Understand HTTPS Accesslog Format in Secure Web Appliance

Contents

Introduction

This document describes Secure Web Appliance (SWA) accesslogs for HTTPS traffic.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual SWA Installed.
- License activated or installed.
- Secure Shell (SSH) Client.
- The setup wizard is completed.

- Administrative Access to the SWA.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The way Cisco SWA HTTPS traffic logs in the accesslogs are different compared to normal HTTP traffic.

Note: The logs are depend on the Proxy deployment mode, in explicit forward mode or transparent mode the logs are deferent.

Keywords in the Accesslogs

Here are some important keywords you can see in the Accesslogs:

TCP_CONNECT : This shows traffic was received transparently (via WCCP, L4 redirect or other transparent redirection methods)
CONNECT : This shows traffic was received explicitly.
DECRYPT_WBRS : This shows SWA has Decrypt the traffic due to Web Reputation Score (WBRS) score.
PASSTHRU_WBRS : This shows SWA has Pass Through the traffic due to WBRS score.
DROP_WBRS : This shows SWA has Drop the traffic due to WBRS score

HTTPS Logs in the Accesslogs

When HTTPS traffic is decrypted, WSA logs two entries.

- **TCP_CONNECT tunnel://** or **CONNECT tunnel://** depends on the type of request received, which means that the traffic is encrypted (has not yet been decrypted).
- **GET https://** shown the decrypted URL.

Note: Full URL in transparent mode is only visible if SWA decrypts the traffic.

```
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: In transparent mode, SWA has the destination IP address initially when the traffic is redirected to it.

Here are some examples of what you see in accesslogs:`

Transparent Deployment- Decrypted Traffic
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,-,-,-,-,-,-,-> -
Transparent Deployment- Passthrough Traffic
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparent Deployment - Drop
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Explicit Deployment- Decrypted Traffic
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,-,-,-,-,-,-,-> -
Explicit Deployment - Passthrough traffic
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Explicit Deployment - Drop
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -

Related Information

- User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooti...
- Configure Performance Parameter in Access Logs - Cisco