

セキュアWebアプライアンスのパケットフローについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[さまざまなタイプのプロキシ導入](#)

[TLSハンドシェイク](#)

[HTTP応答コード](#)

[1xx：情報](#)

[2xx：成功](#)

[3xx：リダイレクション](#)

[4xxコード：クライアントエラー](#)

[5xx：サーバエラー](#)

[明示的な展開](#)

[認証を使用しない明示的な導入でのHTTPトラフィック](#)

[クライアントとSWA](#)

[SWAおよびWebサーバ](#)

[キャッシュされたデータを持つトラフィック](#)

[認証を使用しない明示的な導入でのHTTPトラフィック](#)

[クライアントとSWA](#)

[SWAおよびWebサーバ](#)

[パススルーHTTPSトラフィック](#)

[透過的な導入](#)

[認証を使用しない透過型導入でのHTTPトラフィック](#)

[クライアントとSWA](#)

[SWAおよびWebサーバ](#)

[キャッシュされたデータを持つトラフィック](#)

[認証を使用しない透過型導入でのHTTPトラフィック](#)

[クライアントとSWA](#)

[SWAおよびWebサーバ](#)

[関連情報](#)

はじめに

このドキュメントでは、特にセキュアWebアプライアンス(SWA)に重点を置いた、プロキシ設定ネットワークのネットワークフローについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- TCP/IPの基本概念。
- プロキシ設定に関する基本的な知識。
- プロキシを使用する環境で使用される認証メカニズムに関する基礎知識。

この記事では、次の略語を使用します。

TCP:Transmission Control Protocol (伝送制御プロトコル)

UDP:User Datagram Protocol (ユーザデータグラムプロトコル)

IP:Internet Protocol (インターネットプロトコル)

GRE : 総称ルーティングカプセル化

HTTP : ハイパーテキスト転送プロトコル。

HTTPS:Hypertext Transfer Protocol Secure (ハイパーテキスト転送プロトコルによるセキュリティ)。

URL:Uniform Resource Locator

TLS:Transport Layer Security (トランスポート層セキュリティ)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

さまざまなタイプのプロキシ導入

TLSハンドシェイク

HTTPSでのTLSハンドシェイクは、クライアントとサーバがインターネット経由で通信し、セキュアな接続を提供する際に発生します。このプロセスは、通信する2つのアプリケーション間のプライバシーとデータ整合性を維持します。これは、クライアントとサーバが後続のすべての送信に対する暗号化標準とコードに合意する一連の手順を通じて動作します。このハンドシェイクの目的は、第三者による不正なアクセスや操作を防止することです。また、偽装を排除するために、通信相手のIDも認証します。このプロセスは、転送中のデータの安全性を確保するため、HTTPSでは非常に重要です。

TLSハンドシェイクの手順を次に示します。

1. Client Hello : クライアントがhelloメッセージを使用してハンドシェイクプロセスを開始します。このメッセージには、クライアントのTLSバージョン、サポートされている暗号スイート、および「クライアントランダム」と呼ばれるランダムバイト文字列が含まれています。
2. Server Hello : サーバはhelloメッセージで応答します。このメッセージには、サーバが選択したTLSバージョン、選択した暗号スイート、「サーバランダム」と呼ばれるランダムバイト文字列、およびサーバのデジタル証明書が含まれます。必要に応じて、サーバは、相互認証のためにクライアントのデジタル証明書も要求します。
3. クライアントがサーバ証明書を確​​認する : クライアントは、サーバのデジタル証明書を、それを発行した認証局と照合します。これにより、クライアントが正規のサーバと通信していることが保証されます。
4. プレマスターシークレット : クライアントは「プレマスターシークレット」と呼ばれるランダムなバイト文字列を送信し、セッションキーの作成に使用します。クライアントは、このプレマスターシークレットをサーバ公開キーで暗号化するため、サーバだけが秘密キーで復号化できます。
5. マスターシークレット : クライアントとサーバの両方が、プレマスターシークレットとhelloメッセージのランダムバイト文字列を使用して、同じ「マスターシークレット」を個別に計算します。この共有秘密がセッションキーを生成する基礎になります。
6. Client Finished : クライアントは「Finished」メッセージをセッションキーで暗号化して送信し、ハンドシェイクのクライアント部分の完了を通知します。
7. Server Finished : サーバは「Finished」メッセージを送信します。このメッセージもセッションキーで暗号化され、ハンドシェイクのサーバ部分の完了を通知します。

HTTP応答コード

1xx : 情報

コード	詳細
100継続	通常は、ICAP プロトコル関連の応答です。これは、データの送信を続行できることをクライアントに知らせる情報応答です。ICAPサービス(ウイルススキャンなど)に関しては、サーバは最初のxバイトのみを参照できます。最初のバイトセットのスキャンが完了し、ウイルスを検出しなかった場合、クライアントにオブジェクトの残りの部分の送信を通知するために100 Continueを送信します。

2xx : 成功

コード	詳細
-----	----

200 OK	最も一般的な応答コードです。これは、要求が問題なく成功したことを示します。
--------	---------------------------------------

3xx : リダイレクト

コード	詳細
301永続的リダイレクション	これは永続的なリダイレクトです。wwwサブドメインにリダイレクトする際に、このコードが表示されます。
302一時リダイレクション	一時的なリダイレクションです。クライアントは、Location : ヘッダーで指定されたオブジェクトに対して新しい要求を作成するように指示されます。
304未変更	GIMS (GET If-modified-since) に対する応答です。これは文字通り、ヘッダーIf-modified-since: <date>を含む標準HTTP GETです。このヘッダーは、クライアントが要求されたオブジェクトのコピーをローカルキャッシュに持っており、オブジェクトがフェッチされた日付を含んでいることをサーバに通知します。その日付以降にオブジェクトが変更されている場合、サーバは200 OKとオブジェクトの新しいコピーで応答します。フェッチされた日付以降にオブジェクトが変更されていない場合、サーバは304 Not Modified応答を返信します。
307認証リダイレクション	これは、透過的なプロキシ導入では、プロキシサーバが要求を認証し、ユーザを認証するために要求を別のURLにリダイレクトするように設定されている場合に最も多く見られます。

4xxコード : クライアントエラー

コード	詳細
400件の不正な要求	これは、HTTP要求が適切な構文に準拠していないため、この要求に関する問題があることを示唆しています。1行に複数のヘッダーがある、ヘッダー内にスペースがある、URIにHTTP/1.1が含まれていない、などの理由が考えられます。正しい構文については、RFC 2616を参照してください。
401不正 Webサーバー認証が必要です	要求されたオブジェクトへのアクセスには認証が必要です。401コードは、ターゲットWebサーバとの認証に使用されます。SWAがトランスペアレントモードで動作し、プロキシで認証が有効である場合、アプライアンスはそれ自体をOCS (元のコンテンツサーバ) で

	<p>あるかのように認識するため、クライアントに401を返します。</p> <p>使用できる認証方式は、「www-authenticate:」HTTP応答ヘッダーに詳細が記述されています。これにより、サーバがNTLM、基本、またはその他の形式の認証を要求しているかどうかをクライアントに通知します。</p>
403拒否	<p>クライアントは要求されたオブジェクトにアクセスできません。さまざまな理由により、サーバがオブジェクトアクセスを拒否する可能性があります。サーバは通常、HTTPデータまたはHTML応答内に原因の説明を提供します。</p>
404が見つかりません	<p>要求されたオブジェクトがサーバ上にありません。</p>
407プロキシ認証が必要	<p>これは401と同じですが、OCSではなくプロキシに対する認証に特化している点が異なります。この応答が返されるのは、要求が明示的にプロキシに送信された場合のみです。</p> <p>SWAがトランスペアレントプロキシとして設定されている場合、クライアントはプロキシの存在を認識しないため、407をクライアントに送信することはできません。この場合、クライアントはおそらくTCPソケットをFINまたはRSTします。</p>

5xx : サーバエラー

コード	詳細
501内部サーバエラー	<p>汎用Webサーバーのエラーです。</p>
502不正なゲートウェイ	<p>ゲートウェイまたはプロキシとして動作しているサーバーが受信サーバーから無効な応答を受信したときに発生します。これは、ゲートウェイがアップストリームまたは発信元サーバから不適切な応答を受信したことを示します。</p>
503サービス使用不可	<p>一時的な過負荷またはスケジュールされたメンテナンスが原因で、サーバが現在要求を処理できないことを示します。これは、サーバが一時的にアウトオブサービスになっているが、しばらくすると再び使用可能になる可能性があることを意味します。</p>
504ゲートウェイタイムアウト	<p>クライアントまたはプロキシが、Webページをロードまたはブラウザによる別の要求を実行するためにアクセスしようとしたWebサー</p>

バから、タイムリーな応答を受信しなかったことを示します。これは、多くの場合、アップストリームサーバがダウンしていることを意味します。

明示的な展開

Here....

認証を使用しない明示的な導入でのHTTPトラフィック

クライアントとSWA

ネットワークトラフィックは、クライアントのIPアドレスとSWAプロキシインターフェイスのIPアドレスの間で送受信されます (通常はP1インターフェイスですが、プロキシの設定によってはP2または管理インターフェイスになる場合があります) 。

クライアントからのトラフィックは、TCPポート80または3128を経由してSWAに到達します (デフォルトのSWAプロキシポートはTCP 80および3128です。この例では、ポート3128を使用します)

- TCPハンドシェイク。
- クライアントからのHTTP Get (宛先IP = SWA IP、宛先ポート = 3128)
- プロキシからのHTTP応答 (送信元IP = SWA)
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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=1762371708 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=322700808
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=3227008037
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=3227008047 TSecr=1762371849
12851	2024-01-25 09:35:26.286288	10.48.48.185	Vmware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	1254	2	3128 - 65238 [ACK] Seq=1 Ack=123 Win=65408 Len=1188 TSval=3227001086 TSecr=1762371849 [TCP
12852	2024-01-25 09:35:26.286297	10.48.48.185	Vmware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	HTTP	599	2	HTTP/1.1 200 OK (text/html)
12992	2024-01-25 09:35:26.347713	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	TCP	66	2	65238 - 3128 [ACK] Seq=123 Ack=1189 Win=131072 Len=0 TSval=1762372145 TSecr=3227001086
12993	2024-01-25 09:35:26.347815	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	TCP	66	2	65238 - 3128 [ACK] Seq=123 Ack=1722 Win=130560 Len=0 TSval=1762372145 TSecr=3227001086
12994	2024-01-25 09:35:26.353174	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	TCP	66	2	65238 - 3128 [FIN, ACK] Seq=123 Ack=1722 Win=131072 Len=0 TSval=1762372150 TSecr=3227001086
12995	2024-01-25 09:35:26.353217	10.48.48.185	Vmware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 - 65238 [ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12996	2024-01-25 09:35:26.353397	10.48.48.185	Vmware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 - 65238 [FIN, ACK] Seq=1722 Ack=124 Win=65408 Len=0 TSval=3227001147 TSecr=1762372150
12997	2024-01-25 09:35:26.412438	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	TCP	66	2	65238 - 3128 [ACK] Seq=124 Ack=1723 Win=131072 Len=0 TSval=1762372212 TSecr=3227001147

イメージクライアントからSWA、HTTP明示的モード

SWAおよびWebサーバ

ネットワークトラフィックは、プロキシのIPアドレスとWebサーバのIPアドレスの間で発生します。

SWAからのトラフィックはTCPポート80を宛先とし、送信元はランダムなポート (プロキシポートではない) です

- TCPハンドシェイク。
- プロキシからのHTTP Get (宛先IP = Webサーバ、宛先ポート = 80)
- WebサーバからのHTTP応答 (送信元IP = プロキシサーバ)
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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=1360 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

イメージ : WebサーバへのHTTP-SWA-Explicit-no cache

クライアントからのHTTP Getの例を次に示します

```

> 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]

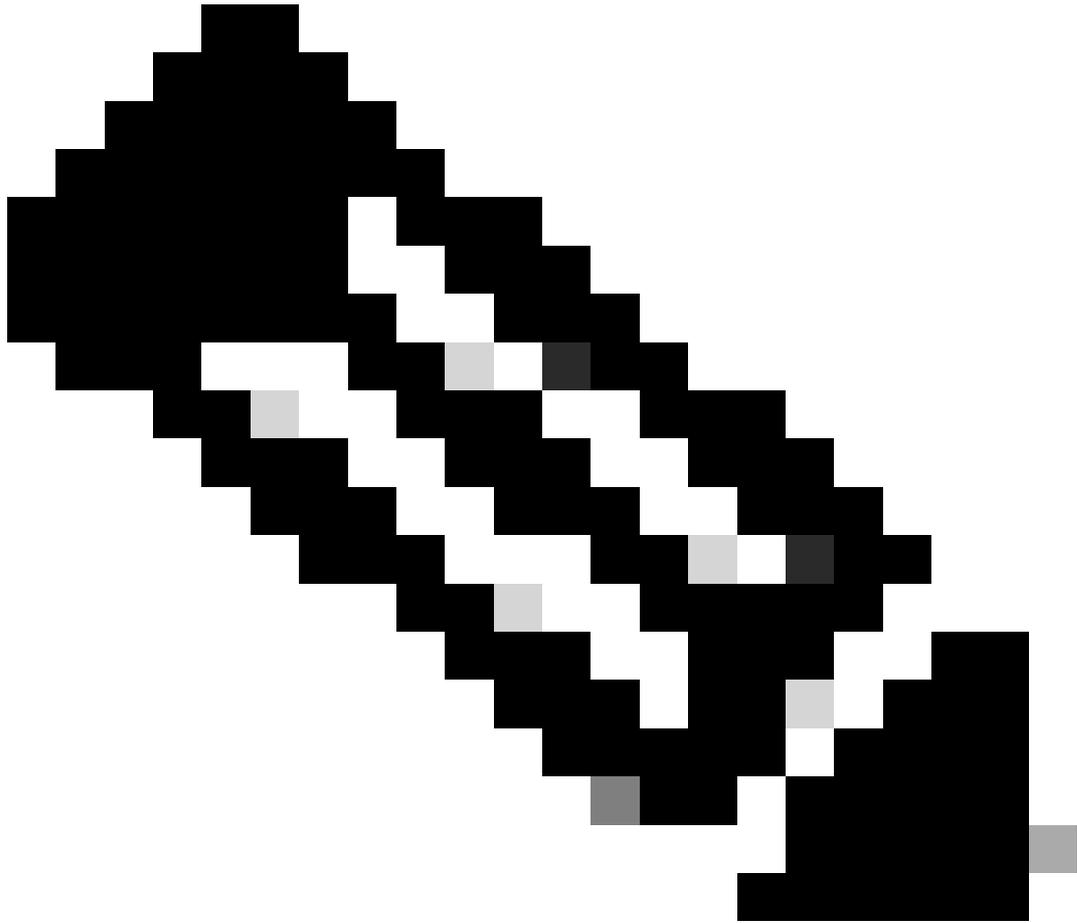
```

イメージ - SWAへのクライアントHTTP GET - 明示的

これは、クライアントからSWA、Webサーバ、そして最後にクライアントに戻るトラフィックのフロー全体を表します。

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 TSval=1762371849 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=322700883
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=132288 Len=0 TSval=1762371848 TSecr=3227008837
12568	2024-01-25 09:35:26.046877	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 09:35:26.046945	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=3227008847 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=1360 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 09:35:26.347113	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

イメージ - すべてのトラフィックHTTP明示的 - キャッシュなし



注：トラフィックの各ストリームは異なる色で区別されます。クライアントからSWAへのフローは1色で、SWAからWebサーバへのフローは別の色です。

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...	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...	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...	TCP: 23146 → 80 [ACK] Seq=1 Ack=1 Win=135...
2024-01-25 09:35:26.168172			GET / HTTP/1.1	HTTP: GET / HTTP/1.1
2024-01-25 09:35:26.280446			80 → 23146 [ACK] Seq=1 Ack=177 Win=67072	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	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...	TCP: 23146 → 80 [ACK] Seq=177 Ack=1349 WL...
2024-01-25 09:35:26.281793			HTTP/1.1 200 OK (text/html)	HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:35:26.281801			23146 → 80 [ACK] Seq=177 Ack=1608 Win=11...	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 ...

イメージ - トラフィックフロー - HTTP明示 - キャッシュなし

アクセスログの例を次に示します。

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

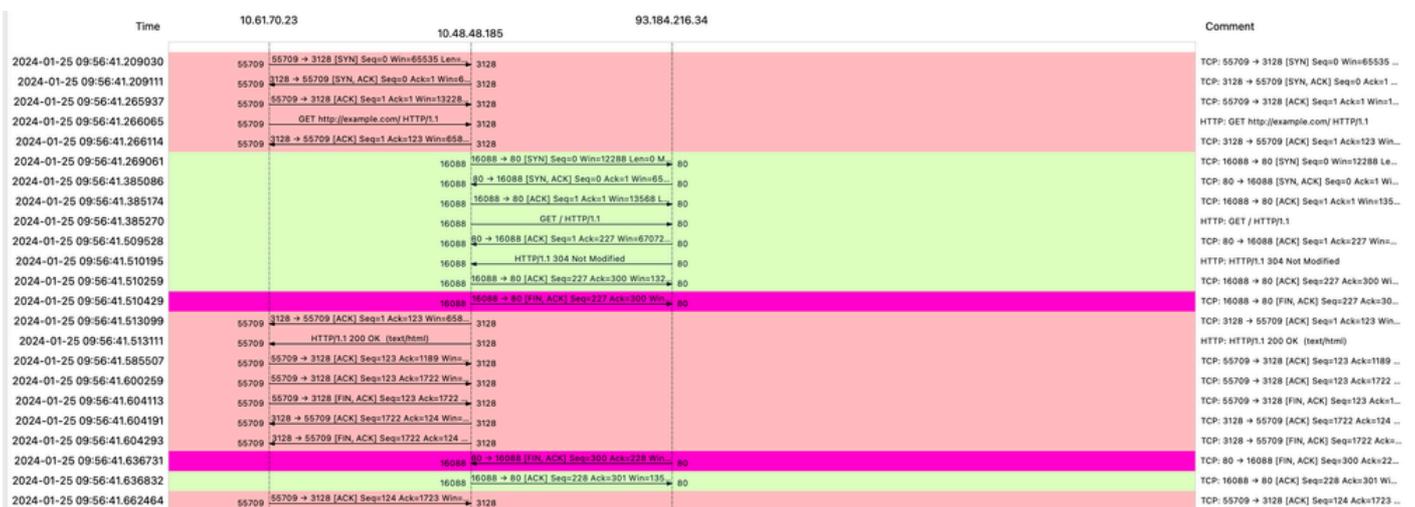
キャッシュされたデータを持つトラフィック

これは、データがSWAキャッシュにある場合の、クライアントからSWAへのトラフィックのプロ全体を表します。

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	TCP	66	2	55709 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=3417110333 TSecr=3687923930
1923	2024-01-25 09:56:41.266065	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	Vmware_8d:f3:64	HTTP	188	2	GET http://example.com/ HTTP/1.1
1924	2024-01-25 09:56:41.266114	10.48.48.185	Vmware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65856 Len=0 TSval=3687923930 TSecr=3417110333
1925	2024-01-25 09:56:41.269061	10.48.48.185	Vmware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	74	3	16088 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1360 WS=64 SACK_PERM TSval=3191296932 TSecr=0
1943	2024-01-25 09:56:41.385806	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

イメージ : HTTP明示的にキャッシュされたデータ

注：ご覧のように、WebサーバはHTTP応答304：キャッシュは変更されていません (HTTP response 304: Cache not Modified)を返します。(この例では、パケット番号 1947)



イメージ：キャッシュを使用した明示的なフローHTTP

HTTP応答304の例を次に示します

```
> 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/]
```

イメージ : HTTP明示的304応答

アクセスログの例を次に示します。

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

認証を使用しない明示的な導入でのHTTPトラフィック

クライアントとSWA

ネットワークトラフィックは、クライアントのIPアドレスとSWAプロキシインターフェイスのIPアドレスの間で送受信されます (通常はP1インターフェイスですが、プロキシの設定によってはP2または管理インターフェイスになる場合があります)。

クライアントからのトラフィックは、TCPポート80または3128を経由してSWAに到達します (デフォルトのSWAプロキシポートはTCP 80および3128です。この例では、ポート3128を使用します)

- TCPハンドシェイク。
- クライアントからのHTTP CONNECT (宛先IP = SWA、宛先ポート= 3128)
- プロキシからのHTTP応答 (送信元IP = SWA)
- Client HelloとURLのSNI (送信元IP =クライアント)
- Server Hello (送信元IP = SWA)
- サーバキー交換 (送信元IP = SWA)
- クライアントキー交換 (送信元IP =クライアント)
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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_PERM
19	2024-01-25 12:31:37.330015315	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	74	12	3128 → 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1468 WS=64 SACK_PERM TSval=441495437
20	2024-01-25 12:31:37.370297760	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1 Ack=1 Win=132288 Len=0 TSval=1676451392 TSecr=441495437
21	2024-01-25 12:31:37.383167	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	HTTP	277	12	CONNECT example.com:443 HTTP/1.1
22	2024-01-25 12:31:37.324946619	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=1 Ack=212 Win=65344 Len=0 TSval=441495507 TSecr=1676451392
26	2024-01-25 12:31:38.731815	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	HTTP	105	12	HTTP/1.1 200 Connection established
27	2024-01-25 12:31:38.308877561	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=1676451630 TSecr=441495677
28	2024-01-25 12:31:38.322347166	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TLSv1.2	715	12	Client Hello [SNI=example.com]
29	2024-01-25 12:31:38.182072475	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=441495747 TSecr=1676451630
49	2024-01-25 12:31:38.282097660	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Server Hello
50	2024-01-25 12:31:38.153429867	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Certificate
51	2024-01-25 12:31:38.965425	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	190	12	Server Key Exchange, Server Hello Done
54	2024-01-25 12:31:38.824826	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=441496237
55	2024-01-25 12:31:38.344661913	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=441496237
56	2024-01-25 12:31:38.173832950	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TLSv1.2	159	12	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2024-01-25 12:31:38.422856787	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2540 Ack=954 Win=64640 Len=0 TSval=441496317 TSecr=1676452193
58	2024-01-25 12:31:38.244514147	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	117	12	Change Cipher Spec, Encrypted Handshake Message
59	2024-01-25 12:31:38.328702336	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=954 Ack=2591 Win=131008 Len=0 TSval=1676452265 TSecr=441496317
60	2024-01-25 12:31:38.151248214	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TLSv1.2	562	12	Application Data
61	2024-01-25 12:31:38.257435452	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=2591 Ack=1450 Win=64192 Len=0 TSval=441496387 TSecr=1676452265
82	2024-01-25 12:31:39.165086323	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	112	12	Application Data
83	2024-01-25 12:31:39.342008	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=2637 Win=131008 Len=0 TSval=1676452764 TSecr=441496807
84	2024-01-25 12:31:39.200484740	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1209	12	Application Data, Application Data
85	2024-01-25 12:31:39.128618294	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=441496807
86	2024-01-25 12:31:39.092047	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TLSv1.2	497	12	Application Data
87	2024-01-25 12:31:39.277809790	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 → 61484 [ACK] Seq=3780 Ack=1881 Win=63808 Len=0 TSval=441496997 TSecr=1676452884
94	2024-01-25 12:31:39.126123713	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	119	12	Application Data
95	2024-01-25 12:31:39.680580	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1881 Ack=3833 Win=131008 Len=0 TSval=1676453324 TSecr=441497377
96	2024-01-25 12:31:39.288575172	10.48.48.165	Vmware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1192	12	Application Data, Application Data
97	2024-01-25 12:31:39.295531248	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	66	12	61484 → 3128 [ACK] Seq=1881 Ack=4959 Win=129920 Len=0 TSval=1676453397 TSecr=441497447
150	2024-01-25 12:31:49.143314836	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	Vmware_8d:9a:f4	TCP	60	12	[TCP Keep-Alive] 61484 → 3128 [ACK] Seq=1880 Ack=4959 Win=131072 Len=0

イメージ – SWAへのHTTPSクライアント – 明示的 – キャッシュなし

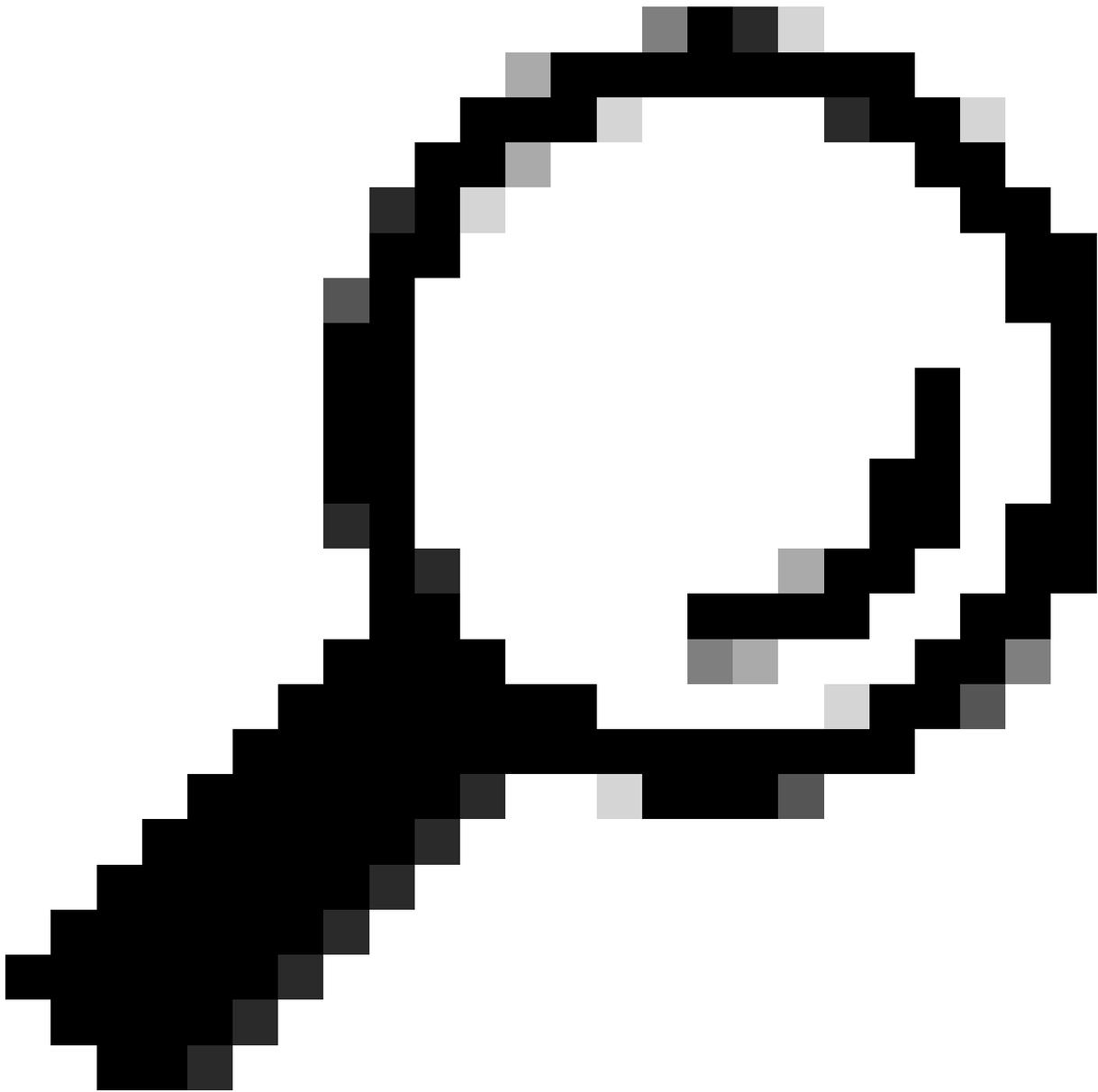
Server Name Indication(SNI)でWebサーバのURLを確認できるように、クライアントからSWAへのClient Helloの詳細を次に示します。この例では、www.example.comであり、クライアントは17個の暗号スイートをアドバタイズしています。

```

> 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]

```

イメージ – HTTPSクライアントhello – 明示的 – SWAへのクライアント



ヒント : このフィルタをWiresharkで使用して、URL/SNI
:tls.handshake.extensions_server_name == "www.example.com"を検索できます。

次に、SWAがクライアントに送信した証明書の例を示します

```

> 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)]
> Hypertext Transfer Protocol
  [Proxy-Connect-Hostname: example.com]
  [Proxy-Connect-Port: 443]
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 2100
  > Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2096
    Certificates Length: 2093
  > Certificates (2093 bytes)
    Certificate Length: 1105
  > Certificate [truncated]: 3082044d30820335a00302010202140279103122f2aad73d32683b716d2a7d4ead7d47300d06092a864886f70d010b05003047310b3009060355040613025553310e300c060355040a1.
  > signedCertificate
    version: v3 (2)
    serialNumber: 0x0279103122f2aad73d32683b716d2a7d4ead7d47
    > signature (sha256WithRSAEncryption)
    > issuer: rdnsSequence (0)
  > rdnsSequence: 4 items (id-at-commonName=CISCO LAB Explicit, id-at-organizationalUnitName=IT, id-at-organizationName=Cisco, id-at-countryName=US)
    > RDNSSequence item: 1 item (id-at-countryName=US)
      > RelativeDistinguishedName item (id-at-countryName=US)
        Object Id: 2.5.4.6 (id-at-countryName)
        CountryName: US
    > RDNSSequence item: 1 item (id-at-organizationName=Cisco)
      > RelativeDistinguishedName item (id-at-organizationName=Cisco)
        Object Id: 2.5.4.10 (id-at-organizationName)
        > DirectoryString: printableString (1)
          printableString: Cisco
    > RDNSSequence item: 1 item (id-at-organizationalUnitName=IT)
      > RelativeDistinguishedName item (id-at-organizationalUnitName=IT)
        Object Id: 2.5.4.11 (id-at-organizationalUnitName)
        > DirectoryString: printableString (1)
          printableString: IT
    > RDNSSequence item: 1 item (id-at-commonName=CISCO LAB Explicit)
      > RelativeDistinguishedName item (id-at-commonName=CISCO LAB Explicit)
        Object Id: 2.5.4.3 (id-at-commonName)
        > DirectoryString: printableString (1)
          printableString: CISCO LAB Explicit

```

イメージ - HTTPS証明書 - 明示的 - クライアントへのSWA

SWAおよびWebサーバ

ネットワークトラフィックは、プロキシのIPアドレスとWebサーバのIPアドレスの間で発生します。

SWAからのトラフィックは、TCPポート443 (プロキシポートではない)宛てです

- TCPハンドシェイク。
- クライアントHello (宛先IP = Webサーバ、宛先ポート= 443)
- Server Hello (送信元IP = Webサーバ)
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=1727280976 TSecr=0
25	2024-01-25 12:31:38.893381	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 (SNIM=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 12:31:38.1341489009.	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=254935368
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 12:31:38.161048344..	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 12:31:38.1414028590.	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=2549353908 TSecr=1727281420
64	2024-01-25 12:31:38.1296760748..	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 12:31:38.141911657..	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 12:31:38.3480012513..	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 12:31:39.2832080660..	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=1727282019 TSecr=2549354468
79	2024-01-25 12:31:39.1395843076..	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 12:31:39.1305106563..	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 12:31:39.1347738670..	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 12:31:39.1186179736..	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 12:31:39.128228742..	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

イメージ - HTTPS - 明示的 - WebサーバへのSWA

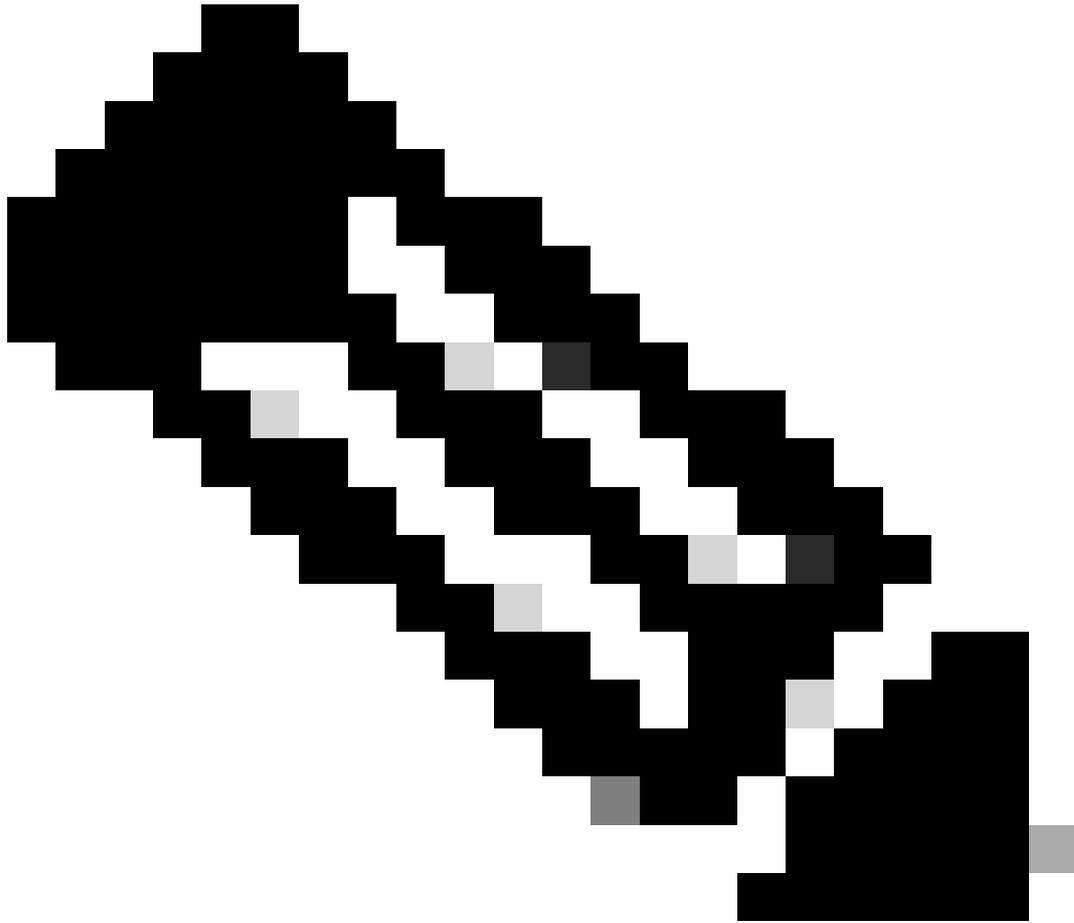
SWAからWebサーバへのClient Helloの詳細を次に示します。これは、SWAが12の暗号スイートをアドバタイズしたためです。

```

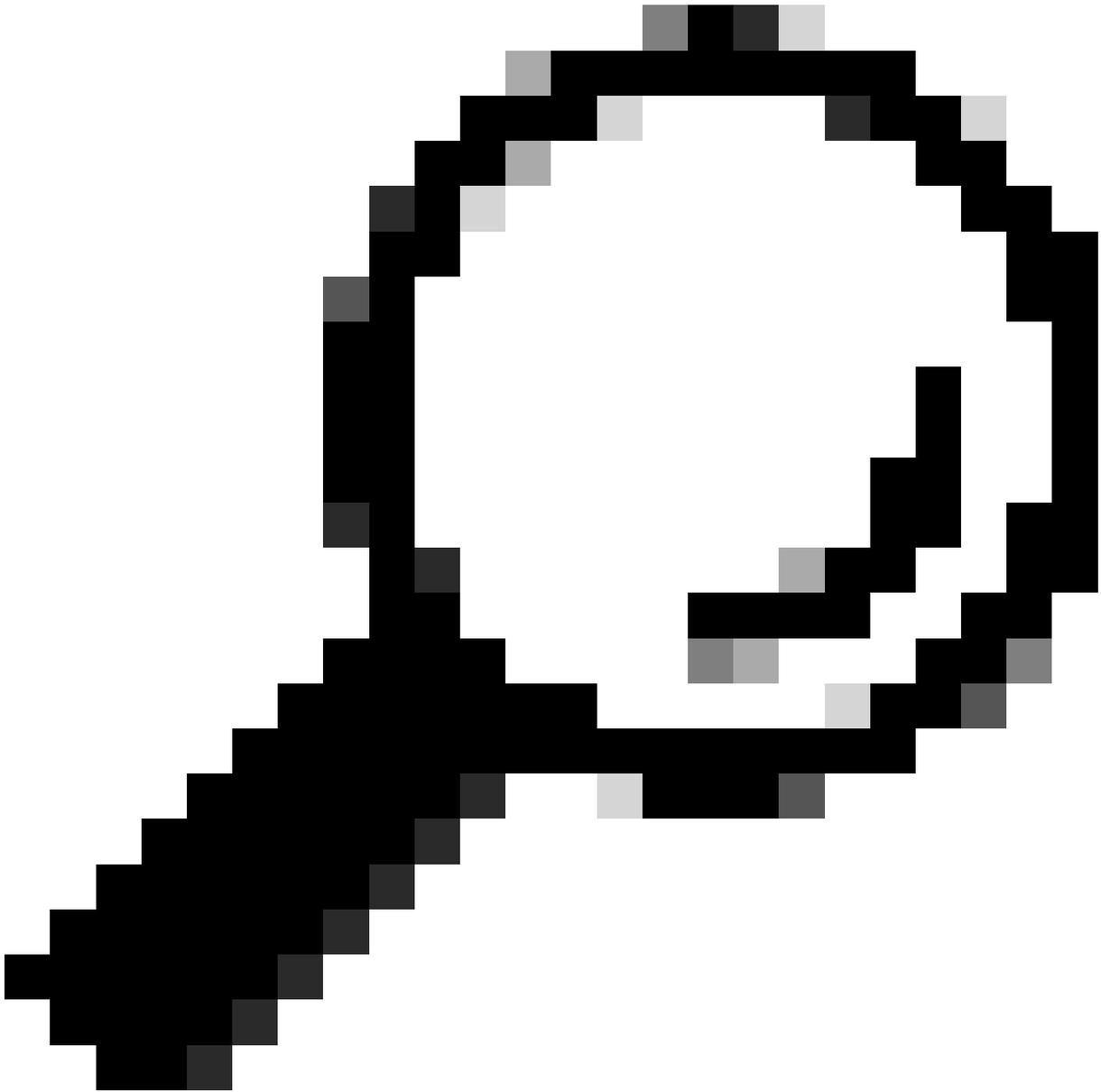
> Frame 30: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits)
> Ethernet II, Src: VMware_8d:9a:f4 (00:50:56:8d:9a:f4), Dst: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff)
> Internet Protocol Version 4, Src: 10.48.48.165, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 24953, Dst Port: 443, 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: 6601ee708d9db71cf5c7c4584e5facdf08d4de00b208f6d6eb6ade08cc7d3e14
      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]

```

イメージ – HTTPSクライアントHello - WebサーバへのSWA – キャッシュなし



注：ここで観察された暗号スイートは、クライアントからSWAへのClient Helloの暗号スイートとは異なります。これは、このトラフィックを復号化するように設定されたSWAが独自の暗号を使用するためです。



ヒント:SWAからWebサーバへのサーバキー交換では、Webサーバ証明書が表示されます。ただし、アップストリームプロキシがSWAの設定を検出すると、Webサーバ証明書の代わりに証明書が表示されます。

クライアントからのHTTP CONNECTのサンプルを次に示します。

```

> 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]

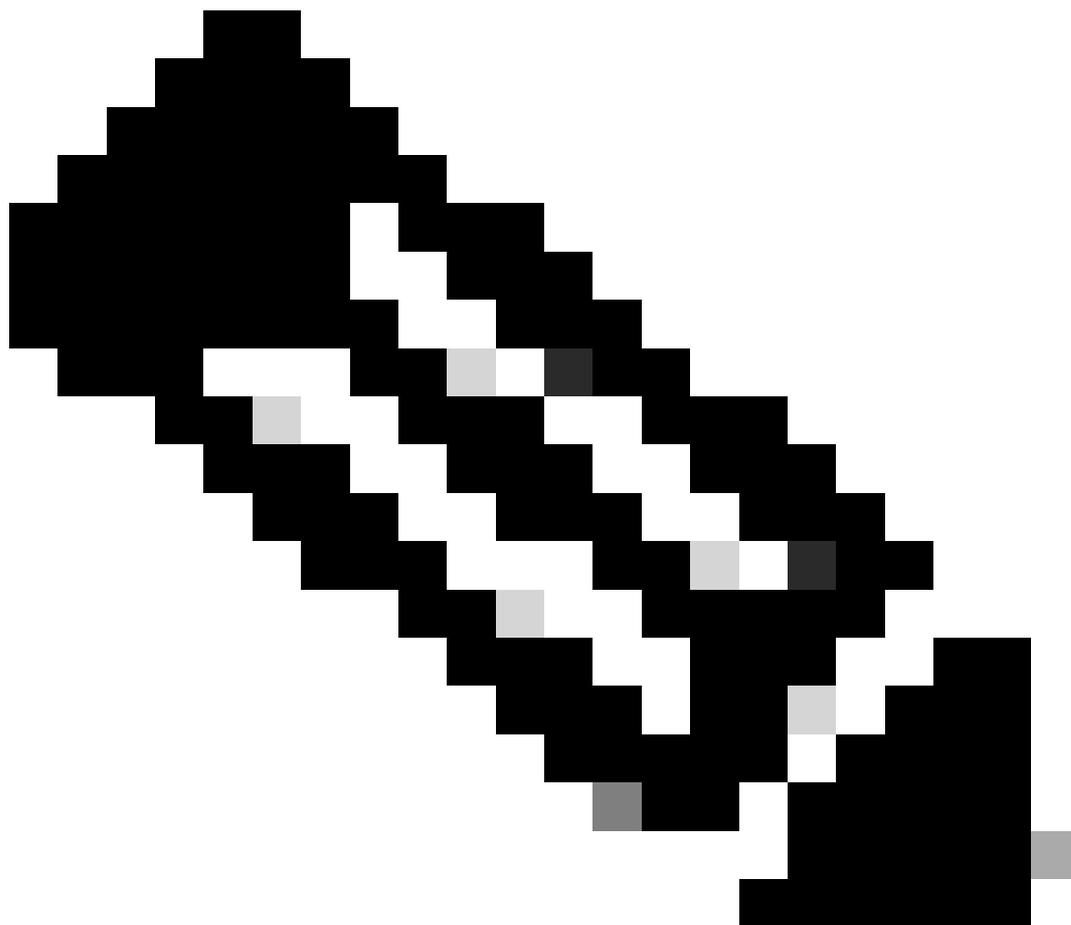
```

イメージ：クライアントHTTP接続

これは、クライアントからSWA、Webサーバ、そして最後にクライアントに戻るトラフィックのフロー全体を表します。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
18	2024-01-25 12:31:37.31816644...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	78	12	61484 - 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1676451324 TSecr=0 SACK_PERM TSval=44
19	2024-01-25 12:31:37.330015315...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	74	12	3128 - 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1727280971
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 12:31:37.383991...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	74	13	24953 - 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=2549353418 TSecr=0
24	2024-01-25 12:31:38.006918...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	74	13	443 - 24953 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=1727280971
25	2024-01-25 12:31:38.009381...	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 12:31:38.380897561...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 - 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=1676451630 TSecr=441495677
28	2024-01-25 12:31:38.322347166...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	715	12	Client Hello (SNI=example.com)
29	2024-01-25 12:31:38.182072475...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 - 61484 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=4414955747 TSecr=1676451630
30	2024-01-25 12:31:38.350314...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	259	13	Client Hello (SNI=example.com)
31	2024-01-25 12:31:38.146535406...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 - 24953 [ACK] Seq=1 Ack=194 Win=67072 Len=0 TSval=1727281239 TSecr=2549353688
32	2024-01-25 12:31:38.273839971...	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 12:31:38.1723349971...	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 12:31:38.141480909...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	1434	13	443 - 24953 [PSH, ACK] Seq=1369 Ack=194 Win=67072 Len=1368 TSval=1727281240 TSecr=254
35	2024-01-25 12:31:38.178681044...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 - 443 [ACK] Seq=194 Ack=2737 Win=11072 Len=0 TSval=2549353818 TSecr=1727281240
36	2024-01-25 12:31:38.345520...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	896	13	Certificate, Server Key Exchange, Server Hello Done
37	2024-01-25 12:31:38.161040344...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 - 443 [ACK] Seq=194 Ack=3567 Win=10304 Len=0 TSval=2549353818 TSecr=1727281240
38	2024-01-25 12:31:38.062391...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	192	13	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
39	2024-01-25 12:31:38.414028500...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	117	13	Change Cipher Spec, Encrypted Handshake Message
40	2024-01-25 12:31:38.109573742...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 - 443 [ACK] Seq=320 Ack=3618 Win=12480 Len=0 TSval=2549353988 TSecr=1727281420
49	2024-01-25 12:31:38.282097660...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Server Hello
50	2024-01-25 12:31:38.1153429067...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1254	12	Certificate
51	2024-01-25 12:31:38.965425...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	190	12	Server Key Exchange, Server Hello Done
54	2024-01-25 12:31:38.824826...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 - 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=441496237
55	2024-01-25 12:31:38.344661913...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 - 3128 [ACK] Seq=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=441496237
56	2024-01-25 12:31:38.173832950...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	159	12	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2024-01-25 12:31:38.422856787...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 - 61484 [ACK] Seq=2540 Ack=954 Win=64640 Len=0 TSval=441496317 TSecr=1676452193
58	2024-01-25 12:31:38.244514147...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	117	12	Change Cipher Spec, Encrypted Handshake Message
59	2024-01-25 12:31:38.328702336...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 - 3128 [ACK] Seq=954 Ack=2591 Win=131008 Len=0 TSval=1676452265 TSecr=441496317
60	2024-01-25 12:31:38.151248214...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	562	12	Application Data
61	2024-01-25 12:31:38.257435452...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TCP	66	12	3128 - 61484 [ACK] Seq=2591 Ack=1450 Win=64192 Len=0 TSval=441496387 TSecr=1676452265
64	2024-01-25 12:31:38.296760748...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	111	13	Application Data
73	2024-01-25 12:31:38.411911657...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 - 24953 [ACK] Seq=3618 Ack=365 Win=67072 Len=0 TSval=1727281896 TSecr=2549354298
74	2024-01-25 12:31:38.340812513...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	640	13	Application Data, Application Data
78	2024-01-25 12:31:39.283208060...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	443 - 24953 [ACK] Seq=3618 Ack=939 Win=68096 Len=0 TSval=1727282019 TSecr=2549354468
79	2024-01-25 12:31:39.159943076...	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	1146	13	Application Data, Application Data
80	2024-01-25 12:31:39.305106563...	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 - 443 [ACK] Seq=939 Ack=4698 Win=11456 Len=0 TSval=2549354588 TSecr=1727282020
82	2024-01-25 12:31:39.165986323...	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 12:31:39.200484740...	10.48.48.165	VMware_8d:9a:f4	10.61.70.23	Cisco_9d:b9:ff	TLSv1.2	1209	12	Application Data, Application Data
85	2024-01-25 12:31:39.128618294...	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	12	61484 - 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=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

イメージ：フルHTTPS明示的 - キャッシュなし



注：トラフィックの各ストリームは異なる色で区別されます。クライアントからSWAへのフローは1色で、SWAからWebサーバへのフローは別の色です。



イメージ - HTTPSフロー - 明示的 - キャッシュなし

アクセスログの例を次に示します。

```
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：HTTPSトラフィックの透過型導入で確認できるように、アクセスログに2行あります。最初の行はトラフィックが暗号化されている場合を示し、CONNECTと表示されます。WebサーバのURLはtunnel://で始まります。SWAでDecryptionが有効になっている場合は、2行目にGETが含まれ、URL全体がHTTPSで始まります。これは、トラフィックが復号化されたことを意味します。

パススルーHTTPSトラフィック

トラフィックをパススルーするようにSWAを設定した場合のフロー全体を次に示します。

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	TLSh1.3: 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	17517 → 443 [ACK] Seq=1 Ack=1 Win=12...
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	17517 → 443 [ACK] Seq=650 Ack=1369 Win=11136 Len=0 TSval=900013138 TSec...
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	TLSh1.3: 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	17517 → 443 [ACK] Seq=650 Ack=4105 Win=12416 Len=0 TSval=900013138 TSec...
2024-01-25 13:21:42.3850714352 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=4105 Win=12416 Len=0 TSval=900013138 TSec...
2024-01-25 13:21:42.542333	60250	Application Data	3128	TLSh1.3: Application Data
2024-01-25 13:21:42.2351706320 (nanoseconds)	60250	Application Data	3128	TLSh1.3: Application Data
2024-01-25 13:21:42.4080650144 (nanoseconds)			17517	17517 → 443 [ACK] Seq=650 Ack=4171 Win=12416 Len=0 TSval=900013138 TSec...
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	TLSh1.3: 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...

イメージ - HTTPSパズル - 明示的 - フロー

SWAからWebサーバへのClient Helloのサンプルを次に示します。

```

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: 86da348af5508fc24f18f3cbd9829c7282b77e0499e5d2f38466ccbbd66821e2
│   └── 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)

```

イメージ - HTTPSパズル - 明示的 - WebサーバへのSWA - クライアントhello

これは、クライアントからSWAへのClient Helloと同じです。

```

  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 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc032)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc033)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc034)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc035)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc036)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc037)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc038)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc039)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0xc03a)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0xc03b)
    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)

```

イメージ – HTTPSパススルー – 明示的 – SWAへのクライアント – Client hello

次にアクセスログの例を示します。

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

注：ご覧のように、これは1行のみで、アクションはPASSTHRUです。

透過的な導入

認証を使用しない透過型導入でのHTTPトラフィック

クライアントとSWA

ネットワークトラフィックは、クライアントのIPアドレスとWebサーバのIPアドレスの間を移動します。

クライアントからのトラフィックはTCPポート80 (プロキシポートではない) 宛てです。

- TCPハンドシェイク。
- クライアントからのHTTP Get (宛先IP = Webサーバ、宛先ポート = 80)
- プロキシからのHTTP応答 (送信元IP = Webサーバ)

- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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
-	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

イメージ - クライアントからプロキシ - HTTP - 透過 - 認証なし

クライアントからのHTTP Getの例を次に示します

```

> 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]

```

イメージ - クライアントからプロキシ - HTTP - トランスペアレント - 認証なし - クライアントHTTP Get

SWAおよびWebサーバ

ネットワークトラフィックは、プロキシのIPアドレスとWebサーバのIPアドレスの間で発生します。

SWAからのトラフィックは、TCPポート80 (プロキシポートではない)宛てです

- TCPハンドシェイク。
- プロキシからのHTTP Get (宛先IP = Webサーバ、宛先ポート = 80)
- WebサーバからのHTTP応答 (送信元IP = プロキシサーバ)
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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=6873463
10	2023-12-11 19:13:47.285008827	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1559577035 TSecr=6873333
11	2023-12-11 19:13:47.307381585	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	243	1	GET / HTTP/1.1
12	2023-12-11 19:13:47.118451681	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=0 TSval=6873333 TSecr=1559577035
13	2023-12-11 19:13:47.209157872	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
17	2023-12-11 19:14:12.270488529	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 → 80 [FIN, ACK] Seq=178 Ack=1732 Win=13184 Len=0 TSval=1559602015 TSecr=6873463
18	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
19	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
20	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

イメージ - プロキシとWebサーバ - HTTP - 透過 - 認証なし

プロキシからのHTTP Getの例を次に示します

```

> 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]

```

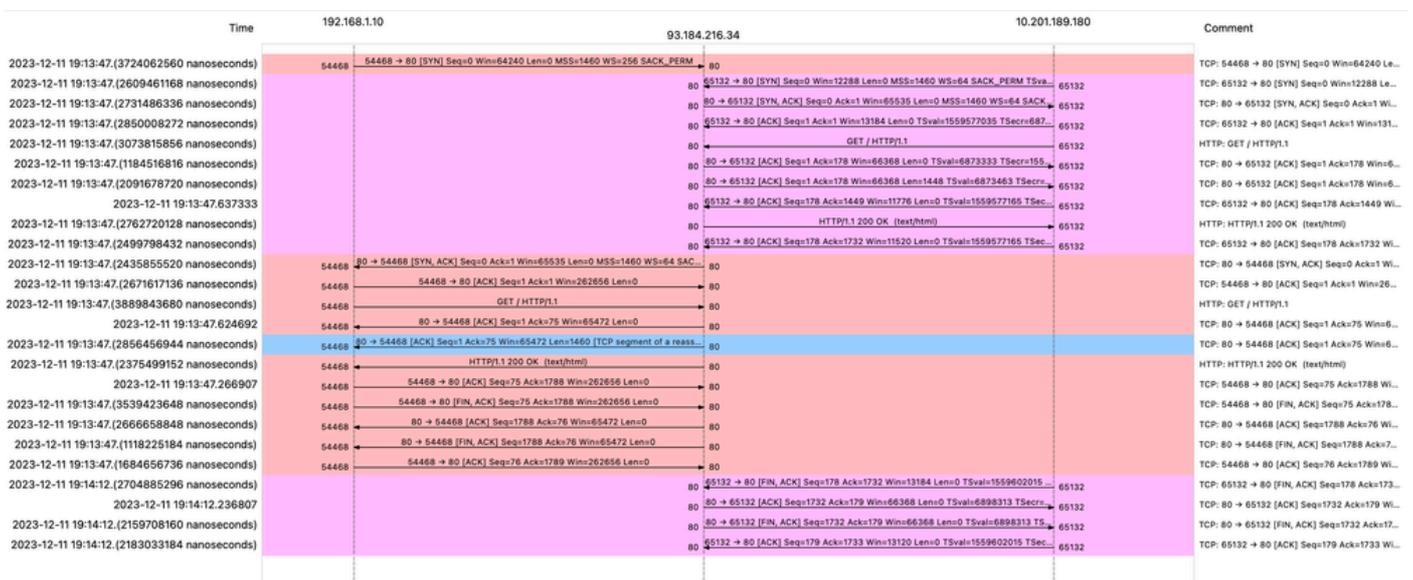
イメージ - Webサーバへのプロキシ - HTTP - トランスペアレント - 認証なし - プロキシHTTP Get

これは、クライアントからSWA、Webサーバ、そして最後にクライアントに戻るトラフィックのフロー全体を表します。

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Len	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 19:13:47.260946116	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	1	65132 -> 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1559577035 TSecr=0
9	2023-12-11 19:13:47.273148633	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1	80 -> 65132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=6873333 TSecr=
10	2023-12-11 19:13:47.285008027	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 19:13:47.307381585	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	243	1	GET / HTTP/1.1
12	2023-12-11 19:13:47.118451681	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 -> 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=0 TSval=6873333 TSecr=1559577035
13	2023-12-11 19:13:47.209167872	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	1514	1	80 -> 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=1559577035 [TCP segment
14	2023-12-11 19:13:47.637333	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 -> 80 [ACK] Seq=178 Ack=1449 Win=11776 Len=0 TSval=1559577165 TSecr=6873463
15	2023-12-11 19:13:47.276272012	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	349	1	HTTP/1.1 200 OK (text/html)
16	2023-12-11 19:13:47.249979843	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 -> 80 [ACK] Seq=178 Ack=1732 Win=11520 Len=0 TSval=1559577165 TSecr=6873463
18	2023-12-11 19:13:47.243585552	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	0	80 -> 54468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
19	2023-12-11 19:13:47.267161713	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 -> 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
20	2023-12-11 19:13:47.388984368	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	HTTP	128	0	GET / HTTP/1.1
21	2023-12-11 19:13:47.624692	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	0	80 -> 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=0
22	2023-12-11 19:13:47.285645694	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	0	80 -> 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
23	2023-12-11 19:13:47.237549915	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	0	HTTP/1.1 200 OK (text/html)
24	2023-12-11 19:13:47.266907	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 -> 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0
25	2023-12-11 19:13:47.353942364	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 -> 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
26	2023-12-11 19:13:47.266665804	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=5472 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=5472 Len=0
28	2023-12-11 19:13:47.168465673	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	0	54468 -> 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0
1.	2023-12-11 19:14:12.270488529	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 -> 80 [FIN, ACK] Seq=178 Ack=1732 Win=13184 Len=0 TSval=1559602015 TSecr=6873463
1.	2023-12-11 19:14:12.236807	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 -> 65132 [ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1.	2023-12-11 19:14:12.215970816	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80 -> 65132 [FIN, ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=1559602015
1.	2023-12-11 19:14:12.218303318	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	65132 -> 80 [ACK] Seq=179 Ack=1733 Win=13120 Len=0 TSval=1559602015 TSecr=6898313

イメージ - トラフィック合計 - HTTP - トランスペアレント - 認証なし

注：トラフィックの各ストリームは異なる色で区別されます。クライアントからSWAへのフローは1色で、SWAからWebサーバへのフローは別の色です。



イメージ : WCCP HTTPフロー

アクセスログの例を次に示します。

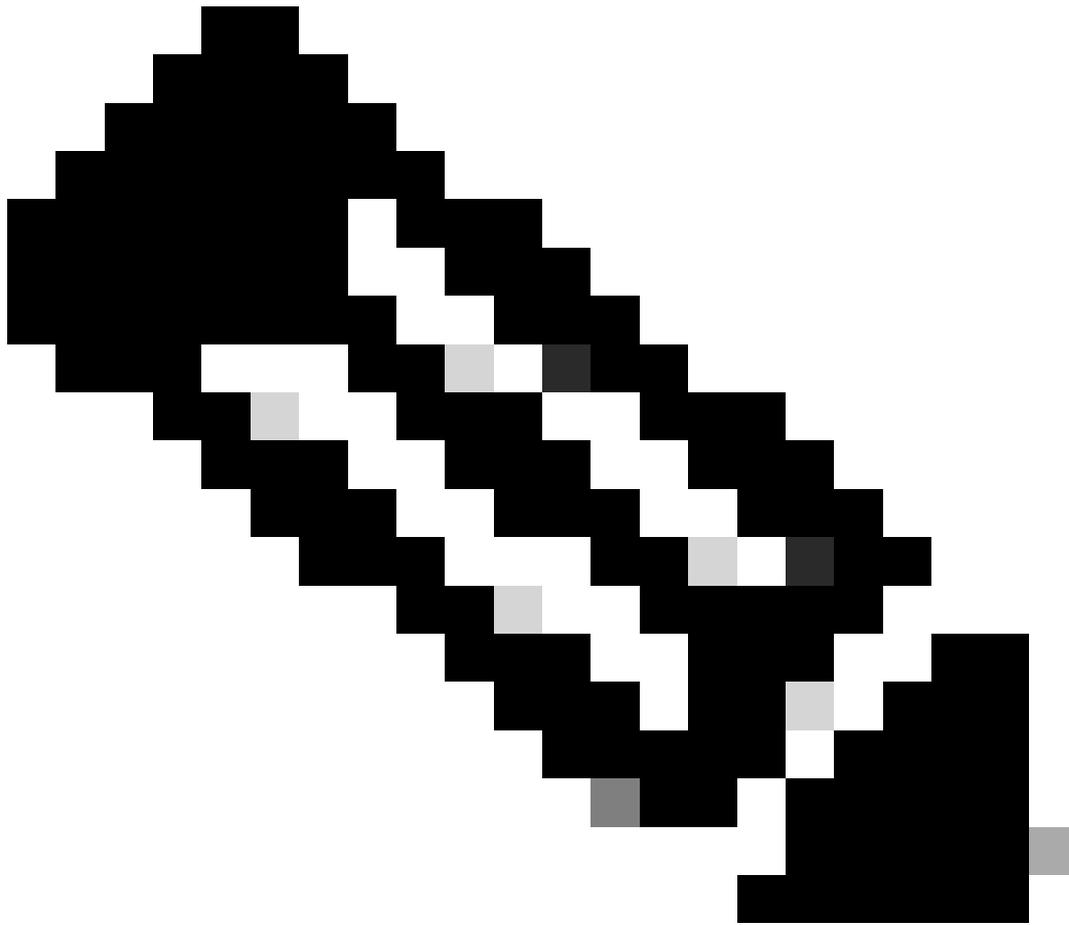
1702318427.181 124 192.168.1.10 TCP_MISS/200 1787 GET http://www.example.com/ - DIRECT/www.example.com

キャッシュされたデータを持つトラフィック

これは、データがSWAキャッシュにある場合の、クライアントからSWAへのトラフィックのフロー全体を表します。

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.	(425926200..	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	2	80	- 54487	[ACK]	Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
17	2023-12-11 19:19:49.	(425926200..	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	2	HTTP/1.1 200 OK			(text/html)
18	2023-12-11 19:19:49.	(270830524..	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487	- 80	[ACK]	Seq=75 Ack=1788 Win=262656 Len=0
19	2023-12-11 19:19:49.	(391010345..	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487	- 80	[FIN, ACK]	Seq=75 Ack=1788 Win=262656 Len=0
20	2023-12-11 19:19:49.	(394258659..	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2	80	- 54487	[ACK]	Seq=1788 Ack=76 Win=65472 Len=0
21	2023-12-11 19:19:49.	(910090	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2	80	- 54487	[FIN, ACK]	Seq=1788 Ack=76 Win=65472 Len=0
22	2023-12-11 19:19:49.	(179047075..	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2	54487	- 80	[ACK]	Seq=76 Ack=1789 Win=262656 Len=0
23	2023-12-11 19:19:49.	(372291046..	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1	80	- 13586	[SYN, ACK]	Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=4080954250 TSecr=4080954250
24	2023-12-11 19:19:49.	(309178142..	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586	- 80	[ACK]	Seq=1 Ack=1 Win=13184 Len=0 TSval=3178050246 TSecr=4080954250
25	2023-12-11 19:19:49.	(226286489..	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	293	1	GET / HTTP/1.1			
26	2023-12-11 19:19:49.	(207193169..	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80	- 13586	[ACK]	Seq=1 Ack=228 Win=66368 Len=0 TSval=4080954250 TSecr=3178050246
27	2023-12-11 19:19:49.	(229948003..	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	489	1	HTTP/1.1 304 Not Modified			
28	2023-12-11 19:19:49.	(336640662..	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586	- 80	[ACK]	Seq=228 Ack=424 Win=12800 Len=0 TSval=3178050356 TSecr=4080954361
29	2023-12-11 19:19:49.	(352537	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586	- 80	[FIN, ACK]	Seq=228 Ack=424 Win=13184 Len=0 TSval=3178050356 TSecr=4080954361
30	2023-12-11 19:19:49.	(194154916..	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80	- 13586	[ACK]	Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
31	2023-12-11 19:19:49.	(349158924..	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1	80	- 13586	[FIN, ACK]	Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
32	2023-12-11 19:19:49.	(103444988..	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1	13586	- 80	[ACK]	Seq=229 Ack=425 Win=13120 Len=0 TSval=3178050356 TSecr=4080954361

イメージ - キャッシュ - 総トラフィック - HTTP - トランスペアレント - 認証なし



注：ご覧のように、WebサーバはHTTP応答304：キャッシュは変更されていません (HTTP response 304: Cache not Modified)を返します。(この例では、パケット番号27)

HTTP応答304の例を次に示します

```
> 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/]
```

イメージ - キャッシュ - HTTP応答304 - HTTP - トランスペアレント - 認証なし

アクセスログの例を次に示します。

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

認証を使用しない透過型導入でのHTTPトラフィック

クライアントとSWA

ネットワークトラフィックは、クライアントのIPアドレスとWebサーバのIPアドレスの間を移動します。

クライアントからのトラフィックはTCPポート443 (プロキシポートではない)宛てです。

- TCPハンドシェイク。
- TLSハンドシェイククライアントHello - Server Hello - Server Key Exchange - Client Key Exchange
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

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 19:36:24.139334096.	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 19:36:24.380754096.	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1.	242	14	Client Hello (SNI=example.com)
248	2023-12-11 19:36:24.366528476.	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	14	443 → 54515 [ACK] Seq=1 Ack=189 Win=65408 Len=0
256	2023-12-11 19:36:24.251614876.	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1.	1514	14	Server Hello
257	2023-12-11 19:36:24.195519830.	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1.	1043	14	Certificate, Server Key Exchange, Server Hello Done
258	2023-12-11 19:36:24.186747024.	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=189 Ack=2450 Win=262656 Len=0
259	2023-12-11 19:36:24.299229398.	93.184.216.34	Cisco_c9:c0:7f	192.168.1.10	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 19:36:24.215995475.	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TLSv1.	157	14	Application Data
263	2023-12-11 19:36:24.298152051.	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 19:36:25.413207139.	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	14	54515 → 443 [ACK] Seq=385 Ack=4007 Win=262656 Len=0
267	2023-12-11 19:36:25.201453091.	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TLSv1.	311	14	Application Data
268	2023-12-11 19:36:25.181582688.	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 19:36:25.404992854.	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
278	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

イメージ - クライアントからプロキシ - HTTP - トランスパレント - 認証なし

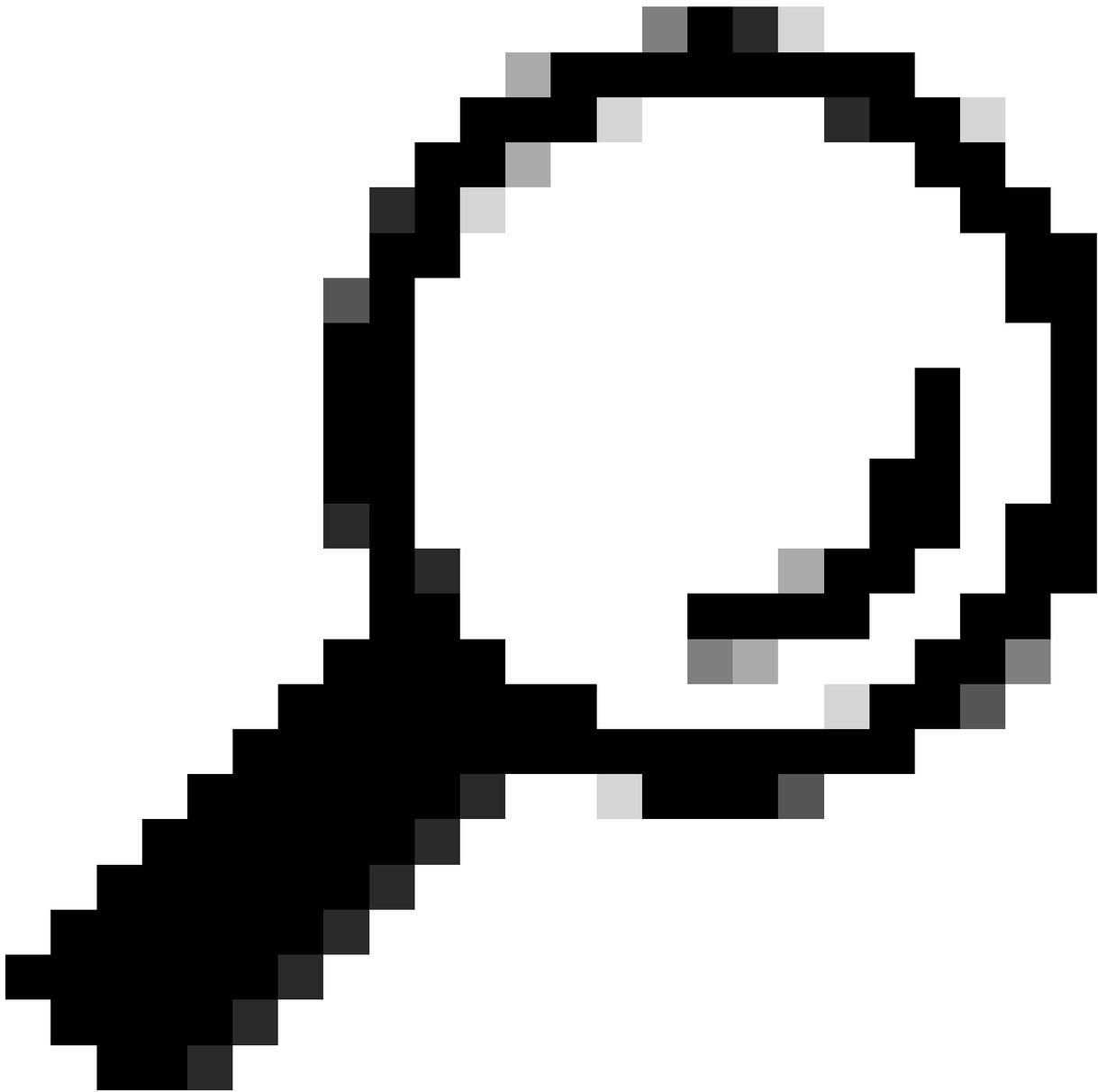
Server Name Indication(SNI)で確認できるように、クライアントからSWAへのClient Helloについて詳しく説明します。この例では、WebサーバのURLはwww.example.comです。

```

> 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: 657756ab224a3f64600e99172a8d38f86b689c7eb4bb121bf5408c96540a0f5d
      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 Names: example.com
        > Extension: supported_groups (len=8)
        > Extension: ec_point_formats (len=2)
        > Extension: signature_algorithms (len=26)
        > Extension: session_ticket (len=0)
        > Extension: application_layer_protocol_negotiation (len=11)
        > Extension: extended_master_secret (len=0)
        > Extension: renegotiation_info (len=1)
          [JA4: t12d2108h1_76e208dd3e22_2dae41c691ec]
          [JA4_r: t12d2108h1_000a,0027,0035,003c,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: 74954ac86284d0d61c4efef92b521]

```

イメージ - Client Hello - クライアントからプロキシ - 透過 - 認証なし

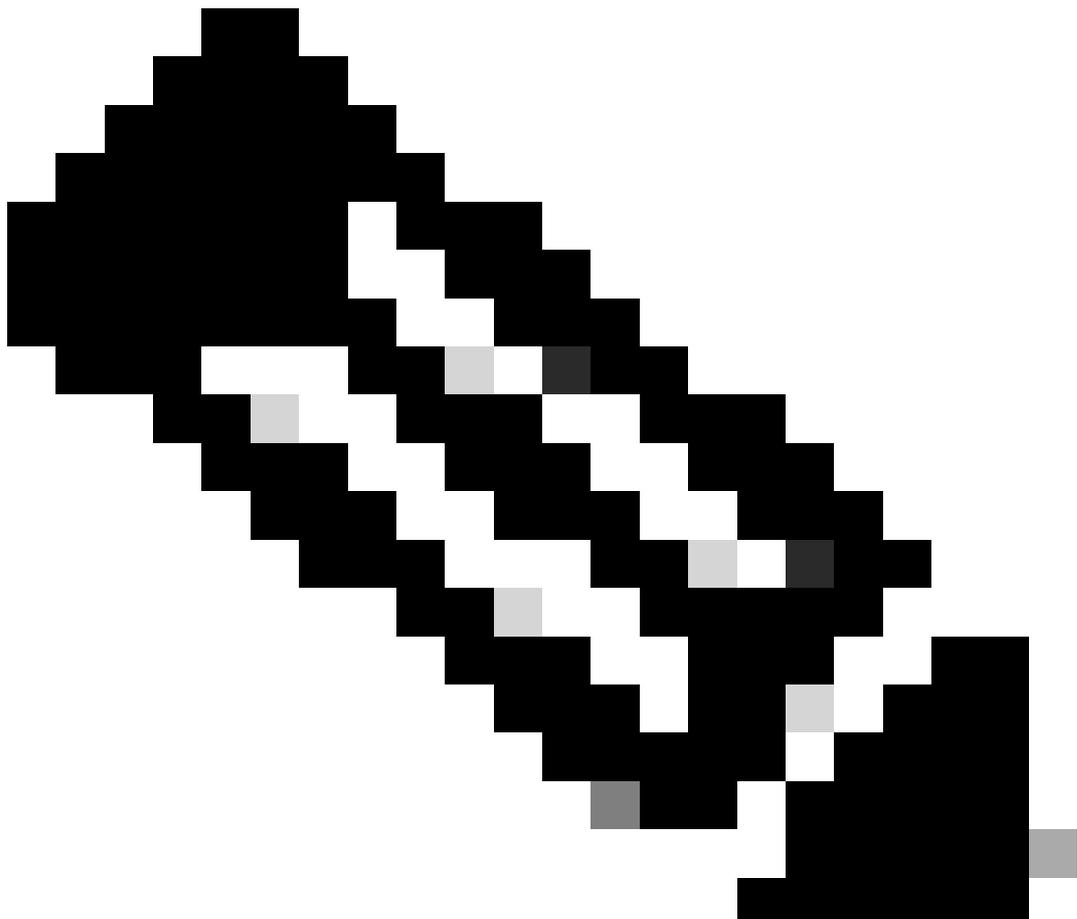


ヒント:Wiresharkでこのフィルタを使用して、
URL/SNI(tls.handshake.extensions_server_name == "www.example.com")を検索できます
。

次に、サーバキー交換の例を示します

```
> 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)
    > RDNSequence item: 1 item (id-at-countryName=US)
    > RDNSequence item: 1 item (id-at-organizationName=wsatest)
    > RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
    > RDNSequence item: 1 item (id-at-commonName=CISCOCALO)
  validity
  subject: rdnSequence (0)
  subjectPublicKeyInfo
  extensions: 5 items
  algorithmIdentifier (sha256WithRSAEncryption)
  Padding: 0
  encrypted [truncated]: 1db2a57a8bbf4def6b1845eace5a7a17f27704e61b102f13c20a696c076bf3e736283d6cffa6c1d9417865ba7f4d4663bd3677423996e23db7f25d232eaa3110a24e72871d8cf2111d3...
  Certificate Length: 938
  Certificate [truncated]: 308203a63082028ea003020102020900a447d8363a186f2f300d06092a864886f70d01010b05003040310b30090603550406130255533110300e060355040a130777736174657374310...
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

イメージ - サーバキー交換 - クライアントからプロキシ - 透過 - 認証なし



注：確認できるように、証明書は復号化証明書としてSWAで設定された証明書です。

SWAおよびWebサーバ

ネットワークトラフィックは、プロキシのIPアドレスとWebサーバのIPアドレスの間で発生します。

SWAからのトラフィックは、TCPポート443 (プロキシポートではない)宛てです

- TCPハンドシェイク。
- TLSハンドシェイククライアントHello - Server Hello - Server Key Exchange - Client Key Exchange
- データ転送
- TCP接続の終了 (4ウェイハンドシェイク)

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Length	Stream	Info
277	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=1563255833 TSecr=0
279	2023-12-11 19:36:24.128841753	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 -> 47868 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3980365294
280	2023-12-11 19:36:24.162744564	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 -> 443 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1563255033 TSecr=3980365294
281	2023-12-11 19:36:24.338198081	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1	263	17	Client Hello (SHA256WithRSAEncryption)
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 19:36:24.134459748	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 19:36:24.298848796	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 19:36:24.240102688	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 19:36:24.281537142	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1	117	17	Change Cipher Spec, Encrypted Handshake Message
293	2023-12-11 19:36:24.896857	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	17	47868 -> 443 [ACK] Seq=324 Ack=3618 Win=13184 Len=0 TSval=1563255233 TSecr=3980365493
325	2023-12-11 19:36:25.383257142	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1	111	17	Application Data
326	2023-12-11 19:36:25.162026084	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 -> 47868 [ACK] Seq=3618 Ack=369 Win=65152 Len=0 TSval=3980365883 TSecr=1563255613
327	2023-12-11 19:36:25.246545451	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TLSv1	285	17	Application Data, Application Data
328	2023-12-11 19:36:25.271978718	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	17	443 -> 47868 [ACK] Seq=3618 Ack=588 Win=64896 Len=0 TSval=3980365883 TSecr=1563255623
329	2023-12-11 19:36:25.283437136	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TLSv1	1514	17	Application Data
330	2023-12-11 19:36:25.244187288	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 19:36:25.424898284	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 19:36:25.187821532	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 19:36:25.145965385	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 19:36:25.351396584	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 19:36:25.372958	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 19:36:25.185516388	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

イメージ - Webサーバへのプロキシ - HTTP - トランスペアレント - 認証なし

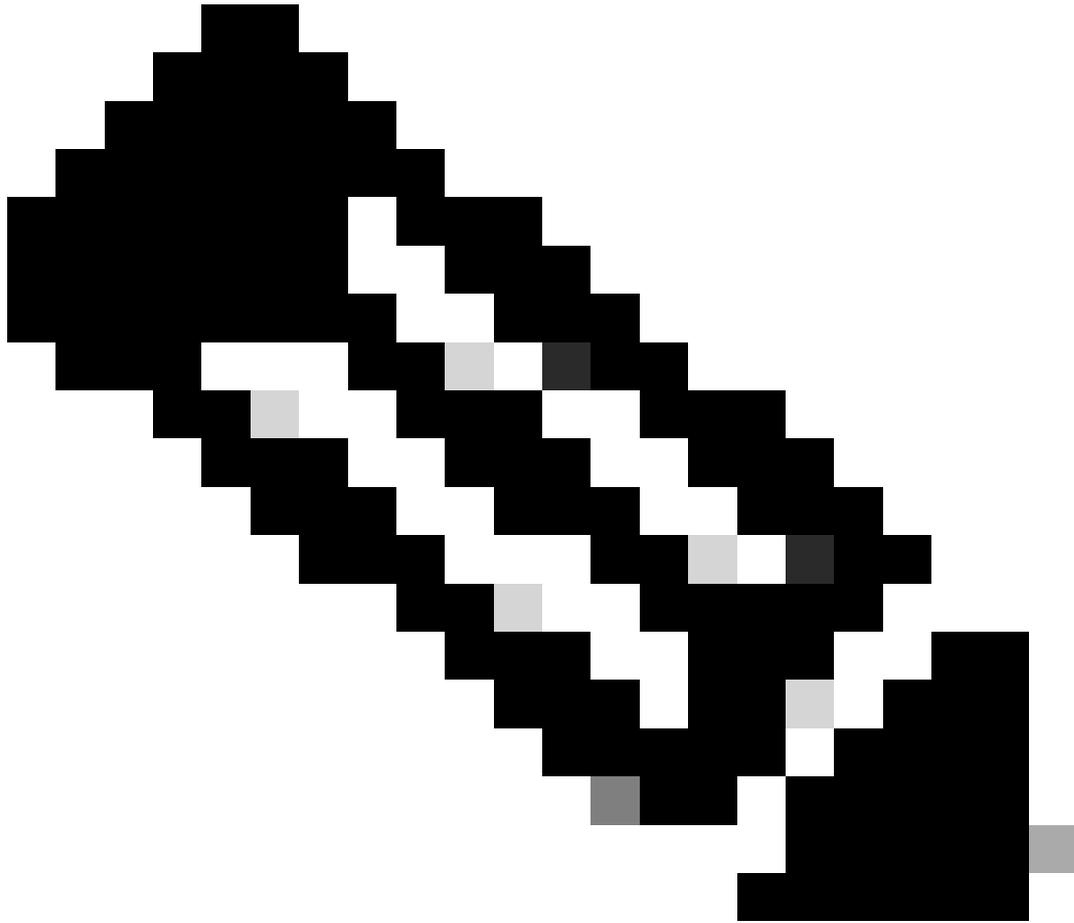
SWAからWebサーバへのClient Helloのサンプルを次に示します

```

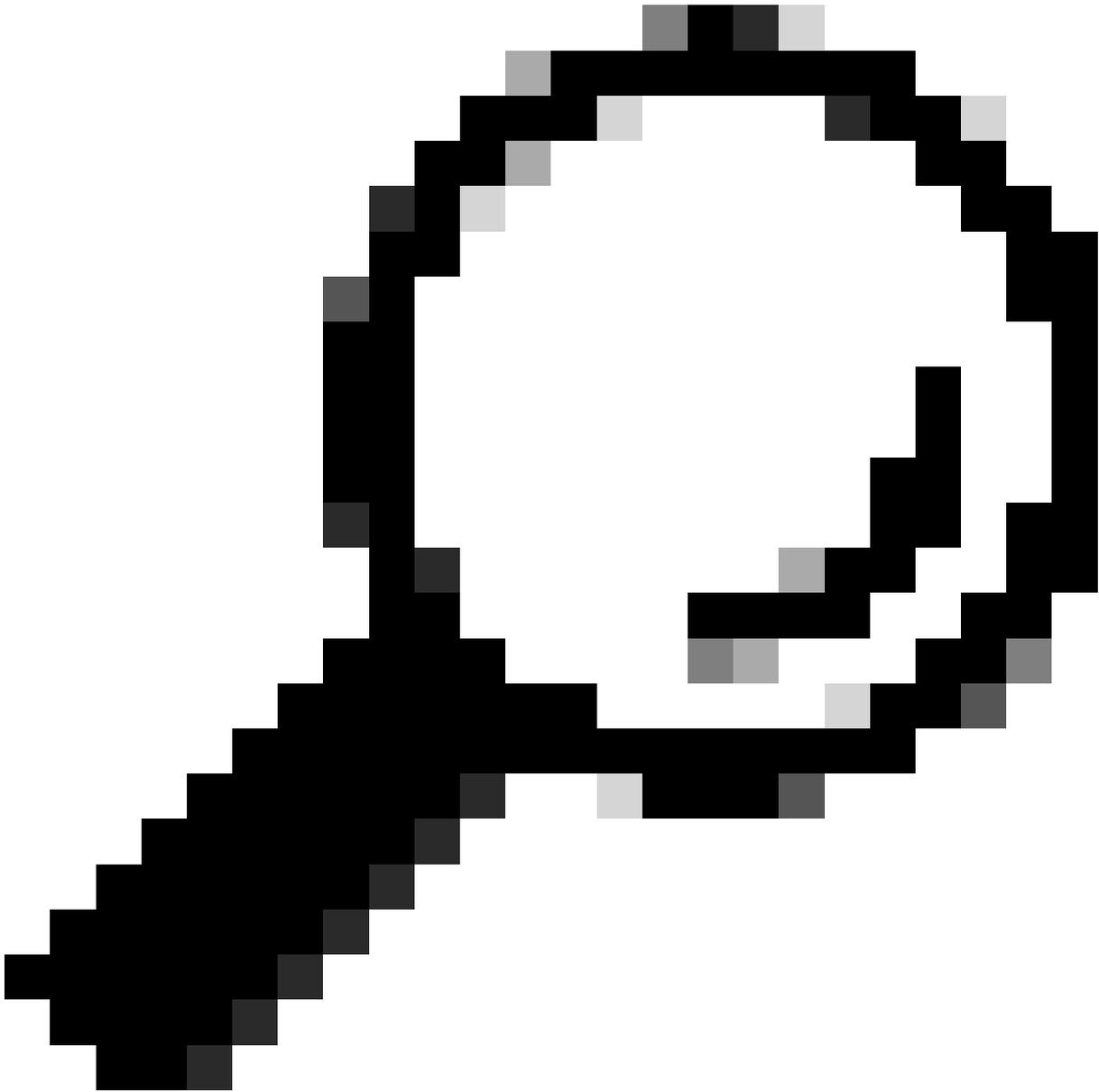
> Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54515, Dst Port: 443, 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_76e208dd3e22_2dae41c691ec]
      [JA4_r: t12d2108h1_000a,002f,0035,003c,003d,009c,009d,009e,009f,c009,c00a,c013,c014,c023,c024,c027,c028,c02b,c02c,c02f,c030_000a,000b,000d,0017,0023,ff01_0804,0805,0806,0401,050]
      [JA3 Fullstring: 771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-65281,29-23-24,0]
      [JA3: 74954a0c86284d0d6e1c4efef92b521]

```

イメージ - Client Hello - Webサーバへのプロキシ - 透過 - 認証なし



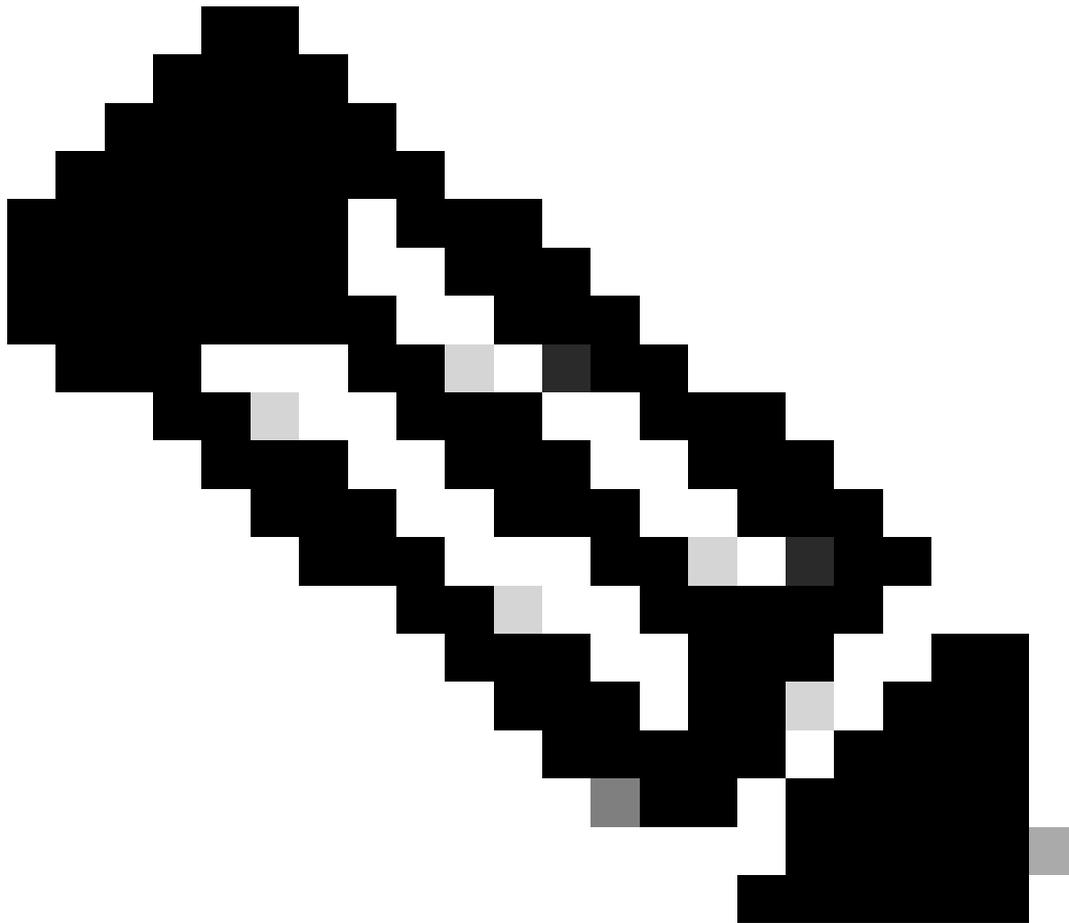
注：ここで観察された暗号スイートは、クライアントからSWAへのClient Helloの暗号スイートとは異なります。これは、このトラフィックを復号化するように設定されたSWAが独自の暗号を使用するためです。



ヒント:SWAからWebサーバへのサーバキー交換では、Webサーバ証明書が表示されます。ただし、アップストリームプロキシがSWAの設定を検出すると、Webサーバ証明書の代わりに証明書が表示されます。

アクセスログの例を次に示します。

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



注：HTTPSトラフィックの透過型導入で確認できるように、アクセスログに2行あります。最初の行は、トラフィックが暗号化された時点、TCP_CONNECT、およびWebサーバのIPアドレスが表示されています。SWAで復号が有効になっている場合、2行目にはGETが含まれ、URL全体がHTTPSで始まります。これは、トラフィックが復号され、SWAでURLが認識されていることを意味します。

関連情報

- [テクニカル サポートとドキュメント - Cisco Systems](#)
- [アクセスログのパフォーマンスパラメータの設定 - Cisco](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。