Entender o fluxo de tráfego não-HTTP(S) do proxy do gateway multicloud

Contents

Introdução

Este documento descreve como o Cisco Multicloud Defense Gateway lida com o tráfego TCP (que não seja a Web) quando um proxy de encaminhamento é configurado.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Conhecimento básico da computação em nuvem
- Conhecimento básico das redes de computadores

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Proxy

Um proxy serve como intermediário para dois endpoints de rede. Funciona como um gateway que faz a transição de uma rede para outra para aplicativos específicos. Os proxies controlam e simplificam a complexidade das solicitações por meio de seus recursos de encaminhamento e processo de solicitação. Eles oferecem diferentes níveis de funcionalidade, segurança e

privacidade, além de serem benéficos na navegação na Web e na proteção de dados.

.

Proxy de Encaminhamento de Gateway de Multicloud

Este diagrama mostra o fluxo de rede quando o gateway de várias nuvens é colocado no caminho entre o cliente e o servidor e o gateway de várias nuvens é configurado para atuar como um proxy de encaminhamento.

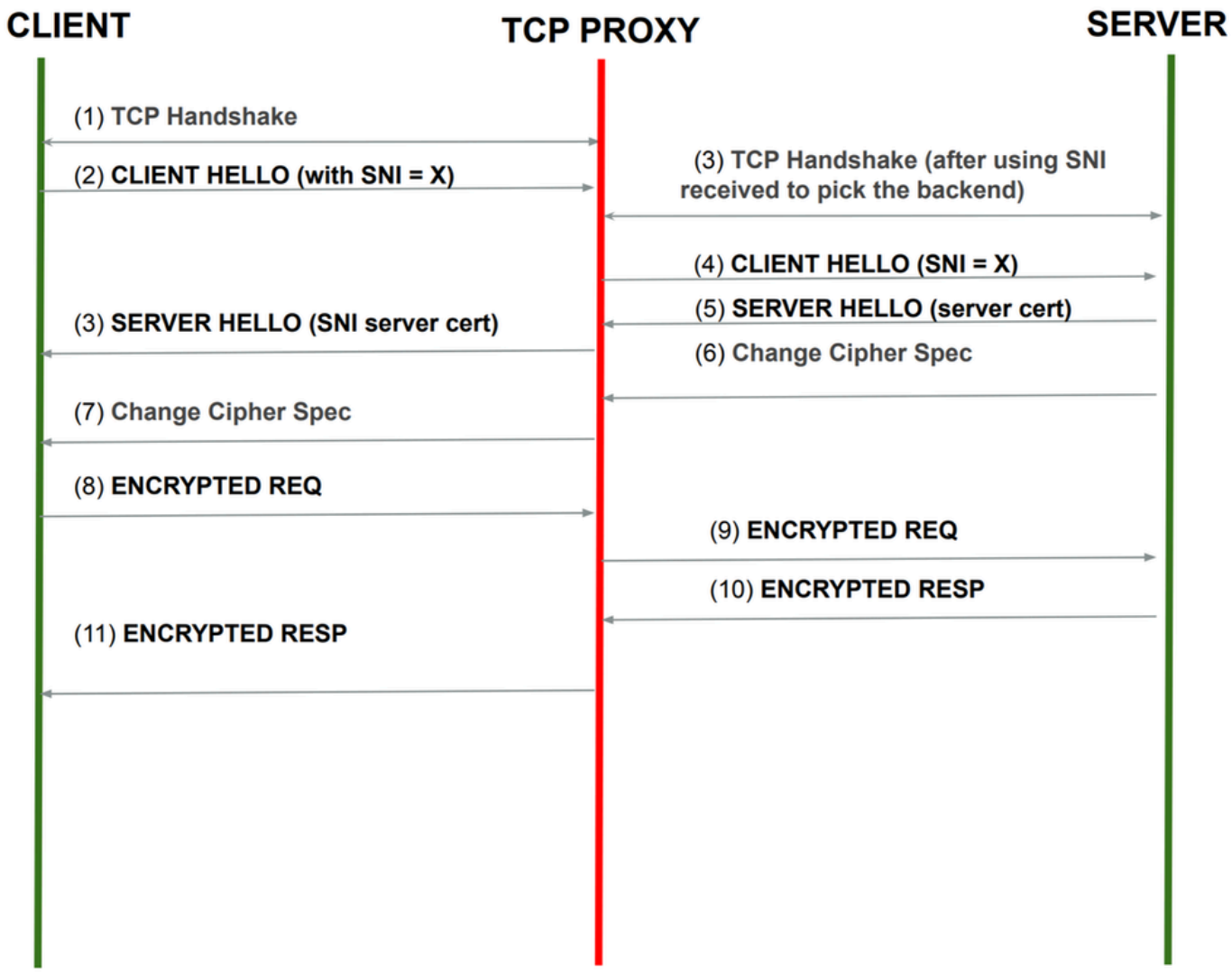
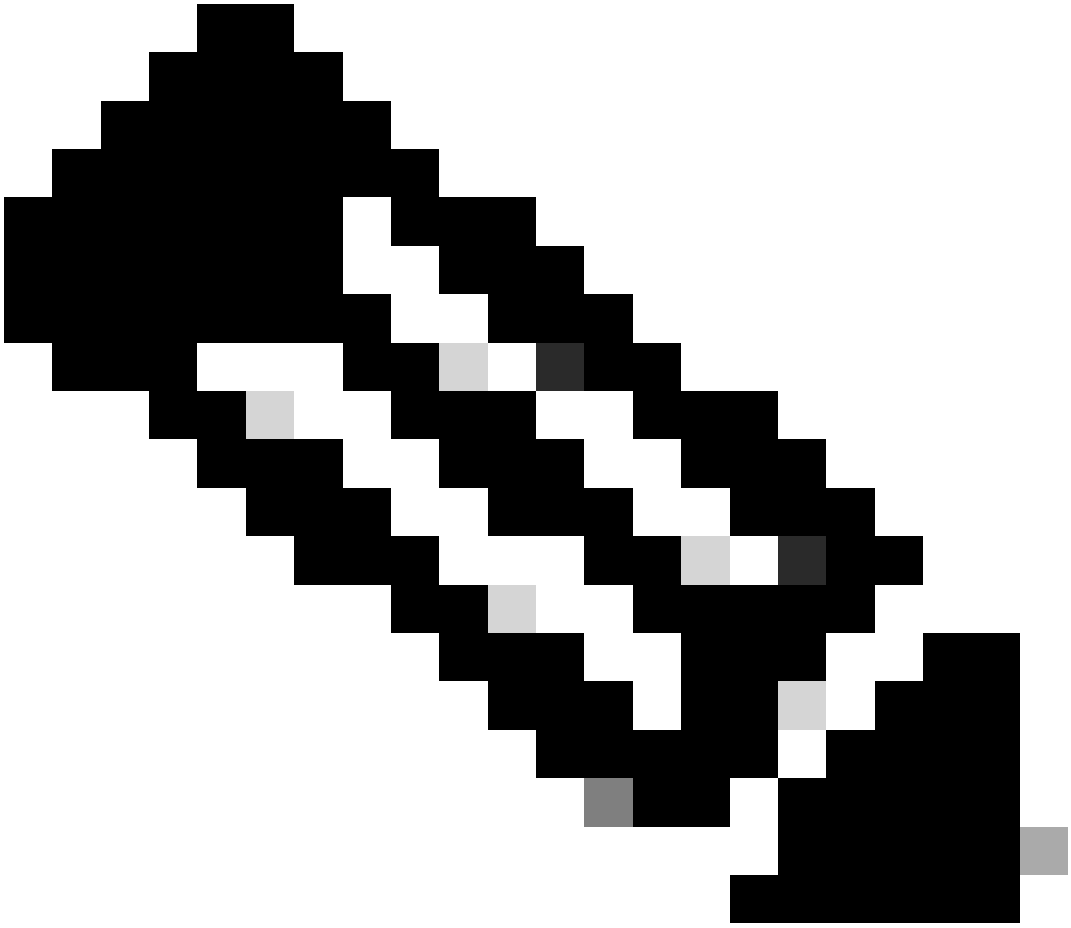
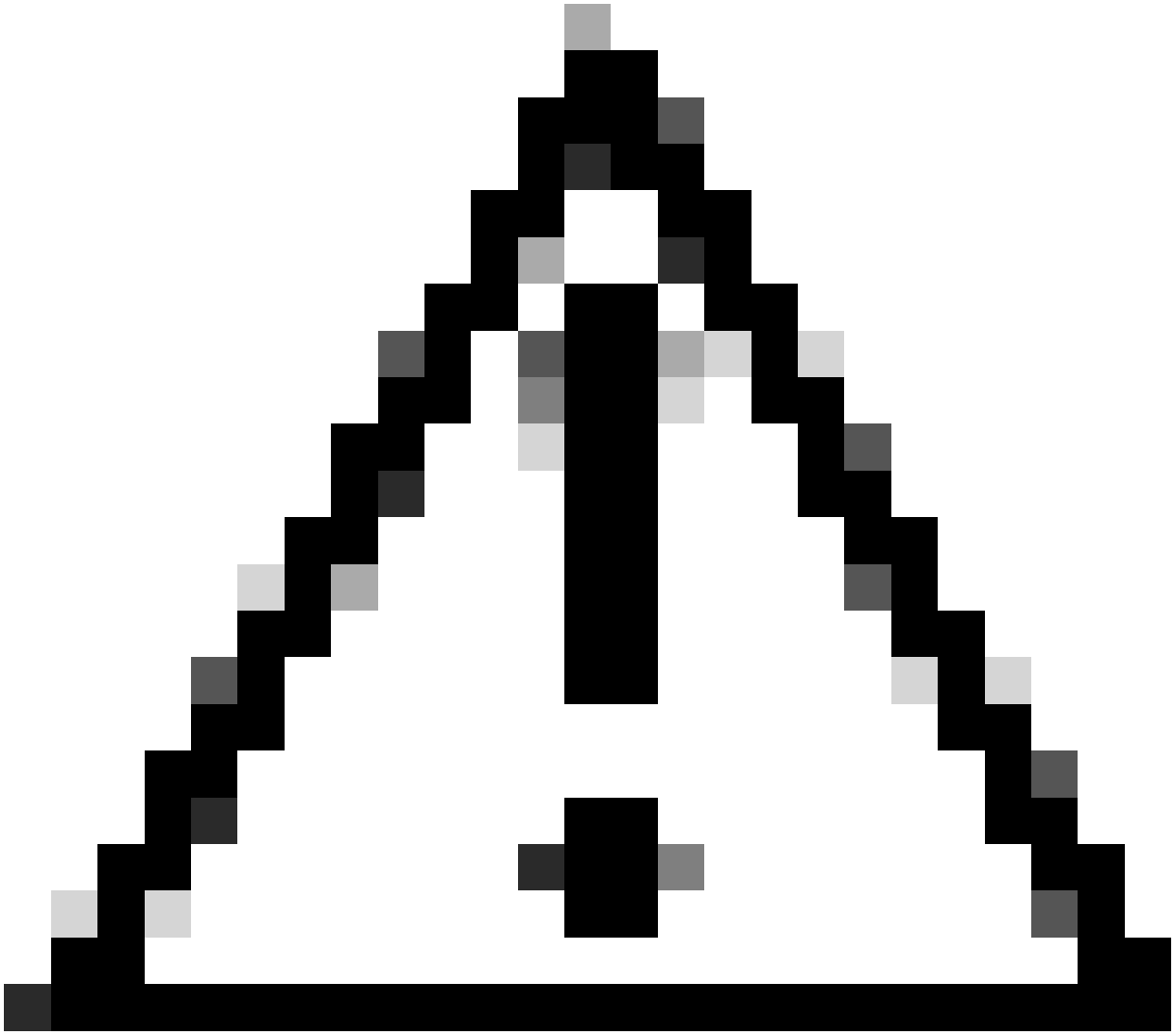


Imagem - Proxy de encaminhamento MCD



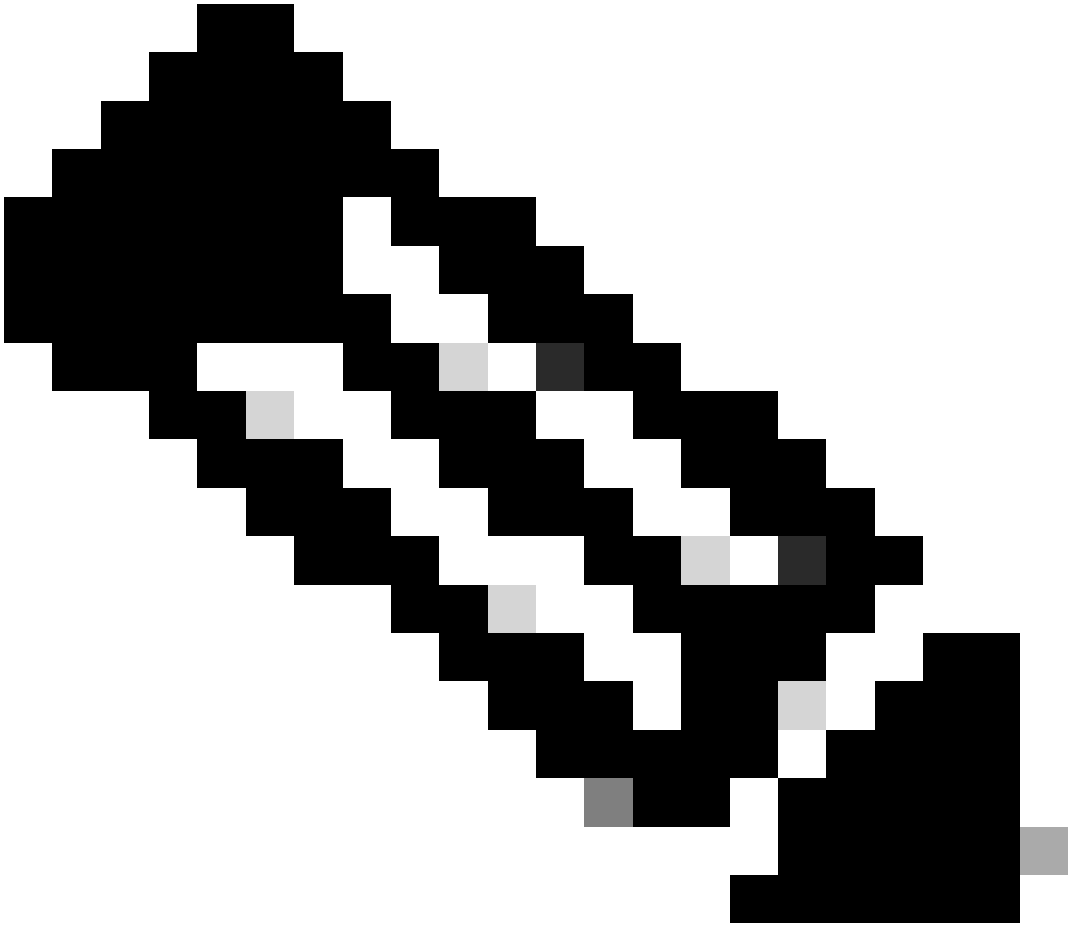
Observação: esse processo é aplicável para o tráfego SSH quando seu cliente está configurado para usar o gateway de várias nuvens como um proxy para se conectar ao servidor SSH.

1. O handshake triplo do TCP é iniciado entre o cliente e o gateway de várias nuvens.
2. O cliente envia um HELLO CLIENTE ao servidor. Este CLIENT HELLO contém o Identificador de Nome de Servidor (SNI). O gateway intercepta esse pacote e executa a política de filtragem FQDN.



Cuidado: Determinadas aplicações configuradas para utilizar protocolos de negociação automática, como as que determinam a versão do SSH, não devem transmitir o Hello do cliente.

3. Se o tráfego for permitido, o gateway inicia uma nova solicitação de handshake TCP para o servidor e encaminha o Hello do cliente. (conforme recebido do cliente)



Observação: se o servidor não recebeu nenhum pacote do gateway de várias nuvens, pode ser porque o cliente não enviou o Hello do cliente.

4. O gateway de várias nuvens encaminhou o Hello do servidor para o cliente.

5. Após a troca de certificados, todos os pacotes são enviados como estão sem nenhuma ação

Informações Relacionadas

- Guia do usuário do Cisco Multicloud Defense - Perfil de filtro FQDN [Cisco Defense Orchestrator] - Cisco
- Perguntas frequentes - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.