

# 瞭解安全Web裝置中的資料包流

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [代理部署的型別不同](#)

### [TLS握手](#)

### [HTTP響應代碼](#)

[1xx：資訊](#)

[2xx：成功](#)

[3xx：重定向](#)

[4xx代碼：客戶端錯誤](#)

[5xx：伺服器錯誤](#)

### [明確部署](#)

[無身份驗證的顯式部署中的HTTP流量](#)

[客戶端和SWA](#)

[SWA和Web伺服器](#)

[包含快取資料的流量](#)

[無身份驗證的顯式部署中的HTTP流量](#)

[客戶端和SWA](#)

[SWA和Web伺服器](#)

[直通HTTPS流量](#)

### [透明部署](#)

[無身份驗證透明部署中的HTTP流量](#)

[客戶端和SWA](#)

[SWA和Web伺服器](#)

[包含快取資料的流量](#)

[無身份驗證透明部署中的HTTP流量](#)

[客戶端和SWA](#)

[SWA和Web伺服器](#)

### [相關資訊](#)

---

## 簡介

本文檔介紹了代理配置網路中的網路流，特別側重於安全Web裝置(SWA)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 基本TCP/IP概念。
- Proxy設定的基本知識。
- 有關使用代理的環境中使用的身份驗證機制的基本知識。

所用縮寫為：

TCP：傳輸控制協定

UDP：使用者資料包協定

IP：Internet協定

GRE：通用路由封裝

HTTP：超文本傳輸協定。

HTTPS：安全超文本傳輸協定。

URL：統一資源定位器

TLS：傳輸層安全性

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 代理部署的型別不同

### TLS握手

當客戶端和伺服器透過Internet通訊時，HTTPS中的TLS握手會發生，從而提供安全連線。此程式可維護兩個通訊應用程式之間的隱私權與資料完整性。它透過一系列步驟運行，其中客戶端和伺服器就所有後續傳輸的加密標準和代碼達成一致。握手的目的是阻止任何未經授權的訪問或第三方操縱。它還驗證通訊方的身份以消除模擬。此過程對於HTTPS至關重要，因為它可確保資料在傳輸過程中保持安全。

以下是TLS握手的步驟：

1. 客戶端Hello：客戶端使用Hello消息啟動握手過程。此消息包含客戶端TLS版本、支援的密碼套件以及稱為「客戶端隨機」的隨機位元組字串。
2. 伺服器Hello：伺服器會以Hello訊息回應。此消息包括伺服器選擇的TLS版本、選擇的密碼套件、稱為「伺服器隨機」的隨機位元組字串以及伺服器數位證書。如果需要，伺服器還會請求客戶端數位證書進行相互身份驗證。

3. 使用者端驗證伺服器憑證：使用者端會向發出該憑證的憑證授權單位檢查伺服器數位憑證。這可以確保客戶端正在與合法伺服器通訊。
4. Pre-master Secret：客戶端傳送一個稱為「Pre-master secret」的隨機位元組字串，用於建立會話金鑰。使用者端會使用伺服器公開金鑰來加密這個預先主要密碼，因此只有伺服器可以使用它的私密金鑰來解密。
5. Master Secret：客戶端和伺服器都使用Hello消息中的預主金鑰和隨機位元組字串來獨立計算相同的「主金鑰」。此共用金鑰是生成會話金鑰的基礎。
6. Client Finished：客戶端傳送「Finished」消息（用會話金鑰加密），以表示完成客戶端部分的握手。
7. Server Finished：伺服器傳送「Finished」消息（也使用會話金鑰加密），以表示已完成部分伺服器握手。

## HTTP響應代碼

### 1xx：資訊

代碼	詳細資料
100繼續	通常在ICAP協定方面可見。此為資訊性響應，使客戶端知道它可以繼續傳送資料。關於ICAP服務（例如病毒掃描），伺服器只希望看到前x個位元組數。當完成掃描第一組位元組並且未檢測到病毒時，它會傳送100 Continue以讓客戶端知道傳送對象的其餘部分。

### 2xx：成功

代碼	詳細資料
200確定	最常見的響應代碼。這表示要求成功而沒有任何問題。

### 3xx：重新導向

代碼	詳細資料
301永久重新導向	這是永久重定向，當您重定向到www子域時，可以看到此代碼。
302暫時重新導向	這是暫時重新導向。會指示使用者端對Location：標頭中指定的物件提出新要求。
304未修改	這是對GIMS (GET If-modified-since)的響應。這實際上是一個標準的HTTP GET，包括報頭If-modified-since：<date>。此標頭告訴伺服

	器使用者端在本機快取中有要求的物件復本，並且內含擷取物件的日期。如果物件自該日期以來已修改，伺服器會以200 OK和物件的新復本來回應。如果物件自擷取日期後未變更，伺服器會傳回304 Not Modified回應。
307驗證重新導向	這在透明代理部署中最为常見，當代理伺服器配置為驗證請求並將請求重定向到另一個URL以驗證使用者時，

#### 4xx代碼：客戶端錯誤

代碼	詳細資料
400錯誤請求	這說明HTTP要求有問題，因為它不符合正確的語法。可能的原因可能包括單行上有多個標頭、標頭中有空格或URI中缺少HTTP/1.1等。有關正確語法，請參閱RFC 2616。
401未授權 需要Web伺服器驗證	存取要求的物件需要驗證。401代碼用於目標Web伺服器的身份驗證。當SWA以透明模式運行並在代理上啟用身份驗證時，它會將一個401返回給客戶端，因為裝置將自己顯示為OCS（源內容伺服器）。  「www-authenticate：」HTTP響應報頭中詳細介紹了可以使用的身份驗證方法。這會通知使用者端伺服器是否要求NTLM、基本或其他形式的驗證。
403已拒絕	客戶端無法訪問請求的對象。多種原因可能導致伺服器拒絕對象訪問。伺服器通常會在HTTP資料或HTML回應中提供原因說明。
404未找到	伺服器上不存在要求的物件。
需要407代理驗證	這與401相同，不同之處在於它專門用於代理而不是OCS的身份驗證。僅當請求已明確傳送到代理時，才會傳送此消息。  當SWA配置為透明代理時，無法將407傳送到客戶端，因為客戶端不知道該代理存在。如果出現這種情況，則客戶端最有可能是FIN或RST的TCP套接字。

#### 5xx：伺服器錯誤

代碼	詳細資料
501內部伺服器錯誤	一般Web伺服器失敗。

502錯誤的網關	當充當網關或代理的伺服器從入站伺服器收到無效響應時發生。它表示網關已從上游或源伺服器接收到不適當的響應。
503服務不可用	表示由於臨時過載或計畫的維護，伺服器當前無法處理該請求。這表示伺服器暫時停止服務，但過一段時間後可以再次使用。
504網關超時	表示使用者端或代理未從它嘗試存取的Web伺服器及時收到回應，因此無法載入網頁或滿足瀏覽器的其他要求。這通常意味著上游伺服器發生故障。

## 明確部署

在這裡....

### 無身份驗證的顯式部署中的HTTP流量

#### 客戶端和SWA

網路流量在客戶端的IP地址和SWA代理介面的IP地址之間傳輸（通常是P1介面，但可以是P2或管理介面，具體取決於代理配置）。

來自客戶端的流量將發往TCP埠80或3128到SWA（預設SWA代理埠為TCP 80和3128，在此示例中使用埠3128）

- TCP握手。
- HTTP Get from Client（目標IP = SWA IP，目標埠= 3128）
- 來自代理的HTTP響應（源IP = SWA）
- 資料傳輸
- TCP連線終止（4次握手）

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	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=322700886
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=322700887
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=322700884 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=3227001886 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=131872 Len=0 TSval=1762372145 TSecr=3227001886
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=3227001886
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=131872 Len=0 TSval=1762372158 TSecr=3227001886
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=1762372158
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=1762372158
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=131872 Len=0 TSval=1762372212 TSecr=3227001147

Image-Client到SWA，HTTP顯式模式

#### SWA和Web伺服器

網路流量發生在代理的IP地址和Web伺服器的IP地址之間。

從SWA發往TCP埠80的流量來自一個隨機埠（非代理埠）

- TCP握手。
- HTTP Get from Proxy ( 目標IP = Web伺服器, 目標埠= 80 )
- 來自Web伺服器的HTTP響應 ( 源IP =代理伺服器 )
- 資料傳輸
- TCP連線終止 ( 4次握手 )

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Len	stream	Info
12570	2024-01-25 09:35:26.053195	10.48.48.185	VWware_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	VWware_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=0
12779	2024-01-25 09:35:26.168077	10.48.48.185	VWware_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	VWware_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	VWware_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	VWware_8d:f3:64	TCP	1414	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=1348 TSval=2163592177 TSecr=3190021832 [TCP seq
12835	2024-01-25 09:35:26.281789	10.48.48.185	VWware_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	VWware_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	VWware_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

影像- HTTP-SWA到Web伺服器-顯式-無快取

下面是客戶端的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
√ Hypertext Transfer Protocol
  √ 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]

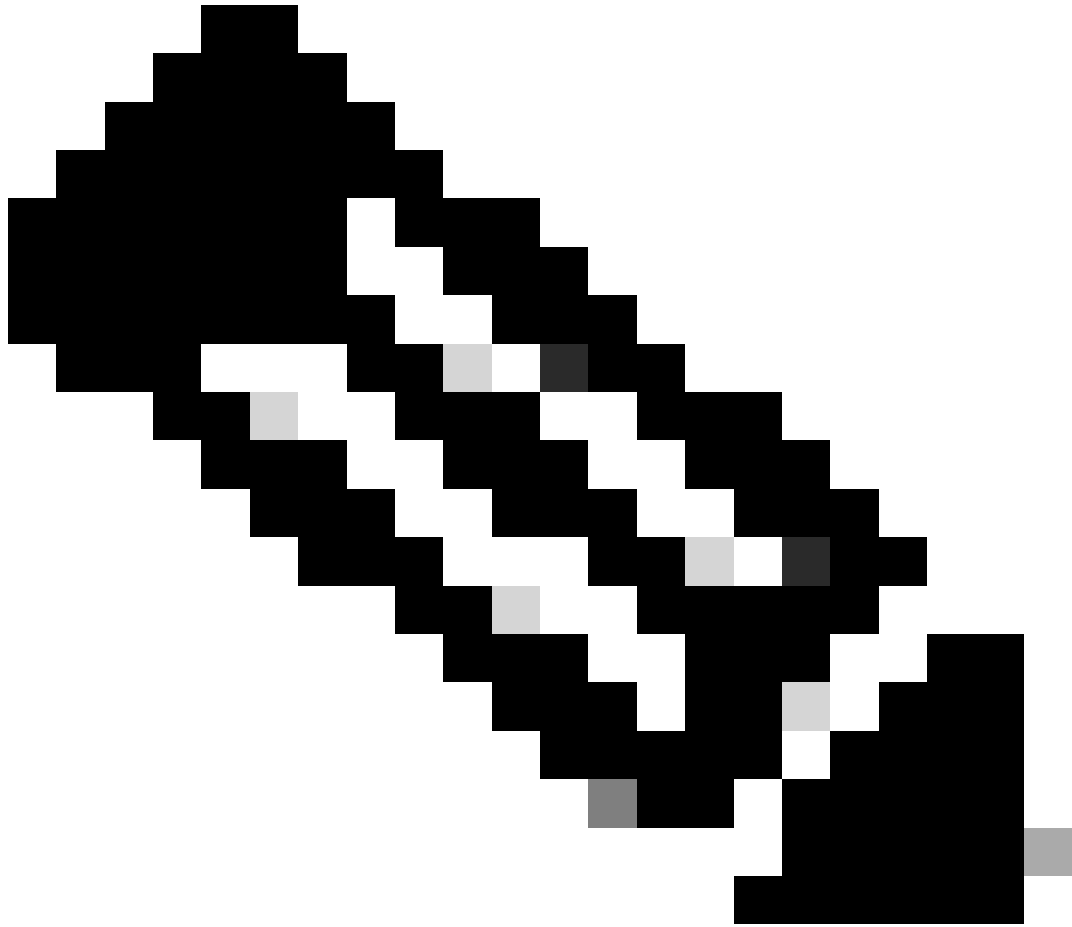
```

映像- SWA HTTP GET的客戶端-明確

這表示從客戶端到SWA, 然後到Web伺服器, 最後返回客戶端的整個流量流。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Len	stream	Info
12544	2024-01-25 09:35:25.989719	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VWware_8d:f3:64	TCP	78	2	65238 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 SACK_PERM TSval=1762371780 TSecr=0 SACK_PERM
12545	2024-01-25 09:35:25.989748	10.48.48.185	VWware_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 TSecr=0
12567	2024-01-25 09:35:26.046546	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VWware_8d:f3:64	TCP	66	2	65238 → 3128 [ACK] Seq=1 Ack=1 Win=13228 Len=0 TSval=1762371848 TSecr=322700083
12568	2024-01-25 09:35:26.046677	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VWware_8d:f3:64	HTTP	188	2	GET http://example.com/ HTTP/1.1
12569	2024-01-25 09:35:26.046695	10.48.48.185	VWware_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	VWware_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	VWware_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=0
12779	2024-01-25 09:35:26.168077	10.48.48.185	VWware_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	VWware_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	VWware_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	VWware_8d:f3:64	TCP	1414	3	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=1348 TSval=2163592177 TSecr=3190021832 [TCP seq
12835	2024-01-25 09:35:26.281789	10.48.48.185	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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顯式-無快取



注意：每個資料流都以不同的顏色區分；從客戶端到SWA的流為一種顏色，從SWA到Web伺服器的流為另一種顏色。

Time	10.61.70.23	10.48.48.185	93.184.216.34	Comment
2024-01-25 09:35:25.989719	65238	65238 → 3128 [SYN] Seq=0 Win=65535 Len=0	3128	TCP: 65238 → 3128 [SYN] Seq=0 Win=65535 ...
2024-01-25 09:35:25.989748	65238	3128 → 65238 [SYN, ACK] Seq=0 Ack=1 Win=0	3128	TCP: 3128 → 65238 [SYN, ACK] Seq=0 Ack=1 ...
2024-01-25 09:35:26.046546	65238	65238 → 3128 [ACK] Seq=1 Ack=1 Win=13228	3128	TCP: 65238 → 3128 [ACK] Seq=1 Ack=1 Win=1...
2024-01-25 09:35:26.046877	65238	GET http://example.com/ HTTP/1.1	3128	HTTP: GET http://example.com/ HTTP/1.1
2024-01-25 09:35:26.046945	65238	3128 → 65238 [ACK] Seq=1 Ack=123 Win=654	3128	TCP: 3128 → 65238 [ACK] Seq=1 Ack=123 Win...
2024-01-25 09:35:26.053195		23146 → 80 [SYN] Seq=0 Win=12288 Len=0 M...	80	TCP: 23146 → 80 [SYN] Seq=0 Win=12288 Le...
2024-01-25 09:35:26.168035		80 → 23146 [SYN, ACK] Seq=0 Ack=1 Win=65...	80	TCP: 80 → 23146 [SYN, ACK] Seq=0 Ack=1 WL...
2024-01-25 09:35:26.168077		23146 → 80 [ACK] Seq=1 Ack=1 Win=13568 L...	80	TCP: 23146 → 80 [ACK] Seq=1 Ack=1 Win=13...
2024-01-25 09:35:26.168172		GET / HTTP/1.1	80	HTTP: GET / HTTP/1.1
2024-01-25 09:35:26.280446		80 → 23146 [ACK] Seq=1 Ack=177 Win=67072	80	TCP: 80 → 23146 [ACK] Seq=1 Ack=177 Win=6...
2024-01-25 09:35:26.281757		80 → 23146 [ACK] Seq=1 Ack=177 Win=67072	80	TCP: 80 → 23146 [ACK] Seq=1 Ack=177 Win=6...
2024-01-25 09:35:26.281789		23146 → 80 [ACK] Seq=177 Ack=1349 Win=12	80	TCP: 23146 → 80 [ACK] Seq=177 Ack=1349 WL...
2024-01-25 09:35:26.281793		HTTP/1.1 200 OK (text/html)	80	HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:35:26.281801		23146 → 80 [ACK] Seq=177 Ack=1608 Win=11	80	TCP: 23146 → 80 [ACK] Seq=177 Ack=1608 WL...
2024-01-25 09:35:26.286288	65238	3128 → 65238 [ACK] Seq=1 Ack=123 Win=654	3128	TCP: 3128 → 65238 [ACK] Seq=1 Ack=123 Win...
2024-01-25 09:35:26.286297	65238	HTTP/1.1 200 OK (text/html)	3128	HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:35:26.347713	65238	65238 → 3128 [ACK] Seq=123 Ack=1189 Win=...	3128	TCP: 65238 → 3128 [ACK] Seq=123 Ack=1189 ...
2024-01-25 09:35:26.347815	65238	65238 → 3128 [ACK] Seq=123 Ack=1722 Win=...	3128	TCP: 65238 → 3128 [ACK] Seq=123 Ack=1722 ...
2024-01-25 09:35:26.353174	65238	65238 → 3128 [FIN, ACK] Seq=123 Ack=1722	3128	TCP: 65238 → 3128 [FIN, ACK] Seq=123 Ack=1...
2024-01-25 09:35:26.353217	65238	3128 → 65238 [ACK] Seq=1722 Ack=124 Win=...	3128	TCP: 3128 → 65238 [ACK] Seq=1722 Ack=124 ...
2024-01-25 09:35:26.353397	65238	3128 → 65238 [FIN, ACK] Seq=1722 Ack=124	3128	TCP: 3128 → 65238 [FIN, ACK] Seq=1722 Ack...
2024-01-25 09:35:26.412438	65238	65238 → 3128 [ACK] Seq=124 Ack=1723 Win=...	3128	TCP: 65238 → 3128 [ACK] Seq=124 Ack=1723 ...

圖-通訊流HTTP顯示-無快取

以下是存取日誌的範例：

1706172876.686 224 10.61.70.23 TCP\_MISS/200 1721 GET http://www.example.com/ - DIRECT/www.example.com t

包含快取資料的流量

這表示當資料在SWA快取中時，從客戶端到SWA的整個流量。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Len	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=368792393
1922	2024-01-25 09:56:41.265937	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	HTTP	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

影像- HTTP明確快取資料



注意：如您所見，Web伺服器傳回HTTP回應304：未修改快取。(在本例中，資料包編號1947)

Time	10.61.70.23	10.48.48.185	93.184.216.34	Comment
2024-01-25 09:56:41.209030	55709	55709 → 3128 [SYN] Seq=0 Win=65535 Len=0	3128	TCP: 55709 → 3128 [SYN] Seq=0 Win=65535 ...
2024-01-25 09:56:41.209111	55709	3128 → 55709 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0	3128	TCP: 3128 → 55709 [SYN, ACK] Seq=0 Ack=1 ...
2024-01-25 09:56:41.265937	55709	55709 → 3128 [ACK] Seq=1 Ack=1 Win=13228 Len=0	3128	TCP: 55709 → 3128 [ACK] Seq=1 Ack=1 Win=1...
2024-01-25 09:56:41.266065	55709	GET http://example.com/ HTTP/1.1	3128	HTTP: GET http://example.com/ HTTP/1.1
2024-01-25 09:56:41.266114	55709	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65535 Len=0	3128	TCP: 3128 → 55709 [ACK] Seq=1 Ack=123 Win...
2024-01-25 09:56:41.269061	16088	16088 → 80 [SYN] Seq=0 Win=12288 Len=0 M...	80	TCP: 16088 → 80 [SYN] Seq=0 Win=12288 Le...
2024-01-25 09:56:41.385086	16088	80 → 16088 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0	80	TCP: 80 → 16088 [SYN, ACK] Seq=0 Ack=1 Wi...
2024-01-25 09:56:41.385174	16088	16088 → 80 [ACK] Seq=1 Ack=1 Win=13568 Len=0	80	TCP: 16088 → 80 [ACK] Seq=1 Ack=1 Win=135...
2024-01-25 09:56:41.385270	16088	GET / HTTP/1.1	80	HTTP: GET / HTTP/1.1
2024-01-25 09:56:41.509528	16088	80 → 16088 [ACK] Seq=1 Ack=227 Win=67072 Len=0	80	TCP: 80 → 16088 [ACK] Seq=1 Ack=227 Win...
2024-01-25 09:56:41.510195	16088	HTTP/1.1 304 Not Modified	80	HTTP: HTTP/1.1 304 Not Modified
2024-01-25 09:56:41.510259	16088	16088 → 80 [ACK] Seq=227 Ack=300 Win=13228 Len=0	80	TCP: 16088 → 80 [ACK] Seq=227 Ack=300 Wi...
2024-01-25 09:56:41.510429	16088	16088 → 80 [FIN, ACK] Seq=227 Ack=300 Win=0 Len=0	80	TCP: 16088 → 80 [FIN, ACK] Seq=227 Ack=30...
2024-01-25 09:56:41.513099	55709	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65535 Len=0	3128	TCP: 3128 → 55709 [ACK] Seq=1 Ack=123 Win...
2024-01-25 09:56:41.513111	55709	HTTP/1.1 200 OK (text/html)	3128	HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:56:41.585507	55709	55709 → 3128 [ACK] Seq=123 Ack=1189 Win=65535 Len=0	3128	TCP: 55709 → 3128 [ACK] Seq=123 Ack=1189 ...
2024-01-25 09:56:41.600269	55709	55709 → 3128 [ACK] Seq=123 Ack=1722 Win=65535 Len=0	3128	TCP: 55709 → 3128 [ACK] Seq=123 Ack=1722 ...
2024-01-25 09:56:41.604113	55709	55709 → 3128 [FIN, ACK] Seq=123 Ack=1722 Win=0 Len=0	3128	TCP: 55709 → 3128 [FIN, ACK] Seq=123 Ack=1...
2024-01-25 09:56:41.604191	55709	3128 → 55709 [ACK] Seq=1722 Ack=124 Win=65535 Len=0	3128	TCP: 3128 → 55709 [ACK] Seq=1722 Ack=124 ...
2024-01-25 09:56:41.604293	55709	3128 → 55709 [FIN, ACK] Seq=1722 Ack=124 Win=0 Len=0	3128	TCP: 3128 → 55709 [FIN, ACK] Seq=1722 Ack=...
2024-01-25 09:56:41.636731	16088	80 → 16088 [FIN, ACK] Seq=300 Ack=228 Win=0 Len=0	80	TCP: 80 → 16088 [FIN, ACK] Seq=300 Ack=22...
2024-01-25 09:56:41.636832	16088	16088 → 80 [ACK] Seq=228 Ack=301 Win=13568 Len=0	80	TCP: 16088 → 80 [ACK] Seq=228 Ack=301 Wi...
2024-01-25 09:56:41.662464	55709	55709 → 3128 [ACK] Seq=124 Ack=1723 Win=65535 Len=0	3128	TCP: 55709 → 3128 [ACK] Seq=124 Ack=1723 ...

影像-含快取的Flow HTTP Explicit

以下是HTTP響應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
< Hypertext Transfer Protocol
  < HTTP/1.1 304 Not Modified\r\n
    < [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/]
```

圖- HTTP顯式304響應

以下是存取日誌的範例：

```
1706173001.489 235 10.61.70.23 TCP_REFRESH_HIT/200 1721 GET http://www.example.com/ - DIRECT/www.examp1
```

## 無身份驗證的顯式部署中的HTTP流量

### 客戶端和SWA

網路流量在客戶端的IP地址和SWA代理介面的IP地址之間傳輸（通常是P1介面，但可以是P2或管理介面，具體取決於代理配置）。

來自客戶端的流量將發往TCP埠80或3128到SWA（預設SWA代理埠為TCP 80和3128，在此示例中使用埠3128）

- TCP握手。
- 來自客戶端的HTTP CONNECT（目標IP = SWA，目標埠= 3128）

- 來自代理的HTTP響應 ( 源IP = SWA )
- 使用URL的SNI的客戶端Hello ( 源IP =客戶端 )
- 伺服器Hello ( 源IP = SWA )
- 伺服器金鑰交換 ( 源IP = SWA )
- 客戶端金鑰交換 ( 源IP =客戶端 )
- 資料傳輸
- TCP連線終止 ( 4次握手 )

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
18	2024-01-25 12:31:37.318166644	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VWware_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 12:31:37.339015315	10.48.48.165	VWware_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	VWware_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	VWware_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	VWware_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	VWware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	HTTP	185	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	VWware_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	VWware_8d:9a:f4	TLSv1.2	715	12	Client Hello (SNI=example.com)
29	2024-01-25 12:31:38.182072475	10.48.48.165	VWware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=40 Ack=861 Win=64784 Len=0 TSval=441495747 TSecr=1676451630
49	2024-01-25 12:31:38.182097668	10.48.48.165	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_8d:9a:f4	TLSv1.2	562	12	Application Data
61	2024-01-25 12:31:38.257435452	10.48.48.165	VWware_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	VWware_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	VWware_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 12:31:39.1280484748	10.48.48.165	VWware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1289	12	Application Data, Application Data
85	2024-01-25 12:31:39.1128618294	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VWware_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 12:31:39.092947	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VWware_8d:9a:f4	TLSv1.2	497	12	Application Data
87	2024-01-25 12:31:39.277889790	10.48.48.165	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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	VWware_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客戶端-顯示-無快取

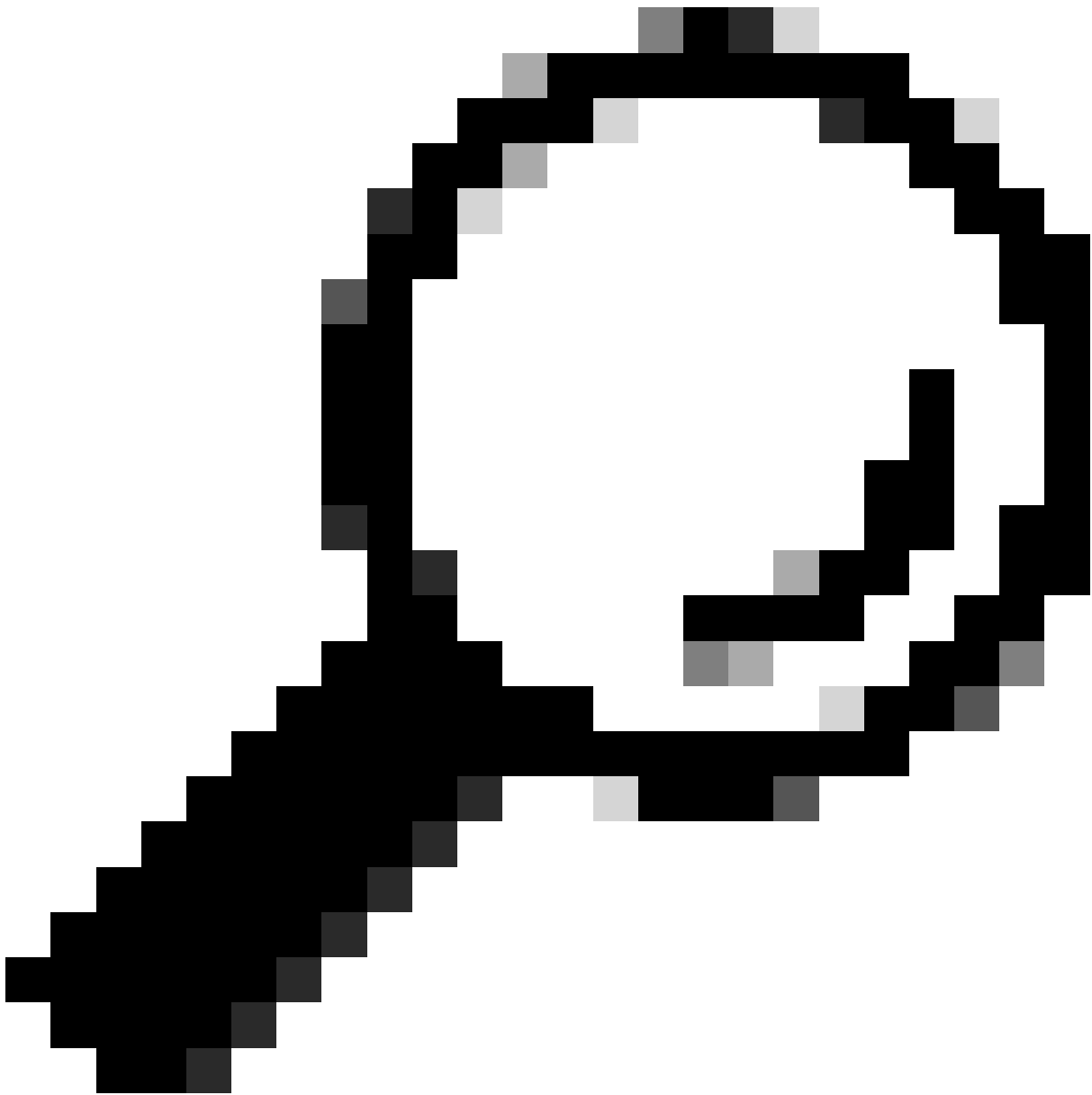
以下是客戶端到SWA的客戶端Hello的詳細資訊，如您在伺服器名稱指示(SNI)中所看到的Web伺服器URL，在本示例中為[www.example.com](http://www.example.com)，並且客戶端通告了17個Cipher Suite：

```

> Frame 28: 715 bytes on wire (5720 bits), 715 bytes captured (5720 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: 212, Ack: 40, Len: 649
< Hypertext Transfer Protocol
  [Proxy-Connect-Hostname: example.com]
  [Proxy-Connect-Port: 443]
< Transport Layer Security
  < TLSv1.2 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: 8f2d33b577f5cd05ab284c0a64a929e5dd29c940aa73ccc3f4bcfaf8509078d
    Session ID Length: 32
    Session ID: e91649fe756a373ce70f5b65c9729b805d864f8f39ac783b2feb9a49ced7de6b
    Cipher Suites Length: 34
  > Cipher Suites (17 suites) ←
    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)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: status_request (len=5)
  > Extension: delegated_credentials (len=10)
  > Extension: key_share (len=107) x25519, secp256r1
  > Extension: supported_versions (len=5) TLS 1.3, TLS 1.2
  > Extension: signature_algorithms (len=24)
  > Extension: record_size_limit (len=2)
  > Extension: encrypted_client_hello (len=281)
    [JA4: t13d1713h2 5h57614c22h0 748f4c70de1c]

```

映像- HTTPS客戶端Hello -顯式- SWA的客戶端



提示：您可以在Wireshark中使用此過濾器搜尋URL/SNI：  
tls.handshake.extensions\_server\_name==「www.example.com」

---

以下是SWA傳送給客戶端的證書示例

```

> Frame 50: 1254 bytes on wire (10032 bits), 1254 bytes captured (10032 bits)
> Ethernet II, Src: VMware_Bd:9a:f4 (00:50:56:8d:9a:f4), Dst: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff)
> Internet Protocol Version 4, Src: 10.48.48.165, Dst: 10.61.70.23
> Transmission Control Protocol, Src Port: 3128, Dst Port: 61484, Seq: 1228, Ack: 861, Len: 1188
> [2 Reassembled TCP Segments (2105 bytes): #49(1107), #50(998)]
v Hypertext Transfer Protocol
  [Proxy-Connect-Hostname: example.com]
  [Proxy-Connect-Port: 443]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 2100
  v Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2096
    Certificates Length: 2093
  v Certificates (2093 bytes)
    Certificate Length: 1105
  v Certificate [truncated]: 3082044d30820335a00302010202140279103122f2aad73d32683b716d2a7d4ead7d47300d06092a864886f70d01010b05003047310b300906035504061302553310e300c0603550401
    v signedCertificate
      version: v3 (2)
      serialNumber: 0x0279103122f2aad73d32683b716d2a7d4ead7d47
      v signature (sha256WithRSAEncryption)
      v issuer: rdnsSequence (0)
    v rdnsSequence: 4 items (id-at-commonName=CISCO LAB Explicit, id-at-organizationalUnitName=IT, id-at-organizationName=Cisco, id-at-countryName=US)
      v RDNSequence item: 1 item (id-at-countryName=US)
      v RelativeDistinguishedName item (id-at-countryName=US)
        Object Id: 2.5.4.6 (id-at-countryName)
        CountryName: US
      v RDNSequence item: 1 item (id-at-organizationName=Cisco)
      v RelativeDistinguishedName item (id-at-organizationName=Cisco)
        Object Id: 2.5.4.10 (id-at-organizationName)
        v DirectoryString: printableString (1)
          printableString: Cisco
      v RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
      v RelativeDistinguishedName item (id-at-organizationalUnitName=IT)
        Object Id: 2.5.4.11 (id-at-organizationalUnitName)
        v DirectoryString: printableString (1)
          printableString: IT
      v RDNSequence item: 1 item (id-at-commonName=CISCO LAB Explicit)
      v RelativeDistinguishedName item (id-at-commonName=CISCO LAB Explicit)
        Object Id: 2.5.4.3 (id-at-commonName)
        v DirectoryString: printableString (1)
          printableString: CISCO LAB Explicit

```

映像- HTTPS證書-明確- SWA到客戶端

## SWA和Web伺服器

網路流量發生在代理的IP地址和Web伺服器的IP地址之間。

從SWA發往TCP埠443的流量 ( 非代理埠 )

- TCP握手。
- 客戶端Hello ( 目標IP = Web伺服器 , 目標埠= 443 )
- 伺服器Hello ( 源IP = Web伺服器 )
- 資料傳輸
- TCP連線終止 ( 4次握手 )

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
23	2024-01-25 12:31:37.383901	10.48.48.165	VMware_Bd: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_Bd:9a:f4	TCP	74	13	443 → 24953 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=1727280976 TSecr=2549353418
25	2024-01-25 12:31:38.093381	10.48.48.165	VMware_Bd: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 12:31:38.358314	10.48.48.165	VMware_Bd:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	259	13	Client Hello (SN=example.com)
31	2024-01-25 12:31:38.146535406	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_Bd: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_Bd:9a:f4	TLSv1.2	1434	13	Server Hello
33	2024-01-25 12:31:38.273349971	10.48.48.165	VMware_Bd: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 12:31:38.141489809	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_Bd:9a:f4	TCP	1434	13	443 → 24953 [PSH, ACK] Seq=1369 Ack=194 Win=67072 Len=1368 TSval=1727281240 TSecr=2549353688
35	2024-01-25 12:31:38.178681044	10.48.48.165	VMware_Bd: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_Bd:9a:f4	TLSv1.2	896	13	Certificate, Server Key Exchange, Server Hello Done
37	2024-01-25 12:31:38.1861040344	10.48.48.165	VMware_Bd: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_Bd: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_Bd:9a:f4	TLSv1.2	117	13	Change Cipher Spec, Encrypted Handshake Message
40	2024-01-25 12:31:38.1809573742	10.48.48.165	VMware_Bd: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=1727281240
64	2024-01-25 12:31:38.296760748	10.48.48.165	VMware_Bd:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	111	13	Application Data
73	2024-01-25 12:31:38.419191657	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_Bd:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=3618 Ack=365 Win=67072 Len=0 TSval=1727281896 TSecr=2549354298
74	2024-01-25 12:31:38.1340012513	10.48.48.165	VMware_Bd: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_Bd:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=3618 Ack=939 Win=68096 Len=0 TSval=2549354468 TSecr=2549354468
79	2024-01-25 12:31:39.159843876	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_Bd:9a:f4	TLSv1.2	1146	13	Application Data, Application Data
80	2024-01-25 12:31:39.385106563	10.48.48.165	VMware_Bd: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_Bd: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_Bd: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_Bd: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_Bd:9a:f4	TCP	66	13	443 → 24953 [ACK] Seq=4698 Ack=1493 Win=69120 Len=0 TSval=1727282678 TSecr=2549355128
92	2024-01-25 12:31:39.282826742	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_Bd:9a:f4	TLSv1.2	1136	13	Application Data, Application Data
93	2024-01-25 12:31:39.048886	10.48.48.165	VMware_Bd: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 -明確- SWA至Web伺服器

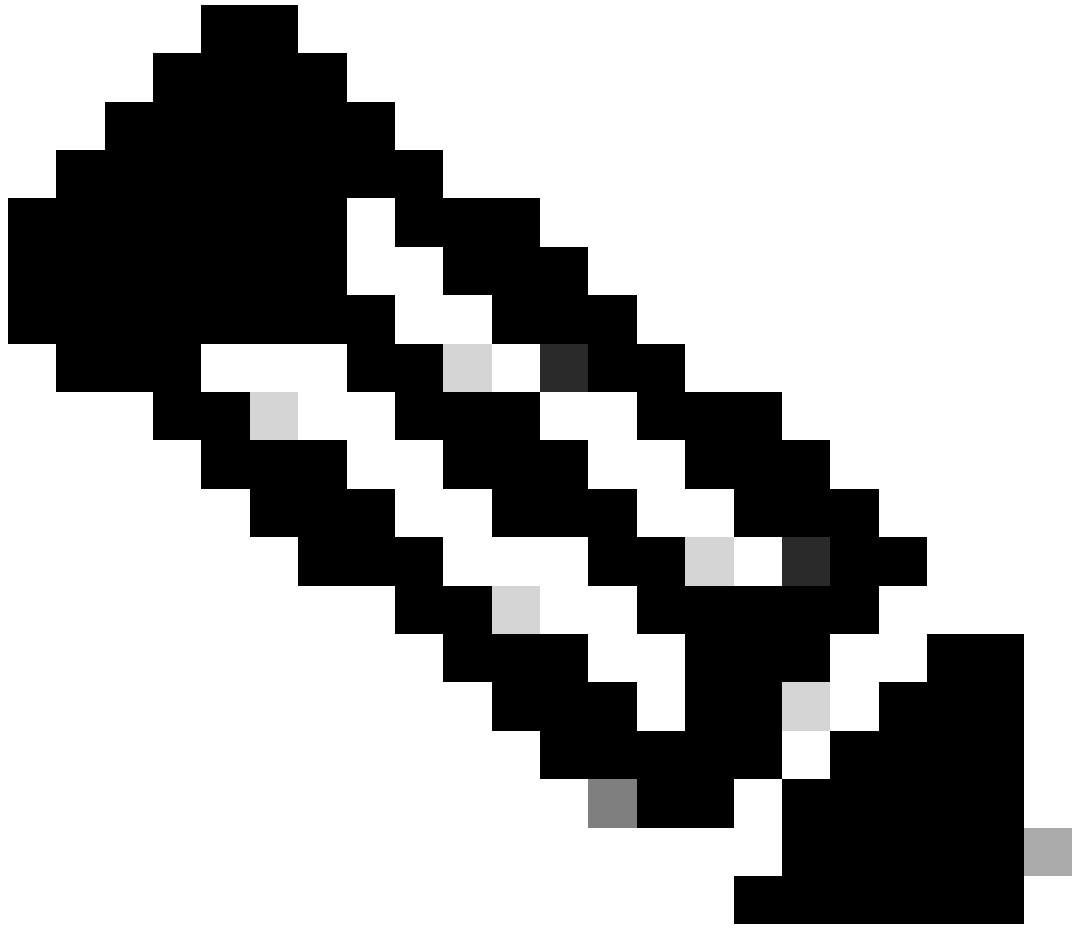
以下是從SWA到Web伺服器的客戶端Hello的詳細資訊，因為您可以看到SWA通告了12個密碼套件：

```

> Frame 30: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits)
> Ethernet II, Src: VMware_8d:9a:f4 (00:50:56:8d:9a:f4), Dst: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff)
> Internet Protocol Version 4, Src: 10.48.48.165, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 24953, Dst Port: 443, Seq: 1, Ack: 1, Len: 193
< Transport Layer Security
  < TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 188
  < Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 184
    Version: TLS 1.2 (0x0303)
  > Random: 6601ee708d9db71cf5c7c4584e5facdf08d4de0b208f6d6eb6ade08cc7d3e14
    Session ID Length: 0
    Cipher Suites Length: 24
  > Cipher Suites (12 suites) ←
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 119
  < 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: ec_point_formats (len=4)
  > Extension: supported_groups (len=12)
  > Extension: application_layer_protocol_negotiation (len=11)
  > Extension: encrypt_then_mac (len=0)
  > Extension: extended_master_secret (len=0)
  > Extension: signature_algorithms (len=48)
  [JA4: t12d1207h1_ea129f91df3f_ed727256b201]
  [JA4_r: t12d1207h1_002f,009c,009d,00ff,c009,c013,c02b,c02c,c02f,c030,cca8,cca9_000a,000b,000d,0016,0017_0403,0503,0603,0807,0808,0809,080a,080b,0804,0805,0806,0401,0501,0601,030]
  [JA3 Fullstring: 771,49195-49199-52393-52392-49196-49200-49161-49171-156-157-47-255,0-11-10-16-22-23-13,29-23-30-25-24,0-1-2]
  [JA3: 485a74d85df6d99eb1db31d9c65efe0f]

```

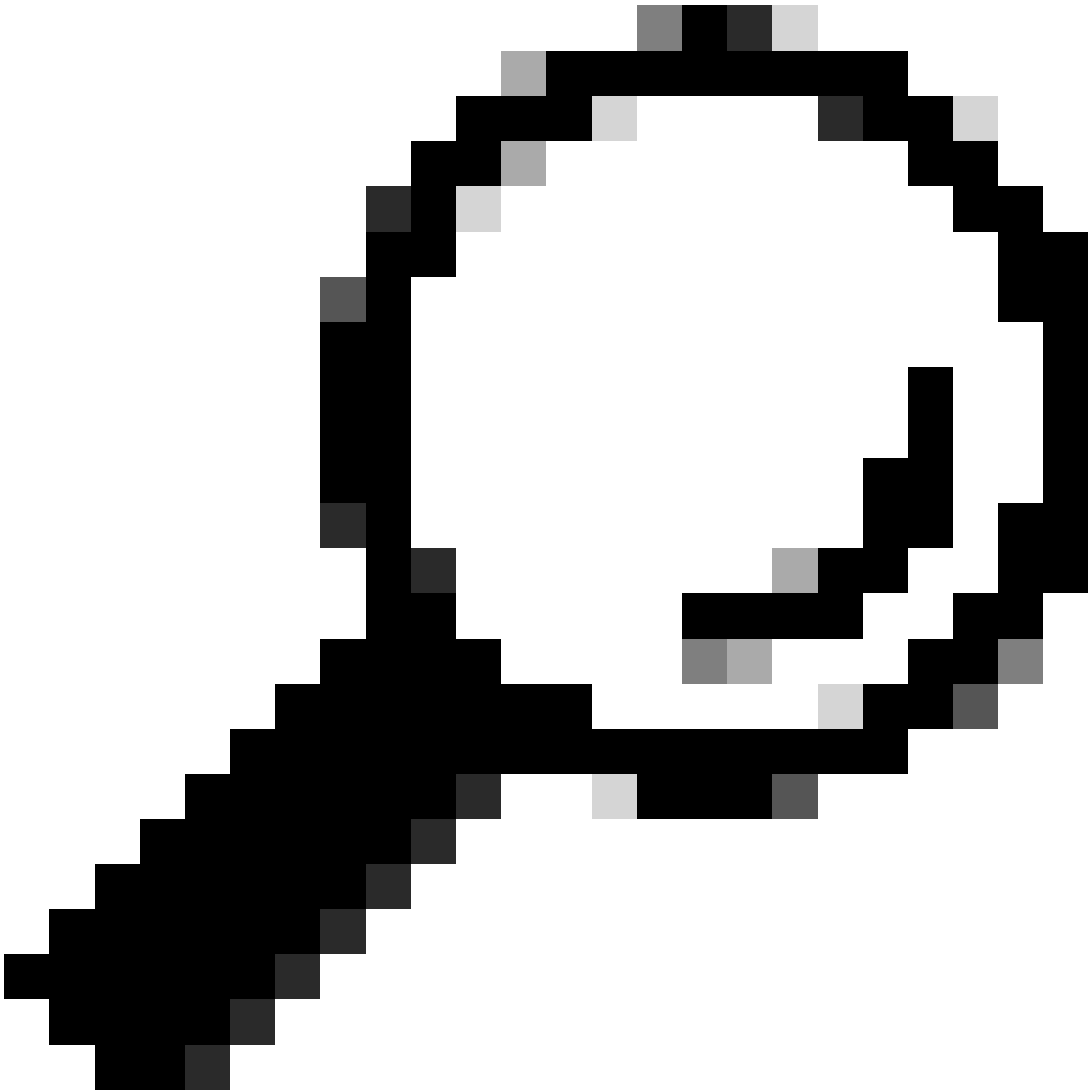
影象- HTTPS客户端Hello - SWA到Web伺服器-無快取



注意：此處觀察的密碼套件與客戶端到SWA的Hello客戶端中的密碼套件不同，因為配置為解密此流量的SWA使用自己的密碼。

---





提示：在從SWA到Web伺服器的伺服器金鑰交換中，將顯示Web伺服器證書。但是，如果上游代理發現SWA的配置，則會顯示其證書而不是Web伺服器證書。

---

以下是來自客戶端的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
< Hypertext Transfer Protocol
  < CONNECT example.com:443 HTTP/1.1\r\n
    < [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]

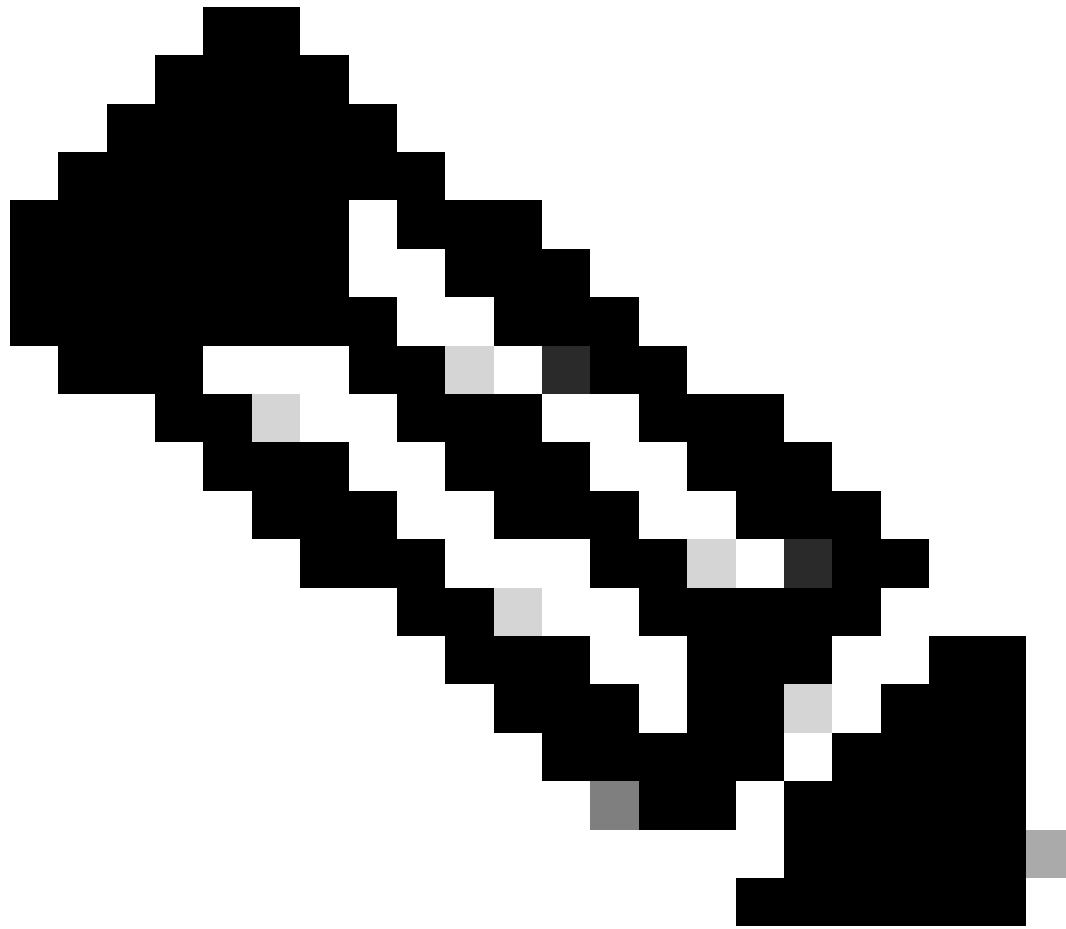
```

影像-客戶端HTTP連線

這表示從客戶端到SWA，然後到Web伺服器，最後返回客戶端的整個流量流。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	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 12:31:37.330915315..	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	185	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=64784 Len=0 TSval=441495747 TSecr=1676451630
30	2024-01-25 12:31:38.358314..	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 12:31:38.1146535406..	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 12:31:38.2147031593..	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=1072 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 12:31:38.414082050..	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=1727281240
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 12:31:38.402285678..	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 12:31:38.157148214..	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 12:31:38.4119116513..	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	116	13	Application Data, Application Data
78	2024-01-25 12:31:38.283208060..	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	TCP	116	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 12:31:39.165906323..	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 12:31:39.342088..	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 12:31:39.1200484740..	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1289	12	Application Data, Application Data
85	2024-01-25 12:31:39.1126618294..	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=44149680
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顯式-無快取



注意：每個資料流都以不同的顏色區分；從客戶端到SWA的流為一種顏色，從SWA到Web伺服器的流為另一種顏色。

---

Time	10.61.70.23	10.48.48.165	93.184.216.34	Comment
2024-01-25 12:31:37.(3181686448 nanoseconds)	61484	61484 → 3128 [SYN] Seq=0 Win=65535 L...	3128	TCP: 61484 → 3128 [SYN] Seq=0 Win=65535 ...
2024-01-25 12:31:37.(3300153152 nanoseconds)	61484	3128 → 61484 [SYN, ACK] Seq=0 Ack=1 ...	3128	TCP: 3128 → 61484 [SYN, ACK] Seq=0 Ack=1 ...
2024-01-25 12:31:37.(3702977600 nanoseconds)	61484	61484 → 3128 [ACK] Seq=1 Ack=1 Win=13 ...	3128	TCP: 61484 → 3128 [ACK] Seq=1 Ack=1 Win=1 ...
2024-01-25 12:31:37.383167	61484	CONNECT example.com:443 HTTP/1.1	3128	HTTP: CONNECT example.com:443 HTTP/1.1
2024-01-25 12:31:37.(3249466192 nanoseconds)	61484	3128 → 61484 [ACK] Seq=1 Ack=212 Win...	3128	TCP: 3128 → 61484 [ACK] Seq=1 Ack=212 Win...
2024-01-25 12:31:37.383901		24953 → 443 [SYN] Seq=0 Win=12288 Len...	443	TCP: 24953 → 443 [SYN] Seq=0 Win=12288 L...
2024-01-25 12:31:38.006918		443 → 24953 [SYN, ACK] Seq=0 Ack=1 Win...	443	TCP: 443 → 24953 [SYN, ACK] Seq=0 Ack=1 ...
2024-01-25 12:31:38.893381		24953 → 443 [ACK] Seq=1 Ack=1 Win=12...	443	TCP: 24953 → 443 [ACK] Seq=1 Ack=1 Win=12...
2024-01-25 12:31:38.731815	61484	HTTP/1.1 200 Connection established	3128	HTTP: HTTP/1.1 200 Connection established
2024-01-25 12:31:38.(3088775616 nanoseconds)	61484	61484 → 3128 [ACK] Seq=212 Ack=40 Win...	3128	TCP: 61484 → 3128 [ACK] Seq=212 Ack=40 W...
2024-01-25 12:31:38.(3223471664 nanoseconds)	61484	Client Hello (SNI=example.com)	3128	TLSv1.2: Client Hello (SNI=example.com)
2024-01-25 12:31:38.(1820724752 nanoseconds)	61484	3128 → 61484 [ACK] Seq=40 Ack=861 Win...	3128	TCP: 3128 → 61484 [ACK] Seq=40 Ack=861 W...
2024-01-25 12:31:38.350314		Client Hello (SNI=example.com)	443	TLSv1.2: Client Hello (SNI=example.com)
2024-01-25 12:31:38.(1465354064 nanoseconds)		443 → 24953 [ACK] Seq=1 Ack=194 Win...	443	TCP: 443 → 24953 [ACK] Seq=1 Ack=194 Win...
2024-01-25 12:31:38.(2470315936 nanoseconds)		Server Hello	443	TLSv1.2: Server Hello
2024-01-25 12:31:38.(2733499712 nanoseconds)		24953 → 443 [ACK] Seq=194 Ack=1369 ...	443	TCP: 24953 → 443 [ACK] Seq=194 Ack=1369 ...
2024-01-25 12:31:38.(1414890096 nanoseconds)		443 → 24953 [PSH, ACK] Seq=1369 Ack...	443	TCP: 443 → 24953 [PSH, ACK] Seq=1369 Ack...
2024-01-25 12:31:38.(1786810448 nanoseconds)		24953 → 443 [ACK] Seq=194 Ack=2737 ...	443	TCP: 24953 → 443 [ACK] Seq=194 Ack=2737 ...
2024-01-25 12:31:38.345520		Certificate, Server Key Exchange, Ser...	443	TLSv1.2: Certificate, Server Key Exchange, Ser...
2024-01-25 12:31:38.(1610403440 nanoseconds)		24953 → 443 [ACK] Seq=194 Ack=3567 ...	443	TCP: 24953 → 443 [ACK] Seq=194 Ack=3567 ...
2024-01-25 12:31:38.062391		Client Key Exchange, Change Cipher Spec...	443	TLSv1.2: Client Key Exchange, Change Cipher ...
2024-01-25 12:31:38.(4140285008 nanoseconds)		Change Cipher Spec, Encrypted Handshak...	443	TLSv1.2: Change Cipher Spec, Encrypted Hand...
2024-01-25 12:31:38.(1095737424 nanoseconds)		24953 → 443 [ACK] Seq=320 Ack=3618 ...	443	TCP: 24953 → 443 [ACK] Seq=320 Ack=3618 ...
2024-01-25 12:31:38.(2820976608 nanoseconds)	61484	Server Hello	3128	TLSv1.2: Server Hello
2024-01-25 12:31:38.(1534298672 nanoseconds)	61484	Certificate	3128	TLSv1.2: Certificate
2024-01-25 12:31:38.965425	61484	Server Key Exchange, Server Hello Done	3128	TLSv1.2: Server Key Exchange, Server Hello D...
2024-01-25 12:31:38.824826	61484	61484 → 3128 [ACK] Seq=861 Ack=1228 ...	3128	TCP: 61484 → 3128 [ACK] Seq=861 Ack=1228 ...
2024-01-25 12:31:38.(3446619136 nanoseconds)	61484	61484 → 3128 [ACK] Seq=861 Ack=2540 ...	3128	TCP: 61484 → 3128 [ACK] Seq=861 Ack=2540...
2024-01-25 12:31:38.(1738329504 nanoseconds)	61484	Client Key Exchange, Change Cipher Spec...	3128	TLSv1.2: Client Key Exchange, Change Cipher ...
2024-01-25 12:31:38.(4228567872 nanoseconds)	61484	3128 → 61484 [ACK] Seq=2540 Ack=954 ...	3128	TCP: 3128 → 61484 [ACK] Seq=2540 Ack=954...
2024-01-25 12:31:38.(2445141472 nanoseconds)	61484	Change Cipher Spec, Encrypted Handshak...	3128	TLSv1.2: Change Cipher Spec, Encrypted Hand...
2024-01-25 12:31:38.(3287023360 nanoseconds)	61484	61484 → 3128 [ACK] Seq=954 Ack=2591 ...	3128	TCP: 61484 → 3128 [ACK] Seq=954 Ack=2591...

映像- HTTPS流-顯式-無快取

以下是存取日誌的範例：

```
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：如同HTTPS流量的透明部署中所見，訪問日誌中有兩行，第一行是流量被加密時，您可以看到CONNECT，並且Web伺服器的URL以tunnel://開頭。如果在SWA中啟用解密，則第二行包含GET，並且整個URL以HTTPS開頭，這意味著流量已解密。

---

## 直通HTTPS流量

如果您將SWA配置為透過流量，則整體流如下：

Time	10.61.70.23	10.48.48.165	93.184.216.34	Comment
2024-01-25 13:21:42.706645	60250	60250 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=341363	3128	TCP: 60250 → 3128 [SYN] Seq=0 Win=65535 ...
2024-01-25 13:21:42.2460867504 (nanoseconds)	60250	3128 → 60250 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SA	3128	TCP: 3128 → 60250 [SYN, ACK] Seq=0 Ack=1 ...
2024-01-25 13:21:42.1279136912 (nanoseconds)	60250	60250 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=341363763 TSecr=1	3128	TCP: 60250 → 3128 [ACK] Seq=1 Ack=1 Win=1...
2024-01-25 13:21:42.4235993424 (nanoseconds)	60250	CONNECT example.com:443 HTTP/1.1	3128	HTTP: CONNECT example.com:443 HTTP/1.1
2024-01-25 13:21:42.2468178944 (nanoseconds)	60250	3128 → 60250 [ACK] Seq=1 Ack=212 Win=65344 Len=0 TSval=1253711229 TSecr=	3128	TCP: 3128 → 60250 [ACK] Seq=1 Ack=212 Win...
2024-01-25 13:21:42.1692445712 (nanoseconds)			17517	17517 → 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSv...
2024-01-25 13:21:42.1675493712 (nanoseconds)			17517	443 → 17517 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM...
2024-01-25 13:21:42.402773			17517	17517 → 443 [ACK] Seq=1 Ack=1 Win=12...
2024-01-25 13:21:42.3955843776 (nanoseconds)	60250	HTTP/1.1 200 Connection established	3128	HTTP: HTTP/1.1 200 Connection established
2024-01-25 13:21:42.044443	60250	60250 → 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=341363960 TSe	3128	TCP: 60250 → 3128 [ACK] Seq=212 Ack=40 W...
2024-01-25 13:21:42.2651980528 (nanoseconds)	60250	Client Hello (SNI=example.com)	3128	TLV.3: Client Hello (SNI=example.com)
2024-01-25 13:21:42.1640450432 (nanoseconds)	60250	3128 → 60250 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=1253711429 TSe	3128	TCP: 3128 → 60250 [ACK] Seq=40 Ack=861 W...
2024-01-25 13:21:42.2261550016 (nanoseconds)			17517	Client Hello (SNI=example.com)
2024-01-25 13:21:42.2572160048 (nanoseconds)			17517	443 → 17517 [ACK] Seq=1 Ack=650 Win=67072 Len=0 TSval=1795164350 TSecr...
2024-01-25 13:21:42.310233			17517	Server Hello, Change Cipher Spec, Application Data
2024-01-25 13:21:42.1377394032 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=1369 Win=11136 Len=0 TSval=900013138 TSec
2024-01-25 13:21:42.1401624816 (nanoseconds)			17517	443 → 17517 [PSH, ACK] Seq=1369 Ack=650 Win=67072 Len=1368 TSval=179516...
2024-01-25 13:21:42.2565014960 (nanoseconds)	60250	Server Hello, Change Cipher Spec, Application Data	3128	TLV.3: Server Hello, Change Cipher Spec, Ap...
2024-01-25 13:21:42.1431156304 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=2737 Win=11072 Len=0 TSval=900013138 TSec
2024-01-25 13:21:42.2106897872 (nanoseconds)	60250	3128 → 60250 [PSH, ACK] Seq=1228 Ack=861 Win=64704 Len=180 TSval=125371...	3128	TCP: 3128 → 60250 [PSH, ACK] Seq=1228 Ack...
2024-01-25 13:21:42.3887370384 (nanoseconds)	60250	3128 → 60250 [ACK] Seq=1408 Ack=861 Win=64704 Len=188 TSval=125371160...	3128	TCP: 3128 → 60250 [ACK] Seq=1408 Ack=861...
2024-01-25 13:21:42.3839993744 (nanoseconds)	60250	3128 → 60250 [PSH, ACK] Seq=2596 Ack=861 Win=64704 Len=180 TSval=12537...	3128	TCP: 3128 → 60250 [PSH, ACK] Seq=2596 Ac...
2024-01-25 13:21:42.1001611472 (nanoseconds)			17517	Application Data, Application Data
2024-01-25 13:21:42.3850714352 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=4105 Win=1072 Len=0 TSval=900013138 TSec
2024-01-25 13:21:42.542333	60250	Application Data	3128	TLV.3: Application Data
2024-01-25 13:21:42.2351706320 (nanoseconds)	60250	Application Data	3128	TLV.3: Application Data
2024-01-25 13:21:42.4080650144 (nanoseconds)			17517	Application Data
2024-01-25 13:21:42.3133660336 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=4171 Win=12416 Len=0 TSval=900013138 TSec
2024-01-25 13:21:42.3354894224 (nanoseconds)	60250	Application Data	3128	TLV.3: Application Data
2024-01-25 13:21:42.400703	60250	60250 → 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=341364213 T	3128	TCP: 60250 → 3128 [ACK] Seq=861 Ack=1228 ...
2024-01-25 13:21:42.367120	60250	60250 → 3128 [ACK] Seq=861 Ack=4210 Win=128064 Len=0 TSval=341364213 T	3128	TCP: 60250 → 3128 [ACK] Seq=861 Ack=4210...
2024-01-25 13:21:42.2112887360 (nanoseconds)		..... [TCP Window Update] 60250 → 3128 [ACK] Seq=861 Ack=4210 Win=131072 Len=...		TCP: [TCP Window Update] 60250 → 3128 [AC...

影像- HTTPS傳輸-明確-流程

以下是從SWA到Web伺服器的客戶端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: 2c545a566b5b3f338dc9dbd80ea91ad61035c786954ced219e266ff0b92b9c1
    Session ID Length: 32
    Session ID: 86da348af5508fc24f18f3cbd9829c7282b77e0499e5d2f38466ccbd66821e2
    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 (0xc0ca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)
    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)

```

影像- HTTPS直通-顯式- SWA到Web伺服器-客戶端Hello

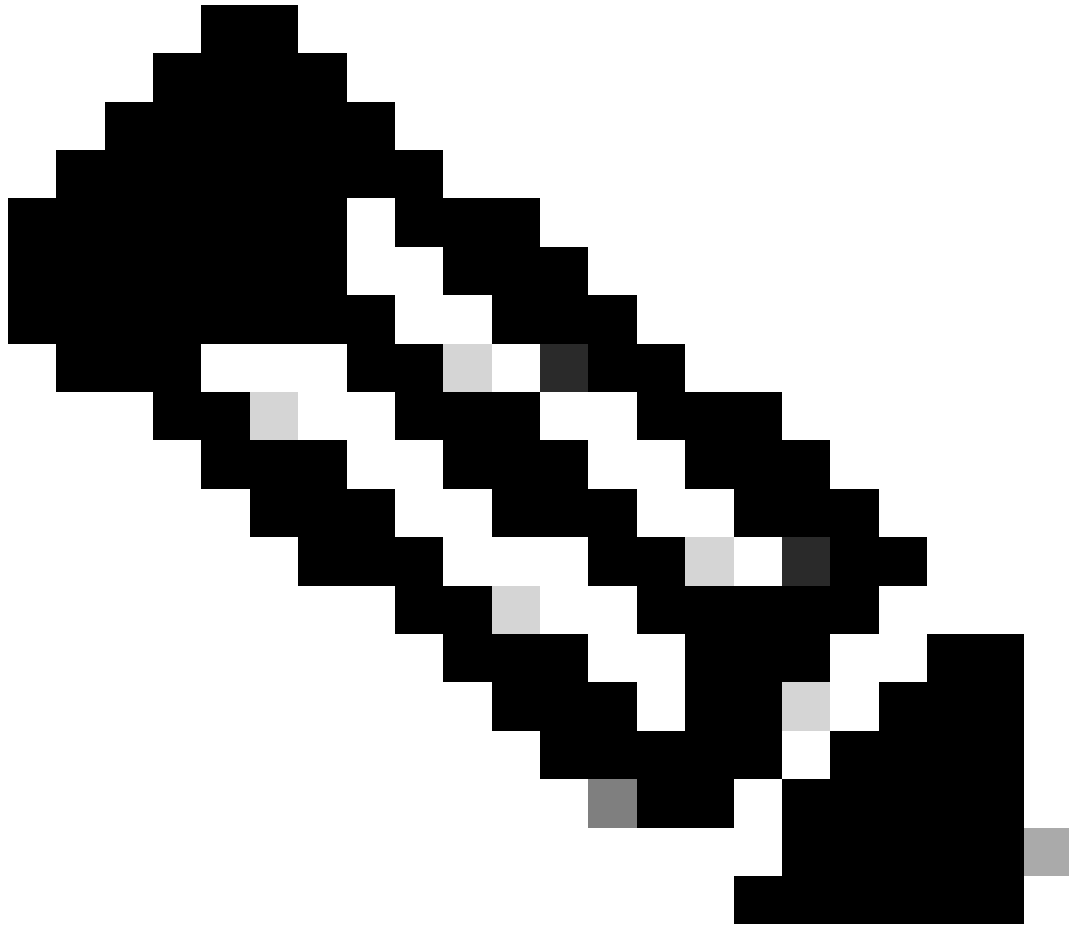
與從客戶端到SWA的客戶端Hello相同：

- ▼ 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 (0xc0a9)
      - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xc0a8)
      - 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)

影象- HTTPS直通-顯式-客戶端到SWA -客戶端Hello

以下是存取日誌範例：

1706185288.920 53395 10.61.70.23 TCP\_MISS/200 6549 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e



附註：如您所見，它只是單行，且動作為PASSTHRU。

---

## 透明部署

### 無身份驗證透明部署中的HTTP流量

#### 客戶端和SWA

網路流量在客戶端的IP地址與Web伺服器的IP地址之間傳輸。

來自使用者端的流量是目的地為TCP連線埠80（不是代理主機連線埠）

- TCP握手。
- 從客戶端獲取HTTP（目標IP = Web伺服器，目標埠= 80）
- 來自代理的HTTP響應（源IP = Web伺服器）
- 資料傳輸



• TCP連線終止 ( 4次握手 )

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	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.	266987	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-客戶端到代理- HTTP -透明-無身份驗證

以下是來自客戶端的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
< 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-客戶端到代理- HTTP -透明-無身份驗證-客戶端HTTP Get

SWA和Web伺服器

網路流量發生在代理的IP地址和Web伺服器的IP地址之間。

從SWA發往TCP埠80的流量 ( 非代理埠 )

- TCP握手。
- HTTP Get from Proxy ( 目標IP = Web伺服器 , 目標埠 = 80 )
- 來自Web伺服器的HTTP響應 ( 源IP =代理伺服器 )
- 資料傳輸
- TCP連線終止 ( 4次握手 )

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	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=6873333
10	2023-12-11 19:13:47.	(285008027...	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.	(387381585...	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=1559577835
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 of a reassembled PDU]
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.	(278488529...	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=11520 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

影像- Proxy和Web伺服器- HTTP -透明-無驗證

以下是來自Proxy的HTTP Get範例

```

> 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
< 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]

```

影象- Proxy to Web Server - HTTP -透明-無身份驗證- Proxy HTTP Get

這表示從客戶端到SWA，然後到Web伺服器，最後返回客戶端的整個流量流。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
7	2023-12-11 19:13:47.372486256	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 19:13:47.372486256	10.201.189.180	Cisco_76:fb:15	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:15	TCP	74	1	80 -> 65132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=6873333 TSecr=0
10	2023-12-11 19:13:47.285000827	10.201.189.180	Cisco_76:fb:15	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:15	93.184.216.34	Cisco_56:5f:44	HTTP	243	1	GET / HTTP/1.1
12	2023-12-11 19:13:47.318451681	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:15	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:15	TCP	1514	1	80 -> 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=1559577035 [TCP segment of a reassembled PDU]
14	2023-12-11 19:13:47.637333	10.201.189.180	Cisco_76:fb:15	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:15	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:15	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 19:14:12.1278488529	10.201.189.180	Cisco_76:fb:15	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:15	TCP	66	1	80 -> 65132 [ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1	2023-12-11 19:14:12.215978816	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:15	TCP	66	1	80 -> 65132 [FIN, ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1	2023-12-11 19:14:12.218383318	10.201.189.180	Cisco_76:fb:15	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

映像-總流量- HTTP -透明-無身份驗證

注意：每個資料流都以不同的顏色區分；從客戶端到SWA的流為一種顏色，從SWA到Web伺服器的流為另一種顏色。

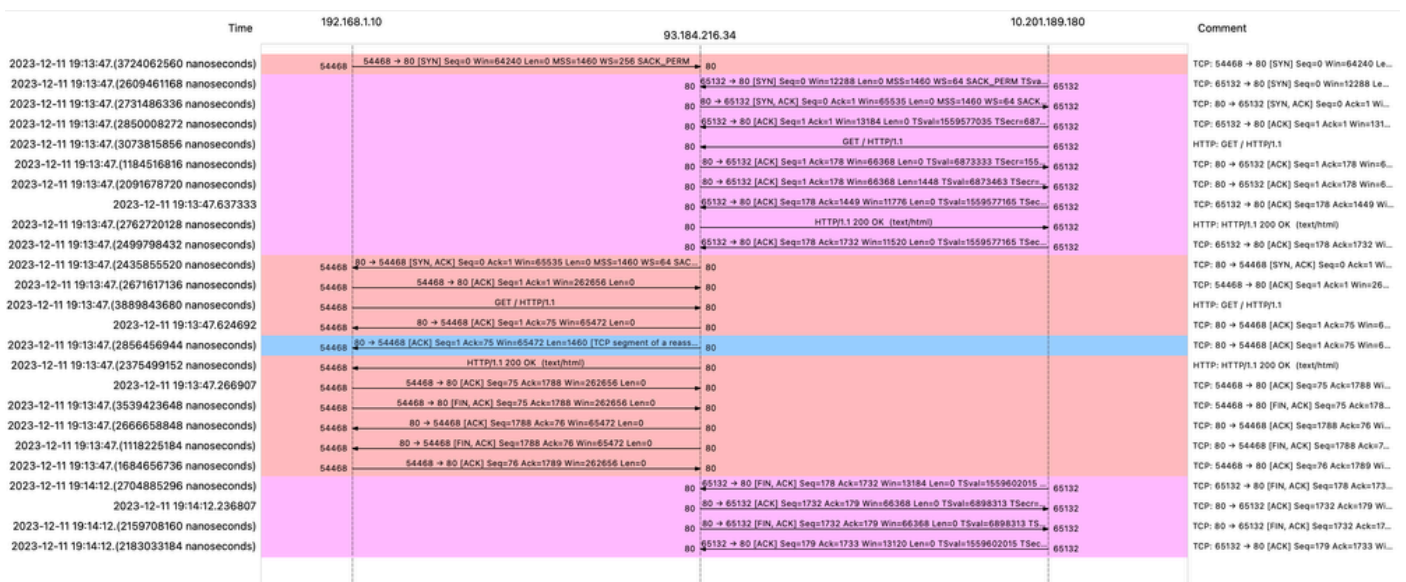


圖- WCCP HTTP流

以下是存取日誌的範例：

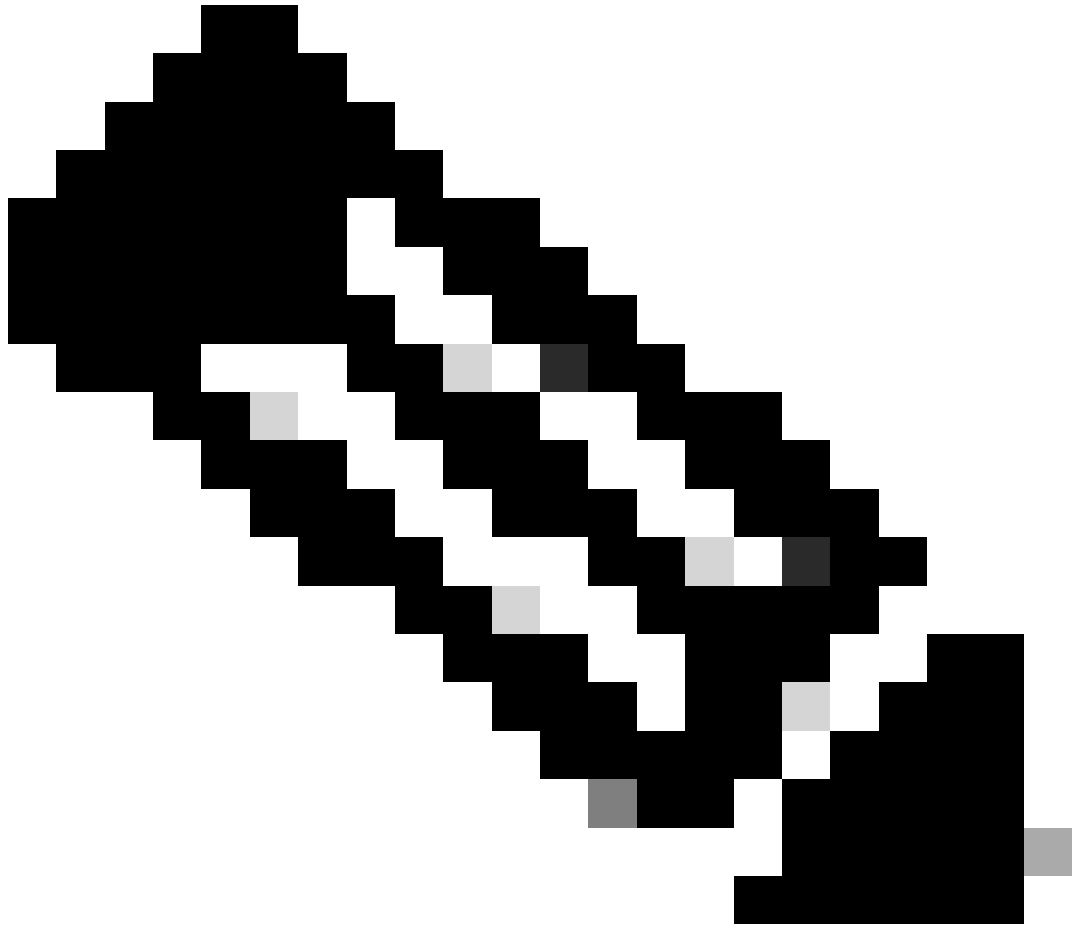
1702318427.181 124 192.168.1.10 TCP\_MISS/200 1787 GET http://www.example.com/ - DIRECT/www.example.com

包含快取資料的流量

這表示當資料在SWA快取中時，從客戶端到SWA的整個流量。

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.	(6563285...	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.	(425926280...	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.	(278830524...	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 TSecr=0
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.	(229146013...	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	439	1	HTTP/1.1 200 OK (text/html)			
28	2023-12-11 19:19:49.	(138640662...	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

映像-快取-總流量- HTTP -透明-無身份驗證



注意：如您所見，Web伺服器傳回HTTP回應304：未修改快取。（在本示例中，資料包編號27）

---

以下是HTTP響應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
< 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-已快取-HTTP響應304 - HTTP -透明-無身份驗證

以下是存取日誌的範例：

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

## 無身份驗證透明部署中的HTTP流量

### 客戶端和SWA

網路流量在客戶端的IP地址與Web伺服器的IP地址之間傳輸。

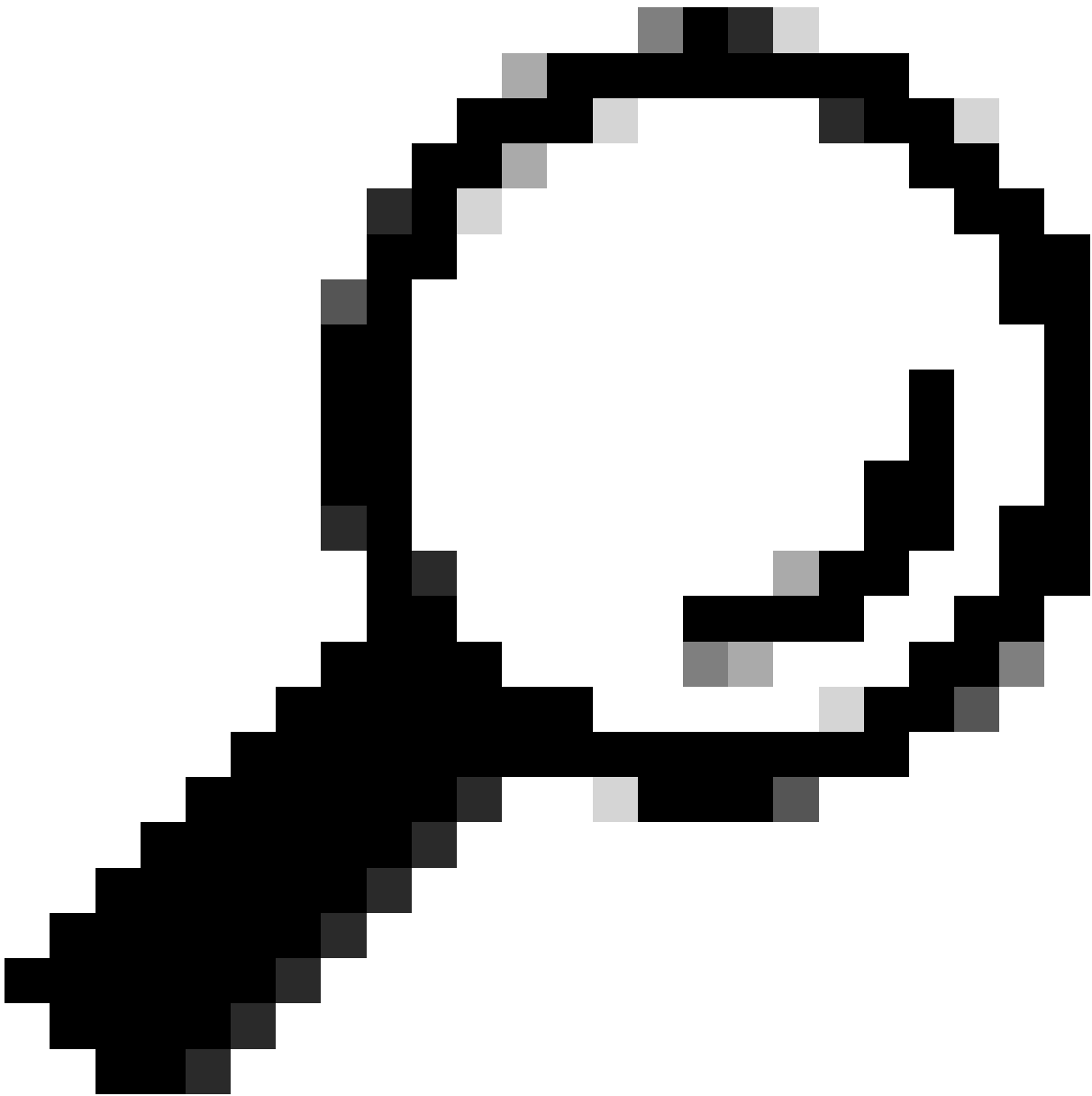
來自客戶端的流量發往TCP埠443 (而不是代理埠)

- TCP握手。
- TLS握手客戶端Hello -伺服器Hello -伺服器金鑰交換-客戶端金鑰交換
- 資料傳輸
- TCP連線終止 (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 19:36:24.387154096	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 19:36:24.366520476	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 19:36:24.258163651	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 19:36:24.215905475	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 19:36:24.298152051	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 19:36:25.413287139	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 19:36:25.181582688	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 19:36:25.186927132	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 19:36:25.378433091	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

以下是客戶端到SWA的客戶端Hello的詳細資訊，如您在伺服器名稱指示(SNI)中看到的Web伺服器的URL，在本示例中為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
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 183
    > 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
      > 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: 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_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_0004,0005,0006,0401,0_]
      [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: 74954a0c86284d0d6e1c4efef92b521]
```



提示：您可以在Wireshark中使用此過濾器搜尋

URL/SNI : `tls.handshake.extensions_server_name == "www.example.com"`

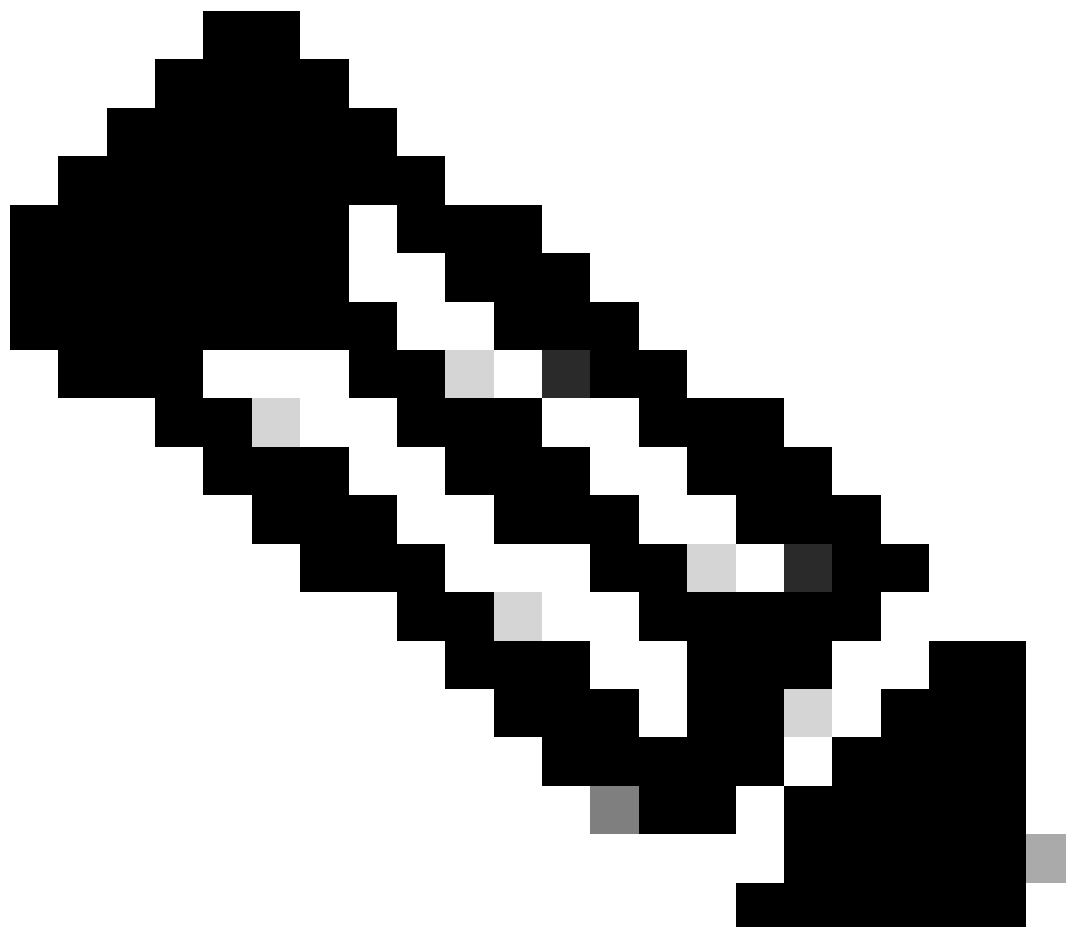
---

以下為伺服器金鑰交換的範例



```
> 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)]
< Transport Layer Security
  < TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 2049
  < Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2045
  < Certificates Length: 2042
  < Certificates (2042 bytes)
    Certificate Length: 1098
  < Certificate [truncated]: 308204463082032ea00302010202140440907379f2aad73d32683b716d2a7ddf2b8e2a300d06092a864886f70d01010b05003040310b30090603550406130255533110300e060355040...
  < signedCertificate
    version: v3 (2)
    serialNumber: 0x0440907379f2aad73d32683b716d2a7ddf2b8e2a
    signature (sha256WithRSAEncryption)
  < issuer: rdnSequence (0)
  < rdnSequence: 4 items (id-at-commonName=CISCOCALO,id-at-organizationalUnitName=IT,id-at-organizationName=wsatest,id-at-countryName=US)
    > RDNSquence item: 1 item (id-at-countryName=US)
    > RDNSquence item: 1 item (id-at-organizationName=wsatest)
    > RDNSquence item: 1 item (id-at-organizationalUnitName=IT)
    > RDNSquence 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]: 308203a63082028ea003020102020900a447d8363a186f2f300d06092a864886f70d01010b05003040310b30090603550406130255533110300e060355040a13077736174657374310...
< Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

映像-伺服器金鑰交換-客戶端到代理-透明-無身份驗證



注意：如您所見，證書是在SWA中配置為解密證書的證書。

## SWA和Web伺服器

網路流量發生在代理的IP地址和Web伺服器的IP地址之間。

從SWA發往TCP埠443的流量（非代理埠）

- TCP握手。
- TLS握手客戶端Hello -伺服器Hello -伺服器金鑰交換-客戶端金鑰交換
- 資料傳輸
- TCP連線終止（4次握手）

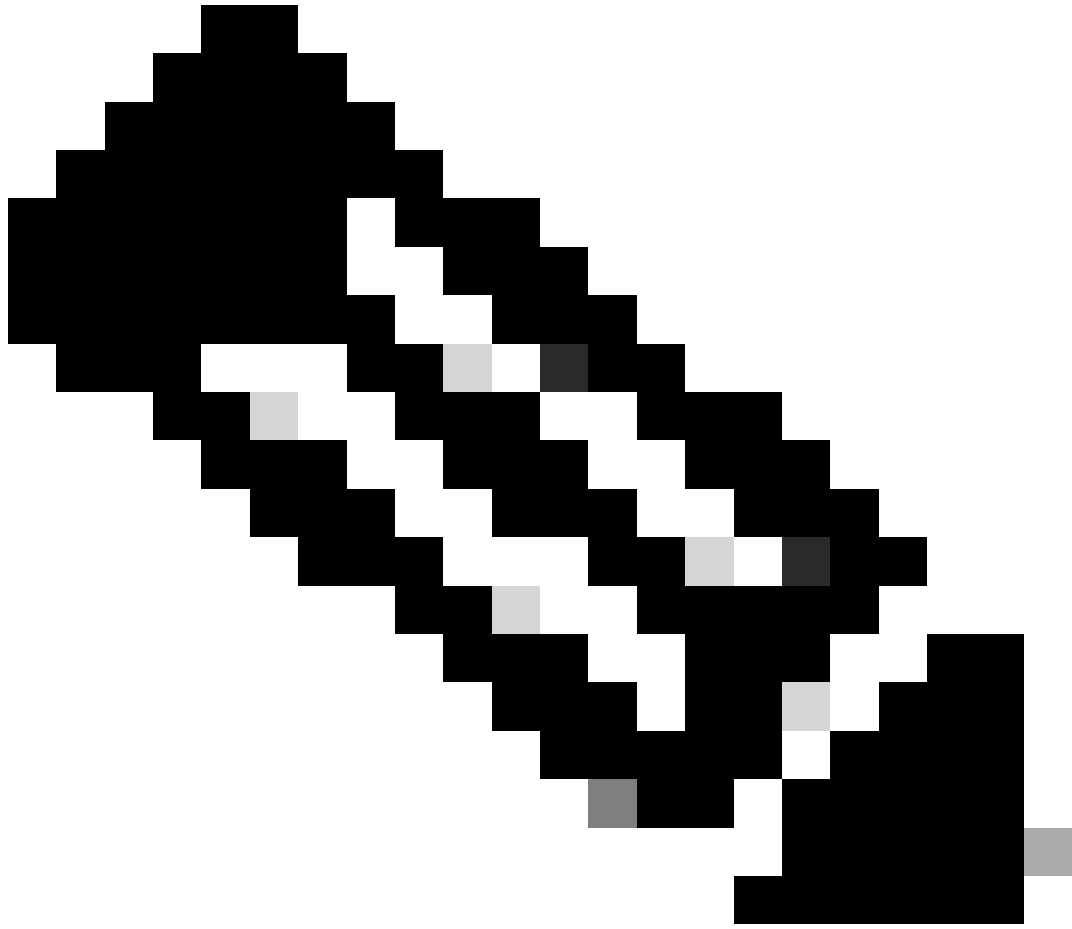
No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
278	2023-12-11 19:36:24.251460652	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	17	47868 → 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1563255033 TSecr=0
279	2023-12-11 19:36:24.128041753	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	17	443 → 47868 [SYN, ACK] Seq=1 Ack=1 Win=13184 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3980365294 TSecr=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 19:36:24.318190081	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 19:36:24.314885984	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 19:36:24.1349459740	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=3980365444
290	2023-12-11 19:36:24.248102688	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 19:36:25.162826084	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 19:36:25.2244187280	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 19:36:25.424899204	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

影像- Web伺服器的代理-HTTP-透明-無驗證

以下是從SWA到Web伺服器的客戶端Hello示例

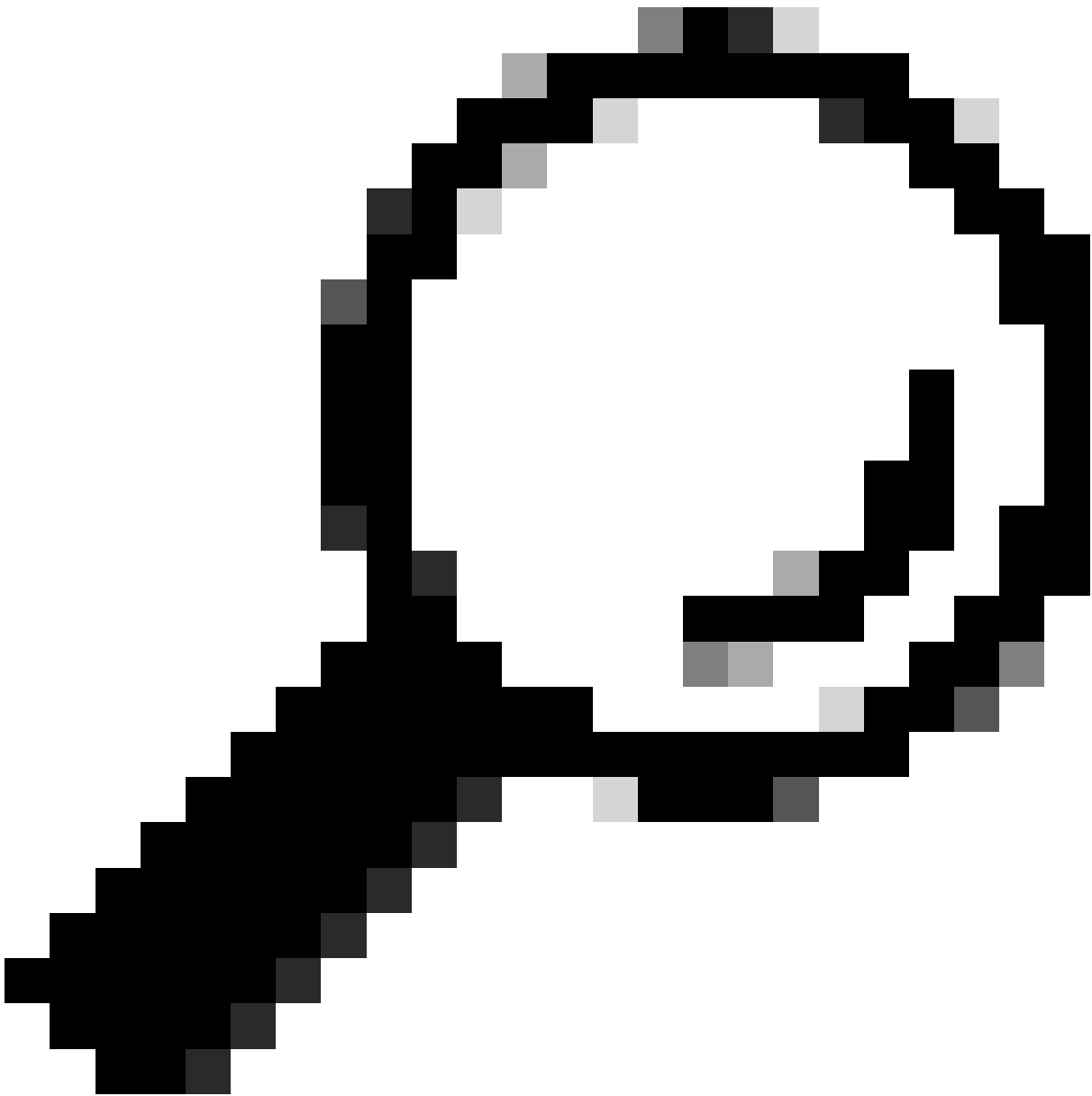
```
> Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface 0
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54515, Dst Port: 443, Seq: 1, Ack: 1, Len: 188
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 183
  > Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 179
    Version: TLS 1.2 (0x0303)
    > Random: 657756ab224a3f6460e99172a8d38f86b689c7eb4bb121bf54d8c96540a0f5d
    Session ID Length: 0
    Cipher Suites Length: 42
    > Cipher Suites (21 suites)
    Compression Methods Length: 1
    > Compression Methods (1 method)
    Extensions Length: 96
  > 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: 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_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_0004_0005_0006_0401_0050]
  [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: 74954a0c86284d0d6e1c4efef92b521]
```

影像-客戶端Hello - Web伺服器的代理-透明-無身份驗證



注意：此處觀察的密碼套件與客戶端到SWA的Hello客戶端中的密碼套件不同，因為配置為解密此流量的SWA使用自己的密碼。

---



提示：在從SWA到Web伺服器的伺服器金鑰交換中，將顯示Web伺服器證書。但是，如果上游代理發現SWA的配置，則會顯示其證書而不是Web伺服器證書。

---

以下是存取日誌的範例：

```
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：如同HTTPS流量的透明部署中所見，訪問日誌中有兩行，第一行是流量被加密時，您可以看到TCP\_CONNECT和Web伺服器的IP地址。如果SWA中啟用了解密，則第二行包含GET，並且整個URL都以HTTPS開頭，這意味著流量已解密並且SWA知道該URL。

---

## 相關資訊

- [技術支援與文件 - Cisco Systems](#)
- [在訪問日誌中配置效能引數- Cisco](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。