Entender o fluxo de tráfego HTTPS do proxy do Gateway de Defesa em Várias Nuvens

Contents

Introdução

Este documento descreve como o Cisco Multicloud Defense Gateway lida com o tráfego HTTPS quando a ação de encaminhamento ou reversão de proxy é configurada.

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.

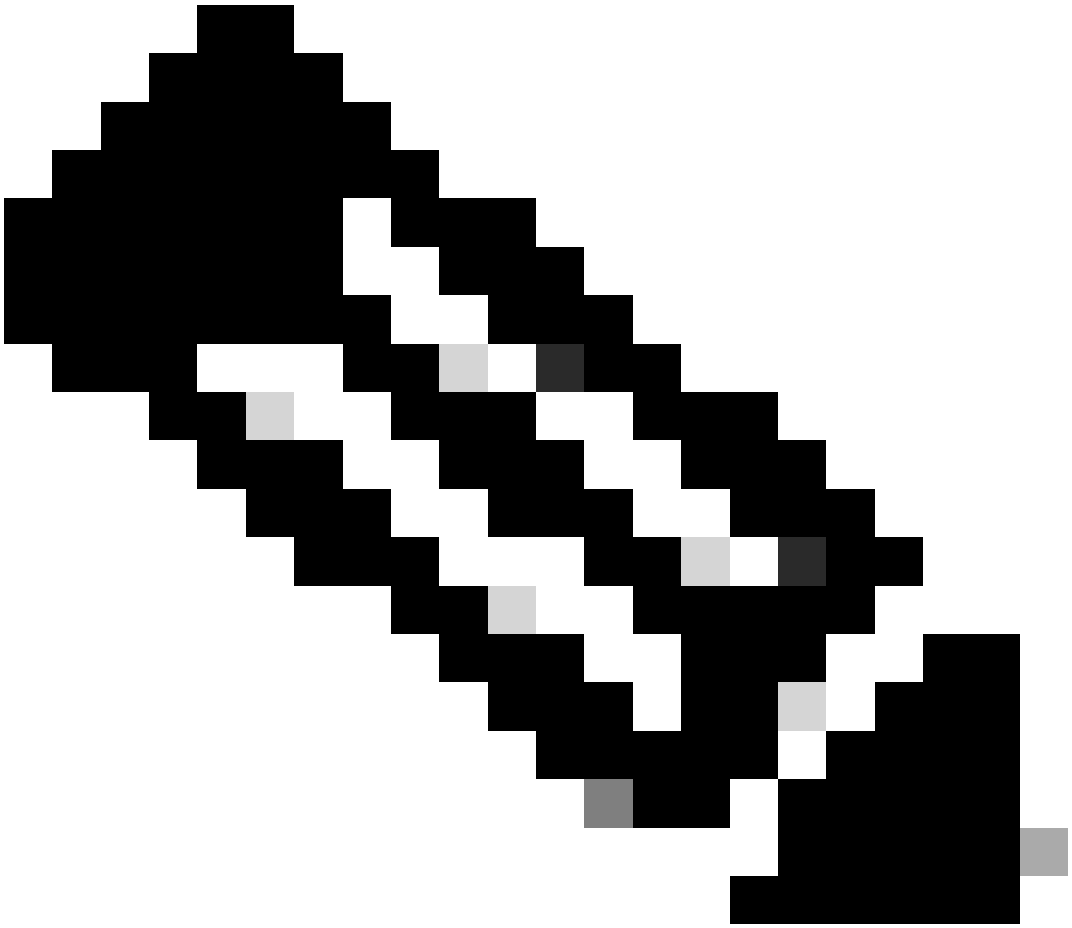
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Proxy de Encaminhamento Explícito

Proxy de encaminhamento explícito significa que as configurações de rede do computador estão definidas para usar explicitamente o proxy. O tráfego do cliente é destinado ao servidor proxy e o servidor proxy o examina antes de encaminhar o tráfego ao destino real.

Proxy de encaminhamento explícito (com exceção de descriptografia)

Este diagrama mostra o fluxo de rede quando o gateway de Multicloud é colocado no caminho entre o cliente e o servidor Web e o gateway de Multicloud é configurado para atuar como um proxy de encaminhamento com exceção de descriptografia.



> Observação: as exceções de descriptografia se referem a cenários nos quais você prefere que o Gateway de várias nuvens não descriptografe e inspecione o tráfego, geralmente aplicável a sites de finanças, serviços de saúde e governo. Nessas situações, você ativa exceções de descriptografia para FQDNs específicos.

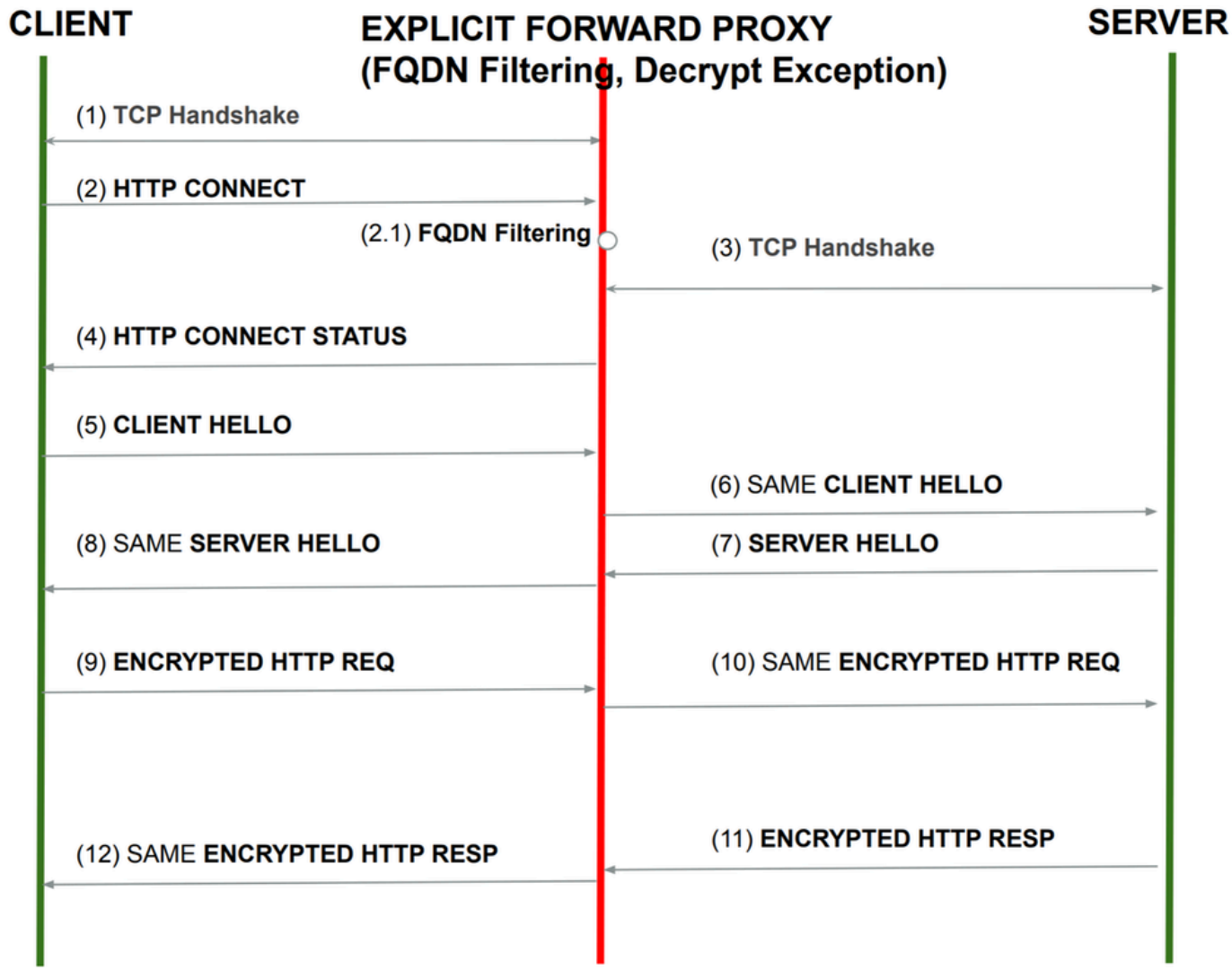


Imagem - Fluxo de proxy de encaminhamento explícito (com exceção de descriptografia)

[1] O handshake triplo do TCP é iniciado entre o cliente e o gateway da nuvem múltipla.

[2] Quando o handshake é concluído, o cliente envia o HTTP CONNECT.

[3] No cabeçalho CONNECT, o Gateway de Várias Nuvens identifica o FQDN e aplica a política de filtragem do FQDN.

[4] Se o tráfego for permitido, o gateway inicia uma nova solicitação de handshake TCP para o servidor e encaminha o HTTP CONNECT.

[5] A mensagem de resposta HTTP STATUS é encaminhada de forma transparente para o cliente.

[6] A partir deste ponto, todas as mensagens são enviadas diretamente sem qualquer intercepção.

Proxy de encaminhamento explícito (com descriptografia)

Aqui está o fluxo de tráfego, enquanto o proxy de encaminhamento explícito é configurado para descriptografar o tráfego.

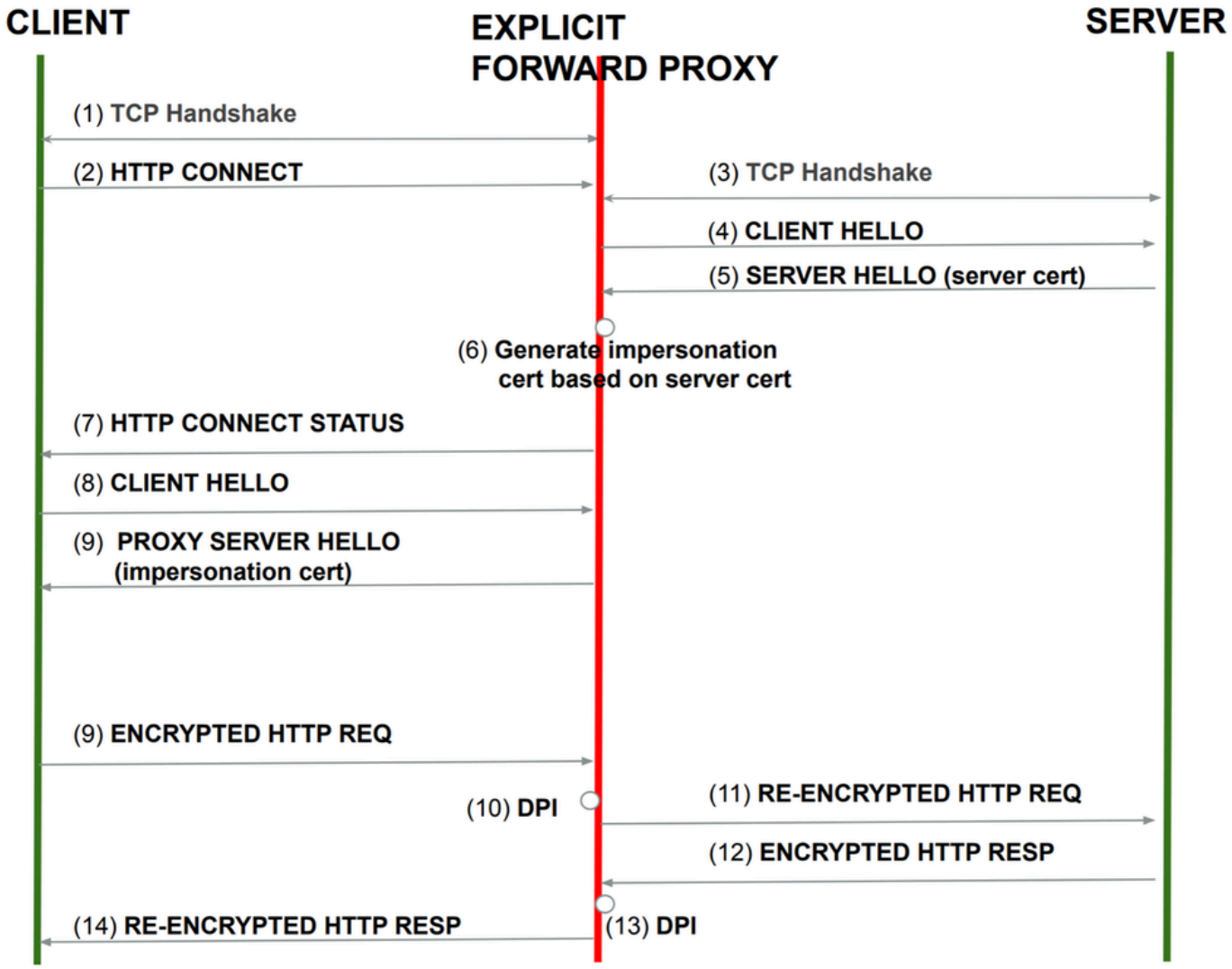


Imagem - Proxy de encaminhamento explícito (com descriptografia)

[1] O handshake triplo do TCP é iniciado entre o cliente e o gateway da nuvem múltipla.

[2] Quando o handshake é concluído, o cliente envia o HTTP CONNECT.

[3] No cabeçalho CONNECT, o Gateway de Várias Nuvens identifica o FQDN e aplica a política de filtragem do FQDN.

[4] O Gateway de Multicloud inicia o handshake TCP com o servidor.

[5] Depois que o handshake TLS foi concluído com êxito entre o Gateway Multicloud e o servidor, o Gateway Multicloud emitiu um certificado para o tráfego descriptografado entre o Cliente e o Gateway Multicloud.

[6] Desse ponto em diante, todo o tráfego entre o cliente e o servidor é descriptografado e criptografado novamente.

Transparent Forward Proxy

Transparent Forward Proxy (com exceção de descriptografia)

O cenário subsequente descreve o processo quando o tráfego é direcionado a um servidor público e o gateway tem uma configuração para encaminhar proxy com uma exceção de descriptografia.

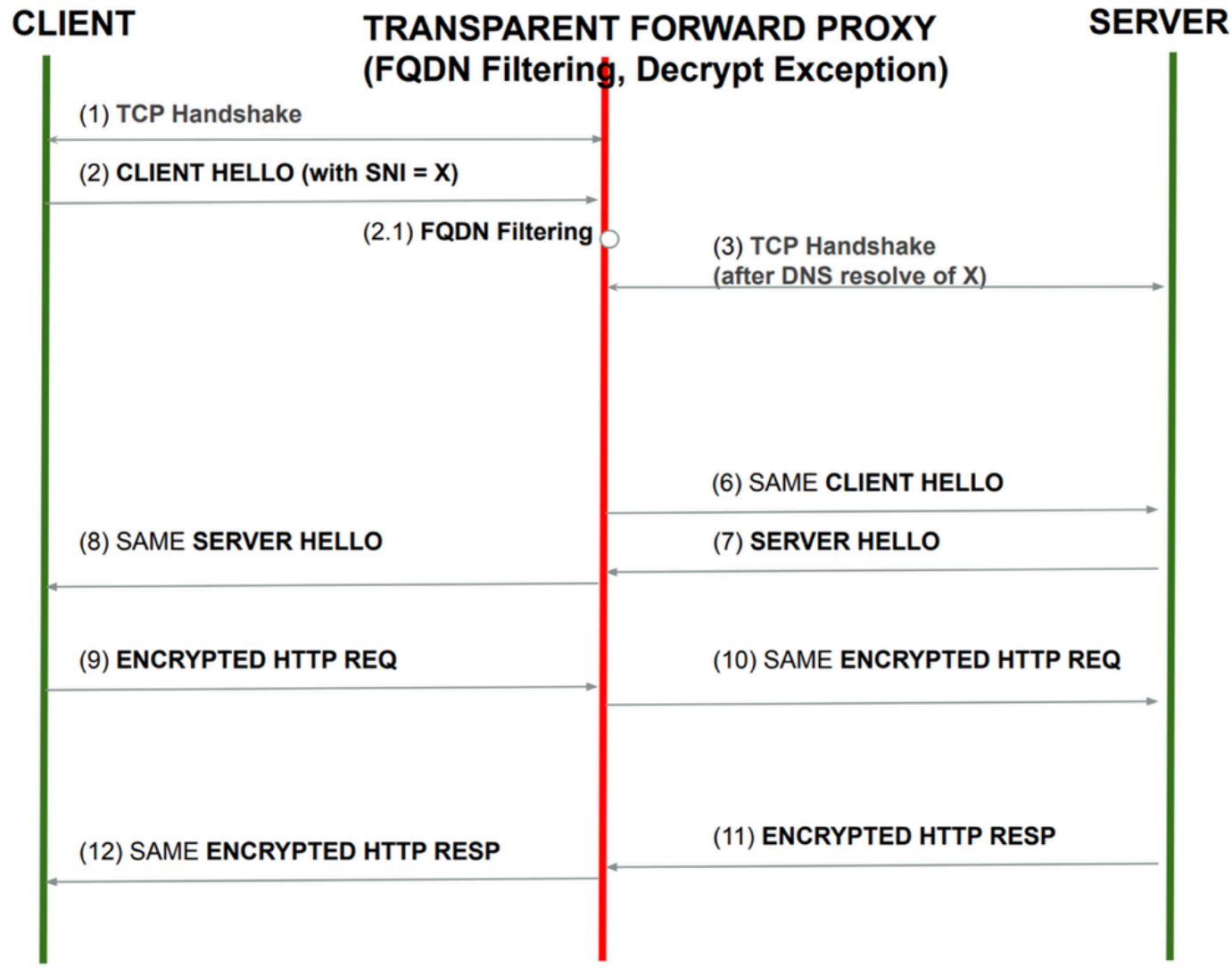


Imagem - Proxy de encaminhamento transparente (com exceção de descriptografia)

[1] O gateway multicloud responde ao handshake TCP.

[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.

[3] Se o tráfego for permitido e a exceção de descriptografia estiver configurada para a URL, o gateway de várias nuvens executará outra resolução DNS para a SNI.

[4] O Gateway de Multicloud inicia um handshake TCP para o servidor.

[5] O Gateway de Multicloud encaminha o mesmo CLIENT HELLO para o servidor (como recebido do cliente).

[6] A SAUDAÇÃO DO SERVIDOR recebida do servidor é encaminhada como está sem nenhuma modificação.

[7] A partir desse ponto, todos os pacotes são enviados como estão sem nenhuma ação

Transparent Forward Proxy (com descriptografia)

O cenário subsequente descreve o processo quando o tráfego é direcionado a um servidor público e o gateway tem uma configuração para que o proxy de encaminhamento descriptografe o tráfego.

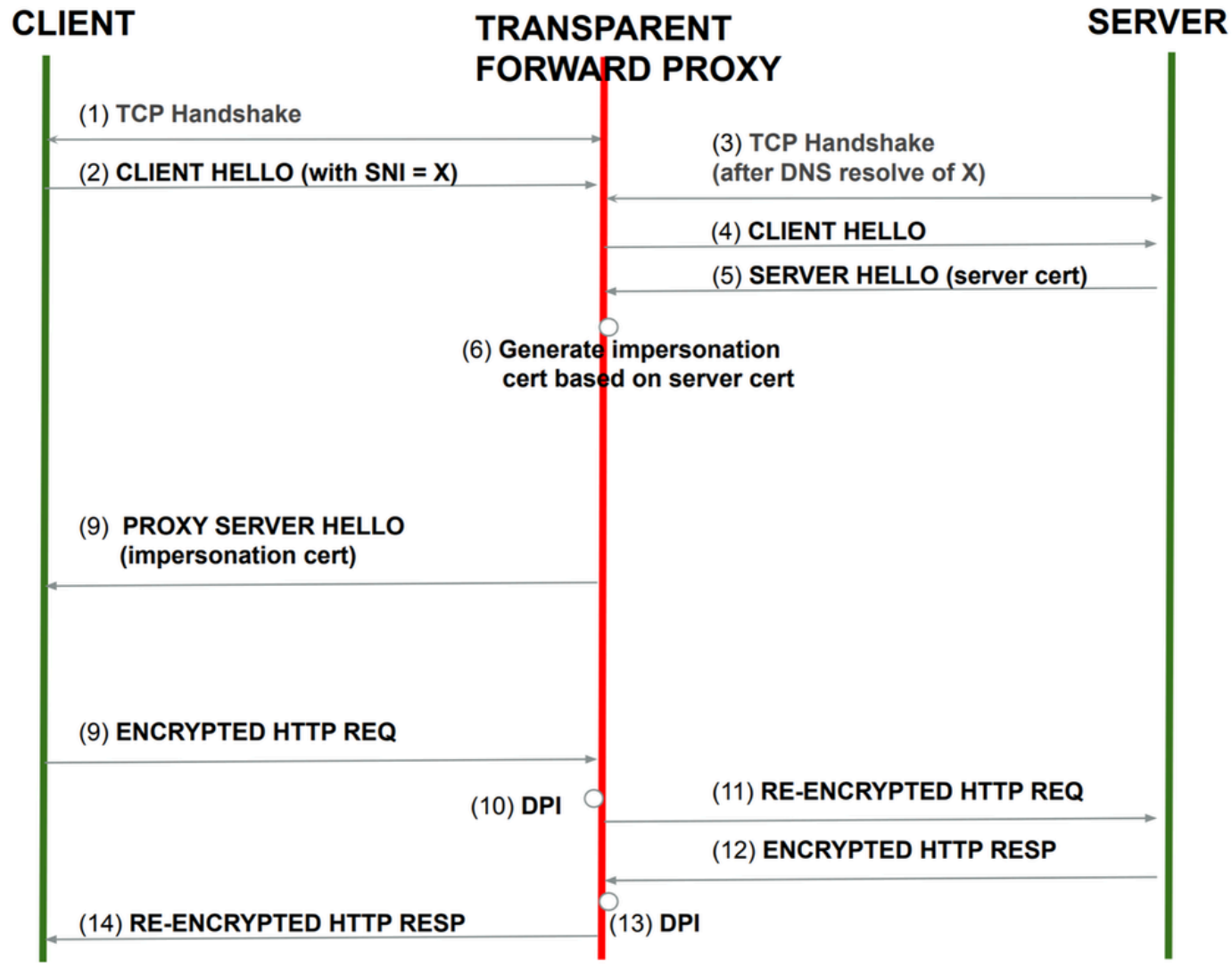


Imagem - Transparent Forward Proxy (com descriptografia)

[1] O gateway multicloud responde ao handshake TCP.

[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.

[3] Se o tráfego for permitido e a Descriptografia for configurada para o URL, o gateway de Multicloud executa outra resolução DNS para o SNI.

[4] O Gateway de Multicloud começa a iniciar um handshake TCP para o servidor.

[5] Depois que o handshake TLS foi concluído com êxito entre o Gateway Multicloud e o servidor, o Gateway Multicloud emitiu um certificado para o tráfego descriptografado entre o Cliente e o Gateway Multicloud.

[6] Desse ponto em diante, todo o tráfego entre o cliente e o servidor é descriptografado e criptografado novamente.

Informações Relacionadas

- Guia do usuário do Cisco Multicloud Defense - Perfil de filtro FQDN [Cisco Defense Orchestrator] - Cisco
- Guia do usuário do Cisco Multicloud Defense - Gerenciar gateways [Cisco Defense Orchestrator] - 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.