了解安全Web设备中的HTTPS访问日志格式

目录

简介

本文档介绍HTTPS流量的安全网络设备(SWA)访问日志。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安全外壳(SSH)客户端。
- 安装向导已完成。
- 对SWA的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco SWA HTTPS流量在访问日志中的记录方式与常规HTTP流量不同。

注意：日志取决于代理部署模式，在显式转发模式或透明模式下，日志是不同的。

访问日志中的关键字

以下是您可以在Accesslogs中看到的一些重要关键字：

TCP_CONNECT:这显示流量是以透明方式接收的（通过WCCP、L4重定向或其他透明重定向方法）
连接:这显示流量是显式接收的。
DECRYPT_WBRS :这显示SWA已根据Web信誉得分(WBRS)得分解密流量。
PASSTHRU_WBRS :这显示由于WBRS得分，SWA已通过流量。
DROP_WBRS :这显示SWA已丢弃由于WBRS得分的流量

访问日志中的HTTPS日志

当HTTPS流量解密时，WSA会记录两个条目。

- TCP_CONNECT tunnel://或CONNECT tunnel://取决于收到的请求类型，这意味着流量已加密（尚未解密）。
- GET https://显示已解密的URL。

注意：仅当SWA解密流量时，透明模式中的完整URL才可见。

```
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.examp
```

注意：在透明模式下，当流量重定向到SWA时，SWA最初具有目标IP地址。

以下是您在访问日志中看到的一些示例：'

透明部署 — 解密的流量
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-DefaultRouting <A 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,-,-,-,-> -
透明部署 — 直通流量

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 <A sear，9.0,-,-,-,-,-,-,-,-,-,-,-,-,-,->
透明部署 — 丢弃
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 <A sear、-9.1.0、-、-、-、-、-、-、-、-、-、-、-、-、-、->
显式部署 — 解密的流量
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,-,-,-,-,-> -
显式部署 — 直通流量
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,-,-,-,-,-,-,-,-,-,-,-,-,-,-
显式部署 — 丢弃
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -

相关信息

- 思科安全网络设备AsyncOS 15.0用户指南 — LD（有限部署） — 故障排除……
- 配置访问日志中的性能参数 — 思科

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。