¿Cuál es registro abierto una sesión del acceso para el tráfico HTTPS?

Contenido

Contribuido por Kei Ozaki y Siddharth Rajpathak, ingenieros de Cisco TAC.

Pregunta:

¿Cuál es registro abierto una sesión del acceso para el tráfico HTTPS?

Entorno: Versiones 7.1.x de AsyncOS del dispositivo de seguridad de la red de Cisco que se ejecutan (WSA) y arriba, proxy HTTPS habilitado

El tráfico de los registros HTTPS del dispositivo de seguridad de la red de Cisco de la manera (WSA) es diferente comparado al tráfico HTTP normal. Las entradas HTTPS registradas en los accesslogs parecerán diferentes dependiendo de cómo la petición fue tratada. En el general tiene diversas características comparadas al tráfico HTTP normal.

Se registra qué dependerá de qué modo del despliegue usted está utilizando (modo o modo transparente delantero explícito).

Primero miremos algunas palabras claves que le ayudarían acceso de lectura registra fácilmente.

TCP_CONNECT - esto muestra que el tráfico fue recibido transparente (vía el WCCP o el L4 reoriente… el etc)
CONECTE - esto muestra que el tráfico fue recibido explícitamente
DECRYPT_WBRS - esto muestra que WSA ha decidido a desencriptar el tráfico debido a la calificación WBRS
PASSTHRU_WBRS - esto muestra que WSA ha decidido a pasar con el tráfico debido a la calificación WBRS
DROP_WBRS - esto muestra que WSA ha decidido a caer el tráfico debido a la calificación WBRS

- Cuando se desencripta el tráfico **HTTPS**, WSA registrará dos entradas.
- **TCP_CONNECT** o **CONECTAN** dependiendo del tipo de petición que es recibida y de **"GET https://"** que muestra el URL desencriptado.
- **El URL** lleno será solamente visible si WSA desencripta el tráfico.

También observe por favor eso:

- En el modo transparente, WSA verá solamente el IP Address de destino inicialmente
- En el modo explícito, WSA verá el nombre del host de destino

Abajo están algunos ejemplos de lo que usted vería en los accesslogs:

Transparente - Decrypt
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT tunnel://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 imagen/GIF DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
Traspaso transparente
1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparente - Descenso
1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-,-> -
Explícito - Decrypt
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONECTAN tunnel://www.example.com:443/ - www.example.com DIRECTO - 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 - imagen DIRECTA/GIF DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> de www.example.com -
Explícito - Pase a través
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 CONECTAN tunnel://www.example.com:443/ - www.example.com DIRECTO - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-> -
Explícito - Descenso
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONECTA tunnel://www.example.com:443/ - NINGUNOS - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-> -