HTTP-verkeersstroom door multi-cloud Defense Gateway

Inhoud

Inleiding

Dit document beschrijft hoe de Cisco Multicloud Defense Gateway het HTTPS-verkeer verwerkt wanneer de proxyactie voor- of achteruit is geconfigureerd.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Basiskennis van cloud computing
- Basiskennis van computernetwerken

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

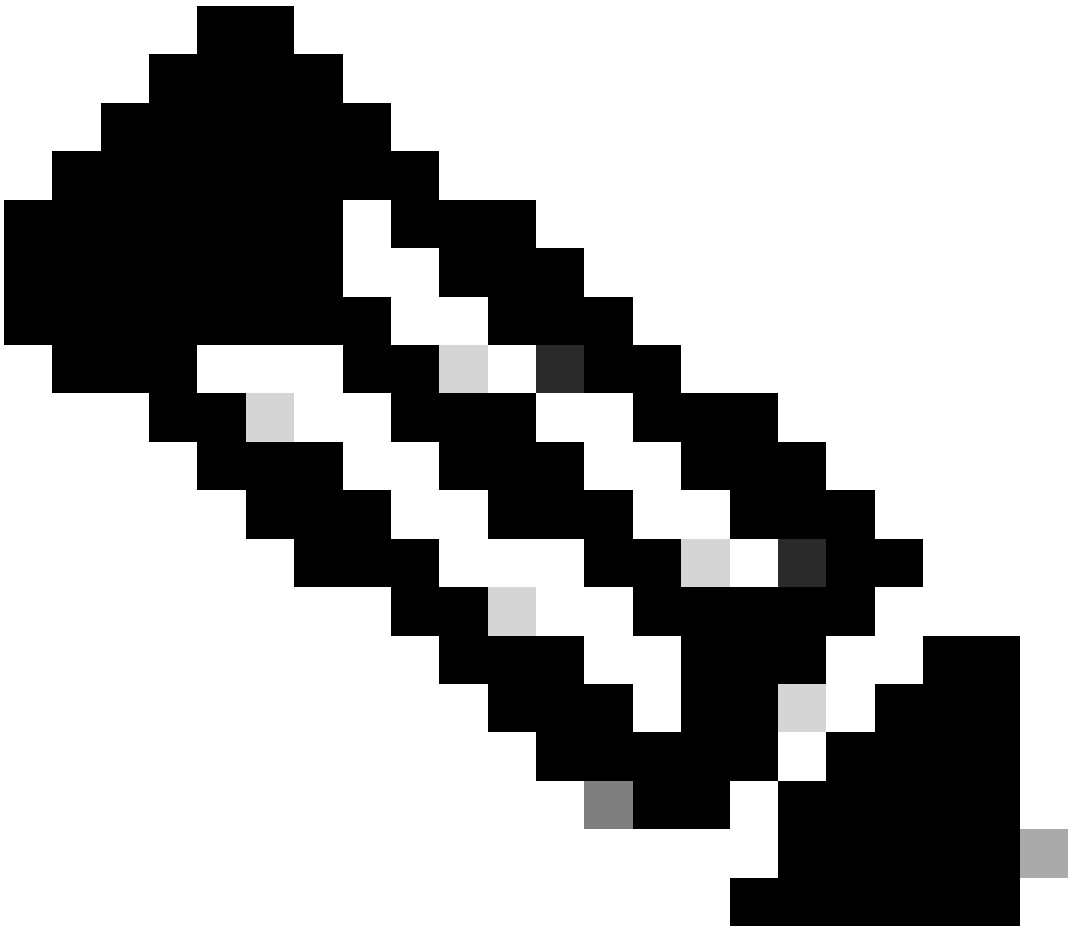
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Expliciete voorwaartse proxy

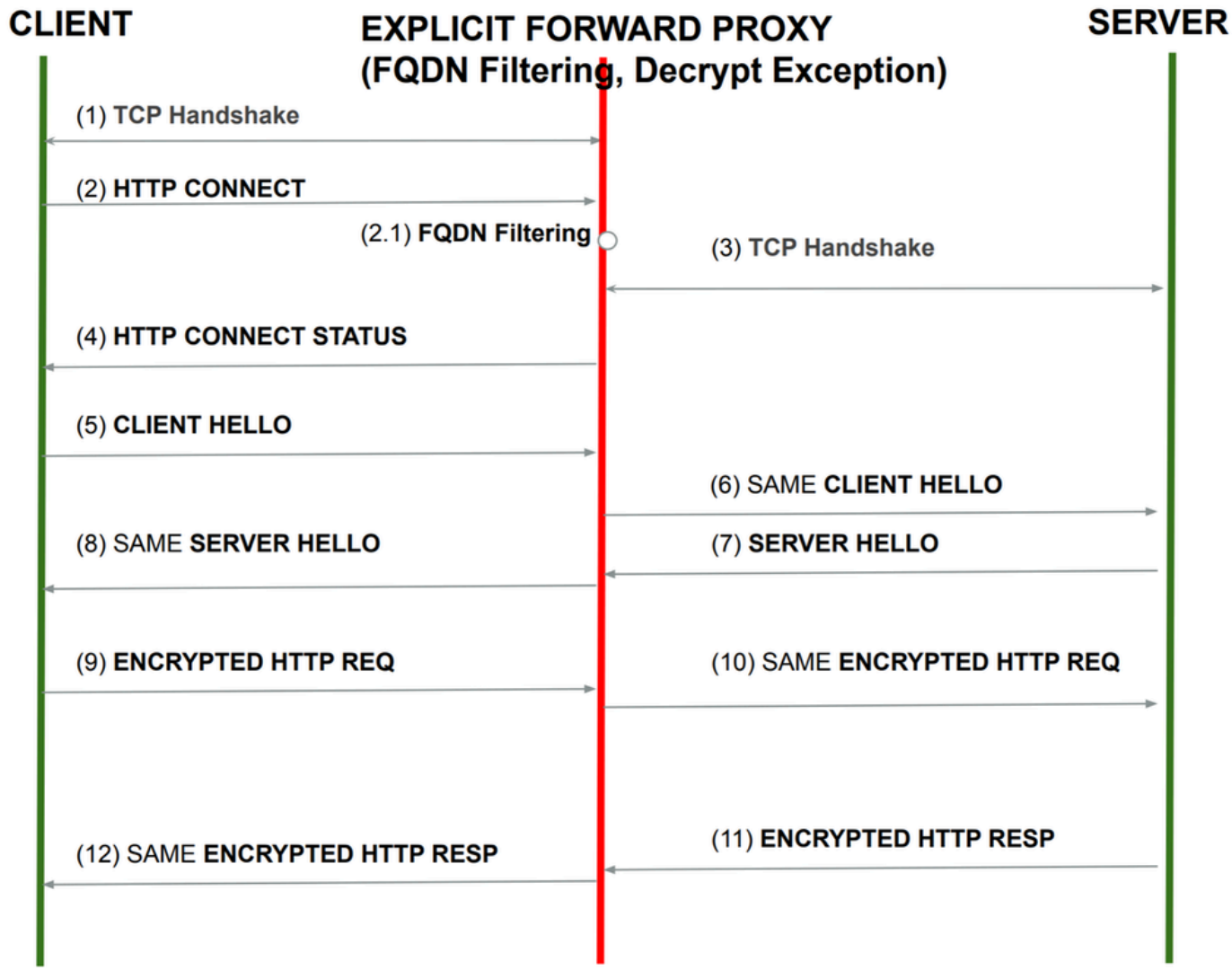
Expliciete voorwaartse proxy betekent dat uw computer netwerk instellingen worden geconfigureerd om expliciet de proxy te gebruiken. Het verkeer van de client is bestemd voor de proxyserver en de proxyserver onderzoekt het voordat het verkeer naar de eigenlijke bestemming wordt doorgestuurd.

Expliciete voorwaartse proxy (met uitzondering van decryptie)

Dit diagram toont de netwerkstroom wanneer de Multicloud gateway in het pad tussen de client en de webserver wordt geplaatst en de Multicloud gateway is geconfigureerd om als een voorwaartse proxy met decryptie-uitzondering te fungeren.



Opmerking: Uitzonderingen voor decryptie verwijzen naar scenario's waarin u liever hebt dat Multicloud Gateway geen verkeer decrypteert en inspecteert, vaak van toepassing op financiële, gezondheidszorg- en overheidswebsites. In deze situaties activeert u decryptie-uitzonderingen voor specifieke FQDN’s.



Afbeelding - Expliciete voorwaartse proxy (met uitzondering van decryptie)-stroom

[1] De TCP 3-weg handshake wordt geïnitieerd tussen de client en de Multicloud gateway.

[2] Zodra de handdruk volledig is, verzendt de cliënt HTTP CONNECT.

[3] Vanaf de CONNECT-header identificeert Multicloud Gateway de FQDN en past het FQDN-filterbeleid toe.

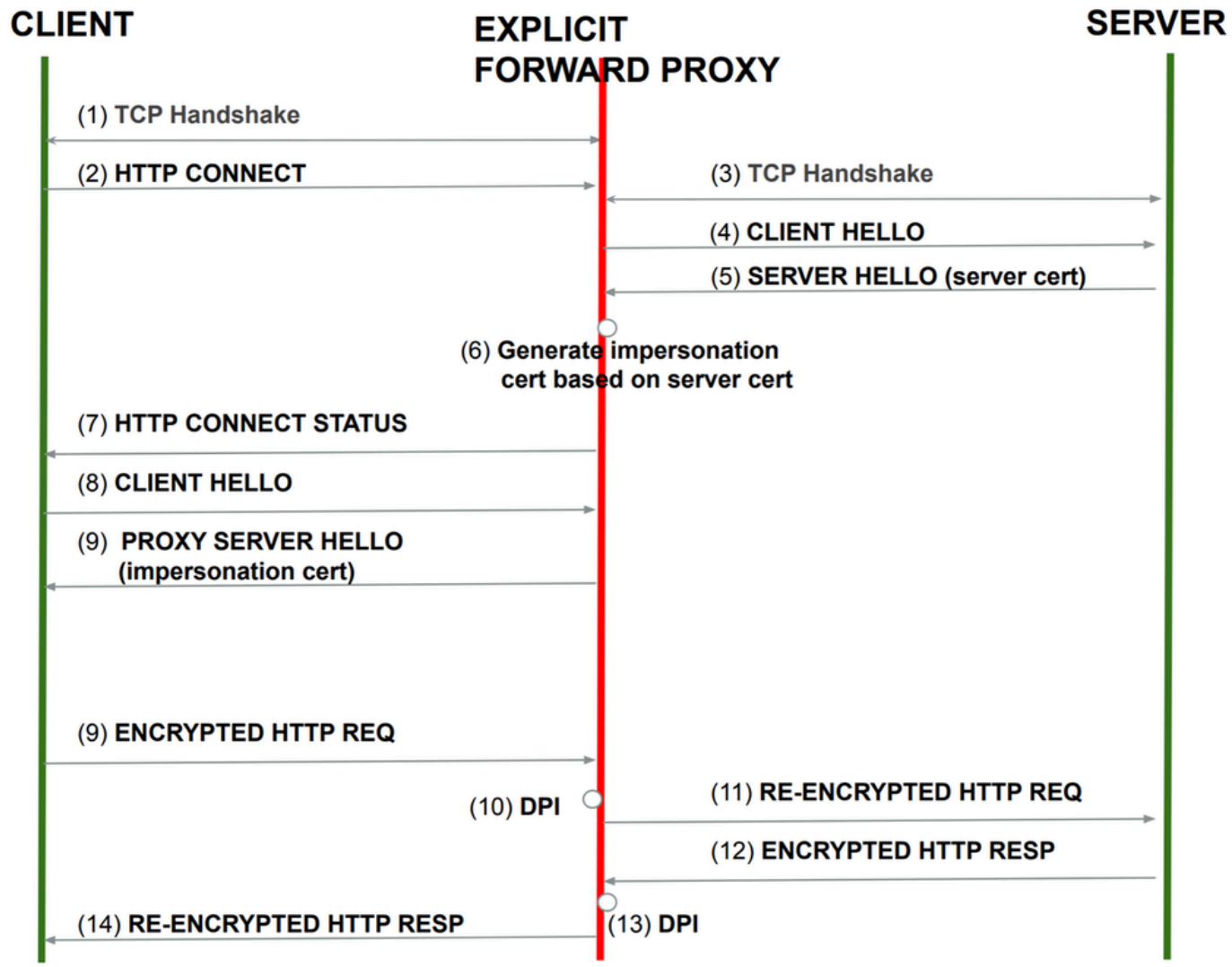
[4] Als het verkeer is toegestaan, stelt de gateway een nieuw TCP-handshake-verzoek in bij de server en stuurt de HTTP CONNECT door.

[5] HTTP STATUS-antwoordbericht wordt op transparante wijze naar de client doorgestuurd.

[6] Vanaf dit punt worden alle berichten rechtstreeks en zonder interceptie verzonden.

Expliciete voorwaartse proxy (met decryptie)

Hier is de verkeersstroom, terwijl de Expliciete voorwaartse proxy is geconfigureerd om het verkeer te decoderen.



Afbeelding - expliciete voorwaartse proxy (met decryptie)

[1] De TCP 3-weg handshake wordt geïnitieerd tussen de client en de Multicloud gateway.

[2] Zodra de handdruk volledig is, verzendt de cliënt HTTP CONNECT.

[3] Vanuit de CONNECT-header identificeert Multicloud Gateway de FQDN en past het FQDN-filterbeleid toe.

[4] Multicloud Gateway start de TCP handshake met de server.

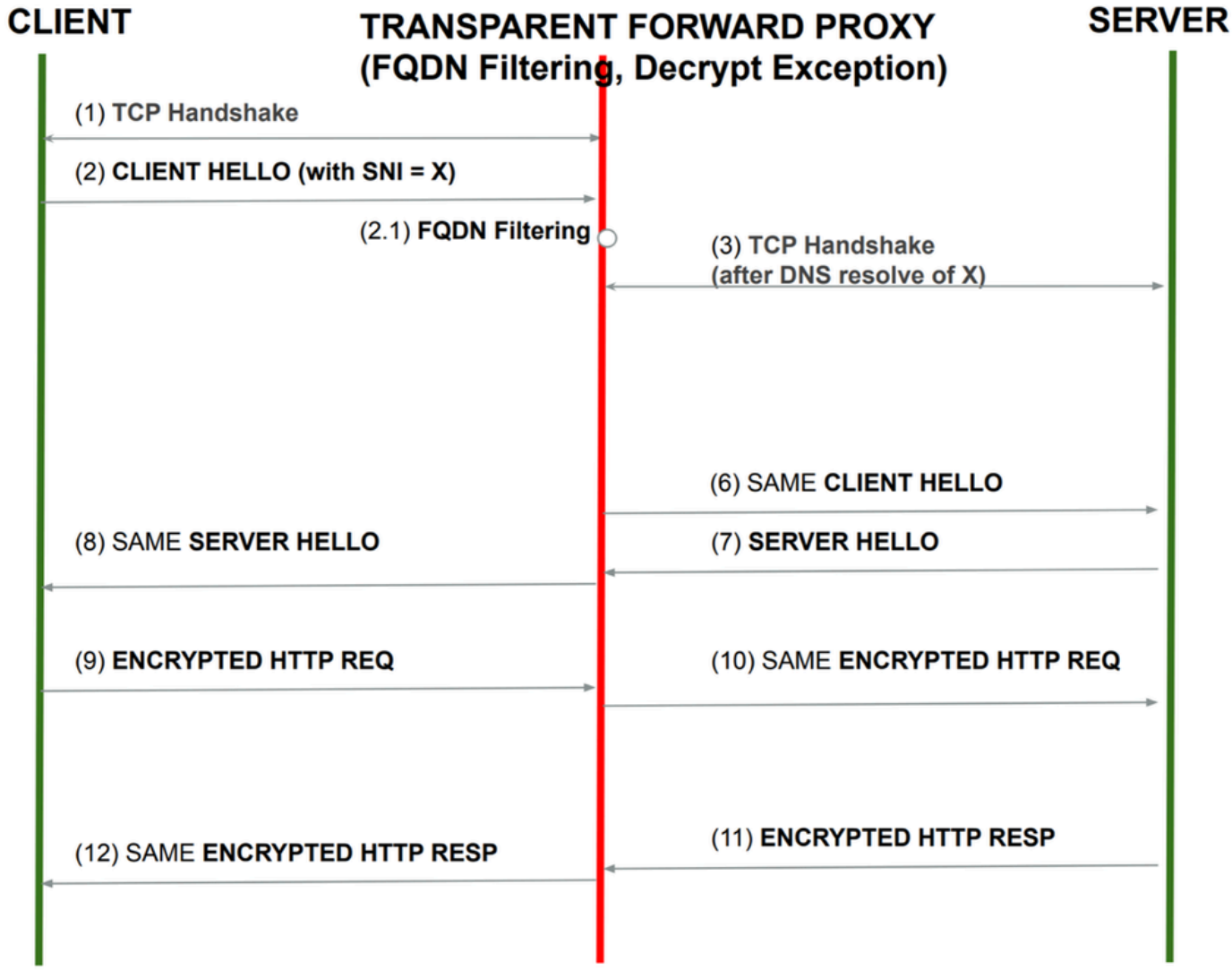
[5] Nadat de TLS-handdruk met succes is voltooid tussen Multicloud Gateway en de server, heeft Multicloud Gateway een certificaat afgegeven voor het gedecrypteerde verkeer tussen client en Multicloud Gateway.

[6] Vanaf dit punt wordt al het verkeer tussen de client en de server opnieuw gedecodeerd en versleuteld.

Transparante voorwaartse proxy

Transparante voorwaartse proxy (met uitzondering van decryptie)

Het volgende scenario schetst het proces wanneer het verkeer een openbare server richt en de gateway een configuratie voor voorwaartse volmacht met een decryptie uitzondering heeft.



Afbeelding - Transparante voorwaartse proxy (met uitzondering van decryptie)

[1] Multicloud gateway reageert op TCP handshake.

[2] De client stuurt een CLIENT HELLO naar de server. Deze CLIENT-HELLO bevat de Server Name Identifier (SNI). De gateway onderschept dit pakket en voert FQDN-filterbeleid uit.

[3] Als het verkeer is toegestaan en de uitzondering voor decryptie is ingesteld voor de URL, voert de Multicloud-gateway een andere DNS-resolutie uit voor de SNI.

[4] Multicloud Gateway start een TCP-handdruk op de server.

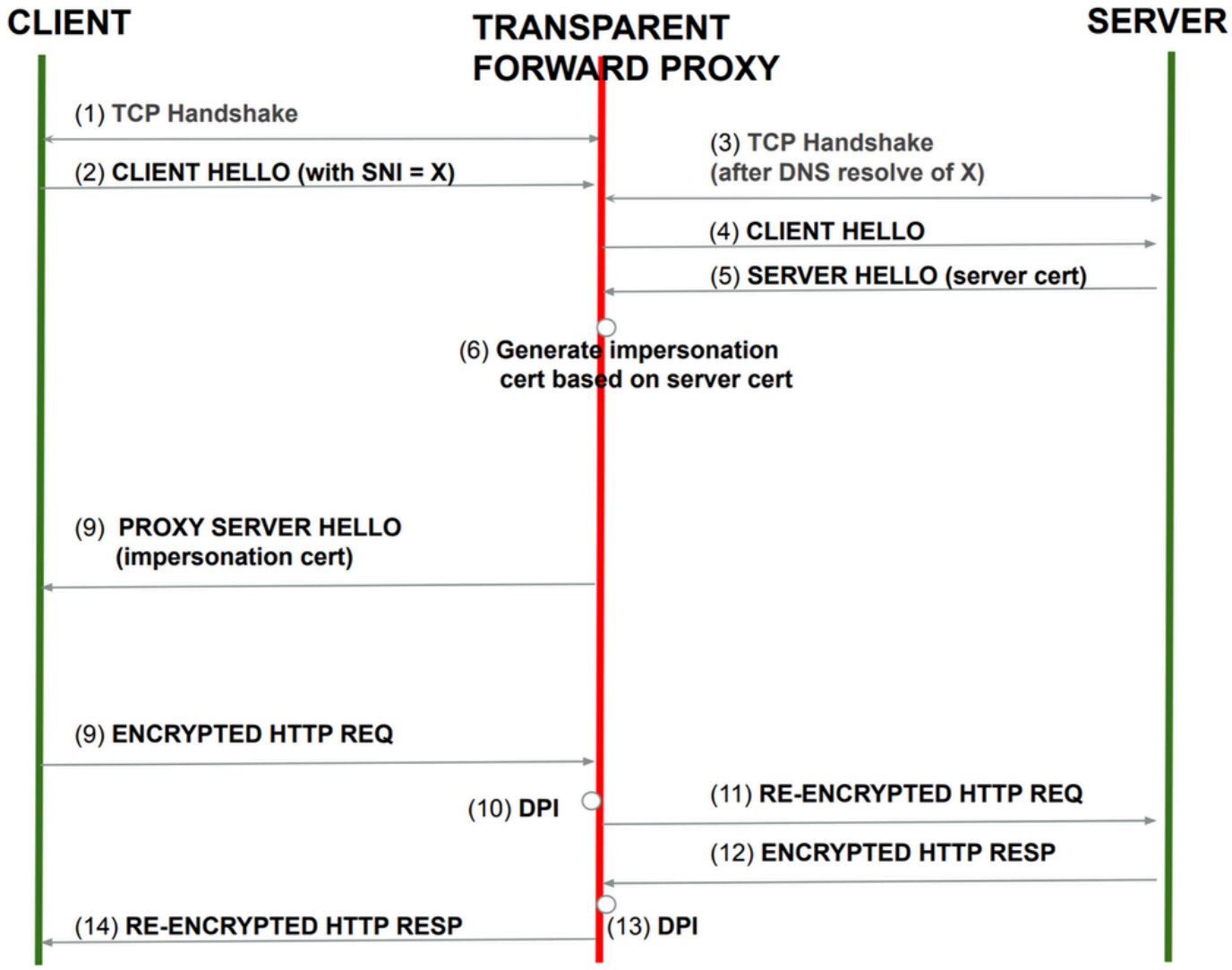
[5] Multicloud Gateway stuurt dezelfde CLIENT HALLO door naar de server (zoals deze van de client werd ontvangen).

[6] De SERVER HELLO ontvangen van de server wordt doorgestuurd zoals het is zonder enige wijziging.

[7] Vanaf dit punt worden alle pakketten verzonden zoals het is zonder enige actie

Transparante voorwaartse proxy (met decryptie)

Het volgende scenario schetst het proces wanneer het verkeer een openbare server richt en de gateway een configuratie voor de voorwaartse volmacht heeft om het verkeer te decrypteren.



Afbeelding - Transparent Forward Proxy (met decryptie)

[1] Multicloud gateway reageert op TCP handshake.

[2] De client stuurt een CLIENT HELLO naar de server. Deze CLIENT-HELLO bevat de Server Name Identifier (SNI). De gateway onderschept dit pakket en voert FQDN-filterbeleid uit.

[3] Als het verkeer is toegestaan en de decryptie is geconfigureerd voor de URL, voert de Multicloud-gateway een andere DNS-resolutie uit voor de SNI.

[4] Multicloud Gateway start een TCP handshake naar de server.

[5] Nadat de TLS-handdruk met succes is voltooid tussen Multicloud Gateway en de server, heeft Multicloud Gateway een certificaat afgegeven voor het gedecrypteerde verkeer tussen de client en Multicloud Gateway.

[6] Vanaf dit punt wordt al het verkeer tussen de client en de server opnieuw gedecodeerd en versleuteld.

Gerelateerde informatie

- Cisco MultiCloud Defense Gebruikershandleiding - FQDN-filterprofiel [Cisco Defense Orchestrator] - Cisco
- Cisco-gebruikershandleiding voor meerdere defensiematerieel - Gateways beheren [Cisco Defense Orchestrator] - Cisco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.