Secure Web Appliance의 패킷 흐름 이해

목차

소개

이 문서에서는 특히 SWA(Secure Web Appliance)에 초점을 맞춘 프록시 구성 네트워크의 네트워크 흐름에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 TCP/IP 개념
- 프록시 설정에 대한 기본 지식
- 프록시가 있는 환경에서 사용되는 인증 메커니즘에 대한 기본 지식

이 문서에는 다음과 같은 약어가 사용됩니다.

TCP: 전송 제어 프로토콜

UDP: 사용자 데이터그램 프로토콜

IP: 인터넷 프로토콜

GRE: 일반 라우팅 캡슐화

HTTP: 하이퍼텍스트 전송 프로토콜.

HTTPS: Hypertext Transfer Protocol Secure입니다.

URL: Uniform Resource Locator

TLS: 전송 계층 보안

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.

프록시 구축의 다른 유형

TLS 핸드셰이크

HTTPS의 TLS 핸드셰이크는 클라이언트와 서버가 인터넷을 통해 통신하면서 안전한 연결을 제공할 때 발생합니다. 이 프로세스는 두 통신 애플리케이션 간의 프라이버시 및 데이터 무결성을 유지합니다. 클라이언트와 서버가 모든 후속 전송에 대한 암호화 표준 및 코드에 동의하는 일련의 단계를 통해 작동합니다. 이 악수는 제3자에 의한 무단 접근이나 조작을 막는 것을 목적으로 한다. 또한 가장을 제거하기 위해 통신 당사자의 ID를 인증합니다. 이 프로세스는 HTTPS에서 데이터가 전송 중에 안전하게 유지되도록 하기 때문에 중요합니다.

다음은 TLS 핸드셰이크의 단계입니다.

1. Client Hello: 클라이언트가 hello 메시지로 핸드셰이크 프로세스를 시작합니다. 이 메시지에는 클라이언트 TLS 버전, 지원되는 암호 그룹 및 "클라이언트 임의"라는 임의 바이트 문자열이 포함되어 있습니다.

2. Server Hello: 서버가 hello 메시지로 응답합니다. 이 메시지에는 서버에서 선택한 TLS 버전, 선택한 암호 그룹, "서버 임의"로 알려진 임의 바이트 문자열 및 서버 디지털 인증서가 포함됩니다. 필요한 경우 서버는 상호 인증을 위해 클라이언트 디지털 인증서도 요청합니다.

3. 클라이언트가 서버 인증서를 확인: 클라이언트는 서버 디지털 인증서를 발급한 인증 기관에서 서버 디지털 인증서를 확인 합니다. 그러면 클라이언트가 합법적인 서버와 통신하게 됩니다.

4. Pre-master Secret: 클라이언트가 임의의 바이트 문자열("pre-master secret"이라고 함)을 전송하며, 이는 세션 키 생성에 기여합니다. 클라이언트는 서버 공개 키로 이 사전 마스터 암호를 암호화하므로 서버만 개인 키로 암호를 해독할 수 있습니다.

5. 마스터 보안: 클라이언트와 서버 모두 사전 마스터 보안 및 hello 메시지의 임의 바이트 문자열을 사용하여 동일한 "마스터 보안"을 독립적으로 계산합니다. 이 공유 암호는 세션 키를 생성하기 위한 기본입니다.

6. Client Finished(클라이언트 완료): 클라이언트가 세션 키로 암호화된 "Finished(완료)" 메시지를 보내 핸드셰이크의 클라이언트 부분이 완료되었음을 알립니다.

7. Server Finished(서버 완료): 서버가 핸드셰이크의 서버 부분이 완료되었음을 알리기 위해 세션 키로 암호화된 "Finished(완료)" 메시지를 보냅니다.

HTTP 응답 코드

1xx: 정보

코드	세부사항
100 계속	일반적으로 ICAP 프로토콜과 관련하여 표시됩니다. 이 메시지는 클라이언트에서 데이터를 계속 전송할 수 있음을 알리는 정보 응답입니다. ICAP 서비스(예: 바이러스 검사)와 관련하여 서버는 처음 x바이트의 양만 볼 수 있습니다. 첫 번째 바이트 집합 검사가 완료되었지만 바이러스를 탐지하지 못한 경우 100 Continue(계속)를 전송하여 클라이언트에서 나머지 개체를 전송할 것을 알립니다.

2xx: 성공

코드	세부사항
200개	가장 일반적인 응답 코드입니다. 이는 요청이 문제 없이 성공했음을 의미합니다.

3xx: 리디렉션

코드	세부사항

301 영구 리디렉션	영구 리디렉션입니다. www 하위 도메인으로 리디렉션하는 경우 이 코드를 볼 수 있습니다.
302 임시 리디렉션	이는 임시 리디렉션입니다. 클라이언트는 Location: 헤더에 지정된 객체에 대해 새 요청을 하도록 지시받습니다.
304 수정되지 않음	이는 GIMS(GET If-modified-since)에 대한 응답입니다. 이것은 문자 그대로 표준 HTTP GET이며 헤더 If-modified-since: <date>를 포함합니다. 이 헤더는 클라이언트에 로컬 캐시에 요청된 객체의 복사본이 있으며 객체를 가져온 날짜가 포함되었음을 서버에 알립니다. 해당 날짜 이후에 객체가 수정된 경우 서버는 200 OK 및 객체의 새 복사본으로 응답합니다. 가져온 날짜 이후 객체가 변경되지 않은 경우 서버는 304 Not Modified 응답을 다시 보냅니다.
307 인증 리디렉션	이는 대부분 투명 프록시 배포에서 프록시 서버가 요청을 인증하도록 구성되어 있고 다른 URL로 요청을 리디렉션하여 사용자를 인증하면 나타납니다.

4xx 코드: 클라이언트 오류

코드	세부사항
400 잘못된 요청	이는 HTTP 요청이 올바른 구문을 준수하지 않기 때문에 HTTP 요청에 문제가 있음을 나타냅니다. 한 줄에 여러 개의 헤더가 있거나, 헤더 내의 공백이 있거나, URI에 HTTP/1.1이 없는 것 등이 원인일 수 있습니다. 올바른 구문은 RFC 2616을 참조하십시오.
401 무단 웹 서버 인증 필요	요청한 객체에 액세스하려면 인증이 필요합니다. 401 코드는 대상 웹 서버와의 인증에 사용됩니다. SWA가 투명 모드에서 작동하고 프록시에서 인증이 활성화되면 어플라이언스가 OCS(origin content server)인 것처럼 표시되므로 클라이언트에 401을 반환합니다. 사용할 수 있는 인증 방법은 'www-authenticate:' HTTP 응답 헤더에 자세히 설명되어 있습니다. 그러면 서버가 NTLM, 기본 또는 기타 인증 형식을 요청하는지 여부를 클라이언트에 알립니다.
403 거부됨	클라이언트가 요청된 개체에 액세스할 수 없습니다. 여러 가지 이유로 인해 서버에서 개체 액세스를 거부할 수 있습니다. 일반적으로 서버는 HTTP 데이터 또는 HTML 응답 내에서 원인 설명을 제공합니다.
404 찾을 수 없음	요청한 개체가 서버에 없습니다.

407 프록시 인증 필요	이는 OCS가 아닌 프록시에 대한 인증용이라는 점을 제외하면 401과 동일합니다. 요청이 프록시에 명시적으로 전송된 경우에만 전송됩니다. 클라이언트가 프록시가 있는지 모르기 때문에 SWA가 투명 프록시로 구성된 동안에는 407을 클라이언트로 전송할 수 없습니다. 이 경우 클라이언트는 TCP 소켓을 FIN 또는 RST할 가능성이 높습니다.

5xx: 서버 오류

코드	세부사항
501 내부 서버 오류	일반 웹 서버 오류입니다.
502 불량 게이트웨이	게이트웨이 또는 프록시 역할을 하는 서버가 인바운드 서버로부터 잘못된 응답을 받을 때 발생합니다. 게이트웨이가 업스트림 또는 원천 서버로부터 부적절한 응답을 받았음을 알립니다.
503 서비스를 사용할 수 없음	서버가 현재 일시적인 오버로드 또는 예약된 유지 관리로 인해 요청을 처리할 수 없음을 나타냅니다. 서버가 일시적으로 작동하지 않지만 시간이 지나면 다시 사용할 수 있음을 의미합니다.
504 게이트웨이 시간 초과	클라이언트 또는 프록시가 웹 페이지를 로드하기 위해 액세스하거나 브라우저의 다른 요청을 수행하려고 시도한 웹 서버로부터 적시에 응답을 받지 못했음을 나타냅니다. 이는 업스트림 서버가 다운되었음을 시사하는 경우가 많습니다.

명시적 구축

....

인증이 없는 명시적 구축의 HTTP 트래픽

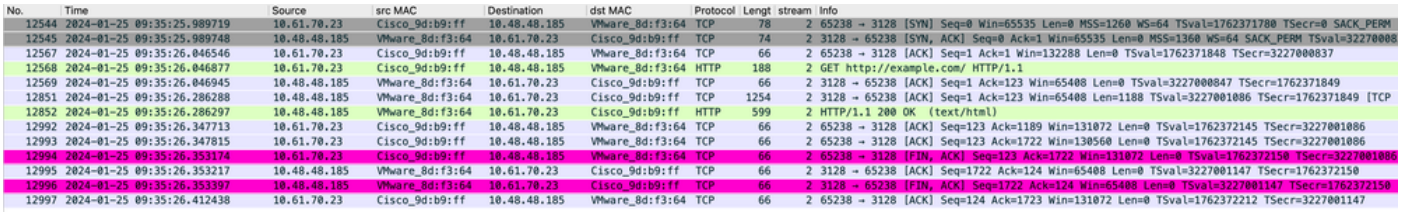
클라이언트 및 SWA

네트워크 트래픽은 클라이언트의 IP 주소와 SWA 프록시 인터페이스의 IP 주소 간에 전달됩니다(일반적으로 P1 인터페이스이지만 프록시 컨피그레이션에 따라 P2 또는 관리 인터페이스일 수 있음).

클라이언트에서 오는 트래픽은 TCP 포트 80 또는 3128에서 SWA로 전달됩니다(기본 SWA 프록시 포트는 TCP 80 및 3128이며, 이 예에서는 포트 3128을 사용합니다).

- TCP 핸드셰이크.

- 클라이언트에서 HTTP 가져오기(대상 IP = SWA IP, 대상 포트 = 3128)
- 프록시의 HTTP 응답(소스 IP = SWA)
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
12544	2024-01-25 09:35:25.989719	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	78	2	65238 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1762371780 TSecr=0 SACK_PERM
12545	2024-01-25 09:35:25.989748	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	74	2	3128 → 65238 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=64 SACK_PERM TSval=32270008
12567	2024-01-25 09:35:26.046546	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=1762371848 TSecr=3227000837
12568	2024-01-25 09:35:26.046877	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	188	2	GET http://example.com/ HTTP/1.1
12569	2024-01-25 09:35:26.046945	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [ACK] Seq=1 Ack=123 Win=65408 Len=0 TSval=3227000847 TSecr=1762371849
12851	2024-01-25 09:35:26.286288	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	1254	2	3128 → 65238 [ACK] Seq=1 Ack=123 Win=65408 Len=1188 TSval=3227001086 TSecr=1762371849 [TCP
12852	2024-01-25 09:35:26.286297	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	HTTP	599	2	HTTP/1.1 200 OK (text/html)
12992	2024-01-25 09:35:26.347713	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=123 Ack=1189 Win=131072 Len=0 TSval=1762372145 TSecr=3227001086
12993	2024-01-25 09:35:26.347815	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=123 Ack=1722 Win=130560 Len=0 TSval=1762372145 TSecr=3227001086
12994	2024-01-25 09:35:26.353174	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [FIN, ACK] Seq=123 Ack=1722 Win=131072 Len=0 TSval=1762372150 TSecr=3227001086
12995	2024-01-25 09:35:26.353217	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12996	2024-01-25 09:35:26.353397	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [FIN, ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12997	2024-01-25 09:35:26.412438	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=124 Ack=1723 Win=131072 Len=0 TSval=1762372212 TSecr=3227001147

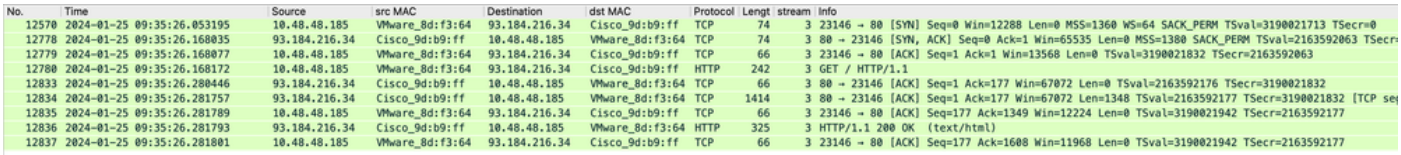
SWA, HTTP 명시적 모드에 대한 이미지 클라이언트

SWA 및 웹 서버

네트워크 트래픽은 프록시의 IP 주소와 웹 서버의 IP 주소 간에 발생합니다.

SWA의 트래픽은 TCP 포트 80으로 향하며 프록시 포트가 아닌 임의 포트를 통해 소싱됩니다

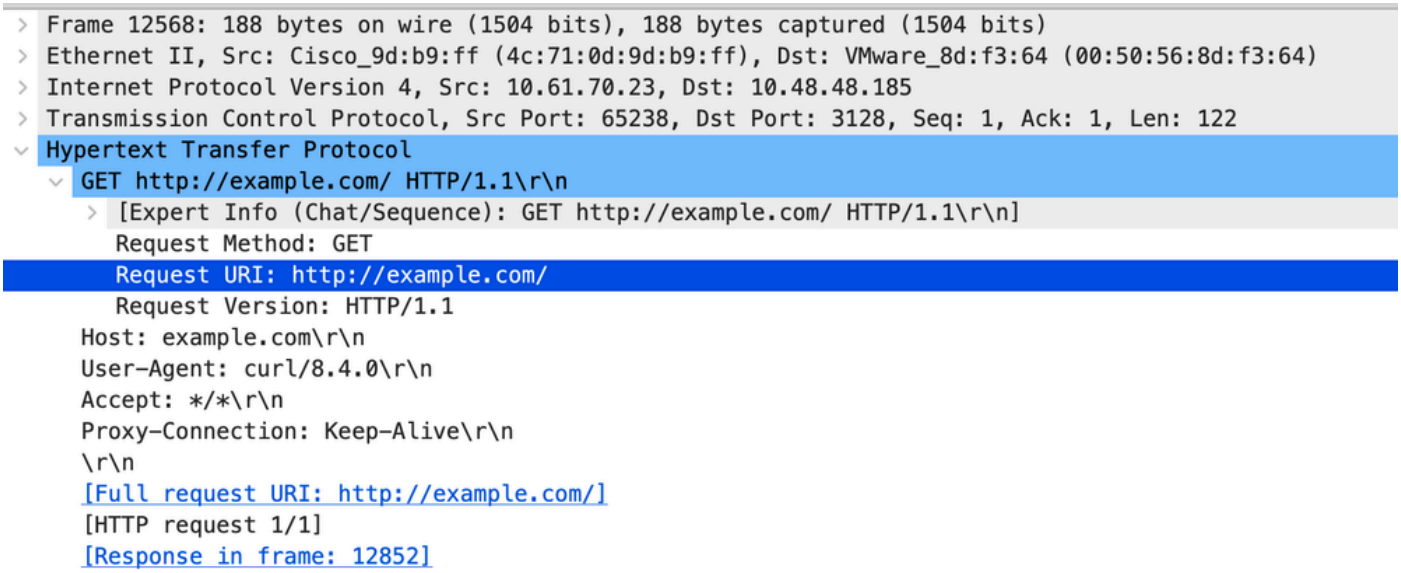
- TCP 핸드셰이크.
- 프록시에서 HTTP 가져오기(대상 IP = 웹 서버, 대상 포트 = 80)
- 웹 서버의 HTTP 응답(소스 IP = 프록시 서버)
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
12570	2024-01-25 09:35:26.053195	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	74	3	23146 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1360 WS=64 SACK_PERM TSval=3190021713 TSecr=0
12778	2024-01-25 09:35:26.168035	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	74	3	80 → 23146 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=2163592063 TSecr
12779	2024-01-25 09:35:26.168077	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=1 Ack=1 Win=13568 Len=0 TSval=3190021832 TSecr=2163592063
12780	2024-01-25 09:35:26.168172	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	HTTP	242	3	GET / HTTP/1.1
12833	2024-01-25 09:35:26.280446	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=0 TSval=2163592176 TSecr=3190021832
12834	2024-01-25 09:35:26.281757	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	1414	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=1348 TSval=2163592177 TSecr=3190021832 [TCP se
12835	2024-01-25 09:35:26.281789	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=177 Ack=1349 Win=12224 Len=0 TSval=3190021942 TSecr=2163592177
12836	2024-01-25 09:35:26.281793	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	325	3	HTTP/1.1 200 OK (text/html)
12837	2024-01-25 09:35:26.281801	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=177 Ack=1608 Win=11968 Len=0 TSval=3190021942 TSecr=2163592177

이미지 - HTTP-SWA-웹 서버-명시적-캐시 없음

다음은 Client에서 HTTP Get의 샘플입니다



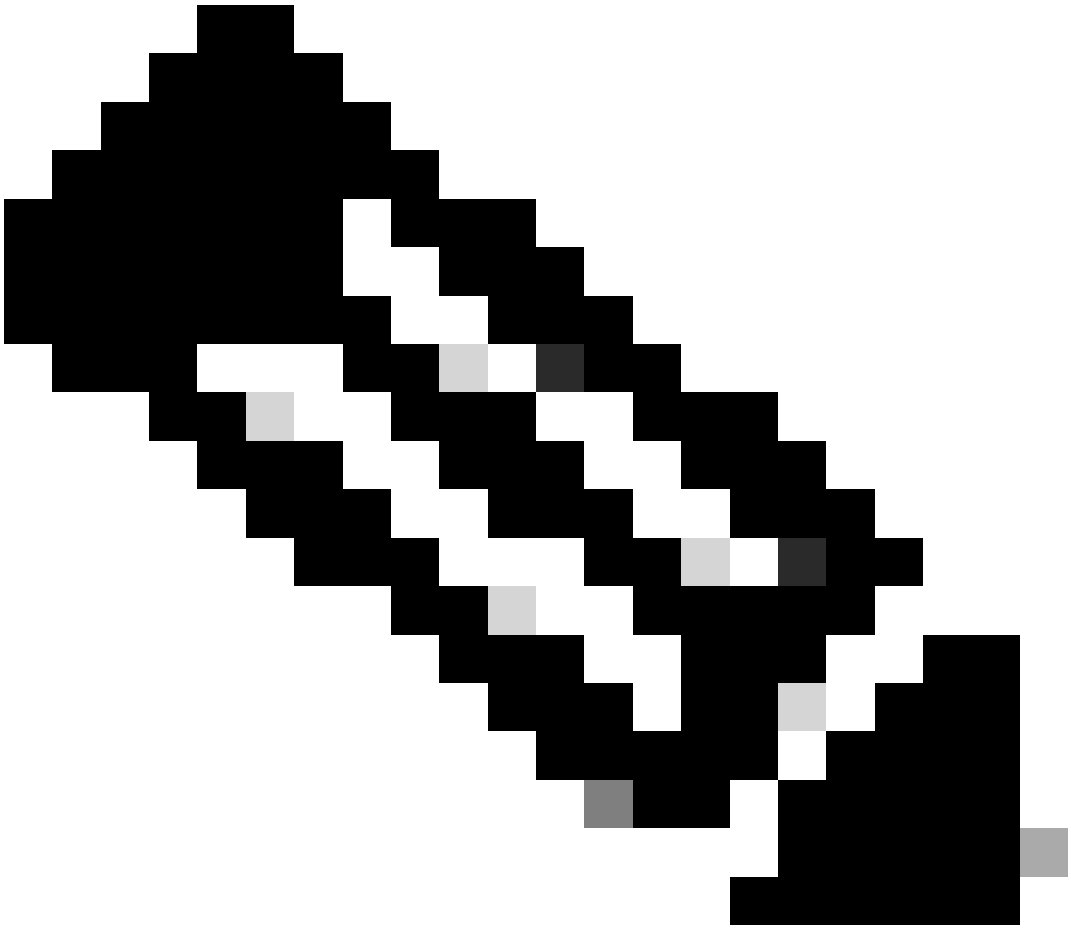
```
> Frame 12568: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:f3:64 (00:50:56:8d:f3:64)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.185
> Transmission Control Protocol, Src Port: 65238, Dst Port: 3128, Seq: 1, Ack: 1, Len: 122
v Hypertext Transfer Protocol
  v GET http://example.com/ HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET http://example.com/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: http://example.com/
      Request Version: HTTP/1.1
    Host: example.com\r\n
    User-Agent: curl/8.4.0\r\n
    Accept: */*\r\n
    Proxy-Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://example.com/]
    [HTTP request 1/1]
    [Response in frame: 12852]
```

이미지- 클라이언트에서 SWA HTTP GET- 명시적

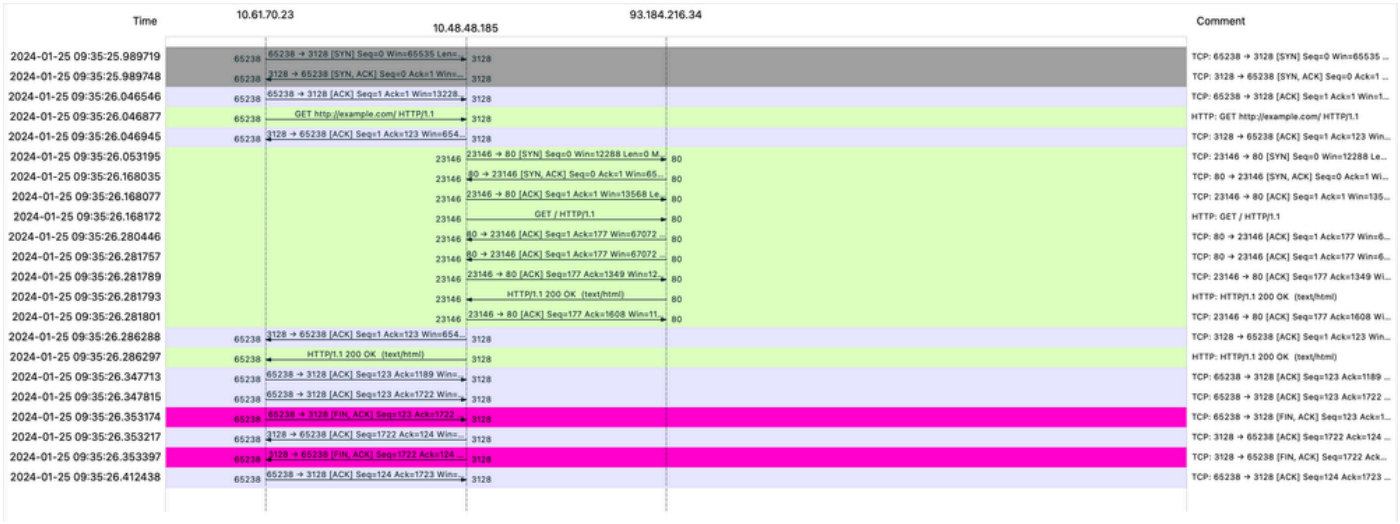
이는 클라이언트에서 SWA로, 웹 서버로, 마지막으로 클라이언트로 다시 이동하는 트래픽의 전체 흐름을 나타냅니다.

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
12544	2024-01-25 09:35:25.989719	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	78	2	65238 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1762371780 TSecr=0 SACK_PERM
12545	2024-01-25 09:35:25.989748	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	74	2	3128 → 65238 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=64 SACK_PERM TSval=322700083
12567	2024-01-25 09:35:26.046546	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=1762371848 TSecr=3227000837
12568	2024-01-25 09:35:26.046877	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	188	2	GET http://example.com/ HTTP/1.1
12569	2024-01-25 09:35:26.046945	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [ACK] Seq=1 Ack=123 Win=65408 Len=0 TSval=3227000847 TSecr=1762371849
12570	2024-01-25 09:35:26.053195	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	74	3	23146 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1360 WS=64 SACK_PERM TSval=3190021713 TSecr=0
12778	2024-01-25 09:35:26.168035	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	74	3	80 → 23146 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=2163592063 TSecr=
12779	2024-01-25 09:35:26.168077	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=1 Ack=1 Win=13568 Len=0 TSval=3190021832 TSecr=2163592063
12780	2024-01-25 09:35:26.168172	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	HTTP	242	3	GET / HTTP/1.1
12833	2024-01-25 09:35:26.280446	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=0 TSval=2163592176 TSecr=3190021832
12834	2024-01-25 09:35:26.281757	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	1414	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=1348 TSval=2163592177 TSecr=3190021832 [TCP seg
12835	2024-01-25 09:35:26.281789	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=177 Ack=1349 Win=12224 Len=0 TSval=3190021942 TSecr=2163592177
12836	2024-01-25 09:35:26.281793	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	325	3	HTTP/1.1 200 OK (text/html)
12837	2024-01-25 09:35:26.281801	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	23146 → 80 [ACK] Seq=177 Ack=1608 Win=11968 Len=0 TSval=3190021942 TSecr=2163592177
12851	2024-01-25 09:35:26.286288	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	1254	2	3128 → 65238 [ACK] Seq=1 Ack=123 Win=65408 Len=1188 TSval=3227001086 TSecr=1762371849 [TCP s
12852	2024-01-25 09:35:26.286297	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	HTTP	599	2	HTTP/1.1 200 OK (text/html)
12992	2024-01-25 09:35:26.347713	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=123 Ack=1189 Win=131072 Len=0 TSval=1762372145 TSecr=3227001086
12993	2024-01-25 09:35:26.347815	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=123 Ack=1722 Win=130560 Len=0 TSval=1762372145 TSecr=3227001086
12994	2024-01-25 09:35:26.353174	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [FIN, ACK] Seq=123 Ack=1722 Win=131072 Len=0 TSval=1762372150 TSecr=3227001086
12995	2024-01-25 09:35:26.353217	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12996	2024-01-25 09:35:26.353397	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 65238 [FIN, ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12997	2024-01-25 09:35:26.412438	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=124 Ack=1723 Win=131072 Len=0 TSval=1762372212 TSecr=3227001147

Image(이미지) - 모든 트래픽 HTTP Explicit-no cache



참고: 각 트래픽 스트림은 서로 다른 색상으로 구분됩니다. 클라이언트에서 SWA로의 흐름은 한 색상이고 SWA에서 웹 서버로의 흐름은 다른 색상입니다.



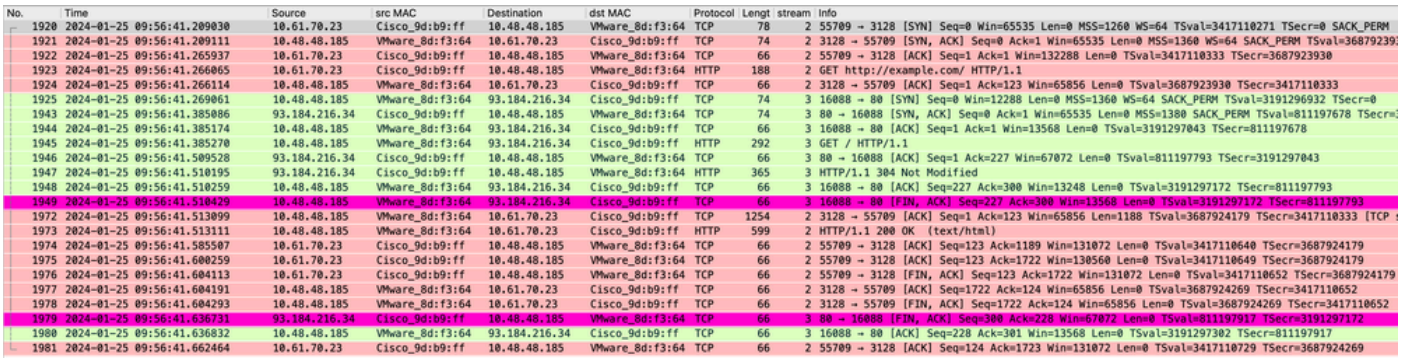
이미지 - 트래픽 흐름 HTTP Explicit - 캐시 없음

다음은 액세스 로그의 예입니다.

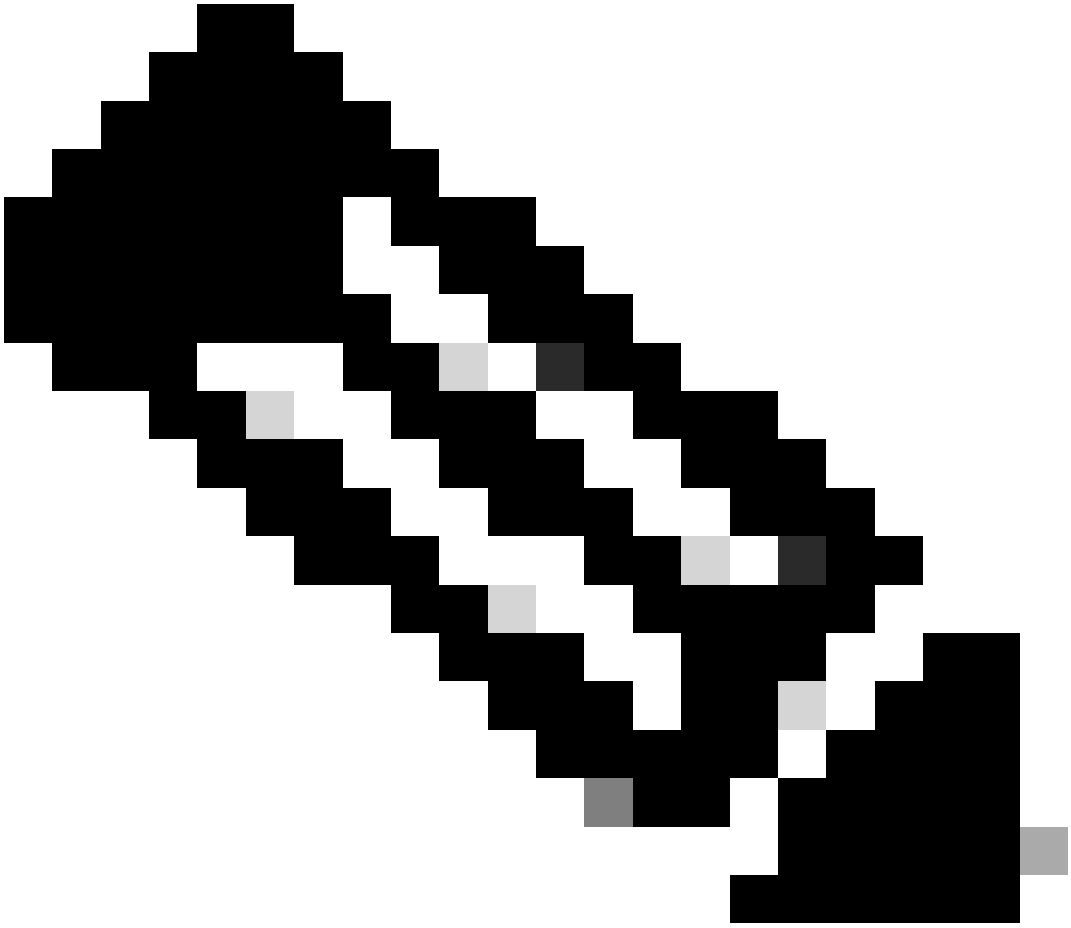
```
1706172876.686 224 10.61.70.23 TCP_MISS/200 1721 GET http://www.example.com/ - DIRECT/www.example.com t
```

캐시된 데이터가 있는 트래픽

데이터가 SWA 캐시에 있을 때 클라이언트에서 SWA로의 전체 트래픽 흐름을 나타냅니다.



이미지 - HTTP 명시적 캐시 데이터



참고: 웹 서버에서 HTTP 응답 304: Cache not Modified를 반환하는 것을 볼 수 있습니다. (이 예에서는 패킷 번호 1947)

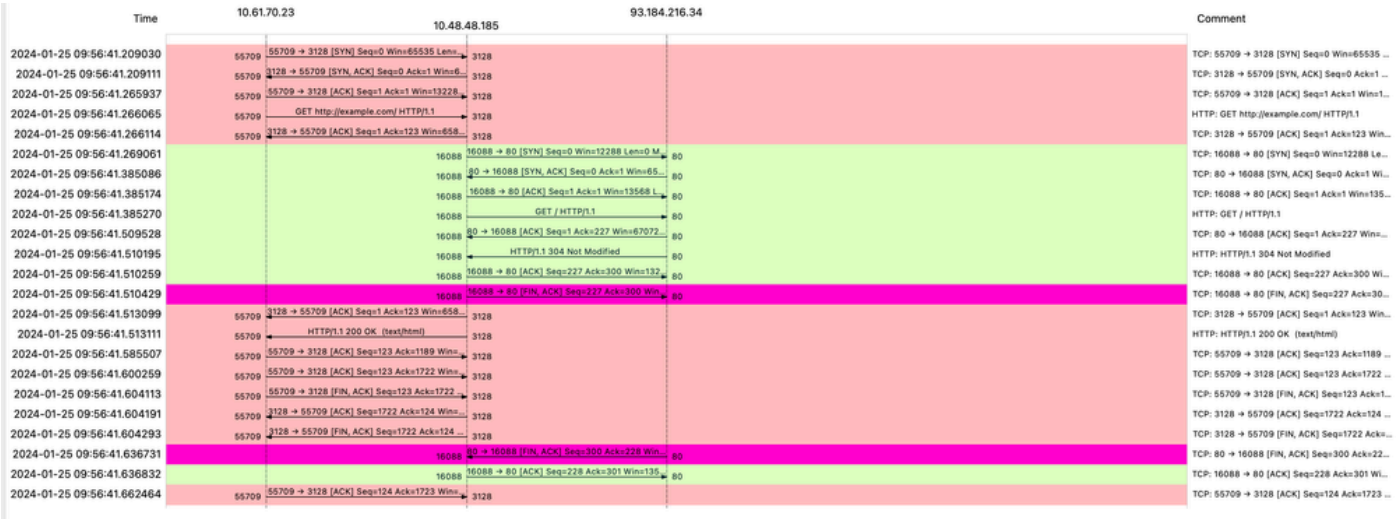


Image- Flow HTTP Explicit(캐시 포함)

다음은 HTTP 응답 304의 샘플입니다

```
> Frame 1947: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:f3:64 (00:50:56:8d:f3:64)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.48.48.185
> Transmission Control Protocol, Src Port: 80, Dst Port: 16088, Seq: 1, Ack: 227, Len: 299
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
  Accept-Ranges: bytes\r\n
  Age: 519756\r\n
  Cache-Control: max-age=604800\r\n
  Date: Thu, 25 Jan 2024 08:57:08 GMT\r\n
  Etag: "3147526947"\r\n
  Expires: Thu, 01 Feb 2024 08:57:08 GMT\r\n
  Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n
  Server: ECS (dce/2694)\r\n
  Vary: Accept-Encoding\r\n
  X-Cache: HIT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.124925000 seconds]
  [Request in frame: 1945]
  [Request URI: http://example.com/]
```

Image(이미지) - HTTP Explicit 304 응답

다음은 액세스 로그의 예입니다.

```
1706173001.489 235 10.61.70.23 TCP_REFRESH_HIT/200 1721 GET http://www.example.com/ - DIRECT/www.exampl
```

인증이 없는 명시적 구축의 HTTP 트래픽

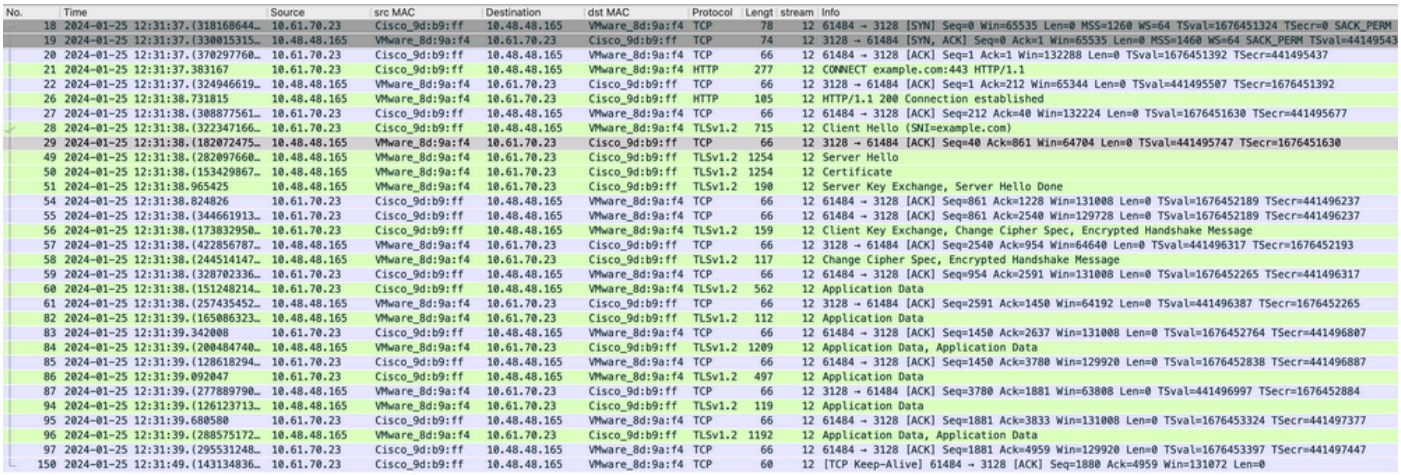
클라이언트 및 SWA

네트워크 트래픽은 클라이언트의 IP 주소와 SWA 프록시 인터페이스의 IP 주소 간에 전달됩니다(일반적으로 P1 인터페이스이지만 프록시 컨피그레이션에 따라 P2 또는 관리 인터페이스일 수 있음).

클라이언트에서 오는 트래픽은 TCP 포트 80 또는 3128에서 SWA로 전달됩니다(기본 SWA 프록시 포트는 TCP 80 및 3128이며, 이 예에서는 포트 3128을 사용합니다).

- TCP 핸드셰이크.
- 클라이언트에서 HTTP 연결(대상 IP = SWA, 대상 포트 = 3128)

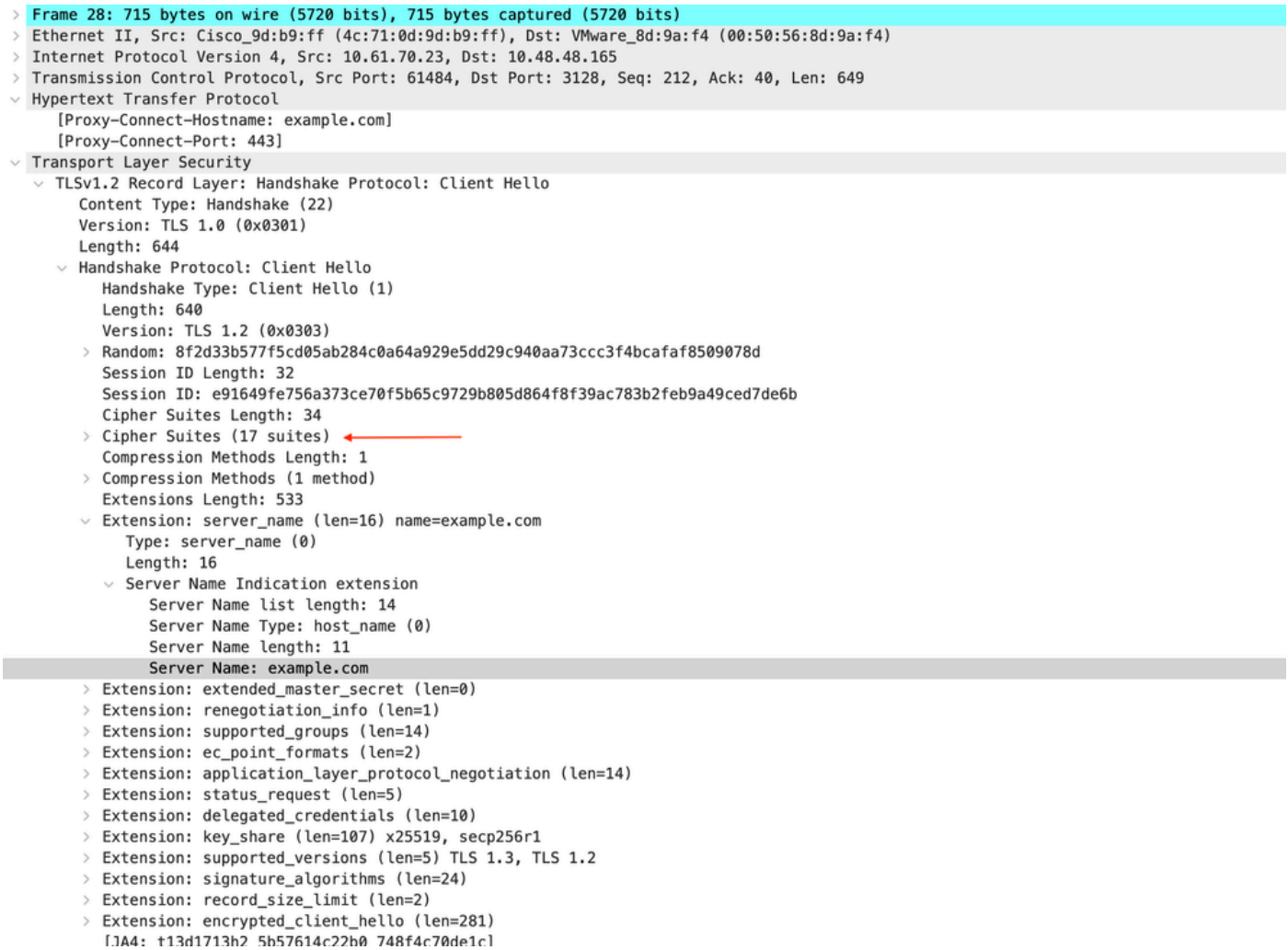
- 프록시의 HTTP 응답(소스 IP = SWA)
- URL의 SNI를 사용하는 Client Hello(소스 IP = 클라이언트)
- 서버 Hello(소스 IP = SWA)
- 서버 키 교환(소스 IP = SWA)
- 클라이언트 키 교환(소스 IP = 클라이언트)
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)



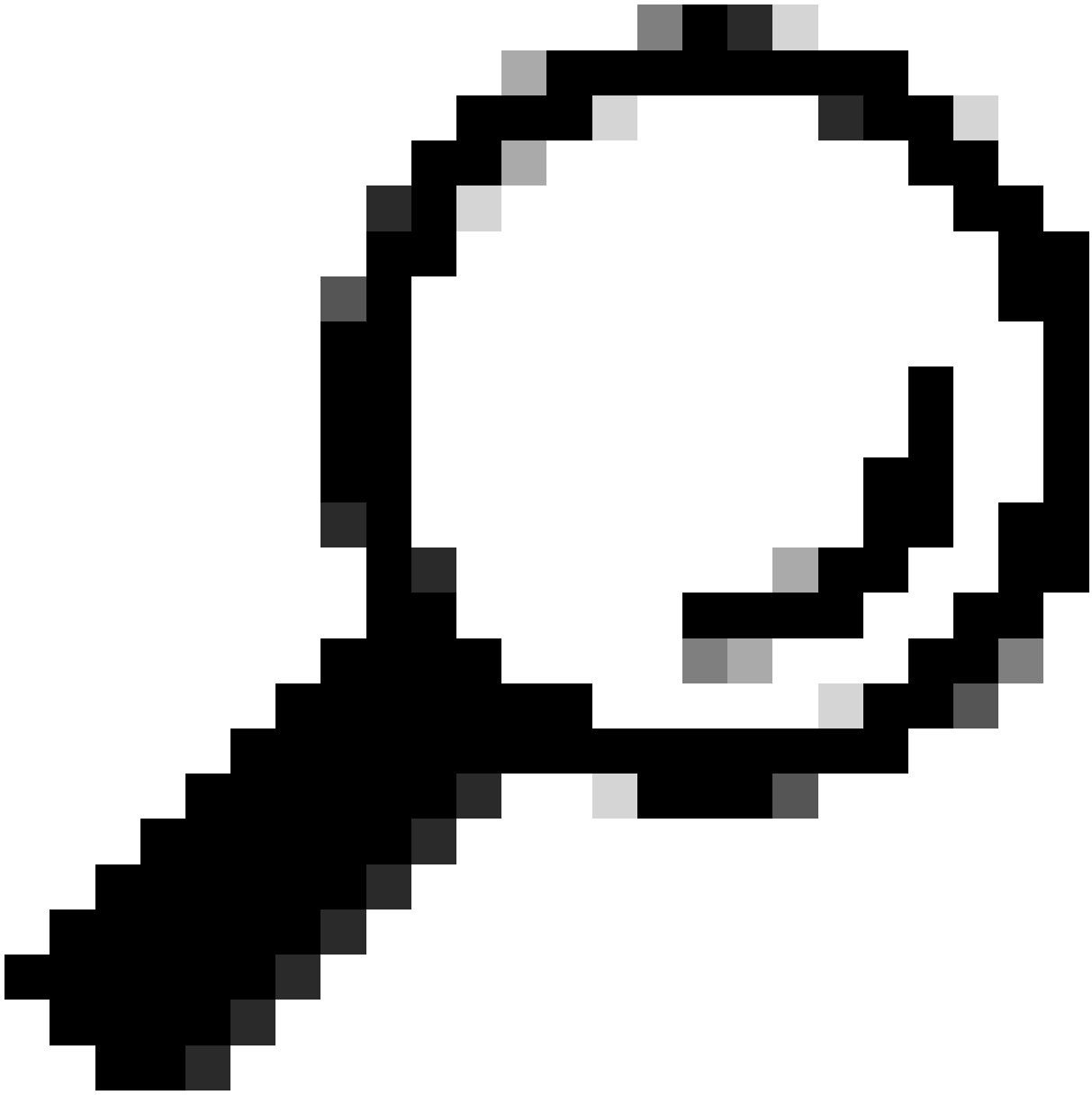
No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
18	2024-01-25 12:31:37.(318168644…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	78	12	61484 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1676451324 TSecr=0 SACK_PERM
19	2024-01-25 12:31:37.(330015315…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	74	12	3128 → 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=44149543
20	2024-01-25 12:31:37.(370297760…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=1676451392 TSecr=441495437
21	2024-01-25 12:31:37.383167	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	HTTP	277	12	CONNECT example.com:443 HTTP/1.1
22	2024-01-25 12:31:37.(324946619…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=1 Ack=212 Win=65344 Len=0 TSval=441495507 TSecr=1676451392
26	2024-01-25 12:31:38.731815	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	HTTP	105	12	HTTP/1.1 200 Connection established
27	2024-01-25 12:31:38.(308877561…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=1676451630 TSecr=441495677
28	2024-01-25 12:31:38.(322347166…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	715	12	Client Hello (SNI=example.com)
29	2024-01-25 12:31:38.(182072475…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=441495747 TSecr=1676451630
49	2024-01-25 12:31:38.(282097660…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Server Hello
50	2024-01-25 12:31:38.(153429867…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Certificate
51	2024-01-25 12:31:38.965425	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	190	12	Server Key Exchange, Server Hello Done
54	2024-01-25 12:31:38.824826	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=441496237
55	2024-01-25 12:31:38.(344661913…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=441496237
56	2024-01-25 12:31:38.(173832950…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	159	12	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2024-01-25 12:31:38.(422856787…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2540 Ack=954 Win=64640 Len=0 TSval=441496317 TSecr=1676452193
58	2024-01-25 12:31:38.(244514147…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	117	12	Change Cipher Spec, Encrypted Handshake Message
59	2024-01-25 12:31:38.(328702336…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=954 Ack=2591 Win=131008 Len=0 TSval=1676452265 TSecr=441496317
60	2024-01-25 12:31:38.(151248214…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	562	12	Application Data
61	2024-01-25 12:31:38.(257435452…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2591 Ack=1450 Win=64192 Len=0 TSval=441496387 TSecr=1676452265
82	2024-01-25 12:31:39.(165086323…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	112	12	Application Data
83	2024-01-25 12:31:39.342008	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=2637 Win=131008 Len=0 TSval=1676452764 TSecr=441496807
84	2024-01-25 12:31:39.(200484740…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1209	12	Application Data, Application Data
85	2024-01-25 12:31:39.(128618294…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=441496887
86	2024-01-25 12:31:39.092047	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	497	12	Application Data
87	2024-01-25 12:31:39.(277889790…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=3780 Ack=1881 Win=63808 Len=0 TSval=441496997 TSecr=1676452884
94	2024-01-25 12:31:39.(126123713…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	119	12	Application Data
95	2024-01-25 12:31:39.680580	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1881 Ack=3833 Win=131008 Len=0 TSval=1676453324 TSecr=441497377
96	2024-01-25 12:31:39.(288575172…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1192	12	Application Data, Application Data
97	2024-01-25 12:31:39.(295531248…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1881 Ack=4959 Win=129920 Len=0 TSval=1676453397 TSecr=441497447
150	2024-01-25 12:31:49.(143134836…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	60	12	[TCP Keep-Alive] 61484 → 3128 [ACK] Seq=1880 Ack=4959 Win=131072 Len=0

이미지- HTTPS 클라이언트에서 SWA-Explicit- 캐시 없음

다음은 SNI(Server Name Indication)에서 볼 수 있듯이 클라이언트에서 SWA로의 클라이언트 Hello에 대한 세부 정보입니다. 이 예에서 볼 수 있는 웹 서버의 URL은 www.example.com 및 클라이언트 알림 17 Cipher Suites입니다.

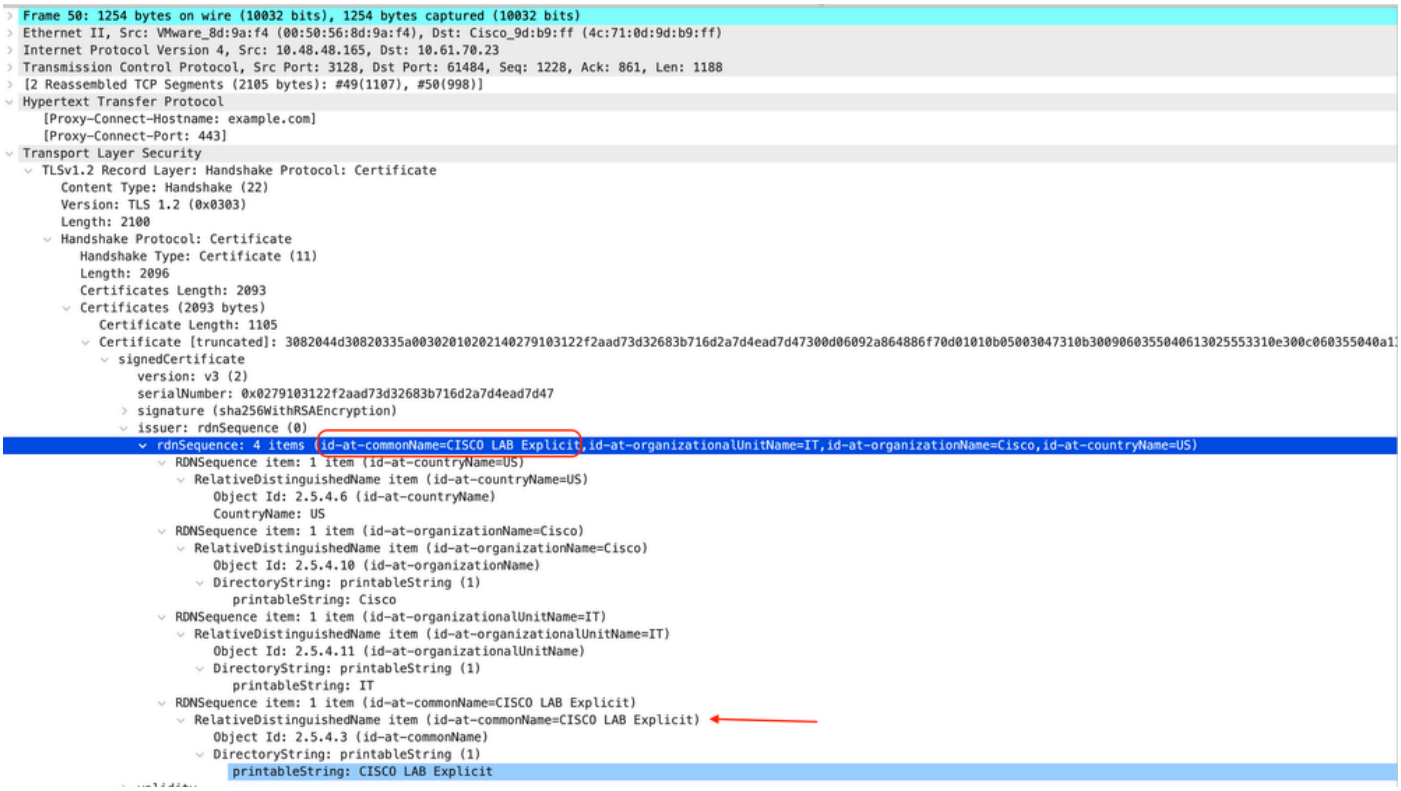


이미지- HTTPS 클라이언트 hello - 명시적 - 클라이언트-SWA



팁: Wireshark에서 이 필터를 사용하여 URL/SNI : tls.handshake.extensions_server_name == "www.example.com"를 검색할 수 있습니다.

다음은 SWA가 클라이언트로 보낸 인증서의 샘플입니다



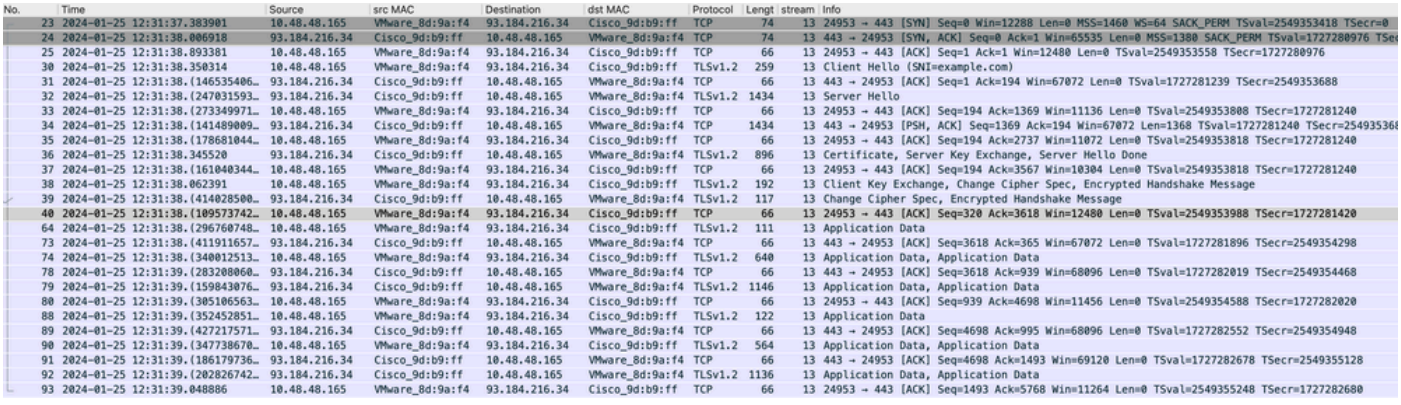
이미지 - HTTPS 인증서 - 명시적 - 클라이언트에 대한 SWA

SWA 및 웹 서버

네트워크 트래픽은 프록시의 IP 주소와 웹 서버의 IP 주소 간에 발생합니다.

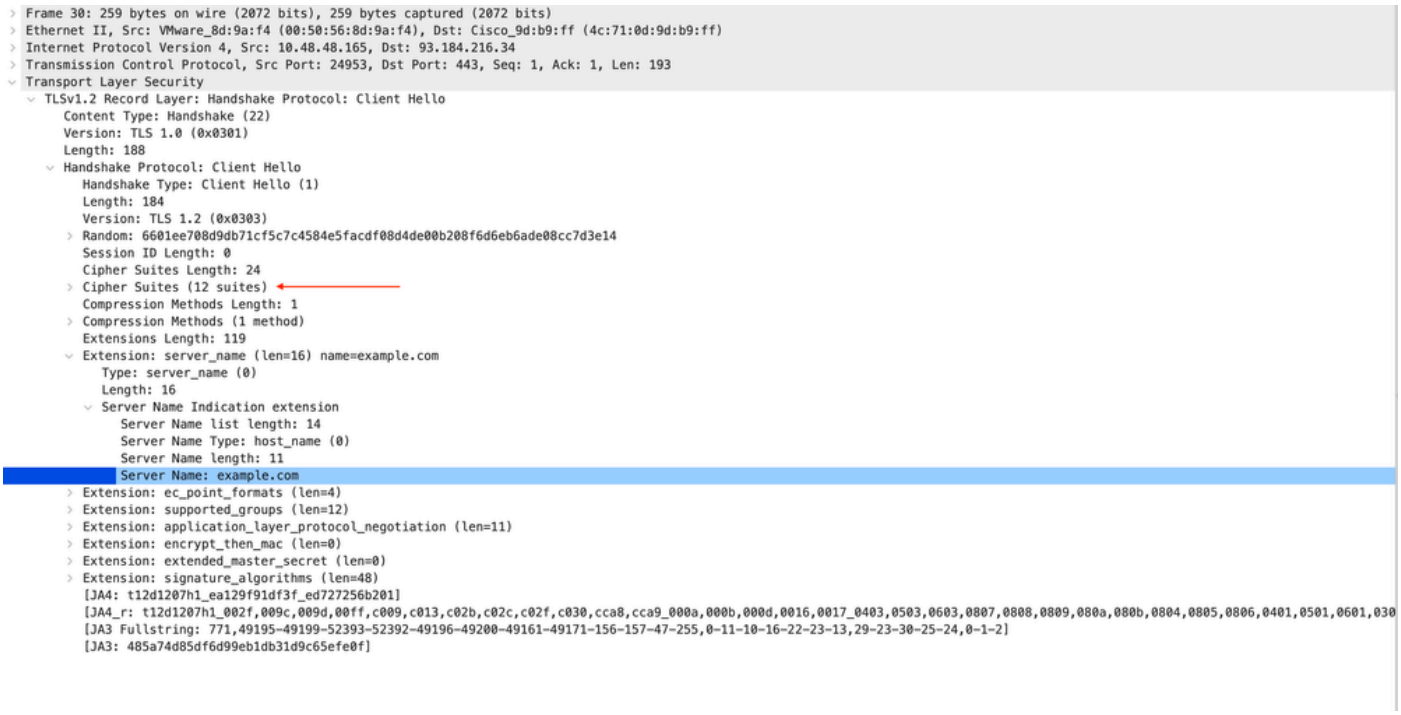
SWA의 트래픽은 프록시 포트가 아니라 TCP 포트 443으로 전달됩니다

- TCP 핸드셰이크.
- Client Hello(대상 IP = 웹 서버, 대상 포트 = 443)
- Server Hello(소스 IP = 웹 서버)
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)

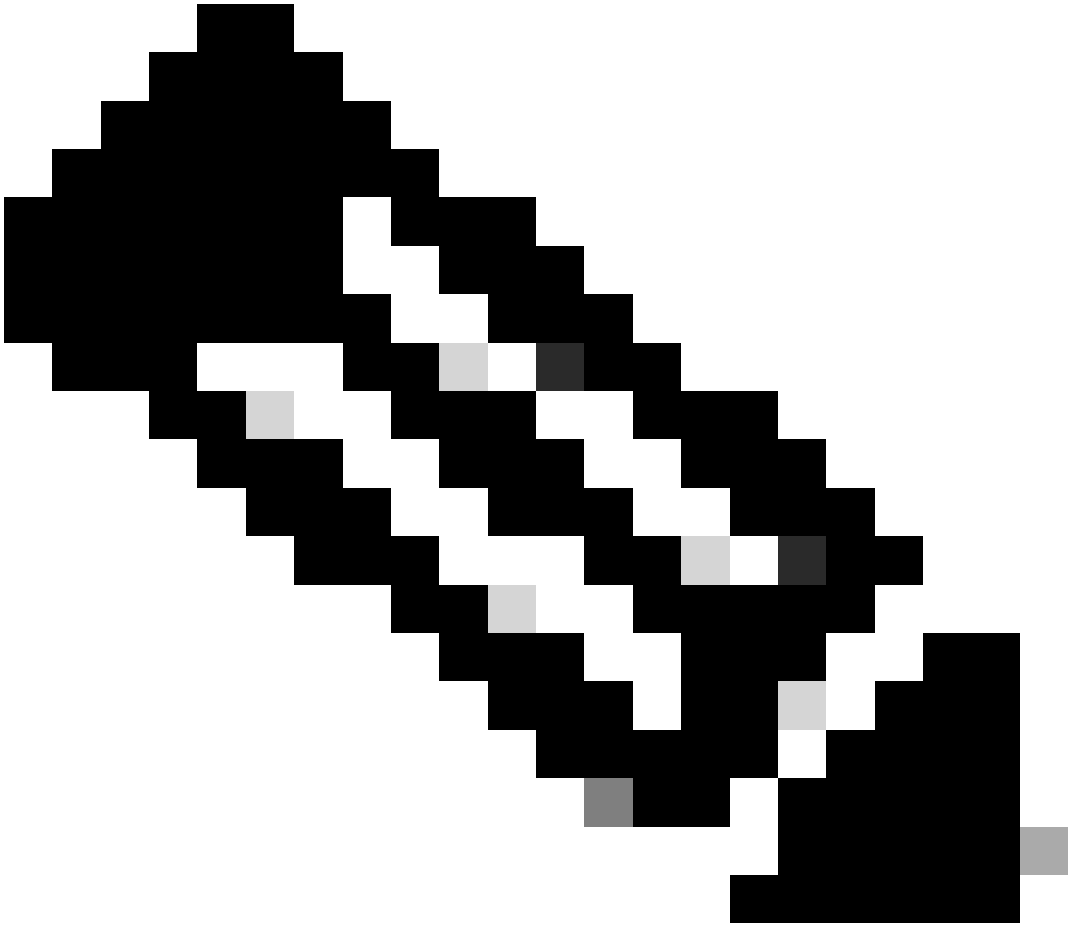


이미지 - HTTPS - 명시적 - 웹 서버에 대한 SWA

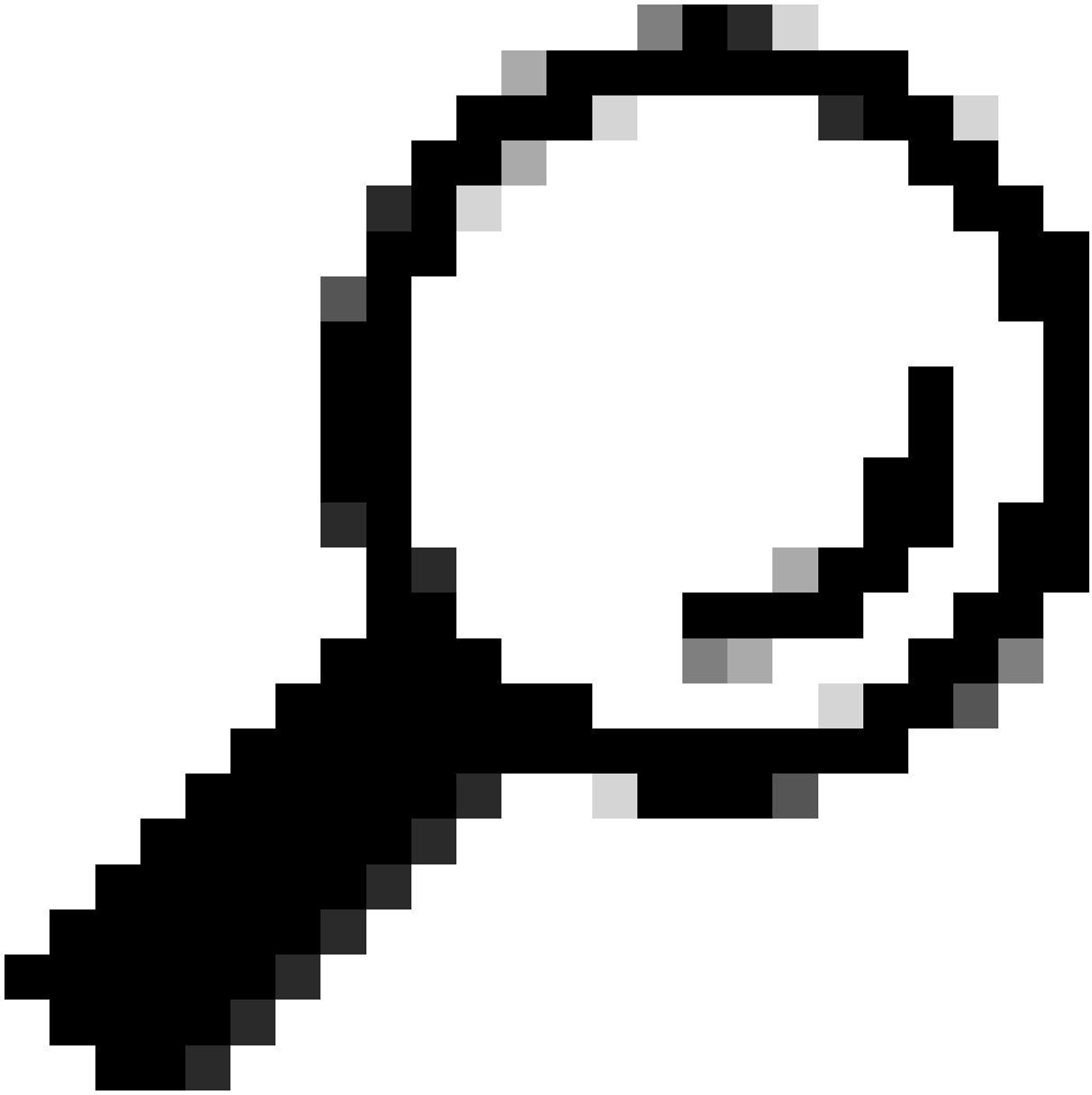
다음은 SWA에서 웹 서버로의 Client Hello에 대한 세부 정보입니다. SWA 알림 12 암호 그룹을 확인할 수 있습니다.



이미지- HTTPS 클라이언트 Hello - SWA-웹 서버- 캐시 없음



참고: 여기에서 관찰된 암호 그룹은 이 트래픽을 해독하도록 구성된 SWA가 자체 암호를 사용하므로 클라이언트에서 SWA로의 클라이언트 Hello의 암호 그룹과 다릅니다.



팁: Server Key Exchange(서버 키 교환)에서 SWA에서 웹 서버로, 웹 서버 인증서가 나타납니다. 그러나 업스트림 프록시가 SWA에 대한 컨피그레이션을 찾으면 웹 서버 인증서 대신 해당 인증서가 표시됩니다.

다음은 클라이언트의 HTTP CONNECT 샘플입니다

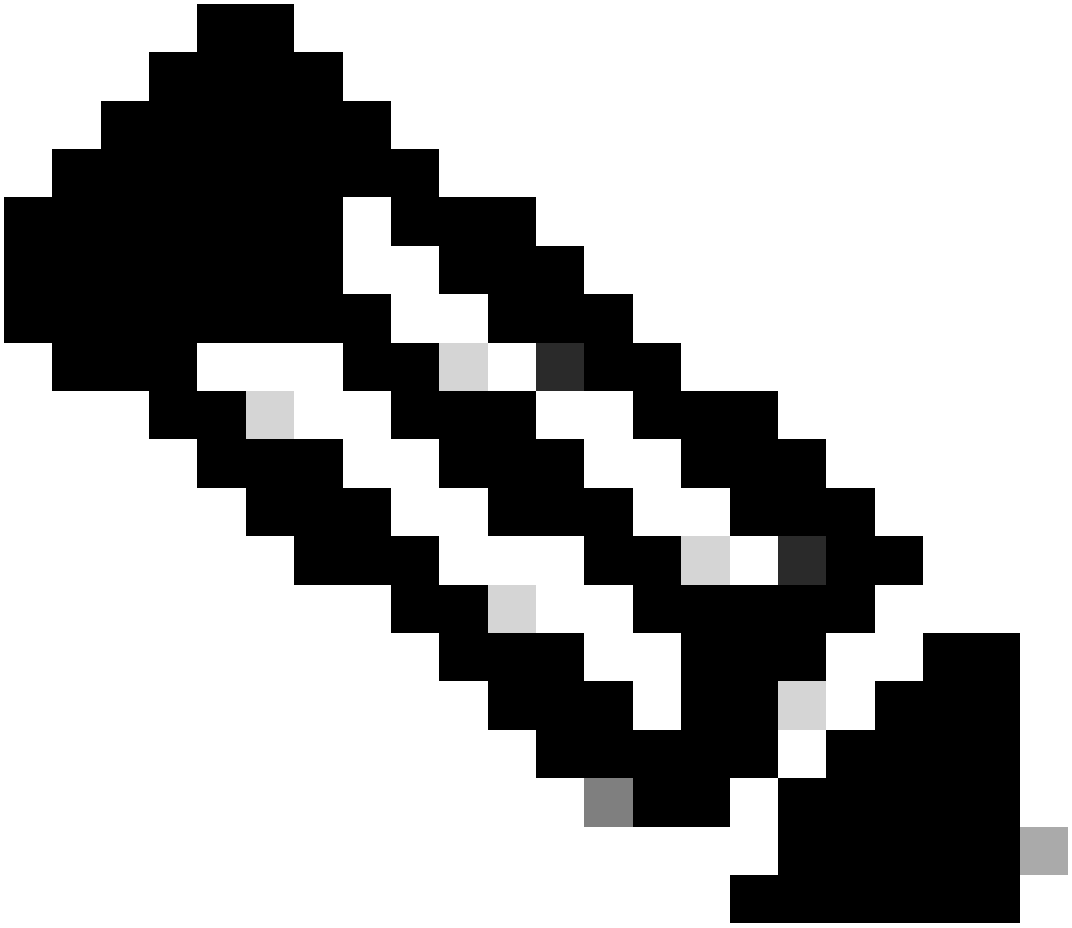
```
> Frame 21: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:9a:f4 (00:50:56:8d:9a:f4)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.165
> Transmission Control Protocol, Src Port: 61484, Dst Port: 3128, Seq: 1, Ack: 1, Len: 211
v Hypertext Transfer Protocol
  v CONNECT example.com:443 HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): CONNECT example.com:443 HTTP/1.1\r\n]
        [CONNECT example.com:443 HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: CONNECT
      Request URI: example.com:443
      Request Version: HTTP/1.1
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
    Proxy-Connection: keep-alive\r\n
    Connection: keep-alive\r\n
    Host: example.com:443\r\n
    \r\n
    [Full request URI: example.com:443]
    [HTTP request 1/1]
    [Response in frame: 26]
```

이미지 - 클라이언트 HTTP 연결

이는 클라이언트에서 SWA로, 웹 서버로, 마지막으로 클라이언트로 다시 이동하는 트래픽의 전체 흐름을 나타냅니다.

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
18	2024-01-25 12:31:37.(318168644…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	78	12	61484 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1676451324 TSecr=0 SACK_
19	2024-01-25 12:31:37.(330015315…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	74	12	3128 → 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=44
20	2024-01-25 12:31:37.(370297760…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=1676451392 TSecr=441495437
21	2024-01-25 12:31:37.383167	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	HTTP	277	12	CONNECT example.com:443 HTTP/1.1
22	2024-01-25 12:31:37.(324946619…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=1 Ack=212 Win=65344 Len=0 TSval=441495507 TSecr=1676451392
23	2024-01-25 12:31:37.383901	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	74	13	24953 → 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=2549353418 TSe
24	2024-01-25 12:31:38.006918	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	74	13	443 → 24953 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=172728097
25	2024-01-25 12:31:38.893381	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=1 Ack=1 Win=12480 Len=0 TSval=2549353558 TSecr=1727280976
26	2024-01-25 12:31:38.731815	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	HTTP	105	12	HTTP/1.1 200 Connection established
27	2024-01-25 12:31:38.(308877561…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=1676451630 TSecr=441495677
28	2024-01-25 12:31:38.(322347166…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	715	12	Client Hello (SNI=example.com)
29	2024-01-25 12:31:38.(182072475…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=441495747 TSecr=1676451630
30	2024-01-25 12:31:38.350314	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	259	13	Client Hello (SNI=example.com)
31	2024-01-25 12:31:38.(146535406…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=1 Ack=194 Win=67072 Len=0 TSval=1727281239 TSecr=2549353688
32	2024-01-25 12:31:38.(247031593…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	1434	13	Server Hello
33	2024-01-25 12:31:38.(273349971…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=194 Ack=1369 Win=11136 Len=0 TSval=2549353808 TSecr=1727281240
34	2024-01-25 12:31:38.(141489009…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	1434	13	443 → 24953 [PSH, ACK] Seq=1369 Ack=194 Win=67072 Len=1368 TSval=1727281240 TSecr=254
35	2024-01-25 12:31:38.(178681044…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=194 Ack=2737 Win=11072 Len=0 TSval=2549353818 TSecr=1727281240
36	2024-01-25 12:31:38.345520	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	896	13	Certificate, Server Key Exchange, Server Hello Done
37	2024-01-25 12:31:38.(161040344…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=194 Ack=3567 Win=10304 Len=0 TSval=2549353818 TSecr=1727281240
38	2024-01-25 12:31:38.062391	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	192	13	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
39	2024-01-25 12:31:38.(414028500…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	117	13	Change Cipher Spec, Encrypted Handshake Message
40	2024-01-25 12:31:38.(109573742…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=320 Ack=3618 Win=12480 Len=0 TSval=2549353988 TSecr=1727281420
49	2024-01-25 12:31:38.(282097660…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Server Hello
50	2024-01-25 12:31:38.(153429867…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Certificate
51	2024-01-25 12:31:38.965425	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	190	12	Server Key Exchange, Server Hello Done
54	2024-01-25 12:31:38.824826	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=441496237
55	2024-01-25 12:31:38.(344661913…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=441496237
56	2024-01-25 12:31:38.(173832950…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	159	12	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2024-01-25 12:31:38.(422856787…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2540 Ack=954 Win=64640 Len=0 TSval=441496317 TSecr=1676452193
58	2024-01-25 12:31:38.(244514147…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	117	12	Change Cipher Spec, Encrypted Handshake Message
59	2024-01-25 12:31:38.(328702336…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=954 Ack=2591 Win=131008 Len=0 TSval=1676452265 TSecr=441496317
60	2024-01-25 12:31:38.(151248214…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	562	12	Application Data
61	2024-01-25 12:31:38.(257435452…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2591 Ack=1450 Win=64192 Len=0 TSval=441496387 TSecr=1676452265
64	2024-01-25 12:31:38.(296760748…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	111	13	Application Data
73	2024-01-25 12:31:38.(411911657…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=3618 Ack=365 Win=67072 Len=0 TSval=1727281896 TSecr=2549354298
74	2024-01-25 12:31:38.(340012513…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	640	13	Application Data, Application Data
78	2024-01-25 12:31:39.(283208060…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=3618 Ack=939 Win=68096 Len=0 TSval=1727282019 TSecr=2549354468
79	2024-01-25 12:31:39.(159843076…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	1146	13	Application Data, Application Data
80	2024-01-25 12:31:39.(305106563…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=939 Ack=4698 Win=11456 Len=0 TSval=2549354588 TSecr=1727282020
82	2024-01-25 12:31:39.(165086323…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	112	12	Application Data
83	2024-01-25 12:31:39.342008	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=2637 Win=131008 Len=0 TSval=1676452764 TSecr=44149680
84	2024-01-25 12:31:39.(200484740…	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1209	12	Application Data, Application Data
85	2024-01-25 12:31:39.(128618294…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=44149688
86	2024-01-25 12:31:39.092047	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	497	12	Application Data

이미지 - 전체 HTTPS 명시적-캐시 없음

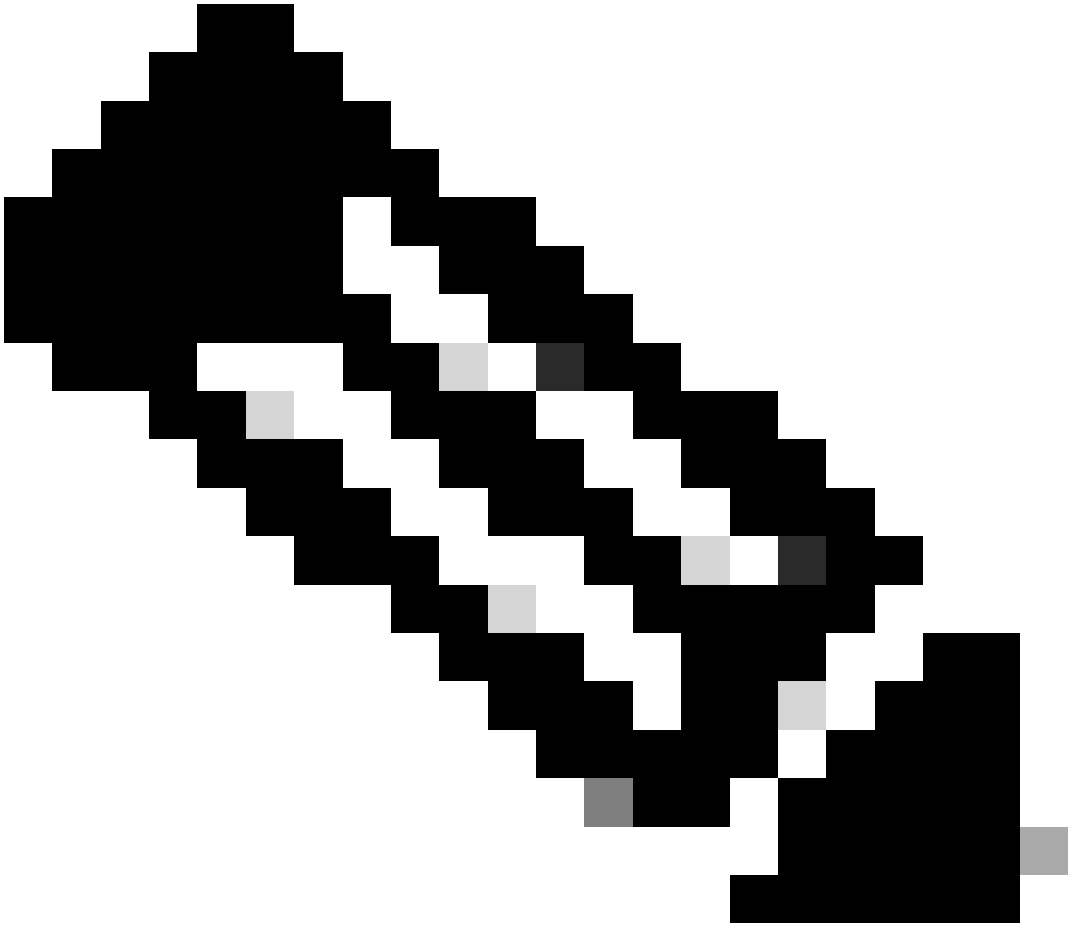


참고: 각 트래픽 스트림은 서로 다른 색상으로 구분됩니다. 클라이언트에서 SWA로의 흐름은 한 색상이고 SWA에서 웹 서버로의 흐름은 다른 색상입니다.

이미지- HTTPS 흐름- 명시적 - 캐시 없음

다음은 액세스 로그의 예입니다.

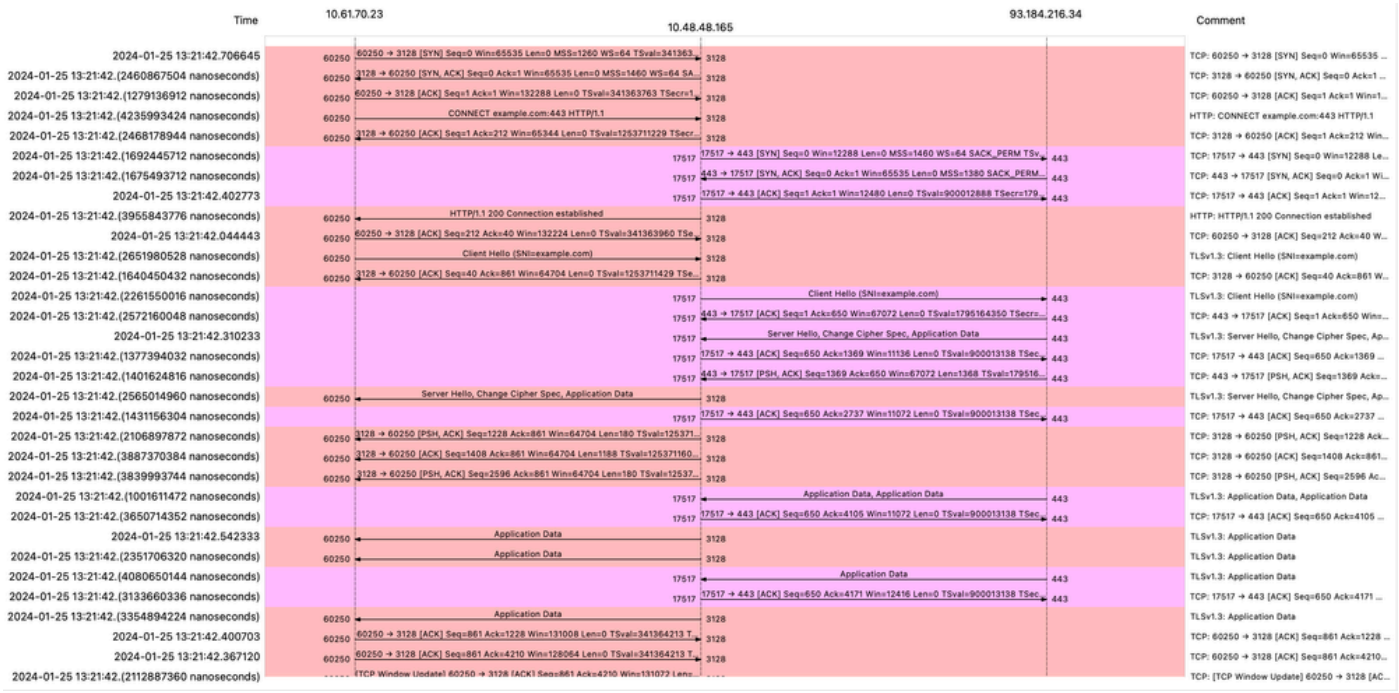
```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.examp
```



참고: HTTPS 트래픽에 대한 투명 배포에서 볼 수 있듯이 Accesslogs에는 2개의 줄이 있습니다. 첫 번째 줄은 트래픽이 암호화되어 CONNECT를 볼 수 있으며 웹 서버의 URL이 tunnel://으로 시작됩니다. SWA에서 암호 해독이 활성화된 경우 두 번째 줄에 GET이 포함되고 전체 URL이 HTTPS로 시작되므로 트래픽이 암호 해독되었습니다.

통과 HTTPS 트래픽

트래픽을 통과하도록 SWA를 구성한 경우, 전체적인 흐름은 다음과 같습니다.



이미지 - HTTPS 통과 - 명시적 - 흐름

다음은 SWA에서 웹 서버로의 Client Hello 샘플입니다.

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 644
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 640
      Version: TLS 1.2 (0x0303)
      Random: 2c545a566b5b3f338dc9dbd80ea91ad61035c786954ced2191e266ff0b92b9c1
      Session ID Length: 32
      Session ID: 86da348af5508fc24f18f3cbd9829c7282b77e0499e5d2f38466cccbd66821e2
      Cipher Suites Length: 34
    Cipher Suites (17 suites)
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Compression Methods Length: 1
    > Compression Methods (1 method)
      Extensions Length: 533
    Extension: server_name (len=16) name=example.com
        Type: server_name (0)
        Length: 16
      Server Name Indication extension
          Server Name list length: 14
          Server Name Type: host_name (0)
          Server Name length: 11
          Server Name: example.com
    > Extension: extended_master_secret (len=0)
    > Extension: renegotiation_info (len=1)
    > Extension: supported_groups (len=14)
    > Extension: ec_point_formats (len=2)
```

이미지- HTTPS Passthrough - Explicit - SWA to Webserver - Client hello

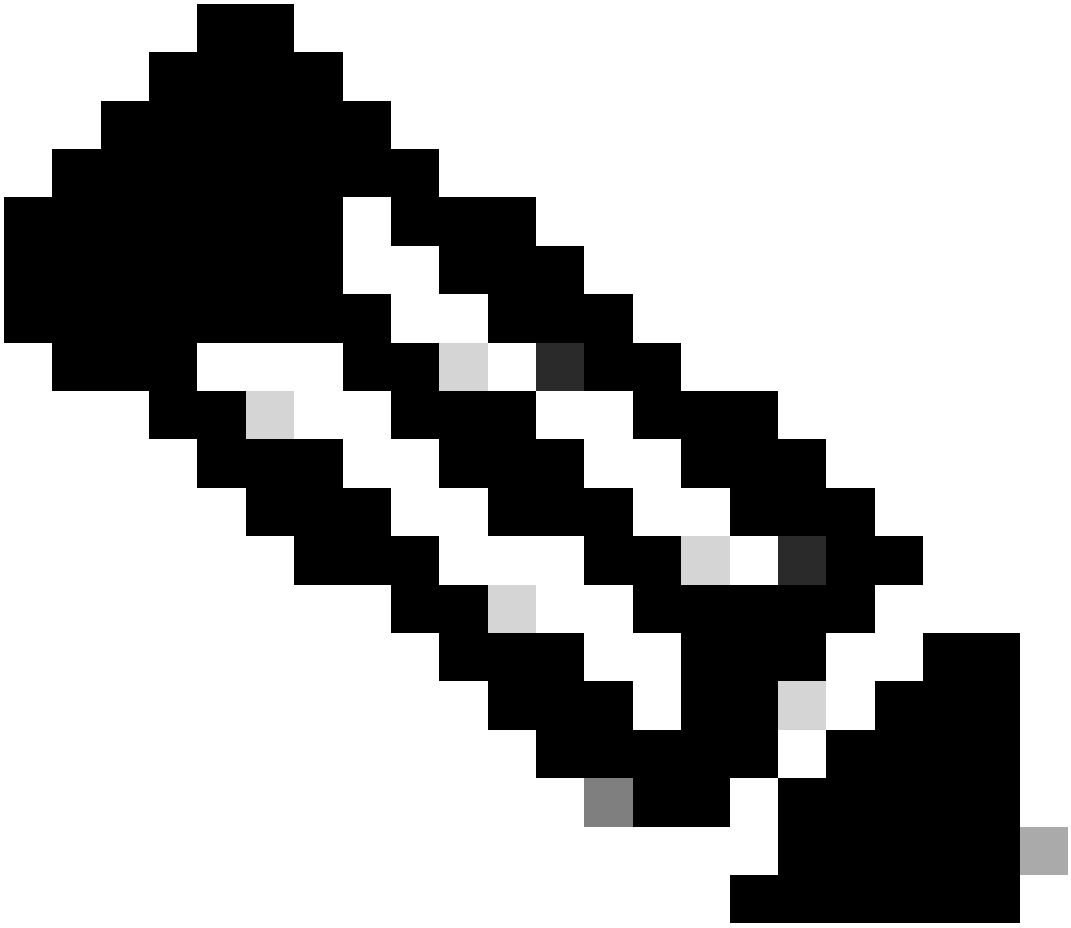
이는 클라이언트에서 SWA로의 클라이언트 Hello와 동일합니다.

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 644
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 640
      Version: TLS 1.2 (0x0303)
      Random: 2c545a566b5b3f338dc9dbd80ea91ad61035c786954ced2191e266ff0b92b9c1
      Session ID Length: 32
      Session ID: 86da348af5508fc24f18f3cbd9829c7282b77e0499e5d2f38466cccbd66821e2
      Cipher Suites Length: 34
    Cipher Suites (17 suites)
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Compression Methods Length: 1
    Compression Methods (1 method)
      Extensions Length: 533
    Extension: server_name (len=16) name=example.com
      Type: server_name (0)
      Length: 16
    Server Name Indication extension
        Server Name list length: 14
        Server Name Type: host_name (0)
        Server Name length: 11
        Server Name: example.com
    Extension: extended_master_secret (len=0)
      Type: extended_master_secret (23)
      Length: 0
    Extension: renegotiation_info (len=1)
```

이미지- HTTPS 패스스루 - 명시적 - 클라이언트-SWA - 클라이언트 hello

다음은 샘플 액세스 로그입니다.

```
1706185288.920 53395 10.61.70.23 TCP_MISS/200 6549 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
```



참고: 보시다시피 한 줄이며 작업은 PASSTHRU입니다.

투명한 구축

인증 없는 투명 구축의 HTTP 트래픽

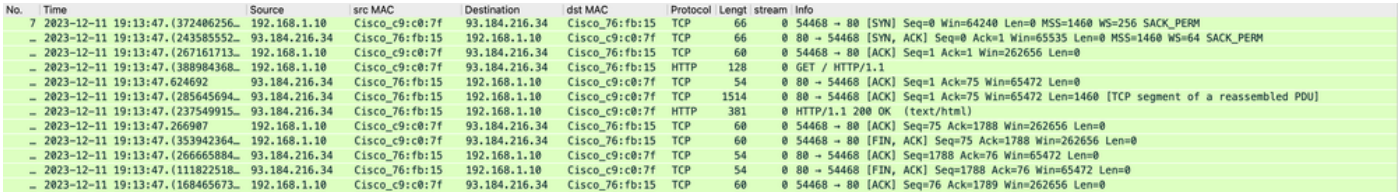
클라이언트 및 SWA

네트워크 트래픽은 클라이언트의 IP 주소와 웹 서버의 IP 주소 간에 전달됩니다.

클라이언트에서 오는 트래픽은 프록시 포트가 아닌 TCP 포트 80으로 전달됩니다

- TCP 핸드셰이크.
- 클라이언트에서 HTTP 가져오기(대상 IP = 웹 서버, 대상 포트 = 80)
- 프록시의 HTTP 응답(소스 IP = 웹 서버)
- 데이터 전송

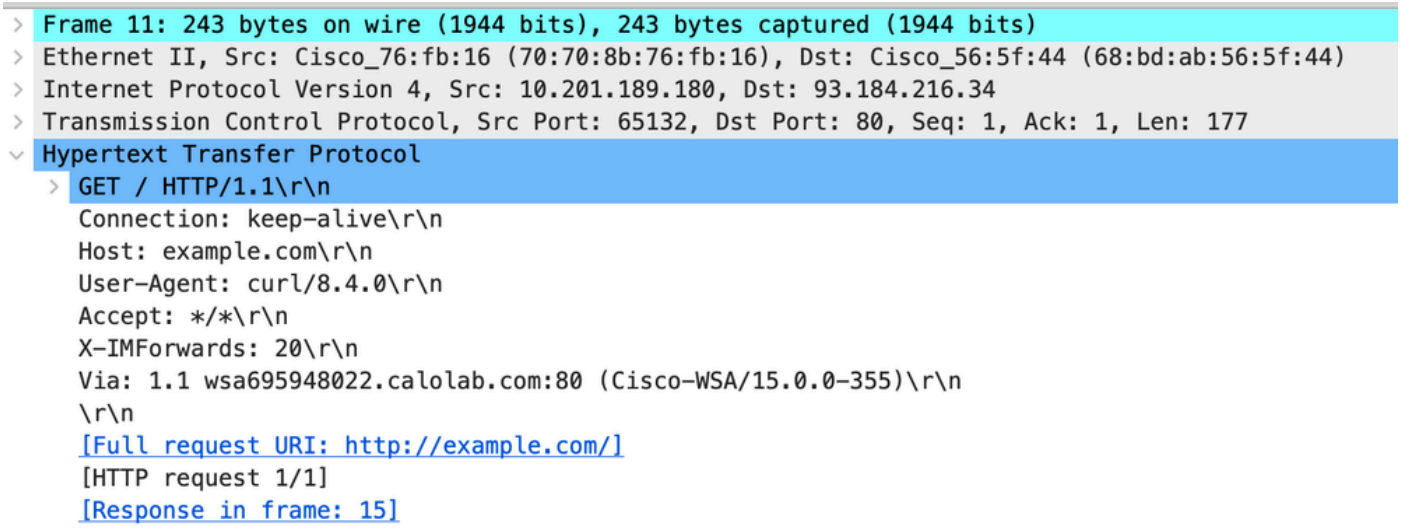
- TCP 연결 종료(4-Way Handshake)



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
7	2023-12-11 19:13:47.(372406256…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	66	0	54468 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
…	2023-12-11 19:13:47.(243585552…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	0	80 → 54468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
…	2023-12-11 19:13:47.(267161713…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
…	2023-12-11 19:13:47.(388984368…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	HTTP	128	0	GET / HTTP/1.1
…	2023-12-11 19:13:47.624692	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=0
…	2023-12-11 19:13:47.(285645694…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	0	80 → 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
…	2023-12-11 19:13:47.(237549915…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	0	HTTP/1.1 200 OK (text/html)
…	2023-12-11 19:13:47.266907	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0
…	2023-12-11 19:13:47.(353942364…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
…	2023-12-11 19:13:47.(266665884…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [ACK] Seq=1788 Ack=76 Win=65472 Len=0
…	2023-12-11 19:13:47.(111822518…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [FIN, ACK] Seq=1788 Ack=76 Win=65472 Len=0
…	2023-12-11 19:13:47.(168465673…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0

이미지 - 클라이언트에서 프록시로 - HTTP - 투명 - 인증 없음

다음은 클라이언트에서 가져온 HTTP Get의 샘플입니다



```
> Frame 11: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: Cisco_76:fb:16 (70:70:8b:76:fb:16), Dst: Cisco_56:5f:44 (68:bd:ab:56:5f:44)
> Internet Protocol Version 4, Src: 10.201.189.180, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 65132, Dst Port: 80, Seq: 1, Ack: 1, Len: 177
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Connection: keep-alive\r\n
    Host: example.com\r\n
    User-Agent: curl/8.4.0\r\n
    Accept: */*\r\n
    X-IMForwards: 20\r\n
    Via: 1.1 wsa695948022.calolab.com:80 (Cisco-WSA/15.0.0-355)\r\n
    \r\n
    [Full request URI: http://example.com/]
    [HTTP request 1/1]
    [Response in frame: 15]
```

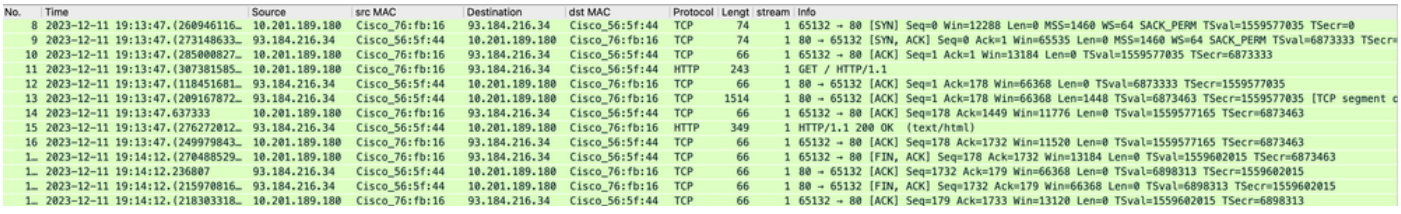
이미지 - 클라이언트에서 프록시로 - HTTP - 투명 - 인증 없음 - 클라이언트 HTTP 가져오기

SWA 및 웹 서버

네트워크 트래픽은 프록시의 IP 주소와 웹 서버의 IP 주소 간에 발생합니다.

SWA의 트래픽은 프록시 포트가 아닌 TCP 포트 80으로 전달됩니다

- TCP 핸드셰이크.
- 프록시에서 HTTP 가져오기(대상 IP = 웹 서버, 대상 포트 = 80)
- 웹 서버의 HTTP 응답(소스 IP = 프록시 서버)
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
8	2023-12-11 19:13:47.(260946116…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	1	65132 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1559577035 TSecr=0
9	2023-12-11 19:13:47.(273148633…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1	80 → 65132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=6873333 TSecr=
10	2023-12-11 19:13:47.(285000827…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1559577035 TSecr=6873333
11	2023-12-11 19:13:47.(307381585…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	243	1	GET / HTTP/1.1
12	2023-12-11 19:13:47.(118451681…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=0 TSval=6873333 TSecr=1559577035
13	2023-12-11 19:13:47.(209167872…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	1514	1	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=1559577035 [TCP segment c
14	2023-12-11 19:13:47.637333	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=178 Ack=1449 Win=11776 Len=0 TSval=1559577165 TSecr=6873463
15	2023-12-11 19:13:47.(276272012…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	349	1	HTTP/1.1 200 OK (text/html)
16	2023-12-11 19:13:47.(249979843…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=178 Ack=1732 Win=11520 Len=0 TSval=1559577165 TSecr=6873463
1…	2023-12-11 19:14:12.(270488529…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [FIN, ACK] Seq=178 Ack=1732 Win=13184 Len=0 TSval=1559602015 TSecr=6873463
1…	2023-12-11 19:14:12.236807	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1…	2023-12-11 19:14:12.(215970816…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [FIN, ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1…	2023-12-11 19:14:12.(218303318…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=179 Ack=1733 Win=13120 Len=0 TSval=1559602015 TSecr=6898313

이미지 - 프록시 및 웹 서버 - HTTP - 투명 - 인증 없음

다음은 프록시에서 HTTP Get의 샘플입니다.

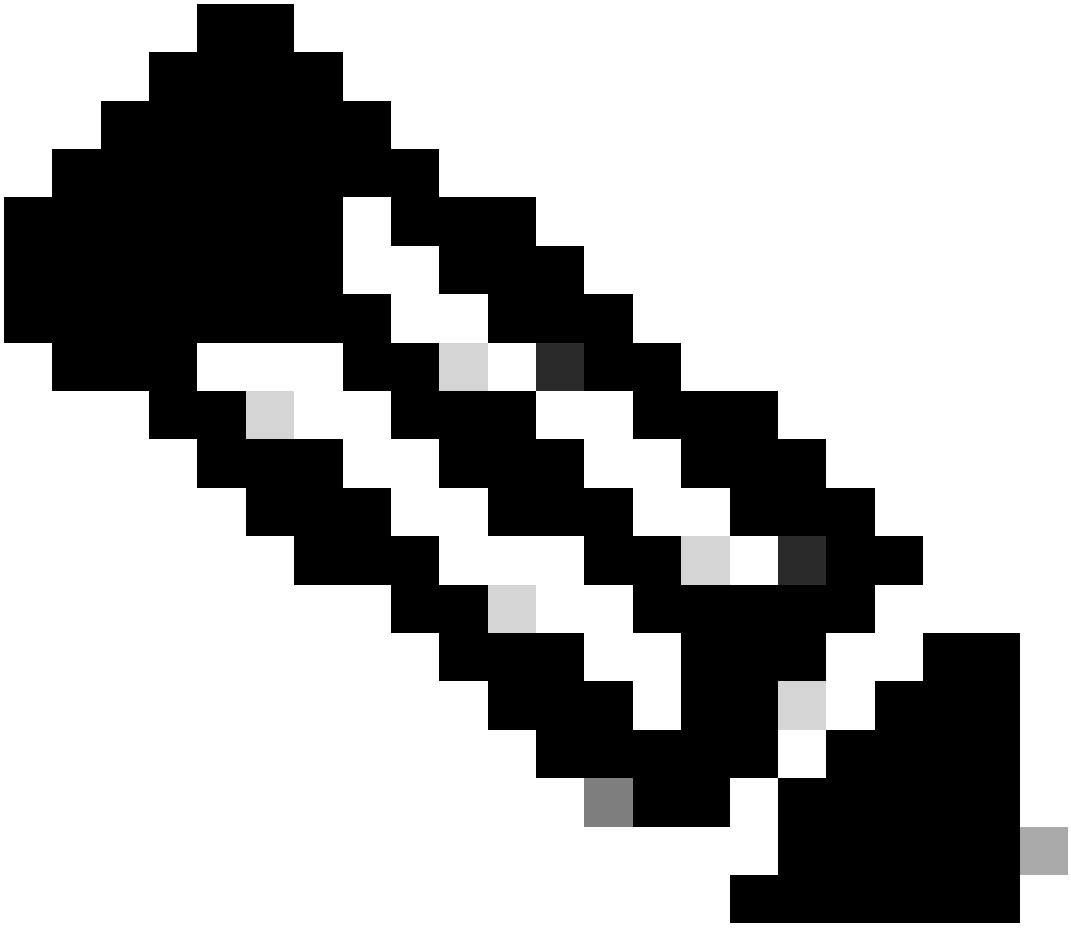
```
> Frame 20: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54468, Dst Port: 80, Seq: 1, Ack: 1, Len: 74
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: example.com\r\n
    User-Agent: curl/8.4.0\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://example.com/]
    [HTTP request 1/1]
    [Response in frame: 23]
```

이미지 - 웹 서버에 대한 프록시 - HTTP - 투명 - 인증 없음 - 프록시 HTTP 가져오기

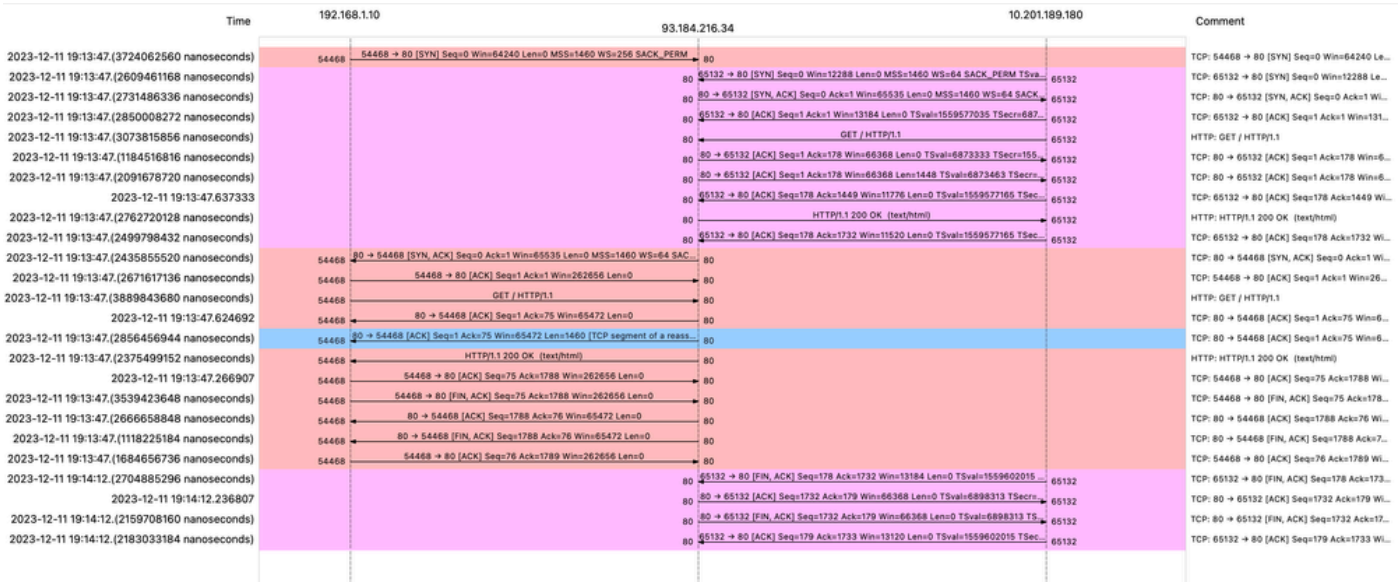
이는 클라이언트에서 SWA로, 웹 서버로, 마지막으로 클라이언트로 다시 이동하는 트래픽의 전체 흐름을 나타냅니다.

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
7	2023-12-11 19:13:47.(372406256…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	66	0	54468 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8	2023-12-11 19:13:47.(260946116…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	1	65132 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1559577035 TSecr=0
9	2023-12-11 19:13:47.(273148633…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1	80 → 65132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=6873333 TSecr
10	2023-12-11 19:13:47.(285000827…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1559577035 TSecr=6873333
11	2023-12-11 19:13:47.(307381585…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	243	1	GET / HTTP/1.1
12	2023-12-11 19:13:47.(118451681…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=0 TSval=6873333 TSecr=1559577035
13	2023-12-11 19:13:47.(209167872…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	1514	1	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=1559577035 [TCP segment
14	2023-12-11 19:13:47.637333	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=178 Ack=1449 Win=11776 Len=0 TSval=1559577165 TSecr=6873463
15	2023-12-11 19:13:47.(276272012…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	349	1	HTTP/1.1 200 OK (text/html)
16	2023-12-11 19:13:47.(249979843…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=178 Ack=1732 Win=11520 Len=0 TSval=1559577165 TSecr=6873463
18	2023-12-11 19:13:47.(243585552…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	0	80 → 54468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
19	2023-12-11 19:13:47.(267161713…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
20	2023-12-11 19:13:47.(388984368…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	HTTP	128	0	GET / HTTP/1.1
21	2023-12-11 19:13:47.624692	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=0
22	2023-12-11 19:13:47.(285645694…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	0	80 → 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
23	2023-12-11 19:13:47.(237549915…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	0	HTTP/1.1 200 OK (text/html)
24	2023-12-11 19:13:47.266907	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0
25	2023-12-11 19:13:47.(353942364…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
26	2023-12-11 19:13:47.(266665884…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [ACK] Seq=1788 Ack=76 Win=65472 Len=0
27	2023-12-11 19:13:47.(111822518…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 → 54468 [FIN, ACK] Seq=1788 Ack=76 Win=65472 Len=0
28	2023-12-11 19:13:47.(168465673…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 → 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0
1…	2023-12-11 19:14:12.(270488529…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [FIN, ACK] Seq=178 Ack=1732 Win=13184 Len=0 TSval=1559602015 TSecr=6873463
1…	2023-12-11 19:14:12.236807	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1…	2023-12-11 19:14:12.(215970816…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [FIN, ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1…	2023-12-11 19:14:12.(218303318…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=179 Ack=1733 Win=13120 Len=0 TSval=1559602015 TSecr=6898313

이미지 - 총 트래픽 - HTTP - 투명 - 인증 없음



참고: 각 트래픽 스트림은 서로 다른 색상으로 구분됩니다. 클라이언트에서 SWA로의 흐름은 한 색상이고 SWA에서 웹 서버로의 흐름은 다른 색상입니다.



이미지 - WCCP HTTP 흐름

다음은 액세스 로그의 예입니다.

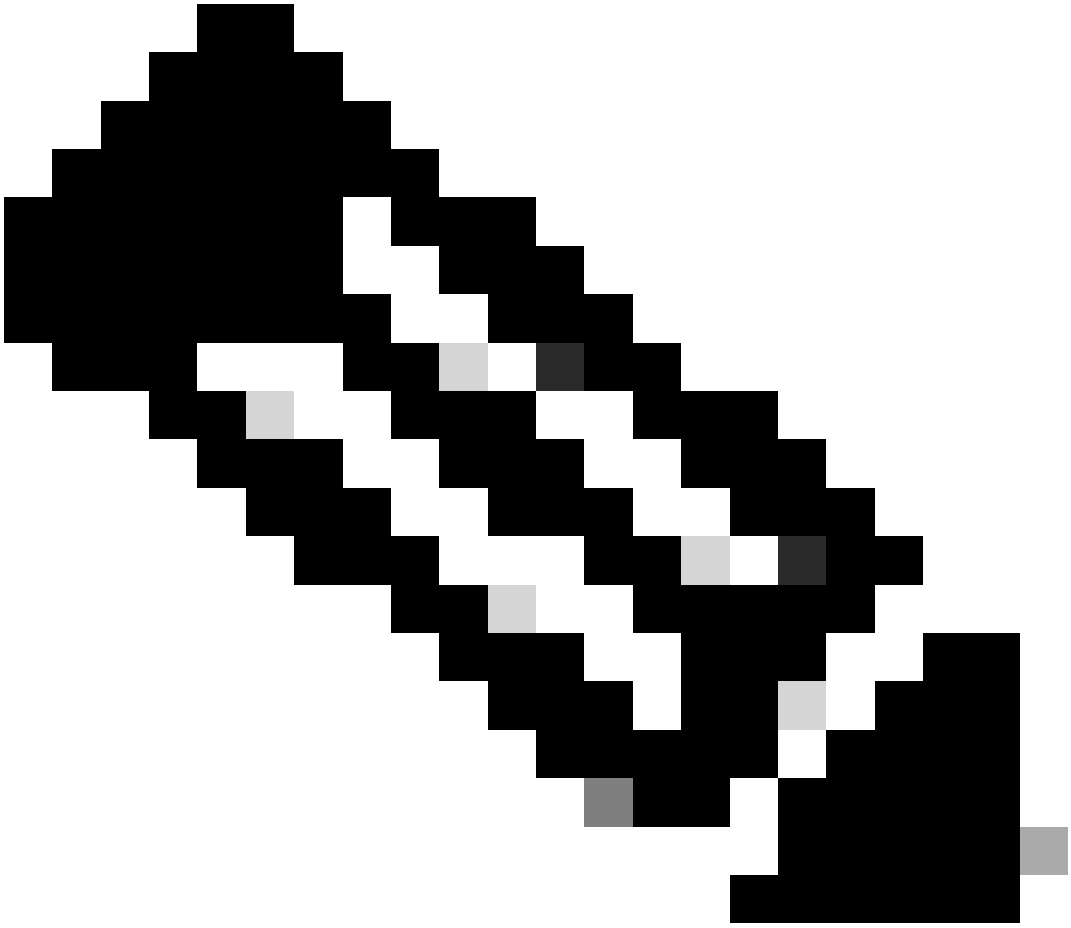
```
1702318427.181 124 192.168.1.10 TCP_MISS/200 1787 GET http://www.example.com/ - DIRECT/www.example.com
```

캐시된 데이터가 있는 트래픽

데이터가 SWA 캐시에 있을 때 클라이언트에서 SWA로의 전체 트래픽 흐름을 나타냅니다.

9	2023-12-11 19:19:49.(111544768…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	1	13586 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3178050246 TSecr=0
11	2023-12-11 19:19:49.(259539926…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	66	2	54487 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	2023-12-11 19:19:49.(254858128…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	2	80 → 54487 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
13	2023-12-11 19:19:49.(272497027…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
14	2023-12-11 19:19:49.(178847280…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	HTTP	128	2	GET / HTTP/1.1
15	2023-12-11 19:19:49.(104967324…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2	80 → 54487 [ACK] Seq=1 Ack=75 Win=65472 Len=0
16	2023-12-11 19:19:49.656205	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	2	80 → 54487 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
17	2023-12-11 19:19:49.(425926200…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	2	HTTP/1.1 200 OK (text/html)
18	2023-12-11 19:19:49.(270830524…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487 → 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0
19	2023-12-11 19:19:49.(391010345…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487 → 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
20	2023-12-11 19:19:49.(394258659…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2	80 → 54487 [ACK] Seq=1788 Ack=76 Win=65472 Len=0
21	2023-12-11 19:19:49.910090	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2	80 → 54487 [FIN, ACK] Seq=1788 Ack=76 Win=65472 Len=0
22	2023-12-11 19:19:49.(179047075…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487 → 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0
23	2023-12-11 19:19:49.(372291046…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1	80 → 13586 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=4080954250 TSe
24	2023-12-11 19:19:49.(309178142…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586 → 80 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=3178050246 TSecr=4080954250
25	2023-12-11 19:19:49.(226286489…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	293	1	GET / HTTP/1.1
26	2023-12-11 19:19:49.(207193169…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 13586 [ACK] Seq=1 Ack=228 Win=66368 Len=0 TSval=4080954250 TSecr=3178050246
27	2023-12-11 19:19:49.(229948003…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	489	1	HTTP/1.1 304 Not Modified
28	2023-12-11 19:19:49.(336640662…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586 → 80 [ACK] Seq=228 Ack=424 Win=12800 Len=0 TSval=3178050356 TSecr=4080954361
29	2023-12-11 19:19:49.352537	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586 → 80 [FIN, ACK] Seq=228 Ack=424 Win=13184 Len=0 TSval=3178050356 TSecr=4080954361
30	2023-12-11 19:19:49.(194154916…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 13586 [ACK] Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
31	2023-12-11 19:19:49.(349158924…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 13586 [FIN, ACK] Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
32	2023-12-11 19:19:49.(103444988…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586 → 80 [ACK] Seq=229 Ack=425 Win=13120 Len=0 TSval=3178050356 TSecr=4080954361

이미지 - 캐시됨 - 총 트래픽 - HTTP - 투명 - 인증 없음



참고: 웹 서버에서 HTTP 응답 304: Cache not Modified를 반환하는 것을 볼 수 있습니다. (이 예에서는 패킷 번호 27)

다음은 HTTP 응답 304의 샘플입니다

```
> Frame 27: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Cisco_56:5f:44 (68:bd:ab:56:5f:44), Dst: Cisco_76:fb:16 (70:70:8b:76:fb:16)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.201.189.180
> Transmission Control Protocol, Src Port: 80, Dst Port: 13586, Seq: 1, Ack: 228, Len: 423
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Accept-Ranges: bytes\r\n
    Cache-Control: max-age=604800\r\n
    Date: Mon, 11 Dec 2023 18:22:17 GMT\r\n
    Etag: "3147526947"\r\n
    Expires: Mon, 18 Dec 2023 18:22:17 GMT\r\n
    Server: ECS (dce/26C6)\r\n
    Vary: Accept-Encoding\r\n
    X-Cache: HIT\r\n
    Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n
    Age: 492653\r\n
    Via: 1.1 rtp1-lab-wsa-1.cisco.com:80 (Cisco-WSA/X), 1.1 proxy.rcdn.local:80 (Cisco-WSA/12.5.5-004)\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.036615136 seconds]
    [Request in frame: 25]
    [Request URI: http://example.com/]
```

Image(이미지) - Cached(캐시됨) - HTTP response(HTTP 응답) 304 - HTTP - Transparent(투명) - No Auth(인증 없음)

다음은 액세스 로그의 예입니다.

```
1702318789.560 105 192.168.1.10 TCP_REFRESH_HIT/200 1787 GET http://www.example.com/ - DIRECT/www.examp
```

인증 없는 투명 구축의 HTTP 트래픽

클라이언트 및 SWA

네트워크 트래픽은 클라이언트의 IP 주소와 웹 서버의 IP 주소 간에 전달됩니다.

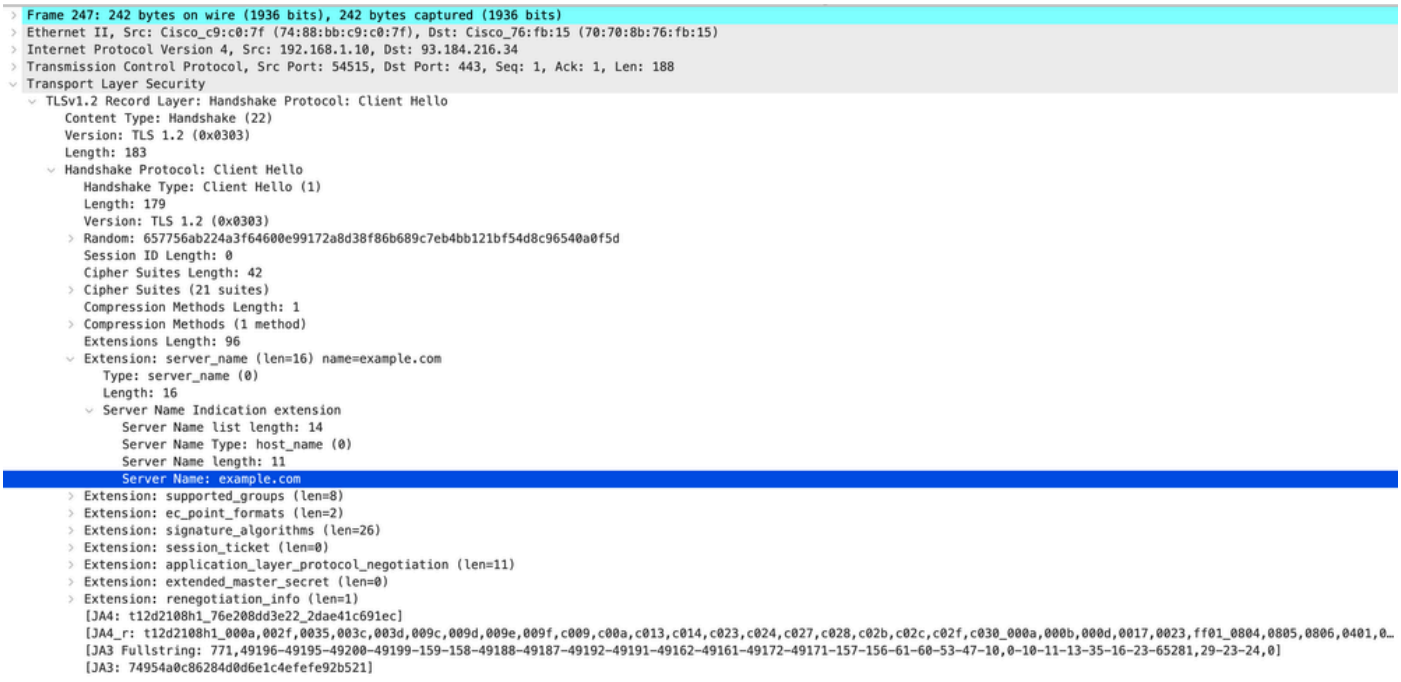
클라이언트에서 오는 트래픽은 프록시 포트가 아닌 TCP 포트 443으로 전달됩니다

- TCP 핸드셰이크.
- TLS 핸드셰이크 클라이언트 Hello - 서버 Hello - 서버 키 교환 - 클라이언트 키 교환
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)

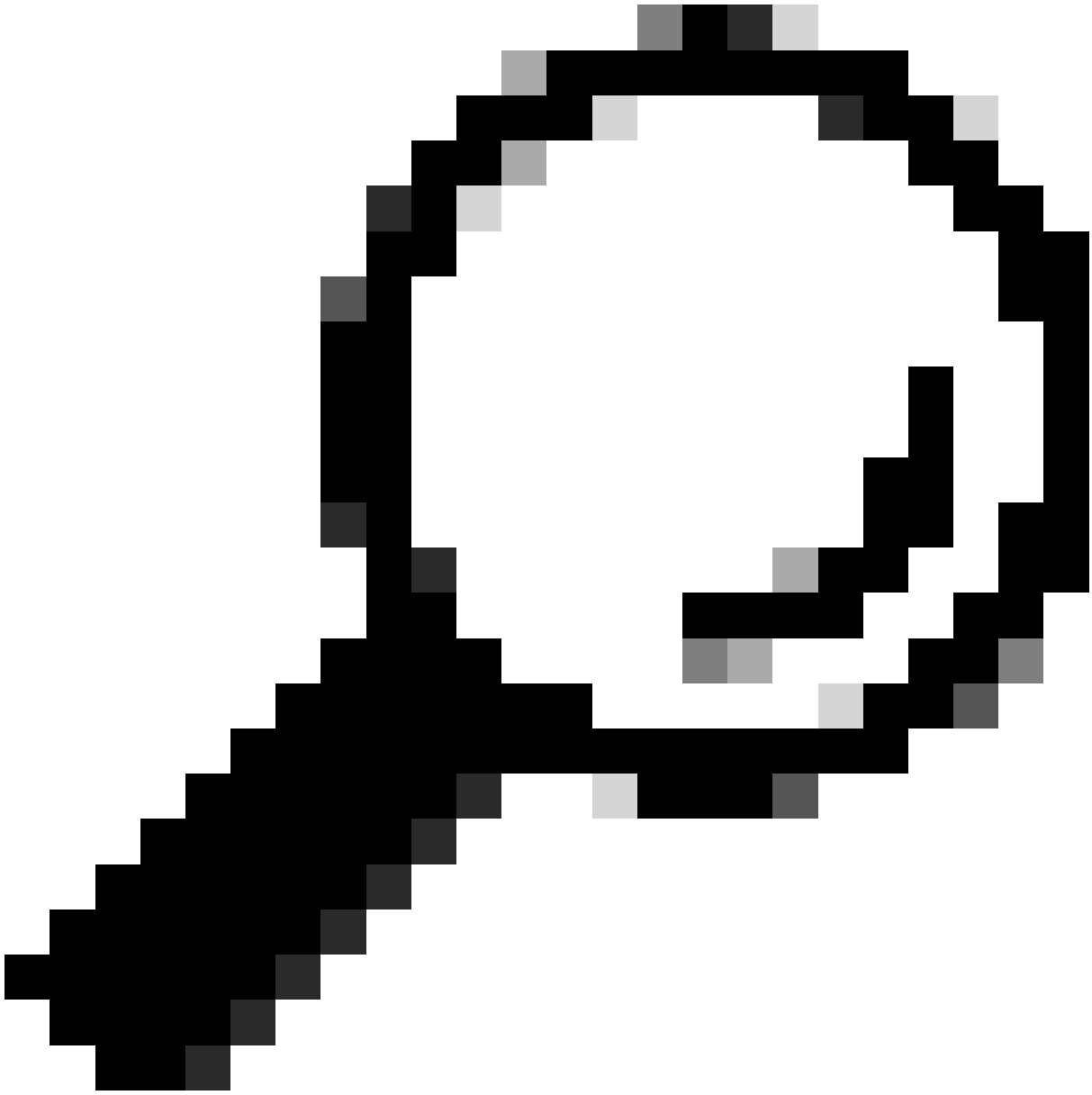
No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
243	2023-12-11 19:36:24.(416304924…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	66	14	54515 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
245	2023-12-11 19:36:24.(107989635…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	14	443 → 54515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
246	2023-12-11 19:36:24.(139334096…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
247	2023-12-11 19:36:24.(307154096…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1…	242	14	Client Hello (SNI=example.com)
248	2023-12-11 19:36:24.(366528476…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=1 Ack=189 Win=65408 Len=0
256	2023-12-11 19:36:24.(251614876…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	1514	14	Server Hello
257	2023-12-11 19:36:24.(195519830…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	1043	14	Certificate, Server Key Exchange, Server Hello Done
258	2023-12-11 19:36:24.(186747024…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=189 Ack=2450 Win=262656 Len=0
259	2023-12-11 19:36:24.(193961315…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1…	147	14	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
260	2023-12-11 19:36:24.(250163651…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=2450 Ack=282 Win=65344 Len=0
261	2023-12-11 19:36:24.(299229398…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	105	14	Change Cipher Spec, Encrypted Handshake Message
262	2023-12-11 19:36:24.(215995475…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1…	157	14	Application Data
263	2023-12-11 19:36:24.(290152051…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=2501 Ack=385 Win=65280 Len=0
264	2023-12-11 19:36:25.529330	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	100	14	Application Data
265	2023-12-11 19:36:25.994499	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	1514	14	Application Data
266	2023-12-11 19:36:25.(413207139…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=385 Ack=4007 Win=262656 Len=0
267	2023-12-11 19:36:25.(201453091…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1…	311	14	Application Data
268	2023-12-11 19:36:25.(181582608…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1…	85	14	Encrypted Alert
269	2023-12-11 19:36:25.(404992054…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=4264 Ack=416 Win=65280 Len=0
270	2023-12-11 19:36:25.(106927132…	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [FIN, ACK] Seq=416 Ack=4264 Win=262400 Len=0
271	2023-12-11 19:36:25.(370433091…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=4264 Ack=417 Win=65280 Len=0
272	2023-12-11 19:36:25.(342494763…	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [FIN, ACK] Seq=4264 Ack=417 Win=65280 Len=0
273	2023-12-11 19:36:25.794348	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=417 Ack=4265 Win=262400 Len=0

이미지 - 클라이언트에서 프록시로 - HTTP - 투명 - 인증 없음

다음은 SNI(Server Name Indication)에서 볼 수 있듯이 클라이언트에서 SWA로의 클라이언트 Hello에 대한 세부 정보입니다. 웹 서버의 URL을 확인할 수 있으며 이 예에서는 www.example.com입니다.



이미지- 클라이언트 Hello - 클라이언트에서 프록시로 - 투명 - 인증 없음

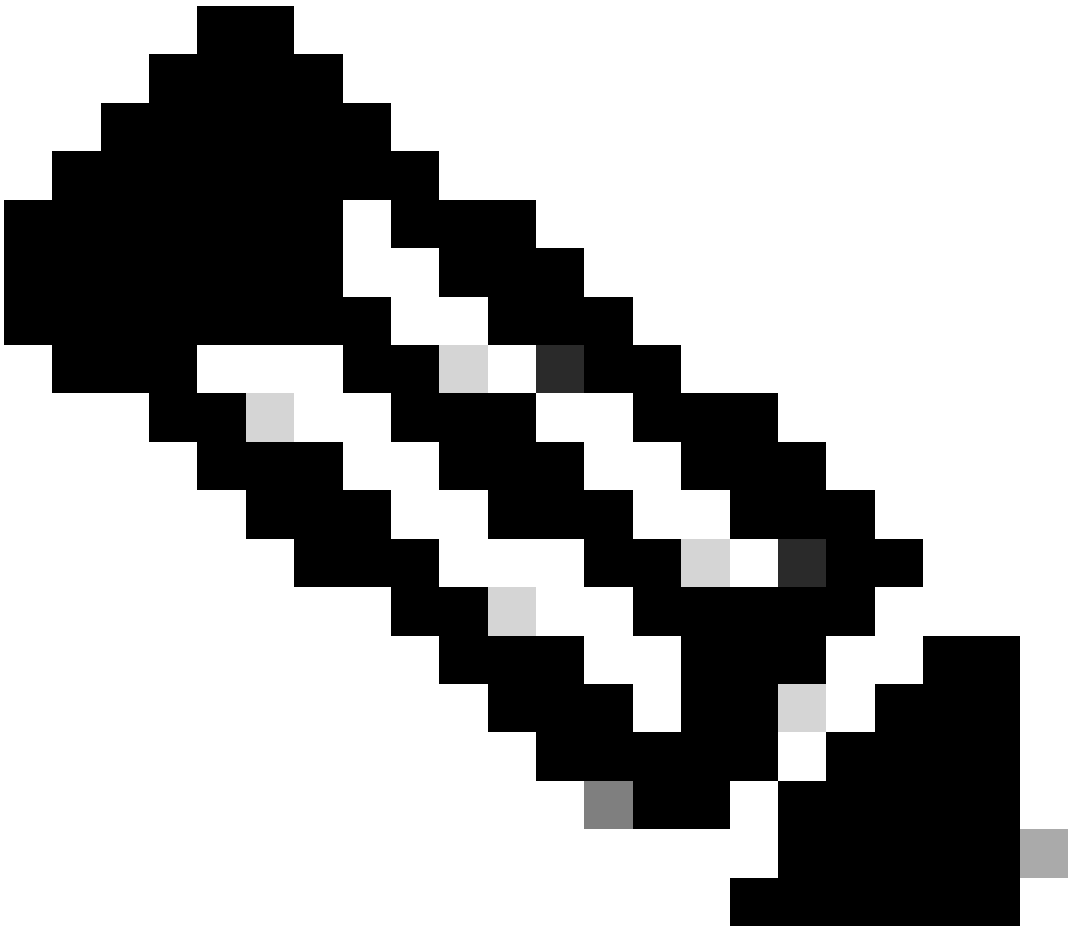


팁: Wireshark에서 이 필터를 사용하여 URL/SNI : tls.handshake.extensions_server_name == "www.example.com"을 검색할 수 있습니다.

다음은 서버 키 교환 샘플입니다.

```
> Frame 257: 1043 bytes on wire (8344 bits), 1043 bytes captured (8344 bits)
> Ethernet II, Src: Cisco_76:fb:15 (70:70:8b:76:fb:15), Dst: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 443, Dst Port: 54515, Seq: 1461, Ack: 189, Len: 989
> [2 Reassembled TCP Segments (2054 bytes): #256(1379), #257(675)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2049
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2045
        Certificates Length: 2042
      v Certificates (2042 bytes)
          Certificate Length: 1098
        v Certificate [truncated]: 30820446308203 2ea003020102021404409073 79f2aad73d32683b716d2a7ddf2b8e2a300d06092a864886f70d01010b05003040310b3009060355040613025553110300e060355040…
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x0440907379f2aad73d32683b716d2a7ddf2b8e2a
            > signature (sha256WithRSAEncryption)
            v issuer: rdnSequence (0)
              v rdnSequence: 4 items (id-at-commonName=CISCOCALo,id-at-organizationalUnitName=IT,id-at-organizationName=wsatest,id-at-countryName=US)
                > RDNSequence item: 1 item (id-at-countryName=US)
                > RDNSequence item: 1 item (id-at-organizationName=wsatest)
                > RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
                > RDNSequence item: 1 item (id-at-commonName=CISCOCALo)
            > validity
            > subject: rdnSequence (0)
            > subjectPublicKeyInfo
            > extensions: 5 items
          > algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted [truncated]: 1db2a57a8bbf4def6b1845eace5a7a17f27704e61b102f13c20a696c076bf3e736283d6cffa6c1d9417865ba7f4d4663bd3677423996e23db7f25d232eaa3110a24e72871d8cf2111d3…
          Certificate Length: 938
        > Certificate [truncated]: 308203a63082028ea003020102020900a447d8363a186f2f300d06092a864886f70d01010b05003040310b3009060355040613025553110300e060355040a13077773617465737431 0…
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

이미지 - 서버 키 교환 - 클라이언트에서 프록시로 - 투명 - 인증 없음



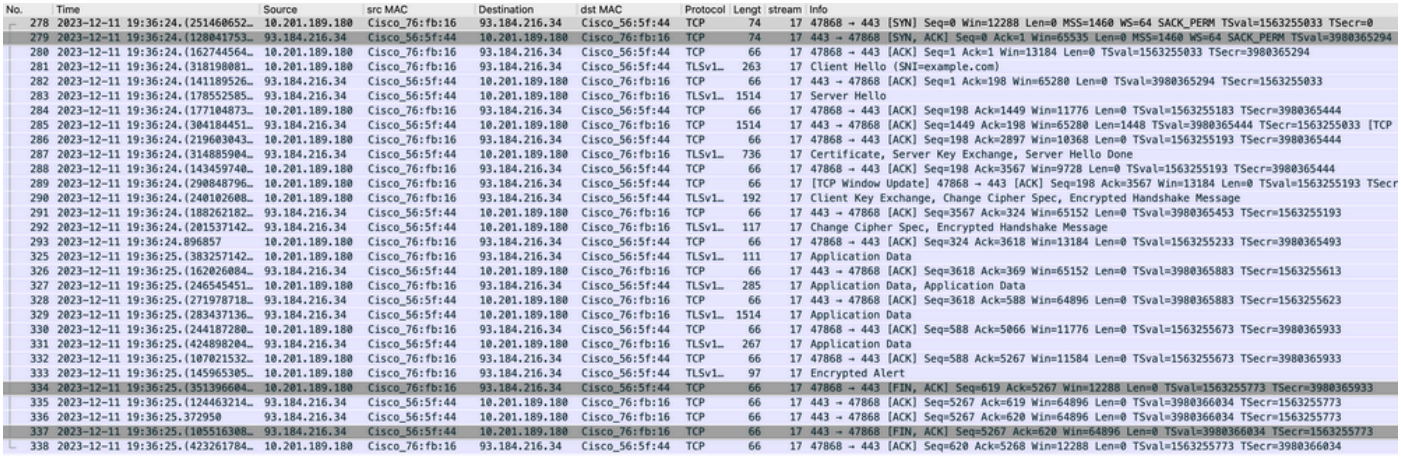
참고: 보시다시피 인증서가 SWA에서 암호 해독 인증서로 구성된 인증서입니다.

SWA 및 웹 서버

네트워크 트래픽은 프록시의 IP 주소와 웹 서버의 IP 주소 간에 발생합니다.

SWA의 트래픽은 프록시 포트가 아니라 TCP 포트 443으로 전달됩니다

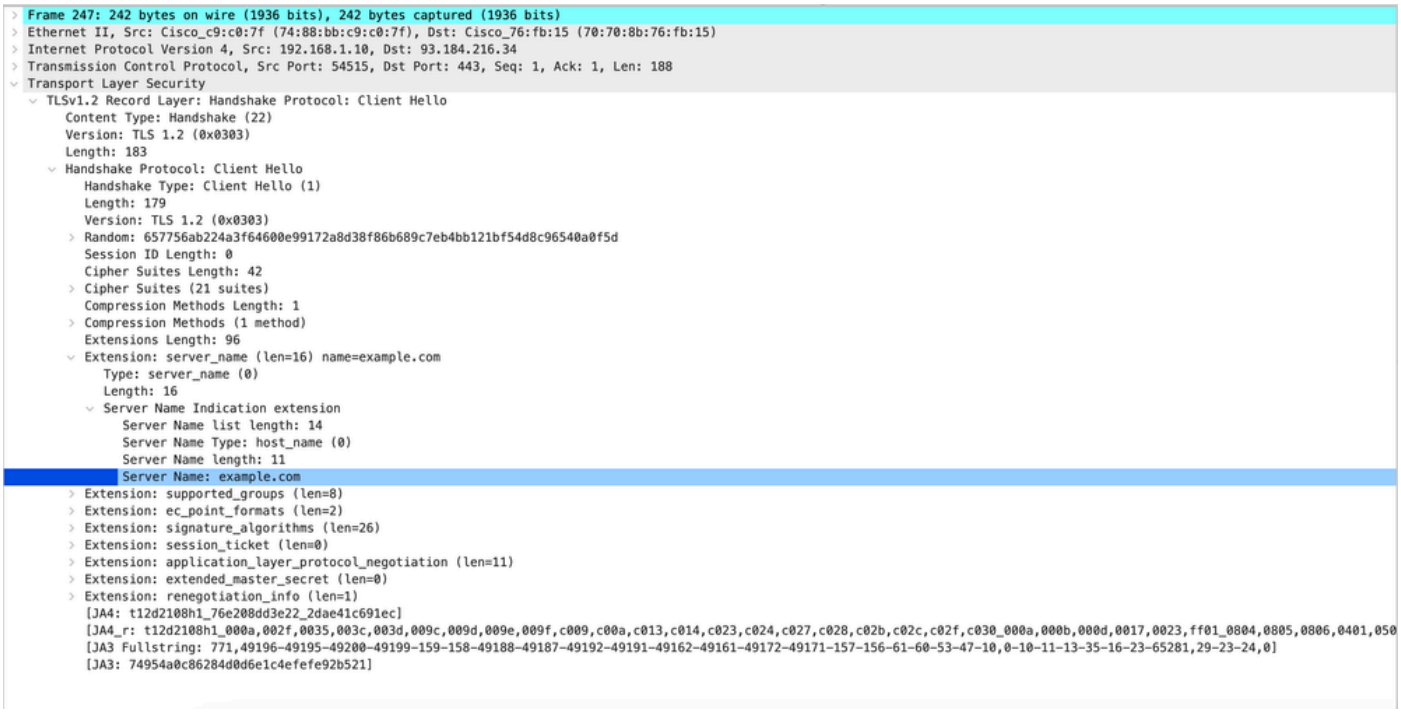
- TCP 핸드셰이크.
- TLS 핸드셰이크 클라이언트 Hello - 서버 Hello - 서버 키 교환 - 클라이언트 키 교환
- 데이터 전송
- TCP 연결 종료(4-Way Handshake)



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
278	2023-12-11 19:36:24.(251460652…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	17	47868 → 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1563255033 TSecr=0
279	2023-12-11 19:36:24.(128041753…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	17	443 → 47868 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3980365294
280	2023-12-11 19:36:24.(162744564…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1563255033 TSecr=3980365294
281	2023-12-11 19:36:24.(318198081…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1…	263	17	Client Hello (SNI=example.com)
282	2023-12-11 19:36:24.(141189526…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=1 Ack=198 Win=65280 Len=0 TSval=3980365294 TSecr=1563255033
283	2023-12-11 19:36:24.(178552585…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1…	1514	17	Server Hello
284	2023-12-11 19:36:24.(177104873…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=198 Ack=1449 Win=11776 Len=0 TSval=1563255183 TSecr=3980365444
285	2023-12-11 19:36:24.(304184451…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	1514	17	443 → 47868 [ACK] Seq=1449 Ack=198 Win=65280 Len=1448 TSval=3980365444 TSecr=1563255033 [TCP
286	2023-12-11 19:36:24.(219603043…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=198 Ack=2897 Win=10368 Len=0 TSval=1563255193 TSecr=3980365444
287	2023-12-11 19:36:24.(314885904…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1…	736	17	Certificate, Server Key Exchange, Server Hello Done
288	2023-12-11 19:36:24.(143459740…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=198 Ack=3567 Win=9728 Len=0 TSval=1563255193 TSecr=3980365444
289	2023-12-11 19:36:24.(290848796…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	[TCP Window Update] 47868 → 443 [ACK] Seq=198 Ack=3567 Win=13184 Len=0 TSval=1563255193 TSecr
290	2023-12-11 19:36:24.(240102608…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1…	192	17	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
291	2023-12-11 19:36:24.(188262182…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=3567 Ack=324 Win=65152 Len=0 TSval=3980365453 TSecr=1563255193
292	2023-12-11 19:36:24.(201537142…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1…	117	17	Change Cipher Spec, Encrypted Handshake Message
293	2023-12-11 19:36:24.896857	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=324 Ack=3618 Win=13184 Len=0 TSval=1563255233 TSecr=3980365493
325	2023-12-11 19:36:25.(383257142…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1…	111	17	Application Data
326	2023-12-11 19:36:25.(162026084…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=3618 Ack=369 Win=65152 Len=0 TSval=3980365883 TSecr=1563255613
327	2023-12-11 19:36:25.(246545451…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1…	285	17	Application Data, Application Data
328	2023-12-11 19:36:25.(271978718…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=3618 Ack=588 Win=64896 Len=0 TSval=3980365883 TSecr=1563255623
329	2023-12-11 19:36:25.(283437136…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1…	1514	17	Application Data
330	2023-12-11 19:36:25.(244187280…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=588 Ack=5066 Win=11776 Len=0 TSval=1563255673 TSecr=3980365933
331	2023-12-11 19:36:25.(424898204…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1…	267	17	Application Data
332	2023-12-11 19:36:25.(107021532…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=588 Ack=5267 Win=11584 Len=0 TSval=1563255673 TSecr=3980365933
333	2023-12-11 19:36:25.(145965305…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1…	97	17	Encrypted Alert
334	2023-12-11 19:36:25.(351396604…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [FIN, ACK] Seq=619 Ack=5267 Win=12288 Len=0 TSval=1563255773 TSecr=3980365933
335	2023-12-11 19:36:25.(124463214…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=5267 Ack=619 Win=64896 Len=0 TSval=3980366034 TSecr=1563255773
336	2023-12-11 19:36:25.372950	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [ACK] Seq=5267 Ack=620 Win=64896 Len=0 TSval=3980366034 TSecr=1563255773
337	2023-12-11 19:36:25.(105516308…	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 → 47868 [FIN, ACK] Seq=5267 Ack=620 Win=64896 Len=0 TSval=3980366034 TSecr=1563255773
338	2023-12-11 19:36:25.(423261784…	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 → 443 [ACK] Seq=620 Ack=5268 Win=12288 Len=0 TSval=1563255773 TSecr=3980366034

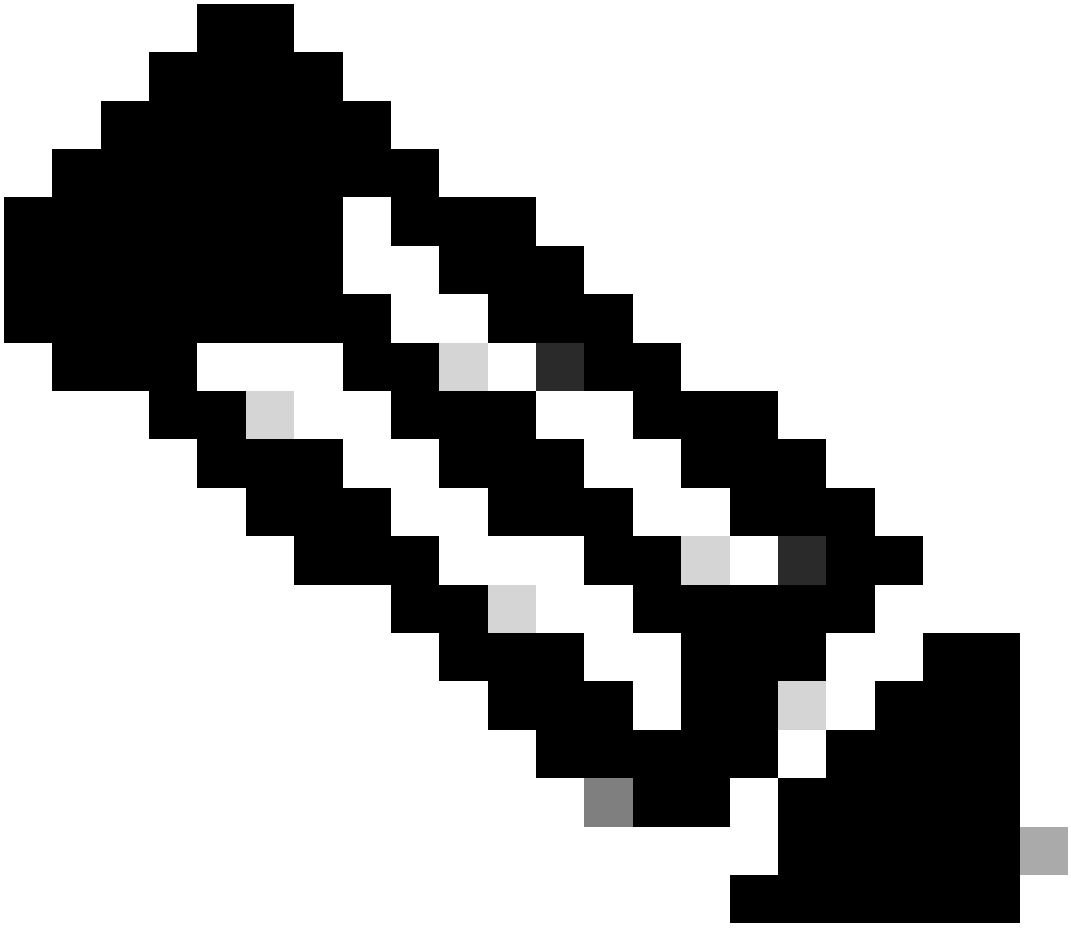
이미지 - 웹 서버에 대한 프록시 - HTTP - 투명 - 인증 없음

다음은 SWA에서 웹 서버로의 Client Hello 샘플입니다

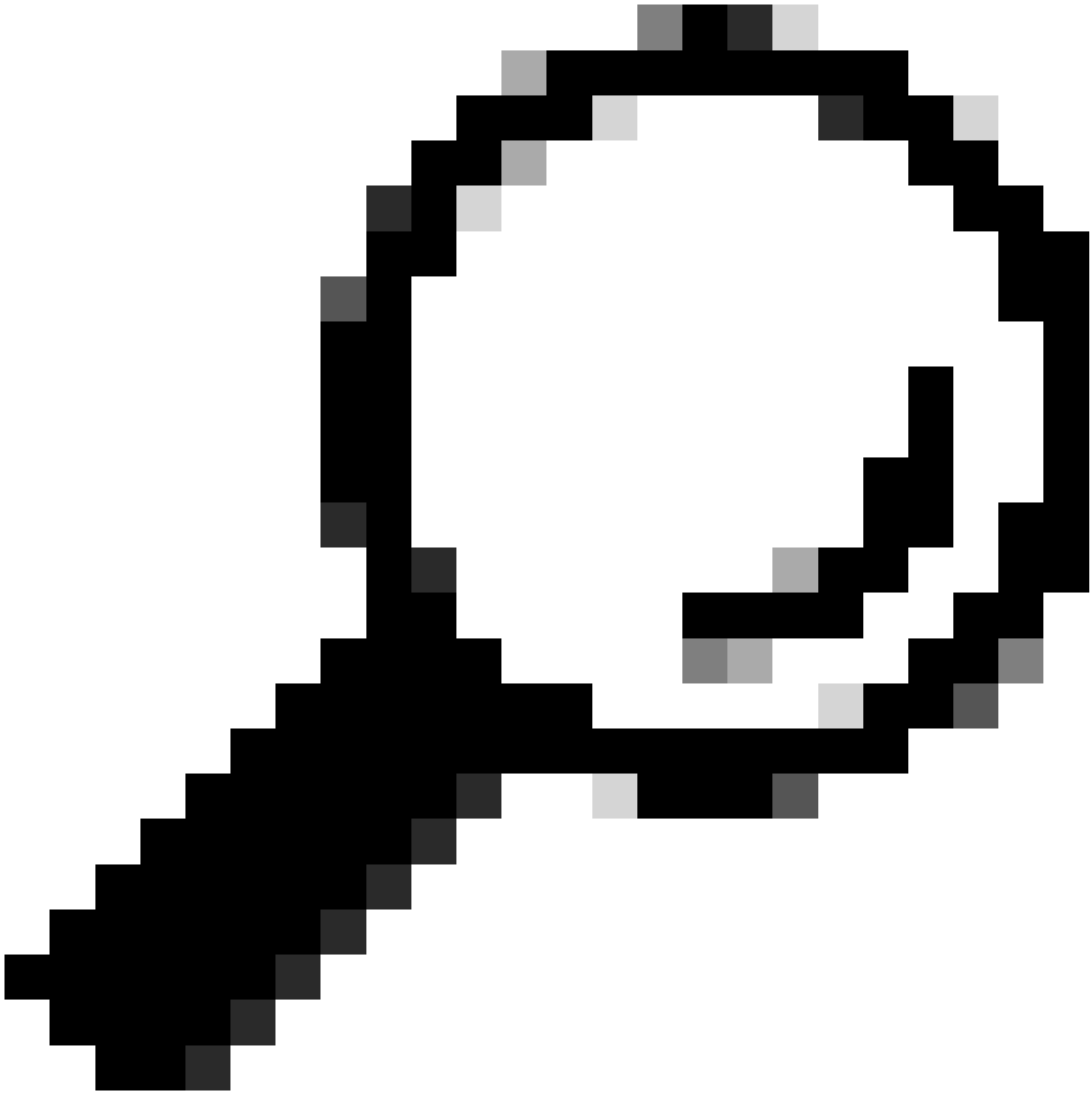


```
> Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54515, Dst Port: 443, Seq: 1, Ack: 1, Len: 188
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 183
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 179
        Version: TLS 1.2 (0x0303)
      > Random: 657756ab224a3f64600e99172a8d38f86b689c7eb4bb121bf54d8c96540a0f5d
        Session ID Length: 0
        Cipher Suites Length: 42
      > Cipher Suites (21 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 96
      v Extension: server_name (len=16) name=example.com
          Type: server_name (0)
          Length: 16
        v Server Name Indication extension
            Server Name list length: 14
            Server Name Type: host_name (0)
            Server Name length: 11
            Server Name: example.com
      > Extension: supported_groups (len=8)
      > Extension: ec_point_formats (len=2)
      > Extension: signature_algorithms (len=26)
      > Extension: session_ticket (len=0)
      > Extension: application_layer_protocol_negotiation (len=11)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
        [JA4: t12d2108h1_76e208dd3e22_2dae41c691ec]
        [JA4_r: t12d2108h1_000a,002f,0035,003c,003d,009c,009d,009e,009f,c009,c00a,c013,c014,c023,c024,c027,c028,c02b,c02c,c02f,c030_000a,000b,000d,0017,0023,ff01_0804,0805,0806,0401,050
        [JA3 Fullstring: 771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-65281,29-23-24,0]
        [JA3: 74954a0c86284d0d6e1c4efefe92b521]
```

이미지- 클라이언트 Hello - 웹 서버에 대한 프록시 - 투명 - 인증 없음



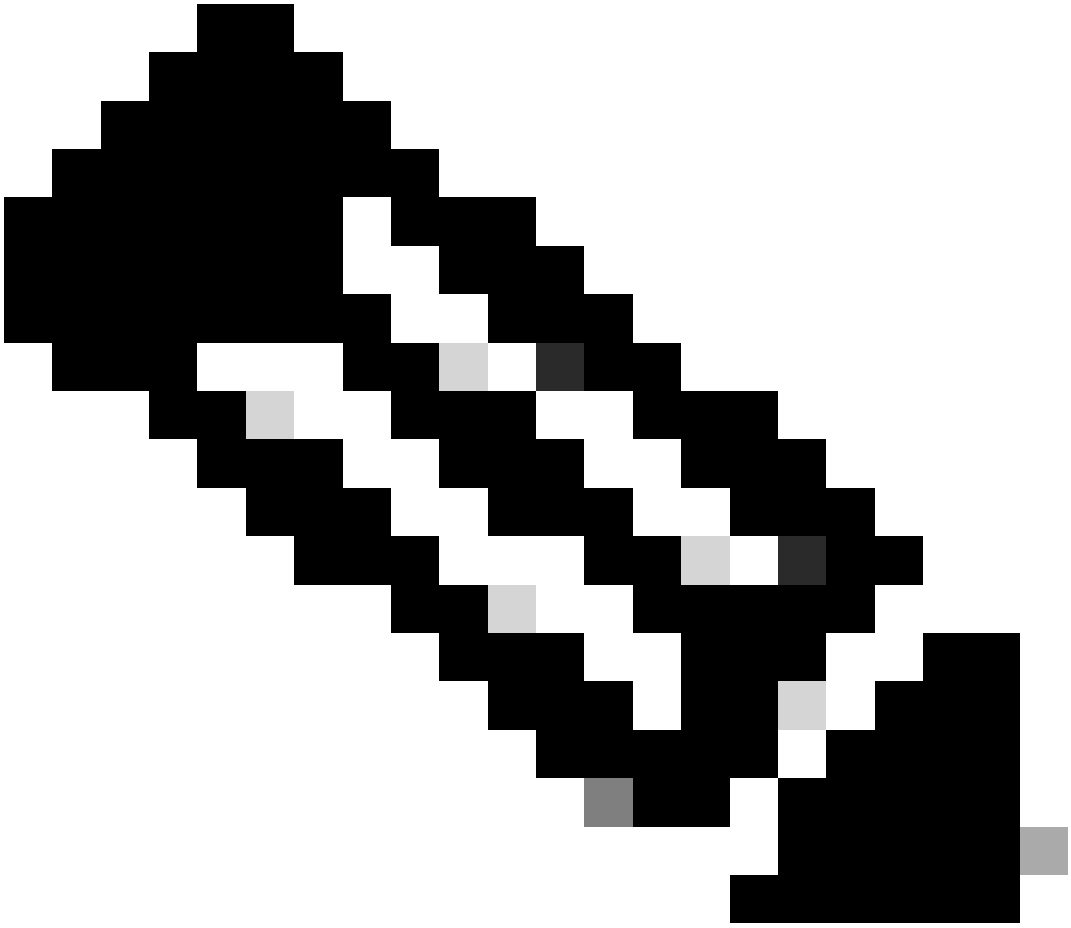
참고: 여기에서 관찰된 암호 그룹은 이 트래픽을 해독하도록 구성된 SWA가 자체 암호를 사용하므로 클라이언트에서 SWA로의 클라이언트 Hello의 암호 그룹과 다릅니다.



팁: Server Key Exchange(서버 키 교환)에서 SWA에서 웹 서버로, 웹 서버 인증서가 나타납니다. 그러나 업스트림 프록시가 SWA에 대한 컨피그레이션을 찾으면 웹 서버 인증서 대신 해당 인증서가 표시됩니다.

다음은 액세스 로그의 예입니다.

```
1702319784.943 558 192.168.1.10 TCP_MISS_SSL/200 0 TCP_CONNECT 10.184.216.34:443 - DIRECT/www.example.c
1702319785.190 247 192.168.1.10 TCP_MISS_SSL/200 1676 GET https://www.example.com:443/ - DIRECT/www.exa
```



참고: HTTPS 트래픽에 대한 투명 구축에서 볼 수 있듯이 Accesslogs에는 2개의 줄이 있습니다. 첫 번째 줄은 트래픽이 암호화되어 있는 경우이며 TCP_CONNECT 및 웹 서버의 IP 주소를 볼 수 있습니다. SWA에서 암호 해독이 활성화된 경우 두 번째 줄에 GET이 포함되고 전체 URL이 HTTPS로 시작합니다. 이는 트래픽이 암호 해독되었고 SWA가 URL을 알고 있음을 의미합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- 액세스 로그의 성능 매개변수 구성 - 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.