Entender o fluxo de pacotes no Secure Web Appliance

Contents

Introdução Pré-requisitos **Requisitos** Componentes Utilizados Tipos diferentes de implantação de proxy Handshake TLS Código de Resposta HTTP 1xx : informativo 2xx: êxito 3xx:redirecionamento Códigos 4xx: erro do cliente 5xx: erro do servidor Implantação Explícita Tráfego HTTP em implantação explícita sem autenticação Cliente e SWA Servidor Web e SWA Tráfego Com Dados Armazenados Em Cache Tráfego HTTPs em implantação explícita sem autenticação Cliente e SWA Servidor Web e SWA Tráfego HTTPS de passagem Implantação transparente Tráfego HTTP na implantação transparente sem autenticação Cliente e SWA Servidor Web e SWA Tráfego Com Dados Armazenados Em Cache Tráfego HTTPs em implantação transparente sem autenticação Cliente e SWA Servidor Web e SWA Informações Relacionadas

Introdução

Este documento descreve o fluxo de rede em uma rede configurada de Proxy, focada especificamente no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos básicos de TCP/IP.
- Conhecimento básico da configuração do Proxy.
- Conhecimento básico do mecanismo de autenticação usado no ambiente com o Proxy.

As abreviações usadas nestes artigos são:

TCP: Transmission Control Protocol (Protocolo de controle de transmissão)

- UDP: Protocolo de datagrama de usuário
- IP: Protocolo de Internet
- GRE: Encapsulamento de roteamento genérico
- HTTP: Protocolo HTTP.
- HTTPS: protocolo de transferência de hipertexto seguro.
- URL: Uniform Resource Locator
- TLS: Segurança da camada de transporte

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Tipos diferentes de implantação de proxy

Handshake TLS

Um handshake TLS em HTTPS ocorre quando um cliente e um servidor se comunicam pela Internet, fornecendo uma conexão segura. O processo mantém a privacidade e a integridade dos dados entre dois aplicativos em comunicação. Ele opera através de uma série de etapas em que o cliente e o servidor concordam com os padrões e códigos de criptografia para todas as transmissões subsequentes. O handshake tem como objetivo impedir qualquer acesso não autorizado ou manipulação por terceiros. Ele também autentica as identidades das partes que se comunicam para eliminar a representação. Esse processo é crucial no HTTPS, pois garante que os dados permaneçam seguros durante o trânsito. Estas são as etapas de um handshake TLS:

- 1. Hello do cliente: o cliente inicia o processo de handshake com uma mensagem hello. Essa mensagem contém a versão TLS do cliente, conjuntos de cifras suportados e uma string de bytes aleatórios conhecida como "aleatório do cliente".
- 2. Alô do servidor: o servidor responde com uma mensagem de saudação. Essa mensagem inclui a versão TLS escolhida pelo servidor, o conjunto de cifras selecionado, uma sequência de bytes aleatória conhecida como "servidor aleatório" e o certificado digital do servidor. Se necessário, o servidor também solicita o certificado digital do cliente para autenticação mútua.
- 3. O cliente verifica o certificado do servidor: o cliente verifica o certificado digital do servidor com a autoridade de certificação que o emitiu. Isso garante ao cliente que está se comunicando com o servidor legítimo.
- 4. Segredo Pré-mestre: O cliente envia uma string de bytes aleatória, conhecida como "segredo pré-mestre", que contribui para a criação das chaves de sessão. O cliente criptografa esse segredo pré-mestre com a chave pública do servidor, de modo que somente o servidor pode descriptografá-lo com sua chave privada.
- Master Secret: o cliente e o servidor usam o segredo pré-mestre e as strings de byte aleatórias das mensagens de saudação para calcular independentemente o mesmo "segredo mestre". Esse segredo compartilhado é a base para a geração das chaves de sessão.
- 6. Cliente finalizado: O cliente envia uma mensagem "finalizado", criptografada com a chave de sessão, para sinalizar a conclusão da parte do cliente do handshake.
- 7. Servidor concluído: o servidor envia uma mensagem "Concluído", também criptografada com a chave de sessão, para sinalizar a conclusão da parte do handshake do servidor.

Código de Resposta HTTP

1xx : informativo

Code	Detalhes
100 Continuar	Geralmente visto em relação ao protocolo ICAP. Esta é uma resposta informativa que permite que o cliente saiba que pode continuar a enviar dados. Em relação aos serviços ICAP (como varredura de vírus), o servidor pode querer ver somente a primeira quantidade x de bytes. Quando ele termina de examinar o primeiro conjunto de bytes e não detectou um vírus, ele envia uma mensagem 100 Continue (Continuar) para informar ao cliente que ele deve enviar o restante do objeto.

2xx: Êxito

Code	Detalhes
200 OK	O código de resposta mais comum. Isso significa que a solicitação foi bem-sucedida sem problemas.

3xx: Redirecionamento

Code	Detalhes
301 Redirecionamento Permanente	Este é um redirecionamento Permanente, você pode ver este código quando estiver redirecionando para o subdomínio www.
302 Redirecionamento Temporário	Este é um redirecionamento temporário. O cliente é instruído a fazer uma nova solicitação para o objeto especificado no cabeçalho Location:.
304 Não Modificado	Isto é em resposta a um GIMS (GET If-modified-since). Este é literalmente um HTTP GET padrão que inclui o cabeçalho If- modified-since: <date>. Esse cabeçalho informa ao servidor que o cliente tem uma cópia do objeto solicitado em seu cache local e que a data em que o objeto foi buscado está incluída. Se o objeto tiver sido modificado desde essa data, o servidor responderá com 200 OK e uma cópia nova do objeto. Se o objeto não tiver sido alterado desde a data de busca, o servidor retornará uma resposta 304 Não modificado.</date>
Redirecionamento de Autenticação 307	Isso é visto principalmente, na Implantação de Proxy transparente, quando o servidor Proxy é configurado para autenticar a solicitação e redireciona a solicitação para outra URL para autenticar o usuário,

Códigos 4xx: erro do cliente

Code	Detalhes
400 Solicitação Incorreta	Isso sugere um problema com a solicitação HTTP, pois ela não está em conformidade com a sintaxe apropriada. Possíveis razões podem incluir vários cabeçalhos em uma única linha, espaços dentro de um cabeçalho ou a falta de HTTP/1.1 no URI, entre outros. Para obter a sintaxe correta, consulte RFC 2616.

401 Não autorizado Autenticação de Servidor Web Necessária	O acesso ao objeto solicitado requer autenticação. O código 401 é utilizado para autenticação com um servidor Web de destino. Quando o SWA opera em modo transparente e a autenticação é habilitada no proxy, ele retorna um 401 para o cliente, já que o dispositivo se apresenta como se fosse o OCS (servidor de conteúdo de origem). Os métodos de autenticação que podem ser usados estão detalhados em um cabeçalho de resposta HTTP 'www-authenticate:'. Isso informa ao cliente se o servidor está solicitando NTLM, básico ou outras formas de autenticação.
403 Negado	O cliente não pode acessar o objeto solicitado. Várias razões podem levar um servidor a negar acesso a objetos. O servidor normalmente fornece uma descrição da causa dentro dos dados HTTP ou da resposta HTML.
404 Não encontrado	O objeto solicitado não existe no servidor.
407 Autenticação de proxy necessária	Isso é o mesmo que um 401, exceto que ele é especificamente para autenticação em um proxy e não no OCS. Isso é enviado somente se a solicitação tiver sido enviada explicitamente ao proxy. Um 407 não pode ser enviado a um cliente enquanto o SWA estiver configurado como proxy transparente, pois o cliente não sabe que o proxy existe. Se este for o caso, o cliente provavelmente FIN ou RST o soquete TCP.

5xx: erro do servidor

Code	Detalhes					
501 Erro interno do servidor	Falha genérica do servidor Web.					
502 Gateway com problema	Ocorre quando um servidor que atua como gateway ou proxy recebe uma resposta inválida de um servidor de entrada. Ele sinaliza que o gateway recebeu uma resposta inadequada do servidor upstream ou de origem.					
Serviço 503 Indisponível	Significa que o servidor não pode lidar com a solicitação devido a uma sobrecarga temporária ou manutenção agendada. Isso implica que o servidor está temporariamente fora de serviço, mas					

	pode estar disponível novamente após algum tempo.
504 Tempo limite do gateway	Indica que um cliente ou proxy não recebeu uma resposta em tempo hábil do servidor Web ao tentar acessar para carregar a página da Web ou atender outra solicitação do navegador. Isso geralmente implica que o servidor upstream está inoperante.

Implantação Explícita

Aqui

Tráfego HTTP em implantação explícita sem autenticação

Cliente e SWA

O tráfego de rede transpira entre o endereço IP do cliente e o endereço IP da interface proxy SWA (geralmente é a interface P1, mas pode ser a interface P2 ou de gerenciamento, depende da configuração do proxy).

O tráfego do cliente é destinado à porta TCP 80 ou 3128 para o SWA (as portas proxy do SWA padrão são TCP 80 e 3128, neste exemplo, usamos a porta 3128)

- Handshake TCP.
- HTTP Get do cliente (IP de destino = SWA IP , Porta de destino = 3128)
- Resposta HTTP do proxy (IP de origem = SWA)
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream Info
125	44 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
125	45 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=3227000
125	67 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
125	58 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
125	69 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
128	51 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
128	52 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)
129	92 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
129	93 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
129	94 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=322700108
129	95 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
129	96 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
129	97 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

Cliente de imagem para SWA, modo HTTP explícito

Servidor Web e SWA

O tráfego de rede ocorre entre o endereço IP do Proxy e o endereço IP do servidor Web.

O tráfego do SWA é destinado à porta TCP 80 e originado com uma porta aleatória (não a porta de proxy)

- Handshake TCP.
- HTTP Get do Proxy (IP de Destino = Servidor Web , Porta de Destino = 80)
- Resposta HTTP do servidor Web (IP de origem = servidor proxy)
- Transferência de dados

• Encerramento da conexão TCP (Handshake de 4 Vias)

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt s	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 set
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=3198021942 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 2	00 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

Imagem - HTTP-SWA para servidor Web-Explicit-no cache

Aqui está um exemplo de HTTP Get do cliente

>	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
\sim	Hypertext Transfer Protocol
	<pre>GET http://example.com/ HTTP/1.1\r\n</pre>
	> [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
	<pre>[Full request URI: http://example.com/]</pre>
	[HTTP request 1/1]
	[Response in frame: 12852]

Imagem - Cliente para SWA HTTP GET - Explícito

No Time

Isso representa todo o fluxo de tráfego do cliente para o SWA, depois para o servidor Web e, finalmente, de volta para o cliente.

	¥0.	THING	Source	SIC MAG	Deschauon	OSC MAG	PIOLOCOL	cenge sure	earn mito
	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	WMware_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	Whware_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	WMware_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	Whware_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	Whware_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	Whware_8d:f3:64	TCP	1414	3 80 → 23146 [ACK] Seq=1 Ack=177 Win=67072 Len=1348 TSval=2163592177 TSecr=3190021832 [TCP sec
	12835	2024-01-25 09:35:26.281789	10.48.48.185	WMware_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	WMware_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
1	12851	2024-01-25 09:35:26.286288	10.48.48.185	WMware_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 =
İ	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	Whware_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	Whware_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	WMware_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
I	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
i	12997	2024-01-25 09:35:26.412438	10.61.70.23	Cisco 9d:b9:ff	10.48.48.185	Whyare 8d:f3:64	TCP	66	2 65238 → 3128 [ACK] Seg=124 Ack=1723 Win=131072 Len=0 TSval=1762372212 TSecr=3227001147

Bertrad Land





Observação: cada fluxo de tráfego é diferenciado por uma cor diferente; o fluxo do cliente para o SWA é de uma cor e o fluxo do SWA para o servidor Web é de outra.

Time	10.61	70.23	93.184	.216.34	Comment
		10.48	48.185		
2024-01-25 09:35:25.989719	65238	65238 -> 3128 [SYN] Seq=0 Win=65535 Len=	3128		TCP: 65238 + 3128 [SYN] Seq=0 Win=65535
2024-01-25 09:35:25.989748	65238	3128 → 65238 [SYN, ACK] Seq=0 Ack=1 Win=	3128		TCP: 3128 → 65238 [SYN, ACK] Seq=0 Ack=1
2024-01-25 09:35:26.046546	65238	65238 → 3128 [ACK] Seg=1 Ack=1 Win=13228.	3128		TCP: 65238 → 3128 [ACK] Seq=1 Ack=1 Win=1_
2024-01-25 09:35:26.046877	65238	GET http://example.com/ HTTP/1.1	3128		HTTP: GET http://example.com/ HTTP/1.1
2024-01-25 09:35:26.046945	65238	3128 → 65238 [ACK] Seq=1 Ack=123 Win=654	3128		TCP: 3128 → 65238 [ACK] Seq=1 Ack=123 Win_
2024-01-25 09:35:26.053195		23146	23146 → 80 [SYN] Seq=0 Win=12288 Len=0 M	80	TCP: 23146 → 80 [SYN] Seq=0 Win=12288 Le
2024-01-25 09:35:26.168035		23146	80 → 23146 [SYN, ACK] Seq=0 Ack=1 Win=65	80	TCP: 80 + 23146 [SYN, ACK] Seq=0 Ack=1 Wi
2024-01-25 09:35:26.168077		23146	23146 → 80 [ACK] Seq=1 Ack=1 Win=13568 Le	- 80	TCP: 23146 → 80 [ACK] Seq=1 Ack=1 Win=135
2024-01-25 09:35:26.168172		23146	GET / HTTP/1.1	80	HTTP: GET / HTTP/1.1
2024-01-25 09:35:26.280446		23146	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072	80	TCP: 80 → 23146 [ACK] Seq=1 Ack=177 Win=6
2024-01-25 09:35:26.281757		23146	80 → 23146 [ACK] Seq=1 Ack=177 Win=67072	80	TCP: 80 → 23146 [ACK] Seq=1 Ack=177 Win=6
2024-01-25 09:35:26.281789		23146	23146 → 80 [ACK] Seq=177 Ack=1349 Win=12.	- 80	TCP: 23146 → 80 [ACK] Seq=177 Ack=1349 Wi
2024-01-25 09:35:26.281793		23146	HTTP/1.1 200 OK (text/html)	- 80	HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:35:26.281801		23146	23146 → 80 [ACK] Seq=177 Ack=1608 Win=11.	80	TCP: 23146 → 80 [ACK] Seq=177 Ack=1608 Wi
2024-01-25 09:35:26.286288	65238	3128 → 65238 [ACK] Seq=1 Ack=123 Win=654	3128		TCP: 3128 → 65238 [ACK] Seq=1 Ack=123 Win_
2024-01-25 09:35:26.286297	65238	HTTP/1.1 200 OK (text/html)	3128		HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:35:26.347713	65238	65238 → 3128 [ACK] Seq=123 Ack=1189 Win=.	3128		TCP: 65238 → 3128 [ACK] Seq=123 Ack=1189
2024-01-25 09:35:26.347815	65238	65238 -> 3128 [ACK] Seq=123 Ack=1722 Win=.	3128		TCP: 65238 → 3128 [ACK] Seq=123 Ack=1722
2024-01-25 09:35:26.353174	65238	65238 + 3128 [FIN, ACK] Seq=123 Ack=1722	3128		TCP: 65238 → 3128 [FIN, ACK] Seq=123 Ack=1
2024-01-25 09:35:26.353217	65238	3128 + 65238 [ACK] Seq=1722 Ack=124 Win=	3128		TCP: 3128 → 65238 [ACK] Seq=1722 Ack=124
2024-01-25 09:35:26.353397	65238	3128 -> 65238 [FIN, ACK] Seq=1722 Ack=124	3128		TCP: 3128 → 65238 [FIN, ACK] Seq=1722 Ack
2024-01-25 09:35:26.412438	65238	65238 + 3128 [ACK] Seq=124 Ack=1723 Win=.	3128		TCP: 65238 → 3128 [ACK] Seq=124 Ack=1723

Imagem - Fluxo de Tráfego HTTP Explícito - sem cache

Aqui está um exemplo de registros de acesso:

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

Tráfego Com Dados Armazenados Em Cache

Isso representa todo o fluxo de tráfego do cliente para o SWA, quando os dados estão no cache SWA.

No		Time	Source	src MAC	Destination	dst MAC	Protocol Leng	t stream	n 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	3 2	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	1 3	2 3128 - 55709 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=64 SACK_PERM TSval=36879239:
	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	5 2	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	3 3	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] Seg=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	1 3	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	1 3	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	5 3	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	2 3	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	5 3	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	5 3	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	5 3	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	5	3 16088 - 80 [FIN, ACK] Seg=227 Ack=300 Win=13568 Len=0 TSval=3191297172 TSecr=811197793
Т	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	1 3	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) 3	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	5 3	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	5 3	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	i 3	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	5 3	3 16088 - 80 [ACK] Seq=228 Ack=301 Win=13568 Len=0 TSval=3191297302 TSecr=811197917
L	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

Imagem - dados em cache explícitos do HTTP



Observação: Como você pode ver, o Servidor Web retorna a resposta HTTP 304: Cache não Modificado. (neste exemplo, o número de pacote 1947)

Time	10.61	.70.23 10.48.	48.185	.216.34	Comment
2024-01-25 09:56:41.209030	55709	55709 → 3128 [SYN] Seq=0 Win=65535 Len=.	3128		TCP: 55709 → 3128 [SYN] Seq=0 Win=65535
2024-01-25 09:56:41.209111	55709	3128 + 55709 [SYN, ACK] Seq=0 Ack=1 Win=6	3128		TCP: 3128 → 55709 [SYN, ACK] Seq=0 Ack=1
2024-01-25 09:56:41.265937	55709	55709 → 3128 [ACK] Seq=1 Ack=1 Win=13228	3128		TCP: 55709 → 3128 [ACK] Seq=1 Ack=1 Win=1
2024-01-25 09:56:41.266065	55709	GET http://example.com/ HTTP/1.1	3128		HTTP: GET http://example.com/ HTTP/1.1
2024-01-25 09:56:41.266114	55709	3128 -> 55709 [ACK] Seq=1 Ack=123 Win=658	3128		TCP: 3128 → 55709 [ACK] Seg=1 Ack=123 Win
2024-01-25 09:56:41.269061		16088	16088 → 80 [SYN] Seq=0 Win=12288 Len=0 M	80	TCP: 16088 → 80 [SYN] Seq=0 Win=12288 Le
2024-01-25 09:56:41.385086		16088	80 → 16088 [SYN, ACK] Seq=0 Ack=1 Win=65	80	TCP: 80 → 16088 [SYN, ACK] Seq=0 Ack=1 Wi
2024-01-25 09:56:41.385174		16088	16088 + 80 [ACK] Seg=1 Ack=1 Win=13568 L.	- 80	TCP: 16088 → 80 [ACK] Seq=1 Ack=1 Win=135
2024-01-25 09:56:41.385270		16088	GET / HTTP/1.1	- 80	HTTP: GET / HTTP/1.1
2024-01-25 09:56:41.509528		16088	80 → 16088 [ACK] Seq=1 Ack=227 Win=67072_	80	TCP: 80 → 16088 [ACK] Seq=1 Ack=227 Win=
2024-01-25 09:56:41.510195		16088	HTTP/1.1 304 Not Modified	- 80	HTTP: HTTP/1.1 304 Not Modified
2024-01-25 09:56:41.510259		16088	16088 → 80 [ACK] Seq=227 Ack=300 Win=132	80	TCP: 16088 → 80 [ACK] Seq=227 Ack=300 Wi
2024-01-25 09:56:41.510429		16088	16088 -> 80 [FIN, ACK] Seq=227 Ack=300 Win	80	TCP: 16088 → 80 [FIN, ACK] Seq=227 Ack=30
2024-01-25 09:56:41.513099	55709	3128 + 55709 [ACK] Seq=1 Ack=123 Win=658	3128		TCP: 3128 → 55709 [ACK] Seg=1 Ack=123 Win
2024-01-25 09:56:41.513111	55709	HTTP/1.1 200 OK (text/html)	3128		HTTP: HTTP/1.1 200 OK (text/html)
2024-01-25 09:56:41.585507	55709	55709 → 3128 [ACK] Seq=123 Ack=1189 Win=	3128		TCP: 55709 → 3128 [ACK] Seq=123 Ack=1189
2024-01-25 09:56:41.600259	55709	55709 → 3128 [ACK] Seq=123 Ack=1722 Win=.	3128		TCP: 55709 → 3128 [ACK] Seg=123 Ack=1722
2024-01-25 09:56:41.604113	55709	55709 -> 3128 [FIN, ACK] Seq=123 Ack=1722	3128		TCP: 55709 → 3128 [FIN, ACK] Seq=123 Ack=1
2024-01-25 09:56:41.604191	55709	3128 -> 55709 [ACK] Seq=1722 Ack=124 Win=	3128		TCP: 3128 → 55709 [ACK] Seq=1722 Ack=124
2024-01-25 09:56:41.604293	55709	3128 → 55709 [FIN, ACK] Seq=1722 Ack=124	3128		TCP: 3128 → 55709 [FIN, ACK] Seq=1722 Ack=
2024-01-25 09:56:41.636731		16088	80 → 16088 [FIN, ACK] Seq=300 Ack=228 Win	80	TCP: 80 → 16088 [FIN, ACK] Seq=300 Ack=22
2024-01-25 09:56:41.636832		16088	16088 → 80 [ACK] Seq=228 Ack=301 Win=135	80	TCP: 16088 → 80 [ACK] Seq=228 Ack=301 Wi
2024-01-25 09:56:41.662464	55709	55709 → 3128 [ACK] Seq=124 Ack=1723 Win=.	3128		TCP: 55709 → 3128 [ACK] Seq=124 Ack=1723

Imagem - Fluxo HTTP Explícito com cache

Aqui está um exemplo da Resposta 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 Hypertext Transfer Protocol HTTP/1.1 304 Not Modified\r\n // [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n] [HTTP/1.1 304 Not Modified\r\n] [Severity level: Chat] [Group: Sequence] Response Version: HTTP/1.1 Status Code: 304 [Status Code Description: Not Modified] Response Phrase: Not Modified Accept-Ranges: bytes\r\n Age: 519756\r\n Cache-Control: max-age=604800\r\n Date: Thu, 25 Jan 2024 08:57:08 GMT\r\n Etag: "3147526947"\r\n Expires: Thu, 01 Feb 2024 08:57:08 GMT\r\n Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n Server: ECS (dce/2694)\r\n Vary: Accept-Encoding\r\n X-Cache: HIT\r\n \r\n [HTTP response 1/1] [Time since request: 0.124925000 seconds] [Request in frame: 1945] [Request URI: http://example.com/]

Imagem - Resposta HTTP 304 explícita

Aqui está um exemplo de registros de acesso:

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

Tráfego HTTPs em implantação explícita sem autenticação

Cliente e SWA

O tráfego de rede transpira entre o endereço IP do cliente e o endereço IP da interface proxy SWA (normalmente é a interface P1, mas pode ser a interface P2 ou de gerenciamento, depende da configuração do proxy).

O tráfego do cliente é destinado à porta TCP 80 ou 3128 para o SWA (as portas proxy do SWA padrão são TCP 80 e 3128, neste exemplo, usamos a porta 3128)

• Handshake TCP.

- HTTP CONNECT do cliente (IP de destino = SWA, Porta de destino = 3128)
- Resposta HTTP do proxy (IP de origem = SWA)
- Hello do cliente com SNI do URL (IP de origem = Cliente)
- Hello do servidor (IP de origem = SWA)
- Server Key Exchange (IP de origem = SWA)
- Intercâmbio de chave do cliente (IP de origem = Cliente)
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

N	a	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	m Info
5		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	2 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	.2 3128 → 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=44149543
П		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	2 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	2 CONNECT example.com:443 HTTP/1.1
		2 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	2 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	2 HTTP/1.1 200 Connection established
Т		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	.2 61484 → 3128 [ACK] Seq=212 Ack=40 Win=132224 Len=0 TSval=1676451630 TSecr=441495677
ł		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	2 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	2 3128 - 61484 [ACK] Seq=40 Ack=861 Win=64704 Len=0 TSval=441495747 TSecr=1676451630
	0	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	2 Server Hello
		0 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	2 Certificate
		1 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	2 Server Key Exchange, Server Hello Done
н	1	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	2 61484 → 3128 [ACK] Seq=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=441496237
1	8	5 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	2 61484 → 3128 [ACK] Seq=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=441496237
1		6 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	2 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Т	8	7 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	2 3128 → 61484 [ACK] Seq=2540 Ack=954 Win=64640 Len=0 TSval=441496317 TSecr=1676452193
		8 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	2 Change Cipher Spec, Encrypted Handshake Message
Т	1	9 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	2 61484 → 3128 [ACK] Seq=954 Ack=2591 Win=131008 Len=0 TSval=1676452265 TSecr=441496317
	1	0 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	2 Application Data
н)	1 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	.2 3128 → 61484 [ACK] Seq=2591 Ack=1450 Win=64192 Len=0 TSval=441496387 TSecr=1676452265
T	1	2 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	2 Application Data
1	3	33 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	.2 61484 → 3128 [ACK] Seq=1450 Ack=2637 Win=131008 Len=0 TSval=1676452764 TSecr=441496807
Т	1	4 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	2 Application Data, Application Data
	1	35 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	2 61484 → 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=441496887
н	1	36 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	2 Application Data
	3	37 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	.2 3128 → 61484 [ACK] Seq=3780 Ack=1881 Win=63808 Len=0 TSval=441496997 TSecr=1676452884
т	1	4 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	2 Application Data
1	1	5 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	2 61484 → 3128 [ACK] Seq=1881 Ack=3833 Win=131008 Len=0 TSval=1676453324 TSecr=441497377
1	1	6 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	2 Application Data, Application Data
1	1	7 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	2 61484 → 3128 [ACK] Seq=1881 Ack=4959 Win=129920 Len=0 TSval=1676453397 TSecr=441497447
L	1	0 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	.2 [TCP Keep-Alive] 61484 → 3128 [ACK] Seq=1880 Ack=4959 Win=131072 Len=0

Imagem - Cliente HTTPS para SWA-Explicit - Sem cache

Aqui estão os detalhes do cliente Hello do cliente para o SWA, como você pode ver na indicação de nome de servidor (SNI) o URL do servidor web pode ser visto, que neste exemplo, é <u>www.example.com</u> e o cliente anunciou 17 conjuntos de cifras:

>	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							
\sim	Hypertext Transfer Protocol							
	[Proxy-Connect-Hostname: example.com]							
	[Proxy-Connect-Port: 443]							
\vee	Transport Layer Security							
	V TLSV1.2 Record Layer: Handshake Protocol: Client Hello							
	Content Type: Handshake (22)							
	Version: TLS 1.0 (0x0301)							
	Length: 644							
	Handshake Protocol: Clent Hello							
	Handshake Type: Client Hello (1)							
	Version: ILS 1.2 (0x00/03)							
	Rdituolii: 61203305771520030204204080489296300230540804350005140061616305990760 Secretion: TD Learneth, 22							
3655101 10 LENGUI 32 Sacsion The adifadfa756373ca70f5h65c0720h805d864f8f3Qac783h2fahQa4Qcad7da6h								
	Cinher Suites Length 34							
	> Cipher Suites (17 suites)							
	Compression Methods Length: 1							
	> Compression Methods (1 method)							
	Extensions Length: 533							
	Extension: server_name (len=16) name=example.com							
	Type: server_name (0)							
	Length: 16							
	Server Name Indication extension							
	Server Name list length: 14							
	Server Name Type: host_name (0)							
	Server Name length: 11							
	Server Name: example.com							
	> Extension: extended_master_secret (len=0)							
	<pre>> Extension: renegotiation_info (len=1)</pre>							
	<pre>> Extension: supported_groups (len=14)</pre>							
	> Extension: ec_point_formats (len=2)							
	<pre>> Extension: application_layer_protocol_negotiation (len=14)</pre>							
	> Extension: status_request (ten=5)							
	Extension: delegated_credentials (ten=10)							
	> Extension: supported versions ($10 = 5$) T[S 1.2]							
	> Extension: signature algorithms (len=24)							
	> Extension: record size limit (len=2)							
	> Extension: encrypted client hello (len=281)							
	[]A4: t13d1713b2 5b57614c22b0 748f4c70de1c1							

Imagem - hello do cliente HTTPS - Explícito - Cliente para SWA



Dica: você pode usar esse filtro no Wireshark para procurar URL/SNI : tls.handshake.extensions_server_name == "www.example.com"

Aqui está um exemplo de certificado que SWA enviou ao cliente

> Frame 50: 1254 bytes on wire (10032 bits), 1254 bytes captured (10032 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: 10.61.70.23
> Transmission Control Protocol, Src Port: 3128, Dst Port: 61484, Seq: 1228, Ack: 861, Len: 1188
[2 Reassembled TCP Segments (2105 bytes): #49(1107), #50(998)]
V Hypertext Transfer Protocol
[Proxy-Connect-Hostname: example.com]
[Proxy-Connect-Port: 443]
V Transport Laver Security
v Tisvi 2 Decord Javer, Handshake Protocol: Certificate
Contest Tuesday Ladebase (3)
Concent Type: nationale (22)
version: 1.5 1.2 (0x0303)
Length: 2100
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 2096
Certificates Length: 2093
V Certificates (2093 bytes)
Certificate Length: 1105
Certificate [truncated]: 3082044d30820335a00302010202140279103122f2aad73d32683b716d2a7d4ead7d47300d06092a864886f70d01010b05003047310b3009060355040613025553310e300c060355040a1
v signedCertificate
version: v3 (2)
containing to (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
ciantura (hajSGUibbRAEncrutia)
signature (sheadanace)
> 15500 . This equation (if a transmission of the company of th
 Forsequence: 4 items to accounting mental sector of gargest on gargest on the account of gargest on the account of the account o
 www.sequence item: 1 item (10-at-countrywame=us)
v ketativeustinguismedname item (id-at-countryname=us)
Upject Id: 2.5.4.6 (Id-at-countryName)
CountryName: US
RDNSequence item: 1 item (id-at-organizationName=Cisco)
RelativeDistinguishedName item (id-at-organizationName=Cisco)
Object Id: 2.5.4.10 (id-at-organizationName)
DirectoryString: printableString (1)
printableString: Cisco
V RDNSequence item: 1 item (id-at-organizationalUnitName=IT)
RelativeDistinguishedName item (id-at-organizationalUnitName=IT)
Object Id: 2.5.4.11 (id-at-organizationalUnitName)
 DirectoryString: printableString (1)
netratal Section IT
DNMSonare itam (id-st-compoName=CTCC) IAB Eval(cit)
 Replete tem, i tem (destruction by an englished to be price) Replete tem in the destruction of the second sec
Object 14: 25: 4 2 (id at companyment)
UJECT 10: 2-5-4-5 (10-8C-COMPONNAME)
<pre>vurectorystring: printablestring (1)</pre>
printablestring: CISCU LAB Explicit

Imagem - Certificado HTTPS - Explícito - SWA para cliente

Servidor Web e SWA

O tráfego de rede ocorre entre o endereço IP do Proxy e o endereço IP do servidor Web.

O tráfego do SWA é destinado à porta TCP 443 (não à porta proxy)

- Handshake TCP.
- Hello do cliente (IP de destino = servidor Web, porta de destino = 443)
- Servidor Hello (IP de origem = servidor Web)
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

No	l,	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt	stream	Info
-	2	3 2024-01-25 12:31:37.383901	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	74	13	24953 → 443 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=2549353418 TSecr=0
	2	4 2024-01-25 12:31:38.006918	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	74	13	443 → 24953 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=1727280976 TSec
Т	2	5 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
	3	0 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)
	3	1 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	3 443 → 24953 [ACK] Seq=1 Ack=194 Win=67072 Len=0 TSval=1727281239 TSecr=2549353688
	3	2 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
	3	3 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
	3	4 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	8 443 → 24953 [PSH, ACK] Seq=1369 Ack=194 Win=67072 Len=1368 TSval=1727281240 TSecr=254935368
	3	5 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
	3	6 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
	3	87 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
	3	8 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
4	3	9 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
	4	0 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
н	6	4 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
	7	3 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	3 443 → 24953 [ACK] Seq=3618 Ack=365 Win=67072 Len=0 TSval=1727281896 TSecr=2549354298
	7	4 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
	7	8 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	3 443 → 24953 [ACK] Seq=3618 Ack=939 Win=68096 Len=0 TSval=1727282019 TSecr=2549354468
	7	9 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
	8	0 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
	8	8 2024-01-25 12:31:39.(352452851	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	122	13	Application Data
	8	9 2024-01-25 12:31:39.(427217571	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	8 443 → 24953 [ACK] Seq=4698 Ack=995 Win=68096 Len=0 TSval=1727282552 TSecr=2549354948
	9	0 2024-01-25 12:31:39.(347738670	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	564	13	Application Data, Application Data
	9	1 2024-01-25 12:31:39.(186179736	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TCP	66	13	8 443 → 24953 [ACK] Seq=4698 Ack=1493 Win=69120 Len=0 TSval=1727282678 TSecr=2549355128
	9	2 2024-01-25 12:31:39.(202826742	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:f4	TLSv1.2	1136	13	Application Data, Application Data
L	9	3 2024-01-25 12:31:39.048886	10.48.48.165	VMware_8d:9a:f4	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	24953 → 443 [ACK] Seq=1493 Ack=5768 Win=11264 Len=0 TSval=2549355248 TSecr=1727282680

Imagem - HTTPS - Explícito - SWA para servidor Web

Aqui estão os detalhes do cliente Hello do SWA para o servidor web, como você pode ver SWA anunciado 12 Cipher Suites:

Frame 30: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits) Ethernet II, Src: WMware_8d:9a:f4 (00:59:56:8d:9a:f4), Dst: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff) Internet Protocol Version 4, Src: 10.48.48.165, Dst: 93.184.216.34 Transmission Control Protocol, Src Port: 24953, Dst Port: 443, Seq: 1, Ack: 1, Len: 193 Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 188
Handshake Type: 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 (1 method) Extensions Length: 19
<pre>v Extension: server_name (len=16) name=example.com Type: server_name (0) Length: 16</pre>
 Server Name Indication extension Server Name Type: host name (0)
Server Name length: 11
Server Name: example.com
> Extension: supported_groups (len=12)
> Extension: application_layer_protocol_negotiation (len=11)
> Extension: encrypt_then_mac (len=0)
Extension: extende_master_secret (Len=0) Extension: cionature alorithms (Len=48)
[JA4: 112d1207h1_ea1297b1df3f_ed727256b201]
[JA4_r: tl2d1207h1_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] [IA3: A05-244087464000b1403406c56c464]

Imagem - Hello do cliente HTTPS - SWA para servidor Web - Sem cache



Observação: os conjuntos de cifras observados aqui diferem dos conjuntos de cifras no Hello do cliente para SWA, pois o SWA, configurado para descriptografar esse tráfego, utiliza suas próprias cifras.



Dica: na troca de chaves do servidor de SWA para o servidor Web, o certificado do servidor Web é exibido. No entanto, se um Proxy de Upstream encontrar configuração para o seu SWA, o certificado será exibido em vez do certificado do Servidor Web.

Aqui está um exemplo de HTTP CONNECT do cliente

```
Frame 21: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits)
  Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:9a:f4 (00:50:56:8d:9a:f4)
> Internet Protocol Version 4, Src: 10.61.70.23, Dst: 10.48.48.165
 Transmission Control Protocol, Src Port: 61484, Dst Port: 3128, Seq: 1, Ack: 1, Len: 211
 Hypertext Transfer Protocol
    CONNECT example.com:443 HTTP/1.1\r\n
     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]
```

Imagem - Conexão HTTP do Cliente

Isso representa todo o fluxo de tráfego do cliente para o SWA, depois para o servidor Web e, finalmente, de volta para o cliente.

N).	Time	Source	SIC MAC	Destination	dst MAC	Protocol	Lengt stre	sam	1 Into
Г	18	8 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	2 61484 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=64 TSval=1676451324 TSecr=0 SAC
	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	2 3128 → 61484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=4
	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	2 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	2 CONNECT example.com:443 HTTP/1.1
T	22	2 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	2 3128 - 61484 [ACK] Seg=1 Ack=212 Win=65344 Len=0 TSval=441495507 TSecr=1676451392
	23	3 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	3 24953 - 443 [SYN] Seg=0 Win=12288 Len=0 MSS=1460 WS=64 SACK PERM TSval=2549353418 TS
T	24	2024-01-25 12:31:38.006918	93, 184, 216, 34	Cisco 9d:b9:ff	10.48.48.165	Whware 8d:9a:f4	TCP	74	13	3 443 → 24953 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK PERM TSval=17272809
ł	25	5 2024-01-25 12:31:38,893381	10,48,48,165	Whware 8d:9a:f4	93,184,216,34	Cisco 9d:b9:ff	TCP	66	13	3 24953 → 443 [ACK] Seg=1 Ack=1 Win=12480 Len=0 TSval=2549353558 TSecr=1727280976
ł	26	5 2024-01-25 12:31:38.731815	10.48.48.165	Where 8d:9a:f4	10.61.70.23	Cisco 9d:b9:ff	HTTP	105	12	HTTP/1.1 200 Connection established
÷	27	7 2024-01-25 12:31:38 (308877561	10 61 70 23	Cisco 9d+h9+ff	10 48 48 165	Whyare Sd. Ga.fd	TCP	66	12	51484 - 3128 [ACK] Sen-212 Ark-48 Win-132224 [en-8 TSual-1676451638 TSerr-441405677
	25	2024-01-25 12:31:30 (3030//301	10 61 70 22	Circo OdibBiff	10 40 40 165	Marc_00.90.14	TI Su1 2	715	12	Client Hello (SNT-evane con)
4	20	2024-01-25 12:31:30. (32234/100-	10 40 40 165	Where Rd:0a:fd	10.40.40.105	Circo Od:b0:ff	TCP	66	12	2 2120 - 61404 [Art] Carada Ark-061 Win-64704 [an-0 TCus]-441405747 TCara-1676451630
÷	43	2024-01-25 12.51.50.(1020/24/5-	10.40.40.105	Vriware_ou.sa.r4	02 104 216 24	Cisco_90.09.11	TLEU1 2	250	12	2 Sliget Helle (SNT-severale ack-bol Wined4/64 Lene 13V8L-441435/4/ 13EC1=10/0451030
	30	2024-01-25 12:31:38.350314	10.48.48.105	vriware_ou:9a:14	93.184.210.34	C15C0_90:09:11	TLSV1.2	239	13	
1	31	1 2024-01-25 12:31:38.(140535400	93.184.216.34	C15C0_90:09:11	10.48.48.165	VMware_80:9a:14	TLC	00	13	5 443 - 24953 (ACK) Seq=1 ACK=194 Win=6/0/2 Len=0 15V8(=1/2/281239 15ecr=2549353688
1	34	2 2024-01-25 12:31:38.(247031593_	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_80:9a:14	TLSV1.Z	1434	13	3 Server Hello
1	33	3 2024-01-25 12:31:38.(273349971_	10.48.48.165	VMware_8d:9a:14	93.184.216.34	Cisco_9d:b9:ff	TCP	66	13	3 24953 → 443 [ACK] Seq=194 ACK=1369 Win=11136 Len=0 TSval=2549353808 TSecr=1727281240
	34	4 2024-01-25 12:31:38.(141489009	93.184.216.34	Cisco_9d:b9:ff	10.48.48.165	VMware_8d:9a:14	TCP	1434	13	3 443 → 24953 [PSH, ACK] Seq=1369 Ack=194 Win=67072 Len=1368 TSval=1727281240 TSecr=25
	35	5 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	3 24953 → 443 [ACK] Seq=194 Ack=2737 Win=11072 Len=0 TSval=2549353818 TSecr=1727281240
	36	5 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	3 Certificate, Server Key Exchange, Server Hello Done
	37	7 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	3 24953 → 443 [ACK] Seq=194 Ack=3567 Win=10304 Len=0 TSval=2549353818 TSecr=1727281240
	38	8 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	3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	35	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	3 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	3 24953 → 443 [ACK] Seq=320 Ack=3618 Win=12480 Len=0 TSval=2549353988 TSecr=1727281420
1	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	2 Server Hello
T	56	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	2 Certificate
T	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	2 Server Key Exchange, Server Hello Done
T	54	4 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	2 61484 → 3128 [ACK] Seg=861 Ack=1228 Win=131008 Len=0 TSval=1676452189 TSecr=44149623
T	55	2024-01-25 12:31:38. (344661913	10.61.70.23	Cisco 9d:b9:ff	10.48.48.165	Whyare 8d:9a:f4	TCP	66	12	2 61484 → 3128 [ACK] Seg=861 Ack=2540 Win=129728 Len=0 TSval=1676452189 TSecr=44149623
ł	56	5 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	2 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
÷	57	7 2024-01-25 12:31:38. (422856787	10.48.48.165	Whare 8d:9a:f4	10.61.70.23	Cisco 9d:h9:ff	TCP	66	12	2 3128 - 61484 [ACK] Sec=2540 Ack=954 Win=64640 [en=0 TSva]=441496317 TSecr=1676452193
÷	55	2024-01-25 12:31:38 (244514147	10 48 48 165	Whare Sd:0a:f4	10 61 70 23	Cisco 0d:h0:ff	TI Su1 2	117	12	Change Cipher Sher Encrunted Handshake Message
ł	50	2024-01-25 12:31:30.(244514147	10.40.40.105	Cisco OdihQiff	10.01.70.25	Where Sdigarf4	TCP	66	12	2 Glady _ 2120 [Ark] Constant Arka260 Wine Hessage
÷	51	2024-01-25 12:31:30.(520702550	10.61 70.23	Cisco Odiboiff	10.40.40.105	Vitware_00.90.14	TLE-1 2	563	12	Analisation Date
	00	2024-01-25 12:51:50.(151240214_	10.01./0.25	C15C0_90:09:11	10.40.40.105	Vriware_outsatt4	10391.2	502	12	
÷	0.	1 2024-01-25 12:31:38.(25/435452	10.48.48.105	vmware_60:98:14	10.01.70.23	C15C0_90:09:11	TUP	00	12	5 3159 → 01404 [W/V] 26d=5231 WCK=1420 MIU=04135 F6U=0 12A9f=441430391 126CL=101043550
1	64	2024-01-25 12:31:38.(296/60/48_	10.48.48.165	VMware_80:9a:14	93.184.216.34	Cisco_9d:b9:TT	11591.2	111	13	s Application Data
1	/:	3 2024-01-25 12:31:38.(411911657	93.184.216.34	C15C0_90:09:11	10.48.48.165	VMware_80:9a:14	TCP	66	13	3 443 → 24953 [ACK] Seq=3618 ACK=365 Win=6/072 Len=0 TSV81=1727281896 TSecF=2549354298
	74	4 2024-01-25 12:31:38.(340012513_	10.48.48.165	VMware_8d:9a:14	93.184.216.34	Cisco_9d:b9:ff	TLSv1.2	640	13	3 Application Data, Application Data
1	78	3 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	3 443 → 24953 [ACK] Seq=3618 Ack=939 Win=68096 Len=0 TSval=1727282019 TSecr=2549354468
	75	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	3 Application Data, Application Data
1	84	0 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	3 24953 → 443 [ACK] Seq=939 Ack=4698 Win=11456 Len=0 TSval=2549354588 TSecr=1727282020
1	82	2 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	2 Application Data
	83	3 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	2 61484 → 3128 [ACK] Seq=1450 Ack=2637 Win=131008 Len=0 TSval=1676452764 TSecr=4414968
ľ	84	4 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	2 Application Data, Application Data
	85	5 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	2 61484 → 3128 [ACK] Seq=1450 Ack=3780 Win=129920 Len=0 TSval=1676452838 TSecr=4414968
1	86	5 2024-01-25 12:31:39.092047	10.61.70.23	Cisco 9d:b9:ff	10.48.48.165	VMware 8d:9a:f4	TL5v1.2	497	12	2 Application Data

Imagem - HTTPS completo explícito - Sem cache



Observação: cada fluxo de tráfego é diferenciado por uma cor diferente; o fluxo do cliente para o SWA é de uma cor e o fluxo do SWA para o servidor Web é de outra.



Imagem - Fluxo HTTPS - Explícito - Sem Cache

Aqui está um exemplo de registros de acesso:

1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com:443/ - DIRECT/www.example.com



Observação: como você pode ver na implantação transparente para o tráfego HTTPS, há 2 linhas nos registros de acesso, a primeira linha é quando o tráfego é criptografado e você pode ver CONNECT e a URL do servidor Web começa com tunnel://. Se a Descriptografia estiver habilitada no SWA, a segunda linha conterá GET e a URL inteira começará com HTTPS, o que significa que o tráfego foi descriptografado.

Tráfego HTTPS de passagem

Se você configurou seu SWA para passar pelo tráfego, este é o fluxo geral:



Imagem - Passagem HTTPS - Explícita - Fluxo

Aqui está um exemplo de saudação do cliente do SWA para o servidor Web:



Imagem - Passagem HTTPS - Explícito - SWA para Servidor Web - Hello do cliente

Que é o mesmo que o Hello do cliente para o SWA:

```
    Transport Layer Security

  v TLSv1.3 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: 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
       v Extension: extended_master_secret (len=0)
            Type: extended_master_secret (23)
            Length: 0

    Extension: renegotiation_info (len=1)
```

Imagem - Passagem HTTPS - Explícita - Cliente para SWA - Hello do cliente

Aqui está um exemplo de Accesslog:

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



Observação: como você pode ver, é apenas uma única linha e a ação é PASSTHRU.

Implantação transparente

Tráfego HTTP na implantação transparente sem autenticação

Cliente e SWA

O tráfego de rede ocorre entre o endereço IP do cliente e o endereço IP do servidor Web.

O tráfego do cliente é destinado à porta TCP 80 (não à porta de proxy)

- Handshake TCP.
- HTTP Get do cliente (IP de destino = servidor Web , Porta de destino = 80)
- Resposta HTTP do Proxy (IP de Origem = Servidor Web)
- Transferência de dados

• Encerramento da conexão TCP (Handshake de 4 Vias)

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt st	tream	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 2	88 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

Imagem - Cliente para Proxy - HTTP - Transparente - Sem Autenticação

Aqui está um exemplo de HTTP Get do cliente

>	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									
\sim	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									
	<pre>[Full request URI: http://example.com/]</pre>									
	[HTTP request 1/1]									
	[Response in frame: 15]									

Imagem - Cliente para Proxy - HTTP - Transparente - Sem Autenticação - Cliente HTTP Get

Servidor Web e SWA

O tráfego de rede ocorre entre o endereço IP do Proxy e o endereço IP do servidor Web.

O tráfego do SWA é destinado à porta TCP 80 (não à porta proxy)

- Handshake TCP.
- HTTP Get do Proxy (IP de Destino = Servidor Web, Porta de Destino = 80)
- Resposta HTTP do servidor Web (IP de origem = servidor proxy)
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

No.	Time Source	src MAC Destination	dst MAC	Protocol Lengt	stream Info
	8 2023-12-11 19:13:47.(260946116_ 10.201.189.1	80 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_ 93.184.216.3	4 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=
1	10 2023-12-11 19:13:47.(285000827_ 10.201.189.1	80 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
1	11 2023-12-11 19:13:47.(307381585_ 10.201.189.1	80 Cisco_76:fb:16 93.184.216.34	Cisco_56:5f:44	HTTP 243	1 GET / HTTP/1.1
1	12 2023-12-11 19:13:47.(118451681_ 93.184.216.3	4 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
1	13 2023-12-11 19:13:47.(209167872_ 93.184.216.3	4 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
1	14 2023-12-11 19:13:47.637333 10.201.189.1	80 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
1	15 2023-12-11 19:13:47. (276272012 93.184.216.3	4 Cisco_56:5f:44 10.201.189.180	Cisco_76:fb:16	HTTP 349	1 HTTP/1.1 200 OK (text/html)
1	16 2023-12-11 19:13:47.(249979843_ 10.201.189.1	80 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	1_ 2023-12-11 19:14:12.(270488529_ 10.201.189.1	80 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	1_ 2023-12-11 19:14:12.236807 93.184.216.3	4 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	1_ 2023-12-11 19:14:12.(215970816_ 93.184.216.3	4 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	1_ 2023-12-11 19:14:12.(218303318_ 10.201.189.1	80 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
					~

Imagem - Proxy e Servidor Web - HTTP - Transparente - Sem Autenticação

Aqui está um exemplo de HTTP Get do 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 + 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]

Imagem - Proxy para Servidor Web - HTTP - Transparente - Sem Autenticação - Proxy HTTP Get

Isso representa todo o fluxo de tráfego do cliente para o SWA, depois para o servidor Web e, finalmente, de volta para o cliente.

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt :	stream In	ifo	
	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 5	4468 → 80 [5	SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1	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 6	5132 - 80 [S	SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1559577035 TSecr=0
1	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 8	0 → 65132 [5	SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=6873333 TSecr
1	0 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 6	5132 - 80 [A	ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=1559577035 TSecr=6873333
1	1 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 6	ET / HTTP/1.	.1
1	2 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 8	0 → 65132 [A	ACK] Seq=1 Ack=178 Win=66368 Len=0 TSval=6873333 TSecr=1559577035
1	3 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 8	0 → 65132 [A	ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=1559577035 [TCP segment
1	4 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 6	5132 - 80 [A	ACK] Seq=178 Ack=1449 Win=11776 Len=0 TSval=1559577165 TSecr=6873463
1	5 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 H	TTP/1.1 200	OK (text/html)
1	5 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 6	5132 - 80 [A	ACK] Seq=178 Ack=1732 Win=11520 Len=0 TSval=1559577165 TSecr=6873463
1	8 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 8	Ø → 54468 [S	SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
1	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 5	4468 - 80 [A	ACK) Seg=1 Ack=1 Win=262656 Len=0
2	8 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 G	ET / HTTP/1.	.1
2	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 8	0 → 54468 [A	ACK] Seg=1 Ack=75 Win=65472 Len=0
2	2 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 8	0 → 54468 [A	ACK] Seg=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
2	3 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 H	TTP/1.1 200	OK (text/html)
2	4 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 5	4468 - 80 [A	ACK] Seg=75 Ack=1788 Win=262656 Len=0
2	5 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 5	4468 → 80 [F	FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
2	5 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 8	0 - 54468 [A	ACK] Seg=1788 Ack=76 Win=65472 Len=0
2	7 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 8	0 → 54468 [F	FIN, ACK] Seg=1788 Ack=76 Win=65472 Len=0
2	8 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 5	4468 - 80 [A	ACK] Seg=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 6	5132 → 80 [F	FIN, ACK] Seg=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 8	0 → 65132 [A	ACK] Seg=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 8	0 → 65132 [F	FIN, ACK] Seg=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 6	5132 → 80 [A	ACK] Seg=179 Ack=1733 Win=13120 Len=0 TSval=1559602015 TSecr=6898313

Imagem - Tráfego total - HTTP - Transparente - Sem autenticação



Observação: cada fluxo de tráfego é diferenciado por uma cor diferente; o fluxo do cliente para o SWA é de uma cor e o fluxo do SWA para o servidor Web é de outra.

Time	192.16	8.1.10 93.184	.216.34 10.201.*	189.180	Comment
0000 10 11 10:10:47 (0704020200		54468 → 80 [SYN] Sen=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM			700 F4455 - 00 (599) 5 0 W 54340
2023-12-11 19-13-47 (3724062560 nanoseconds)	54468		80 65132 + 80 (SYN) Sec-0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSva		TCP: 54406 - 60 [31N] 544-0 Win-64240 Le.
2023-12-11 19:13:47.(2609461168 nanoseconds)		80	40 + 85122 [SVN ACV] Search Ark=1 Win-85535 an=0 MSC=1480 WSC#4 C4CV	65132	TCP: 65132 → 80 [STN] Seq=0 Win=12288 Le
2023-12-11 19:13:47.(2731486336 nanoseconds)		80	05195 - 05 14 PUT Con-1 4-L-1 WI-19104 Lon-0 TC-1-155057905 TC	65132	TCP: 80 + 65132 [SYN, ACK] Seq10 Ack:1 W
2023-12-11 19:13:47.(2850008272 hanoseconds)		80		65132	TCP: 65132 → 80 [ACK] Seq=1 Ack=1 Win=131
2023-12-11 19:13:47.(3073815856 nanoseconds)		80	- GET/HTDPLI	65132	HTTP: GET / HTTP/1.1
2023-12-11 19:13:47.(1184516816 nanoseconds)		80	80 + 65132 [ACK] Segi1 ACK:178 Win:66368 Len:0 TSval:68/3333 TSec1:155.	65132	TCP: 80 → 65132 [ACK] Seq=1 Ack=178 Win=6
2023-12-11 19:13:47.(2091678720 nanoseconds)		80	80 → 65132 [ACK] Seq=1 Ack=178 Win=66368 Len=1448 TSval=6873463 TSecr=.	65132	TCP: 80 → 65132 [ACK] Seq=1 Ack=178 Win=6
2023-12-11 19:13:47.637333		80	65132 → 80 [ACK] Seq=178 Ack=1449 Win=11776 Len=0 TSval=1559577165 TSec	65132	TCP: 65132 + 80 [ACK] Seq=178 Ack=1449 Wi_
2023-12-11 19:13:47.(2762720128 nanoseconds)		80	HTTP/1.1 200 OK (text/html)	65132	HTTP: HTTP/1.1 200 OK (text/html)
2023-12-11 19:13:47.(2499798432 nanoseconds)		80	65132 + 80 [ACK] Seq=178 Ack=1732 Win=11520 Len=0 TSval=1559577165 TSec	65132	TCP: 65132 → 80 [ACK] Seq=178 Ack=1732 Wi
2023-12-11 19:13:47.(24358555520 nanoseconds)	54468	80 → 54468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SAC	80		TCP: 80 -> 54468 [SYN, ACK] Seq=0 Ack=1 Wi
2023-12-11 19:13:47.(2671617136 nanoseconds)	54468	54468 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0	80		TCP: 54468 \rightarrow 80 [ACK] Seq=1 Ack=1 Win=26
2023-12-11 19:13:47.(3889843680 nanoseconds)	54468	GET / HTTP/1.1	80		HTTP: GET / HTTP/1.1
2023-12-11 19:13:47.624692	54468	80 → 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=0	80		TCP: 80 → 54468 [ACK] Seq=1 Ack=75 Win=6
2023-12-11 19:13:47.(2856456944 nanoseconds)	54468	80 + 54468 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reass	80		TCP: 80 → 54468 [ACK] Seq=1 Ack=75 Win=6
2023-12-11 19:13:47.(2375499152 nanoseconds)	54468	HTTP/1.1 200 OK (text/html)	80		HTTP: HTTP/1.1 200 OK (text/html)
2023-12-11 19:13:47.266907	54468	54468 → 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0	80		TCP: 54468 → 80 [ACK] Seq=75 Ack=1788 Wi
2023-12-11 19:13:47.(3539423648 nanoseconds)	54468	54468 → 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0	80		TCP: 54468 → 80 [FIN, ACK] Seq=75 Ack=178
2023-12-11 19:13:47.(2666658848 nanoseconds)	54468	80 → 54468 [ACK] Seq=1788 Ack=76 Win=65472 Len=0	80		TCP: 80 -> 54468 [ACK] Seq=1788 Ack=76 Wi
2023-12-11 19:13:47.(1118225184 nanoseconds)	54468	80 → 54468 [FIN, ACK] Seq=1788 Ack=76 Win=65472 Len=0	80		TCP: 80 -> 54468 [FIN, ACK] Seq=1788 Ack=7
2023-12-11 19:13:47.(1684656736 nanoseconds)	54468	54468 + 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0	80		TCP: 54468 → 80 [ACK] Seq=76 Ack=1789 Wi
2023-12-11 19:14:12.(2704885296 nanoseconds)		80	65132 → 80 [FIN, ACK] Seq=178 Ack=1732 Win=13184 Len=0 TSval=1559602015	65132	TCP: 65132 + 80 [FIN, ACK] Seq=178 Ack=173
2023-12-11 19:14:12.236807		80	80 + 65132 [ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TSecr=.	65132	TCP: 80 → 65132 [ACK] Seq=1732 Ack=179 Wi_
2023-12-11 19:14:12.(2159708160 nanoseconds)		80	80 + 65132 [FIN, ACK] Seq=1732 Ack=179 Win=66368 Len=0 TSval=6898313 TS.	65132	TCP: 80 → 65132 [FIN, ACK] Seq=1732 Ack=17
2023-12-11 19:14:12.(2183033184 nanoseconds)		80	65132 -> 80 [ACK] Seq=179 Ack=1733 Win=13120 Len=0 TSval=1559602015 TSec	65132	TCP: 65132 → 80 [ACK] Seg=179 Ack=1733 Wi_

Aqui está um exemplo de registros de acesso:

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

Tráfego Com Dados Armazenados Em Cache

Isso representa todo o fluxo de tráfego do cliente para o SWA, quando os dados estão no cache SWA.

r (9 2023-17	2-11	19:19:49.	.(111544768_	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	74	1 13586 → 80 [SYN] Seq=0 Win=12288 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3178050246 TSecr=0
1	1 2023-17	2-11	19:19:49.	. (259539926_	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	66	2 54487 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1	2 2023-17	2-11	19:19:49.	(254858128	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	66	2 80 → 54487 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
1	3 2023-17	2-11	19:19:49.	(272497027_	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2 54487 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1	4 2023-17	2-11	19:19:49.	. (178847280	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	HTTP	128	2 GET / HTTP/1.1
1	5 2023-17	2-11	19:19:49.	. (104967324_	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2 80 - 54487 [ACK] Seq=1 Ack=75 Win=65472 Len=0
1	6 2023-17	2-11	19:19:49.	656205	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	1514	2 80 → 54487 [ACK] Seq=1 Ack=75 Win=65472 Len=1460 [TCP segment of a reassembled PDU]
1	7 2023-17	2-11	19:19:49.	. (425926200_	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	HTTP	381	2 HTTP/1.1 200 OK (text/html)
1	8 2023-17	2-11	19:19:49.	. (270830524_	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2 54487 → 80 [ACK] Seq=75 Ack=1788 Win=262656 Len=0
1	9 2023-17	2-11	19:19:49.	(391010345	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2 54487 → 80 [FIN, ACK] Seq=75 Ack=1788 Win=262656 Len=0
2	0 2023-17	2-11	19:19:49.	(394258659_	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2 80 - 54487 [ACK] Seq=1788 Ack=76 Win=65472 Len=0
2	1 2023-17	2-11	19:19:49.	910090	93.184.216.34	Cisco_76:fb:15	192.168.1.10	Cisco_c9:c0:7f	TCP	54	2 80 → 54487 [FIN, ACK] Seq=1788 Ack=76 Win=65472 Len=0
2	2 2023-17	2-11	19:19:49.	(179047075_	192.168.1.10	Cisco_c9:c0:7f	93.184.216.34	Cisco_76:fb:15	TCP	60	2 54487 - 80 [ACK] Seq=76 Ack=1789 Win=262656 Len=0
2	3 2023-17	2-11	19:19:49.	(372291046	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	74	1 80 → 13586 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=4080954250 TSe
2	4 2023-17	2-11	19:19:49.	. (309178142_	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1 13586 - 80 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=3178050246 TSecr=4080954250
+ 2	5 2023-17	2-11	19:19:49.	(226286489	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	HTTP	293	1 GET / HTTP/1.1
2	6 2023-17	2-11	19:19:49.	(207193169	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1 80 → 13586 [ACK] Seq=1 Ack=228 Win=66368 Len=0 TSval=4080954250 TSecr=3178050246
- 2	7 2023-17	2-11	19:19:49.	.(229948003	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	HTTP	489	1 HTTP/1.1 304 Not Modified
2	8 2023-17	2-11	19:19:49.	(336640662	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1 13586 → 80 [ACK] Seq=228 Ack=424 Win=12800 Len=0 TSval=3178050356 TSecr=4080954361
2	9 2023-17	2-11	19:19:49.	.352537	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1 13586 - 80 [FIN, ACK] Seq=228 Ack=424 Win=13184 Len=0 TSval=3178050356 TSecr=4080954361
3	0 2023-17	2-11	19:19:49.	(194154916	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1 80 → 13586 [ACK] Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
3	1 2023-17	2-11	19:19:49.	(349158924_	93.184.216.34	Cisco_56:5f:44	10.201.189.180	Cisco_76:fb:16	TCP	66	1 80 → 13586 [FIN, ACK] Seq=424 Ack=229 Win=66368 Len=0 TSval=4080954361 TSecr=3178050356
L 3	2 2023-17	2-11	19:19:49.	(103444988	10.201.189.180	Cisco_76:fb:16	93.184.216.34	Cisco_56:5f:44	TCP	66	1 13586 - 80 [ACK] Seq=229 Ack=425 Win=13120 Len=0 TSval=3178050356 TSecr=4080954361

Imagem - Em Cache - Tráfego Total - HTTP - Transparente - Sem Autenticação



Observação: Como você pode ver, o Servidor Web retorna a resposta HTTP 304: Cache não Modificado. (neste exemplo, Pacote número 27)

Aqui está um exemplo da Resposta 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/]

Imagem - Em Cache - Resposta HTTP 304 - HTTP - Transparente - Sem Autenticação

Aqui está um exemplo de registros de acesso:

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

Tráfego HTTPs em implantação transparente sem autenticação

Cliente e SWA

O tráfego de rede ocorre entre o endereço IP do cliente e o endereço IP do servidor Web.

O tráfego do cliente é destinado à porta TCP 443 (não à porta proxy)

- Handshake TCP.
- Cliente de handshake TLS Hello Servidor Hello Troca de chaves do servidor Troca de chaves do cliente
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

No.	Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt s	stream	n Info
24	3 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	4 54515 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
24	5 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	4 443 → 54515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
24	6 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	4 54515 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
24	7 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	4 Client Hello (SNI=example.com)
24	8 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	4 443 → 54515 [ACK] Seq=1 Ack=189 Win=65408 Len=0
25	6 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	4 Server Hello
25	7 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	4 Certificate, Server Key Exchange, Server Hello Done
25	8 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	4 54515 → 443 [ACK] Seq=189 Ack=2450 Win=262656 Len=0
25	9 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	4 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26	0 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	4 443 → 54515 [ACK] Seq=2450 Ack=282 Win=65344 Len=0
26	1 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	4 Change Cipher Spec, Encrypted Handshake Message
26	2 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	4 Application Data
26	3 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	4 443 → 54515 [ACK] Seq=2501 Ack=385 Win=65280 Len=0
26	4 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	4 Application Data
26	5 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	4 Application Data
26	6 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	4 54515 → 443 [ACK] Seq=385 Ack=4007 Win=262656 Len=0
26	7 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	4 Application Data
26	8 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	4 Encrypted Alert
26	9 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	4 443 → 54515 [ACK] Seq=4264 Ack=416 Win=65280 Len=0
27	0 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	4 54515 - 443 [FIN, ACK] Seq=416 Ack=4264 Win=262400 Len=0
27	1 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	4 443 → 54515 [ACK] Seq=4264 Ack=417 Win=65280 Len=0
27	2 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	4 443 → 54515 [FIN, ACK] Seq=4264 Ack=417 Win=65280 Len=0
27	2 2022 12 11 10.26.25 204240	102 169 1 10	Cicco c0.c0.7f	02 104 216 24	Cicco 76, th. 15	TCD	60	14	4 54515 . 442 [ACK] See-417 Ack-4265 Win-262400 Len-0

Imagem - Cliente para Proxy - HTTPs - Transparente - Sem Autenticação

Aqui estão os detalhes do cliente Hello do cliente para o SWA, como você pode ver na indicação de nome do servidor (SNI), a URL do servidor web pode ser vista, que neste exemplo é 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
ransport 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
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)
<pre>> Extension: ec_point_formats (len=2)</pre>
> 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: tl2d2108h1_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]

Imagem - Hello do cliente - Cliente para proxy - Transparente - Sem autenticação



Dica: você pode usar esse filtro no Wireshark para procurar URL/SNI : tls.handshake.extensions_server_name == "www.example.com"

Aqui está um exemplo de troca de chave de servidor

Frame 257: 1043 bytes on wire (8344 bits), 1043 bytes captured (8344 bits)
Ethernet II, Src: Cisco_76:fb:15 (70:70:8b:76:fb:15), Dst: Cisco_c9:c0:7f (74:88:bb:c9:c0:7f)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 443, Dst Port: 54515, Seq: 1461, Ack: 189, Len: 989
[2 Reassembled TCP Segments (2054 bytes): #256(1379), #257(675)]
 Transport Layer Security
V TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 2049
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 2045
Certificates Length: 2042
Certificates (2042 bytes)
Certificate Length: 1098
Certificate [truncated]: 308204463082032ea00302010202140440907379f2aad73d32683b716d2a7ddf2b8e2a300d06092a864886f70d01010b65003040310b30090603550406130255533110300e060355040.
signedCertificate
version: v3 (2)
serialNumber: 0x0440907379f2aad73d32683b716d2a7ddf2b8e2a
> signature (sha256WithRSAEncryption)
✓ 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]: 308203a63082028ea003020102020900a447d8363a186f2f300d06092a864886f70d01010b05003040310b30090603550406130255533110300e060355040a130777736174657374310
 Transport Layer Security
> TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
> TLSv1.2 Record Laver: Handshake Protocol: Server Hello Done

Imagem - Troca de chaves do servidor - Cliente para proxy - Transparente - Sem autenticação



Observação: como você pode ver, o certificado é o que foi configurado no SWA como certificado de descriptografia.

Servidor Web e SWA

O tráfego de rede ocorre entre o endereço IP do Proxy e o endereço IP do servidor Web.

O tráfego do SWA é destinado à porta TCP 443 (não à porta proxy)

- Handshake TCP.
- Cliente de handshake TLS Hello Servidor Hello Troca de chaves do servidor Troca de chaves do cliente
- Transferência de dados
- Encerramento da conexão TCP (Handshake de 4 Vias)

No		Time	Source	src MAC	Destination	dst MAC	Protocol	Lengt st	tream	Info		
F	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 - 4	443 (S	YN] 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 - 478	868 [5	YN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=3980365294
Т	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 - 4	443 (A	CK] 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 He	ello (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 - 478	868 [A	CK] 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 He	ello	
	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 - 4	443 [A	CK] 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 - 478	868 (A	CK] 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 - 4	443 [A	CK] 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	Certifica	ate, S	erver 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 - 4	443 [A	CK] 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 Wind	dow Up	date] 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 Ke	ey Exc	hange, 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 - 478	868 [A	CK] 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 Ci	ipher	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 - 4	443 [A	(K] 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	Applicati	ion Da	ta
	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 - 478	868 [A	CK] 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	Applicati	ion Da	ta, 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 - 478	868 [A	CK] 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	Applicati	ion Da	ta
	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 - 4	443 [A	CK] 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	Applicati	ion Da	ta
	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 - 4	443 (A	CK] 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	d Aler	t
	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 - 4	443 [F	IN, ACK] Seq=619 Ack=5267 Win=12288 Len=0 TSval=1563255773 TSecr=3980365933
T	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 - 478	868 [A	CK] 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 - 478	868 [A	CK] 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 - 478	868 (F	IN, ACK] Seq=5267 Ack=620 Win=64896 Len=0 TSval=3980366034 TSecr=1563255773
	220	2022-12-11 10:26:25 (422261704	18 281 100 108	Circo 76: fb: 16	02 104 216 24	Circo SE-SF-44	TCD	66	17	47060	442 [A	(V) Sec-529 Ack-5269 Min-12209 Len-9 TSus1-1562255773 TSec-2009266924

Imagem - Proxy para Servidor Web - HTTPs - Transparente - Sem autenticação

Aqui está um exemplo de Hello do cliente do SWA para o servidor Web

> 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
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
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)
<pre>> Extension: session_ticket (len=0)</pre>
> 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]

Imagem - Hello do cliente - Proxy para servidor Web - Transparente - Sem autenticação



Observação: os conjuntos de cifras observados aqui diferem dos conjuntos de cifras no Hello do cliente para SWA, pois o SWA, configurado para descriptografar esse tráfego, utiliza suas próprias cifras.



Dica: na troca de chaves do servidor de SWA para o servidor Web, o certificado do servidor Web é exibido. No entanto, se um Proxy de Upstream encontrar configuração para o seu SWA, o certificado será exibido em vez do certificado do Servidor Web.

Aqui está um exemplo de registros de acesso:

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



Observação: como você pode ver na implantação transparente para o tráfego HTTPS, há 2 linhas nos registros de acesso, a primeira linha é quando o tráfego é criptografado e você pode ver TCP_CONNECT e o endereço IP do servidor Web. Se a Descriptografia estiver habilitada no SWA, a segunda linha conterá GET e a URL inteira começará com HTTPS, o que significa que o tráfego foi descriptografado e o SWA conhece a URL.

Informações Relacionadas

- Suporte Técnico e Documentação Cisco Systems
- Configurar Parâmetro de Desempenho em Logs de Acesso Cisco

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.