Informazioni sul flusso del traffico HTTPS del proxy gateway di difesa multicolore

Sommario

Introduzione

In questo documento viene descritto come Cisco Multicast Defense Gateway gestisce il traffico HTTPS quando viene configurata l'azione proxy inoltra o inversa.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del cloud computing
- Conoscenze base delle reti di computer

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

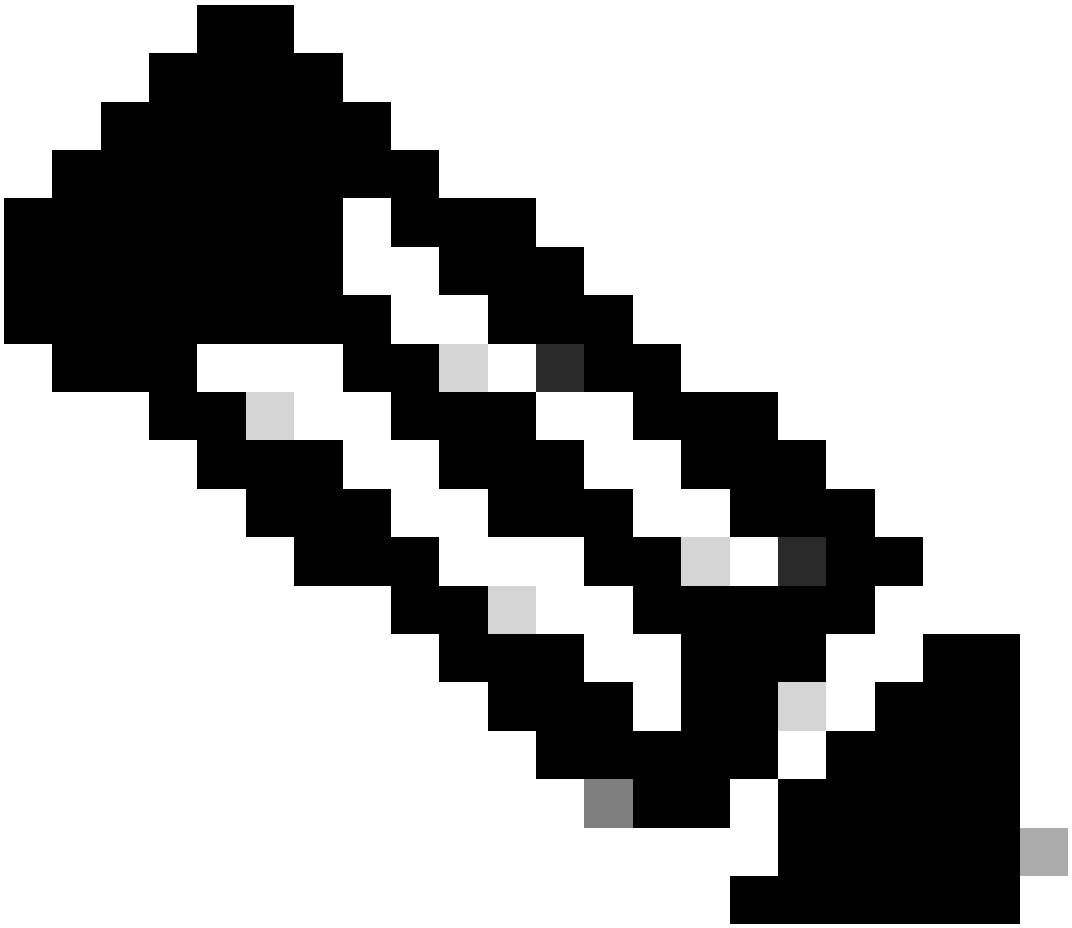
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Proxy di inoltro esplicito

Proxy di inoltro esplicito indica che le impostazioni di rete del computer sono configurate per l'utilizzo esplicito del proxy. Il traffico proveniente dal client è destinato al server proxy che lo esamina prima di inoltrarlo alla destinazione effettiva.

Proxy di inoltro esplicito (con eccezione di decrittografia)

Questo diagramma mostra il flusso di rete quando il gateway Multicast viene posizionato nel percorso tra il client e il server Web e il gateway Multicast è configurato per fungere da proxy di inoltro con eccezione di decrittografia.



Nota: le eccezioni di decrittografia si riferiscono a scenari in cui si preferisce che Multicoud Gateway non decrittografi e non ispezioni il traffico, spesso applicabili ai siti Web di finanza, sanità e governativi. In questi casi, è possibile attivare le eccezioni di decrittografia per FQDN specifici.

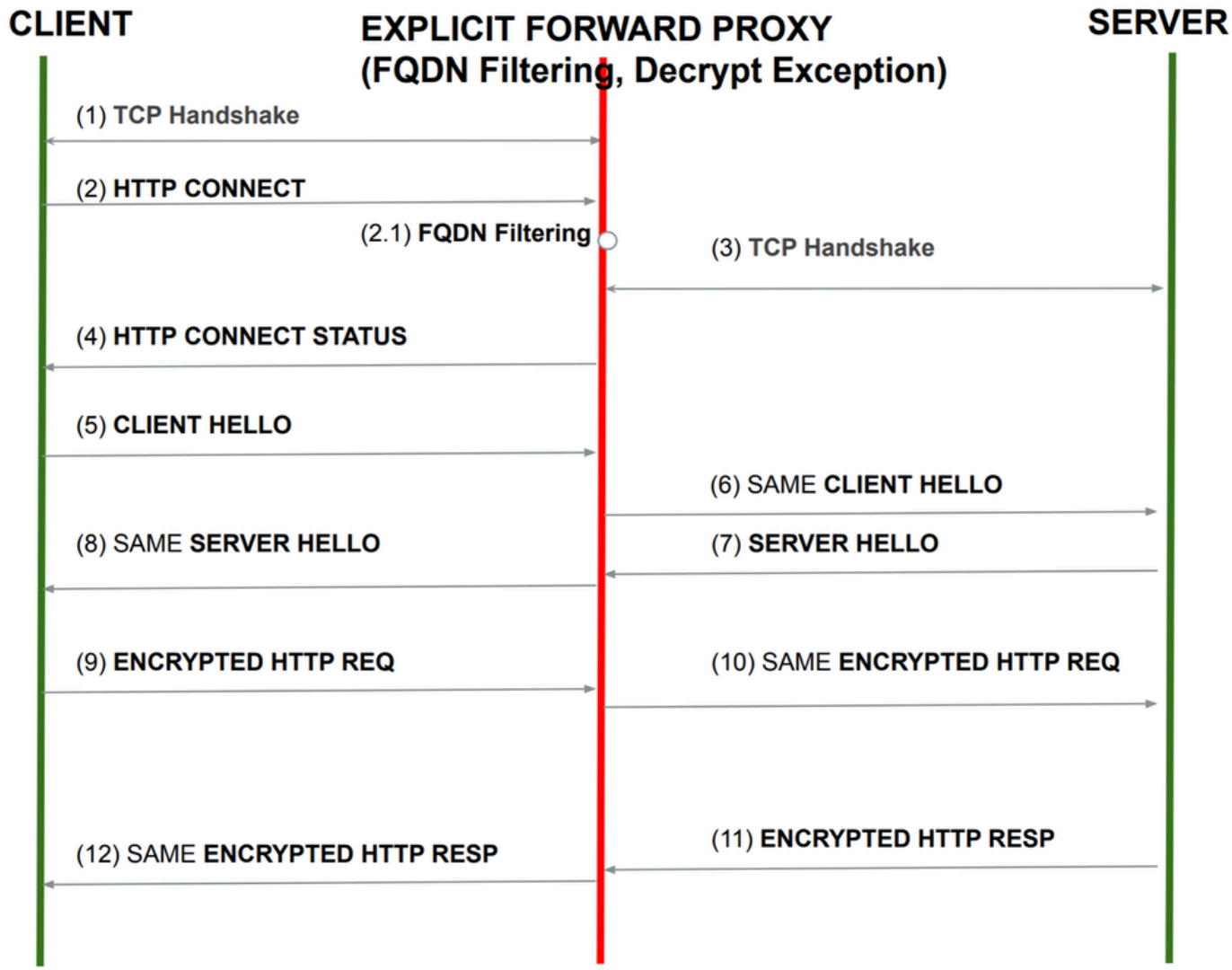


Immagine - Flusso proxy di inoltro esplicito (con eccezione di decrittografia)

[1] L'handshake a 3 vie TCP viene avviato tra il client e il gateway Multicast.

[2] Una volta completato l'handshake, il client invia HTTP CONNECT.

[3] Dall'intestazione CONNECT, il gateway multicast identifica l'FQDN e applica i criteri di filtro FQDN.

[4] Se il traffico è consentito, il gateway avvia una nuova richiesta di handshake TCP al server e inoltra HTTP CONNECT.

[5] Il messaggio di risposta HTTP STATUS viene inoltrato in modo trasparente al client.

[6] Da questo momento in poi tutti i messaggi sono inviati direttamente senza alcuna intercettazione

Proxy di inoltro esplicito (con decrittografia)

Questo è il flusso del traffico, mentre il proxy di inoltro esplicito è configurato per decrittografare il traffico.

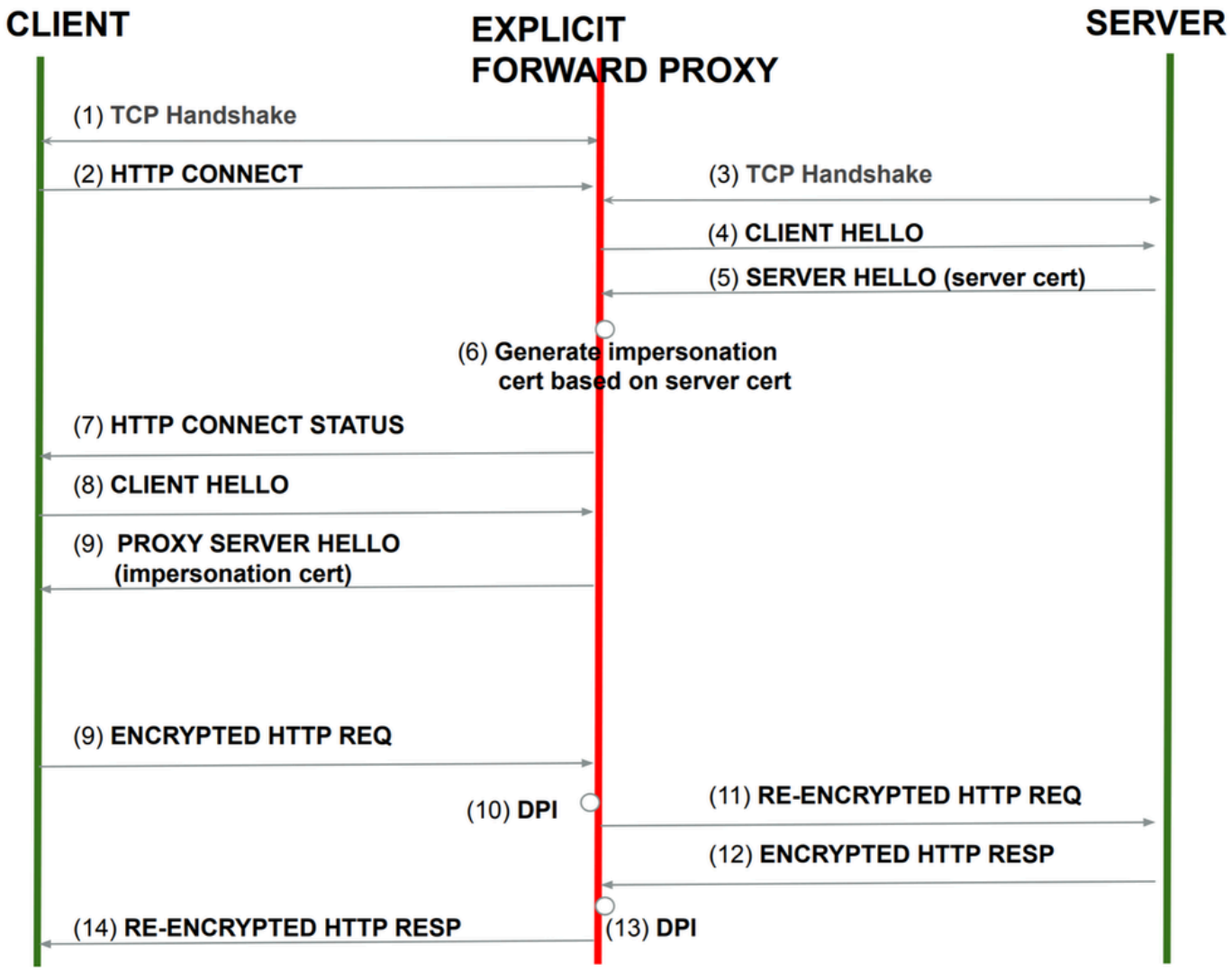


Immagine - Proxy di inoltro esplicito (con decrittografia)

[1] L'handshake a 3 vie TCP viene avviato tra il client e il gateway Multicast.

[2] Una volta completato l'handshake, il client invia HTTP CONNECT.

[3] Dall'intestazione CONNECT, Multicast Gateway identifica l'FQDN e applica i criteri di filtro FQDN.

[4] Gateway multicast avvia l'handshake TCP con il server.

[5] Dopo il completamento dell'handshake TLS tra il gateway multicast e il server, il gateway multicast ha emesso un certificato per il traffico decrittografato tra il client e il gateway multicast.

[6] Da questo punto in avanti, tutto il traffico tra il client e il server viene decriptato e criptato di nuovo.

Proxy di inoltro trasparente

Proxy di inoltro trasparente (con eccezione di decrittografia)

Nello scenario successivo viene descritto il processo in cui il traffico è indirizzato a un server pubblico e il gateway dispone di una configurazione per il proxy di inoltro con un'eccezione di decrittografia.

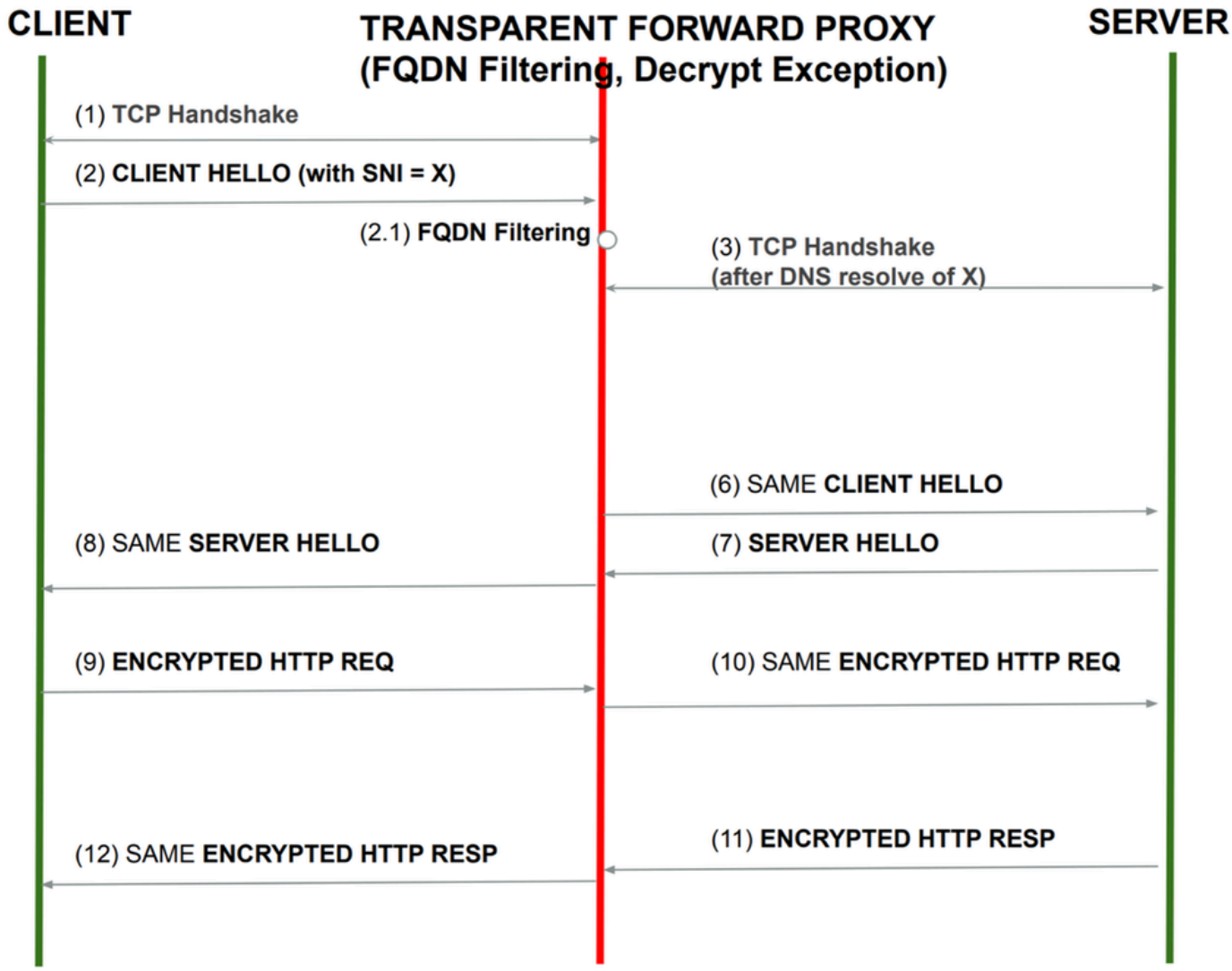


Immagine - Proxy di inoltro trasparente (con eccezione decrittografia)

[1] Il gateway multicast risponde all'handshake TCP.

[2] Il client invia un HELLO CLIENT al server. Questo HELLO CLIENT contiene l'identificatore del nome del server (SNI, Server Name Identifier). Il gateway intercetta il pacchetto ed esegue i criteri di filtro FQDN.

[3] Se il traffico è consentito e l'eccezione di decrittografia è configurata per l'URL, il gateway Multicast esegue un'altra risoluzione DNS per l'SNI.

[4] Gateway multicast avvia un handshake TCP al server.

[5] Multicast Gateway inoltra lo stesso HELLO CLIENT al server (ricevuto dal client).

[6] Il SERVER HELLO ricevuto dal server viene inoltrato così com'è senza alcuna modifica.

[7] Da questo momento in poi tutti i pacchetti vengono inviati così come sono senza alcuna azione

Proxy di inoltro trasparente (con decrittografia)

Nello scenario successivo viene descritto il processo in cui il traffico è indirizzato a un server pubblico e il gateway dispone di una configurazione per la decrittografia del traffico da parte del proxy di inoltro.

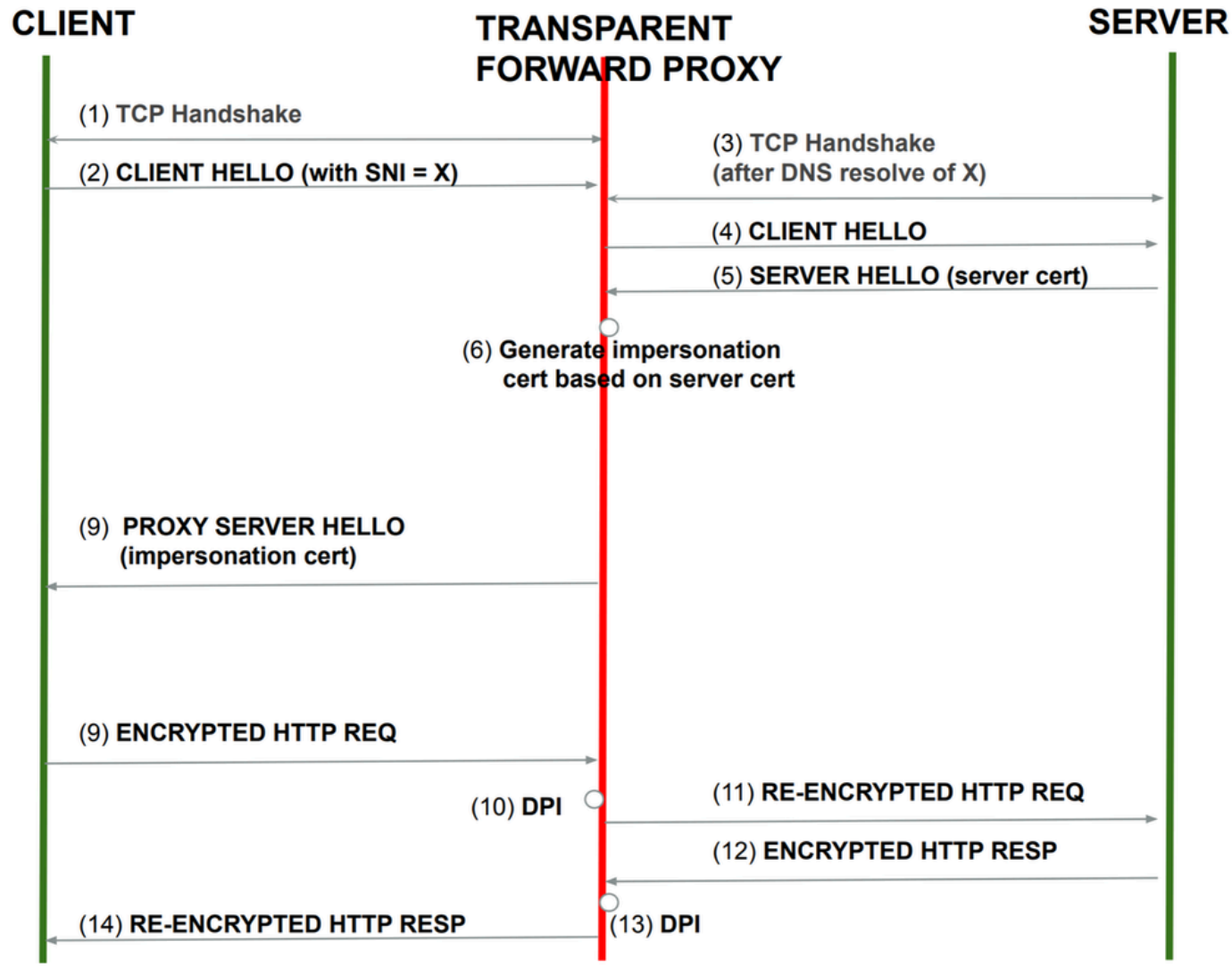


Immagine - Il proxy di inoltro trasparente (con decrittografia)

[1] Il gateway multicolore risponde all'handshake TCP.

[2] Il client invia un HELLO CLIENT al server. Questo HELLO CLIENT contiene l'identificatore del nome del server (SNI, Server Name Identifier). Il gateway intercetta il pacchetto ed esegue i criteri di filtro FQDN.

[3] Se il traffico è consentito e la decrittografia è configurata per l'URL, il gateway Multicast esegue un'altra risoluzione DNS per l'SNI.

[4] Multicast Gateway avvia l'handshake TCP al server.

[5] Dopo il completamento dell'handshake TLS tra il gateway multicast e il server, il gateway multicast ha emesso un certificato per il traffico decrittografato tra il client e il gateway multicast.

[6] Da questo punto in avanti, tutto il traffico tra il client e il server viene decriptato e criptato di nuovo.

Informazioni correlate

- Guida per l'utente di Cisco Multicast Defense - Profilo filtro FQDN [Cisco Defense Orchestrator] - Cisco
- Guida per l'utente di Cisco Multicast Defense - Gestisci gateway [Cisco Defense Orchestrator] - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).