Multicloud Defense Gateway Proxy HTTPS 트래픽 흐름 이해

목차

소개

이 문서에서는 전달 또는 역방향 프록시 작업이 구성된 경우 Cisco Multicholoud Defense Gateway에서 HTTPS 트래픽을 처리하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 클라우드 컴퓨팅에 대한 기본 지식
- 컴퓨터 네트워크에 대한 기본 지식

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

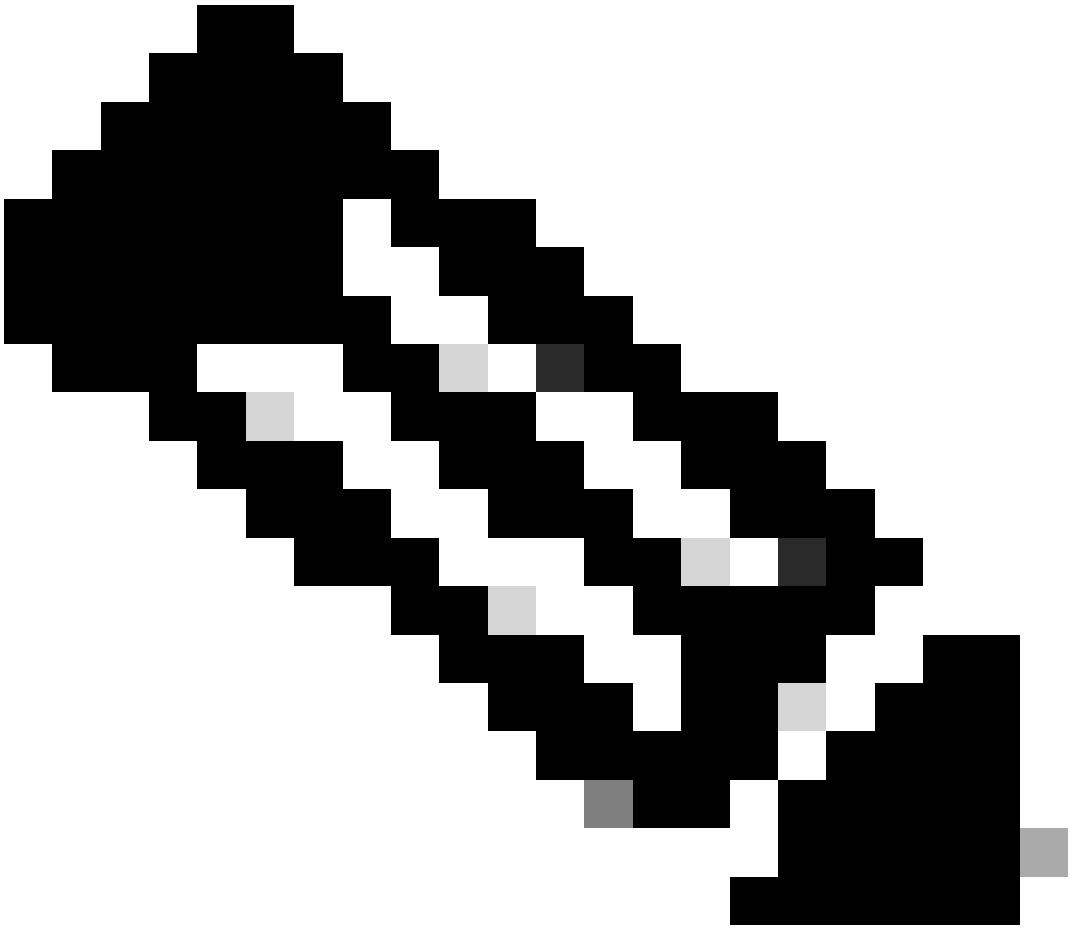
명시적 전달 프록시

명시적 전달 프록시는 컴퓨터 네트워크 설정이 프록시를 명시적으로 사용하도록 구성되어 있음을

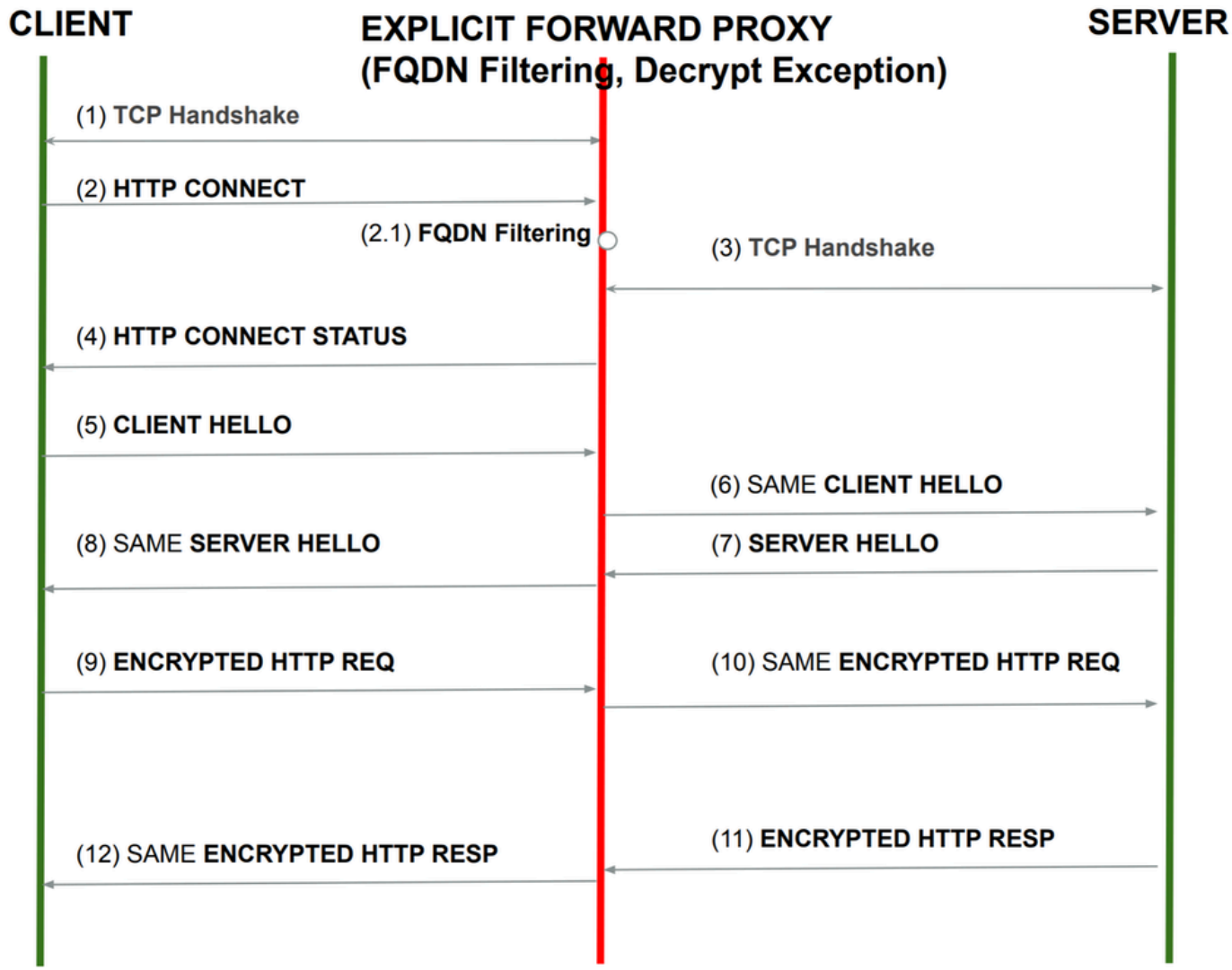
의미합니다. 클라이언트에서 오는 트래픽은 프록시 서버로 전달되며, 프록시 서버는 트래픽을 실제 대상으로 전달하기 전에 이를 검사합니다.

명시적 전달 프록시(암호 해독 예외 있음)

이 다이어그램은 멀티클라우드 게이트웨이가 클라이언트와 웹 서버 사이의 경로에 배치되고 멀티클라우드 게이트웨이가 암호 해독 예외가 있는 포워드 프록시 역할을 하도록 구성된 경우의 네트워크 흐름을 보여줍니다.



참고: 해독 예외는 트래픽을 해독 및 검사하지 않고 Multicloud Gateway를 선호하는 시나리오를 말하며, 금융, 의료 및 정부 웹 사이트에 종종 적용됩니다. 이러한 경우 특정 FQDN에 대한 해독 예외를 활성화합니다.



이미지 - 명시적 전달 프록시(암호 해독 예외 있음) 흐름

[1] TCP 3-way 핸드셰이크가 클라이언트와 Multicholoud 게이트웨이 사이에서 시작됩니다.

[2] 핸드셰이크가 완료되면 클라이언트는 HTTP CONNECT를 전송합니다.

[3] CONNECT 헤더에서 멀티클라우드 게이트웨이는 FQDN을 식별하고 FQDN 필터링 정책을 적용합니다.

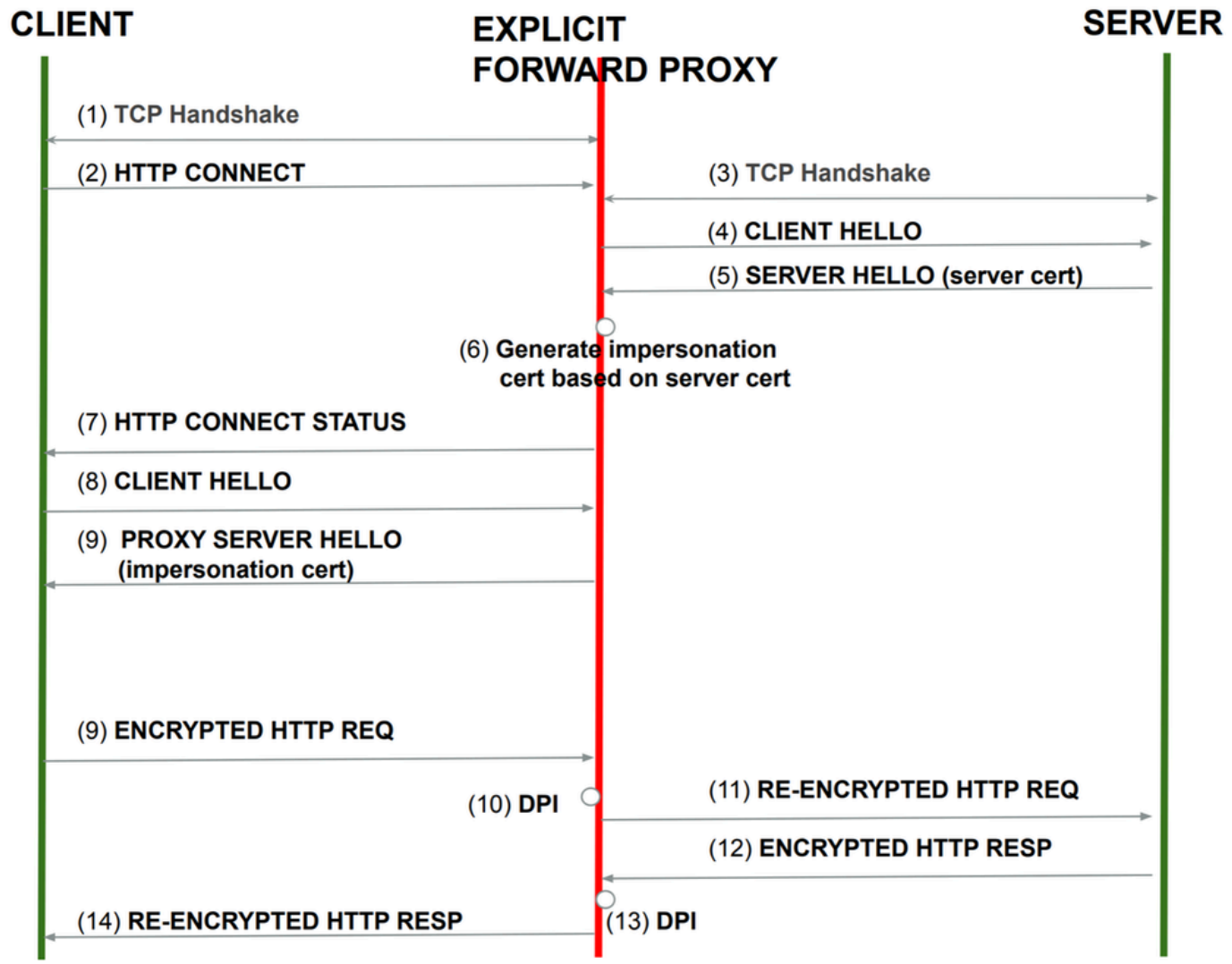
[4] 트래픽이 허용되면 게이트웨이는 서버에 새 TCP 핸드셰이크 요청을 시작하고 HTTP CONNECT를 전달합니다.

[5] HTTP STATUS 응답 메시지는 클라이언트에 투명하게 전달됩니다.

[6] 이 시점부터 모든 메시지는 인터셉션 없이 직접 전송됩니다

명시적 전달 프록시(암호 해독 포함)

다음은 트래픽 흐름이며, 명시적 전달 프록시가 트래픽을 해독하도록 구성되어 있습니다.



이미지 - 명시적 전달 프록시(암호 해독 포함)

[1] TCP 3-way 핸드셰이크가 클라이언트와 Multicholoud 게이트웨이 사이에서 시작됩니다.

[2] 핸드셰이크가 완료되면 클라이언트는 HTTP CONNECT를 전송합니다.

[3] CONNECT 헤더에서 멀티클라우드 게이트웨이는 FQDN을 식별하고 FQDN 필터링 정책을 적용합니다.

[4] Multicloud Gateway가 서버와의 TCP 핸드셰이크를 시작합니다.

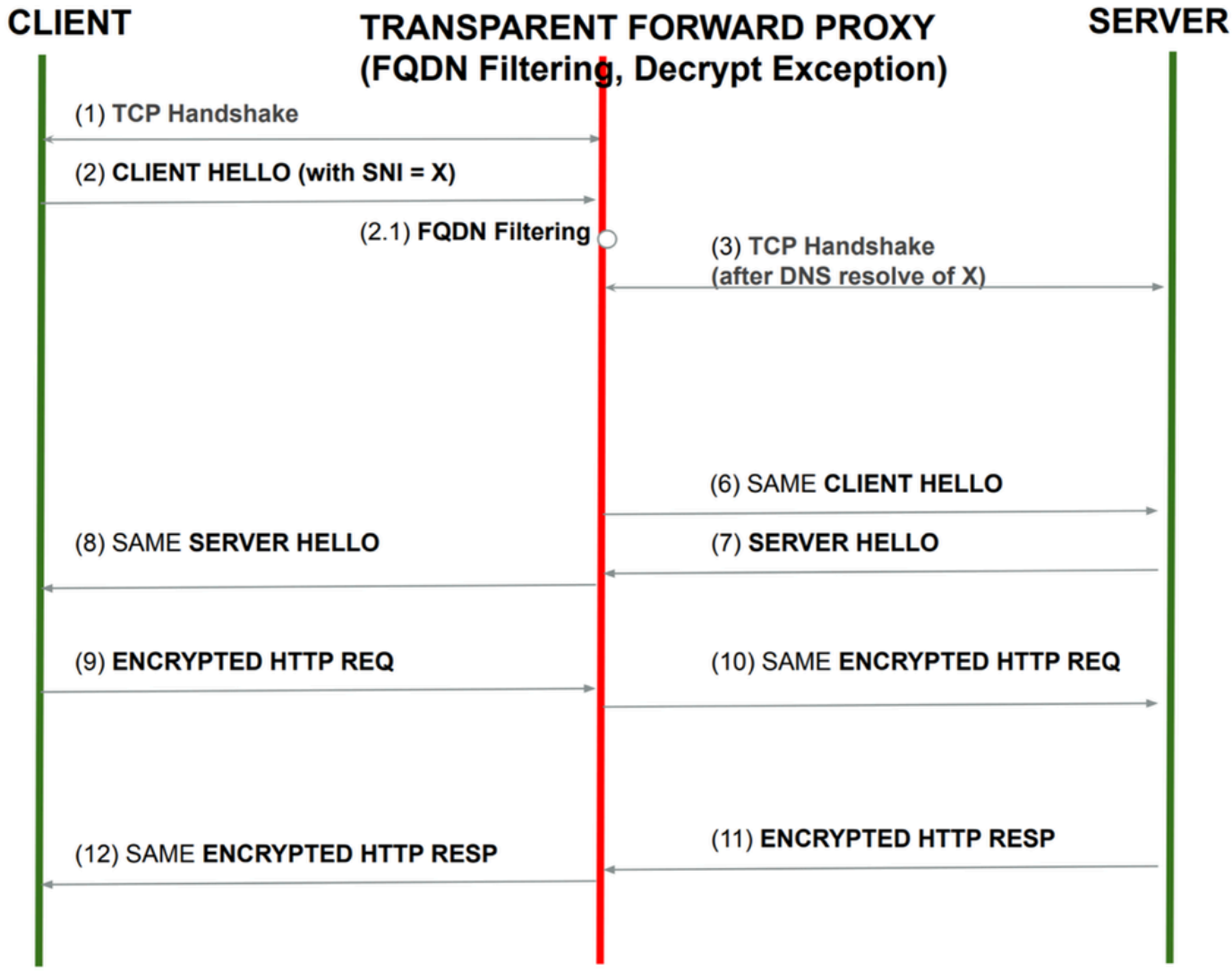
[5] TLS 핸드셰이크가 멀티클라우드 게이트웨이와 서버 간에 성공적으로 완료된 후, 멀티클라우드 게이트웨이는 클라이언트와 멀티클라우드 게이트웨이 간에 해독된 트래픽에 대한 인증서를 발급했습니다.

[6] 이 시점부터 클라이언트와 서버 간의 모든 트래픽이 다시 암호 해독되고 암호화됩니다.

투명 전달 프록시

투명 전달 프록시(암호 해독 예외 있음)

후속 시나리오에서는 트래픽이 공용 서버를 대상으로 하고 게이트웨이가 암호 해독 예외가 있는 전달 프록시에 대한 컨피그레이션을 갖는 경우의 프로세스를 간략하게 설명합니다.



이미지 - 투명 전달 프록시(암호 해독 예외 있음)

[1] 멀티 클라우드 게이트웨이는 TCP 핸드셰이크에 응답합니다.

[2] 클라이언트가 서버에 클라이언트 HELLO를 보냅니다. 이 클라이언트 HELLO에는 SNI(Server Name Identifier)가 포함되어 있습니다. 게이트웨이가 이 패킷을 인터셉트하고 FQDN 필터링 정책을 수행합니다.

[3] 트래픽이 허용되고 URL에 대해 암호 해독 예외가 구성된 경우, 멀티 클라우드 게이트웨이는 SNI에 대해 또 다른 DNS 확인을 수행합니다.

[4] 멀티 클라우드 게이트웨이가 서버에 대한 TCP 핸드셰이크를 시작합니다.

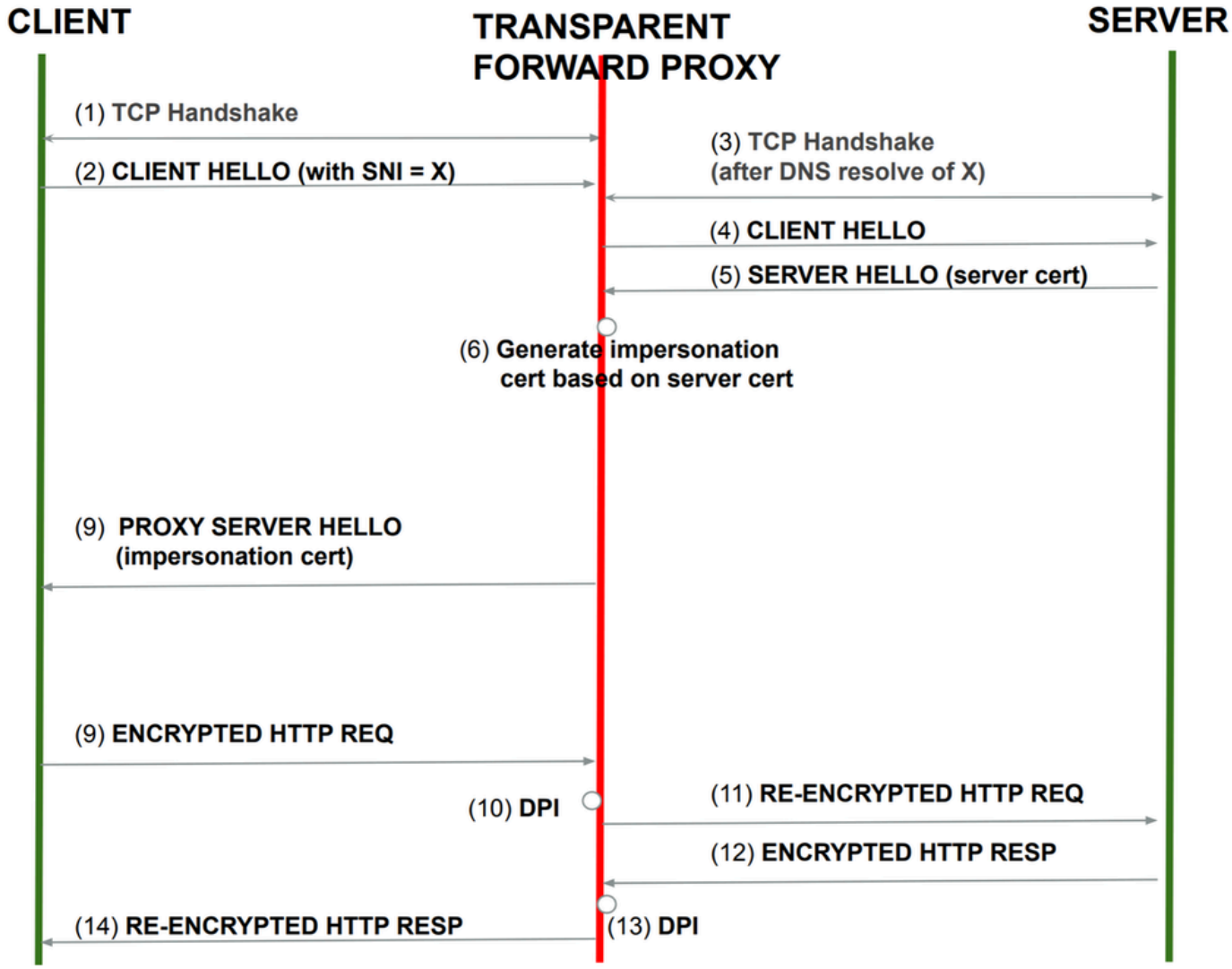
[5] 멀티 클라우드 게이트웨이는 클라이언트에서 받은 것과 동일한 클라이언트 HELLO를 서버에 전달합니다.

[6] 서버에서 받은 SERVER HELLO는 수정 없이 그대로 전달됩니다.

[7] 이 시점부터 모든 패킷이 아무런 작업 없이 그대로 전송됩니다

투명 전달 프록시(암호 해독 포함)

후속 시나리오에서는 트래픽이 공용 서버를 대상으로 하고 게이트웨이가 전달 프록시에서 트래픽을 해독하도록 구성한 경우의 프로세스를 간략하게 설명합니다.



이미지 - 투명 전달 프록시(암호 해독 포함)

[1] 멀티클라우드 게이트웨이가 TCP 핸드셰이크에 응답합니다.

[2] 클라이언트가 서버에 클라이언트 HELLO를 보냅니다. 이 클라이언트 HELLO에는 SNI(Server Name Identifier)가 포함되어 있습니다. 게이트웨이가 이 패킷을 인터셉트하고 FQDN 필터링 정책을 수행합니다.

[3] 트래픽이 허용되고 URL에 대해 암호 해독이 구성된 경우, Multicholoud 게이트웨이는 SNI에 대해 또 다른 DNS 확인을 수행합니다.

[4] 멀티클라우드 게이트웨이가 서버에 대한 TCP 핸드셰이크 시작을 시작합니다.

[5] TLS 핸드셰이크가 멀티클라우드 게이트웨이와 서버 간에 성공적으로 완료된 후, 멀티클라우드 게이트웨이는 클라이언트와 멀티클라우드 게이트웨이 간에 해독된 트래픽에 대한 인증서를 발급했습니다.

[6] 이 시점부터 클라이언트와 서버 간의 모든 트래픽이 다시 암호 해독되고 암호화됩니다.

관련 정보

- Cisco Multicoloud Defense 사용 설명서 - FQDN 필터 프로필 [Cisco Defense Orchestrator] - Cisco
- Cisco Multicholoud Defense 사용 설명서 - 게이트웨이 관리 [Cisco Defense Orchestrator] - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.