أستكشاف أخطاء الوحدة النمطية Secure Access Roaming Module "؛خدمة السحابة غير متوفرة"؛ أو "؛unprotected"؛ الحالة

المحتويات

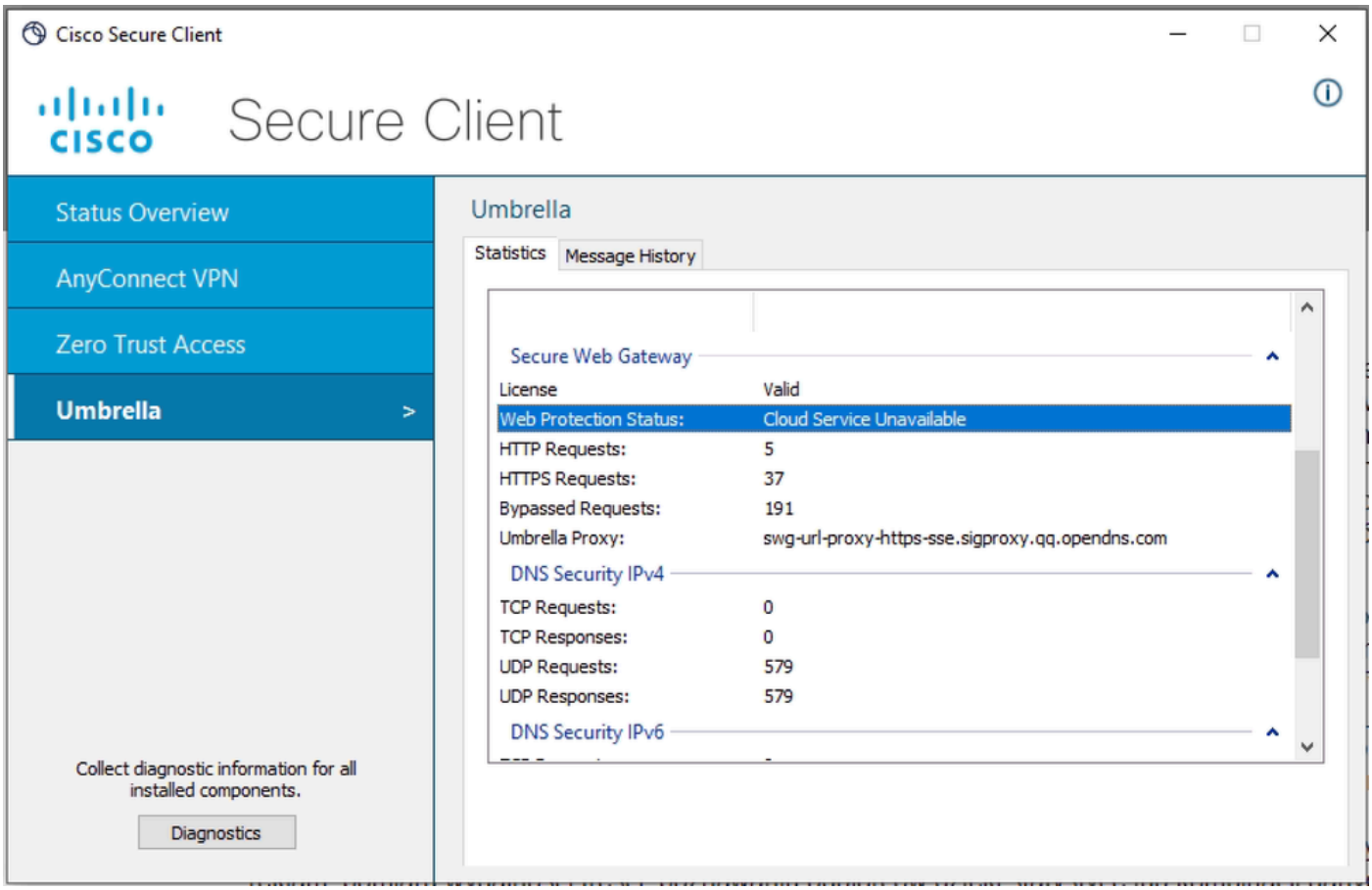
المقدمة

يصف هذا المستند طريقة للتحقيق في السبب الجذري للحالة "خدمة السحابة غير متوفرة" أو "غير محمية" في الوحدة النمطية الجوالة الخاصة بالعميل الآمن.

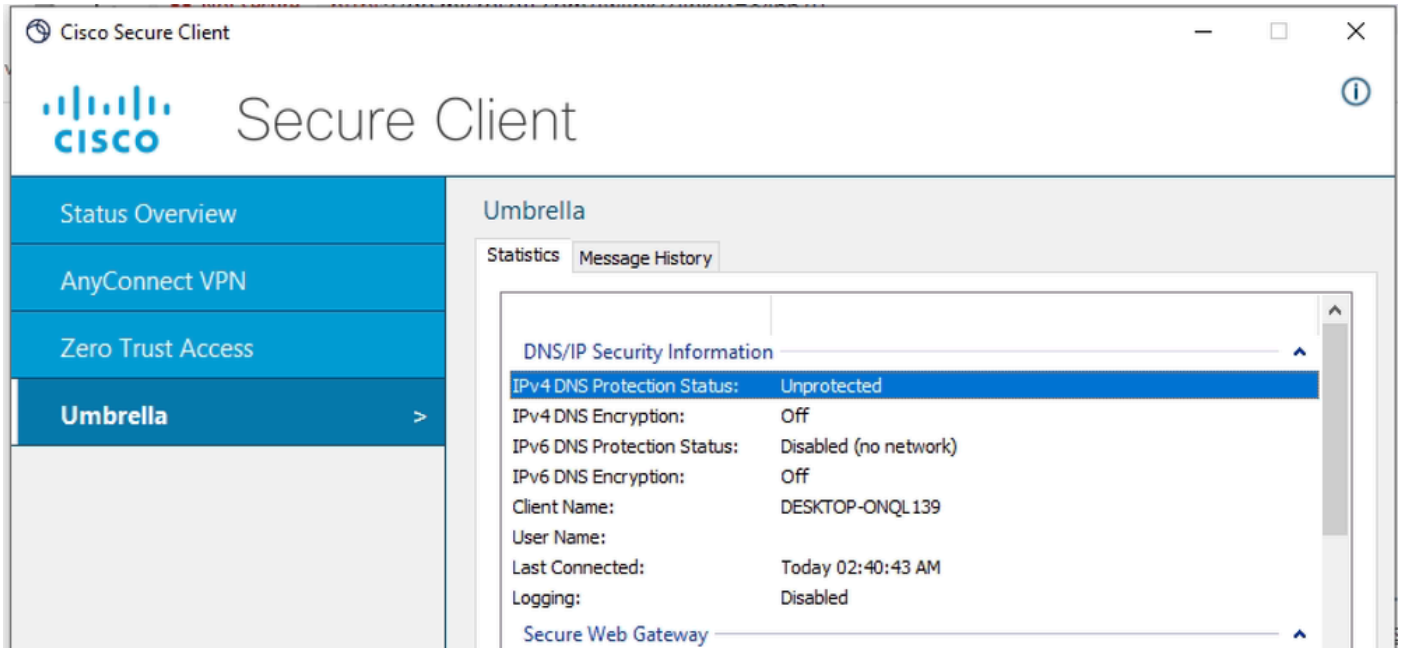
المشكلة

عندما يقوم المستخدم بتشغيل الوحدة النمطية المتجولة الخاصة ب Secure Client ويتوقع إستخدام DNS و/أو حماية الويب، يمكن ملاحظة الحالات الخاطئة في واجهة مستخدم العميل الآمنة:

خدمة السحابة غير متوفرة لحالة حماية الويب



غير محمي لحالة حماية DNS



السبب وراء هذه الأخطاء هو عدم قدرة الوحدة النمطية للتواصل على الاتصال بخدمات السحابة الخاصة بها بسبب مشكل في اتصال الشبكة.

إذا لم يتم ملاحظة هذه المشكلة على جهاز الكمبيوتر العميل المتأثر في الماضي، فهذا يعني أن الشبكة التي يتصل بها جهاز الكمبيوتر مقيدة على الأرجح في بالمتطلبات الموضحة في وثائق SSE

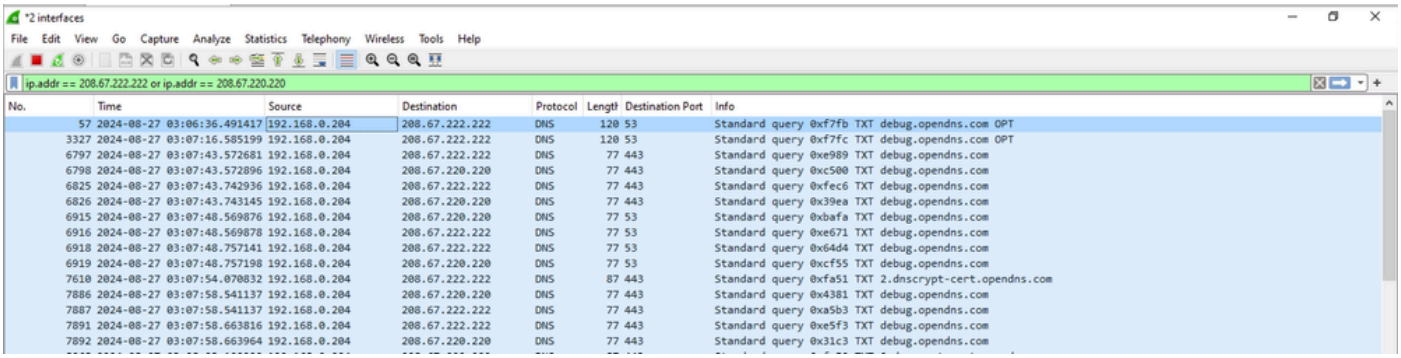
حالة حماية DNS غير محمية

عندما ترى حالة DNS غير المحمية، فمن الأرجح أن الوحدة النمطية المتجولة لا تحتوي على اتصال تدفق البيانات لخوادم OpenDNS (208.67.222.222 و208.67.220.220).
ستر ى سجل الدخول في ملف cscUmbrellaplugin.txt، وهو جزء من حزمة DART.

```
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:43 [8880] [DEBUG] < 13> Dns Protection IPv6 State Machine: rejected all candidate reso
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:53 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: rejected all candidate reso
```

للتحقق من مشاكل الاتصال وتأكيدها مرة أخرى، يمكنك تجميع التقاط الأسلاك على واجهة مخرج المادية للكمبيوتر (WiFi أو Ethernet)، واستخدام مرشح العرض للبحث فقط عن حركة المرور الموجهة إلى تحليلات OpenDNS:

```
ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220
```



كما ترى في القصاصة من Wireshark، من الواضح أن العميل يواصل إرسال استعلامات DNS TXT الموجهة إلى 208.67.222.222 و 208.67.220.220 على UDP ميناء 53 و 443، ولكنه لا يتلقى أي إستجابة.

قد تكون هناك أسباب متعددة وراء هذا السلوك، وعلى الأرجح أن جهاز جدار الحماية المحيط يمنع حركة مرور DNS إلى خادم OpenDNS، أو يسمح فقط لحركة مرور البيانات إلى خوادم DNS معينة.

حالة حماية الويب هي خدمة السحابة غير متوفرة

عندما ترى حالة حماية الويب غير متوفرة للخدمة، فإن الوحدة النمطية المتجولة على الأرجح لا تحتوي على اتصال تدفق البيانات بخوادم بوابة الويب الآمنة.

إذا لم يكن لدى الكمبيوتر اتصال IP بخوادم SWG، فسترى السجل في ملف Umbrella.txt،

والذي يعد جزءا من حزمة DART.

```
Date : 08/27/2024
Time : 06:41:22
Type : Warning
Source : csc_swgagent

Description : WARN | Thread 27cc | TCP handshake to SWG Proxy URL was not successful. Since fail open p
```

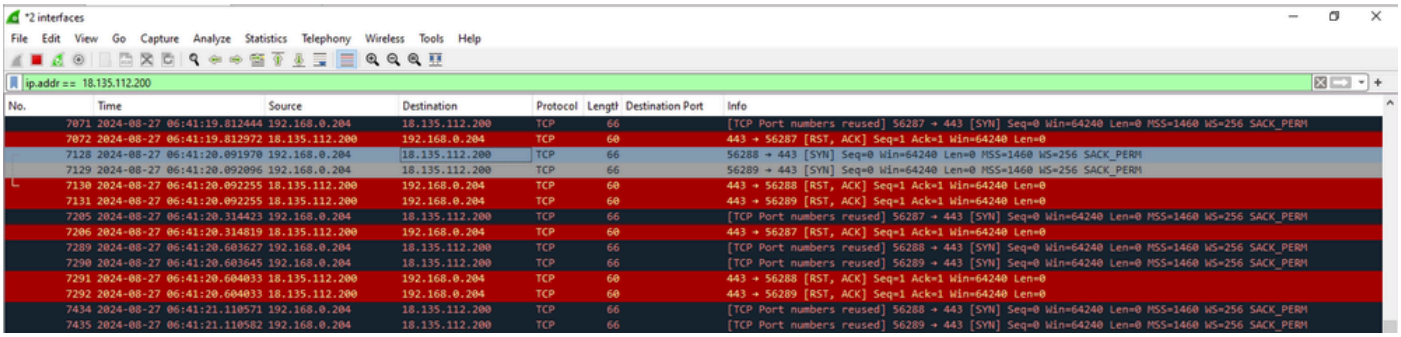
للتحقيق أكثر، قم بجمع التقاط الحزم لإثبات أن الكمبيوتر لا يتضمن اتصال بخادم SWG.
أصدرت الأمر في انتمائية أن يحصل SWG عنوان:

<#root>

```
C:\Users\admin>

nslookup swg-url-proxy-https-sse.sigproxy.qq.opendns.com


Server: ad.lab.local
Address: 192.168.0.65

Non-authoritative answer:
Name: k8s-sigproxy-sigproxy-c8f482b42a-ddf1929ae349b3e5.elb.eu-west-2.amazonaws.com
Address:

18.135.112.200


Aliases: swg-url-proxy-https-sse.sigproxy.qq.opendns.com
swg-proxy_eu-west-2_1_1n.sigproxy.aws.umbrella.com
```

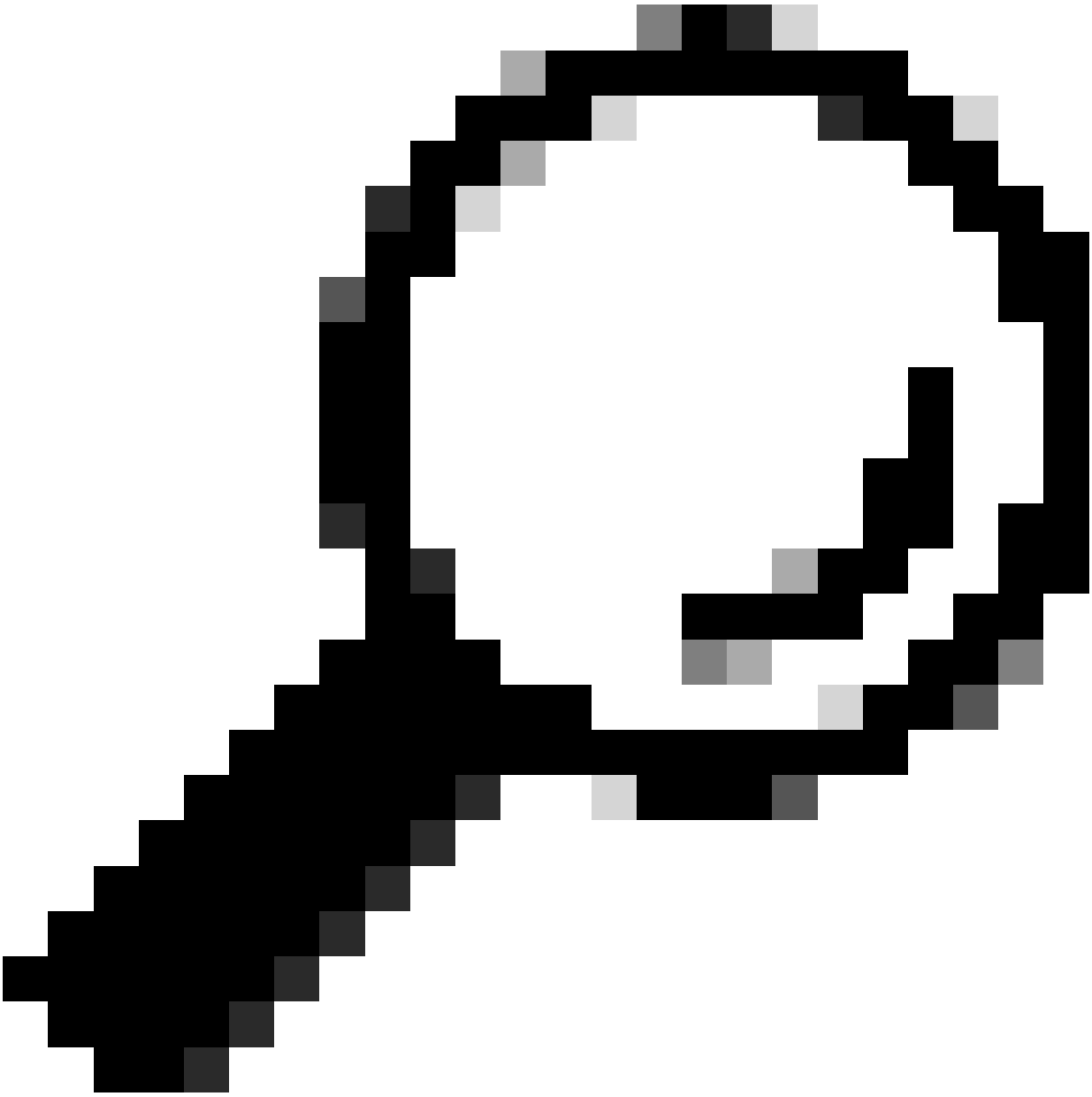
للتحقق من مشاكل الاتصال وتأكيدها، يمكنك تجميع التقاط الأسلاك على واجهة مخرج المادية للكمبيوتر (WiFi أو Ethernet)، واستخدام مرشح العرض للبحث فقط عن حركة المرور الموجهة إلى خادم SWG (إستخدام عنوان IP الذي تم الحصول عليه في الخطوة السابقة)

```
ip.addr == 18.135.112.200
```



كما ترى في التعليمة البرمجية الصغيرة من Wireshark، من الواضح أن العميل يواصل إرسال حزم TCP SYN الموجهة إلى 18.135.112.200، ولكنه يتلقى TCP RST كاستجابة.

في سيناريو المعمل المحدد هذا، كان جدار حماية النطاق يمنع حركة مرور البيانات إلى عنوان IP لـ SWG.
في سيناريو الواقع، يمكنك مشاهدة عمليات إعادة إرسال TCP SYN فقط، وليس TCP RST.



تلميح: إذا لم يتمكن العميل من الوصول إلى خوادم SWG، فإنه بشكل افتراضي في حالة فتح فشل عند خروج حركة مرور ويب من خلال الوصول المباشر إلى الإنترنت (WiFi أو إيثرنت). لا يتم تطبيق حماية الويب في وضع فتح الفشل.

الحل

من أجل التعرف بسرعة على أن الشبكة الأساسية تتسبب في حدوث مشاكل، يمكن للمستخدم الاتصال بأي شبكة مفتوحة أخرى (Hotstop، Home WiFi) لا تحتوي على أي جدار حماية محيط.

لإصلاح خطأ الاتصال المومض، الرجاء التأكد من أن الكمبيوتر لديه اتصال غير مقيد للتحميل كما هو موضح في وثائق SSE.

مشاكل حالة حماية DNS:

- المنفذ 208.67.22.222 TCP/UDP 53
- المنفذ 208.67.220.220 TCP/UDP 53

بالنسبة لمشاكل حالة حماية الويب، تأكد من السماح بحركة مرور البيانات للدخول إلى وثائق SSE - عناوين IP على جدار الحماية المحيط

يعتمد نطاق معين من مدخل عنوان على موقعك.

معلومات ذات صلة

- دليل مستخدم Secure Access
- كيفية تجميع حزمة DART من Cisco Secure Client
- الدعم التقني والمستندات - Cisco Systems

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).