Comprendre le flux de paquets dans l'appliance Web sécurisée

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Différents types de déploiement de proxy
- Connexion TLS
- Code de réponse HTTP
  - 1xx : Informatif
  - 2xx : Réussi
  - 3xx : redirection
  - Codes 4xx : Erreur client
  - 5xx : Erreur du serveur
- Déploiement explicite
  - Trafic HTTP dans un déploiement explicite sans authentification
    - Client et SWA
    - Serveur Web et SWA
    - Trafic Avec Données Mises En Cache
  - Trafic HTTP dans un déploiement explicite sans authentification
    - Client et SWA
    - Serveur Web et SWA
    - Trafic HTTPS de transit
- Déploiement transparent
  - Trafic HTTP dans un déploiement transparent sans authentification
    - Client et SWA
    - Serveur Web et SWA
    - Trafic Avec Données Mises En Cache
  - Trafic HTTP dans un déploiement transparent sans authentification
    - Client et SWA
    - Serveur Web et SWA
- Autres informations utiles

Introduction

Ce document décrit le flux réseau dans le réseau configuré par proxy, en particulier sur l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Concepts TCP/IP de base.
- Connaissances de base de la configuration du proxy.
- Connaissance de base du mécanisme d'authentification utilisé dans un environnement de proxy.

Les abréviations utilisées dans ces articles sont les suivantes :

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

IP : protocole Internet

GRE : encapsulation de routage générique

HTTP : Hypertext Transfer Protocol.

HTTPS: Protocole de transfert hypertexte sécurisé.

URL : Uniform Resource Locator

TLS : Sécurité de la couche transport

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Différents types de déploiement de proxy

Connexion TLS

Une connexion TLS en HTTPS se produit lorsqu'un client et un serveur communiquent via Internet, fournissant ainsi une connexion sécurisée. Le processus assure la confidentialité et l'intégrité des données entre deux applications en communication. Il fonctionne selon une série d'étapes au cours desquelles le client et le serveur s'accordent sur les normes et les codes de cryptage pour toutes les transmissions ultérieures. La prise de contact vise à dissuader tout accès non autorisé ou toute manipulation par des tiers. Il authentifie également les identités des parties communicantes pour éliminer l'usurpation d'identité. Ce processus est essentiel dans HTTPS, car il garantit que les données restent sécurisées pendant leur transit.

Voici les étapes d'une prise de contact TLS :

1. Allô du client: Le client lance le processus de connexion avec un message Hello. Ce message contient la version TLS du client, les suites de chiffrement prises en charge et une chaîne d'octets aléatoire appelée « aléatoire du client ».
2. Allô du serveur: Le serveur répond par un message Hello. Ce message inclut la version TLS choisie par le serveur, la suite de chiffrement sélectionnée, une chaîne d'octets aléatoire appelée « server random » et le certificat numérique du serveur. Si nécessaire, le serveur demande également le certificat numérique client pour une authentification mutuelle.
3. Le client vérifie le certificat du serveur : Le client vérifie le certificat numérique du serveur auprès de l'autorité de certification qui l'a émis. Cela garantit au client qu'il communique avec le serveur légitime.
4. Pre-master Secret : Le client envoie une chaîne d'octets aléatoire, connue sous le nom de secret prémaître, qui contribue à la création des clés de session. Le client chiffre ce secret prémaître avec la clé publique du serveur, de sorte que seul le serveur peut le déchiffrer avec sa clé privée.
5. Secret principal : Le client et le serveur utilisent le secret principal et les chaînes d’octets aléatoires des messages Hello pour calculer indépendamment le même secret principal. Ce secret partagé est à la base de la génération des clés de session.
6. Client terminé : Le client envoie un message Finished, chiffré avec la clé de session, pour signaler la fin de la partie client de la connexion.
7. Serveur terminé : Le serveur envoie un message Finished (Terminé), également chiffré avec la clé de session, pour signaler la fin de la partie serveur de la connexion.

Code de réponse HTTP

1xx : Informatif

Code	Détails
100 Continuer	Généralement vu en ce qui concerne le protocole ICAP. Il s'agit d'une réponse d'information qui indique au client qu'il peut continuer à envoyer des données. En ce qui concerne les services ICAP (tels que l'analyse antivirus), le serveur ne peut afficher que la première x quantité d'octets. Lorsqu'il a terminé d'analyser le premier ensemble d'octets et qu'il n'a pas détecté de virus, il envoie un message 100 Continue pour informer le client qu'il doit envoyer le reste de l'objet.

2xx : Réussi

Code	Détails
200 OK	Code de réponse le plus courant. Cela signifie que la demande a abouti sans aucun problème.

3xx : redirection

Code	Détails
301 Redirection permanente	Il s'agit d'une redirection permanente, vous pouvez voir ce code lorsque vous redirigez vers le sous-domaine www.
302 Redirection temporaire	Il s'agit d'une redirection temporaire. Le client est invité à effectuer une nouvelle requête pour l'objet spécifié dans l'emplacement : Header (En-tête) .
304 Non modifié	Ceci est en réponse à un GET If-modified-Since (GIMS). Il s'agit littéralement d'un HTTP GET standard qui inclut l'en-tête If-modified-Since: <date>. Cet en-tête indique au serveur que le client dispose d'une copie de l'objet demandé dans son cache local et qu'il inclut la date à laquelle l'objet a été récupéré. Si l'objet a été modifié depuis cette date, le serveur répond avec un 200 OK et une nouvelle copie de l'objet. Si l'objet n'a pas été modifié depuis la date d'extraction, le serveur renvoie une réponse 304 Not Modified.

307 Redirection d'authentification	Ceci est principalement vu dans le déploiement transparent du proxy, lorsque le serveur proxy est configuré pour authentifier la demande et redirige la demande vers une autre URL pour authentifier l'utilisateur,

Codes 4xx : Erreur client

Code	Détails
400 Requête incorrecte	Cela suggère un problème avec la requête HTTP, car elle n'est pas conforme à la syntaxe appropriée. Parmi les raisons possibles, citons plusieurs en-têtes sur une seule ligne, des espaces dans un en-tête ou l'absence de HTTP/1.1 dans l'URI, entre autres. Pour connaître la syntaxe correcte, consultez la RFC 2616.
401 Non autorisé Authentification du serveur Web requise	L'accès à l'objet demandé nécessite une authentification. Le code 401 est utilisé pour l'authentification avec un serveur Web cible. Lorsque le SWA fonctionne en mode transparent et que l'authentification est activée sur le proxy, il renvoie un 401 au client, puisque l'appliance se présente comme s'il s'agissait du serveur de contenu d'origine (OCS). Les méthodes d'authentification pouvant être utilisées sont détaillées dans un fichier www-authenticate : En-tête de réponse HTTP. Indique au client si le serveur demande l'authentification NTLM, de base ou d'autres formes d'authentification.
403 Refusé	Le client ne peut pas accéder à l'objet demandé. Diverses raisons peuvent amener un serveur à refuser l'accès aux objets. Le serveur fournit généralement une description de cause dans les données HTTP ou la réponse HTML.
404 Introuvable	L'objet demandé n'existe pas sur le serveur.
Authentification proxy 407 requise	Il s'agit du même nom qu'un 401, à ceci près qu'il s'agit spécifiquement de l'authentification à un proxy et non à l'OCS. Ceci n'est envoyé que si la demande a été envoyée explicitement au proxy. Un 407 ne peut pas être envoyé à un client tant que SWA est configuré comme proxy transparent, car le client ne sait pas que le proxy existe. Si c'est le cas, le client est très probablement FIN ou RST sur le socket TCP.

5xx : Erreur du serveur

Code	Détails
501 Erreur interne du serveur	Échec du serveur Web générique.
502 Passerelle incorrecte	Se produit lorsqu'un serveur agissant en tant que passerelle ou proxy reçoit une réponse non valide d'un serveur entrant. Il signale que la passerelle a reçu une réponse inappropriée du serveur en amont ou d'origine.
503 Service non disponible	Signifie que le serveur n'est actuellement pas en mesure de traiter la demande en raison d'une surcharge temporaire ou d'une maintenance planifiée. Cela implique que le serveur est temporairement hors service, mais qu'il peut être à nouveau disponible après un certain temps.
504 Délai d'attente de passerelle	Indique qu'un client ou un proxy n'a pas reçu de réponse en temps voulu du serveur Web auquel il a tenté d'accéder pour charger la page Web ou répondre à une autre demande du navigateur. Cela implique souvent que le serveur en amont est en panne.

Déploiement explicite

Trafic HTTP dans un déploiement explicite sans authentification

Client et SWA

Le trafic réseau transite entre l'adresse IP du client et l'adresse IP de l'interface proxy SWA (il s'agit généralement de l'interface P1, mais il peut s'agir de l'interface P2 ou de l'interface de gestion, selon la configuration du proxy).

Le trafic du client est destiné au port TCP 80 ou 3128 vers le SWA (les ports proxy SWA par défaut sont TCP 80 et 3128, dans cet exemple, le port 3128 est utilisé)

- Connexion TCP.
- HTTP Get from Client (IP de destination = IP SWA , Port de destination = 3128)
- Réponse HTTP du proxy (IP source = SWA)
- Transfert de données

- Fin de connexion TCP (connexion en 4 étapes)

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

Image-Client vers SWA, mode HTTP Explicit

Serveur Web et SWA

Le trafic réseau se produit entre l'adresse IP du proxy et l'adresse IP du serveur Web.

Le trafic provenant de SWA est destiné au port TCP 80 et provient d'un port aléatoire (et non du port proxy)

- Connexion TCP.
- HTTP Get from Proxy (Adresse IP de destination = serveur Web , Port de destination = 80)
- Réponse HTTP du serveur Web (IP source = serveur proxy)
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

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

Image- HTTP-SWA vers serveur Web-Explicit-no cache

Voici un exemple de HTTP Get from Client.

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

Image- Client vers SWA HTTP GET- Explicit

Cela représente l'ensemble du flux de trafic du client vers le SWA, puis vers le serveur Web, et enfin vers le client.

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

Image - Tout le trafic HTTP Explicit-no cache

Remarque : Chaque flux de trafic se distingue par une couleur différente ; le flux du client vers le SWA est d'une couleur, et le flux du SWA vers le serveur Web en est une autre.

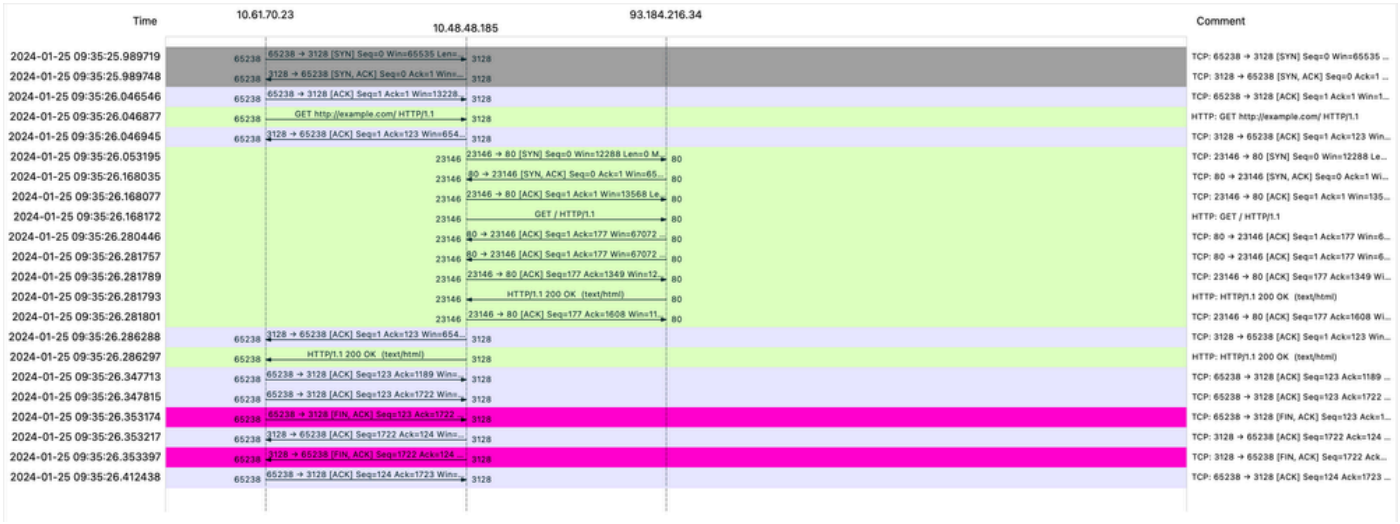


Image - Flux de trafic HTTP explicite - pas de cache

Voici un exemple de journaux d'accès :

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

Trafic Avec Données Mises En Cache

Cela représente le flux entier du trafic du client vers le SWA, lorsque les données se trouvent dans le cache SWA.

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
1920	2024-01-25 09:56:41.209030	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	78	2	55709 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=3417110271 TSecr=0 SACK_PERM
1921	2024-01-25 09:56:41.209111	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	74	2	3128 → 55709 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=64 SACK_PERM TSval=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 09:56:41.385086	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	74	3	80 → 16088 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=811197678 TSecr=
1944	2024-01-25 09:56:41.385174	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=1 Ack=1 Win=13568 Len=0 TSval=3191297043 TSecr=811197678
1945	2024-01-25 09:56:41.385270	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	HTTP	292	3	GET / HTTP/1.1
1946	2024-01-25 09:56:41.509528	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 16088 [ACK] Seq=1 Ack=227 Win=67072 Len=0 TSval=811197793 TSecr=3191297043
1947	2024-01-25 09:56:41.510195	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	HTTP	365	3	HTTP/1.1 304 Not Modified
1948	2024-01-25 09:56:41.510259	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=227 Ack=300 Win=13248 Len=0 TSval=3191297172 TSecr=811197793
1949	2024-01-25 09:56:41.510429	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [FIN, ACK] Seq=227 Ack=300 Win=13568 Len=0 TSval=3191297172 TSecr=811197793
1972	2024-01-25 09:56:41.513099	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	1254	2	3128 → 55709 [ACK] Seq=1 Ack=123 Win=65856 Len=1188 TSval=3687924179 TSecr=3417110333 [TCP
1973	2024-01-25 09:56:41.513111	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	HTTP	599	2	HTTP/1.1 200 OK (text/html)
1974	2024-01-25 09:56:41.585507	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=123 Ack=1189 Win=131072 Len=0 TSval=3417110640 TSecr=3687924179
1975	2024-01-25 09:56:41.600259	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=123 Ack=1722 Win=130560 Len=0 TSval=3417110649 TSecr=3687924179
1976	2024-01-25 09:56:41.604113	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [FIN, ACK] Seq=123 Ack=1722 Win=131072 Len=0 TSval=3417110652 TSecr=3687924179
1977	2024-01-25 09:56:41.604191	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [ACK] Seq=1722 Ack=124 Win=65856 Len=0 TSval=3687924269 TSecr=3417110652
1978	2024-01-25 09:56:41.604293	10.48.48.185	VMware_8d:f3:64	10.61.70.23	Cisco_9d:b9:ff	TCP	66	2	3128 → 55709 [FIN, ACK] Seq=1722 Ack=124 Win=65856 Len=0 TSval=3687924269 TSecr=3417110652
1979	2024-01-25 09:56:41.636731	93.184.216.34	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	3	80 → 16088 [FIN, ACK] Seq=300 Ack=228 Win=67072 Len=0 TSval=811197917 TSecr=3191297172
1980	2024-01-25 09:56:41.636832	10.48.48.185	VMware_8d:f3:64	93.184.216.34	Cisco_9d:b9:ff	TCP	66	3	16088 → 80 [ACK] Seq=228 Ack=301 Win=13568 Len=0 TSval=3191297302 TSecr=811197917
1981	2024-01-25 09:56:41.662464	10.61.70.23	Cisco_9d:b9:ff	10.48.48.185	VMware_8d:f3:64	TCP	66	2	55709 → 3128 [ACK] Seq=124 Ack=1723 Win=131072 Len=0 TSval=3417110729 TSecr=3687924269

Image - Données HTTP explicites mises en cache

Remarque : Comme vous pouvez le voir, le serveur Web renvoie la réponse HTTP 304 : Cache non modifié. (Dans cet exemple, le paquet numéro 1947.)

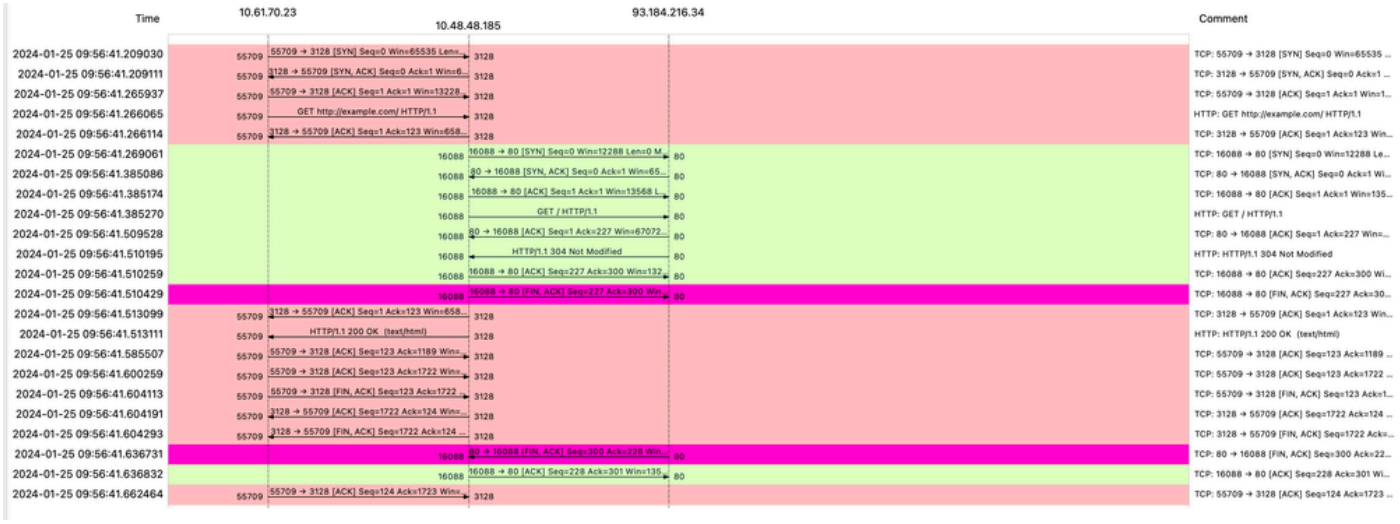


Image - Flux HTTP explicite avec cache

Voici un exemple de réponse HTTP 304.

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

Image- Réponse HTTP Explicit 304

Voici un exemple de journaux d'accès :

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

Trafic HTTP dans un déploiement explicite sans authentification

Client et SWA

Le trafic réseau transite entre l'adresse IP du client et l'adresse IP de l'interface proxy SWA (il s'agit généralement de l'interface P1, mais il peut s'agir de l'interface P2 ou de l'interface de gestion, selon la configuration du proxy).

Le trafic du client est destiné au port TCP 80 ou 3128 vers le SWA (les ports proxy SWA par défaut sont TCP 80 et 3128, dans cet exemple. le port 3128 est utilisé).

- Connexion TCP.
- HTTP CONNECT from Client (Destination IP = SWA , Destination Port = 3128)
- Réponse HTTP du proxy (IP source = SWA)
- Client Hello avec SNI de l'URL (IP source = Client)
- Hello du serveur (IP source = SWA)
- Échange de clés de serveur (IP source = SWA)
- Échange de clés client (IP source = client)
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

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

Image- Client HTTPS vers SWA-Explicit- Pas de cache

Voici les détails de Client Hello de Client à SWA, comme vous pouvez le voir dans l'indication de nom de serveur (SNI) l'URL du serveur Web peut être vu qui dans cet exemple, est www.example.com et le client annoncé 17 suites de chiffrement :

```
> 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
v Hypertext Transfer Protocol
    [Proxy-Connect-Hostname: example.com]
    [Proxy-Connect-Port: 443]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 644
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 640
        Version: TLS 1.2 (0x0303)
      > Random: 8f2d33b577f5cd05ab284c0a64a929e5dd29c940aa73ccc3f4bcafaf8509078d
        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
      v Extension: server_name (len=16) name=example.com
          Type: server_name (0)
          Length: 16
        v Server Name Indication extension
            Server Name list length: 14
            Server Name Type: host_name (0)
            Server Name length: 11
            Server Name: example.com
      > Extension: 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_5b57614c22b0_748f4c70de1c]
```

Image - Hello du client HTTPS - Explicite - Client vers SWA

Conseil : Vous pouvez utiliser ce filtre dans Wireshark pour rechercher URL/SNI : tls.handshake.extensions_server_name == "www.example.com"

Voici un exemple de certificat que SWA a envoyé au Client.

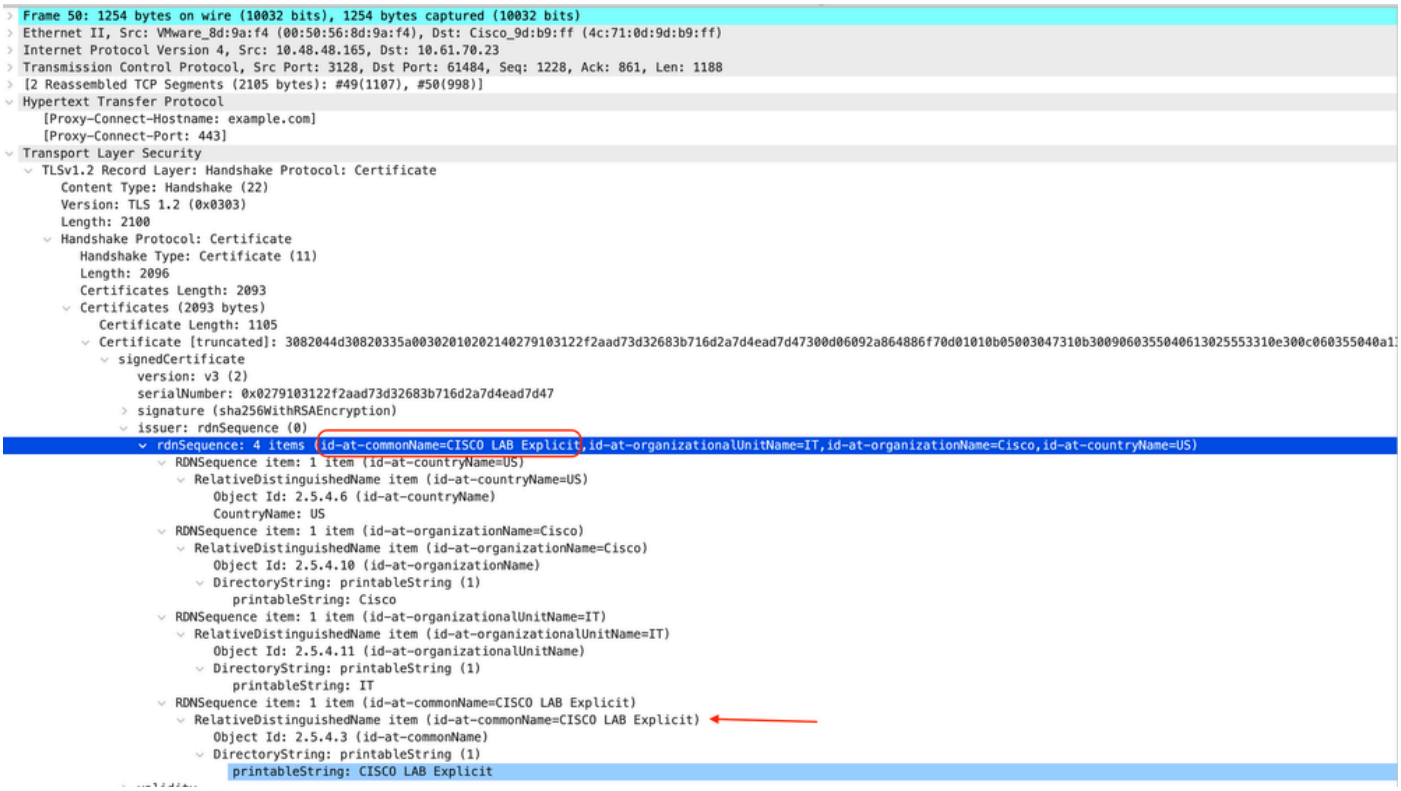


Image - Certificat HTTPS - Explicite - SWA au client

Serveur Web et SWA

Le trafic réseau se produit entre l'adresse IP du proxy et l'adresse IP du serveur Web.

Le trafic provenant de SWA est destiné au port TCP 443 (et non au port proxy)

- Connexion TCP
- Client Hello (IP de destination = serveur Web, port de destination = 443)
- Hello du serveur (IP source = serveur Web)
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

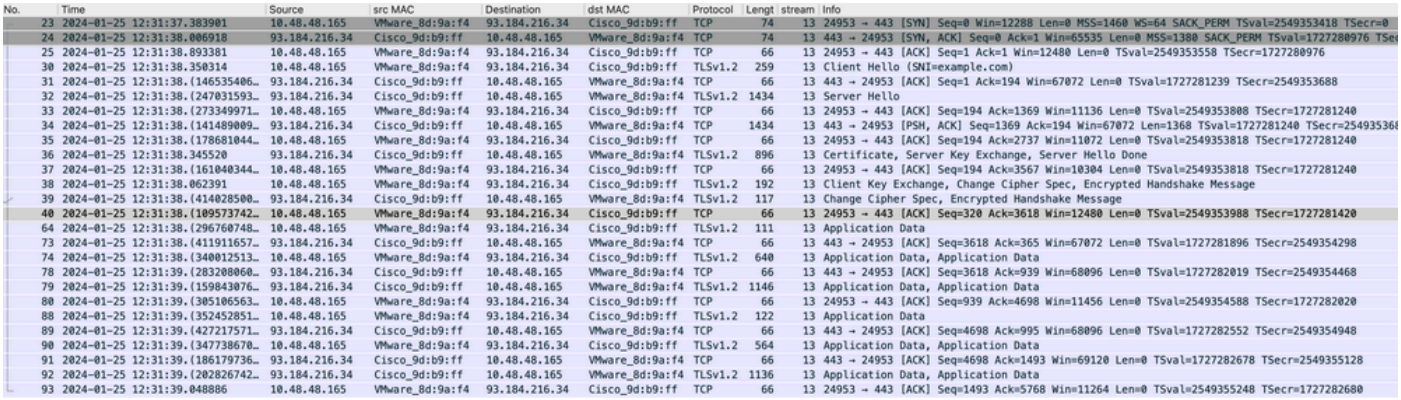


Image- HTTPS - Explicit - SWA vers serveur Web

Voici les détails de Client Hello de SWA vers le serveur Web, comme vous pouvez le voir SWA annoncé 12 suites de chiffrement :

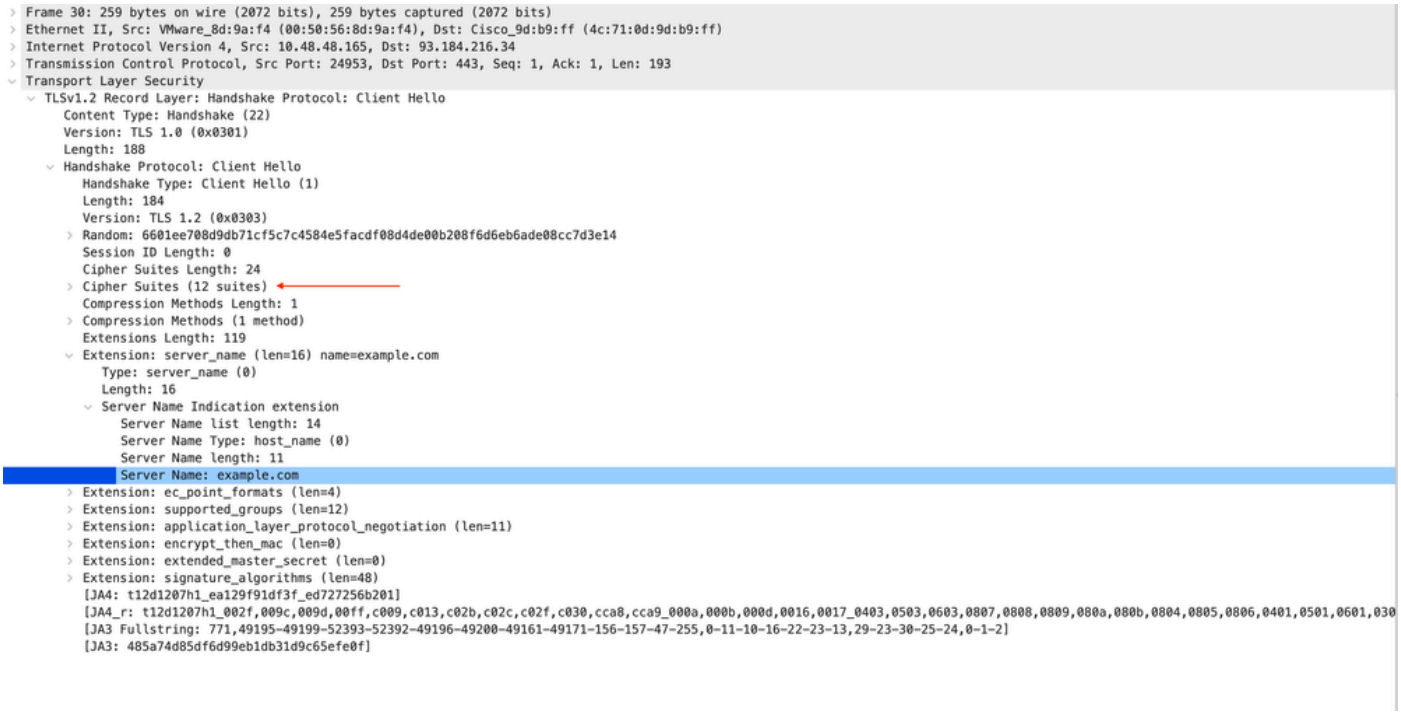


Image- Client HTTPS Hello - SWA vers serveur Web- Pas de cache

Remarque : Les suites de chiffrement observées ici diffèrent des suites de chiffrement dans le paquet Hello du client à SWA, car le SWA, configuré pour décrypter ce trafic, utilise ses propres chiffrements.

Conseil : Dans l'échange de clés de serveur entre SWA et Web Server, le certificat de serveur Web apparaît. Cependant, si un proxy en amont trouve la configuration pour votre SWA, son certificat s'affiche à la place du certificat du serveur Web.

Voici un exemple de HTTP CONNECT du client.

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

Image - Client HTTP Connect

Cela représente l'ensemble du flux de trafic du client vers le SWA, puis vers le serveur Web, et enfin vers le client.

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

Image - HTTPS explicite complet - Pas de cache

Remarque : Chaque flux de trafic se distingue par une couleur différente ; le flux du client

vers le SWA est d'une couleur, et le flux du SWA vers le serveur Web en est une autre.



Image- Flux HTTPS- Explicite - Pas de cache

Voici un exemple de journaux d'accès :

```
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
```

Remarque : Comme vous pouvez le voir dans le déploiement transparent pour le trafic HTTPS, il y a 2 lignes dans les journaux d'accès, la première ligne est lorsque le trafic est chiffré et vous pouvez voir CONNECT et l'URL du serveur Web commence par tunnel://. Si le déchiffrement est activé dans SWA, la deuxième ligne contient GET et l'URL entière commence par HTTPS, ce qui signifie que le trafic a été déchiffré.

Trafic HTTPS de transit

Si vous avez configuré votre SWA pour qu'il traverse le trafic, voici le flux global :

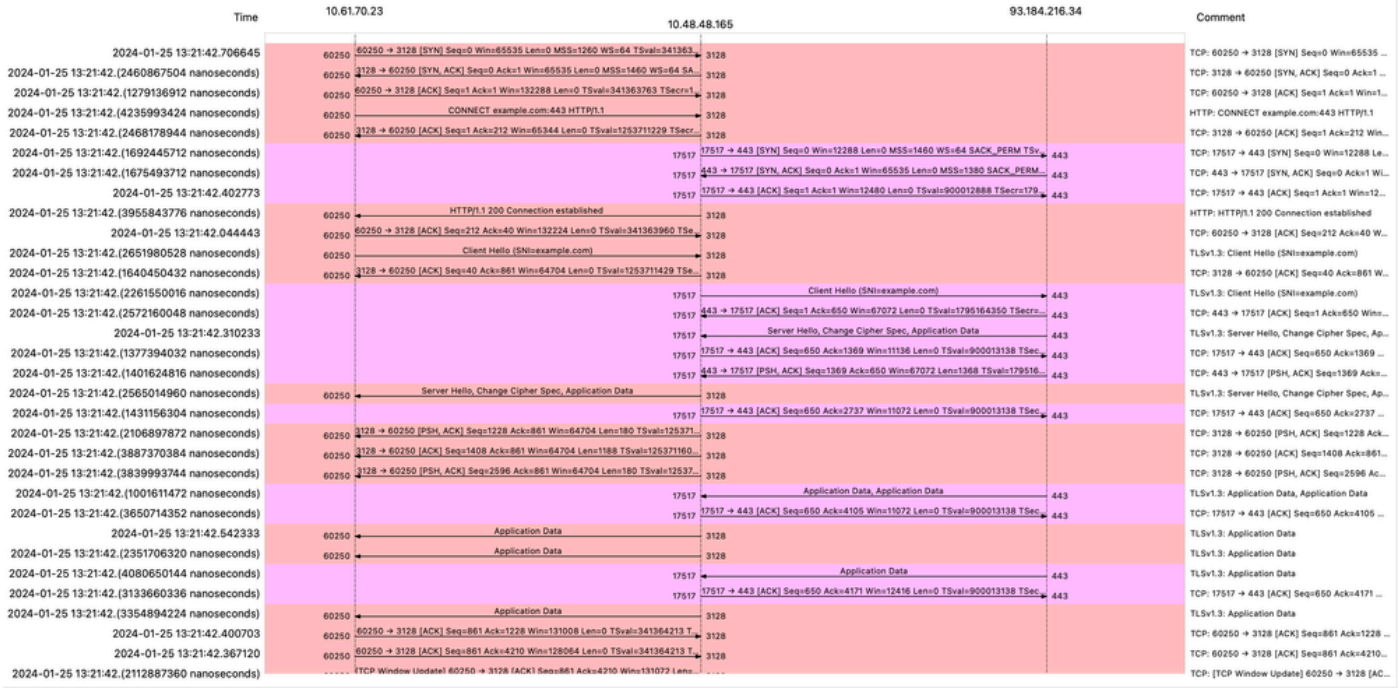


Image - Passthrough HTTPS - Explicite - Flux

Voici l'exemple de Client Hello de SWA vers le serveur Web :

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

Image - Passthrough HTTPS - Explicite - SWA vers Webserver - Hello du client

Identique à l'Hello client du client à SWA :

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

Image - Passthrough HTTPS - Explicite - Client vers SWA - Hello du client

Voici un exemple de journal d'accès :

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



Remarque : Comme vous pouvez le voir, il ne s'agit que d'une seule ligne et l'action est PASSTHRU.

Déploiement transparent

Trafic HTTP dans un déploiement transparent sans authentification

Client et SWA

Le trafic réseau transite entre l’adresse IP du client et l’adresse IP du serveur Web.

Le trafic du client est destiné au port TCP 80 (et non au port proxy)

- Connexion TCP
- HTTP Get from Client (Adresse IP de destination = serveur Web , Port de destination = 80)
- Réponse HTTP du proxy (IP source = serveur Web)
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

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

Image - Client vers proxy - HTTP - Transparent - Aucune authentification

Voici un exemple de HTTP Get from Client.

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

Image - Client vers proxy - HTTP - Transparent - Aucune authentification - Client HTTP Get

Serveur Web et SWA

Le trafic réseau se produit entre l'adresse IP du proxy et l'adresse IP du serveur Web.

Le trafic provenant de SWA est destiné au port TCP 80 (et non au port proxy)

- Connexion TCP
- HTTP Get from Proxy (IP de destination = serveur Web , port de destination = 80)
- Réponse HTTP du serveur Web (IP source = serveur proxy)
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

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

Image - Proxy et serveur Web - HTTP - Transparent - Aucune authentification

Voici un exemple de HTTP Get from Proxy.

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

Image - Proxy vers serveur Web - HTTP - Transparent - Pas d'authentification - Proxy HTTP Get

Cela représente l'ensemble du flux de trafic du client vers le SWA, puis vers le serveur Web, et enfin vers le client.

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

Image - Trafic total - HTTP - Transparent - Aucune authentification

Remarque : Chaque flux de trafic se distingue par une couleur différente ; le flux du client vers le SWA est d'une couleur, et le flux du SWA vers le serveur Web en est une autre.

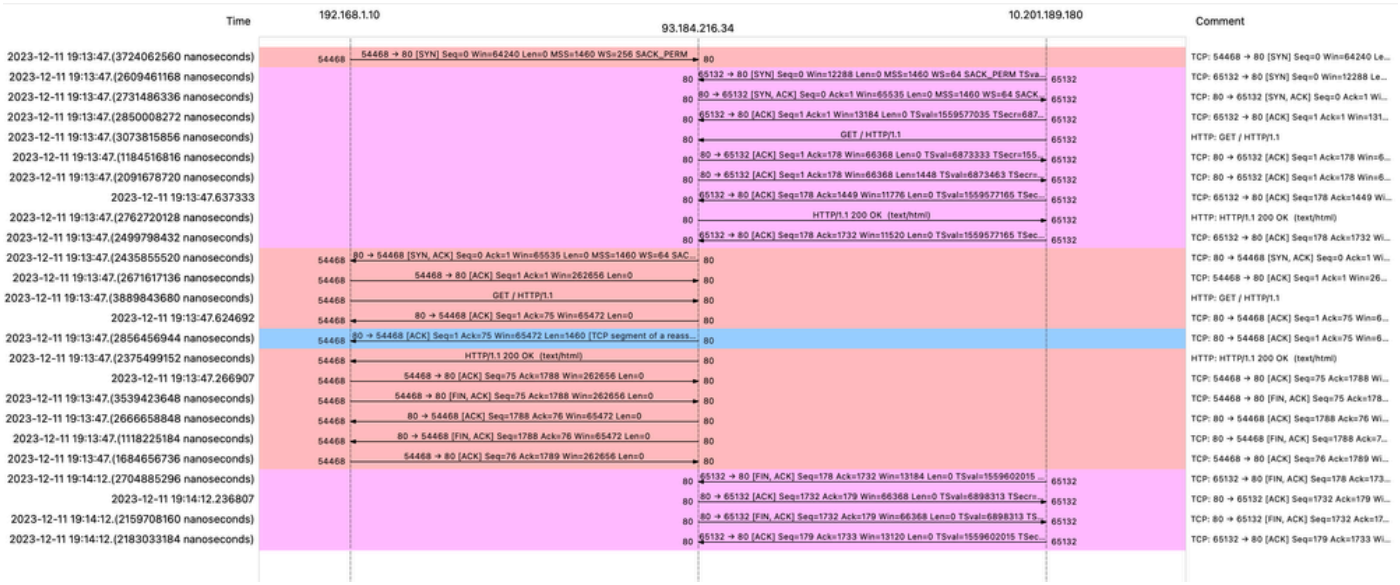


Image- Flux HTTP WCCP

Voici un exemple de journaux d'accès :

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

Trafic Avec Données Mises En Cache

Cela représente le flux entier du trafic du client vers le SWA, lorsque les données se trouvent dans le cache SWA.

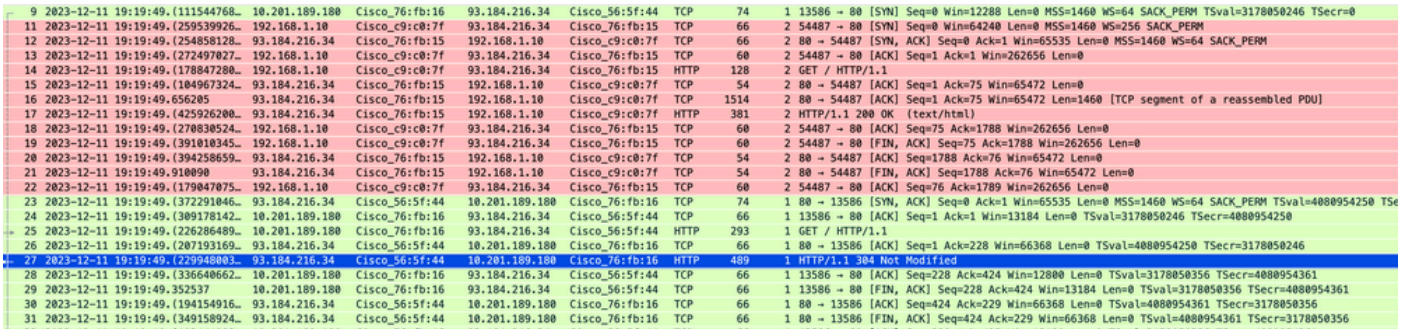


Image - Mise en cache - Trafic total - HTTP - Transparent - Aucune authentification

Remarque : Comme vous pouvez le voir, le serveur Web renvoie la réponse HTTP 304 : Cache non modifié. (Dans cet exemple, le paquet numéro 27.)

Voici un exemple de réponse HTTP 304.

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

Image - Mise en cache - Réponse HTTP 304 - HTTP - Transparent - Aucune authentification

Voici un exemple de journaux d'accès :

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

Trafic HTTP dans un déploiement transparent sans authentification

Client et SWA

Le trafic réseau transite entre l’adresse IP du client et l’adresse IP du serveur Web.

Le trafic du client est destiné au port TCP 443 (et non au port proxy)

- Connexion TCP
- TLS Handshake Client Hello - Server Hello - Server Key Exchange - Client Key Exchange
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)

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

Image - Client vers proxy - HTTPs - Transparent - Aucune authentification

Voici les détails de Client Hello de Client à SWA, comme vous pouvez le voir dans l'indication de nom de serveur (SNI) l'URL du serveur Web peut être vu qui dans cet exemple, est www.example.com.

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

Image - Client Hello - Client vers proxy - Transparent - Aucune authentification

Conseil : Vous pouvez utiliser ce filtre dans Wireshark pour rechercher URL/SNI : tls.handshake.extensions_server_name == "www.example.com"

Voici un exemple d'échange de clés de serveur.

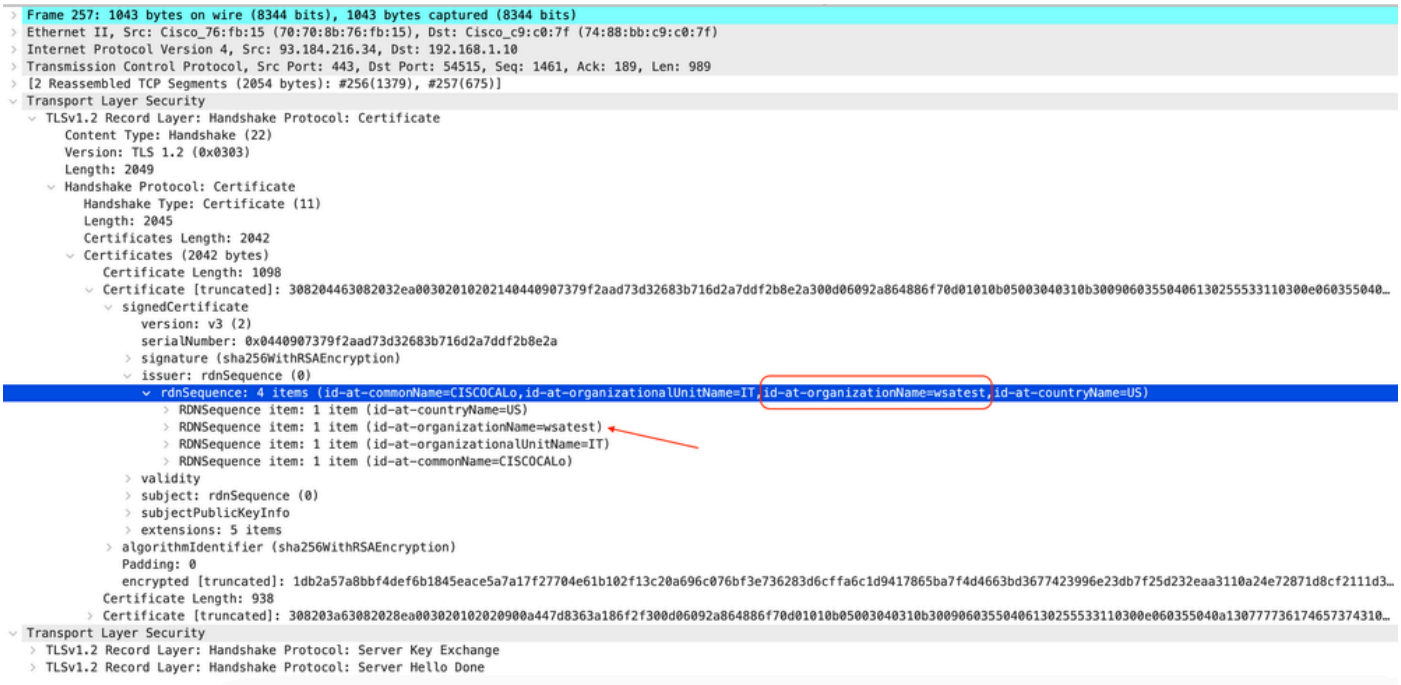


Image - Échange de clés serveur - Client vers proxy - Transparent - Pas d'authentification

---

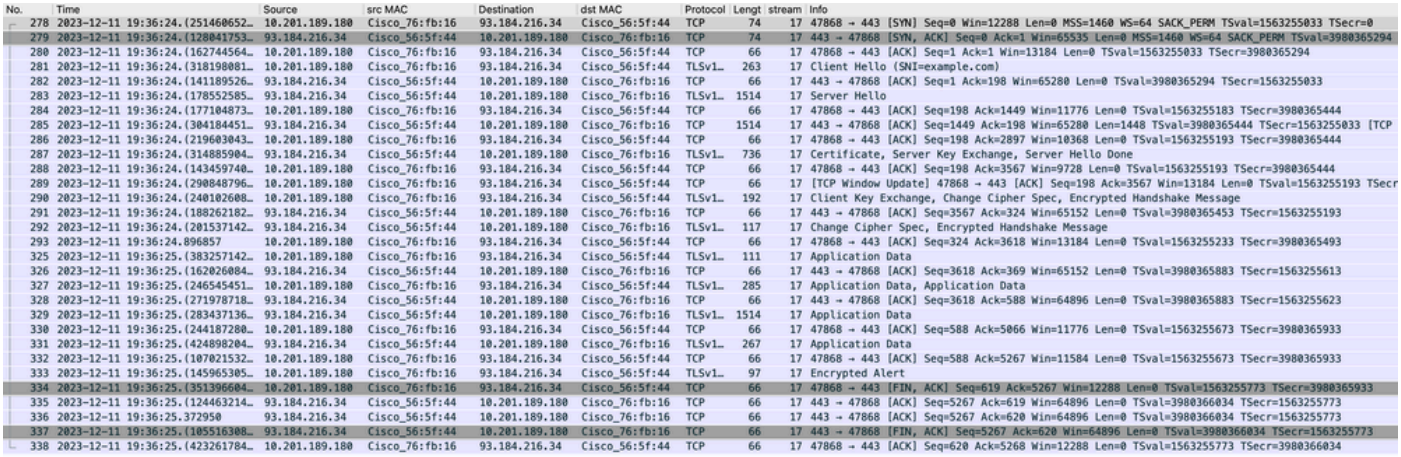
Remarque : Comme vous pouvez le voir, le certificat est celui qui a été configuré dans SWA comme certificat de déchiffrement.

Serveur Web et SWA

Le trafic réseau se produit entre l'adresse IP du proxy et l'adresse IP du serveur Web.

Le trafic provenant de SWA est destiné au port TCP 443 (et non au port proxy)

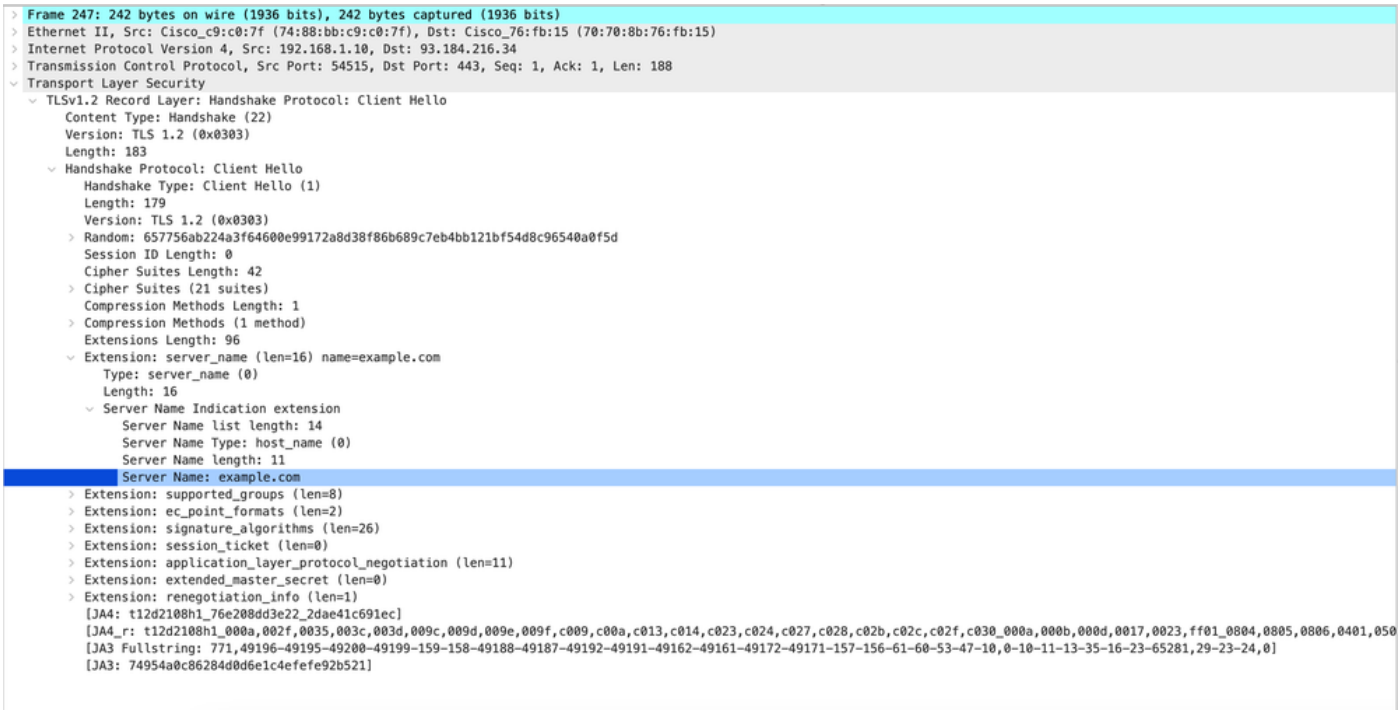
- Connexion TCP
- TLS Handshake Client Hello - Server Hello - Server Key Exchange - Client Key Exchange
- Transfert de données
- Fin de connexion TCP (connexion en 4 étapes)



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

Image - Proxy vers serveur Web - HTTPs - Transparent - Aucune authentification

Voici un exemple de client Hello de SWA vers Web Server.



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

Image- Client Hello - Proxy vers serveur Web - Transparent - Aucune authentification

Remarque : Les suites de chiffrement observées ici diffèrent des suites de chiffrement dans le paquet Hello du client à SWA, car le SWA, configuré pour décrypter ce trafic, utilise ses propres chiffrements.

Conseil : Dans l'échange de clés de serveur entre SWA et Web Server, le certificat de serveur Web apparaît. Cependant, si un proxy en amont trouve la configuration pour votre

SWA, son certificat s'affiche à la place du certificat du serveur Web.

Voici un exemple de journaux d'accès :

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

Remarque : Comme vous pouvez le voir, dans un déploiement transparent pour le trafic HTTPS, il y a 2 lignes dans les journaux d'accès ; la première ligne est lorsque le trafic est chiffré et que vous pouvez voir TCP_CONNECT et l'adresse IP du serveur Web. Si le déchiffrement est activé dans SWA, la deuxième ligne contient GET et l'URL entière commence par HTTPS, ce qui signifie que le trafic a été déchiffré et que SWA connaît l'URL.

Autres informations utiles

- Assistance et documentation techniques - Cisco Systems
- Configuration du paramètre de performance dans les journaux d'accès - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.