了解安全Web设备中的数据包流

目录

简介

先决条件

- 要求
- 使用的组件

不同类型的代理部署

TLS握手

HTTP响应代码

- 1xx :信息
- 2xx:成功
- 3xx：重定向
- 4xx代码：客户端错误
- 5xx:服务器错误

显式部署

- 无身份验证的显式部署中的HTTP流量
  - 客户端和SWA
  - SWA和Web服务器
  - 包含缓存数据的流量
- 无身份验证的显式部署中的HTTP流量
  - 客户端和SWA
  - SWA和Web服务器
  - 直通HTTPS流量

透明部署

- 无身份验证的透明部署中的HTTP流量
  - 客户端和SWA
  - SWA和Web服务器
  - 包含缓存数据的流量
- 无身份验证的透明部署中的HTTP流量
  - 客户端和SWA
  - SWA和Web服务器

相关内容

简介

本文档介绍代理配置网络中的网络流，特别侧重于安全Web设备(SWA)。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本TCP/IP概念。
- 代理设置的基本知识。
- 代理环境中使用的身份验证机制的基本知识。

本文的缩写如下：

TCP：传输控制协议

UDP：用户数据报协议

IP:Internet协议

GRE：通用路由封装

HTTP:超文本传输协议。

HTTPS:安全超文本传输协议.

URL：统一资源定位器

TLS:传输层安全性

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

不同类型的代理部署

TLS握手

当客户端和服务器通过Internet通信时，HTTPS中会发生TLS握手，从而提供安全连接。该过程维护两个通信应用程序之间的隐私和数据完整性。它通过一系列步骤运行，其中客户端和服务器就所有后续传输的加密标准和代码达成一致。握手旨在阻止任何未经授权的访问或第三方操纵。它还对通信方的身份进行身份验证以消除模拟。此过程对于HTTPS至关重要，因为它可确保数据在传输过程中保持安全。

以下是TLS握手的步骤：

1. 客户端问候消息:客户端使用hello消息启动握手过程。此消息包含客户端TLS版本、支持的密码套件以及称为客户端随机的随机字节字符串。
2. 服务器问候消息:服务器以hello消息进行响应。此消息包括服务器选择的TLS版本、选择的密码套件、称为服务器随机的随机字节字符串以及服务器数字证书。如有必要，服务器还会请求客户端数字证书进行相互身份验证。
3. 客户端验证服务器证书：客户端向颁发证书的证书颁发机构检查服务器数字证书。这可以确保客户端正在与合法服务器通信。
4. 准主密钥：客户端发送一个随机字节字符串，称为前主密钥，用于创建会话密钥。客户端使用服务器公钥对此预主密钥进行加密，因此只有服务器才能使用其私钥对其进行解密。
5. 主密钥：客户端和服务器都使用来自问候消息的预主密钥和随机字节字符串来独立计算相同的主密钥。此共享密钥是生成会话密钥的基础。
6. 客户端已完成：客户端发送“已完成”消息，该消息使用会话密钥加密，以发出握手客户端部分的完成信号。
7. 服务器已完成：服务器发送Finished消息（也使用会话密钥加密），以通知服务器部分的握手完成。

HTTP响应代码

1xx :信息

代码	详细信息
100继续	通常在ICAP协议中看到。这是信息性响应，让客户端知道它可以继续发送数据。对于ICAP服务（例如病毒扫描），服务器只能看到前x个字节。当扫描完第一组字节并且未检测到病毒时，它会发送100 Continue以让客户端知道发送对象的其余部分。

2xx:成功

代码	详细信息
200正常	最常见的响应代码。这表示请求成功而没有任何问题。

3xx：重定向

代码	详细信息
301永久重定向	这是永久重定向，当您重定向到www子域时，可以看到此代码。
302临时重定向	这是临时重定向。指示客户端对Location:报头。
304未修改	这是对GET If-modified-since(GIMS)的响应。 这实际上是一个标准HTTP GET，包括报头If-modified-since:<date>。此标头告知服务器，客户端在其本地缓存中有一个所请求对象的副本，其中包括提取对象的日期。如果自该日期以来修改了对象，则服务器将以200 OK和对象的新副本进行响应。如果自获取日期以来对象未更改，服务器将发回304 Not Modified响应。
307身份验证重定向	这在透明代理部署中最为常见，当代理服务器配置为对请求进行身份验证并将请求重定向到另一个URL以对用户进行身份验证时，

4xx代码：客户端错误

代码	详细信息
400错误请求	这表明HTTP请求存在问题，因为它不符合正确的语法。可能的原因可能包括单个行上的多个报头、报头中的空格或URI中缺少HTTP/1.1等。有关正确的语法，请参阅RFC 2616。
401未授权 需要Web服务器身份验证	访问请求的对象需要身份验证。401代码用于与目标Web服务器进行身份验证。当SWA以透明模式运行并在代理上启用身份验证时，它会向客户端返回401，因为设备将自身显示为原始内容服务器(OCS)。 www-authenticate中详细介绍了可以使用的身份验证方法：HTTP响应报头。这将通知客户端服务器是否请求NTLM、基本或其他形式的身份验证。
403被拒绝	客户端无法访问请求的对象。多种原因可能导致服务器拒绝对象访问

	。服务器通常在HTTP数据或HTML响应中提供原因说明。
404未找到	服务器上不存在请求的对象。
需要407代理身份验证	这与401相同，不同之处在于它专门用于代理而不是OCS的身份验证。仅当请求被显式发送到代理时才发送此消息。 当SWA配置为透明代理时，无法将407发送到客户端，因为客户端不知道该代理存在。如果是这种情况，客户端很可能使用FIN或RST作为TCP套接字。

5xx:服务器错误

代码	详细信息
501内部服务器错误	通用Web服务器故障。
502错误网关	当充当网关或代理的服务器从入站服务器收到无效响应时发生。它表示网关从上游或源服务器收到了不适当的响应。
503服务不可用	表示由于临时过载或计划的维护，服务器当前无法处理请求。这意味着服务器暂时停止服务，但一段时间后可以再次使用。
504网关超时	表示客户端或代理未收到来自它尝试访问以加载网页或完成浏览器另一请求的Web服务器的及时响应。这通常意味着上游服务器发生故障。

显式部署

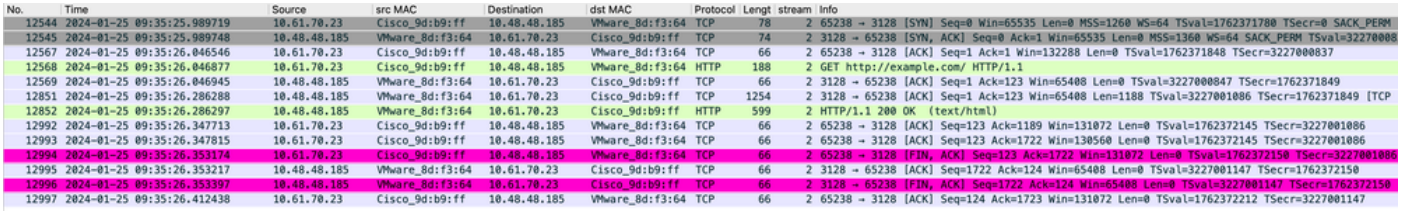
无身份验证的显式部署中的HTTP流量

客户端和SWA

网络流量在客户端的IP地址和SWA代理接口的IP地址之间传输（通常是P1接口，但也可以是P2或管理接口，具体取决于代理配置）。

来自客户端的流量发往TCP端口80或3128到SWA（默认SWA代理端口为TCP 80和3128，在本例中使用端口3128）

- TCP握手。
- 从客户端获取HTTP（目标IP = SWA IP ，目标端口= 3128）
- 来自代理的HTTP响应（源IP = SWA）
- 数据传输
- TCP连接终止（4次握手）



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

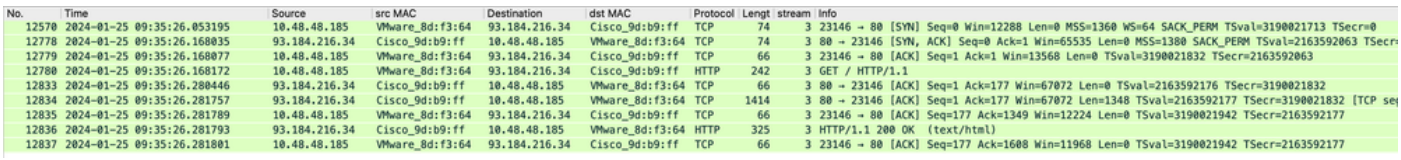
Image-Client to SWA，HTTP显式模式

SWA和Web服务器

网络流量发生在代理的IP地址和Web服务器的IP地址之间。

来自SWA的流量发往TCP端口80，并且来自随机端口（不是代理端口）

- TCP握手。
- 从代理获取HTTP（目标IP = Web服务器，目标端口= 80）
- 来自Web服务器的HTTP响应（源IP =代理服务器）
- 数据传输
- TCP连接终止（4次握手）



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

图像 — HTTP-SWA到Web服务器 — 显式 — 无缓存

以下是来自客户端的HTTP Get示例。

```
> 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]
```

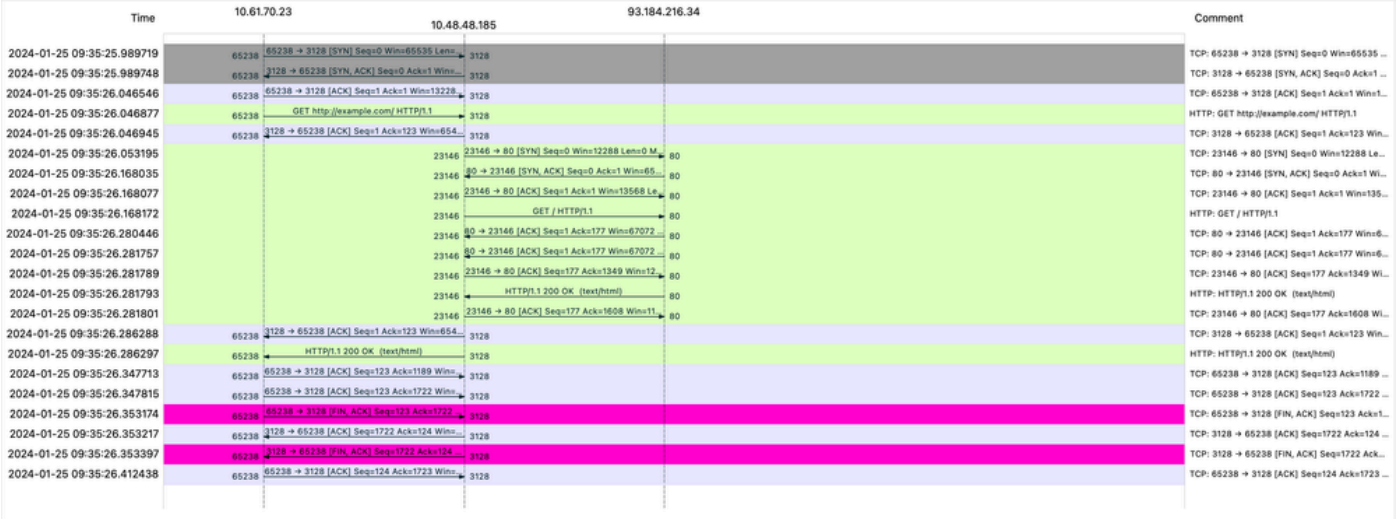
映像 — SWA HTTP GET的客户端 — Explicit

这表示从客户端到SWA、然后到Web服务器、最后返回客户端的整个流量流。

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

映像 — 所有流量HTTP显式 — 无缓存

注意：每个流量流都以不同的颜色区分；从客户端到SWA的流是一种颜色，而从SWA到Web服务器的流是另一种颜色。



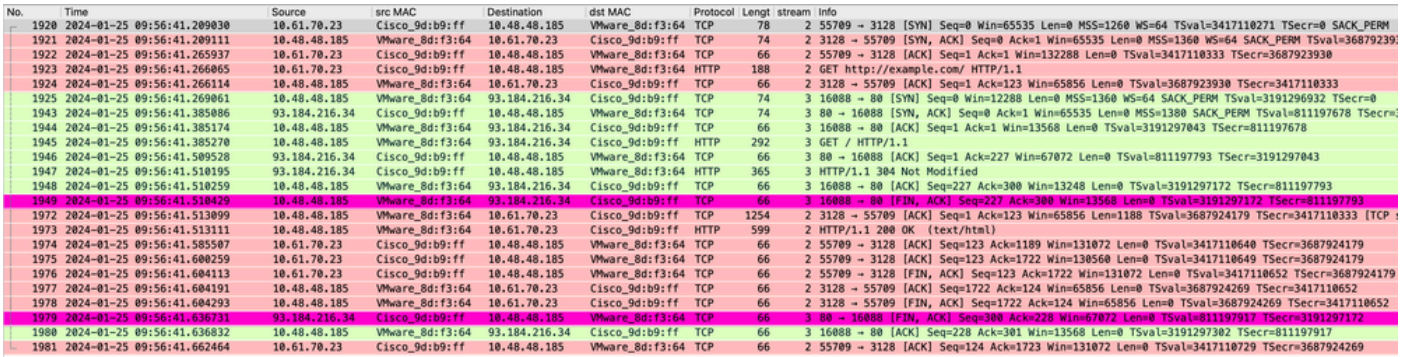
图像 — 流量HTTP显式 — 无缓存

以下是访问日志的示例：

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

包含缓存数据的流量

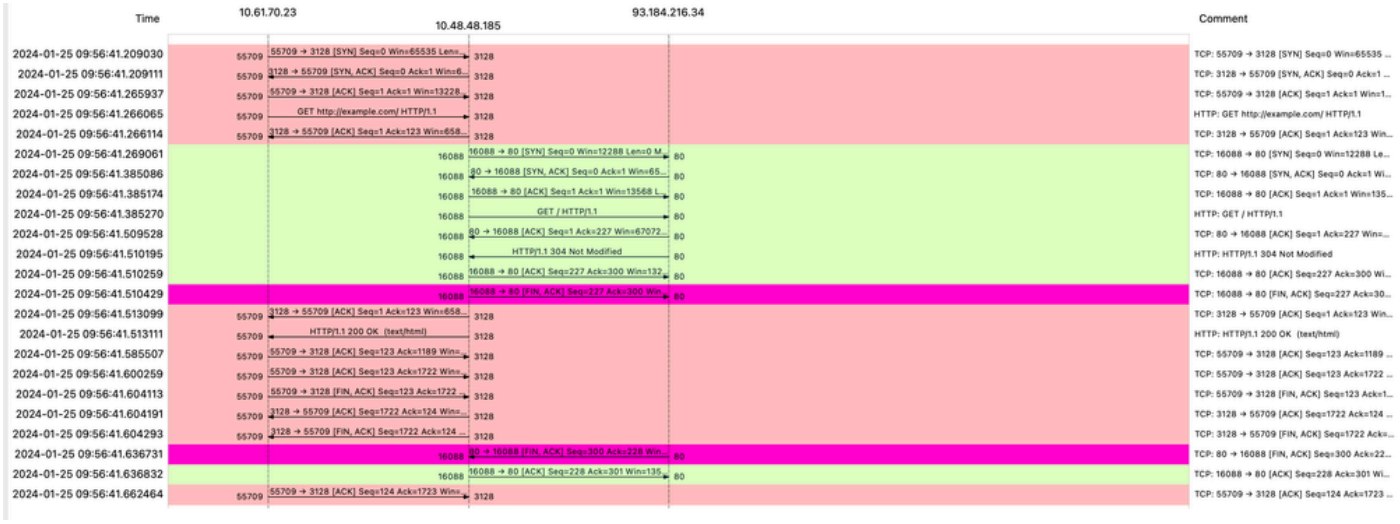
当数据位于SWA缓存中时，这表示从客户端到SWA的整个流量流。



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
1920	2024-01-25 09:56:41.209030	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	78	2	55709 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=3417110271 TSecr=0 SACK_PERM
1921	2024-01-25 09:56:41.209111	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	74	2	3128 → 55709 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=64 SACK_PERM TSval=368792391
1922	2024-01-25 09:56:41.265937	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=3417110333 TSecr=3687923930
1923	2024-01-25 09:56:41.266065	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
1924	2024-01-25 09:56:41.266114	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65856 Len=0 TSval=3687923930 TSecr=3417110333
1925	2024-01-25 09:56:41.269061	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	74	3	16088 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1360 WS=64 SACK_PERM TSval=3191296932 TSecr=0
1943	2024-01-25 09:56:41.385086	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	74	3	80 → 16088 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=811197678 TSecr=
1944	2024-01-25 09:56:41.385174	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=1 Ack=1 Win=13568 Len=0 TSval=3191297043 TSecr=811197678
1945	2024-01-25 09:56:41.385270	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	HTTP	292	3	GET / HTTP/1.1
1946	2024-01-25 09:56:41.509528	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 16088 [ACK] Seq=1 Ack=227 Win=67072 Len=0 TSval=811197793 TSecr=3191297043
1947	2024-01-25 09:56:41.510195	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	365	3	HTTP/1.1 304 Not Modified
1948	2024-01-25 09:56:41.510259	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=227 Ack=300 Win=13248 Len=0 TSval=3191297172 TSecr=811197793
1949	2024-01-25 09:56:41.510429	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [FIN, ACK] Seq=227 Ack=300 Win=13568 Len=0 TSval=3191297172 TSecr=811197793
1972	2024-01-25 09:56:41.513099	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	1254	2	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65856 Len=1188 TSval=3687924179 TSecr=3417110333 [TCP
1973	2024-01-25 09:56:41.513111	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)
1974	2024-01-25 09:56:41.585507	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=123 Ack=1189 Win=131072 Len=0 TSval=3417110640 TSecr=3687924179
1975	2024-01-25 09:56:41.600259	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=123 Ack=1722 Win=130560 Len=0 TSval=3417110649 TSecr=3687924179
1976	2024-01-25 09:56:41.604113	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [FIN, ACK] Seq=123 Ack=1722 Win=131072 Len=0 TSval=3417110652 TSecr=3687924179
1977	2024-01-25 09:56:41.604191	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [ACK] Seq=1722 Ack=124 Win=65856 Len=0 TSval=3687924269 TSecr=3417110652
1978	2024-01-25 09:56:41.604293	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [FIN, ACK] Seq=1722 Ack=124 Win=65856 Len=0 TSval=3687924269 TSecr=3417110652
1979	2024-01-25 09:56:41.636731	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 16088 [FIN, ACK] Seq=300 Ack=228 Win=67072 Len=0 TSval=811197917 TSecr=3191297172
1980	2024-01-25 09:56:41.636832	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=228 Ack=301 Win=13568 Len=0 TSval=3191297302 TSecr=811197917
1981	2024-01-25 09:56:41.662464	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=124 Ack=1723 Win=131072 Len=0 TSval=3417110729 TSecr=3687924269

图像 — HTTP显式缓存数据

注意：如您所见，Web服务器返回HTTP响应304:未修改缓存。（在本示例中，数据包编号为1947。）



图像 — 带缓存的显式HTTP流

以下是HTTP响应304的示例。

```
> 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/]
```

图像 — HTTP显式304响应

以下是访问日志的示例：

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

无身份验证的显式部署中的HTTP流量

客户端和SWA

网络流量在客户端的IP地址和SWA代理接口的IP地址之间传输（通常是P1接口，但也可以是P2或管理接口，具体取决于代理配置）。

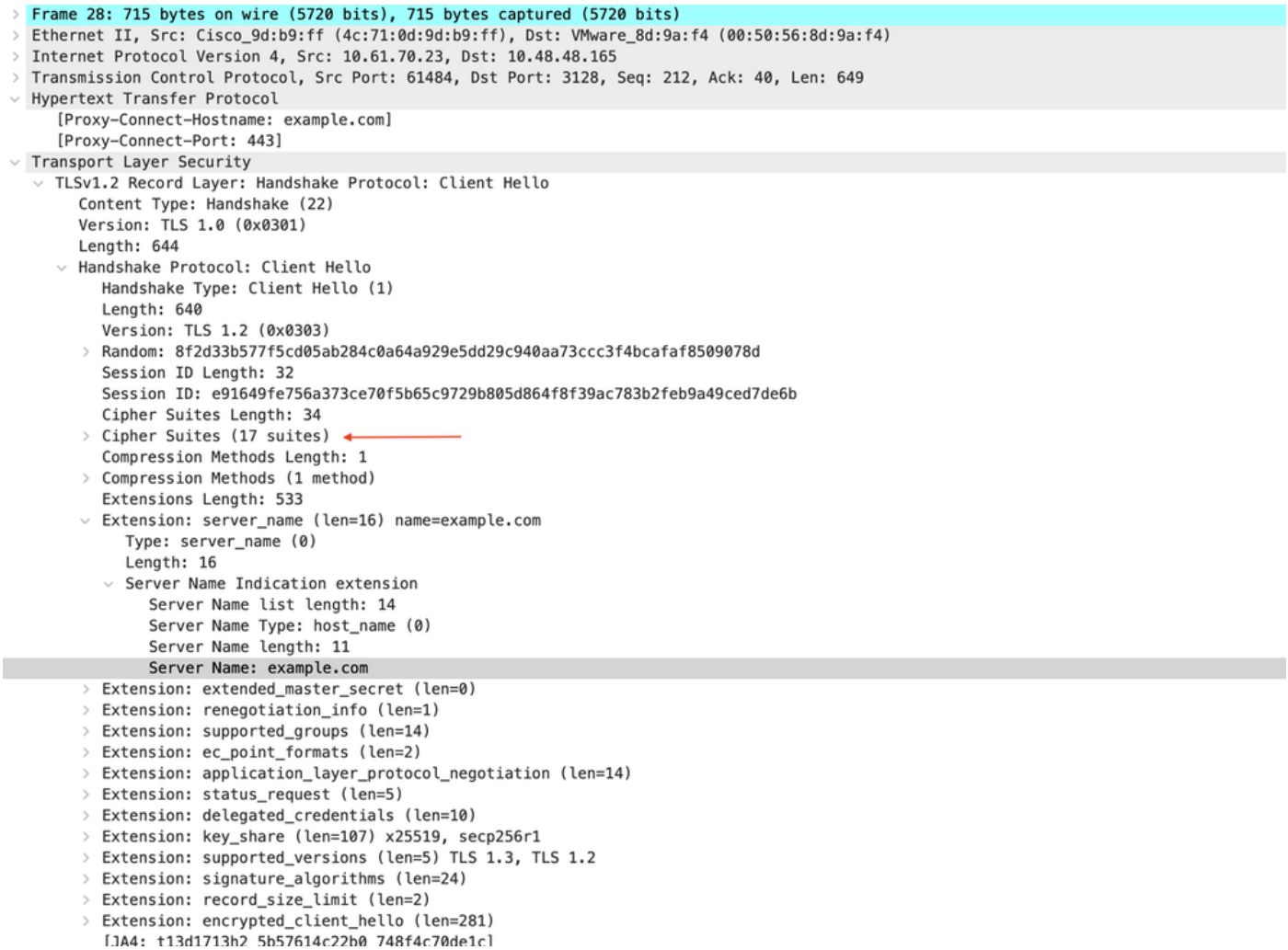
来自客户端的流量发往TCP端口80或3128到SWA（在本例中，默认SWA代理端口为TCP 80和3128）。使用端口3128)。

- TCP握手。
- 来自客户端的HTTP连接（目标IP = SWA，目标端口= 3128）
- 来自代理的HTTP响应（源IP = SWA）
- 使用URL的SNI的客户端Hello（源IP =客户端）
- 服务器Hello（源IP = SWA）
- 服务器密钥交换（源IP = SWA）
- 客户端密钥交换（源IP =客户端）
- 数据传输
- TCP连接终止（4次握手）

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

映像 — SWA的HTTPS客户端 — 显式 — 无缓存

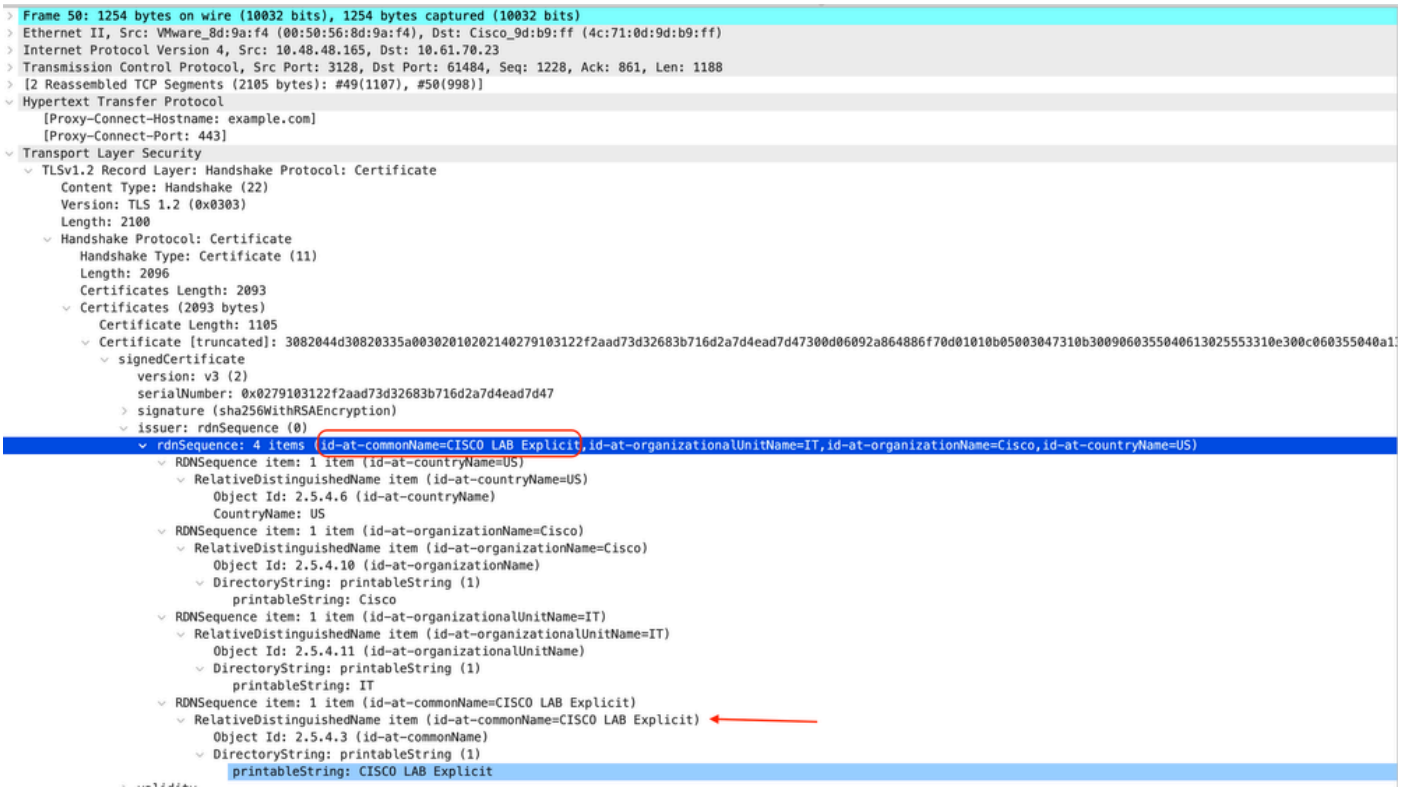
以下是从客户端到SWA的客户端Hello的详细信息，如您在服务器名称指示(SNI)中看到的Web服务器的URL，在本例中为www.example.com，客户端通告17个密码套件：



映像 — HTTPS客户端hello — 显式 — 客户端到SWA

提示：您可以在Wireshark中使用此过滤器搜索URL/SNI:tls.handshake.extensions_server_name == "www.example.com"

以下是SWA发送到客户端的证书示例。



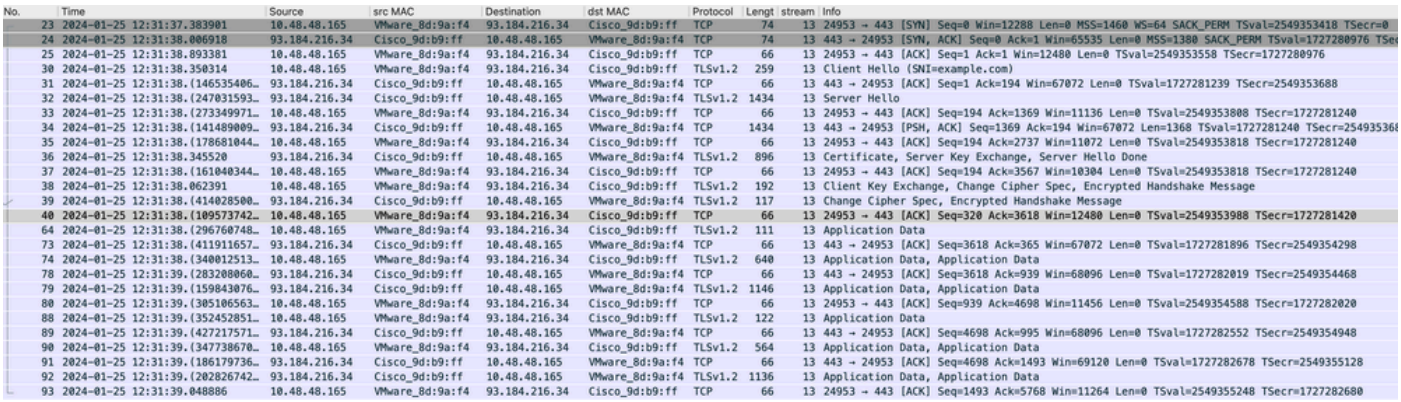
映像 — HTTPS证书 — 显式 — SWA到客户端

SWA和Web服务器

网络流量发生在代理的IP地址和Web服务器的IP地址之间。

来自SWA的流量发往TCP端口443（不是代理端口）

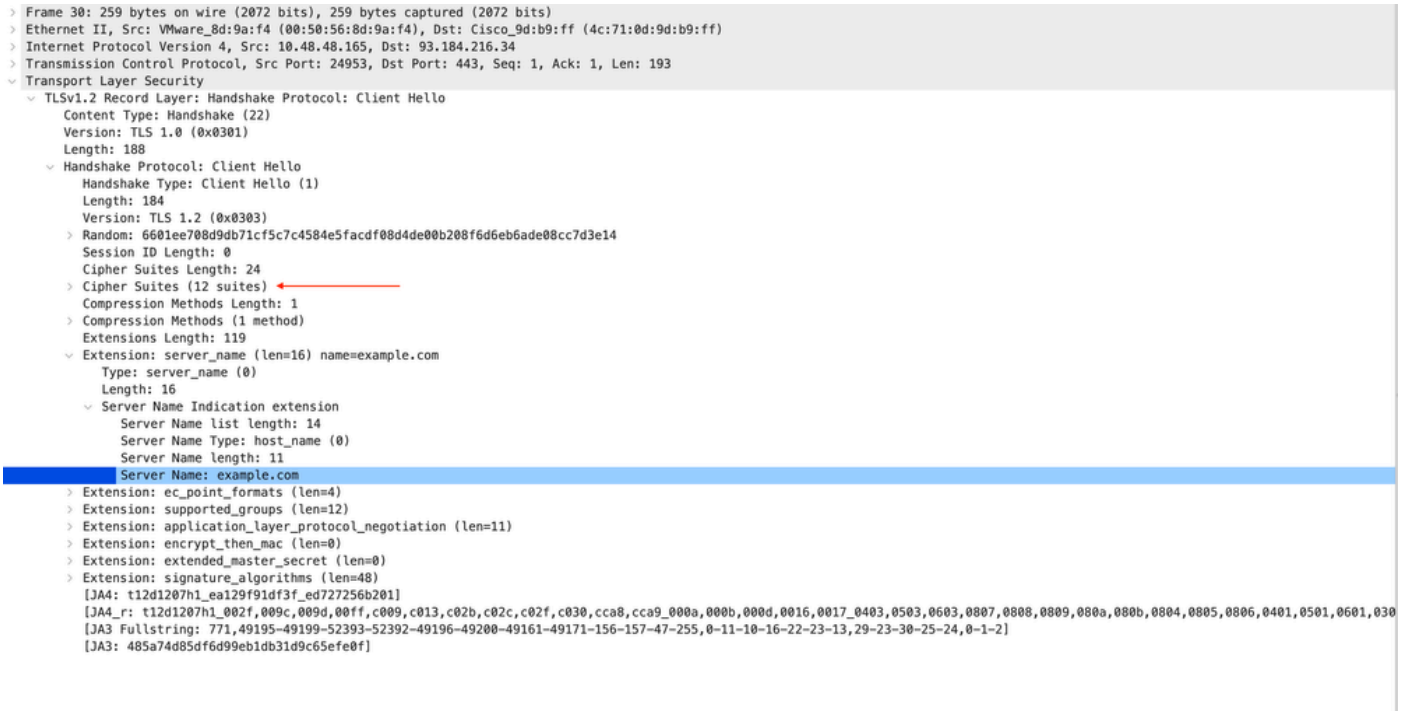
- TCP握手
- 客户端Hello（目标IP = Web服务器，目标端口= 443）
- 服务器Hello（源IP = Web服务器）
- 数据传输
- TCP连接终止（4次握手）



No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
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 TSecr=0
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=1727280976 TSe
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
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=254935368
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
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
88	2024-01-25 12:31:39.(352452851…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	122	13	Application Data
89	2024-01-25 12:31:39.(427217571…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=4698 Ack=995 Win=68096 Len=0 TSval=1727282552 TSecr=2549354948
90	2024-01-25 12:31:39.(347738670…	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	564	13	Application Data, Application Data
91	2024-01-25 12:31:39.(186179736…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=4698 Ack=1493 Win=69120 Len=0 TSval=1727282678 TSecr=2549355128
92	2024-01-25 12:31:39.(202826742…	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	1136	13	Application Data, Application Data
93	2024-01-25 12:31:39.048886	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=1493 Ack=5768 Win=11264 Len=0 TSval=2549355248 TSecr=1727282680

映像 — HTTPS — 显式 — SWA到Web服务器

以下是从SWA到Web服务器的客户端Hello的详细信息，因为您可以看到SWA通告了12个密码套件：



图像 — HTTPS客户端Hello - SWA到Web服务器 — 无聊天

注意：此处观察到的密码套件与客户端到SWA的客户端Hello中的密码套件不同，因为配置为解密此流量的SWA使用自己的密码。

提示：在从SWA到Web服务器的服务器密钥交换中，会显示Web服务器证书。但是，如果上游代理找到您的SWA的配置，则会显示其证书而不是Web服务器证书。

以下是来自客户端的HTTP CONNECT示例。

```
> 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]
```

映像 — 客户端HTTP连接

这表示从客户端到SWA、然后到Web服务器、最后返回客户端的整个流量流。

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.(173832956…	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

映像 — 完整HTTPS显式 — 无缓存



注意：每个流量流都以不同的颜色区分；从客户端到SWA的流是一种颜色，而从SWA到Web服务器的流是另一种颜色。



映像 — HTTPS流 — 显式 — 无缓存

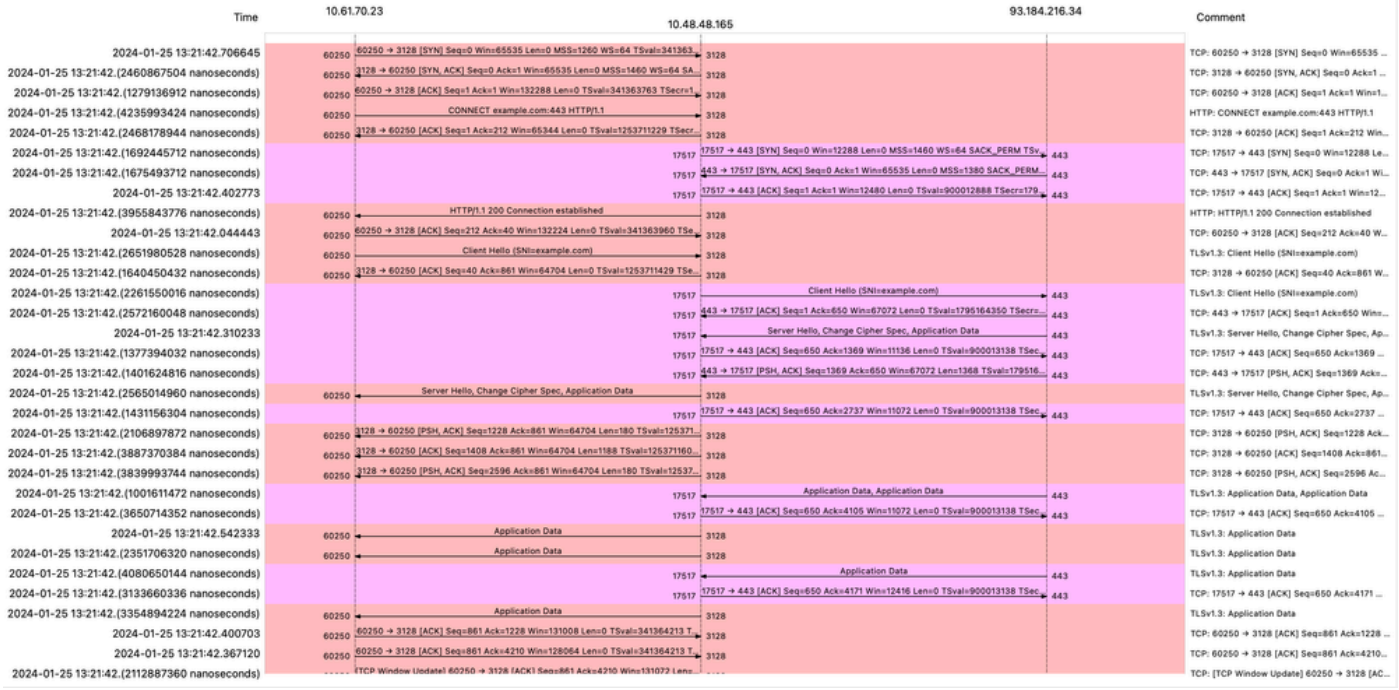
以下是访问日志的示例：

```
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.exam
```

注意：正如您在HTTPS流量的透明部署中所看到的，Accesslogs中有2行，第一行是流量被加密时，您可以看到CONNECT，Web服务器的URL以tunnel://开头。如果在SWA中启用解密，则第二行包含GET，整个URL以HTTPS开头，这意味着流量已解密。

直通HTTPS流量

如果您将SWA配置为通过流量，则以下是总流量：



图像 — HTTPS直通 — 显式 — 流

以下是从SWA到Web服务器的客户端Hello示例：

```
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)
```

图像 — HTTPS直通 — 显式 — SWA到Web服务器 — 客户端hello

与从客户端到SWA的客户端Hello相同：

```
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)
```

映像 — HTTPS直通 — 显式 — 客户端到SWA — 客户端hello

以下是访问日志示例：

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



注意：如您所见，它只是单行，操作为PASSTHRU。

透明部署

无身份验证的透明部署中的HTTP流量

客户端和SWA

网络流量在客户端的IP地址和Web服务器的IP地址之间传输。

来自客户端的流量发往TCP端口80（不是代理端口）

- TCP握手
- 从客户端获取HTTP（目标IP = Web服务器，目标端口= 80）
- 来自代理的HTTP响应（源IP = Web服务器）
- 数据传输
- TCP连接终止（4次握手）

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

映像 — 客户端到代理 — HTTP — 透明 — 无身份验证

以下是来自客户端的HTTP Get示例。

```
> 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]
```

映像 — 客户端到代理 — HTTP — 透明 — 无身份验证 — 客户端HTTP Get

SWA和Web服务器

网络流量发生在代理的IP地址和Web服务器的IP地址之间。

来自SWA的流量发往TCP端口80（不是代理端口）

- TCP握手
- 从代理获取HTTP（目标IP = Web服务器，目标端口= 80）
- 来自Web服务器的HTTP响应（源IP =代理服务器）
- 数据传输
- TCP连接终止（4次握手）

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

图像 — 代理和Web服务器 — HTTP — 透明 — 无身份验证

以下是HTTP Get from Proxy示例。

```
> 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]
```

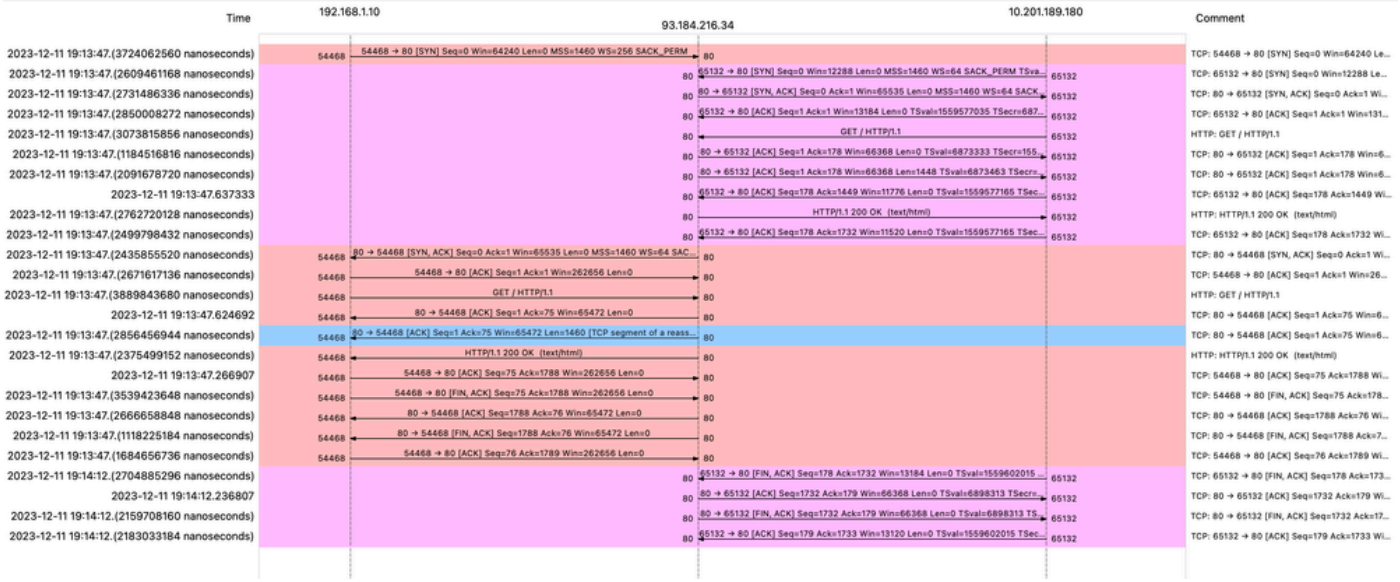
图像 — Web服务器的代理 — HTTP — 透明 — 无身份验证 — Proxy HTTP Get

这表示从客户端到SWA、然后到Web服务器、最后返回客户端的整个流量流。

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

图像 — 总流量 — HTTP — 透明 — 无身份验证

注意：每个流量流都以不同的颜色区分；从客户端到SWA的流是一种颜色，而从SWA到Web服务器的流是另一种颜色。



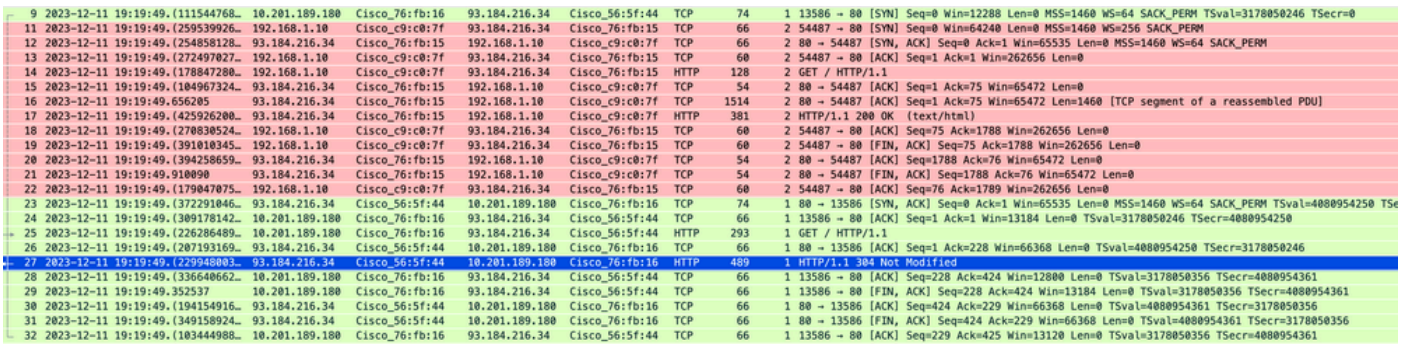
映像 — WCCP HTTP流

以下是访问日志的示例：

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

包含缓存数据的流量

当数据位于SWA缓存中时，这表示从客户端到SWA的整个流量流。



映像 — 缓存 — 总流量 — HTTP — 透明 — 无身份验证

注意：如您所见，Web服务器返回HTTP响应304:未修改缓存。（在本示例中，数据包编号为27。）

以下是HTTP响应304的示例。

```
> 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/]
```

映像 — 缓存 — HTTP响应304 - HTTP — 透明 — 无身份验证

以下是访问日志的示例：

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

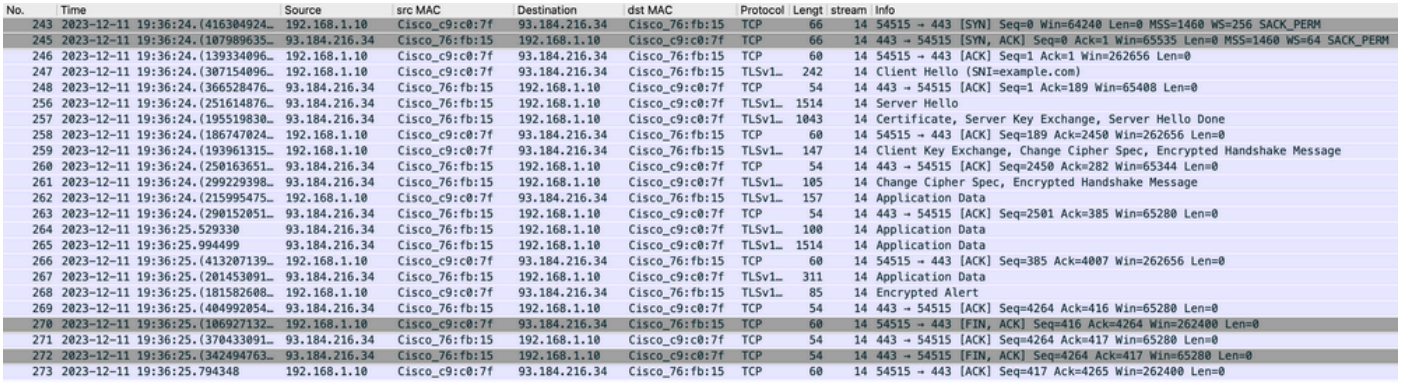
无身份验证的透明部署中的HTTP流量

客户端和SWA

网络流量在客户端的IP地址和Web服务器的IP地址之间传输。

来自客户端的流量发往TCP端口443（不是代理端口）

- TCP握手
- TLS握手客户端Hello — 服务器Hello — 服务器密钥交换 — 客户端密钥交换
- 数据传输
- TCP连接终止（4次握手）



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

映像 — 客户端到代理 — HTTP — 透明 — 无身份验证

以下是从客户端到SWA的客户端Hello的详细信息，如您在服务器名称指示(SNI)中看到的Web服务器的URL，在本例中为www.example.com。



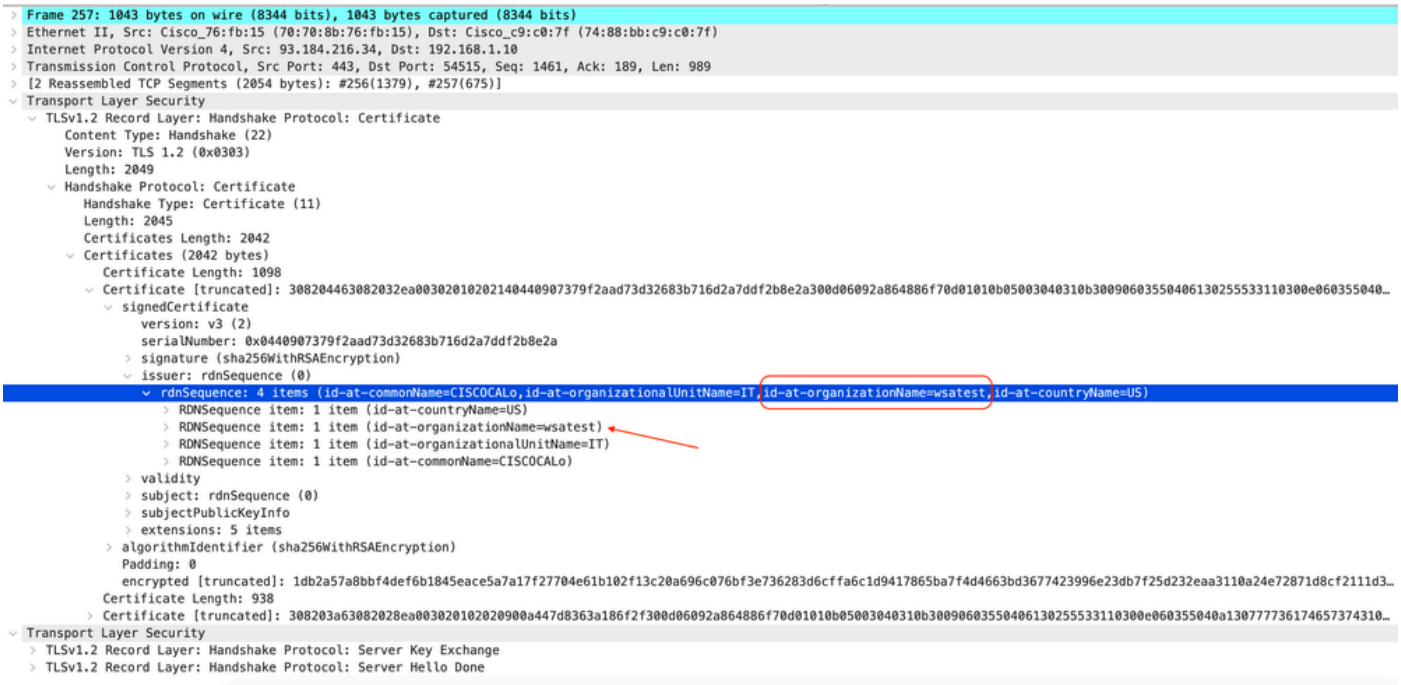
```
> Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54515, Dst Port: 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_0804,0805,0806,0401,0…
        [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]
```

图像 — 客户端Hello — 客户端到代理 — 透明 — 无身份验证



提示：您可以在Wireshark中使用此过滤器搜索URL/SNI:tls.handshake.extensions_server_name == "www.example.com"

以下是服务器密钥交换的示例。



映像 — 服务器密钥交换 — 客户端到代理 — 透明 — 无身份验证

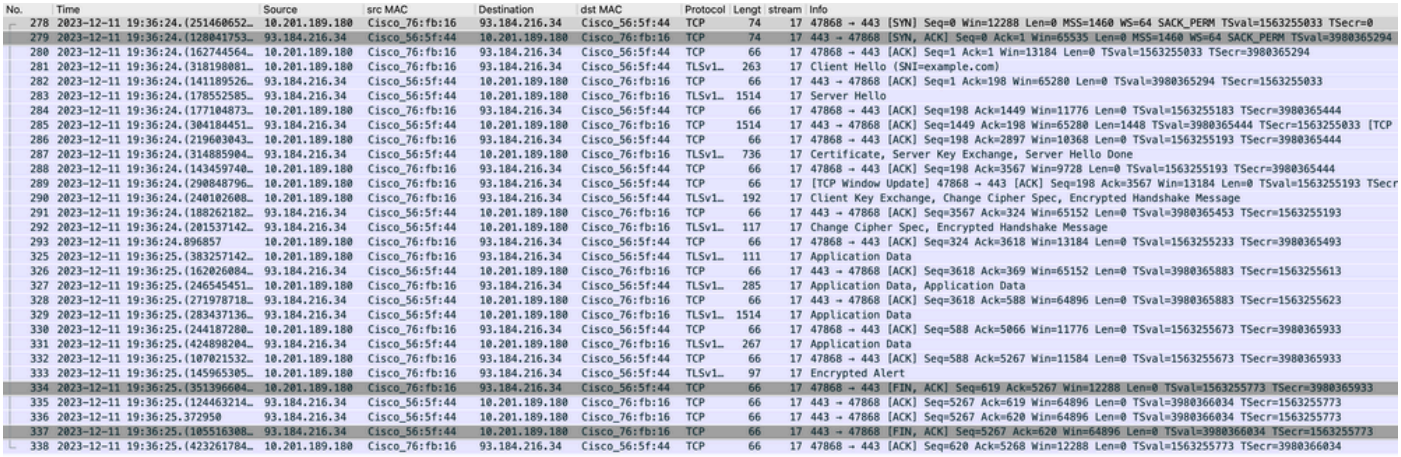
注意：如您所见，证书是在SWA中配置为解密证书的证书。

SWA和Web服务器

网络流量发生在代理的IP地址和Web服务器的IP地址之间。

来自SWA的流量发往TCP端口443（不是代理端口）

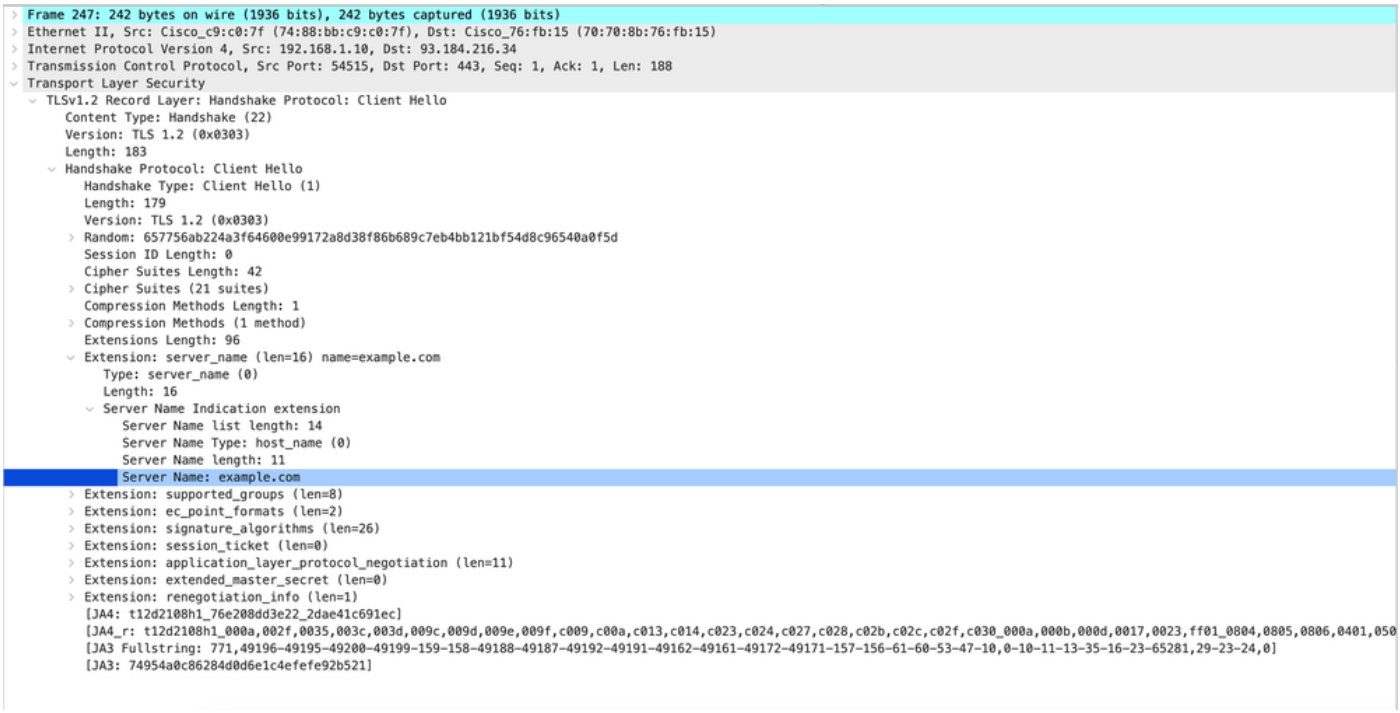
- TCP握手
- TLS握手客户端Hello — 服务器Hello — 服务器密钥交换 — 客户端密钥交换
- 数据传输
- TCP连接终止（4次握手）



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

图像 — Web服务器的代理 — HTTP — 透明 — 无身份验证

以下是从SWA到Web服务器的客户端Hello示例。



```
> 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]
```

图像 — 客户端Hello - Web服务器的代理 — 透明 — 无身份验证

注意：此处观察到的密码套件与客户端到SWA的客户端Hello中的密码套件不同，因为配置为解密此流量的SWA使用自己的密码。

提示：在从SWA到Web服务器的服务器密钥交换中，会显示Web服务器证书。但是，如果上游代理找到您的SWA的配置，则会显示其证书而不是Web服务器证书。

以下是访问日志的示例：

```
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
```

注意：如您所见，在HTTPS流量的透明部署中，Accesslogs中有2行；第一行是流量被加密，您可以看到TCP_CONNECT和Web服务器的IP地址。如果在SWA中启用解密，则第二行包含GET，整个URL以HTTPS开头，这意味着流量已解密，并且SWA知道该URL。

相关内容

- 技术支持和文档 - Cisco Systems
- 配置访问日志中的性能参数 — 思科

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。