ما هو سجل الوصول الذي تم تسجيله لحركة مرور HTTPS؟

المحتويات

تمت المساهمة من قبل كي أوزاكي وسيدهارث راجباتاك، مهندسي TAC من Cisco.

سؤال:

ما الذي تم تسجيل الدخول إلى سجل الوصول لحركة مرور HTTPS؟

البيئة: جهاز أمان الويب (WSA) من Cisco الذي يشغل الإصدار x.7.1 من AsyncOS والإصدارات الأحدث، يتم تمكين وكيل HTTPS

تختلف طريقة تسجيل حركة مرور بيانات HTTPS بواسطة جهاز أمان الويب (WSA) من Cisco مقارنة بحركة مرور HTTP العادية. ستبدو إدخالات HTTPS المسجلة في سجلات الوصول مختلفة وفقا لكيفية معالجة الطلب. بصفة عامة، يتميز بخصائص مختلفة مقارنة بحركة مرور HTTP العادية.

يعتمد ما يتم تسجيله على وضع النشر الذي تستخدمه (وضع إعادة توجيه صريح أو وضع شفاف).

دعنا أولا نلقي نظرة على بعض الكلمات الأساسية التي من شأنها أن تساعدك على قراءة سجلات الوصول بسهولة.

TCP_CONNECT - هذا يبدي حركة مرور كان إستلمت بشفافية (عبر WCCP أو L4 redirect ...إلخ)
الاتصال - هذا يوضح أنه تم تلقي حركة المرور بشكل صريح
decrypt_WBRS - هذا يوضح أن WSA قد قرر فك تشفير حركة المرور بسبب علامة WBRS
passthru_WBRS - هذا يظهر أن WSA قرر المرور عبر حركة المرور بسبب نقاط WBRS
DROP_WBRS - هذا يوضح أن WSA قرر إسقاط حركة المرور بسبب علامة WBRS

- عند فك تشفير حركة مرور **HTTPS**، سيقوم WSA بتسجيل إدخالين.
- **TCP_CONNECT** أو **CONNECT** بناء على نوع الطلب الذي يتم إستقباله و**"GET https://:"** الذي يعرض عنوان URL الذي تم فك تشفيره.
- لن يكون **عنوان URL** الكامل مرئيا إلا إذا قام WSA بفك تشفير حركة المرور.

ويرجى أيضا ملاحظة ما يلي:

- في الوضع الشفاف، سيرى WSA عنوان IP للوجهة فقط مبدئيا
- في الوضع الصريح، سيرى WSA اسم المضيف للوجهة

فيما يلي بعض الأمثلة عما ستراه في سجلات الوصول:

شفاف - فك التشفير
125254370.769 386 192.168.30.103 TCP_CONNECT 0 TCP_MISS_SSL/200

tunnel://192.168.34.32:443/ - Direct/192.168.34.32 - Decrypt_WBRS-DefaultGroup.id-none-none- - <-،-، ،-،None-DefaultRouting <Sear،5.0- الحصول على TCP_MISS_SSL/200 2061 192.168.30.103 395 1252543171.166 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-
شفاف- المرور
TCP_MISS/200 2044 TCP_CONNECT 192.168.30.103 690 125254337.373 tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup.id- - <-،none-none-defaultRouting <Sear،9.0-
شفاف - إسقاط
TCP_DENY/403 0 TCP_CONNECT 192.168.30.103 430 1252543418.175 tunnel://192.168.34.32:443/ - DIRECT/192.168.34.32 - drop_WBRS-DefaultGroup.id-none-none- <،-،DefaultRouting <SEAR، 9.1.0 -
صريح - فك التشفير
TCP_CLIENT_REFRESH_MISS_SSL/200 40 Connect 10.66.71.105 385 25254358.405 tunnel://www.example.com:443/ - DIRECT/www.example.com - decrypt_WBRS-defaultGroup- ---،-------،--------،----،test.id-none-none-defaultRouting <Sear،5.0 -- الحصول على TCP_MISS_SSL/200 2061 10.66.71.105 1127 125254359.535 https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif default_case- -،-،،،-،،-،،-،-،-،-،-،-،-،-،-،test.policy-test.id-none-none-none-none-none-none-none-none<sear،5.0،0 ---،-،-،--،،،
صريح - مرور
TCP_CLIENT_REFRESH_MISS/200 2256 Connect 10.66.71.105 568 125254391.302 tunnel://www.example.com:443/ - DIRECT/www.example.com - passthru_WBRS-DefaultGroup- ----،-،--------،-------،test.id-none-none-DefaultRouting <Sear،9.0 ------------------------------
صريح - إسقاط
TCP_DENY/403 1578 Connect tunnel://www.example.com:443/ - 10.66.71.105 125254368.375 -،-،-،-،-،-،-،-،-،-،-،-،-،-،-،-،-،-،none/- drop_WBRS-DefaultGroup-test.id-none-none-none <Sear، 9.1 ---،-،-،-،-،-،-،-،-،

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).