Multicloud-Gateway-Proxy, kein HTTP(S)-Datenverkehrsfluss

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Proxy

Multicloud-Gateway-Weiterleitungsproxy

Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie das Cisco Multicloud Defense Gateway den TCP-Datenverkehr (außer dem Web) behandelt, wenn ein Forward-Proxy 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.

Proxy

Ein Proxy dient als Vermittlungsstelle für zwei Netzwerkendpunkte. Es fungiert als Gateway, das für bestimmte Anwendungen von einem Netzwerk zu einem anderen wechselt. Proxys steuern und vereinfachen die Komplexität von Anfragen durch ihren Anfrageprozess und ihre Weiterleitungsfunktionen. Sie bieten ein unterschiedliches Maß an Funktionalität, Sicherheit und

Datenschutz und erweisen sich beim Surfen im Internet und beim Datenschutz als vorteilhaft.

.

Multicloud-Gateway-Weiterleitungsproxy

Dieses Diagramm zeigt den Netzwerkfluss, wenn das Multicloud-Gateway im Pfad zwischen dem Client und dem Server platziert wird und das Multicloud-Gateway als Forward-Proxy konfiguriert ist.

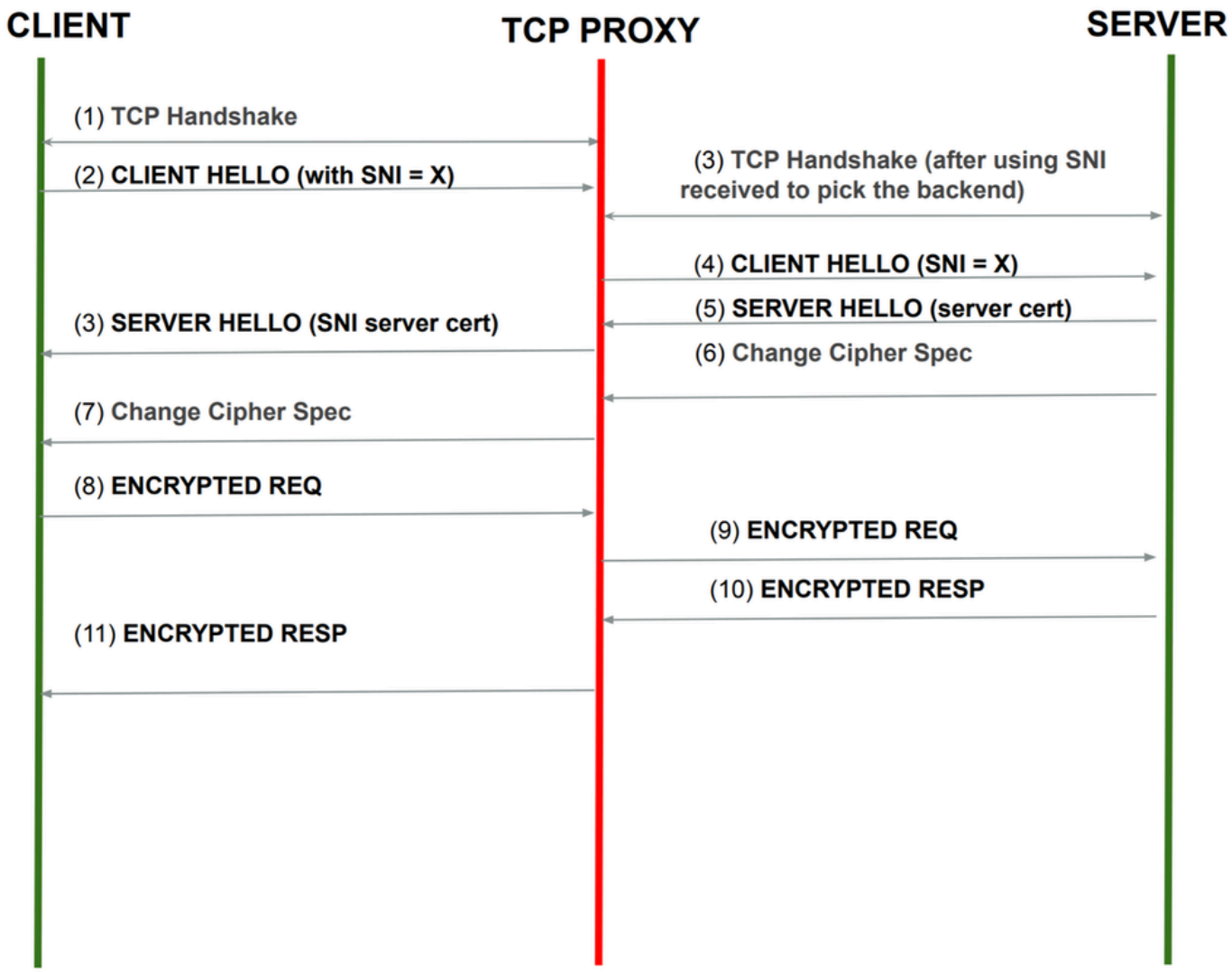
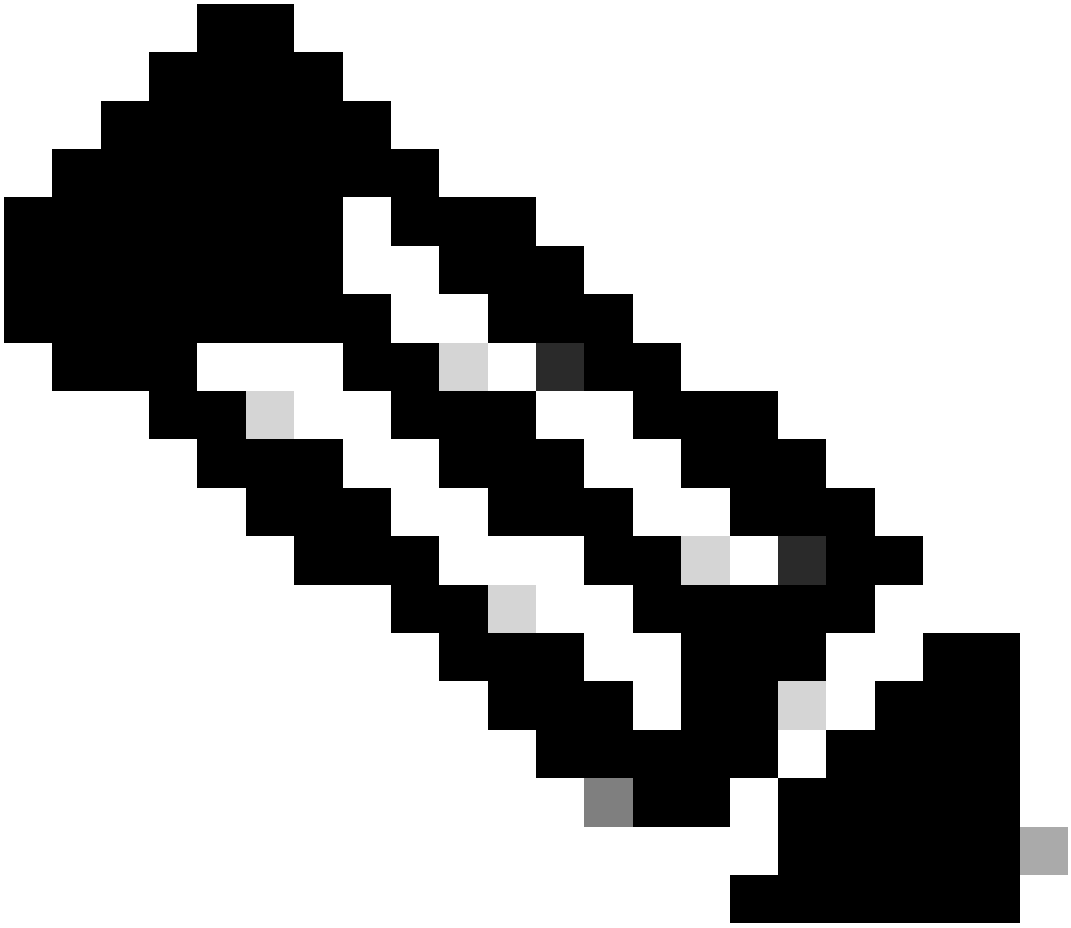
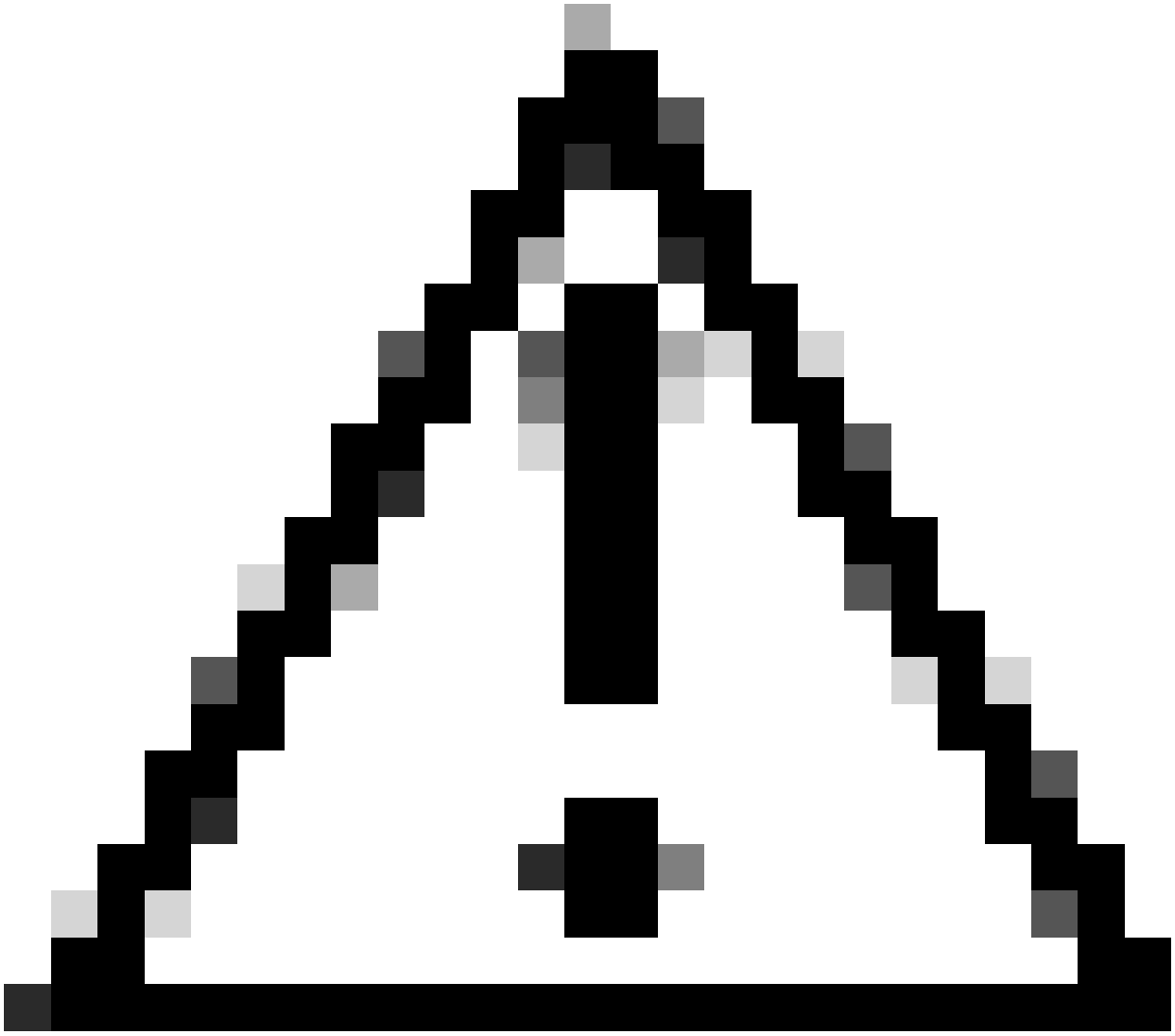


Image - MCD-Weiterleitungsproxy



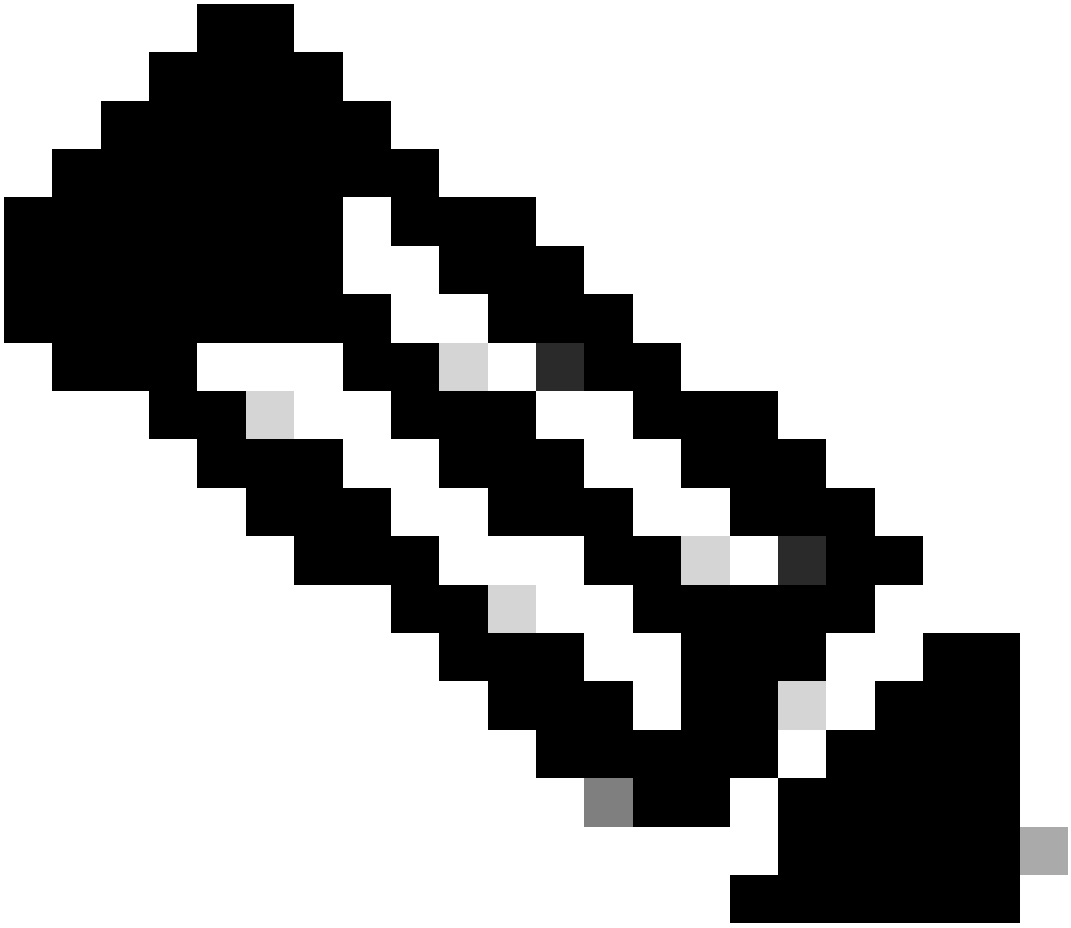
Hinweis: Dieser Prozess gilt für SSH-Datenverkehr, wenn der Client für die Verwendung des Multicloud-Gateways als Proxy für die Verbindung mit dem SSH-Server eingerichtet ist.

1. Der TCP-Drei-Wege-Handshake wird zwischen dem Client und dem Multicloud-Gateway initiiert.
2. Der Client sendet eine CLIENT HELLO an den Server. Diese CLIENT HELLO enthält den Server Name Identifier (SNI). Das Gateway fängt dieses Paket ab und führt die FQDN-Filterrichtlinie aus.



Vorsicht: Bestimmte Anwendungen, die für die Verwendung automatischer Aushandlungsprotokolle konfiguriert wurden, z. B. Anwendungen, die die SSH-Version bestimmen, dürfen Client Hello nicht übertragen.

3. Wenn der Datenverkehr zulässig ist, initiiert das Gateway eine neue TCP-Handshake-Anforderung an den Server und leitet den Client Hello weiter. (wie vom Client empfangen)



Hinweis: Wenn der Server keine Pakete vom Multicloud-Gateway empfangen hat, kann dies daran liegen, dass der Client den Client nicht Hello gesendet hat.

4. Das Multicloud-Gateway hat Server Hello an den Client weitergeleitet.

5. Nach dem Zertifikataustausch werden alle Pakete ohne Aktion gesendet

Zugehörige Informationen

- Cisco Multicloud Defense - Benutzerhandbuch - FQDN-Filterprofil [Cisco Defense Orchestrator] - Cisco
- Häufig gestellte Fragen - 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.