Entender o formato do registro de acesso HTTPS no Secure Web Appliance

Contents

Introdução

Este documento descreve os logs de acesso do Secure Web Appliance (SWA) para o tráfego HTTPS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- Cliente Secure Shell (SSH).
- O assistente de instalação foi concluído.
- Acesso administrativo ao SWA.

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.

Informações de Apoio

A forma como o tráfego HTTPS do Cisco SWA registra os logs de acesso é diferente em comparação ao tráfego HTTP normal.

Note: Os logs dependem do modo de implantação do Proxy, no modo de encaminhamento explícito ou no modo transparente, os logs são diferentes.

Palavras-chave nos registros de acesso

Aqui estão algumas palavras-chave importantes que você pode ver nos registros de acesso:

TCP_CONNECT : Isso mostra que o tráfego foi recebido de forma transparente (via WCCP, redirecionamento L4 ou outros métodos de redirecionamento transparente)
CONNECT: Isso mostra que o tráfego foi recebido explicitamente.
DESCRIPTOGRAFAR_WBRS : Mostra que o SWA descriptografou o tráfego devido à pontuação do Web Reputation Score (WBRS).
PASSTHRU_WBRS : Isso mostra que o SWA passou pelo tráfego devido à pontuação WBRS.
DROP_WBRS: Isso mostra que o SWA tem a opção Drop the traffic due to WBRS score (Descartar o tráfego devido à pontuação WBRS)

Logs HTTPS nos logs de acesso

Quando o tráfego HTTPS é descriptografado, o WSA registra duas entradas.

- TCP_CONNECT tunnel:// ou CONNECT tunnel:// depende do tipo de solicitação recebida, o que significa que o tráfego está criptografado (ainda não foi descriptografado).
- GET https:// mostra o URL descriptografado.

Note: A URL completa no modo transparente só estará visível se o SWA descriptografar o tráfego.

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

Note: No modo transparente, o SWA tem o endereço IP de destino inicialmente quando o tráfego é redirecionado para ele.

Aqui estão alguns exemplos do que você vê nos logs de acesso:`

Implantação transparente - tráfego descriptografado
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5,0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
Implantação transparente - tráfego de passagem
1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9,0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Implantação transparente - Descartar
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT 192.168.34.32:443/ - DIRECT/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Implantação explícita - tráfego descriptografado
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,->- 1252543559.535 1127 10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-> -
Implantação Explícita - Tráfego de passagem
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9,0,-> -
Implantação Explícita - Remover
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,->-

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implantação

limitada) - Solução de problemas...
- 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.