

# Begrijp de Proxy niet-HTTP(S) van de Multiplexing-gateway

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Proxy](#)

[Voorwaartse proxy voor meerdere gateway](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe de Cisco MultiCloud Defense Gateway het TCP-verkeer (anders dan op het web) verwerkt wanneer een voorwaartse proxy 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.

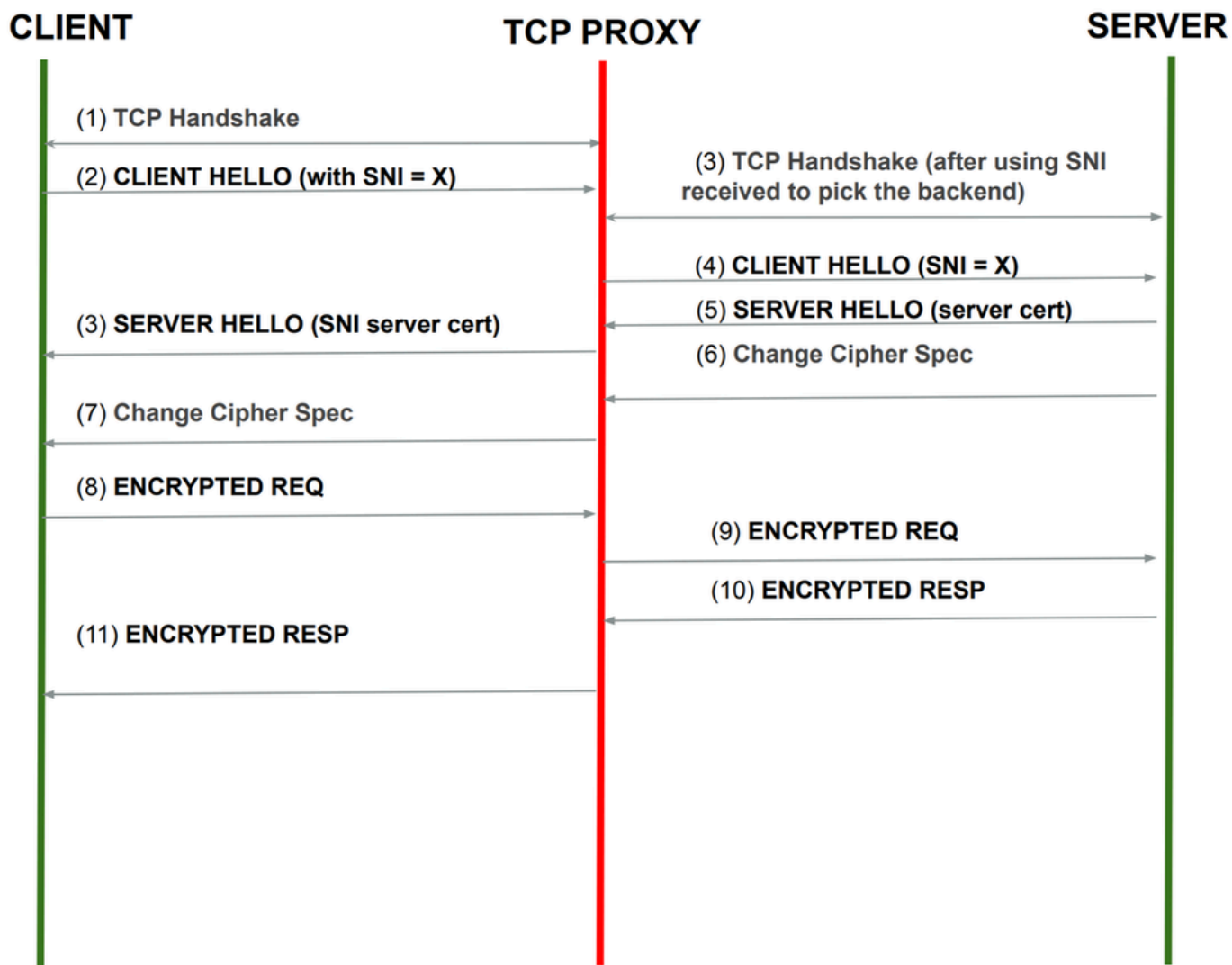
## Proxy

Een proxy fungeert als tussenstap voor twee netwerkendpoints. Het fungeert als een gateway die overgaat van het ene netwerk naar het andere voor specifieke toepassingen. Proxies beheren en vereenvoudigen de complexiteit van verzoeken door hun aanvraagproces en voorwaartse mogelijkheden. Ze bieden verschillende niveaus van functionaliteit, beveiliging en privacy, en

blijken gunstig in webbrowsen en gegevensbescherming.

## Voorwaartse proxy voor meerdere gateway

Dit diagram toont de netwerkstroom wanneer de multicloud gateway in het pad tussen de client en de server wordt geplaatst en de multicloud gateway is geconfigureerd om als een voorwaartse proxy te fungeren.

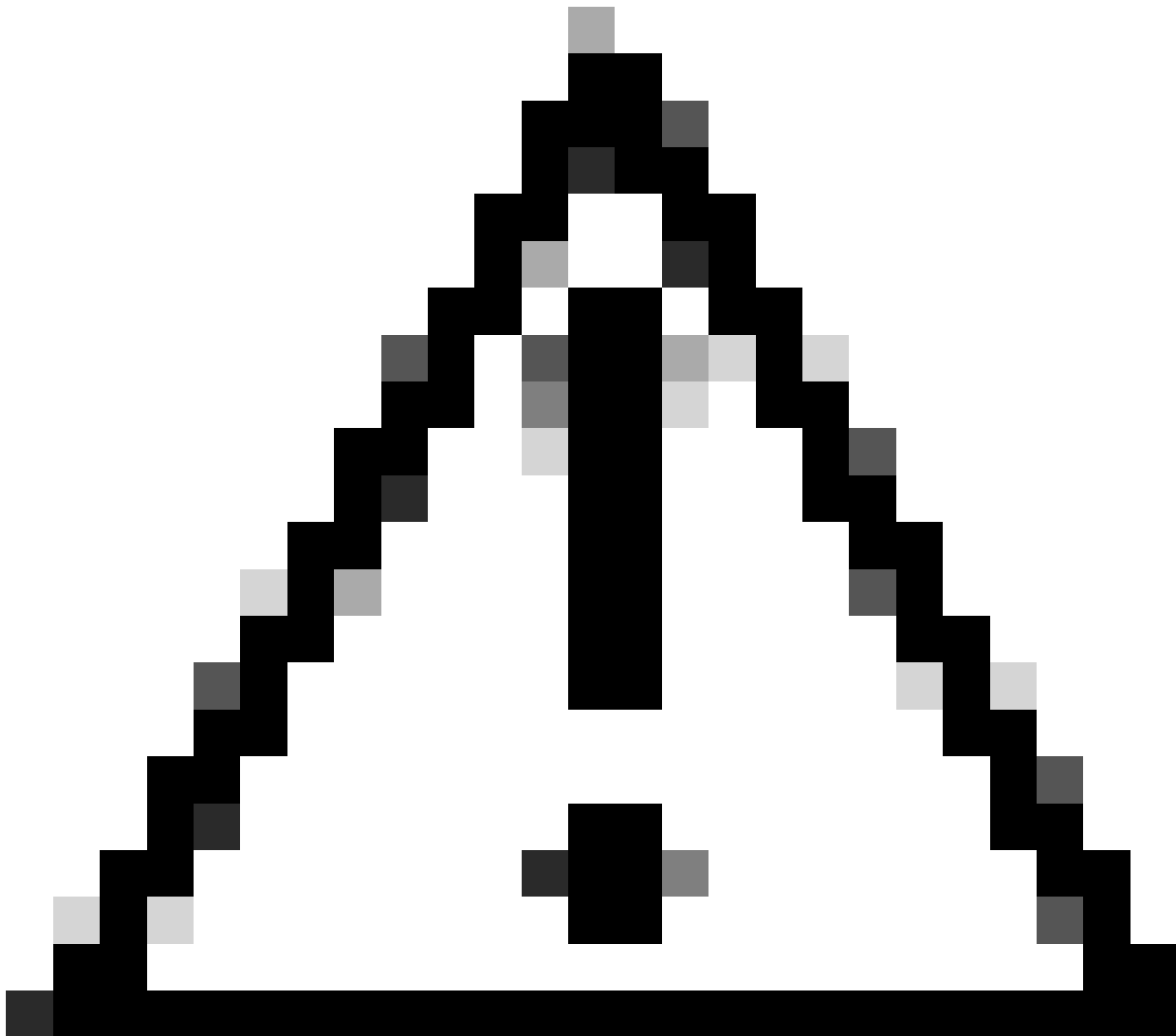


Afbeelding - MCD voorwaartse proxy



Opmerking: dit proces is van toepassing voor SSH-verkeer wanneer uw client is ingesteld om de multicloud-gateway te gebruiken als een proxy om verbinding te maken met de SSH-server.

- 
1. De TCP 3-weg handshake wordt geïnitieerd tussen de client en de multicloud gateway.
  2. De client stuurt een CLIENT HELLO naar de server. Deze CLIENT-HELLO bevat de Server Name Identifier (SNI). De gateway ondertschipt dit pakket en voert het FQDN-filterbeleid uit.



Waarschuwing: Bepaalde toepassingen die zijn geconfigureerd om automatische onderhandelingsprotocollen te gebruiken, zoals die die SSH-versie bepalen, mogen de client Hello niet verzenden.

---

3. Als het verkeer is toegestaan, initieert de gateway een nieuw TCP-handshake-verzoek aan de server en stuurt de client Hello. (zoals ontvangen van de klant)



Opmerking: Als de server geen pakketten heeft ontvangen van de multicloud-gateway, kan dit zijn omdat de client de client Hello niet heeft verzonden.

---

4. De multicloud-gateway verstuurt de Server Hello naar de client.

5. Na de certificaatuitwisseling worden alle pakketten verzonden zoals het is zonder enige actie

## Gerelateerde informatie

- [Cisco MultiCloud Defense Gebruikershandleiding - FQDN-filterprofiel \[Cisco Defense Orchestrator\] - Cisco](#)
- [Veelgestelde vragen - 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.