Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro

Contenido

Introducción

Este documento describe los registros de acceso de Secure Web Appliance (SWA) para el tráfico HTTPS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- Cliente Secure Shell (SSH).
- El asistente de configuración ha finalizado.
- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La forma en que los registros de tráfico HTTPS de Cisco SWA en los registros de acceso son diferentes en comparación con el tráfico HTTP normal.

Nota: Los registros dependen del modo de implementación de proxy; en el modo de reenvío explícito o en el modo transparente, los registros son diferentes.

Palabras clave de los registros de acceso

Estas son algunas palabras clave importantes que puede ver en los registros de accesorios:

TCP_CONNECT: Muestra que el tráfico se recibió de forma transparente (a través de WCCP, redirección L4 u otros métodos de redirección transparente)
CONECTAR: Esto muestra que el tráfico se recibió explícitamente.
DECRYPT_WBRS: Muestra que SWA ha descifrado el tráfico debido a la puntuación de la reputación en la Web (WBRS).
PASSTHRU_WBRS: Muestra que SWA ha pasado a través del tráfico debido a la puntuación WBRS.
DROP_WBRS: Esto muestra que SWA ha descartado el tráfico debido a la puntuación WBRS

Registros HTTPS en los registros de acceso

Cuando se descifra el tráfico HTTPS, WSA registra dos entradas.

- TCP_CONNECT tunnel:// o CONNECT tunnel:// depende del tipo de solicitud recibida, lo que significa que el tráfico está cifrado (aún no se ha descifrado).
- GET https:// muestra la URL descifrada.

Nota: La dirección URL completa en modo transparente solo es visible si SWA descifra el tráfico.

```
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
```

Nota: En el modo transparente, SWA tiene la dirección IP de destino inicialmente cuando el tráfico se redirige a ella.

A continuación se muestran algunos ejemplos de lo que se ve en los registros de acceso:

Implementación transparente - Tráfico descifrado
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-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
Implementación transparente - Tráfico de paso
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,-,-,-,-,-,-,-,-,-,-,-,-> -
Implementación 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,-,-,-,-,-,-,-,-,-,-,-,-> -
Implementación explícita: tráfico descifrado
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,-,-,-,0,-,-,-,-,-,-,-> -
Implementación explícita: tráfico de paso a través
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,-,-,-,-,-,-,-,-,-,-,-,-> -
Implementación explícita: descartar
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,-,-,-,-,-,-,-,-,-,-,-,-> -

Información Relacionada

- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implementación limitada) - Solución de problemas...
- Configuración del parámetro de rendimiento en registros de acceso: Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).