Understand Multicloud Gateway Proxy Non-HTTP(S) Traffic Flow

Contents

Introduction

This document describes how the Cisco Multicloud Defence Gateway handles the TCP traffic (other than the web), when a forward proxy 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.

Proxy

A proxy serves as a go-between for two network endpoints. It functions as a gateway that transitions from one network to another for specific applications. Proxies control and simplify request complexity through their request process and forward capabilities. They provide different levels of functionality, security, and privacy, and prove beneficial in web browsing and data protection.

.

Multicloud Gateway Forward Proxy

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

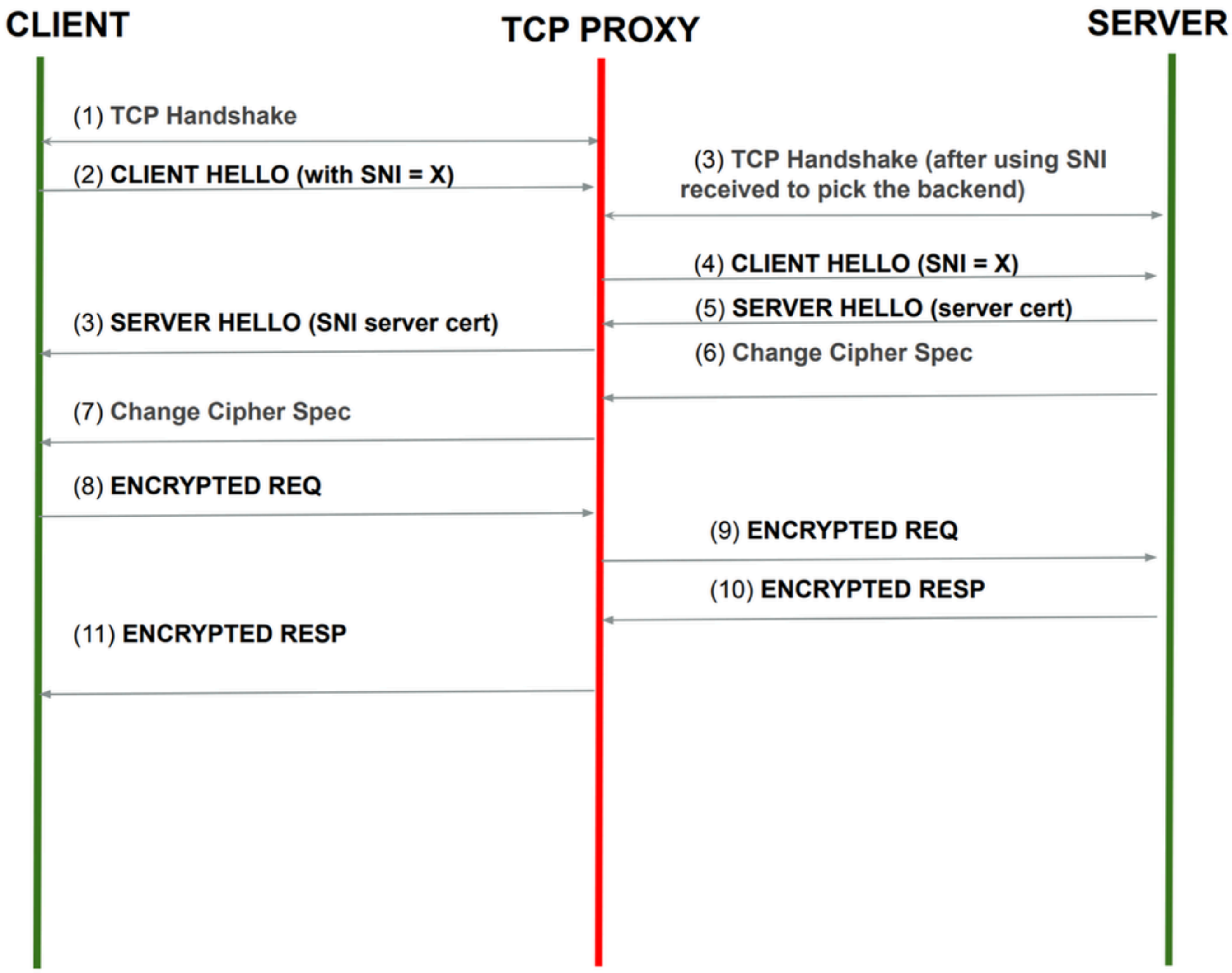
CLIENT
TCP PROXY
SERVER
(1) TCP Handshake
(2) CLIENT HELLO (with SNI = X)
(3) TCP Handshake (after using SNI received to pick the backend)
(4) CLIENT HELLO (SNI = X)
(3) SERVER HELLO (SNI server cert)
(5) SERVER HELLO (server cert)
(6) Change Cipher Spec
(7) Change Cipher Spec
(8) ENCRYPTED REQ
(9) ENCRYPTED REQ
(10) ENCRYPTED RESP
(11) ENCRYPTED RESP

Image - MCD Forward Proxy

Note: This process is applicable for SSH traffic when your client is set up to use the multicloud gateway as a proxy to connect to the SSH server.

1. The TCP 3-way handshake is Initiated between the client and the multicloud gateway.
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 the FQDN filtering policy.

Caution: Certain applications configured to utilize automatic negotiation protocols, such as those determining SSH version, must not transmit the Client Hello.

3. If the traffic is allowed, the gateway initiates a new TCP handshake request to the server and forwards the Client Hello. (as received from the client)

Note: If the server has not received any packets from the multicloud gateway, it could be because the Client did not send the Client Hello.

4. The multicloud gateway forwarded the Server Hello to the Client.

5. After the Certificate Exchange, all the packets are sent out as it is without any action

Related Information

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