什么是HTTPS流量的登陆的访问日志？

目录

贡献用Kei尾崎和Siddharth Rajpathak， Cisco TAC工程师。

问题：

什么是HTTPS流量的登陆的访问日志？

环境：Cisco Web运行AsyncOS版本7.1.x和以上的安全工具(WSA)， HTTPS代理启用

方式思科Web安全工具(WSA)日志HTTPS流量不同的与正常HTTP数据流比较。 在accesslog记录的HTTPS条目将看起来不同的根据请求如何对待。一般它有另外特性与正常HTTP数据流比较。

什么被记录将取决于什么部署模式您使用(明确向前模式或透明模式)。

首先请查看将容易地帮助您读访问日志的一些关键字。

TCP_CONNECT -这显示流量接收透明地(通过WCCP或L4重定向…等)
连接-这显示流量明确地接收
DECRYPT_WBRS -这显示WSA决定解密流量由于WBRS分数
PASSTHRU_WBRS -这显示WSA决定穿过流量由于WBRS分数
DROP_WBRS -这显示WSA决定降低流量由于WBRS分数

- 当**HTTPS流量**解密， WSA将记录两个条目。
- **TCP_CONNECT**或**连接**根据种类请求接收的和**"GET"**显示解密的URL的**https://**。
- 如果WSA解密流量，全双工**URL**只可视。

也请注释那：

- 在透明模式， WSA最初只将看到目的IP地址
- 在明确模式， WSA将看到目的地主机名

下面什么的一些示例您在accesslog会看到：

透明-解密
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个192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32镜像/gif DEFAULT_CASE-

test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
透明转接
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
透明-丢弃
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,-,-,-,-,-,-,-,-,-,-,-,-,-> -
明确-解密
252543558.405 385 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40连接 tunnel://www.example.com:443/ -直接www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543559.535 1127个10.66.71.105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif -直接www.example.com镜像/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-> -
明确-通过
1252543491.302 568 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256连接 tunnel://www.example.com:443/ -直接www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
明确-丢弃
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578连接tunnel://www.example.com:443/ -无- DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-> -