أستكشاف أخطاء تتبع وحدة رؤية الشبكة (NVM) وإصلاحها في تحليلات الشبكة الآمنة AnyConnect

المحتويات

المقدمة

يصف هذا المستند إجراء أستكشاف أخطاء تتبع بيانات وحدة رؤية الشبكة (NVM) وإصلاحها في تحليلات الشبكة الآمنة (SNA).

المتطلبات الأساسية

- معرفة Cisco SNA
- معرفة Cisco AnyConnect

أدلة التكوين

- دليل تكوين ترخيص نقطة نهاية تحليلات الشبكة الآمنة ووحدة رؤية الشبكة (NVM)
- الوحدة النمطية لإمكانية رؤية الشبكة لدليل Cisco AnyConnect Administrator Visibility Module، الإصدار 4.10

المتطلبات

- مدير SNA ومجمع التدفق في الإصدار 7.3.2 أو أحدث
- SNA نقطة نهاية ترخيص
- Cisco AnyConnect مع وحدة رؤية الشبكة 4.3 أو إصدار أحدث

المكونات المستخدمة

- مدير SNA و Flow Collection الإصدار 7.4.0 ونقطة النهاية
- Cisco AnyConnect 4.10.03104 مع VPN وإمكانية رؤية الشبكة
- الوحدة النمطية Windows 10 لنظام التشغيل الظاهري
- الجهاز
- برمجيات وبرنامج تشغيل

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

عملية أستكشاف الأخطاء وإصلاحها

تكوين SNA

التحقق من الترخيص

تأكد من أن الحساب الظاهري للترخيص الذكي الذي تم تسجيل إدارة SNA عليه، لديه ترخيص نقاط النهاية.

التحقق من تطبيق تتبع بيانات NVM

لتأكيد ما إذا كان مجمع تدفق SNA يستلم بيانات تتبع NVM ويدرجها من نقاط النهاية يتم المتابعة كما يلي:

1. سجل الدخول إلى مجمع التدفق عبر SSH أو وحدة التحكم باستخدام بيانات اعتماد **الجذر**.

2. شغل GREP 'NVM يسجل هذه الفترة:' /lancope/var/sw/today/logs/sw.log أمر.

3. من الإخراج المرتجع، تأكد مما إذا كان مجمع التدفق يقوم بإدخال سجلات NVM ويدرجها في قاعدة البيانات.

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:00:01 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:05:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:10:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:15:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
```

من الإخراج، يجب أن يدي أن مجمع التدفق لم يستلم أي سجلات NVM على الإطلاق، ومع ذلك تأكيد ما إذا تم تكوين نقاط النهاية لاستعلام إلى بيانات تتبع NVM.

التحقق من تكوين مجمع التدفق للاستعلام إلى بيانات تتبع NVM

1. سجل الدخول إلى واجهة مستخدم مسؤول مجمع التدفق (UI).

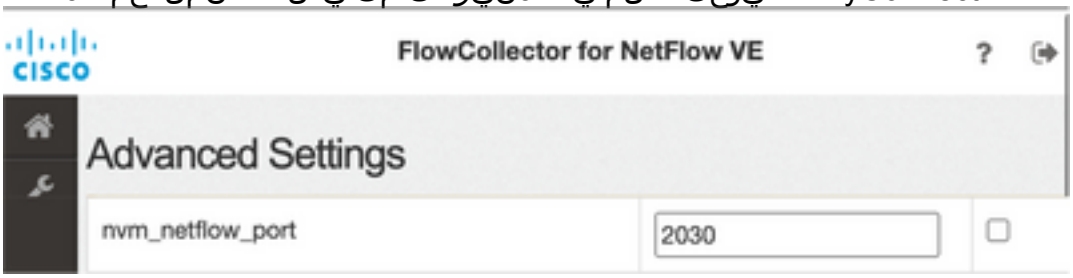
2. انتقل إلى **الدعم > إعدادات متقدمة**.

3. تأكد من تكوين السمات المطلوبة بشكل صحيح:

SNA الإصدار 7.3.2 و 7.4.0

==========

- حدد موقع سمة **nvm_netflow_port** وتحقق من القيمة التي تم تكوينها. يجب أن يتطابق هذا مع المنفذ الذي تم تكوينه في ملف تعريف AnyConnect NVM.



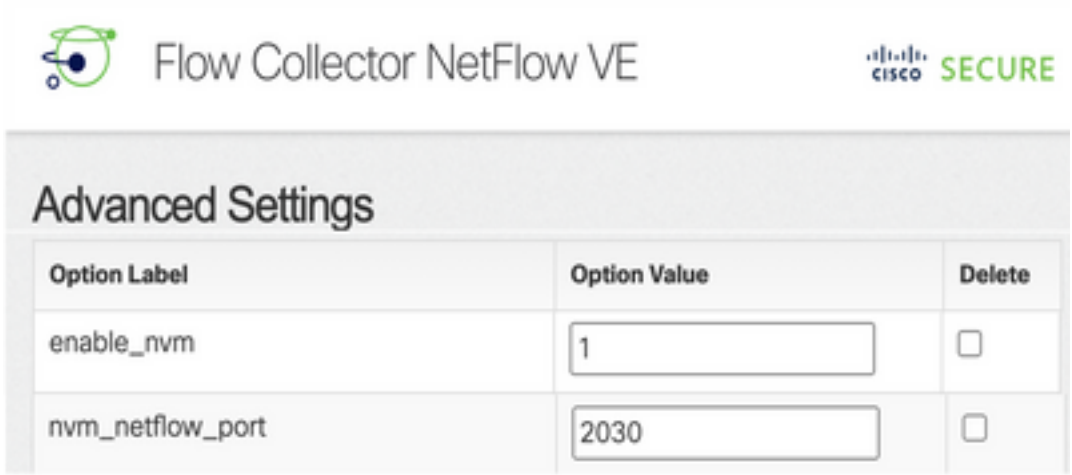
ملاحظة: تأكد من أن المنفذ الذي تم تكوينه هو منفذ غير محجوز وليس 2055 أو 514 أو 8514. إذا كانت القيمة التي تم تكوينها هي "0"، يتم تعطيل الميزة.

ملاحظة: إذا لم يتم عرض حقل، قم بالتمرير إلى أسفل الصفحة. انقر فوق حقل **إضافة خيار جديد**. لمزيد من المعلومات حول الإعدادات المتقدمة في مجمع التدفق، راجع موضوع التعليمات على الإنترنت للإعدادات المتقدمة.

SNA، الإصدار 7.4.1

==========

- حدد موقع سمة **nvm_netflow_port** وتحقق من القيمة التي تم تكوينها. يجب أن يتطابق هذا مع المنفذ الذي تم تكوينه في ملف تعريف AnyConnect NVM.
- حدد موقع سمة **enable_nvm** وتأكد من تعيين القيمة على **1**، وإلا فسيتم تعطيل الميزة.



ملاحظة: تأكد من أن المنفذ الذي تم تكوينه هو منفذ غير محجوز وليس 2055 أو 514 أو 8514.

ملاحظة: إذا لم يتم عرض حقل، قم بالتمرير إلى أسفل الصفحة. انقر فوق حقل **إضافة خيار جديد**. لمزيد من المعلومات حول الإعدادات المتقدمة في مجمع التدفق، راجع موضوع التعليمات على الإنترنت للإعدادات المتقدمة.

4. بمجرد تكوين الإعدادات المتقدمة على مجمع التدفق بشكل صحيح، تحقق مما إذا كان قسم الإجراء كما هو موضح في استخدام نفس باستخدام الآن، تم إستخدامه بعد عن القياس **تتبع NVM من التحقق**.

5. إذا كان تكوين نقطة النهاية مع AnyConnect NVM والإعدادات الموجودة على مجمع التدفق صحيحا، فيجب أن يعكس ملف **sw.log**:

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:35:00 I-pro-t: NVM records this period: received 78 at 0 rps, inserted 78 at 0 rps, discarded
0
04:40:00 I-pro-t: NVM records this period: received 66 at 0 rps, inserted 66 at 0 rps, discarded
0
04:45:00 I-pro-t: NVM records this period: received 91 at 0 rps, inserted 91 at 0 rps, discarded
0
04:50:00 I-pro-t: NVM records this period: received 80 at 0 rps, inserted 80 at 0 rps, discarded
0
```

6. إذا كان مجمع التدفق ال يزال ال يدخل سجالت NVM، فتحقق مما إذا كان مجمع البيانات يستلم الحزم على الواجهة، وعلى أي حال، تأكد من أن تكوين نقاط النهاية صحيح.

تكوين نقطة النهاية

يمكنك نشر وحدة الشبكة الخاصة الظاهرية (NVM) الخاصة ب AnyConnect بإحدى الطريقتين: أ) مع حزمة AnyConnect وأ (ب) مع حزمة NVM المستقلة (على سطح المكتب AnyConnect فقط).

التكوين المطلوب هو نفسه لكل من عمليات النشر، حيث يمكن الفرق في تكوين "اكتشاف الشبكة الموثوق بها".

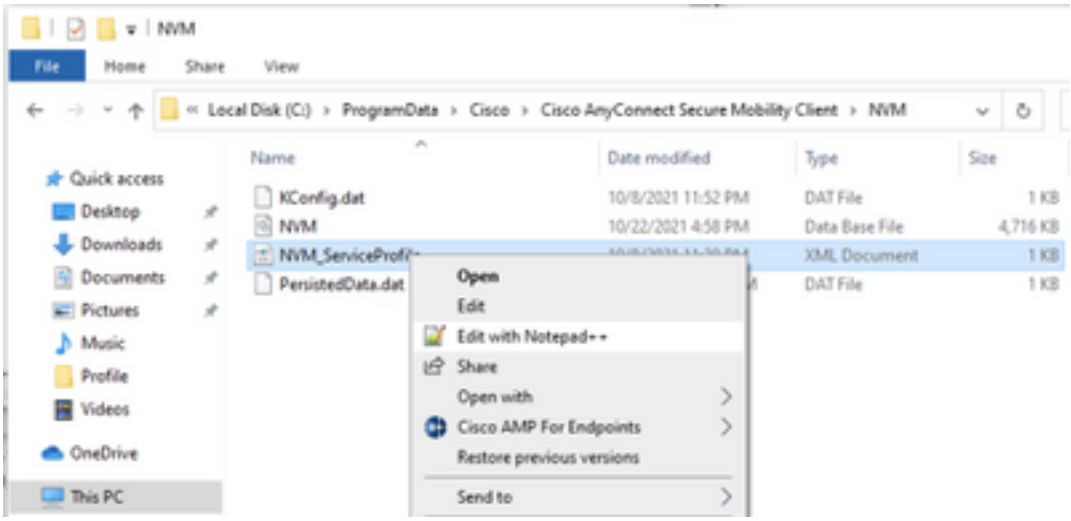
التحقق من ملف تعريف NVM

حدد موقع ملف تعريف NVM المستخدم من قبل نقطة النهاية وتأكد من إعدادات **تكوين مجمع**.

موقع ملف تعريف NVM:

- Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- MAC: /opt/cisco/anyconnect/nvm

ملاحظة: يجب أن يكون اسم ملف تعريف NVM هو NVM_ServiceProfile، وإال فشلت "وحدة رؤية الشبكة" في تجميع البيانات وإرسالها.



يعتمد محتوى ملف تعريف NVM على التكوين الخاص بك، ومع ذلك فإن عناصر ملف التعريف ذات الصلة بـ SNA يتم تعليمها بالخط الغامق. تأكد من مراجعة الملاحظات بعد مثال ملف تعريف NVM:

ملاحظة: تأكد من أن **المنفذ الذي تم تكوينه هو منفذ غير محجوز وليس 2055 أو 514 أو 8514**. يجب أن يكون المنفذ الذي تم تكوينه في ملف التعريف هذا هو نفس المنفذ الذي تم تكوينه في مجمع التدفق.

ملاحظة: تأكد من أنه إذا كان ملف تعريف NVM يحتوي على عنصر XML **الآمن**، فسيتم تعيينه على **false**، وإلا فسيتم تشفير التدفقات باستخدام DTLS ولا يمكن لمجمع التدفق معالجتها.

التحقق من إعدادات اكتشاف الشبكة الموثوق بها (TND)

ترسل الوحدة النمطية لإمكانية رؤية الشبكة معلومات التدفق فقط عندما تكون على الشبكة الموثوق بها. وبشكل افتراضي، لا يتم تجميع أي بيانات. يتم تجميع البيانات فقط عند تكوينها على هذا النحو في ملف التعريف، ويستمر تجميع البيانات عند توصيل نقطة النهاية. إذا تم التجميع على شبكة غير موثوق بها، يتم تخزينها مؤقتا وإرسالها إلى المجمع عندما تكون نقطة النهاية على شبكة موثوق بها. يحتاج مجمع تدفق تحليلات الشبكة الآمنة إلى تكوين إضافي لكي يقوم بمعالجة التدفقات المخزنة مؤقتا

(راجع تكوين مجمع التدفق للتدفقات المخزنة مؤقتا خارج الشبكة للتكوين المطلوب).

يمكن تحديد حالة الشبكة الموثوق بها من خلال ميزة النطاق الترددي العريض (TND) لشبكة VPN (التي تم تكوينها في ملف تعريف شبكة VPN) أو من خلال تكوين النطاق الترددي العريض (TND) في ملف تعريف NVM:

تكوين TND في ملف تعريف VPN

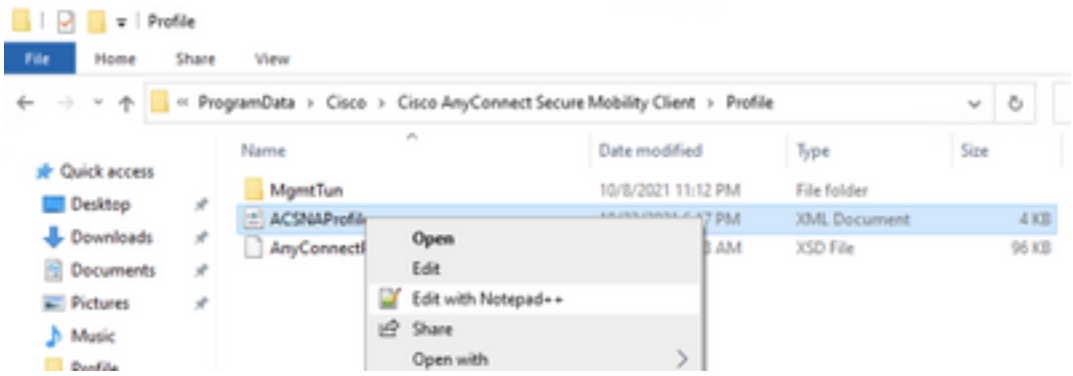
ملاحظة: لا يعد هذا خيارا لعمليات نشر NVM المستقلة.

1. حدد موقع ملف تعريف VPN المستخدم من قبل نقطة النهاية وتأكد من إعدادات **نهج VPN التلقائي** التي تم تكوينها

   موقع ملف تعريف VPN:

   - Windows: **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**
   - MAC: **/opt/cisco/anyconnect/profile**

   في هذا المثال، يسمى ملف تخصيص VPN **ACSNAProfile**.



2. قم بتحرير ملف التخصيص باستخدام محرر نصوص وحدد مكان العنصر **AutoVPNPolicy**. تأكد من صحة النهج الذي تم تكوينه للكشف الناجح عن الشبكة الموثوق بها. في هذه الحالة:

...

ملاحظة: بالنسبة لاتصال NVM: في حالة تعييني كل من نهج الشبكة الموثوق به

ونهج الشبكة غير الموثوق به على عدم القيام بأي شيء، يتم تعطيل اكتشاف VPN.

تكوين TND في ملف تعريف NVM

حدد موقع ملف تعريف NVM المستخدم من قبل نقطة النهاية وتأكد من صحة إعدادات **قائمة الخوادم الموثوق بها** التي تم تكوينها.

موقع ملف تعريف NVM:

- Windows: %ProgramData%\Cisco\AnyConnect Secure Mobility Client\NVM من Cisco
- MAC: /opt/cisco/anyconnect/nvm

...

</NVMProfile>

ملاحظة: يتم إرسال تحقيق SSL إلى وحدة الاستقبال والبث الموثوقة التي تم تكوينها، والتي تستجيب مع شهادة، إذا كان الوصول إليها ممكنا. بعد ذلك يتم تحرير ملف تعريف NVM في مجموعة التجزئة (SHA-256) ومطابقتها مع تجزئة الشهادة المصممة الإبهام إستخراج. يدل التطابق الناجح على أن نقطة النهاية في شبكة موثوق بها، ومع ذلك، إذا كان وحدة الاستقبال والبث غير قابل للوصول، أو إذا لم تتطابق تجزئة الشهادة، عندئذ تعتبر نقطة النهاية في شبكة غير موثوق بها.

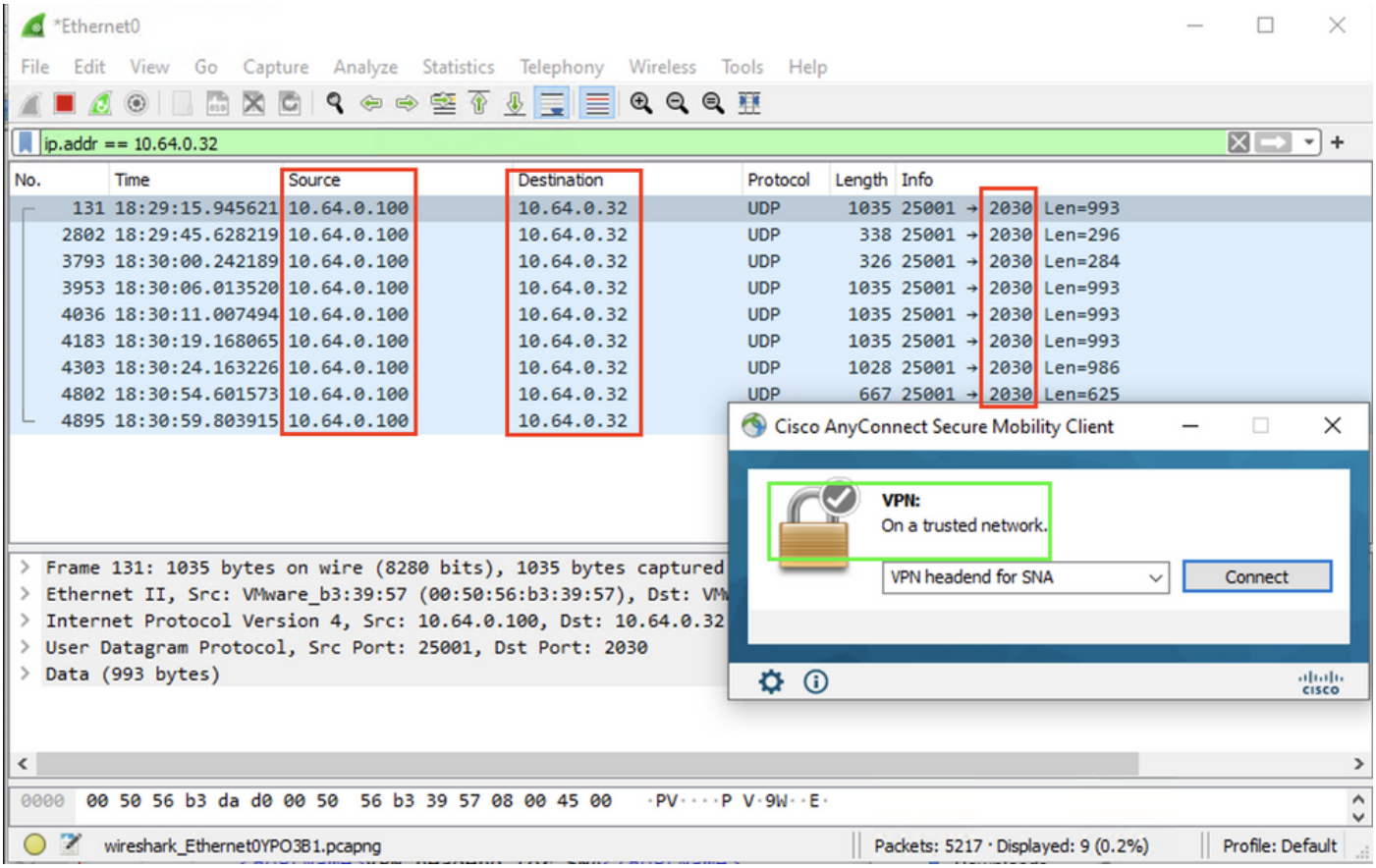
ملاحظة: الخوادم الموثوق بها خلف الوكلاء غير مدعومة.

تجميع التقاط الحزم

يمكنك تجميع التقاط حزمة على محول شبكة نقطة النهاية للتحقق من إرسال التدفقات إلى مجمع التدفق.

أ. إذا كانت نقطة النهاية على شبكة موثوق بها ولكنها غير متصلة بشبكة VPN، فيجب تمكين التقاط على محول الشبكة الفعلي.

في هذه الحالة، يشير عميل AnyConnect إلى أن نقطة النهاية على شبكة موثوق بها، مما يعني أن التدفقات يتم إرسالها إلى مجمع التدفق الذي تم تكوينه عبر المنفذ الذي تم تكوينه من خلال محول الشبكة الداخلية لنقطة النهاية، كما يمكننا أن نرى في نافذة Wireshark المعروضة بعد ذلك ونافذة AnyConnect.

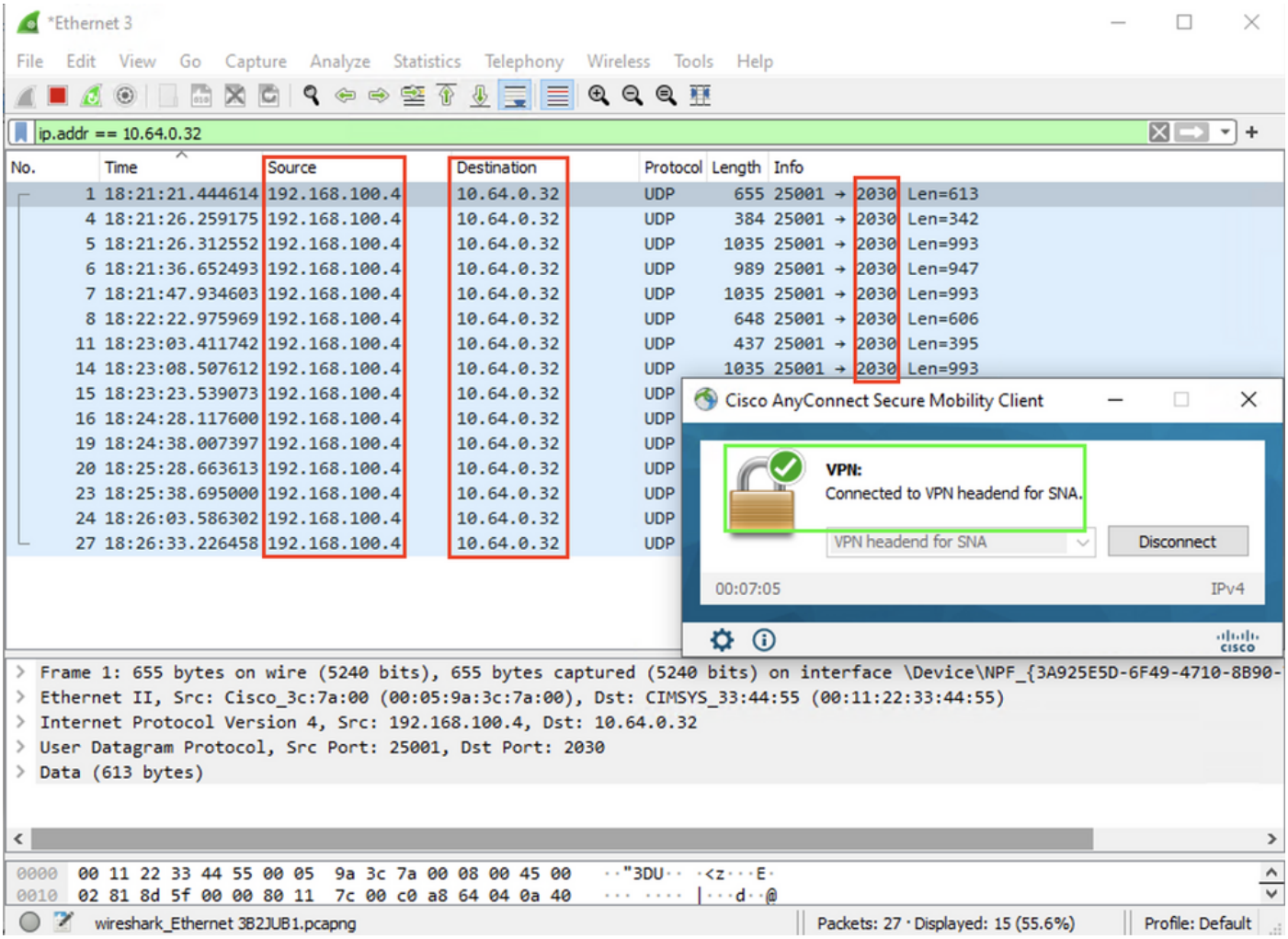


ب. إذا كانت نقطة النهاية متصلة بشبكة AnyConnect VPN، فإنها تعتبر تلقائيا موجودة على الشبكة الموثوق بها، لذلك يجب تمكين الالتقاط على محول الشبكة الظاهرية.

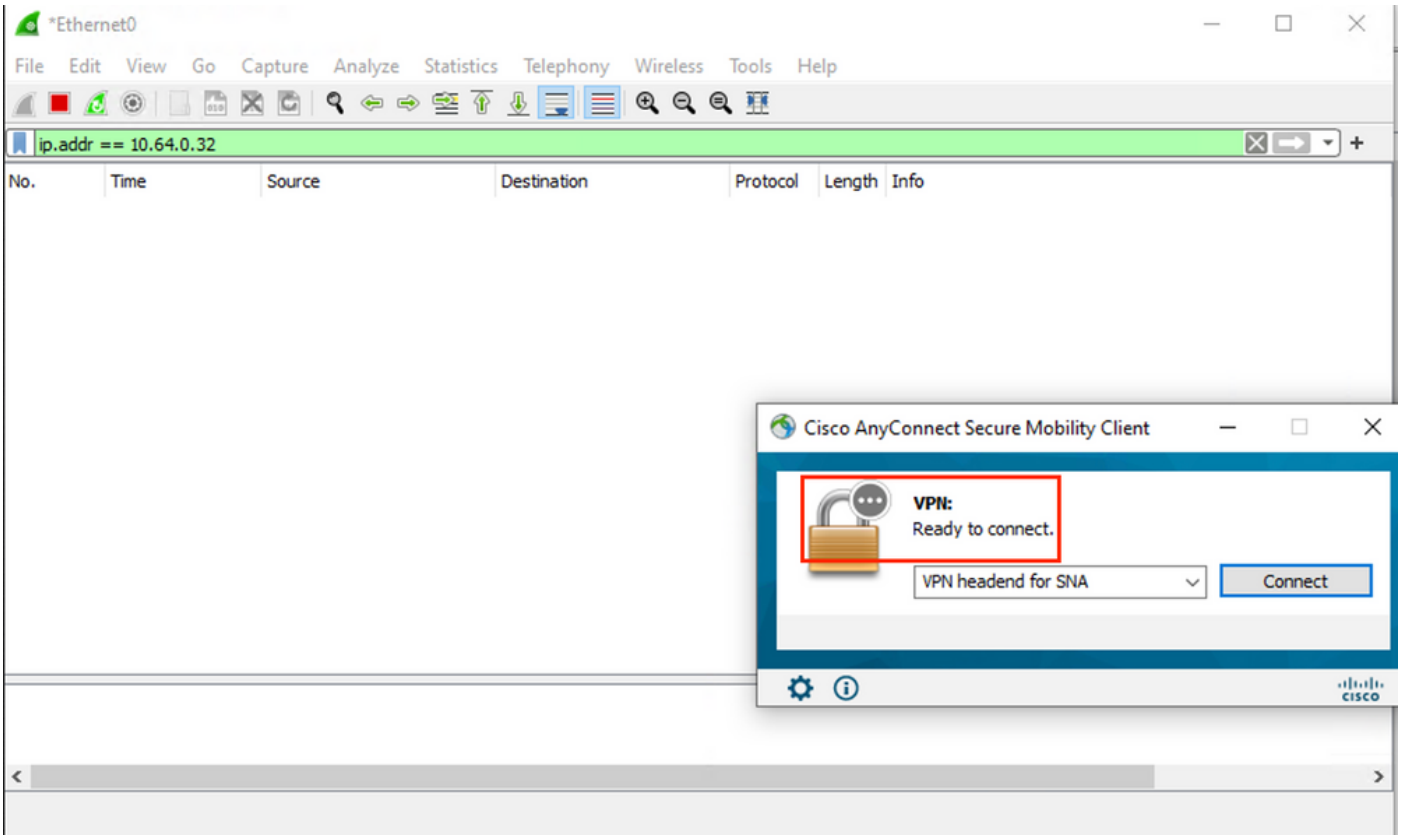
ملاحظة: في حالة تثبيت وحدة VPN النمطية وتكوين TND في ملف تعريف وحدة رؤية الشبكة، تقوم الوحدة النمطية لإمكانية رؤية الشبكة بتنفيذ اكتشاف شبكة موثوق به حتى داخل شبكة VPN.

يشير عميل AnyConnect إلى أن نقطة النهاية متصلة بشبكة VPN، مما يعني أن التدفقات يتم إرسالها إلى مجمع التدفق الذي تم تكوينه عبر المنفذ الذي تم تكوينه من خلال محول الشبكة الظاهرية لنقطة النهاية (نفق VPN)، كما يمكننا أن نرى في نافذة AnyConnect ونافذة Wireshark المعروضة بعد ذلك.

ملاحظة: يجب أن تتضمن تكوين "النفق المقسم" لملف تعريف VPN الذي يتم توصيل نقطة النهاية به عنوان IP الخاص بمجمع التدفق، وإلا فلن يتم إرسال التدفقات عبر نفق VPN.



c. إذا لم تكن نقطة النهاية على شبكة موثوق بها، فلن يتم إرسال التدفقات إلى مجمع التدفق.



عيوب ذات صلة

هناك حاليا إثنان من العيوب المعروفة التي يمكن أن تؤثر على عملية تتبع بيانات تتبع إستخدام NVM على تحليلات الشبكة الآمنة:

- يتعذر على محرك FC إدخال بيانات تتبع NVM على ETH1. رأيت cisco بق id CSCwb84013
- لا يقوم Flow Collector بإدراج سجلات NVM من AnyConnect الإصدار 4.10.04071 وأ إصدارا أعلى. راجع معرف تصحيح الأخطاء من Cisco CSCwb91824

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال دعم Cisco في جميع أنحاء العالم.
- يمكنك أيضا زيارة مجتمع تحليلات الأمان من Cisco هنا.
- 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).