فهم تدفق الحزم في جهاز ويب الآمن

المحتويات

المقدمة

يصف هذا المستند تدفق الشبكة في الشبكة التي تم تكوينها بواسطة الوكيل، والتي تركز بشكل خاص على جهاز الويب الآمن (SWA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مفاهيم TCP/IP الأساسية.
- معرفة أساسية بإعداد الوكيل.
- معرفة أساسية بآلية المصادقة المستخدمة في بيئة الوكيل.

المختصرات المستخدمة هي هذه المقالات:

بروتوكول TCP: بروتوكول التحكم في الإرسال

UDP: بروتوكول مخطط بيانات المستخدم

IP: بروتوكول الإنترنت

GRE: تضمين التوجيه العام

http: بروتوكول نقل النص التشعبي.

https: بروتوكول نقل النص التشعبي آمن.

URL: محدد موقع الموارد الموحد

TLS: أمان طبقة النقل

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

أنواع مختلفة من نشر الوكيل

مصافحة TLS

تحدث مصافحة TLS في HTTPS عند اتصال العميل والخادم عبر الإنترنت، مما يوفر اتصالا آمنا. تحافظ العملية على الخصوصية والسلامة البيانات بين تطبيقين متصلين. ويعمل هذا النظام من خلال سلسلة من الخطوات التي يتفق فيها العميل والخادم على معايير التشفير وأكواد تجميع عمليات الإرسال اللاحقة. وتهدف المصافحة إلى ردع أي محاولة غير مصرح بها للوصول أو التلاعب من قبل أطراف ثالثة. كما أنه يصادق على هويات الأطراف المترابطة للقضاء على الانتحال. تعد هذه العملية حاسمة في HTTPS لأنها تضمن بقاء البيانات آمنة أثناء نقلها.

فيما يلي خطوات مصافحة TLS:

1. Client Hello: يبدأ العميل عملية مصافحة الرسائل برسالة ترحيب. تحتوي هذه الرسالة على إصدار TLS العميل ومجموعات التشفير المدعومة وسلسلة البايت العشوائية المعروفة باسم "العميل العشوائي".

2. Server Hello: يستجيب الخادم برسالة ترحيب. تتضمن هذه الرسالة إصدار TLS الذي اختاره الخادم ومجموعة التشفير المحددة ومجموعة البايت العشوائية المعروفة باسم "الخادم العشوائي" وشهادة الخادم الرقمية. عند الضرورة، يطلب الخادم أيضا شهادة العميل الرقمية للمصادقة المتبادلة.

3. يتحقق العميل من شهادة الخادم: يتحقق العميل من الشهادة الرقمية للخادم باستخدام جهة التخيص التي قامت بإصدارها. وهذا يؤكد للعميل أنه يتصل بالخادم الشرعي.

4. السر المسبق: يرسل العميل سلسلة بايت عشوائية، تعرف باسم "سر المدير المسبق"، والتي تساهم في إنشاء مفاتيح الجلسة. يقوم العميل بتشفير سر المدير المسبق هذا باستخدام مفتاح الخادم العام، وبالتالي يمكن للخادم فقط فك تشفيره باستخدام مفتاحه الخاص.

5. السر الرئيسي: يستخدم كل من العميل والخادم سالسل السر الرئيسي والبايت العشوائي من رسائل HELLO لحساب نفس "السر الرئيسي" بشكل مستقل. هذا السر المشترك هو الأساس لإنشاء مفاتيح الجلسة.

6. انتهى العميل: يرسل العميل رسالة "انتهى"، مشفرة باستخدام مفتاح الجلسة، للإشارة إلى اكتمال جزء العميل من المصافحة.

7. الخادم منتهي: يرسل الخادم رسالة "منتهي"، مشفرة أيضا باستخدام مفتاح الجلسة، للإشارة إلى اكتمال جزء الخادم من المصافحة.

رمز إستجابة HTTP

xx: إعالمية

الرمز	التفاصيل
100 متابعة	ينظر إليه عادة فيما يتعلق ببروتوكول ICAP. هذه إستجابة إعالمية تتيح للعميل معرفة أنه يمكنه االستمرار في إرسال البيانات. فيما يتعلق بخدمات ICAP (مثل الكشف عن الفيروسات)، يمكن أن يرى الخادم رؤية كمية س من وحدات البايت فقط. عند القيام بالمسح الضوئي للمجموعة الأولى من وحدات البايت وعدم اكتشاف فيروس، يتم إرسال 100 متابعة إلى العميل ليعلم بإرسال باقي الكائن.

2xx: نجاح

الرمز	التفاصيل
200 موافق	رمز االستجابة الأكثر شيوعا. وهذا يعني أن الطلب نجح دون أية مشاكل.

3xx: إعادة التوجيه

الرمز	التفاصيل
إعادة التوجيه الدائم 301	هذه إعادة توجيه دائمة، يمكنك رؤية هذا الرمز عند إعادة التوجيه إلى المجال الفرعي www.
302 إعادة التوجيه المؤقتة	هذه إعادة توجيه مؤقتة. تم توجيه العميل لإجراء طلب جديد للكائن المحدد في العنوان الموقع: رأس.
304 غير معدل	هذا إستجابة ل GIMS (GET If-modified-since). هذا هو حرفيا HTTP GET القياسي الذي يتضمن الرأس إذا تم تعديله منذ: <date>. يخبر هذا الرأس الخادم بأن العميل لديه نسخة من الكائن المطلوب في ذاكرة التخزين المؤقت المحلية، ويتم تضمين هو التاريخ الذي تم فيه إحضار الكائن. إذا تم تعديل الكائن منذ ذلك التاريخ، فإن الخادم يستجيب ب 200 OK ونسخة جديدة من الكائن. إذا لم يتم تغيير الكائن منذ تاريخ الإحضار، يرسل الخادم إستجابة 304 غير معدلة.
إعادة توجيه المصادقة 307 عامل	وهذا يظهر غالبا، في نشر الوكيل الشفاف، عند تكوين خادم الوكيل لمصادقة الطلب وإعادة توجيه الطلب إلى عنوان URL آخر لمصادقة المستخدم،

رموز 4xx: خطأ العميل

الرمز	التفاصيل
400 طلب سيئة	وهذا يشير إلى وجود مشكلة في طلب HTTP، حيث أنه لا يتمثل للصياغة المناسبة. قد تتضمن الأسباب المحتملة رؤوس متعددة على سطر واحد، أو مسافات داخل رأس، أو نقص HTTP/1.1 في URI، من بين أسباب أخرى. للحصول على الصياغة الصحيحة، يرجى مراجعة RFC 2616.
401 غير مصرح به مصادقة خادم الويب مطلوبة	يتطلب الوصول إلى الكائن المطلوب المصادقة. يتم إستخدام رمز 401 للمصادقة باستخدام خادم ويب هدف. عندما تعمل SWA في وضع شفاف ويتم تمكين المصادقة على الوكيل، فإنها ترجع رمز 401 إلى العميل، نظرا لأن الجهاز يقدم نفسه كما لو كان OCS (خادم المحتوى الأصلي). أساليب المصادقة التي يمكن إستخدامها مفصلة في 'www-authenticate:' رأس إستجابة HTTP. هذا يوقم بإعلام العميل بما إذا كان الخادم يطلب NTLM أو أشكال أساسية أو أشكال أخرى من المصادقة.

تم رفض 403	يتعذر على العميل الوصول إلى الكائن المطلوب. قد تؤدي مجموعة متنوعة من الأسباب إلى رفض الخادم الوصول إلى الكائن. عادة ما يوفر الخادم وصف سبب داخل بيانات HTTP أو إستجابة HTML.
الخطأ 404، لم يتم العثور عليه	الكائن المطلوب غير موجود على الخادم.
مصادقة الوكيل المطلوبة وفقا للمعيار 407	وهذا هو نفس الشيء بالنسبة لمعيار 401، باستثناء أنه خاص بالمصادقة للوكيل وليس نظام التشغيل OCS. ويتم إرسال هذا الطلب فقط إذا تم إرساله بشكل صريح إلى الوكيل. يمكن إرسال رقم 407 إلى عميل بينما يتم تكوين SWA كوكيل شفاف، حيث لا يعرف العميل وجود الوكيل. إذا كان هذا هو الحال، فالأرجح أن العميل يقوم بإعادة التوجيه وأو إعادة التوجيه (RST) لمأخذ بروتوكول التحكم في الإرسال (TCP).

5xx: خطأ في الخادم

الرمز	التفاصيل
501 خطأ في الخادم الداخلي	فشل خادم ويب العام.
502 Bad عبارة	يحدث عندما يتلقى الخادم الذي يعمل كبوابة أو وكيل إستجابة غير صحيحة من خادم وارد. تشير إلى أن البوابة قد تلقت إستجابة غير مناسبة من الخادم الخادم الأصلي أو الخادم.
503 غير متوفرة الخدمة	يدل على أن الخادم غير قادر حاليا على معالجة الطلب بسبب الحمل الزائد المؤقت أو الصيانة المجدولة. وهذا يعني ضمنا أن الخادم خارج الخدمة مؤقتا ولكن يمكن أن يكون متوفرا مرة أخرى بعد مرور بعض الوقت.
504 مهلة العبارة	يشير إلى أن العميل أو الوكيل لم يتلقى إستجابة في الوقت المناسب من خادم ويب الذي حاول الوصول إليه لتحميل صفحة ويب أو تلبية طلب آخر من المستعرض. غالبا ما يعني ذلك أن خادم الخادم الخادم الخادم قد توقف عن العمل.

نشر صريح

هنا ....

حركة مرور HTTP في النشر الصريح دون مصادقة

العميل و SWA

تنتقل حركة مرور الشبكة بين عنوان IP الخاص بالعميل وعنوان IP الخاص بواجهة وكيل SWA (عادة ما تكون واجهة P1، ولكن يمكن أن تكون P2 أو واجهة الإدارة، استنادا إلى تكوين الوكيل).

يتم توجيه حركة المرور من العميل إلى منفذ TCP 80 أو 3128 إلى SWA (منافذ وكيل SWA الافتراضية هي TCP 80 و 3128، في هذا المثال نستخدم المنفذ 3128)

- مصافحة TCP.
- HTTP الحصول من العميل (غاية ip = swa ip، غاية ميناء = 3128)
- إستجابة HTTP من الوكيل (مصدر IP = SWA)
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

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

عميل الصورة إلى SWA، وضع HTTP الصريح

SWA وخادم الويب

تحدث حركة مرور الشبكة بين عنوان IP الخاص بالوكيل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من SWA إلى منفذ TCP رقم 80 ويتم الحصول عليها من منفذ عشوائي (وليس منفذ الوكيل)

- مصافحة TCP.
- HTTP الحصول من وكيل (الوجهة IP = خادم الويب، الغاية ميناء = 80)
- إستجابة HTTP من خادم ويب (مصدر IP = خادم وكيل)
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

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

الصورة- HTTP-SWA إلى خادم ويب -ذاكرة تخزين مؤقت صريحة-no

فيما يلي عينة من HTTP Get من العميل

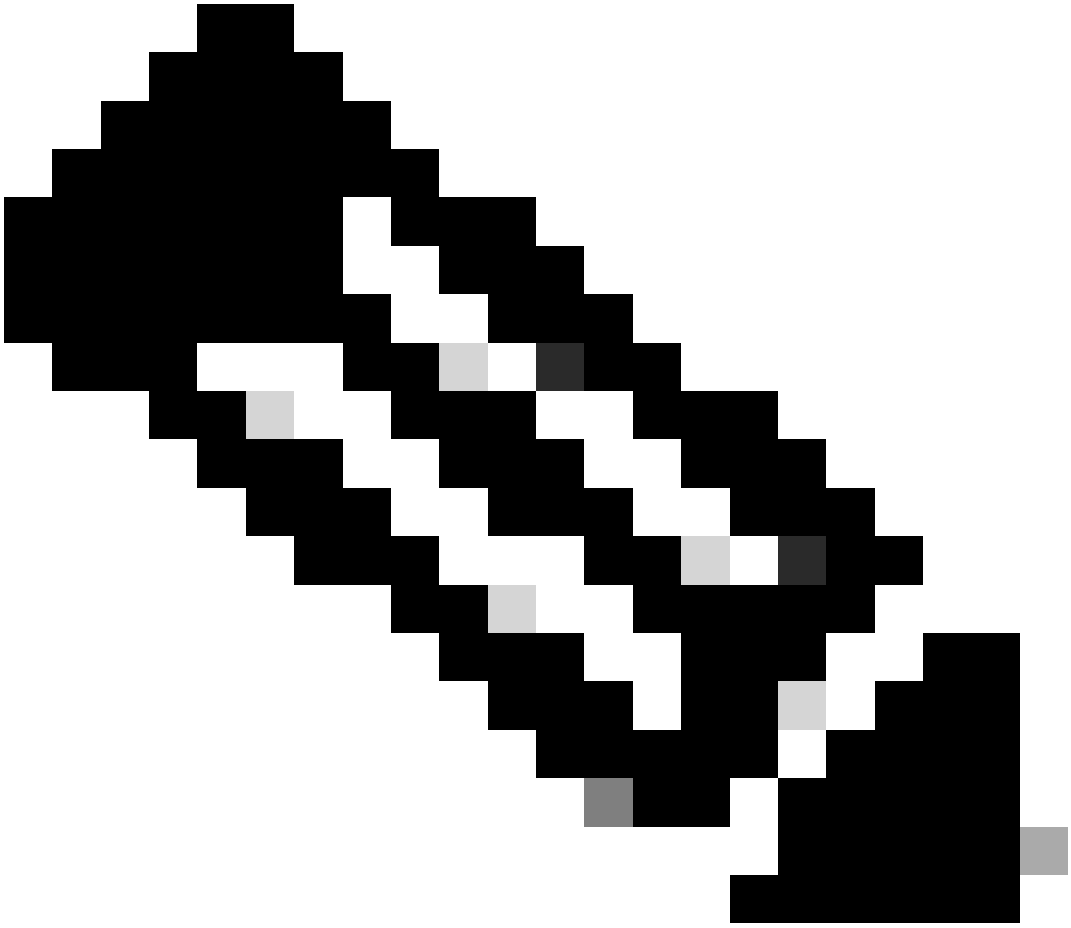
```
> Frame 12568: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:f3:64 (00:50:56:8d:f3:64)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.185
> Transmission Control Protocol, Src Port: 65238, Dst Port: 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- عميل إلى SWA HTTP GET- صريح

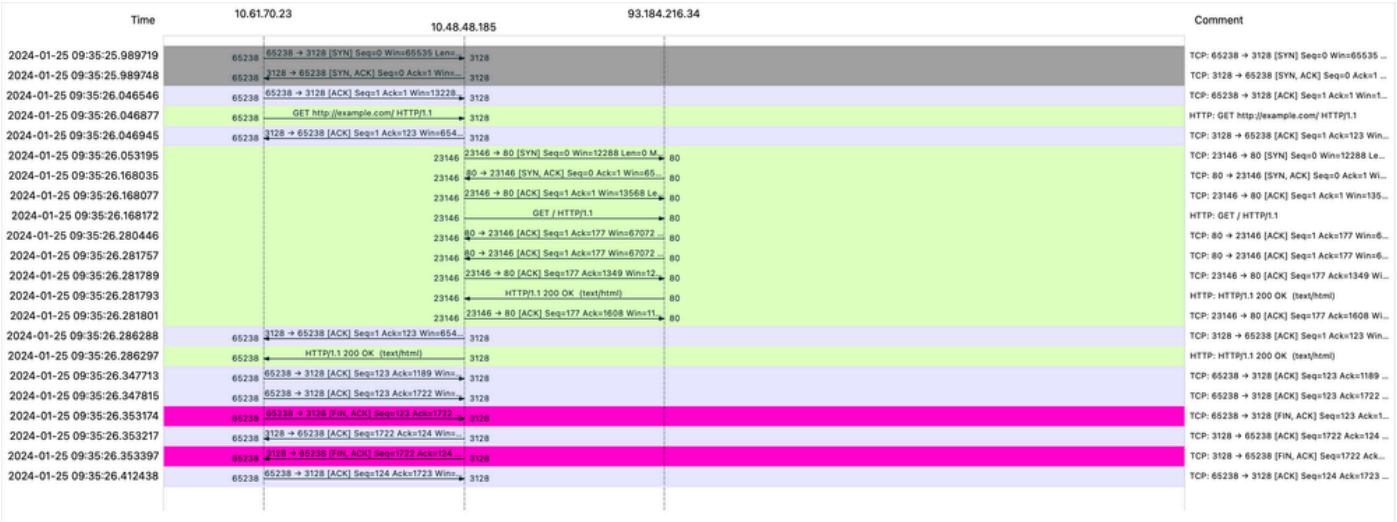
يمثل هذا التدفق الكامل لحركة مرور البيانات من العميل إلى SWA، ثم إلى خادم الويب، وأخيرا إلى العميل.

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

الصورة- كل حركة مرور HTTP ذاكرة تخزين مؤقت صريحة-ال



ملاحظة: يتم تمييز كل تدفق لحركة المرور بلون مختلف، حيث يكون التدفق من العميل إلى SWA هو لون واحد، بينما يكون التدفق من SWA إلى خادم الويب هو لون آخر.



الصورة- تدفق حركة المرور HTTP صريح - لا توجد ذاكرة تخزين مؤقت

هنا عينة من AccessLog:

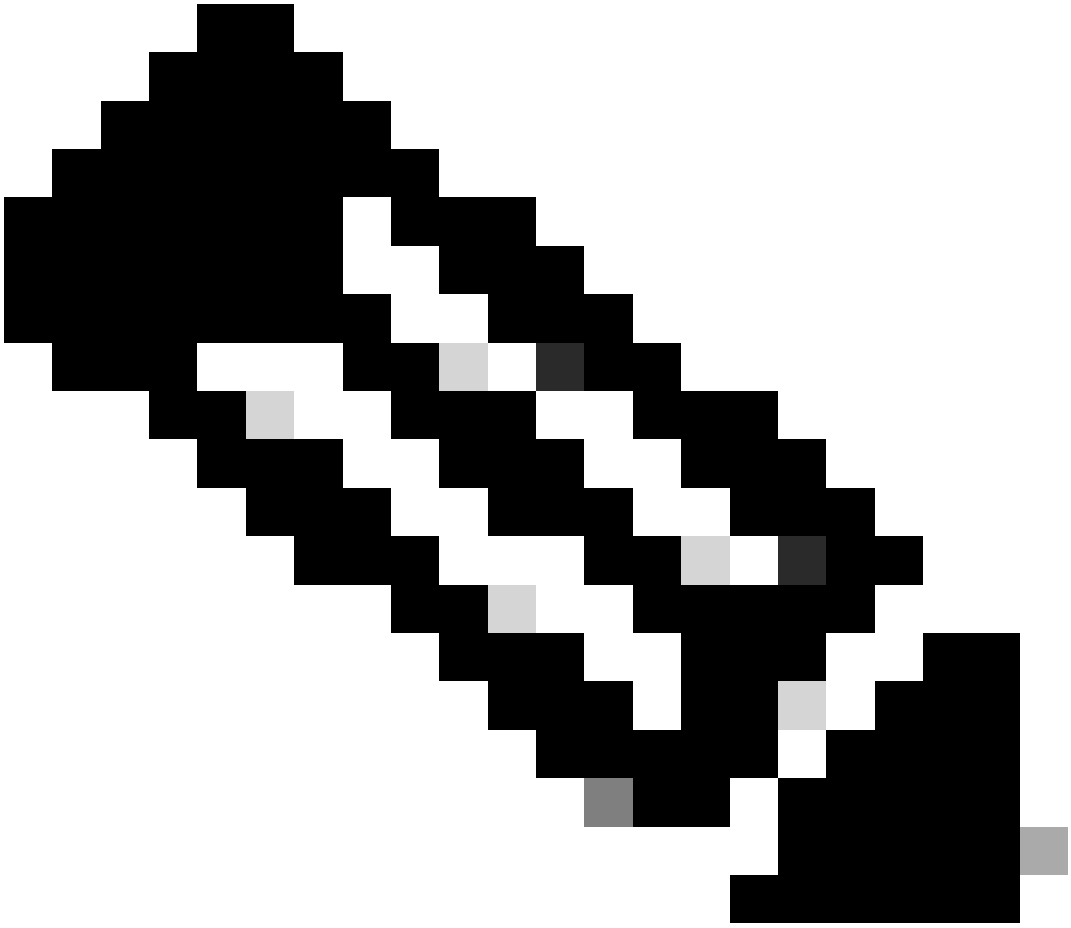
```
1706172876.686 224 10.61.70.23 TCP_MISS/200 1721 GET http://www.example.com/ - DIRECT/www.example.com t
```

حركة المرور مع البيانات المخزنة مؤقتا

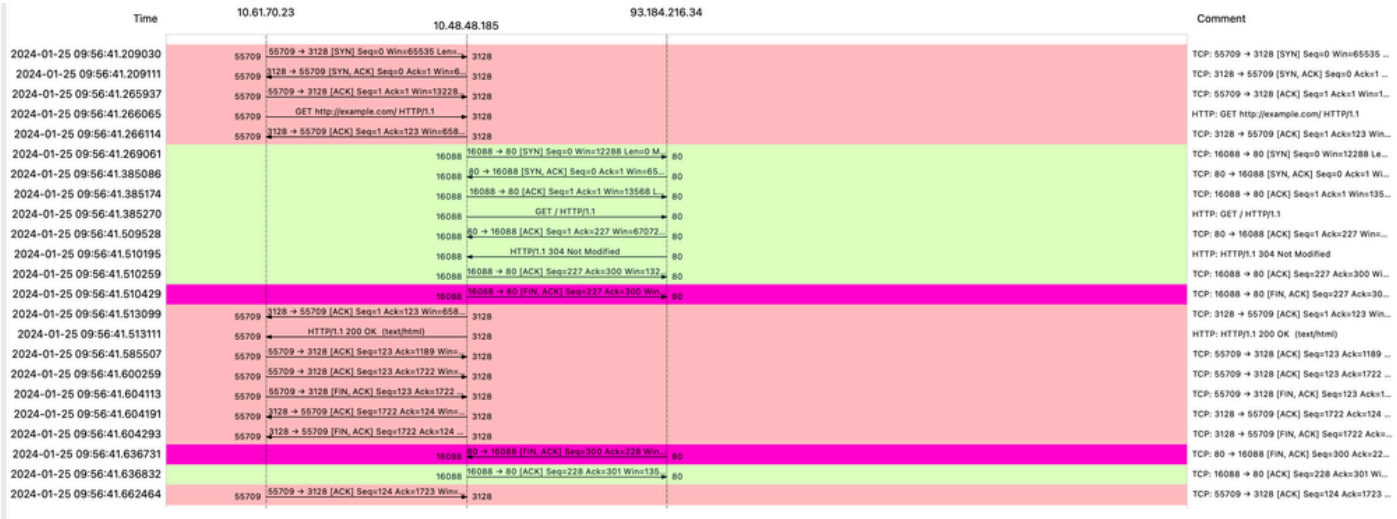
يمثل هذا تدفق حركة المرور بالكامل من العميل إلى SWA، عندما تكون البيانات في ذاكرة التخزين المؤقت ل SWA.

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=368792
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

الصورة- بيانات HTTP الصريحة المخزنة مؤقتا



ملاحظة: كما ترى خادم الويب يرجع إستجابة HTTP 304: لم يتم تعديل ذاكرة التخزين المؤقت. (في هذا المثال، حزمة رقم 1947)



صورة- تدفق HTTP صريح مع ذاكرة التخزين المؤقت

فيما يلي عينة من إستجابة 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/]
```

إستجابة IMAGE- HTTP EXPLICIT 304

هنا عينة من AccessLog:

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

حركة مرور HTTPs في النشر الصريح دون مصادقة

العميل و SWA

تنتقل حركة مرور الشبكة بين عنوان IP الخاص بالعميل وعنوان IP الخاص بواجهة وكيل SWA (عادة ما تكون واجهة P1، ولكن يمكن أن تكون P2 أو واجهة الإدارة، استنادا إلى تكوين الوكيل).

يتم توجيه حركة المرور من العميل إلى منفذ TCP 80 أو 3128 إلى SWA (منافذ وكيل SWA الافتراضية هي TCP 80 و 3128، في هذا المثال نستخدم المنفذ 3128)

- مصافحة TCP.

- http اتصال من عميل (غاية ip = swa، غاية ميناء = 3128)
- إستجابة HTTP من الوكيل (مصدر IP = SWA)
- Client Hello باستخدام SNI لعنوان URL (مصدر IP = عميل)
- Server Hello (المصدر IP = SWA)
- تبادل مفتاح الخادم (مصدر IP = SWA)
- تبادل مفتاح العميل (IP المصدر = العميل)
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

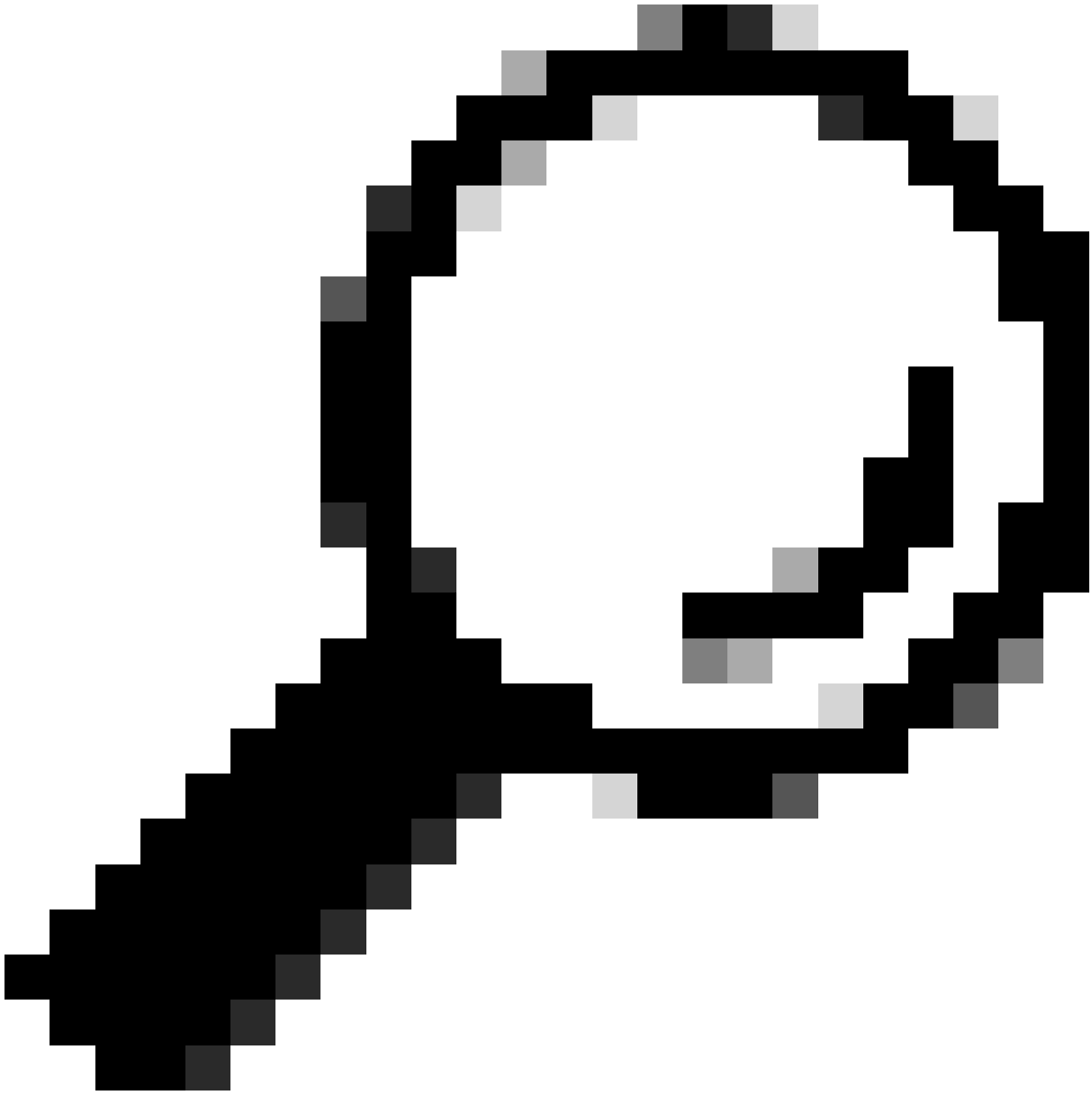
No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
18	2024-01-25 12:31:37.(318168644…	10.61.70.23	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	78	12	61484 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1676451324 TSecr=0 SACK_PERM
19	2024-01-25 12:31:37.(330015315…	10.48.48.165	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

الصورة- عميل HTTPS إلى SWA-Explicit- الـ توجد ذاكرة تخزين مؤقت

فيما يلي تفاصيل Client Hello من Client to SWA، كما يمكنك أن ترى في مؤشر اسم الخادم (SNI) عنوان URL الخاص بخادم الويب الذي يمكن رؤيته في هذا المثال، وهو www.example.com وقام العميل بالإعلان عن 17 مجموعة شفرة:

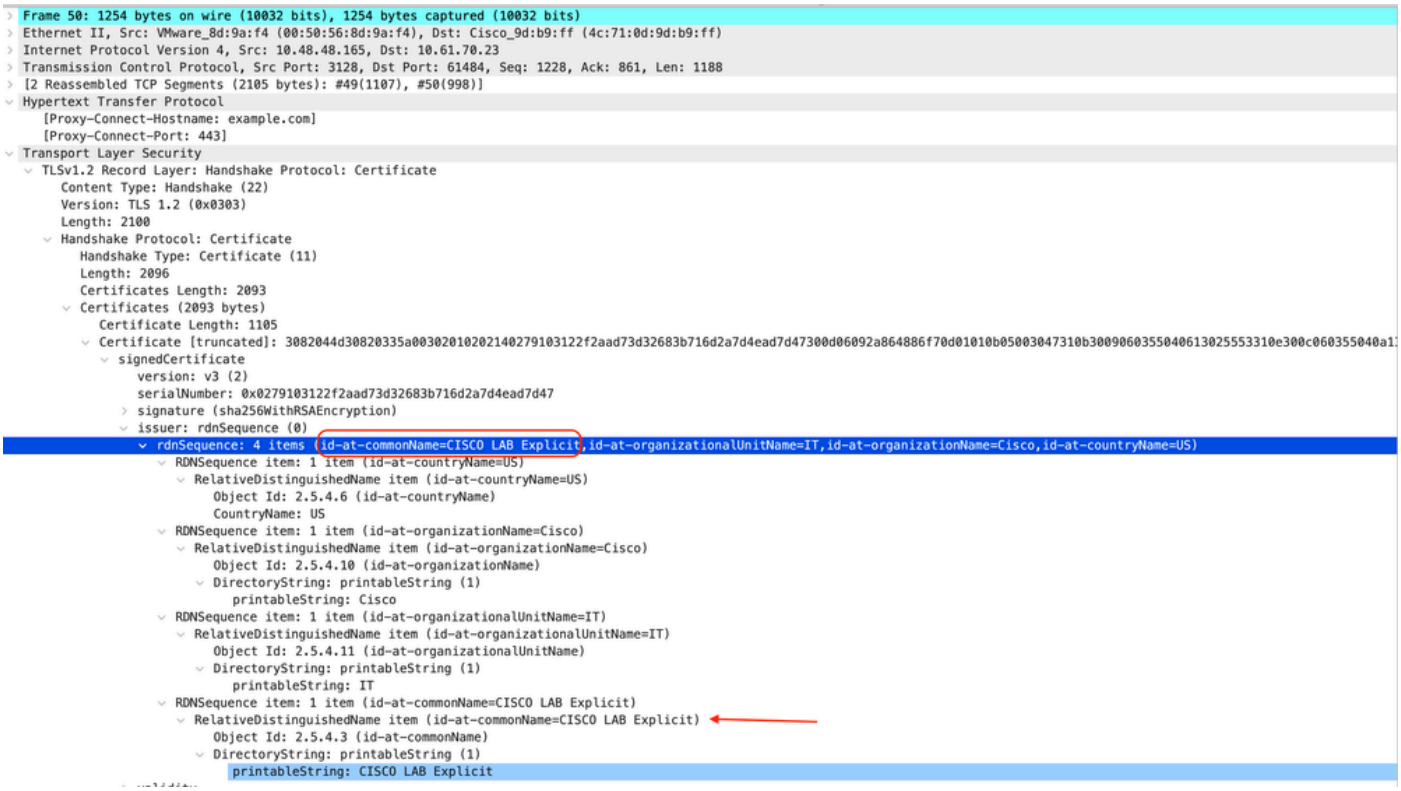
```
> Frame 28: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:9a:f4 (00:50:56:8d:9a:f4)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.165
> Transmission Control Protocol, Src Port: 61484, Dst Port: 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]
```

الصورة- HTTPS Client Hello - صريح - عميل الى SWA



تلميح: يمكنك إستخدام عامل التصفية هذا في Wireshark للبحث عن URL/SNI:
tls.handshake.extensions_server_name == "www.example.com"

هنا عينة من الشهادة التي أرسلتها SWA إلى العميل



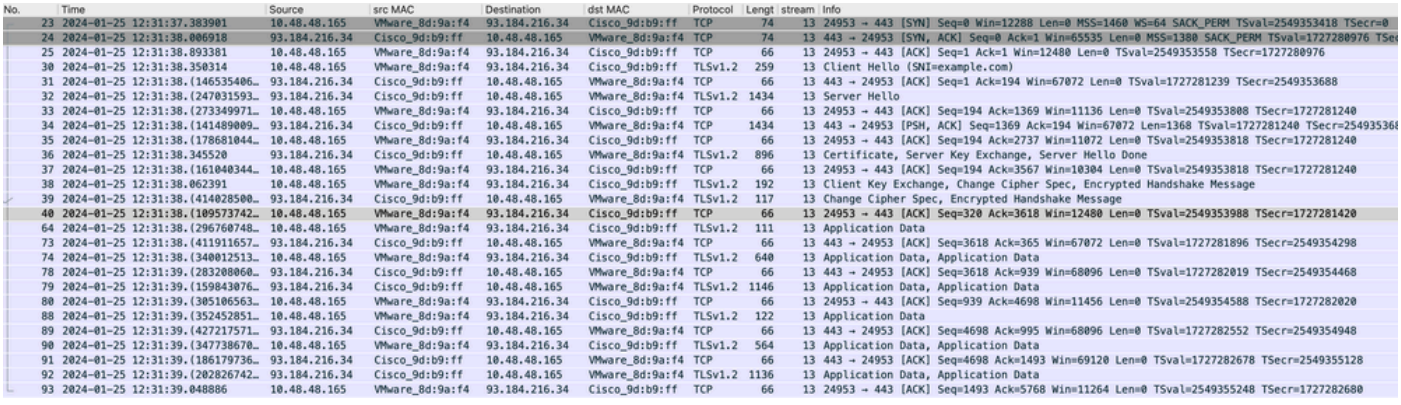
الصورة- شهادة HTTPS - صريح - SWA إلى العميل

SWA وخادم الويب

تحدث حركة مرور الشبكة بين عنوان IP الخاص بالوكيل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من SWA إلى منفذ TCP رقم 443 (ليس منفذ الوكيل)

- مصافحة TCP.
- Client Hello (Destination IP = Web Server، Destination Port = 443)
- Server Hello (مصدر IP = خادم ويب)
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

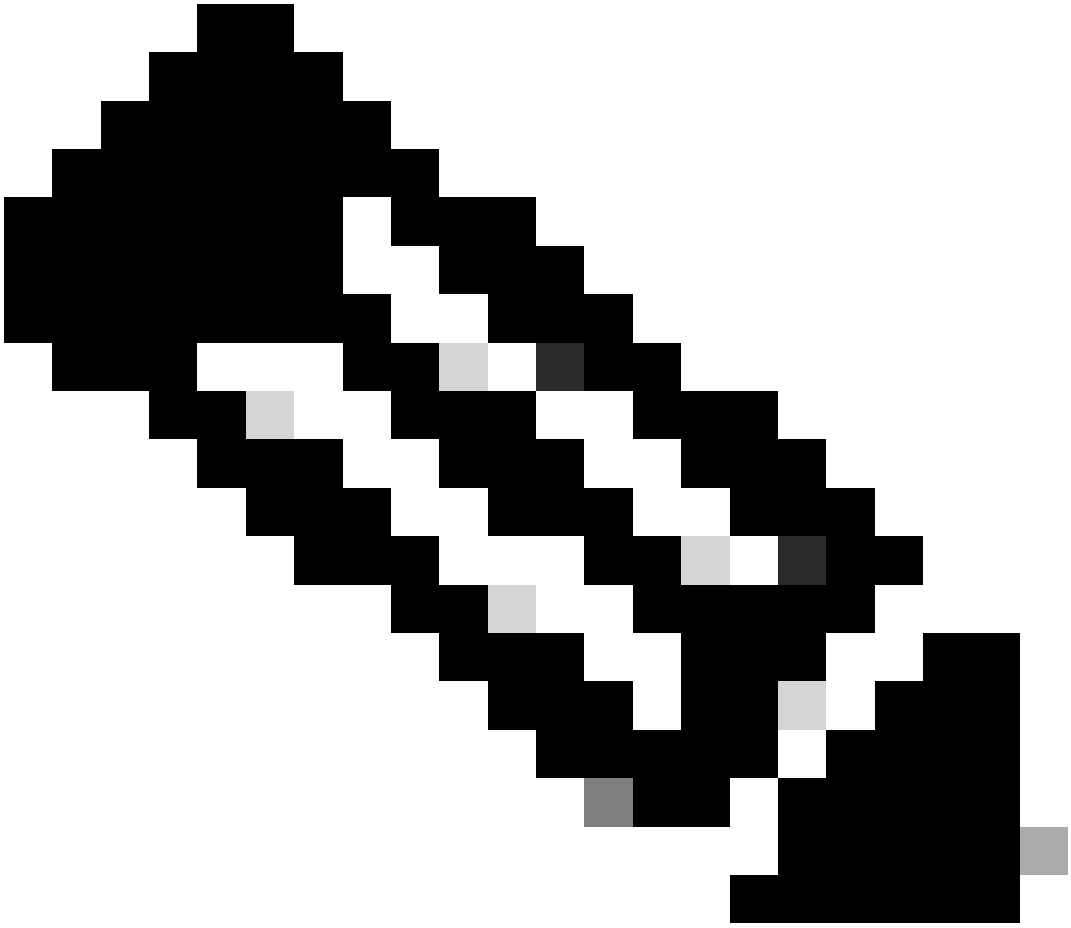


الصورة- HTTPS - صريح - SWA إلى خادم الويب

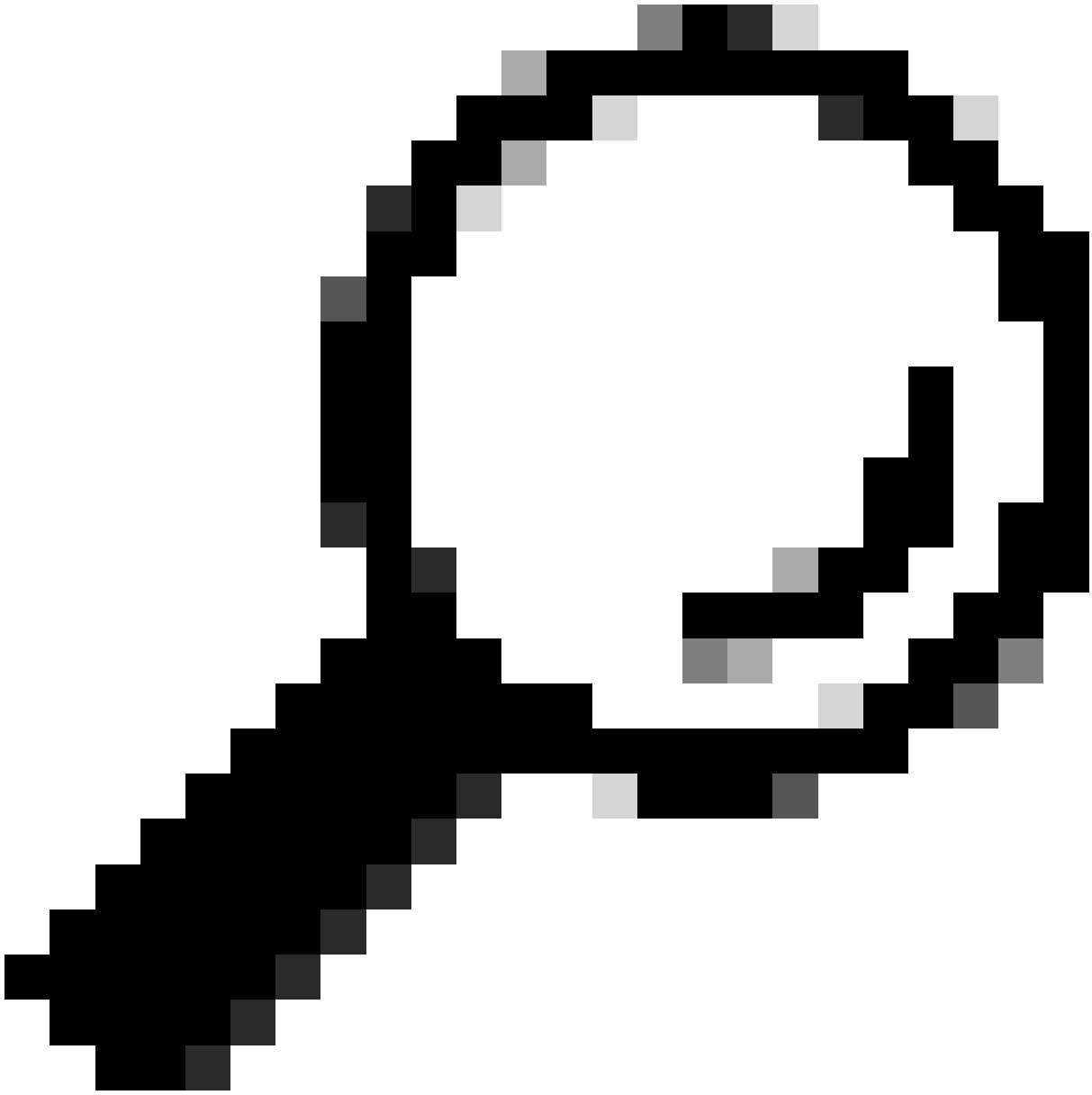
فيما يلي تفاصيل Client Hello من SWA إلى خادم الويب، كما يمكنك مشاهدة SWA المعلن عنها في 12 مجموعة تشفير:

```
> 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
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 188
    v 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
      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: 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]
```

IMAGE - HTTPS Client Hello - SWA إلى خادم ويب - ال مشكلة



ملاحظة: تختلف مجموعات التشفير الموضحة هنا عن مجموعات التشفير في مجموعات برامج Client Hello الخاصة بالعميل من Client إلى SWA، حيث إن SWA، التي تم تكوينها لفك تشفير حركة المرور هذه، تستخدم شفرة خاصة بها.



تلميح: في تبادل مفتاح الخادم من SWA إلى خادم ويب، تظهر شهادة خادم ويب. ومع ذلك، إذا عثر وكيل تدفق البيانات على تكوين SWA، تظهر شهادته بدلا من شهادة خادم الويب.

فيما يلي عينة من اتصال HTTP من العميل

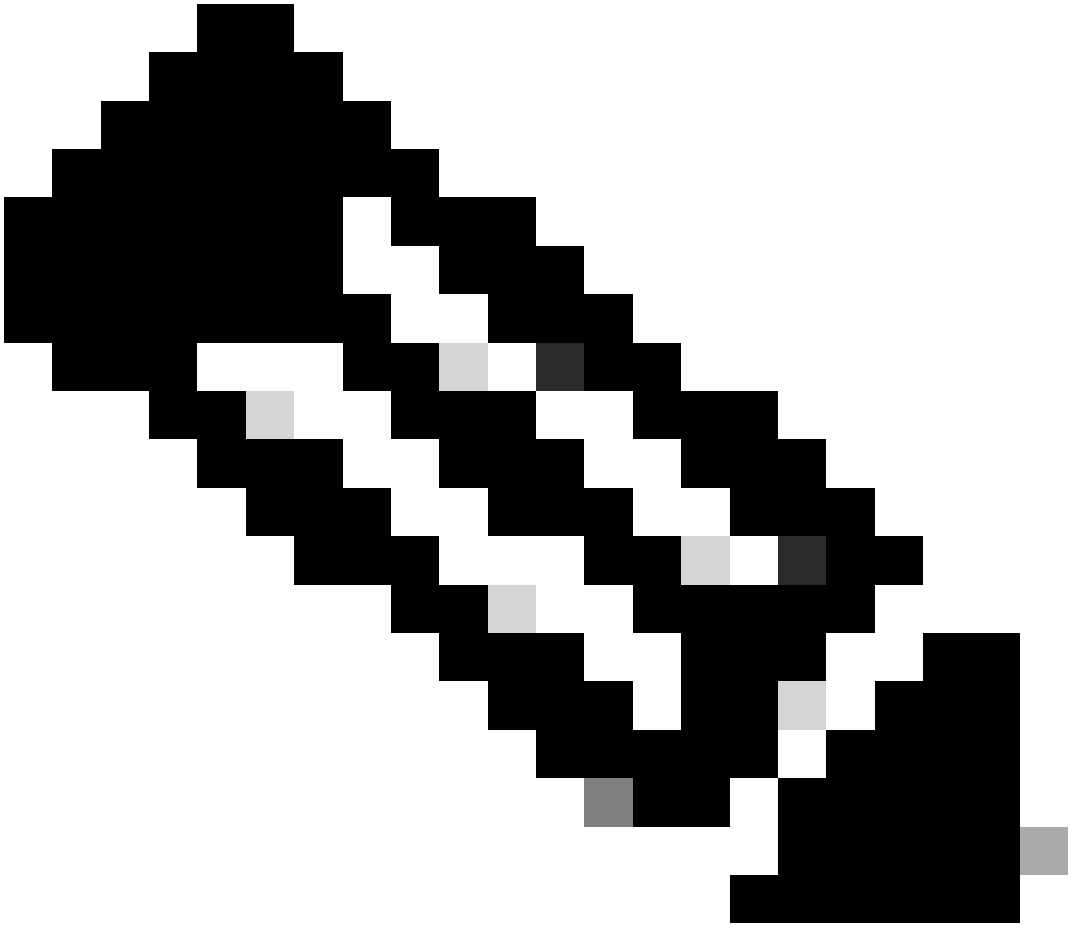
```
> Frame 21: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:9a:f4 (00:50:56:8d:9a:f4)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.165
> Transmission Control Protocol, Src Port: 61484, Dst Port: 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]
```

اتصال HTTP للعميل للصورة

يمثل هذا التدفق الكامل لحركة مرور البيانات من العميل إلى SWA، ثم إلى خادم الويب، وأخيرا إلى العميل.

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

الصورة- ذاكرة تخزين مؤقت كاملة لتدفق HTTPS صريح

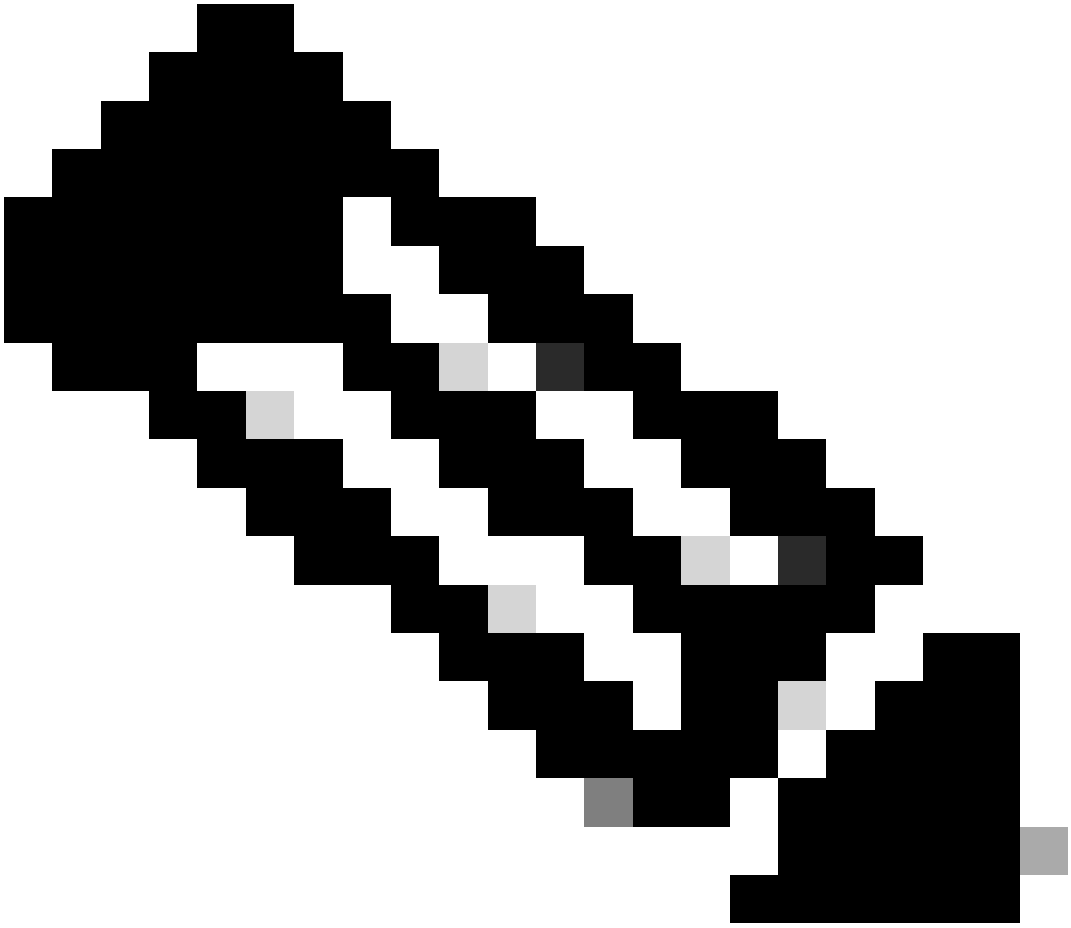


ملاحظة: يتم تمييز كل تدفق لحركة المرور بلون مختلف، حيث يكون التدفق من العميل إلى SWA هو لون واحد، بينما يكون التدفق من SWA إلى خادم الويب هو لون آخر.

الصورة- تدفق HTTPS- صريح - الوجود الذاكرة تخزين مؤقت

هنا عينة من AccessLog:

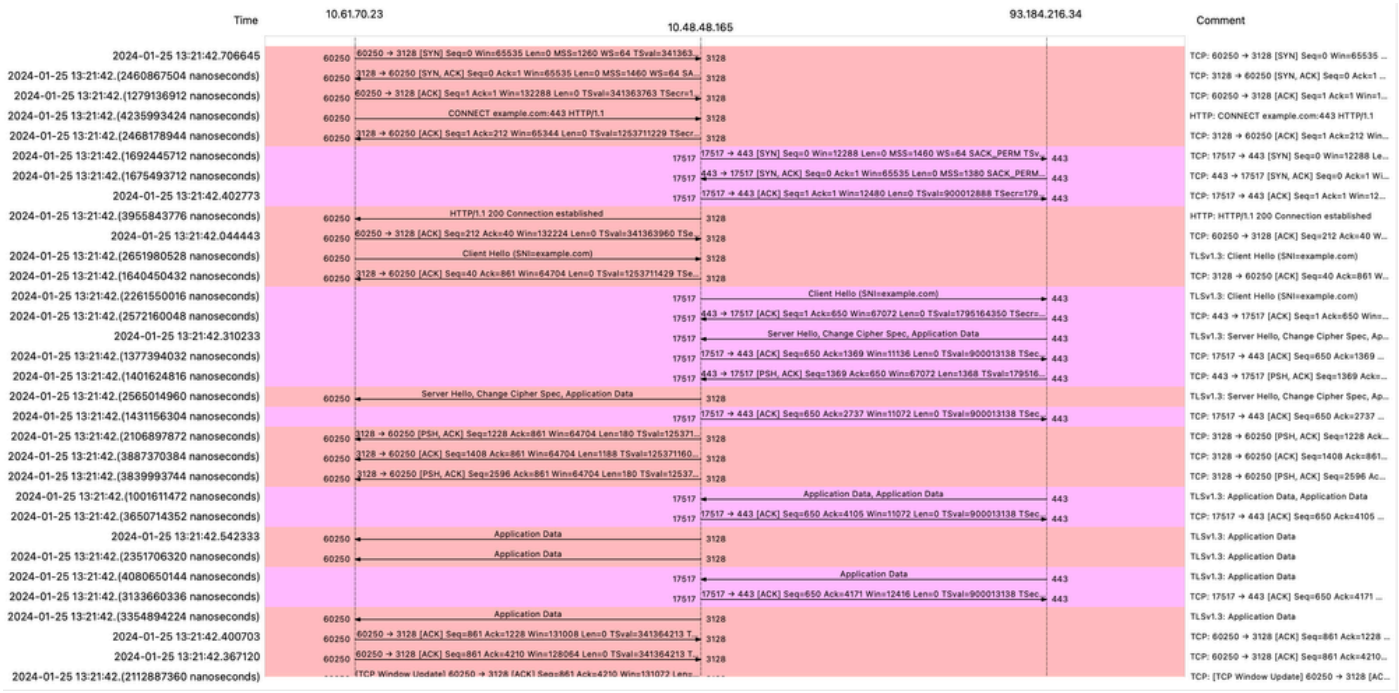
```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.examp
```



ملاحظة: كما ترى في النشر الشفاف لحركة مرور HTTPS، يوجد سطران في سجلات الوصول، السطر الأول هو عندما يتم تشفير حركة مرور البيانات ويمكنك مشاهدة CONNECT وعنوان URL الخاص بخادم الويب يبدأ ب tunnel://. إذا تم تمكين فك التشفير في SWA، فإن السطر الثاني يحتوي على GET ويبدأ عنوان URL بالكامل مع HTTPS، مما يعني أنه تم فك تشفير حركة المرور.

مرور بيانات HTTPS

إذا قمت بتكوين SWA الخاص بك للمرور عبر حركة المرور، هنا هو التدفق الإجمالي:



الصورة- مرور HTTPS - صريح - تدفق

فيما يلي نموذج Client Hello من SWA إلى خادم ويب:

```
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)
```

الصورة- كلمة مرور HTTPS - صريح - SWA إلى WebServer - ترحيب العميل

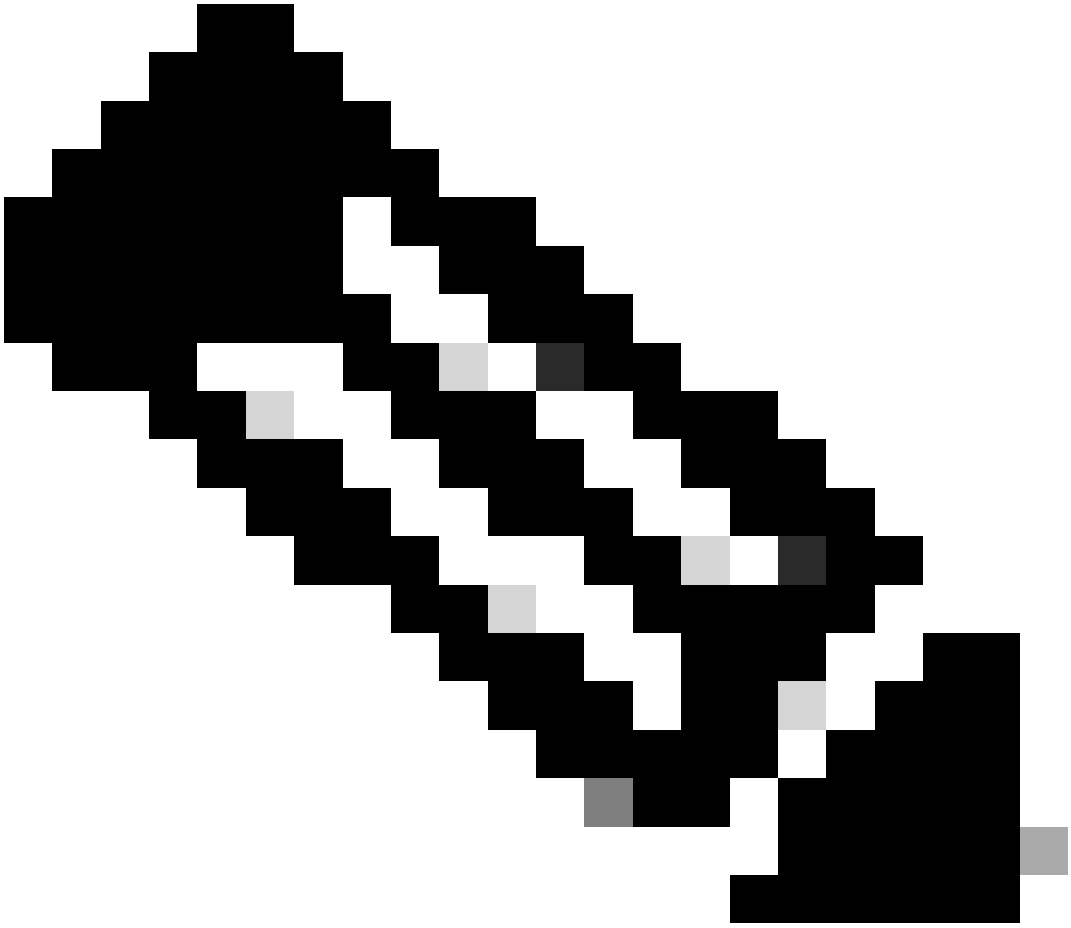
وهو نفس ترجيب العميل من قبل العميل إلى SWA:

```
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)
```

الصورة- كلمة مرور HTTPS - صريح - عميل إلى SWA - ترجيب العميل

هنا نموذج AccessLog:

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



ملاحظة: كما ترى، هو مجرد سطر واحد والإجراء هو PASSTHRU.

النشر الشفاف

حركة مرور HTTP في النشر الشفاف دون مصادقة

العميل و SWA

تنتقل حركة مرور الشبكة بين عنوان IP الخاص بالعميل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من العميل إلى منفذ TCP رقم 80 (ليس منفذ الوكيل)

- مصافحة TCP.
- HTTP الحصول من العميل (غاية ip = ويب دان، غاية ميناء = 80)
- إستجابة HTTP من الوكيل (مصدر IP = خادم ويب)
- نقل البيانات

- إنهاء اتصال TCP (مصافحة 4 طرق)

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

الصورة - عميل إلى وكيل - HTTP - شفاف - الوجود المصادق

فيما يلي عينة من HTTP Get من العميل

```
> 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- عميل إلى وكيل - HTTP - شفاف - الوجود المصادق - HTTP العميل get

SWA وخادم الويب

تحدث حركة مرور الشبكة بين عنوان IP الخاص بالوكيل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من SWA إلى منفذ TCP رقم 80 (ليس منفذ الوكيل)

- مصافحة TCP.
- HTTP الحصول من وكيل (الوجهة IP = خادم الويب، الغاية ميناء = 80)
- إستجابة HTTP من خادم ويب (مصدر IP = خادم وكيل)
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

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 o
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

الصورة- الوكيل وخادم الويب - HTTP - شفاف - الوجود المصادق

فيما يلي عينة من HTTP Get من الوكيل

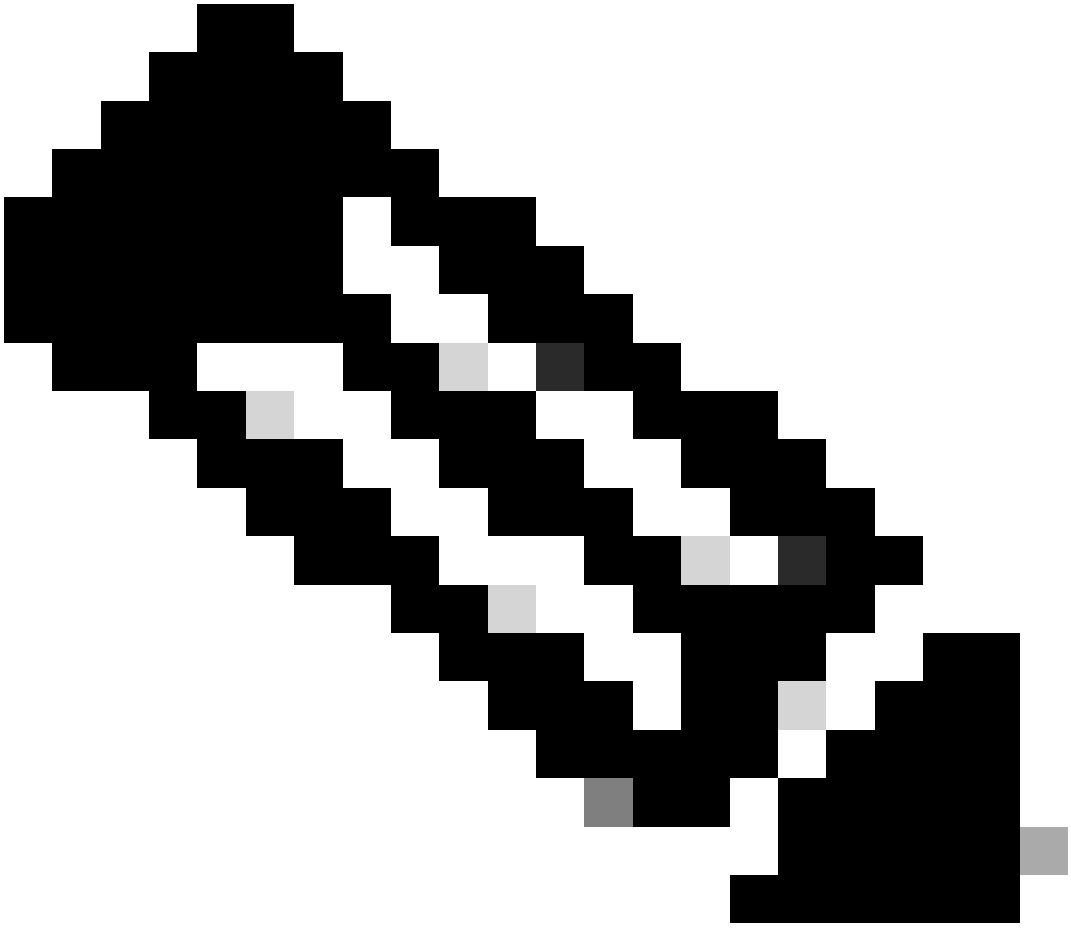
```
> Frame 20: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
> Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
> Transmission Control Protocol, Src Port: 54468, Dst Port: 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- وكيل إلى خادم ويب - HTTP - شفاف - ال توجد مصادقة - HTTP للوكيل

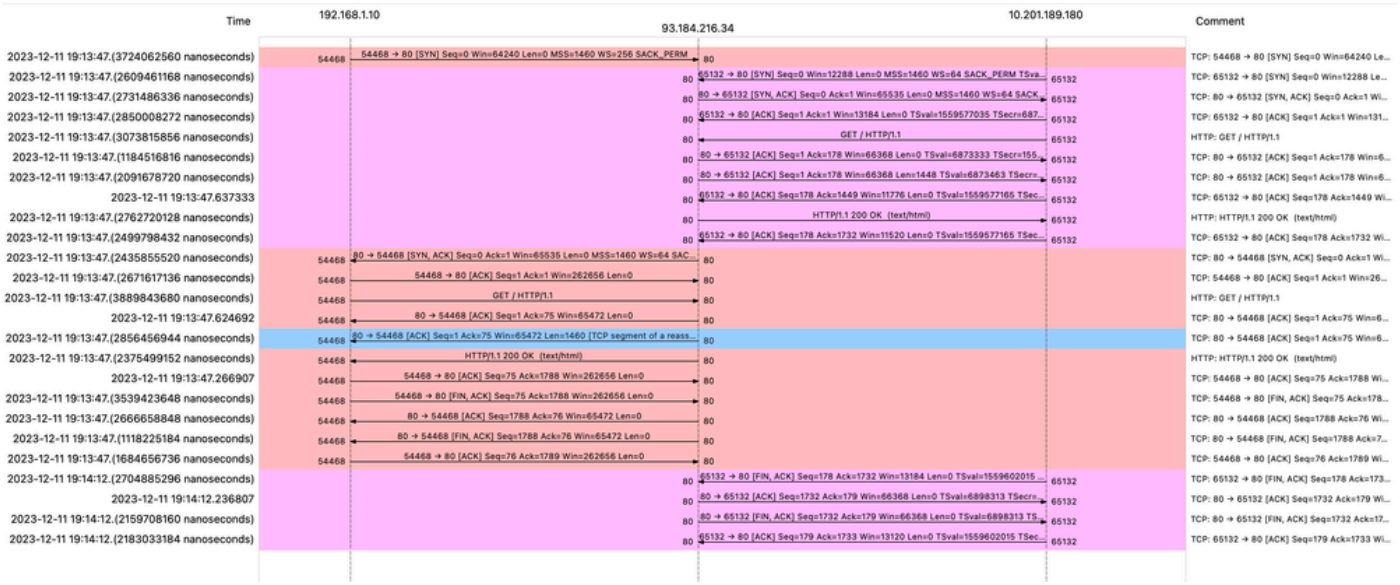
يمثل هذا التدفق الكامل لحركة مرور البيانات من العميل إلى SWA، ثم إلى خادم الويب، وأخيرا إلى العميل.

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

الصورة- حركة مرور إجمالية - HTTP - شفاف - ال توجد مصادقة



ملاحظة: يتم تمييز كل تدفق لحركة المرور بلون مختلف، حيث يكون التدفق من العميل إلى SWA هو لون واحد، بينما يكون التدفق من SWA إلى خادم الويب هو لون آخر.



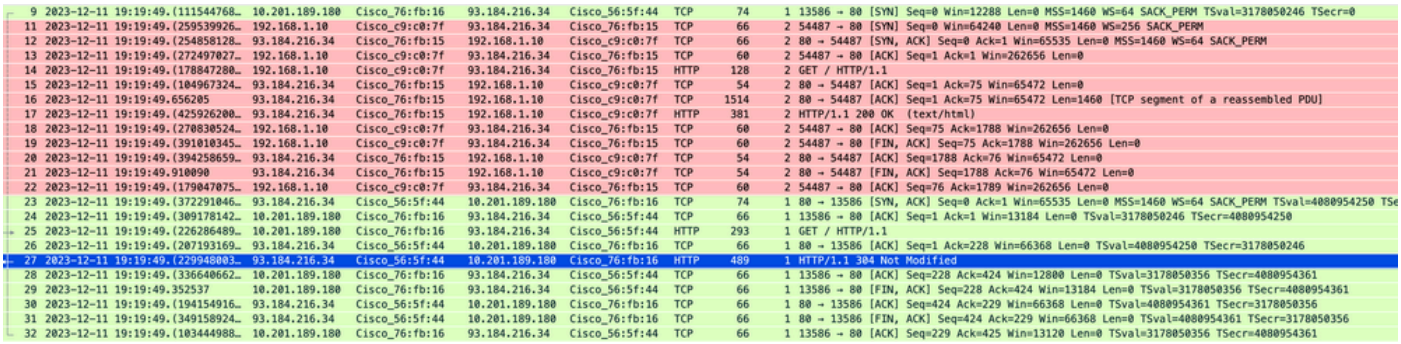
الصورة- تدفق WCCP HTTP

هنا عينة من AccessLog:

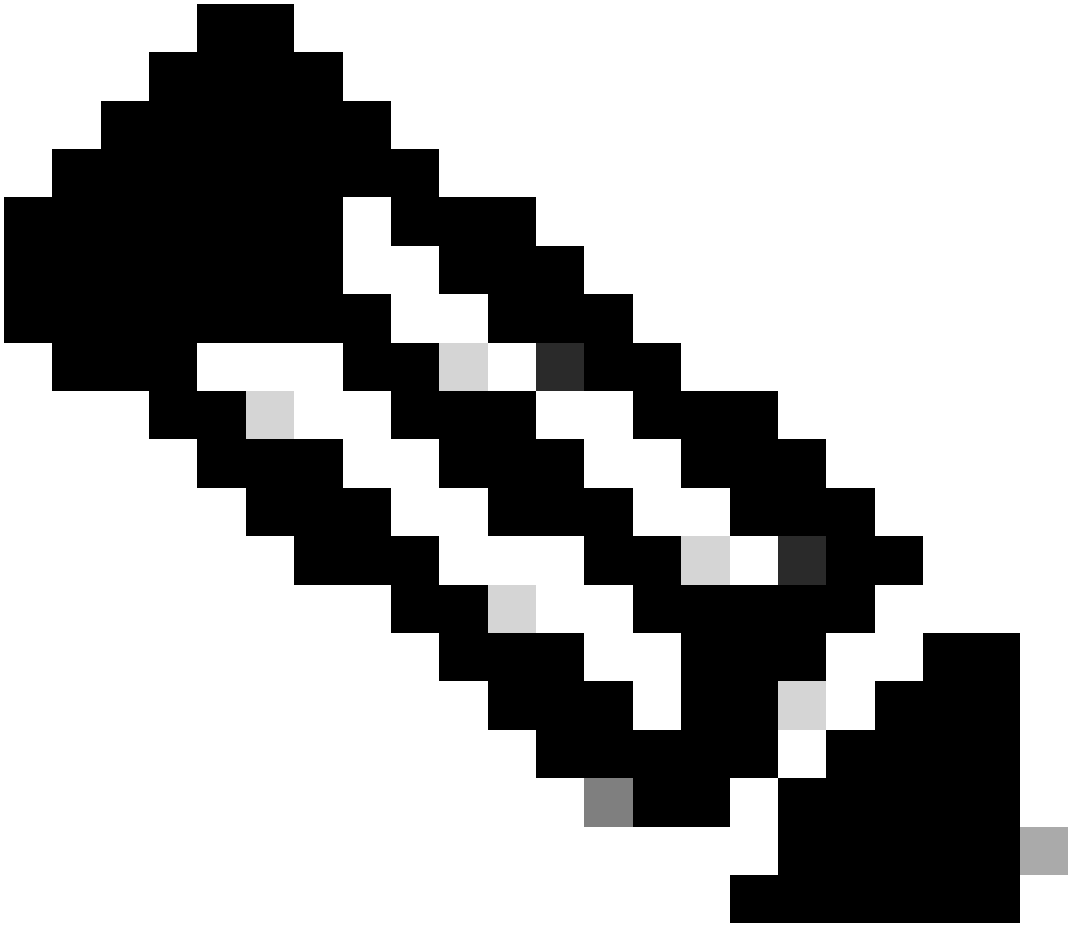
```
1702318427.181 124 192.168.1.10 TCP_MISS/200 1787 GET http://www.example.com/ - DIRECT/www.example.com
```

حركة المرور مع البيانات المخزنة مؤقتا

يمثل هذا تدفق حركة المرور بالكامل من العميل إلى SWA، عندما تكون البيانات في ذاكرة التخزين المؤقت ل SWA.



الصورة- المخزنة مؤقتا- حركة مرور إجمالية - HTTP - شفاف - ال توجد مصادقة



ملاحظة: كما ترى خادم الويب يرجع إستجابة HTTP 304: لم يتم تعديل ذاكرة التخزين المؤقت. (في هذا المثال، الحزمة رقم 27)

فيما يلي عينة من إستجابة 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
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/]
```

الصورة- المخزنة مؤقتا - إستجابة HTTP 304 - HTTP - شفاف - لا توجد مصادقة

هنا عينة من AccessLog:

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

حركة مرور HTTPs في النشر الشفاف دون مصادقة

العميل و SWA

تنتقل حركة مرور الشبكة بين عنوان IP الخاص بالعميل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من العميل إلى منفذ TCP رقم 443 (ليس منفذ الوكيل)

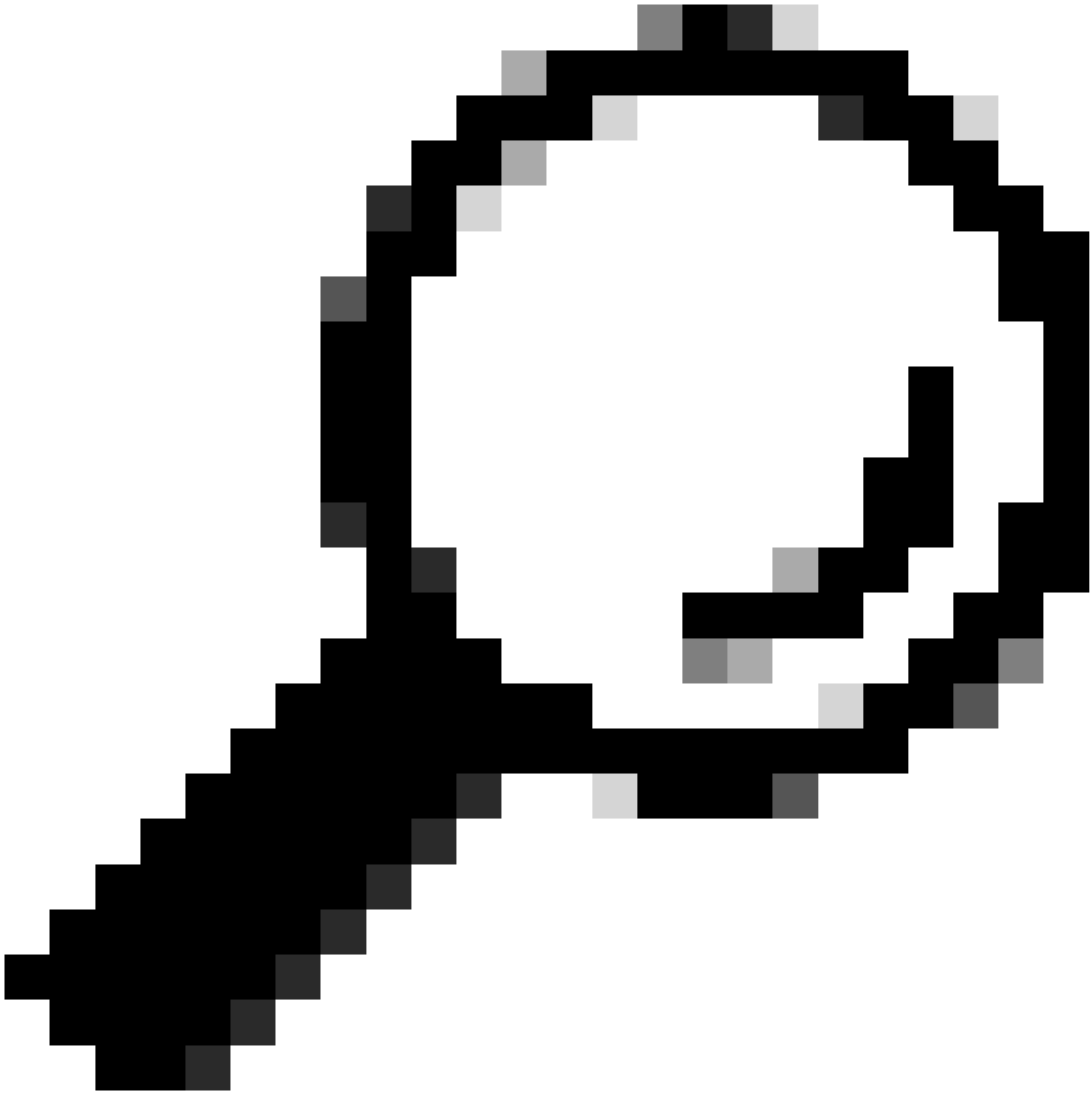
- مصافحة TCP.
- TLS Handshake Client Hello - Server Hello - Server Key Exchange - Client Key Exchange
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)

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

فيما يلي تفاصيل Client Hello من Client إلى SWA، كما يمكنك أن ترى في إشارة اسم الخادم (SNI) عنوان URL الخاص بخادم الويب الذي يمكن رؤيته في هذا المثال وهو www.example.com .

```
Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
Transmission Control Protocol, Src Port: 54515, Dst Port: 443, Seq: 1, Ack: 1, Len: 188
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 183
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 179
        Version: TLS 1.2 (0x0303)
        Random: 657756ab224a3f64600e99172a8d38f86b689c7eb4bb121bf54d8c96540a0f5d
        Session ID Length: 0
        Cipher Suites Length: 42
        Cipher Suites (21 suites)
        Compression Methods Length: 1
        Compression Methods (1 method)
        Extensions Length: 96
        Extension: server_name (len=16) name=example.com
          Type: server_name (0)
          Length: 16
          Server Name Indication extension
            Server Name list length: 14
            Server Name Type: host_name (0)
            Server Name length: 11
            Server Name: example.com
        Extension: supported_groups (len=8)
        Extension: ec_point_formats (len=2)
        Extension: signature_algorithms (len=26)
        Extension: session_ticket (len=0)
        Extension: application_layer_protocol_negotiation (len=11)
        Extension: extended_master_secret (len=0)
        Extension: renegotiation_info (len=1)
        [JA4: t12d2108h1_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]
```

الصورة- Client Hello - عميل إلى وكيل - شفاف - بدون مصادقة

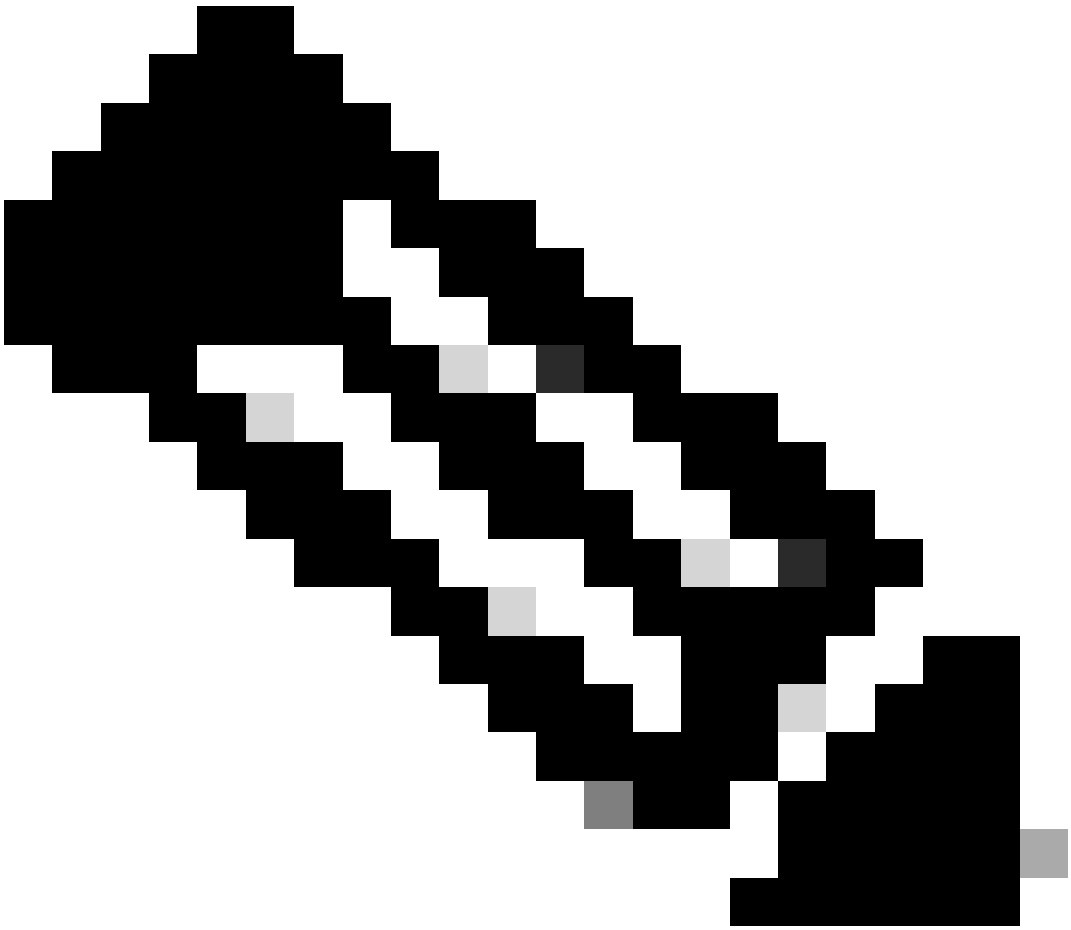


تلميح: يمكنك إستخدام عامل التصفية هذه في Wireshark للبحث عن URL/SNI
tls.handshake.extensions_server_name == "www.example.com"

فيما يلي عينة من Server Key Exchange

```
> Frame 257: 1043 bytes on wire (8344 bits), 1043 bytes captured (8344 bits)
> Ethernet II, Src: Cisco_76:fb:15 (70:70:8b:76:fb:15), Dst: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 443, Dst Port: 54515, Seq: 1461, Ack: 189, Len: 989
> [2 Reassembled TCP Segments (2054 bytes): #256(1379), #257(675)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2049
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2045
        Certificates Length: 2042
      v Certificates (2042 bytes)
          Certificate Length: 1098
        v Certificate [truncated]: 30820446308203 2ea003020102021404409073 79f2aad73d32683b716d2a7ddf2b8e2a300d06092a864886f70d01010b05003040310b3009060355040613025553110300e060355040…
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x0440907379f2aad73d32683b716d2a7ddf2b8e2a
            > signature (sha256WithRSAEncryption)
            v issuer: rdnSequence (0)
              v rdnSequence: 4 items (id-at-commonName=CISCOCALo,id-at-organizationalUnitName=IT,id-at-organizationName=wsatest,id-at-countryName=US)
                > RDNSequence item: 1 item (id-at-countryName=US)
                > RDNSequence item: 1 item (id-at-organizationName=wsatest)
                > RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
                > RDNSequence item: 1 item (id-at-commonName=CISCOCALo)
            > validity
            > subject: rdnSequence (0)
            > subjectPublicKeyInfo
            > extensions: 5 items
          > algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted [truncated]: 1db2a57a8bbf4def6b1845eace5a7a17f27704e61b102f13c20a696c076bf3e736283d6cffa6c1d9417865ba7f4d4663bd3677423996e23db7f25d232eaa3110a24e72871d8cf2111d3…
          Certificate Length: 938
        > Certificate [truncated]: 308203a63082028ea003020102020900a447d8363a186f2f300d06092a864886f70d01010b05003040310b30090603550406130255533110300e060355040a13077773617465737431 0…
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

Image- Server Key Exchange - عميل إلى وكيل - شفاف - ال توجد مصادقة



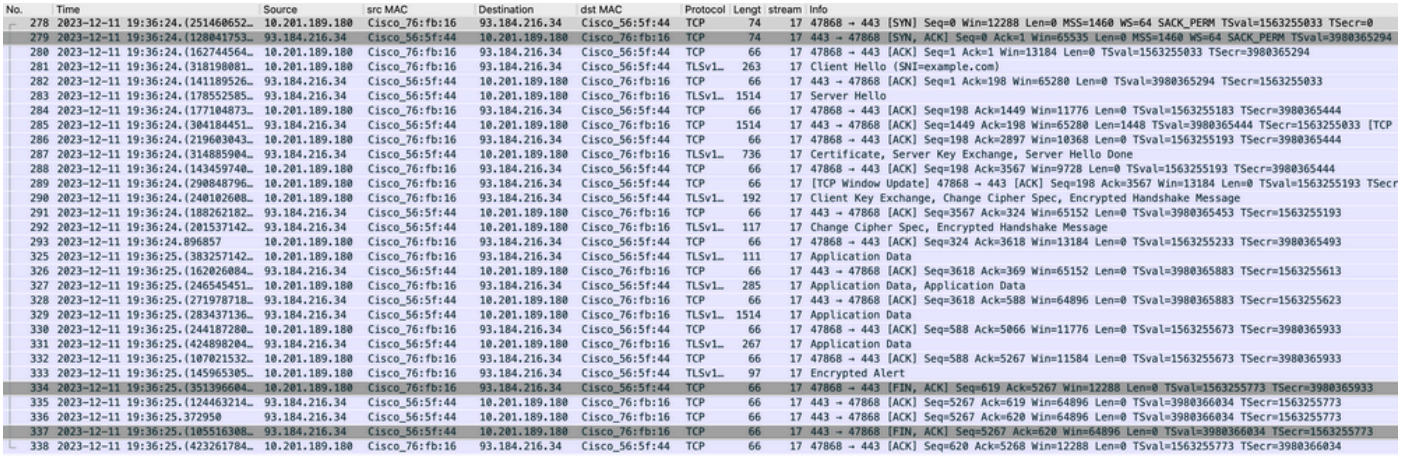
ملاحظة: كما ترى، الشهادة التي تم تكوينها في SWA كشهادة فك تشفير.

SWA وخادم الويب

تحدث حركة مرور الشبكة بين عنوان IP الخاص بالوكيل وعنوان IP الخاص بخادم الويب.

يتم توجيه حركة المرور من SWA إلى منفذ TCP رقم 443 (ليس منفذ الوكيل)

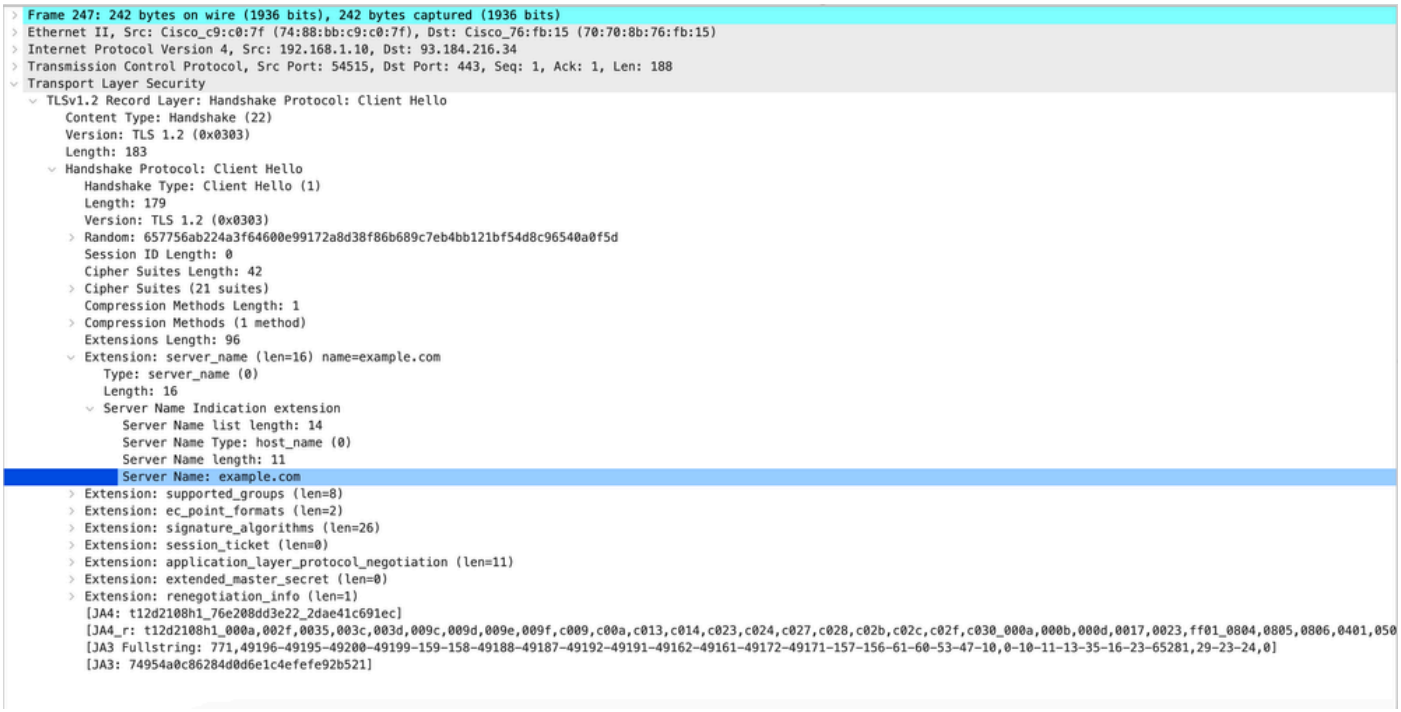
- مصافحة TCP.
- TLS Handshake Client Hello - Server Hello - Server Key Exchange - Client Key Exchange
- نقل البيانات
- إنهاء اتصال TCP (مصافحة 4 طرق)



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

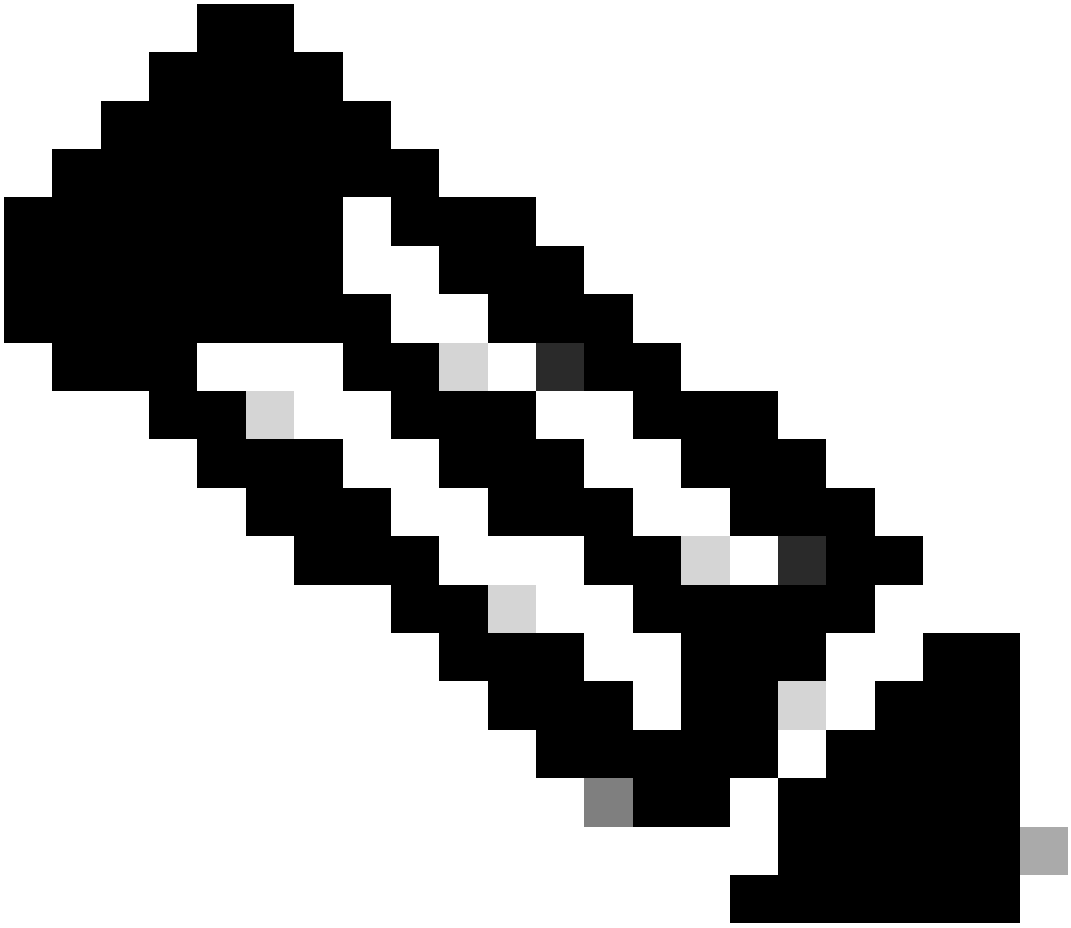
الصورة- وكيل لخادم الويب - HTTP - شفاف - الوجود مصادقة

في ما يلي عينة من Client Hello من SWA إلى خادم ويب

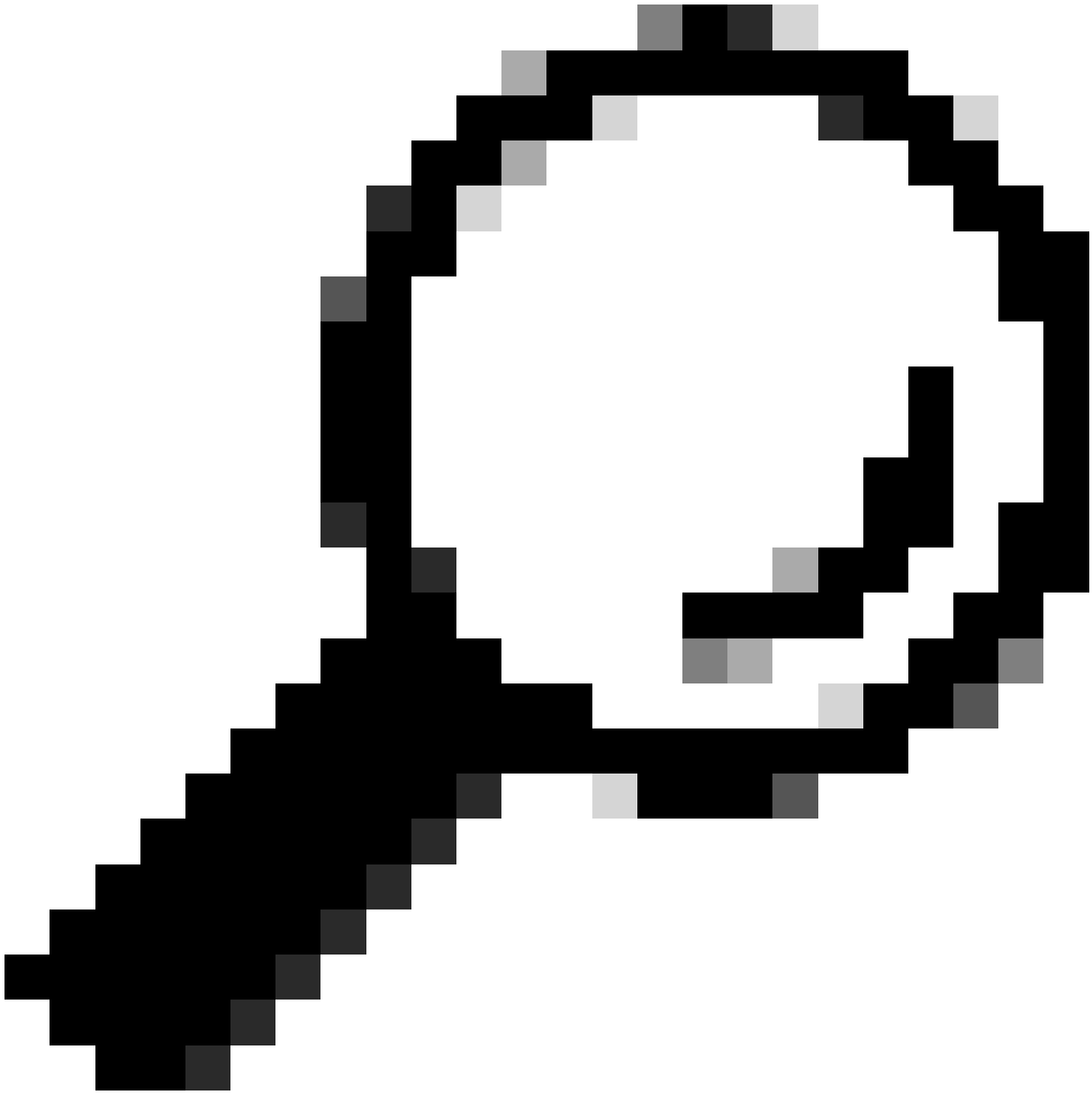


```
Frame 247: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
Ethernet II, Src: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f), Dst: Cisco_76:fb:15 (70:70:8b:76:fb:15)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 93.184.216.34
Transmission Control Protocol, Src Port: 54515, Dst Port: 443, 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: 74954a0c86284d0d6e1c4efefe92b521]
```

الصورة- Client Hello - وكيل إلى خادم ويب - شفاف - الوجود مصادقة



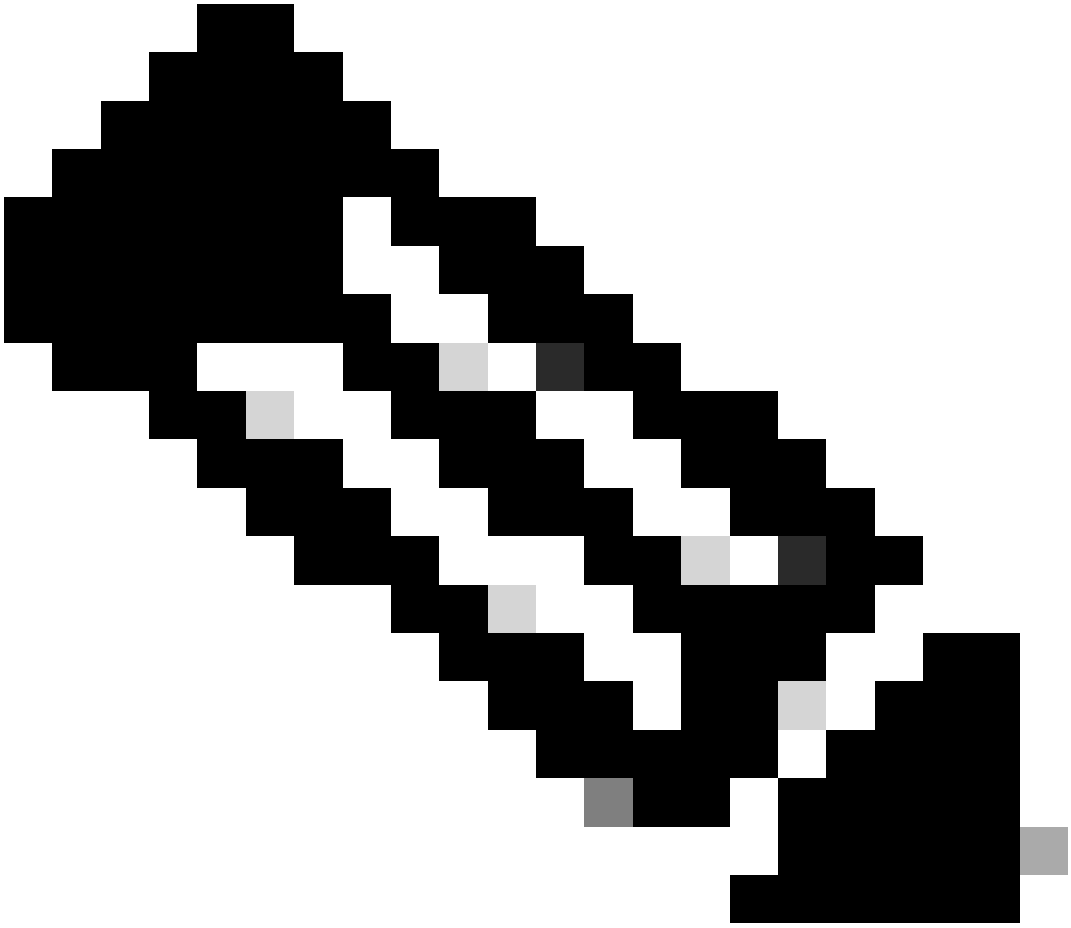
ملاحظة: تختلف مجموعات التشفير الموضحة هنا عن مجموعات التشفير في مجموعات برامج Client Hello الخاصة بالعميل من Client إلى SWA، حيث إن SWA، التي تم تكوينها لفك تشفير حركة المرور هذه، تستخدم شفرة خاصة بها.



تلميح: في تبادل مفتاح الخادم من SWA إلى خادم ويب، تظهر شهادة خادم ويب. وعم ذلك، إذا عثر وكيل تدفق البيانات على تكوين SWA، تظهر شهادته بدلا من شهادة خادم الويب.

هنا عينة من AccessLog:

```
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
```



ملاحظة: كما ترى في النشر الشفاف لحركة مرور HTTPS، يوجد خطان في سجلات الوصول، السطر الأول هو عندما يتم تشفير حركة مرور البيانات ويمكنك الاطلاع على TCP_CONNECT وعنوان IP لخادم الويب. إذا تم تمكين فك التشفير في SWA، فإن السطر الثاني يحتوي على GET وأدبأ عنوان URL بالكامل مع HTTPS، مما يعني أنه تم فك تشفير حركة المرور وأن SWA تعرف عنوان URL.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- تكوين معلمة الأداء في سجلات الوصول - Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).