瞭解多雲防禦網關代理HTTPS流量流

目錄

簡介

本文檔介紹在配置正向或反向代理操作時，思科多雲防禦網關如何處理HTTPS流量。

必要條件

需求

思科建議您瞭解以下主題：

- 雲端計算基礎知識
- 電腦網路基礎知識

採用元件

本文件所述內容不限於特定軟體和硬體版本。

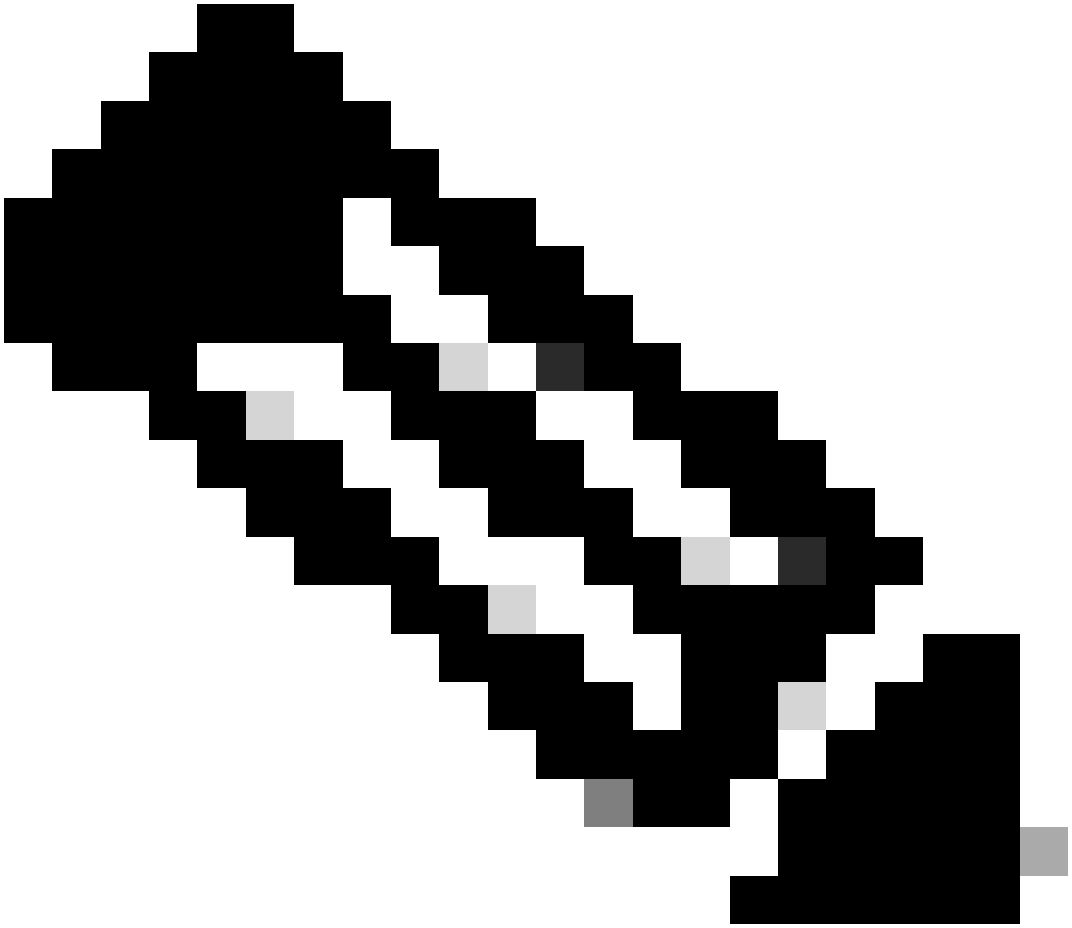
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

顯式轉發代理

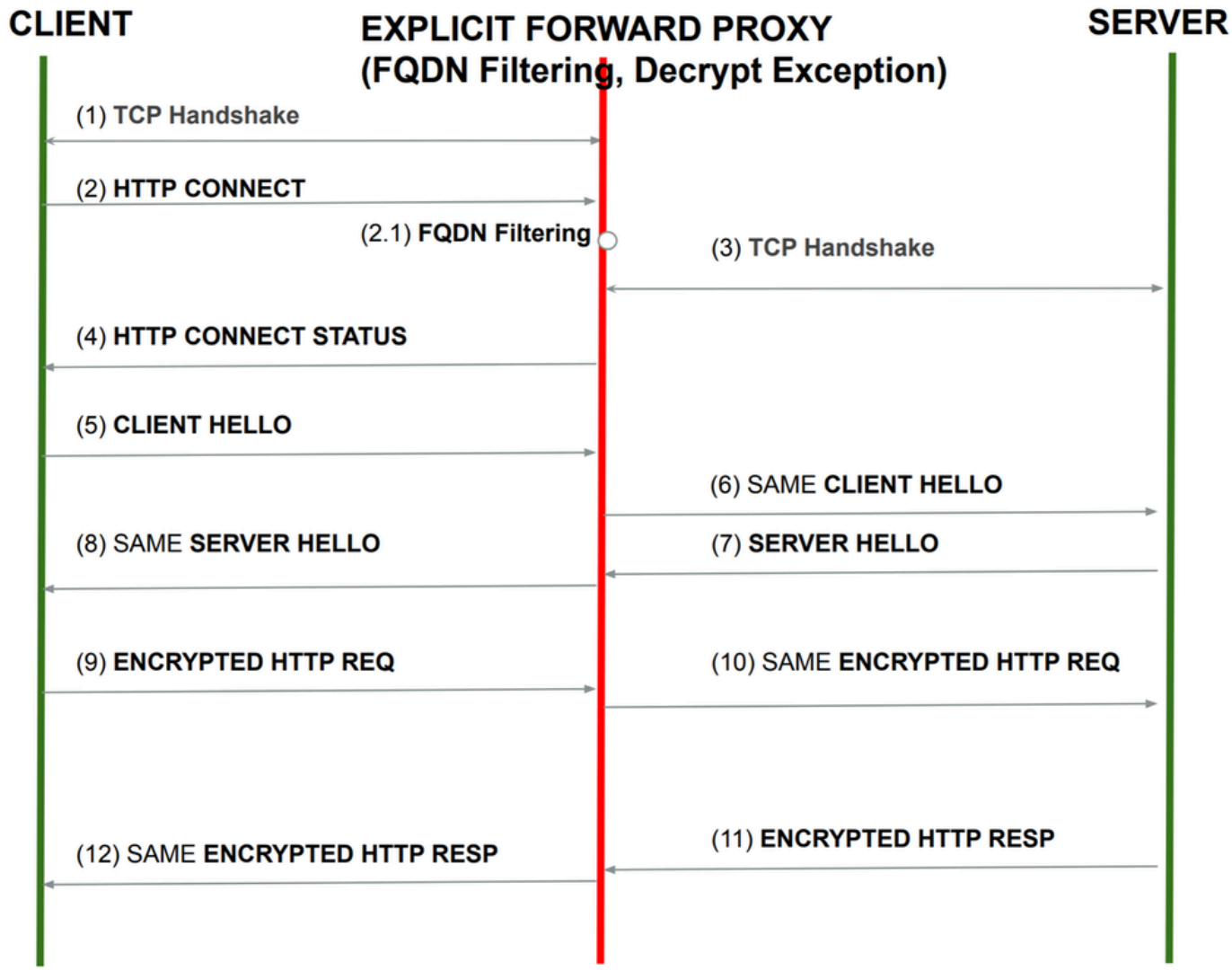
顯式轉發代理意味著您的電腦網路設定被配置為顯式使用代理。來自使用者端的流量是目的地為代理伺服器，代理伺服器會在將流量轉送到實際目的地之前檢查該流量。

顯式轉發代理（解密異常）

下圖顯示了當多雲網關位於客戶端和Web伺服器之間的路徑中，且多雲網關配置為作為具有解密異常的轉發代理時的網路流。



注意：解密例外情況是指您傾向於使用多雲網關而不解密和檢查流量的情況，這些流量通常適用於金融、醫療保健和政府網站。在這些情況下，您可以啟用特定FQDN的解密例外。



影象-顯式轉發代理（有解密例外）流

[1]在客戶端和多雲網關之間啟動TCP三次握手。

[2]握手完成後，客戶端傳送HTTP CONNECT。

[3]從CONNECT報頭，Multicloud網關辨識FQDN並應用FQDN過濾策略。

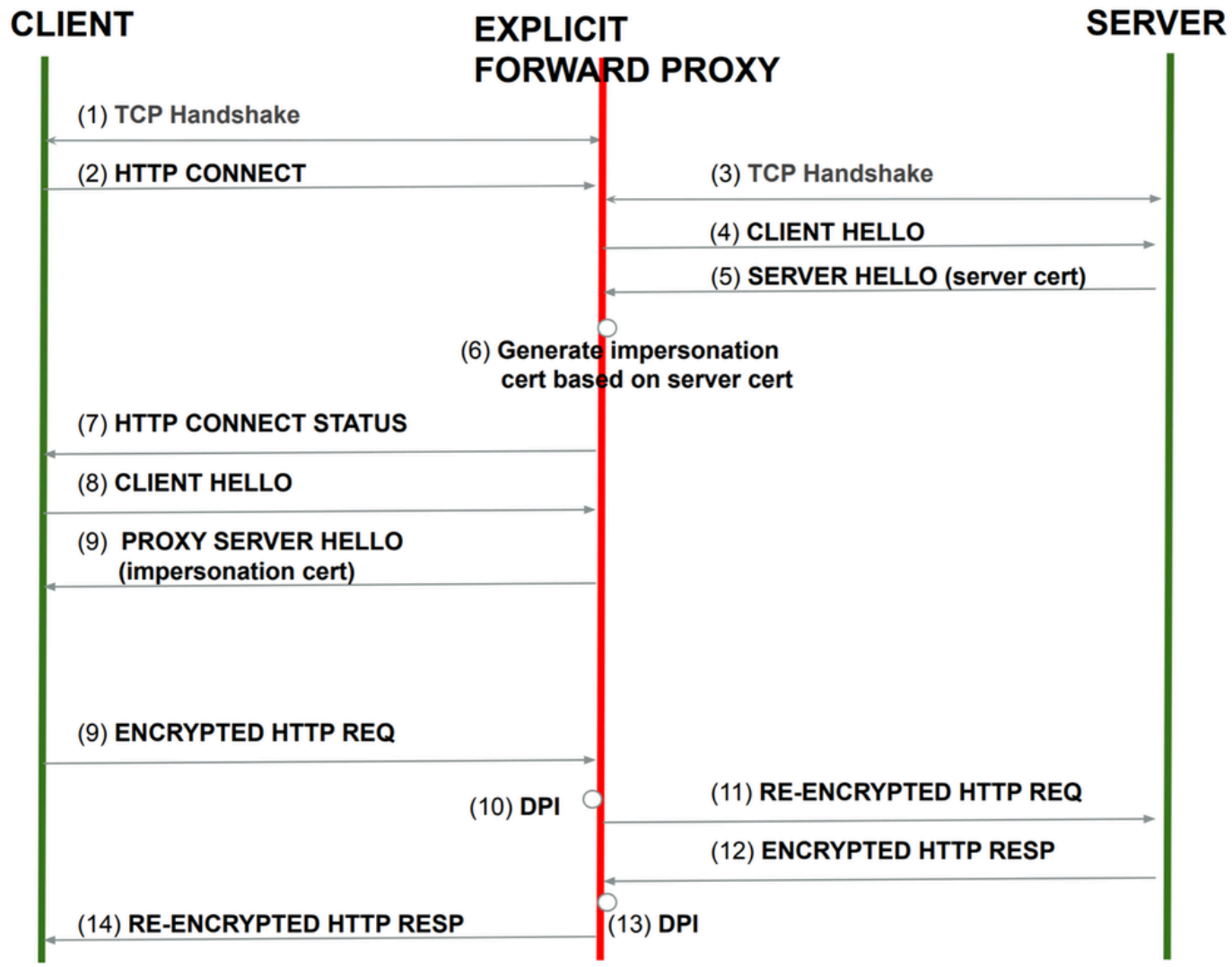
[4]如果流量被允許，網關會向伺服器發起新的TCP握手請求並轉發HTTP CONNECT。

[5] HTTP STATUS響應消息以透明方式轉發到客戶端。

[6]從此時起，所有消息直接傳送，不進行任何攔截

明確轉送代理（含解密）

以下是流量傳輸，而明確轉送代理則設定為解密流量。



影像-明確轉送代理（含解密）

[1]在客戶端和多雲網關之間啟動TCP三次握手。

[2]握手完成後，客戶端傳送HTTP CONNECT。

[3]從CONNECT報頭，Multicloud網關辨識FQDN並應用FQDN過濾策略。

[4] Multicloud Gateway啟動與伺服器的TCP握手。

[5]在Multicloud網關與伺服器之間的TLS握手成功完成後，Multicloud網關為客戶端和多雲網關之間的解密流量頒發證書。

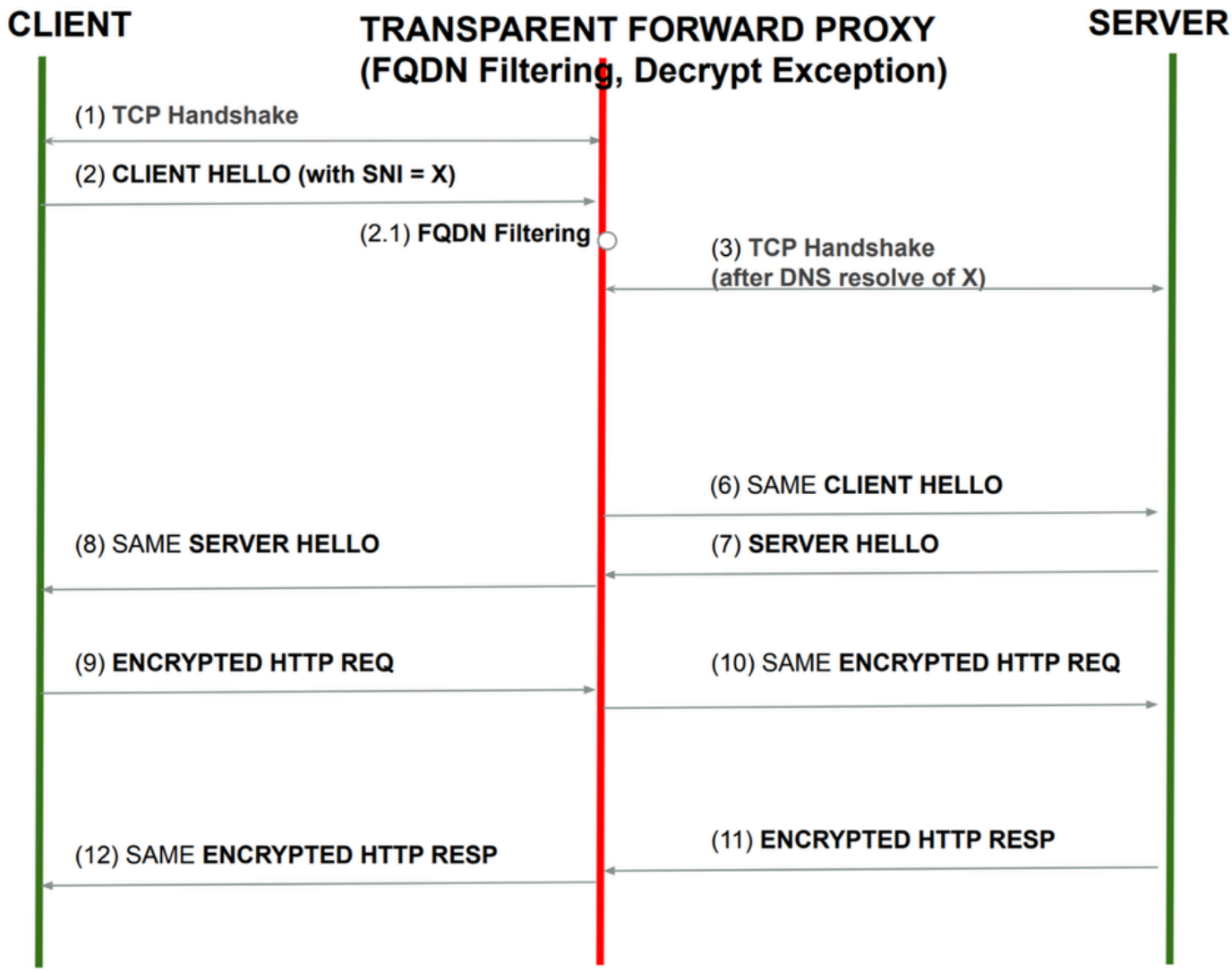
[6]從此以後，客戶端和伺服器之間的所有流量都會被解密並再次加密。

透明轉發代理

透明轉發代理（解密例外）

後續場景概述了當流量以公共伺服器為目標，並且網關具有帶有解密例外的轉發代理的配置時的過

程。



影像-透明轉送Proxy（解密例外）

[1]多雲網關響應TCP握手。

[2]客戶端向伺服器傳送客戶端HELLO。此客戶端HELLO包含伺服器名稱識別符號(SNI)。網關攔截此資料包並執行FQDN過濾策略。

[3]如果允許流量並且為URL配置了解密異常，則多雲網關將對SNI執行另一個DNS解析。

[4] Multicloud網關向伺服器發起TCP握手。

[5] Multicloud網關將相同的客戶端HELLO轉發到伺服器（與從客戶端收到的相同）。

[6]從伺服器接收的SERVER HELLO將原樣轉發，而不做任何修改。

[7]從此時開始，所有資料包按原樣傳送，而不執行任何操作

透明轉發代理（帶解密）

後續場景概述了當流量以公共伺服器為目標，且網關具有轉發代理解密流量的配置時的過程。

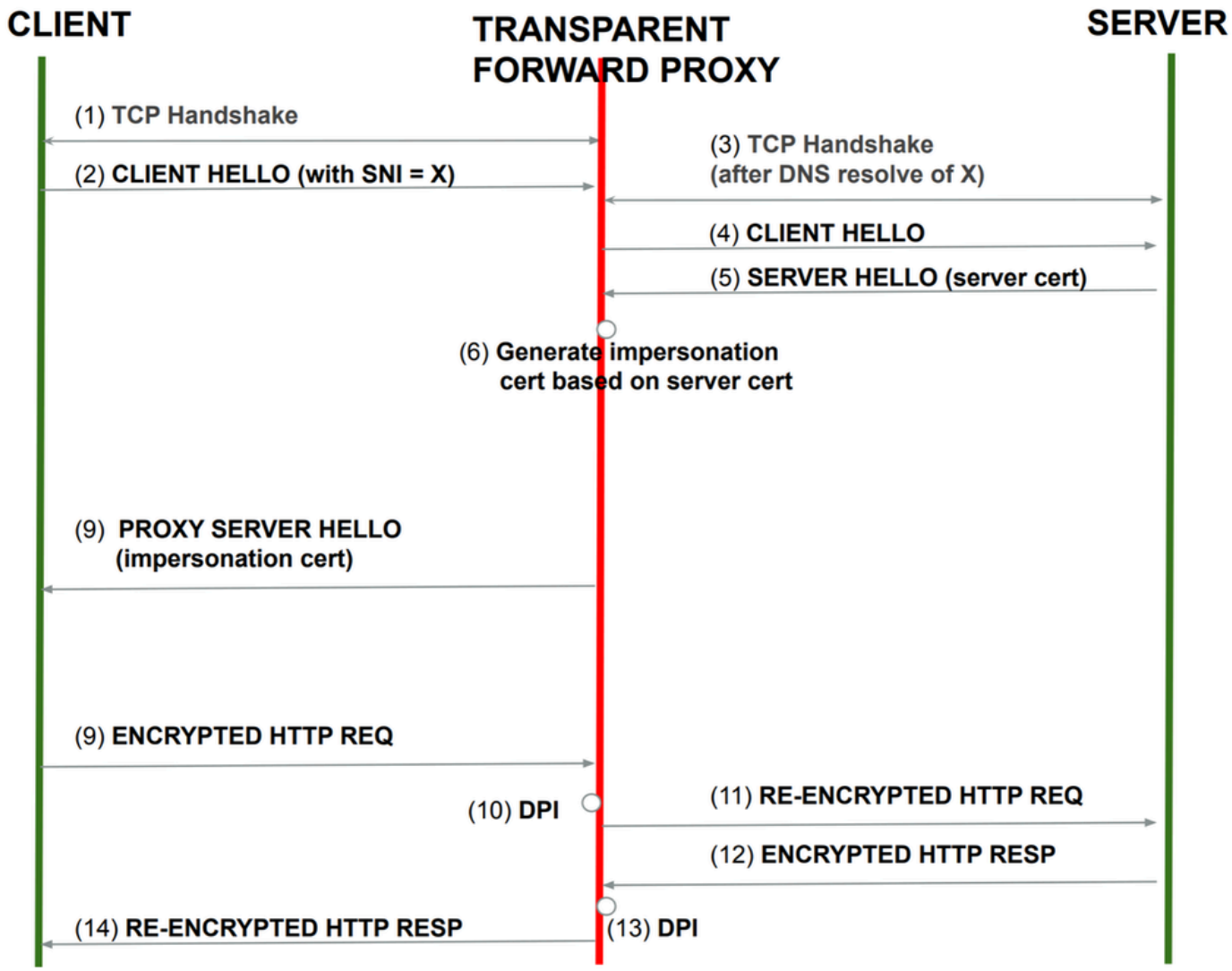


圖-透明轉發代理（含解密）

[1]多雲網關響應TCP握手。

[2]客戶端向伺服器傳送客戶端HELLO。此客戶端HELLO包含伺服器名稱識別符號(SNI)。網關攔截此資料包並執行FQDN過濾策略。

[3]如果允許流量並且為URL配置了解密，則多雲網關會對SNI執行另一個DNS解析。

[4] Multicloud網關開始向伺服器發起TCP握手。

[5]在Multicloud網關與伺服器之間的TLS握手成功完成後，Multicloud網關為客戶端與Multicloud網關之間的解密流量頒發證書。

[6]從此以後，客戶端和伺服器之間的所有流量都會被解密並再次加密。

相關資訊

- 思科多雲防禦使用手冊- FQDN過濾器配置檔案[思科Defense Orchestrator] -思科
- 思科多雲防禦使用手冊-管理網關[思科Defense Orchestrator] -思科

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。