了解多云防御网关代理HTTPS流量

目录

简介

先决条件

- 要求
- 使用的组件

显式转发代理

- 显式转发代理（解密例外）
- 显式转发代理（带解密）

透明转发代理

- 透明转发代理（解密例外）
- 透明转发代理（带解密）

相关信息

简介

本文档介绍在配置转发或反向代理操作时，思科多云防御网关如何处理HTTPS流量。

先决条件

要求

思科建议您了解以下主题：

- 云计算基础知识
- 计算机网络基础知识

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

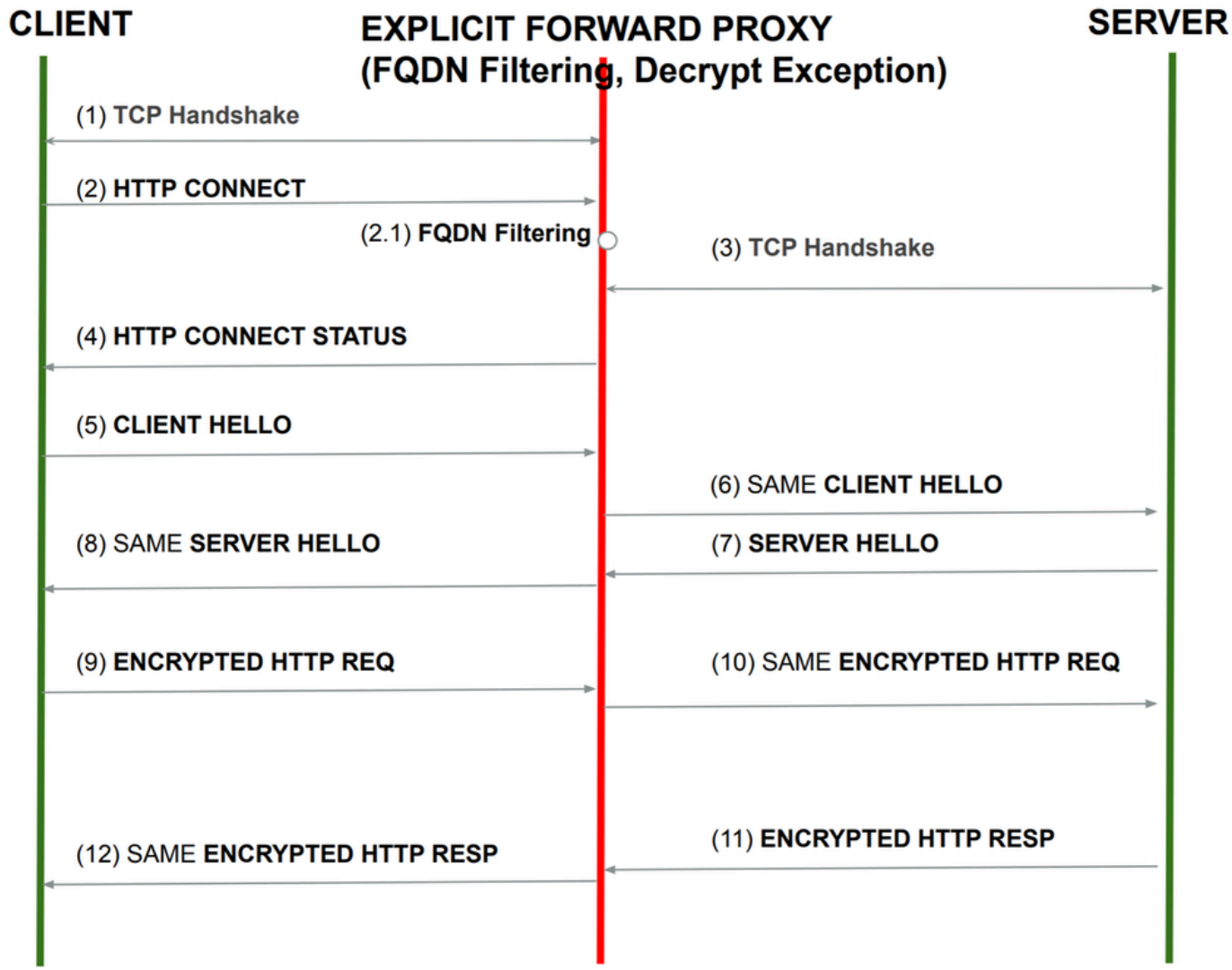
显式转发代理

显式转发代理意味着将您的计算机网络设置配置为显式使用代理。来自客户端的流量发往代理服务器，代理服务器在将流量转发到实际目标之前会对其进行检查。

显式转发代理（解密例外）

下图显示了当多云网关放置在客户端和Web服务器之间的路径中，并且多云网关配置为作为转发代理时解密异常时的网络流。

注意：解密例外是指您倾向于多云网关不解密和检查流量的场景，通常适用于金融、医疗保健和政府网站。在这些情况下，您可以激活特定FQDN的解密例外。



图像 — 显式转发代理（解密例外）流

[1]在客户端和多云网关之间发起TCP三次握手。

[2]握手完成后，客户端发送HTTP CONNECT。

[3]从CONNECT报头中，多云网关识别FQDN并应用FQDN过滤策略。

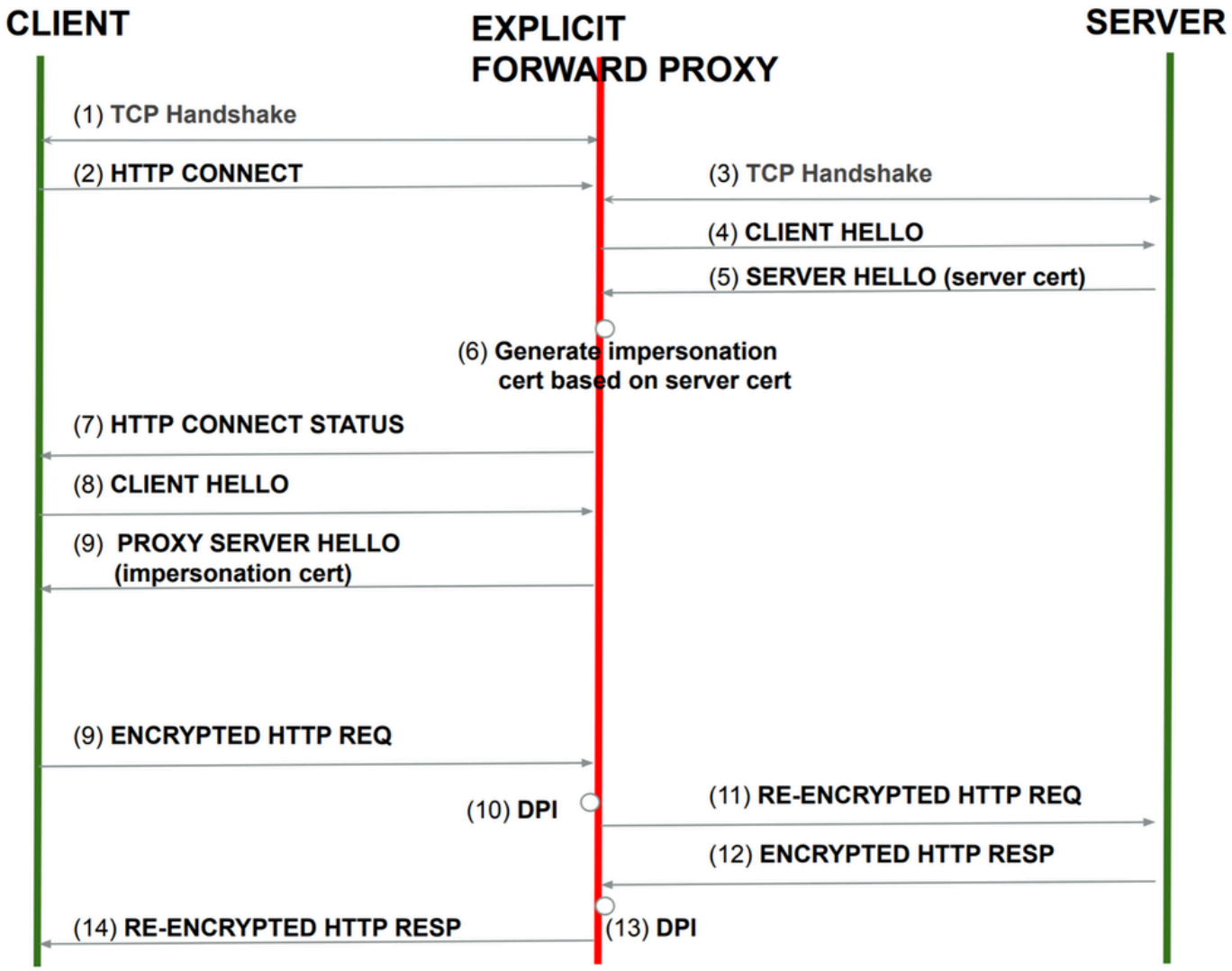
[4]如果允许流量，网关会向服务器发起新的TCP握手请求并转发HTTP CONNECT。

[5] HTTP状态响应消息以透明方式转发到客户端。

[6]从此时起，所有消息直接发送，无需任何拦截

显式转发代理（带解密）

这是流量，而显式转发代理配置为解密流量。



图像 — 显式转发代理（带解密）

[1]在客户端和多云网关之间发起TCP三次握手。

[2]握手完成后，客户端发送HTTP CONNECT。

[3]从CONNECT报头中，多云网关识别FQDN并应用FQDN过滤策略。

[4]多云网关开始与服务器进行TCP握手。

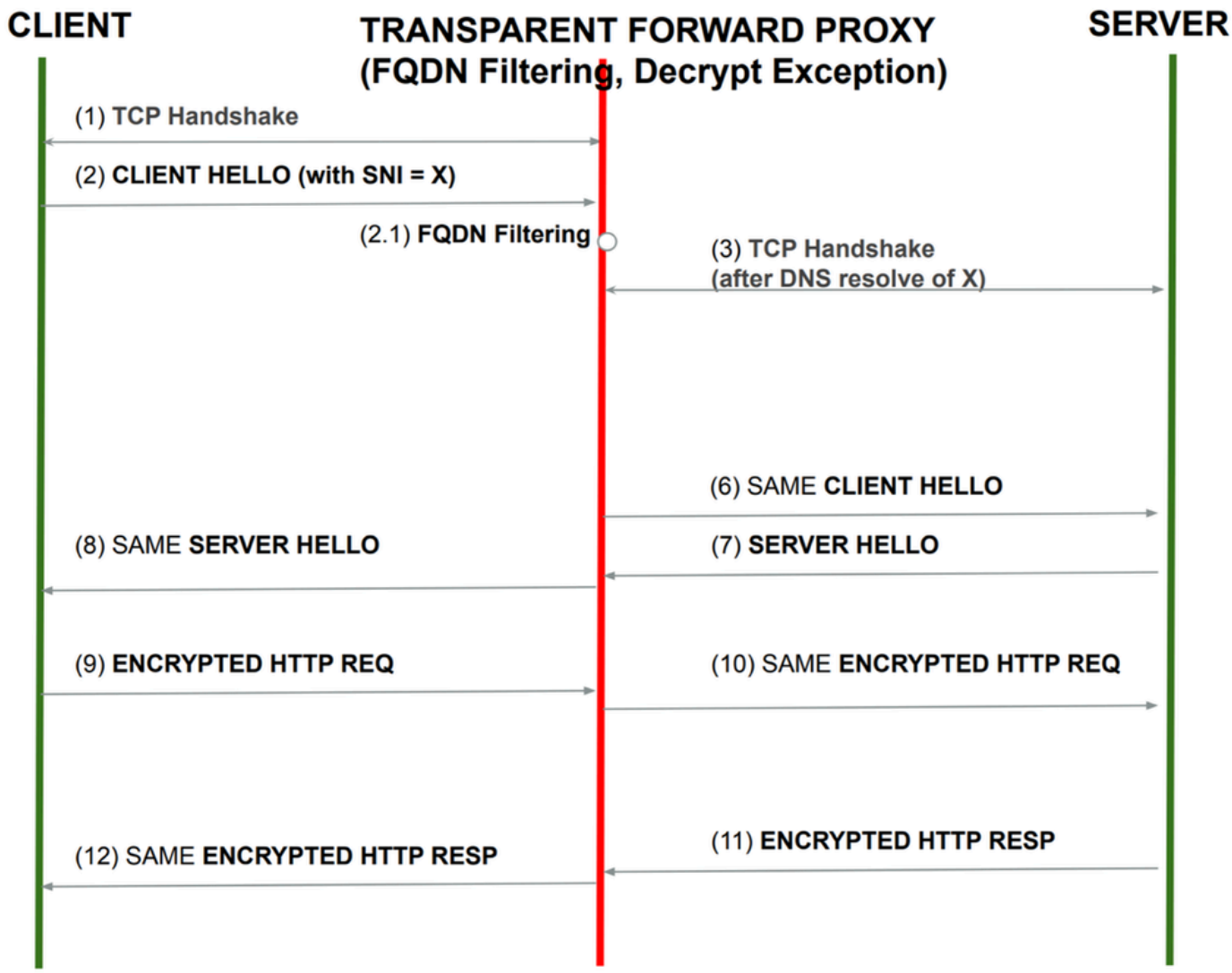
[5]在多云网关与服务器之间的TLS握手成功完成后，多云网关为客户端和多云网关之间的已解密流量颁发证书。

[6]从此时开始转发，客户端和服务器之间的所有流量将再次解密和加密。

透明转发代理

透明转发代理（解密例外）

后续场景概述了流量以公共服务器为目标而网关具有转发代理配置（解密除外）的过程。



图像 — 透明转发代理（解密例外）

[1]多云网关响应TCP握手。

[2]客户端向服务器发送客户端HELLO。此客户端HELLO包含服务器名称标识符(SNI)。 网关会拦截此数据包并执行FQDN过滤策略。

[3]如果允许流量，并且为URL配置了解密例外，则多云网关将对SNI执行另一个DNS解析。

[4]多云网关向服务器发起TCP握手。

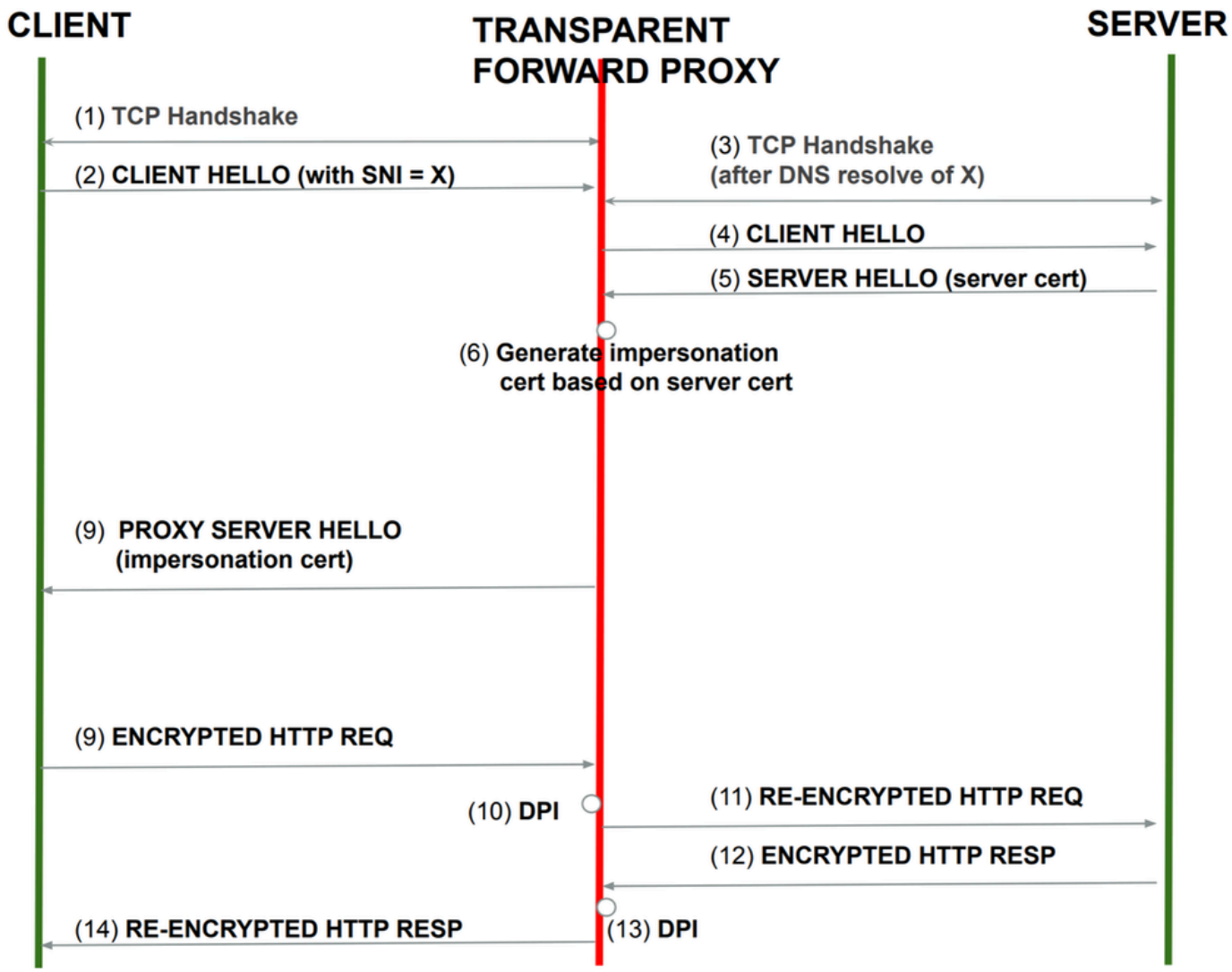
[5]多云网关将相同的客户端HELLO转发到服务器（与从客户端收到的相同）。

[6]从服务器收到的SERVER HELLO将原样转发，而不进行任何修改。

[7]从此时起，所有数据包按原样发送，不采取任何操作

透明转发代理（带解密）

后续场景概述了流量以公共服务器为目标而网关具有转发代理解密流量的配置时的过程。



图像 — 透明转发代理（带解密）

[1]多云网关响应TCP握手。

[2]客户端向服务器发送客户端HELLO。此客户端HELLO包含服务器名称标识符(SNI)。 网关会拦截此数据包并执行FQDN过滤策略。

[3]如果允许流量并且为URL配置了解密，则多云网关会对SNI执行另一个DNS解析。

[4]多云网关开始向服务器发起TCP握手。

[5]在多云网关与服务器之间的TLS握手成功完成后，多云网关为客户端和多云网关之间的已解密流量颁发证书。

[6]从此时开始转发，客户端和服务器之间的所有流量将再次解密和加密。

相关信息

- 思科多云防御用户指南 — FQDN过滤器配置文件[思科防御协调器] — 思科
- Cisco Multicloud Defense User Guide - Manage Gateways [Cisco Defense Orchestrator] - Cisco

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。