Understand Multicloud Defense Gateway Proxy HTTPS Traffic Flow

Contents

Introduction

This document describes how the Cisco Multicloud Defence Gateway handles the HTTPS traffic when the forward or reverse proxy action is configured.

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Basic knowledge of cloud computing
- Basic knowledge of computer networks

Components Used

This document is not restricted to specific software and hardware versions.

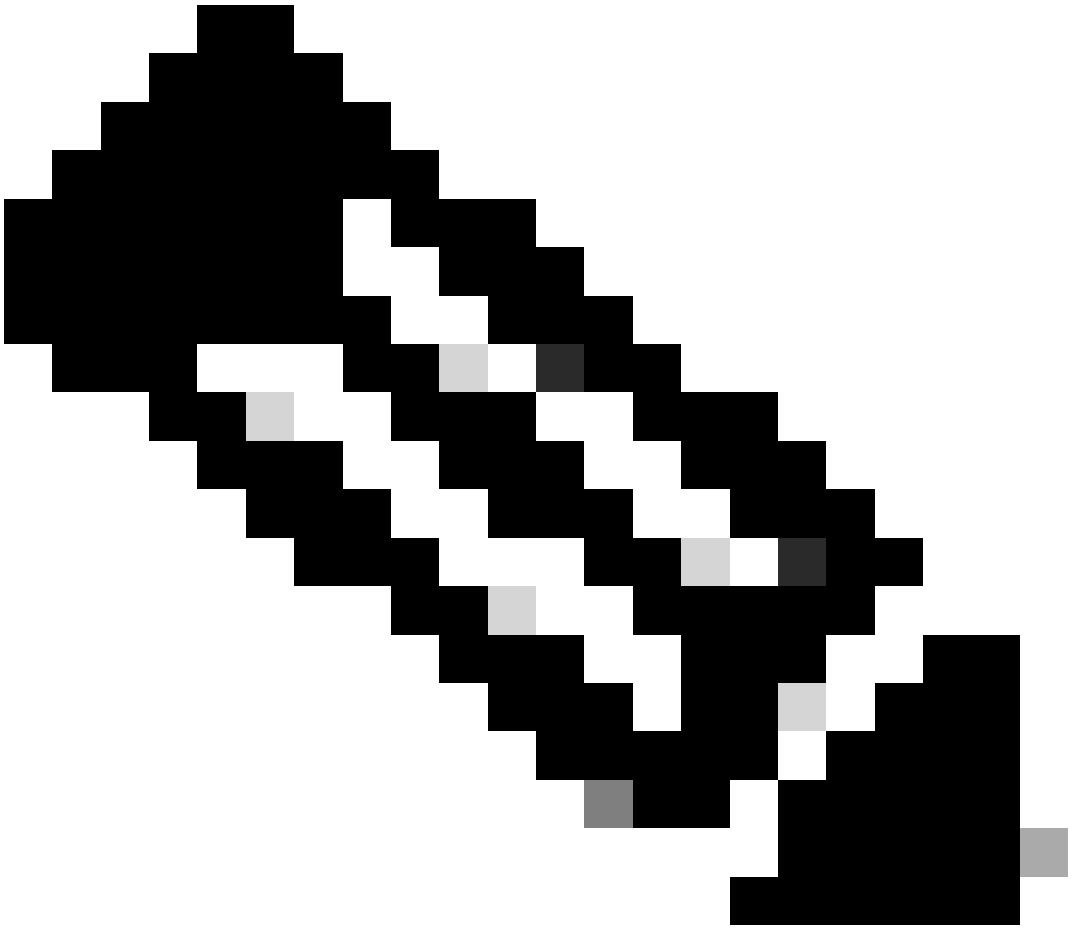
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Explicit Forward Proxy

Explicit forward proxy means that your computer network settings are configured to explicitly use the proxy. The traffic from the client is destined to the proxy server and the proxy server examines it before forwarding the traffic to the actual destination.

Explicit Forward Proxy (with decryption exception)

This diagram shows the network flow when the Multicloud gateway is placed in the path between the client and the web server and the Multicloud gateway is configured to act as a forward proxy with decryption exception.



Note: Decryption exceptions refer to scenarios in which you prefer Multicloud Gateway not to decrypt and inspect traffic, often applicable to finance, healthcare, and government websites. In these situations, you activate decryption exceptions for specific FQDNs.

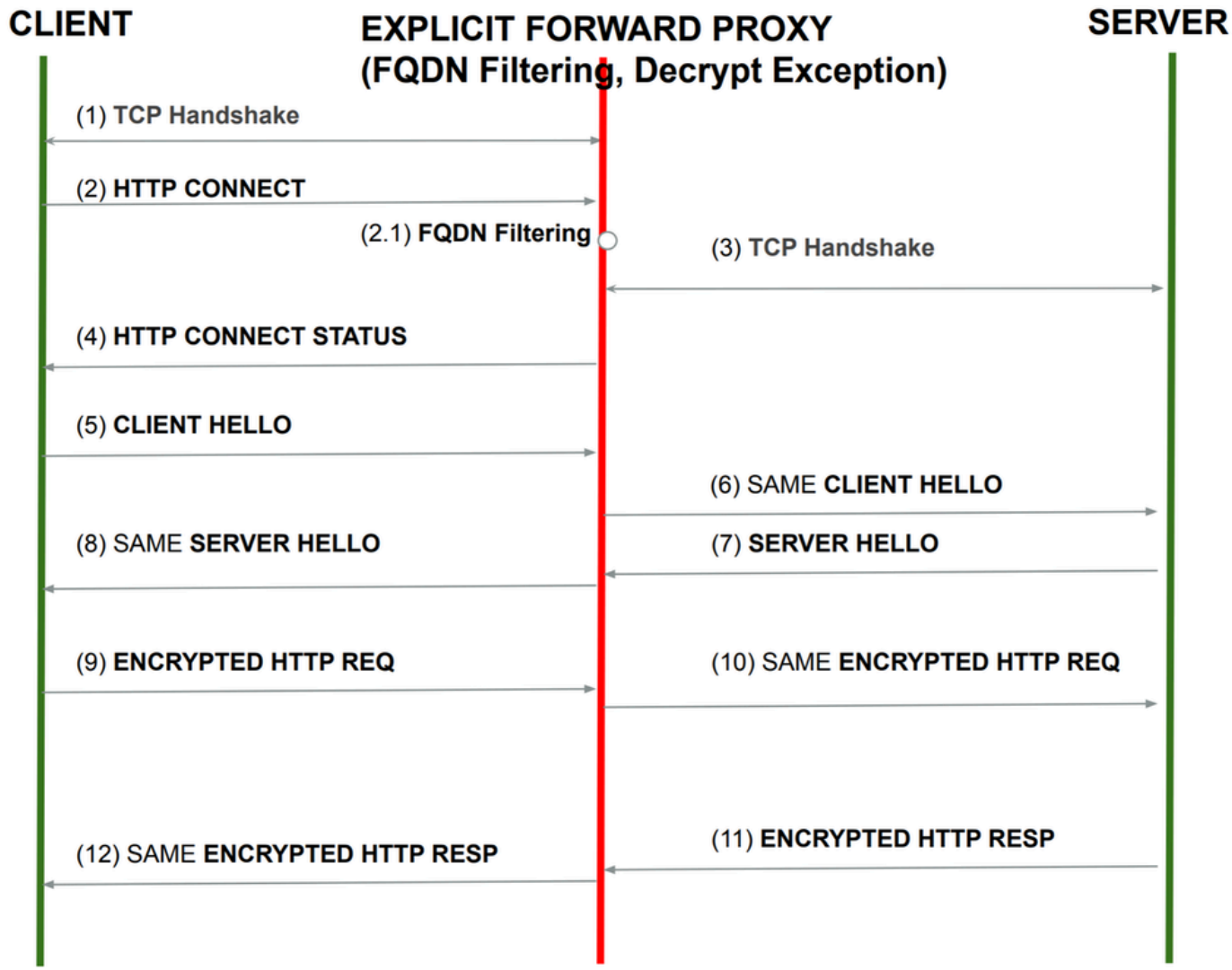


Image - Explicit Forward Proxy ((with decryption exception) flow

[1] The TCP 3-way handshake is Initiated between the client and the Multicloud gateway.

[2] Once the handshake is complete, the client sends HTTP CONNECT.

[3] From the CONNECT header, Multicloud Gateway identifies the FQDN and applies FQDN filtering policy.

[4] If the traffic is allowed, the gateway initiates a new TCP handshake request to the server and forwards the HTTP CONNECT.

[5] HTTP STATUS response message is forwarded transparently to the client.

[6] From this point onwards all the messages are sent directly without any interception

Explicit Forward Proxy (with decryption)

Here is the traffic flow, while the Explicit forward proxy is configured to decrypt the traffic.

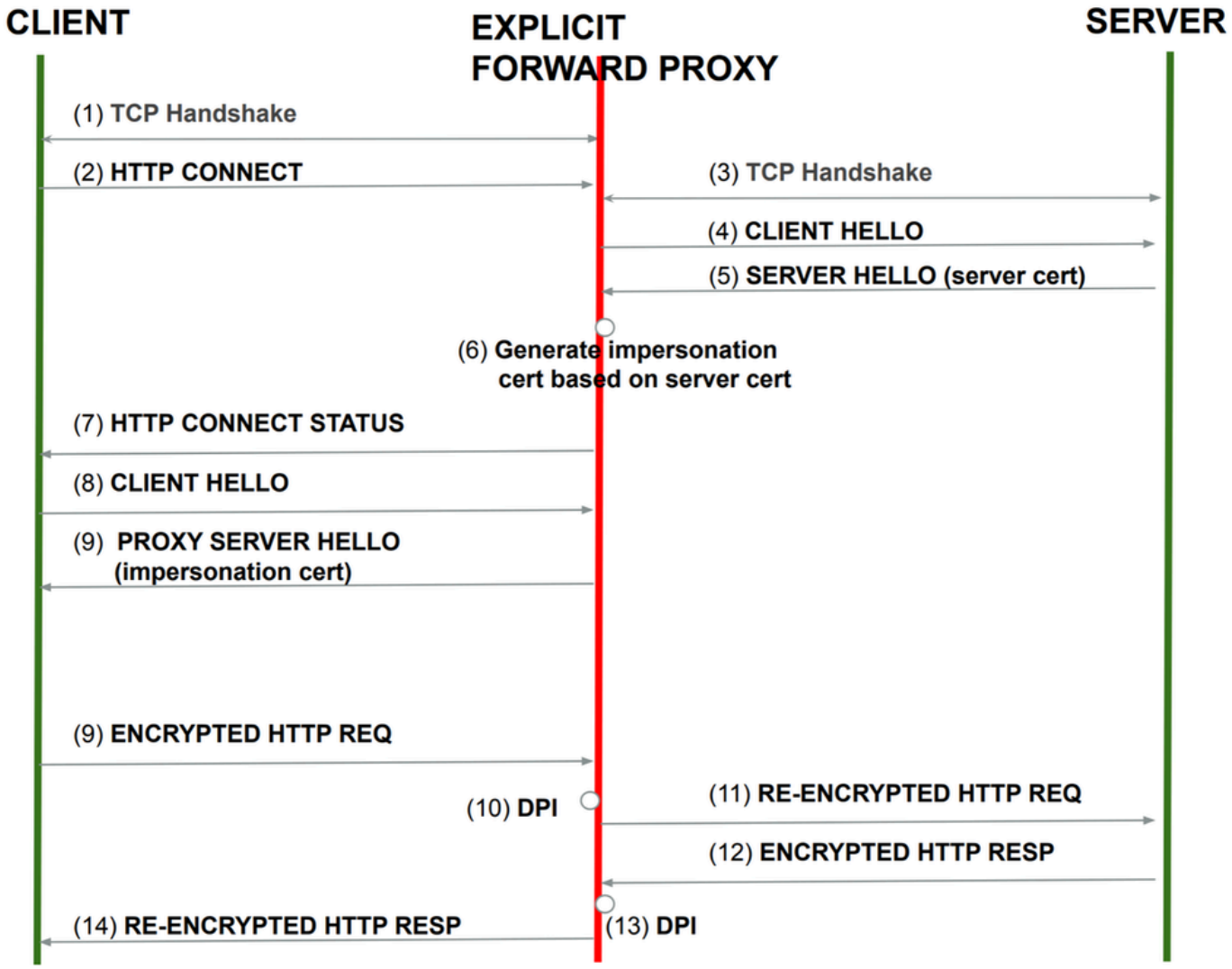


Image - Explicit Forward Proxy (with decryption)

[1] The TCP 3-way handshake is Initiated between the client and the Multicloud gateway.

[2] Once the handshake is complete, the client sends HTTP CONNECT.

[3] From the CONNECT header, Multicloud Gateway identifies the FQDN and applies the FQDN filtering policy.

[4] Multicloud Gateway starts the TCP handshake with the server.

[5] After the TLS handshake finished successfully between Multicloud Gateway and the server, Multicloud Gateway issued a certificate for the decrypted traffic between Client and Multicloud Gateway.

[6] From this point forward, all the traffic between the client and the server is decrypted and encrypted again.

Transparent Forward Proxy

Transparent Forward Proxy (with decryption exception)

The subsequent scenario outlines the process when traffic targets a public server and the gateway has a

configuration for forward proxy with a decryption exception.

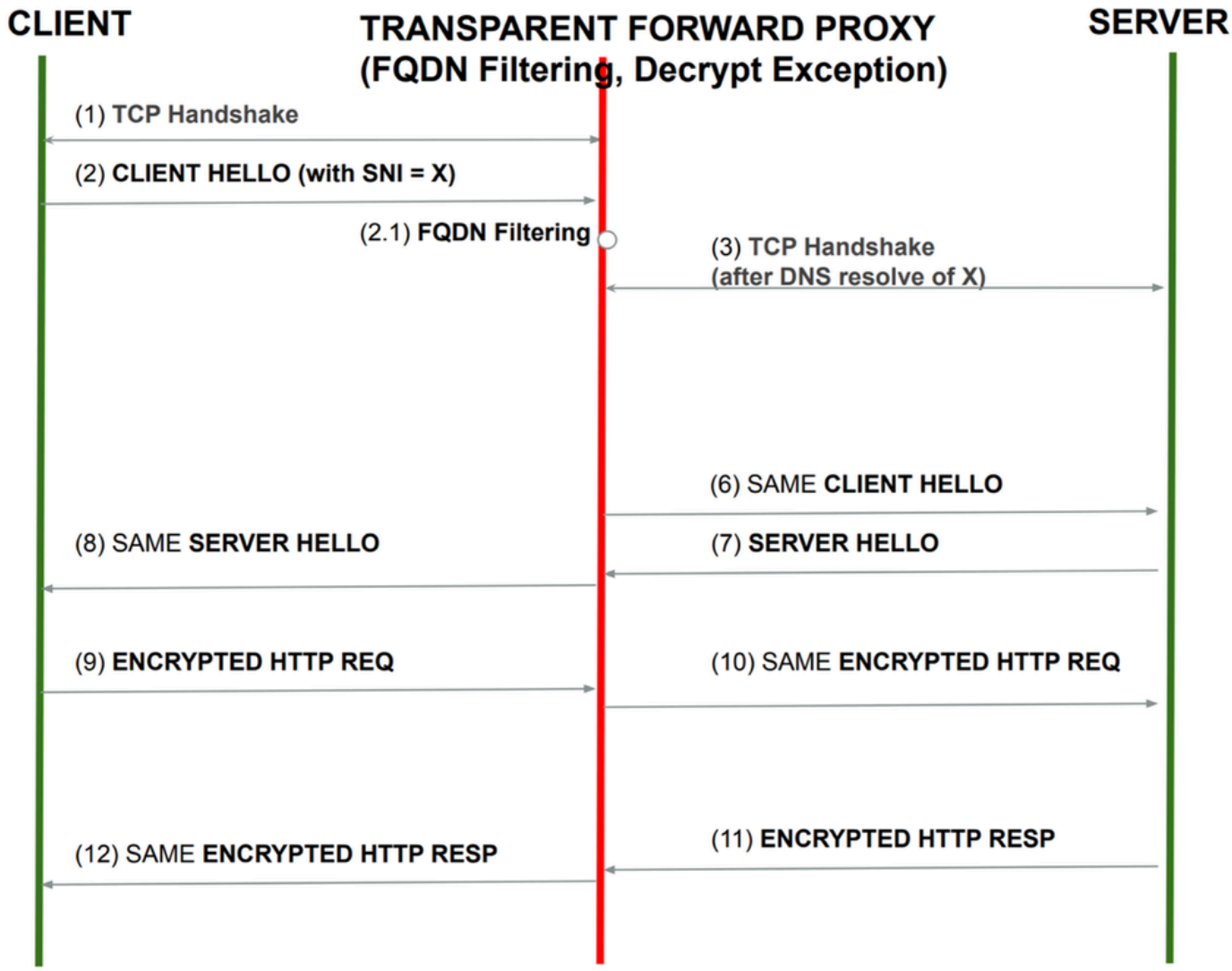


Image - Transparent Forward Proxy (with decryption exception)

[1] Multicloud gateway responds to TCP handshake.

[2] The client sends a CLIENT HELLO to the server. This CLIENT HELLO contains the Server Name Identifier (SNI). Gateway intercepts this packet and performs FQDN filtering policy.

[3] If the traffic is allowed and the Decryption Exception is configured for the URL, the Multicloud gateway performs another DNS resolution for the SNI.

[4] Multicloud Gateway initiates a TCP handshake to the server.

[5] Multicloud Gateway forwards the same CLIENT HELLO to the server (as it received from the client).

[6] The SERVER HELLO received from the server is forwarded as it is without any modification.

[7] From this point onwards all the packets are sent out as it is without any action

Transparent Forward Proxy (with decryption)

The subsequent scenario outlines the process when traffic targets a public server and the gateway has a configuration for the forward proxy to decrypt the traffic.

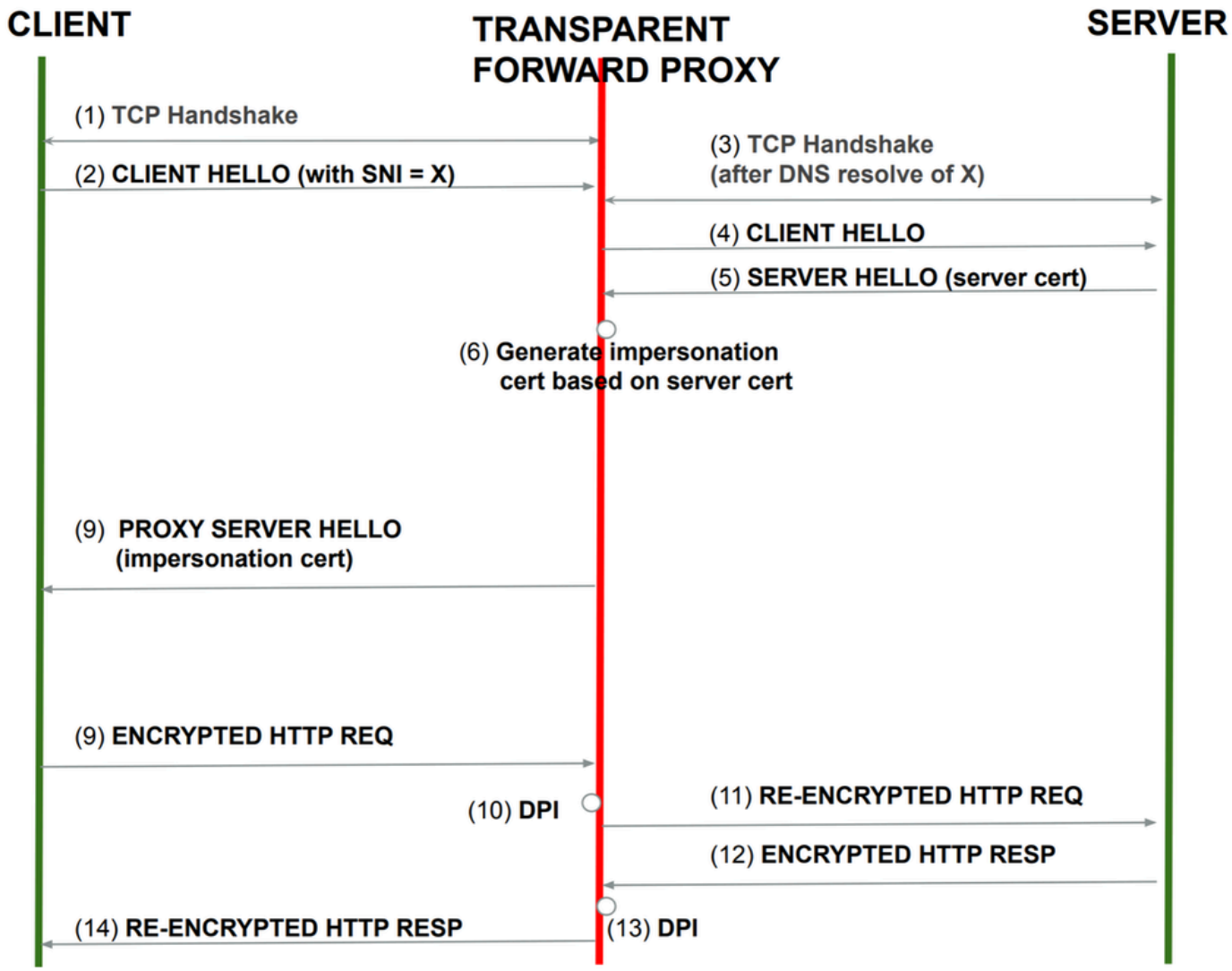


Image - Transparent Forward Proxy (with decryption)

[1] Multicloud gateway responds to TCP handshake.

[2] The client sends a CLIENT HELLO to the server. This CLIENT HELLO contains the Server Name Identifier (SNI). Gateway intercepts this packet and performs FQDN filtering policy.

[3] If the traffic is allowed and the Decryption is configured for the URL, the Multicloud gateway performs another DNS resolution for the SNI.

[4] Multicloud Gateway starts to initiate a TCP handshake to the server.

[5] After the TLS handshake finished successfully between Multicloud Gateway and the server, Multicloud Gateway issued a certificate for the decrypted traffic between the Client and Multicloud Gateway.

[6] From this point forward, all the traffic between the client and the server is decrypted and encrypted again.

Related Information

- Cisco Multicloud Defense User Guide - FQDN Filter Profile [Cisco Defense Orchestrator] - Cisco
- Cisco Multicloud Defense User Guide - Manage Gateways [Cisco Defense Orchestrator] - Cisco