Содержание

Внесенный Kei Ozaki и Siddharth Rajpathak, специалистами службы технической поддержки Cisco.

Вопрос:

Что вошло в журнал доступа для Трафика HTTPS?

Среда: Cisco Web Security Appliance (WSA) рабочие версии AsyncOS 7.1.x и выше, прокси HTTPS включен

Путем Cisco Web Security Appliance Трафик HTTPS журналов (WSA) является другим по сравнению с обычным трафиком HTTP. Записи HTTPS, зарегистрированные в accesslog, будут выглядеть по-другому в зависимости от того, как рассматривался запрос. В целом это имеет другие характеристики по сравнению с обычным трафиком HTTP.

То, что зарегистрировано, будет зависеть, на каком режиме развертываний вы используете (явный режим переадресации или прозрачный режим).

Сначала давайте посмотрим на некоторые ключевые слова, которые помогли бы вам журналы доступа для чтения легко.

Соединение TCP- это показывает, что трафик был получен прозрачно (через WCCP или перенаправление L4... и т.д.)
CONNECT - это показывает, что трафик был получен явно
DECRYPT_WBRS - это показывает, что WSA решил Дешифровать трафик из-за счета WBRS
PASSTHRU_WBRS - это показывает, что WSA решил Пройти через трафик из-за счета WBRS
DROP_WBRS - это показывает, что WSA решил Отбросить трафик из-за счета WBRS

- Когда **Трафик HTTPS** будет дешифрован, WSA регистрирует две записи.
- **TCP_CONNECT** или **ПОДКЛЮЧЕНИЕ** в зависимости от типа получаемого запроса и **"GET https://"** показ дешифрованного URL.
- Если WSA дешифрует трафик, полный **URL** только будет видим.

Также обратите внимание что:

- В прозрачном режиме WSA будет только видеть IP - адрес назначения первоначально
- В явном режиме WSA будет видеть имя хоста назначения

Ниже некоторые примеры того, что вы видели бы в accesslog:

Прозрачный - дешифруют
1252543170.769 386 192.168.30.103 TCP_MISS_SSL/200 0 TCP_CONNECT

tunnel://192.168.34.32:443/-ПРЯМОЙ/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Сухой, 5.0,-> -

1252543171.166 395 192.168.30.103 GET 2061 года TCP_MISS_SSL/200 https://www. пример. com:443/sample.gif - ПРЯМОЙ/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Сухой, 5.0,0, - 0,-> -

Прозрачная транзитная пересылка -

1252543337.373 690 192.168.30.103 TCP_MISS/200 2044 TCP_CONNECT tunnel://192.168.34.32:443/-ПРЯМОЙ/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Сухой, 9.0,-> -

Прозрачный - отбрасывание

1252543418.175 430 192.168.30.103 TCP_DENIED/403 0 TCP_CONNECT tunnel://192.168.34.32:443/-ПРЯМОЙ/192.168.34.32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Сухой,-9.1.0,-> -

Явный - дешифруют

252543558.405 385 ПОДКЛЮЧЕНИЙ 10.66.71.105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 tunnel://www. пример. com:443/-ПРЯМОЙ/WWW. пример. com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Сухой, 5.0,-> -
1252543559.535 1127 10.66.71.105 GET 2061 года TCP_MISS_SSL/200 https://www. пример. com:443/sample.gif - ПРЯМОЙ/WWW. пример. com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Сухой, 5.0,0, - 0,-> -

Явный - проходят

1252543491.302 568 ПОДКЛЮЧЕНИЙ 10.66.71.105 TCP_CLIENT_REFRESH_MISS/200 2256 tunnel://www. пример. com:443/-ПРЯМОЙ/WWW. пример. com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Сухой, 9.0,-> -

Явный - отбрасывание

1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 ПОДКЛЮЧАЮТ tunnel://www. пример. com:443/-NONE/-DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Сухой,-9.1,-> -