マルチクラウド防御ゲートウェイプロキシのHTTPSトラフィックフローについて

内容

はじめに

このドキュメントでは、フォワードプロキシまたはリバースプロキシのアクションが設定されている場合に、Cisco Multicloud Defense Gateway(MFP)がHTTPSトラフィックを処理する方法について説明します。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- クラウドコンピューティングの基礎知識
- コンピュータネットワークの基礎知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

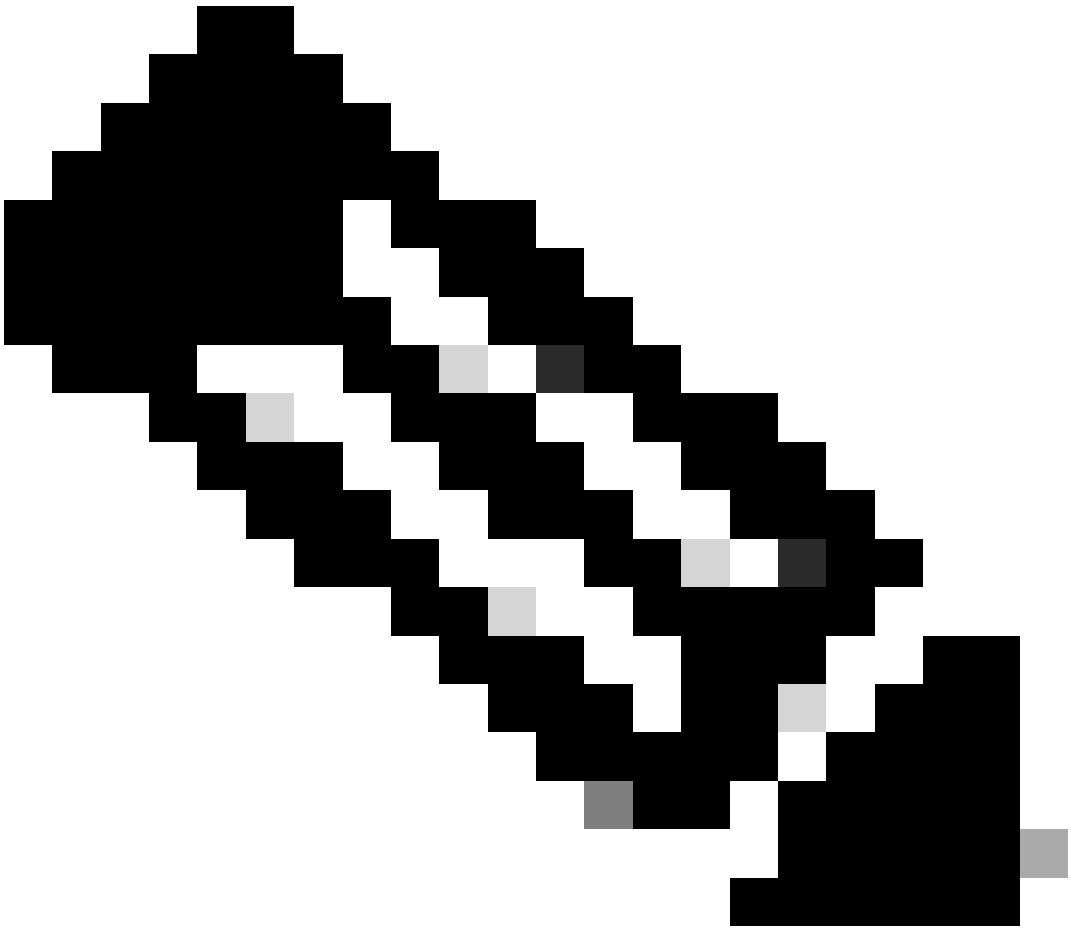
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

明示的なフォワードプロキシ

明示的な転送プロキシとは、明示的にプロキシを使用するようにコンピュータのネットワーク設定が構成されていることを意味します。クライアントからのトラフィックはプロキシサーバ宛てに送信され、プロキシサーバはトラフィックを実際の宛先に転送する前にそれを検査します。

Explicit Forward Proxy（復号化例外あり）

次の図は、マルチクラウドゲートウェイがクライアントとWebサーバ間のパスに配置され、マルチクラウドゲートウェイが復号化例外を伴う転送プロキシとして動作するように設定されている場合のネットワークフローを示しています。



注：復号化の例外とは、マルチクラウドゲートウェイがトラフィックの復号化と検査を行わないことを望むシナリオを指し、多くの場合、財務、医療、政府のWebサイトに適用されます。このような状況では、特定のFQDNの復号化例外をアクティブにします。

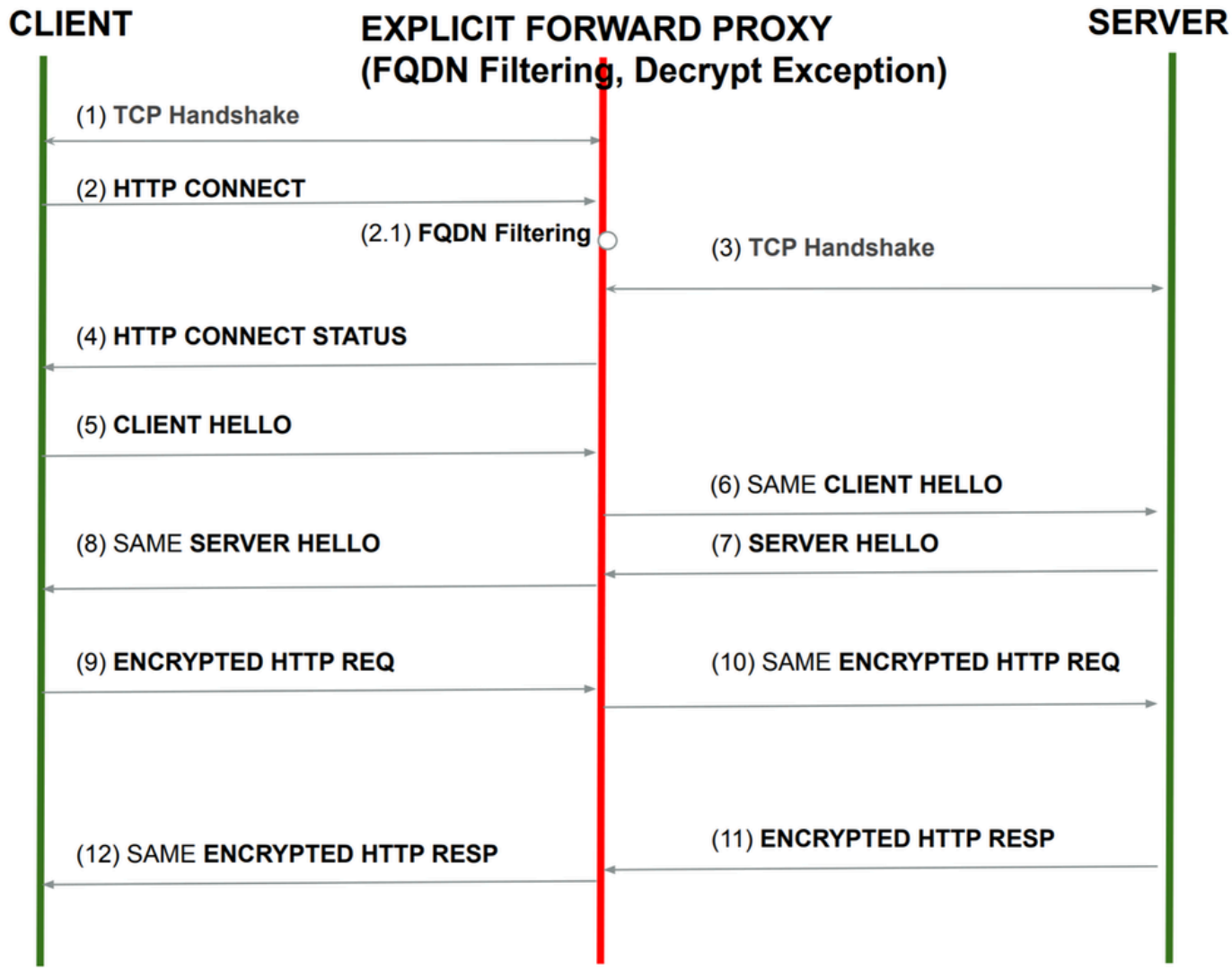


図 – Explicit Forward Proxy(EFH)（復号化例外あり）フロー

[1]クライアントとマルチクラウドゲートウェイ間でTCP 3ウェイハンドシェイクが開始されます。

[2]ハンドシェイクが完了すると、クライアントはHTTP CONNECTを送信します。

[3] CONNECTヘッダーから、マルチクラウドゲートウェイはFQDNを識別し、FQDNフィルタリングポリシーを適用します。

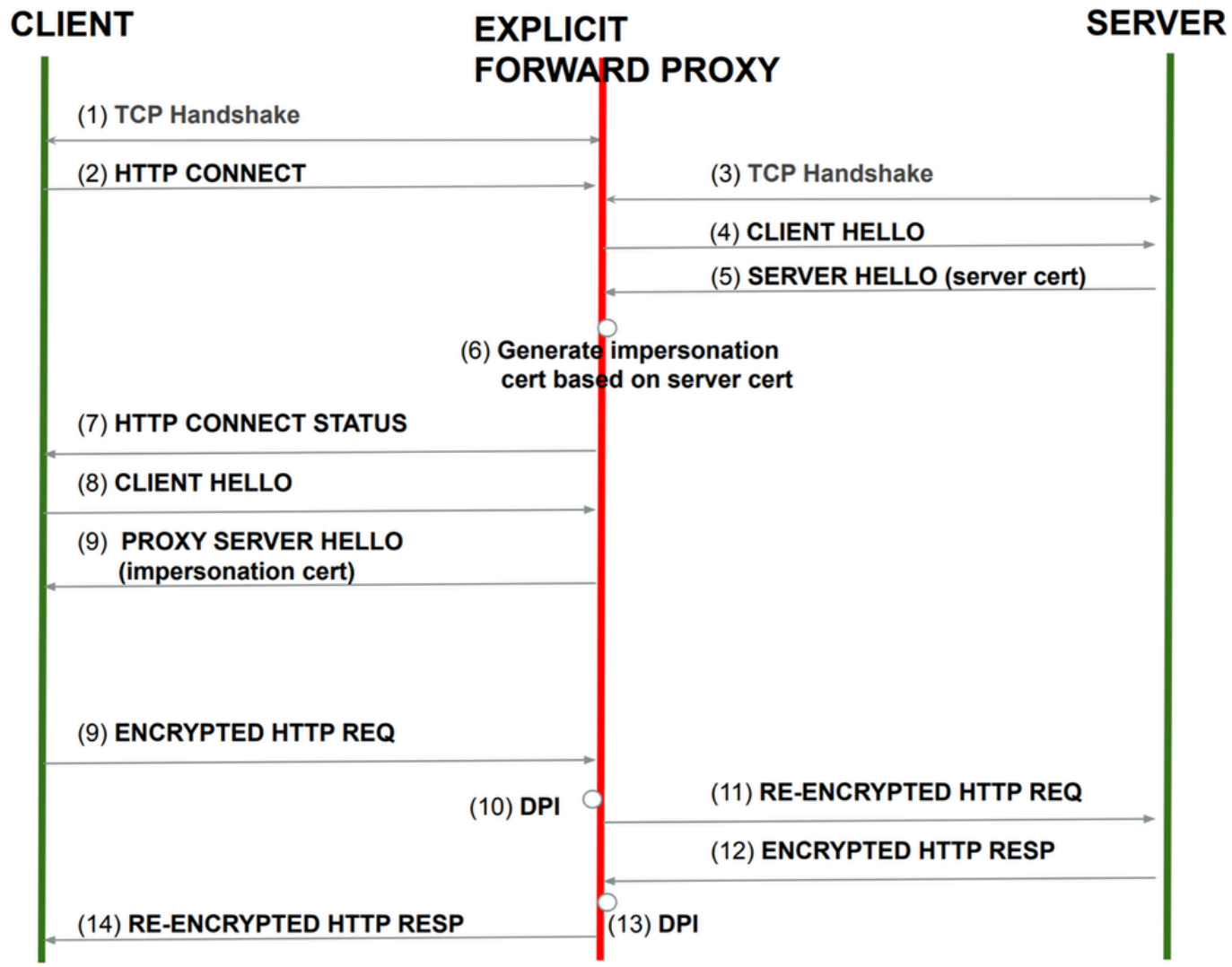
[4]トラフィックが許可されている場合、ゲートウェイはサーバへの新しいTCPハンドシェイク要求を開始し、HTTP CONNECTを転送します。

[5] HTTP STATUS応答メッセージがクライアントに透過的に転送されます。

[6]この時点以降、すべてのメッセージは傍受されることなく直接送信されます

Explicit Forward Proxy (with decryption)(明示的転送プロキシ（復号化付き）)

トラフィックを復号化するように明示的な転送プロキシが設定されている間のトラフィックフローを次に示します。



イメージ：Explicit Forward Proxy（復号あり）

[1]クライアントとマルチクラウドゲートウェイ間でTCP 3ウェイハンドシェイクが開始されます。

[2]ハンドシェイクが完了すると、クライアントはHTTP CONNECTを送信します。

[3] CONNECTヘッダーから、マルチクラウドゲートウェイはFQDNを識別し、FQDNフィルタリングポリシーを適用します。

[4]マルチクラウドゲートウェイは、サーバとのTCPハンドシェイクを開始します。

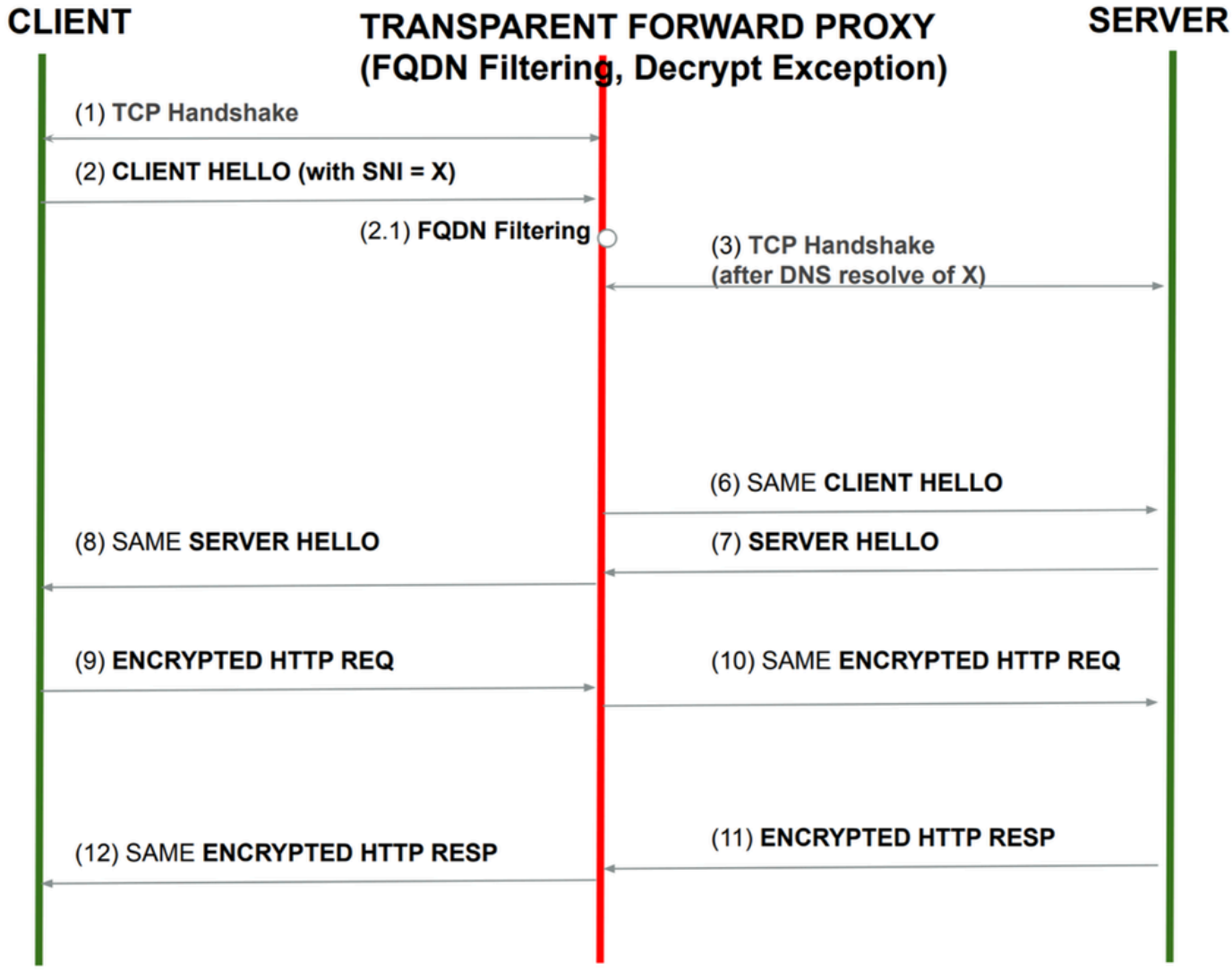
[5]マルチクラウドゲートウェイとサーバ間のTLSハンドシェイクが正常に完了した後、マルチクラウドゲートウェイはクライアントとマルチクラウドゲートウェイ間の復号化されたトラフィックに対して証明書を発行しました。

[6]この時点以降、クライアントとサーバ間のすべてのトラフィックが再度復号化され、暗号化されます。

透過的な転送プロキシ

透過的な転送プロキシ（復号化を除く）

後続のシナリオでは、トラフィックがパブリックサーバをターゲットとし、ゲートウェイに復号化例外を伴う転送プロキシの設定がある場合のプロセスの概要を説明します。



イメージ：Transparent Forward Proxy（復号化例外あり）

[1]マルチクラウドゲートウェイがTCPハンドシェイクに応答します。

[2]クライアントはサーバにCLIENT HELLOを送信します。このCLIENT HELLOには、Server Name Identifier（SNI；サーバ名識別子）が含まれています。ゲートウェイはこのパケットをインターセプトし、FQDNフィルタリングポリシーを実行します。

[3]トラフィックが許可され、URLに対して復号化例外が設定されている場合、マルチクラウドゲートウェイはSNIに対して別のDNS解決を実行します。

[4]マルチクラウドゲートウェイは、サーバへのTCPハンドシェイクを開始します。

[5]マルチクラウドゲートウェイは、クライアントから受信した同じCLIENT HELLOをサーバに転送します。

[6]サーバから受信したSERVER HELLOは、変更なしでそのまま転送されます。

[7]この時点以降、すべてのパケットは何のアクションもなしに現状のまま送信されます

透過的な転送プロキシ（復号化あり）

後続のシナリオでは、トラフィックがパブリックサーバをターゲットとし、ゲートウェイが転送プロキシでトラフィックを復号化する設定になっている場合のプロセスの概要を説明します。

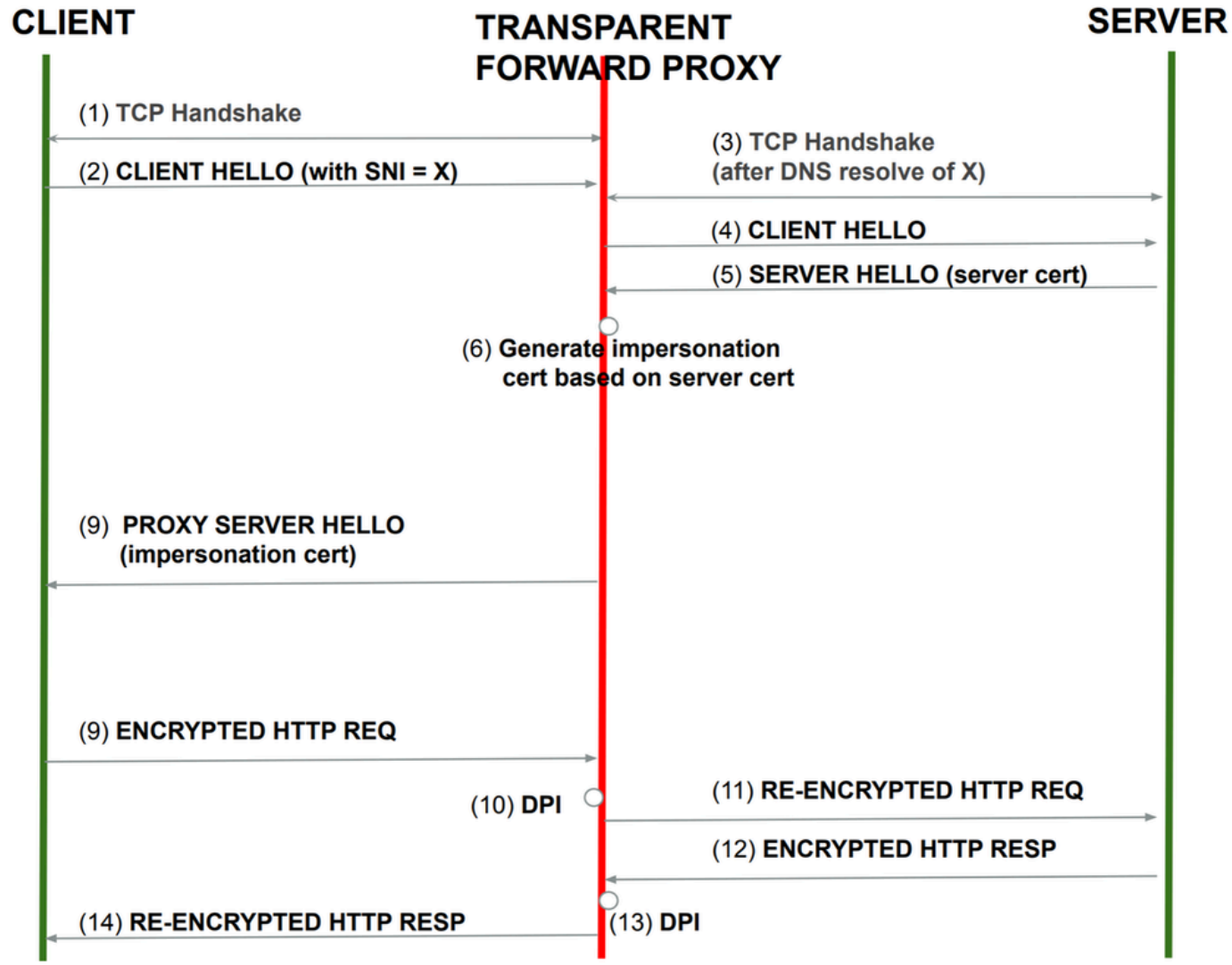


図 – Transparent Forward Proxy (with decryption)

[1]マルチクラウドゲートウェイがTCPハンドシェイクに応答する。

[2]クライアントはサーバにCLIENT HELLOを送信します。このCLIENT HELLOには、Server Name Identifier（SNI；サーバ名識別子）が含まれています。ゲートウェイはこのパケットをインターセプトし、FQDNフィルタリングポリシーを実行します。

[3]トラフィックが許可され、URLの復号化が設定されている場合、マルチクラウドゲートウェイはSNIに対して別のDNS解決を実行します。

[4]マルチクラウドゲートウェイが、サーバへのTCPハンドシェイクを開始します。

[5]マルチクラウドゲートウェイとサーバ間のTLSハンドシェイクが正常に完了した後、マルチクラウドゲートウェイはクライアントとマルチクラウドゲートウェイ間の復号化されたトラフィッ

クに対して証明書を発行しました。

[6]この時点以降、クライアントとサーバ間のすべてのトラフィックが再度復号化され、暗号化されます。

関連情報

- Cisco Multicloud Defenseユーザガイド – FQDNフィルタプロファイル[Cisco Defense Orchestrator] – シスコ
- Cisco Multicloud Defenseユーザガイド – ゲートウェイの管理[Cisco Defense Orchestrator] – シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。