تحديد معدل فك التشفير في SWA

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لحساب النسبة المئوية لحركة المرور التي تم فك تشفيرها في جهاز الويب الآمن (SWA) المعروف سابقا باسم WSA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Physical أو Virtual Secure Web Appliance (SWA) مثبت.
- تم تنشيط الترخيص أو تثبيته.
- عميل Secure Shell (SSH).
- اكتمل معالج الإعداد.
- الوصول الإداري إلى SWA.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تأثير أداء فك التشفير

من بين جميع الخدمات التي يتم إجراؤها بواسطة إدارة الشبكة (SWA)، يعد تقييم حركة مرور بروتوكول نقل النص التشعبي الآمن (HTTPS) هو الأكثر أهمية من وجهة نظر الأداء.

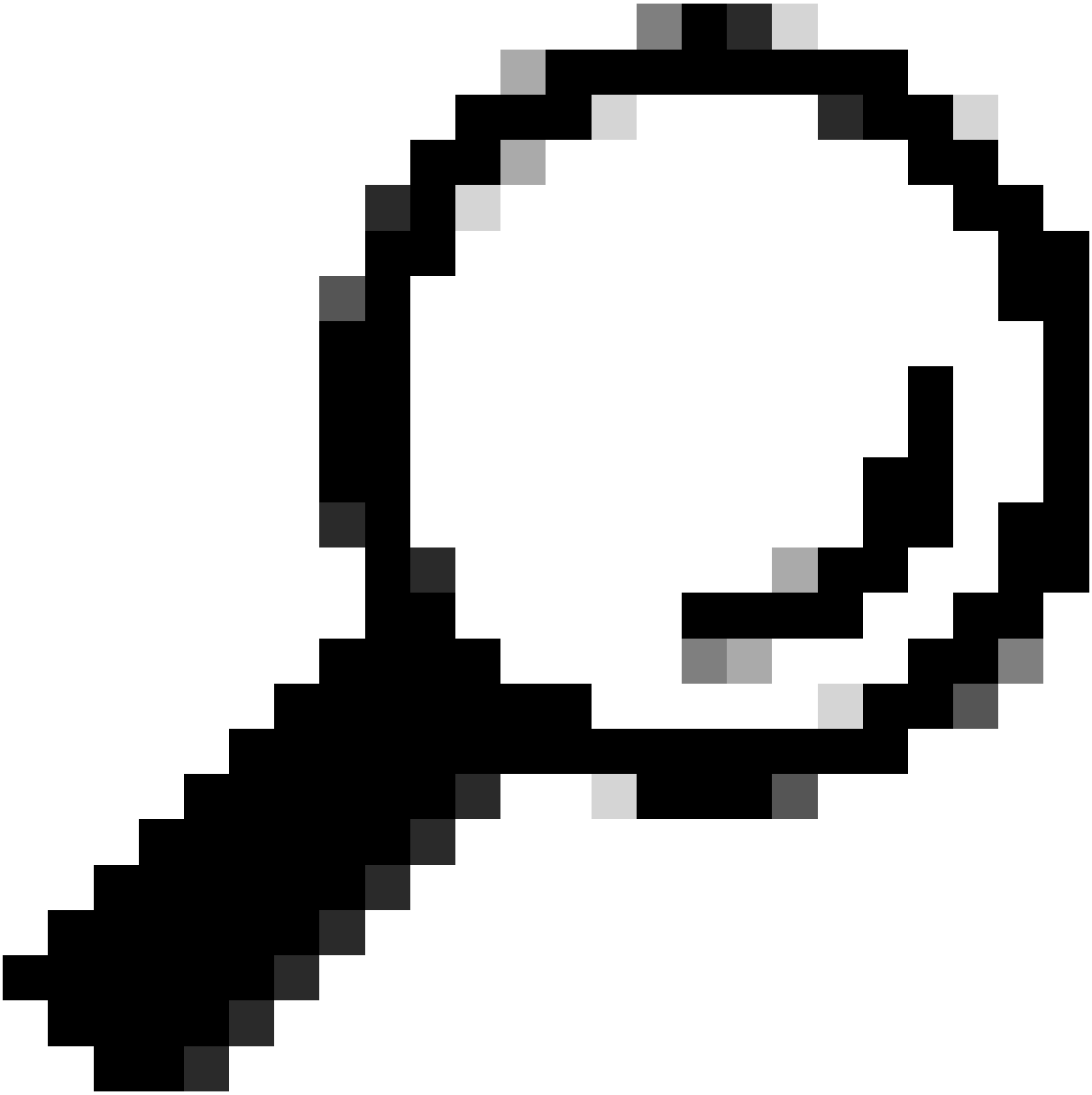
تؤثر النسبة المئوية لحركة المرور التي تم فك تشفيرها بشكل مباشر على كيفية

حجم الجهاز. يمكن أن يعتمد المسؤول على 75٪ على الأقل من حركة مرور الويب لتصبح HTTPS.

بعد التثبيت الأولي، يجب تحديد النسبة المئوية لحركة المرور التي تم فك تشفيرها لضمان تحديد توقعات النمو في المستقبل بدقة. بعد النشر، يجب التحقق من هذا الرقم مرة واحدة في كل ربع عام.

إذا كان معدل فك التشفير أكثر من 30٪ وكانت SWA تعاني من مشكلة في الأداء، ينصح إما:

- إزالة فك التشفير على فئات مختلفة أو عناوين URL موثوقة (مثل تحديثات Microsoft Update أو مكافحة الفيروسات) في نهج فك التشفير
- موازنة التحميل عبر المزيد من SWAs لتوزيع الحمل



تلميح: لمزيد من المعلومات حول كيفية تجاوز فك التشفير في SWA، يرجى زيارة الموقع: https://www.cisco.com/c/en/us/support/docs/security/web-security-

---

appliance/214746-how-to-exempt-office-365-traffic-from-au.html

خطوات لحساب النسبة المئوية لفك التشفير

للعثور على النسبة المئوية لحركة مرور HTTPS التي تم فك تشفيرها مقارنة بجميع حركة مرور HTTPS، انسخ access_log من برنامج نقل ملفات SWA (FTP).

يمكن إستخدام أوامر Simple Bash أو PowerShell للحصول على هذا الرقم. فيما يلي الخطوات الموصوفة لكل بيئة:

1. العثور على عدد إجمالي إتصالات HTTPS (صريحة وشفافة):

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. العثور على عدد إتصالات HTTPS التي تم فك تشفيرها:

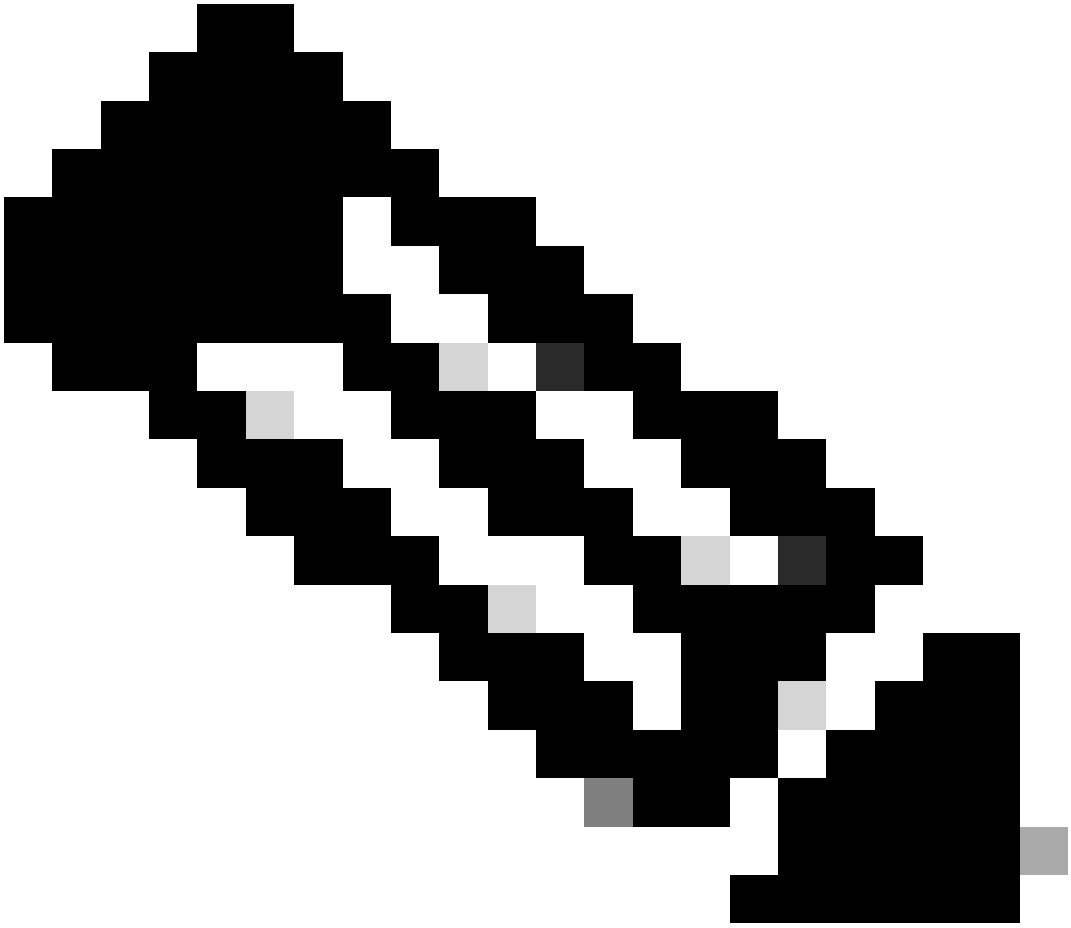
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT’| Select-String -Pattern ‘DE
```

3. قم بقسمة القيمة الثانية على القيمة الأولى وضرب ب 100.

إحصائيات حركة المرور العامة من CLI

يمكنك عرض حالات حركة المرور في CLI، باستخدام أمر accessGanalyzer الذي يمكنك إختيار نطاق الوقت أو ساعات N السابقة، لتقريرك.



ملاحظة: يعتمد وقت تنفيذ الأمر على الفترة الزمنية المحددة.

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes



------------------------------------------------------------------------------------------------
                                        HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- --------------------
Num transactions                        1512509             4170261             5682770
```

Transaction/sec	42	115	157
Bandwidth (Mbps)	0.0001	0.0004	0.0003
Max Resp time (ms)	643269	285036670	285036670
Average Resp time(ms)	95663	141715	129458
Max Object size (KB)	92246	1215832	1215832
Avg Object size (Total Trans)(KB)	5	54	41
Avg Object size (Allowed Trans) (KB)	20	67	62
Methods			
GET	1295658	0	1295658
POST	34968	0	34968
CONNECT	0	4170261	4170261
Others	181883	0	181883
Status Codes			
1xx	0	0	0
2xx	319799	3351382	3671181
3xx	75011	0	75011
4xx	11697	115467	127164
5xx	1105999	703412	1809411

معلومات ذات صلة

دليل المستخدم لـ AsyncOSAsyncOS وأ Cisco SCisco Web Appliance - LD (نشر LimLD) - Cisco

أفضل ممارسات جهاز الويب UCure - Cisco

يعفي HCisco حركة مرور Office 365 من المصادقة وفك التشفير على Cisco WSA Interface Appliance (WSA) - WSAco

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).