wurde, gab das Multicloud-Gateway ein Zertifikat für den entschlüsselten Verkehr zwischen dem Client und dem Multicloud-Gateway aus.

[6] Ab diesem Punkt wird der gesamte Datenverkehr zwischen Client und Server wieder entschlüsselt und verschlüsselt.

Transparenter Weiterleitungsproxy

Transparenter Weiterleitungsproxy (mit Entschlüsselungsausnahme)

Das folgende Szenario beschreibt den Prozess, wenn der Datenverkehr auf einen öffentlichen Server abzielt und das Gateway über eine Konfiguration für einen Weiterleitungsproxy mit einer Entschlüsselungsausnahme verfügt.

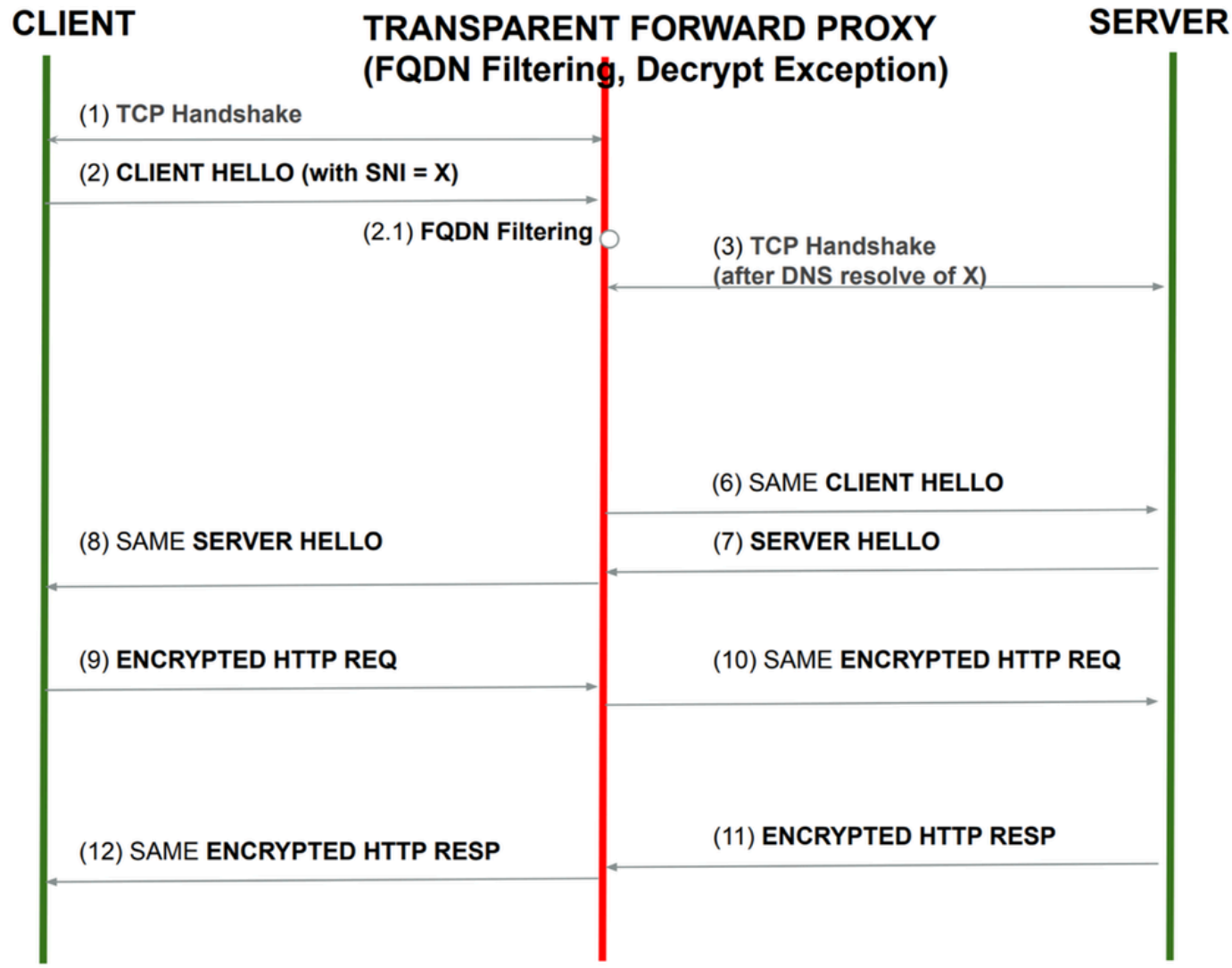


Bild - Transparenter Weiterleitungsproxy (mit Entschlüsselungsausnahme)

[1] Das Multicloud-Gateway reagiert auf TCP-Handshake.

[2] Der Client sendet einen CLIENT HELLO an den Server. Diese CLIENT HELLO enthält den Server Name Identifier (SNI). Das Gateway fängt dieses Paket ab und führt eine FQDN-Filterrichtlinie durch.

[3] Wenn der Datenverkehr zulässig ist und die Entschlüsselungsausnahme für die URL konfiguriert ist, führt das Multicloud-Gateway eine weitere DNS-Auflösung für die SNI durch.

[4] Das Multicloud-Gateway initiiert einen TCP-Handshake zum Server.

[5] Das Multicloud Gateway leitet dieselbe CLIENT HELLO an den Server weiter (wie vom Client empfangen).

[6] Die vom Server empfangene SERVER HELLO wird unverändert weitergeleitet.

[7] Ab diesem Zeitpunkt werden alle Pakete ohne Aktion gesendet

Transparenter Weiterleitungsproxy (mit Entschlüsselung)

Das folgende Szenario beschreibt den Prozess, wenn der Datenverkehr auf einen öffentlichen Server abzielt und das Gateway über eine Konfiguration verfügt, die den Weiterleitungsproxy zum Entschlüsseln des Datenverkehrs verwendet.

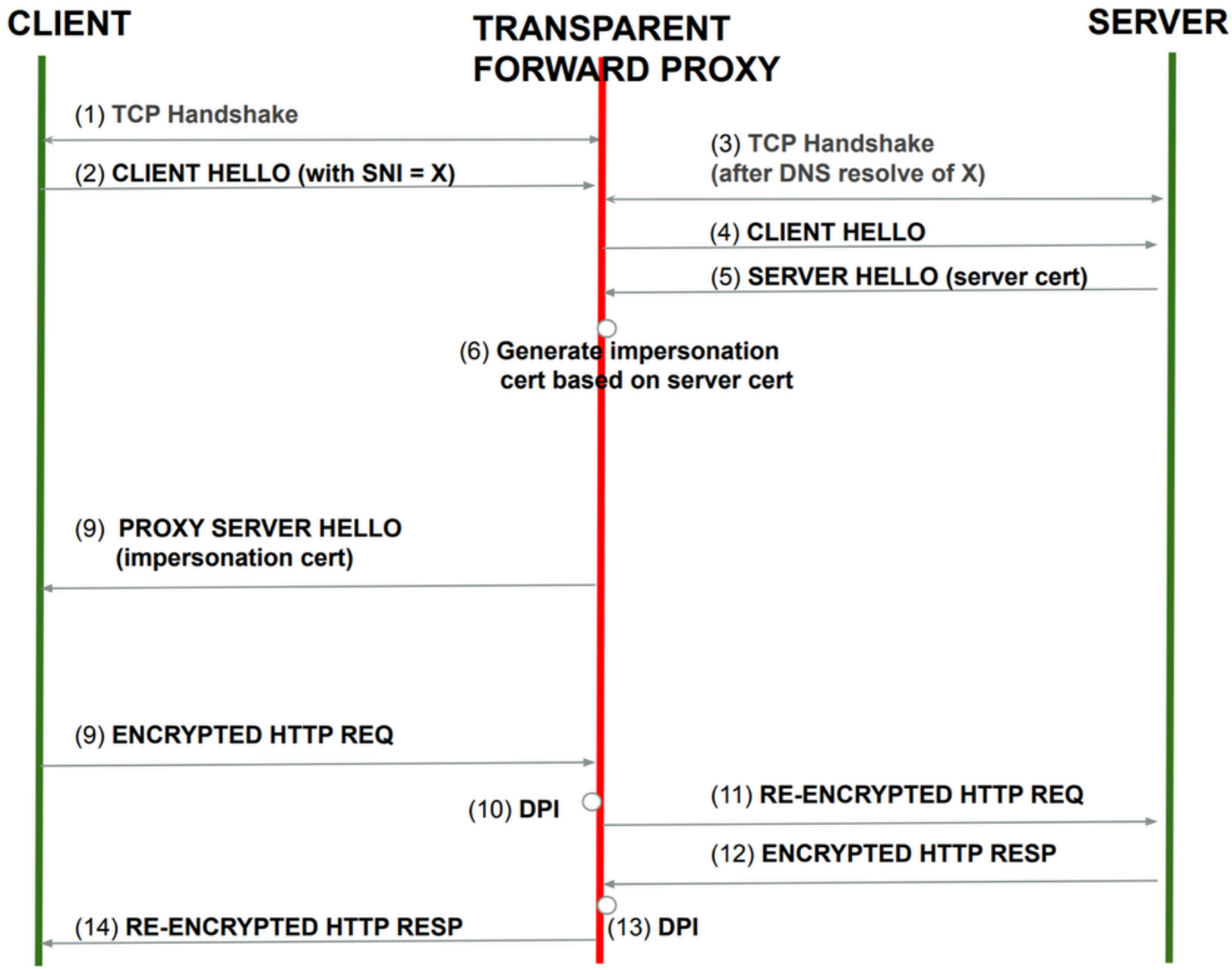


Bild - Transparenter Weiterleitungsproxy (mit Entschlüsselung)

[1] Multicloud-Gateway reagiert auf TCP-Handshake.

[2] Der Client sendet einen CLIENT HELLO an den Server. Diese CLIENT HELLO enthält den Server Name Identifier (SNI). Das Gateway fängt dieses Paket ab und führt eine FQDN-Filterrichtlinie durch.

[3] Wenn der Datenverkehr zulässig ist und die Entschlüsselung für die URL konfiguriert ist, führt das Multicloud-Gateway eine weitere DNS-Auflösung für die SNI durch.

[4] Das Multicloud-Gateway initiiert einen TCP-Handshake zum Server.

[5] Nachdem der TLS-Handshake zwischen dem Multicloud-Gateway und dem Server erfolgreich abgeschlossen wurde, gab das Multicloud-Gateway ein Zertifikat für den entschlüsselten Verkehr zwischen dem Client und dem Multicloud-Gateway aus.

[6] Ab diesem Punkt wird der gesamte Datenverkehr zwischen Client und Server wieder entschlüsselt und verschlüsselt.

Zugehörige Informationen

- Cisco Multicloud Defense - Benutzerhandbuch - FQDN-Filterprofil [Cisco Defense Orchestrator] - Cisco
- Cisco Multicloud Defense User Guide - Manage Gateways [Cisco Defense Orchestrator] - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.