إصلاح اضطرابات تدفق حركة المرور الناجمة عن عمليات إعادة اتصال AnyConnect

المحتويات

المقدمة

يوضح هذا المستند ما يحدث عند إعادة اتصال عميل AnyConnect بجهاز الأمان القابل للتكيف (ASA) في دقيقة واحدة فقط.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

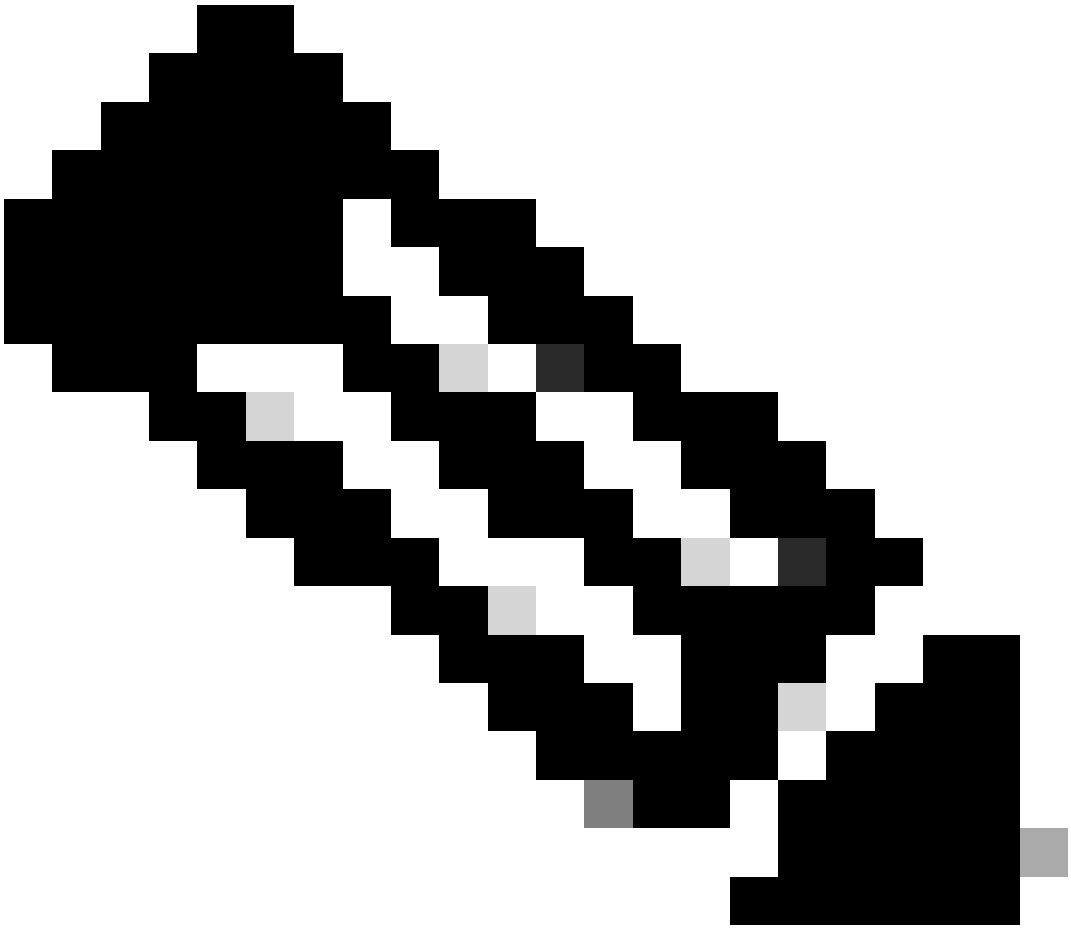
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

هذه المنتجات تأثرت بهذه المشكلة:

- ASA الإصدار 9.17
- AnyConnect Client، الإصدار 4.10

معلومات أساسية

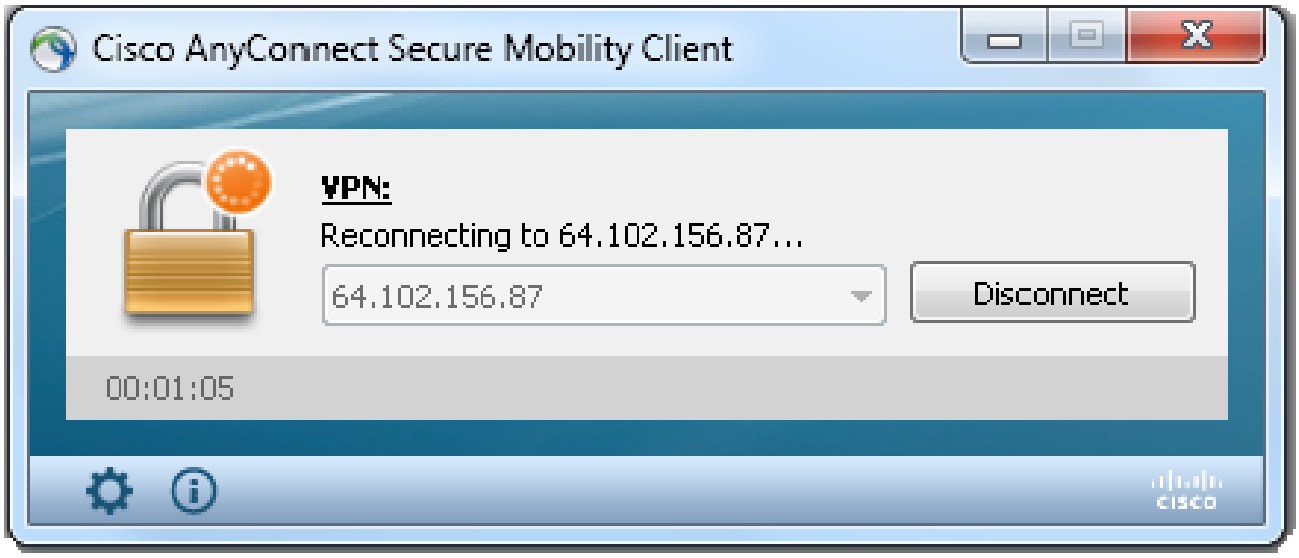


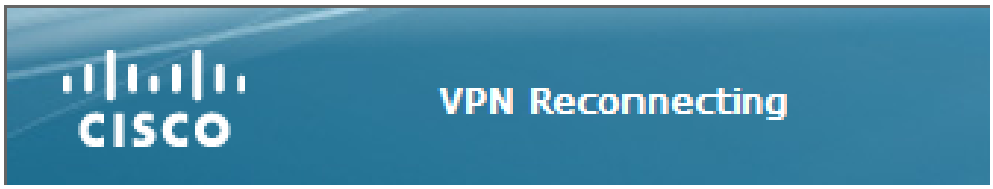
ملاحظة: تمت إعادة تسمية AnyConnect إلى Cisco Secure Client. لم يتغير أي شيء آخر، فقط الاسم، وعملية التثبيت هي نفسها.

إذا قام عميل AnyConnect بإعادة الاتصال بجهاز الأمان القابل للتكيف (ASA) في دقيقة واحدة فقط، فلن يتمكن المستخدمون من إستقبال حركة مرور البيانات عبر نفق أمان طبقة النقل (TLS) حتى تتم إعادة اتصال AnyConnect. ويتوقف ذلك على بضعة عوامل أخرى ترد مناقشتها في هذه الوثيقة.

الأعراض

في هذا المثال، يتم عرض عميل AnyConnect أثناء إعادة إتصاله ب ASA.





رأيت هذا syslog على الـ ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

وصف المشكلة

رأيت هذا التشخيص وأداة Reporting (DART) سجل مع هذا إصدار:

<#root>

```
****************************************

Date         : 11/16/2022
Time         : 01:28:50
Type         : Warning
Source       : acvpnagent

Description : Reconfigure reason code 16:

New MTU configuration.


****************************************

Date         : 11/16/2022
Time         : 01:28:50
Type         : Information
Source       : acvpnagent
```

```
Description : The entire VPN connection is being reconfigured.

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Warning
Source      : acvpnagent

Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.

****************************************
```

الأسباب

سبب هذه المشكلة هو الفشل في إنشاء نفق أمان طبقة نقل مخطط البيانات (DTLS). وقد يكون هذا راجعا إلى سببين:

- تم حظر DTLS في مكان ما في المسار.
- إستخدام منفذ DTLS غير افتراضي.

تم حظر DTLS في مكان ما في المسار

اعتبارا من إصدار ASA 9.x و AnyConnect الإصدار 4.x، تم إدخال تحسين في شكل وحدات الحد الأقصى المميزة للتحول (MTU) التي يتم التفاوض بشأنها ل TLS/DTLS بين العميل/ASA. وفي السابق، كان العميل يستمد تقديرا تقريبيا للنطاق الطرفية المتعددة التي تغطي كل من TLS/DTLS وكان من الواضح أنه أقل من المستوى الأمثل. الآن، يقوم ASA بحساب مصروفات عملية التضمين لكل من TLS/DTLS ويشتق قيم MTU وفقا لذلك.

وطالما تم تمكين DTLS، يطبق العميل وحدة الحد الأقصى للنقل (MTU) ل DTLS (في هذه الحالة 1418) على مهايئ الشبكة الخاصة الظاهرية (الذي يتم تمكينه قبل إنشاء نفق DTLS وهو مطلوب لتنفيذ المهام/عوامل التصفية)، لضمان الأداء الأمثل. إذا تعذر إنشاء نفق DTLS وأ تم إسقاطه عند نقطة ما، يفشل العميل في الاتصال إلى TLS ويضبط وحدة

الحد الأقصى للنقل (MTU) على الجهاز الظاهري (VA) على قيمة TLS MTU (يتطلب ذلك إعادة توصيل مستوى جلسة العمل).

رارق

للقضاء على هذا الانتقال المرئي لـ DTLS > TLS، يمكن للمسؤول تكوين مجموعة نفق مختلفة لـ TLS فقط للوصول للمستخدمين الذين لديهم مشاكل في إنشاء نفق DTLS (مثل بسبب قيود جدار الحماية).

1. الخيار الأفضل هو تعيين قيمة AnyConnect MTU لتكون أقل من قيمة TLS MTU، والتي يتم التفاوض عليها بعد ذلك.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect mtu 1300
```

وهذا يجعل قيم TLS و DTLS MTU متساوية. لا تظهر عمليات إعادة الاتصال في هذه الحالة.

2. الخيار الثاني هو السماح بالتجزئة.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect ssl df-bit-ignore enable
```

باستخدام التجزئة، يمكن تجزئة الحزم الكبيرة (التي يتجاوز حجمها قيمة MTU) وإرسالها من خلال نفق TLS.

3. الخيار الثالث هو تعيين الحد الأقصى لحجم المقطع (MSS) على 1460 كما هو موضح هنا:

```
sysopt conn tcpmss 1460
```

في هذه الحالة، يمكن أن يكون TLS MTU 1427 (RC4/SHA1) وهو أكبر من DTLS MTU 1418 (بفضل AnyConnect) (AES/SHA1/LZS). وهذا يحل المشكلة مع TCP من ASA إلى عميل AnyConnect (MSS)، ولكن يمكن أن تعاني حركة مرور بيانات UDP الكبيرة من ASA إلى عميل AnyConnect بسبب انخفاض MTU. يمكن إسقاطها من قبل عميل AnyConnect لأنه هذا من AnyConnect client MTU 1418. إذا تم تعديل رسائل التحكم في حركة مرور بيانات Sysopt، فقد تؤثر على ميزات أخرى مثل أنفاق (CCPMSS) في الشبكة الفرعية LAN إلى شبكة LAN (L2L) IPSec VPN.

إعادة اتصال سير العمل

لنفترض أن هذه التشفير تم تكوينها:

```
ssl cipher tlsv1.2 custom AES256-SHA256 AES128-SHA256 DHE-RSA-AES256-SHA256
```

هذا التسلسل للأحداث يحدث في هذه الحالة:

- يقوم AnyConnect بإنشاء نفق أصل ونفق بيانات TLS مع AES256-SHA256 كتشفير SSL.
- تم حظر DTLS في المسار ويتعذر إنشاء نفق DTLS.
- يعلن ASA عن معلمات إلى AnyConnect، والتي تتضمن قيم TLS و DTLS MTU، وهما قيمتان منفصلتان.
- DTLS MTU وه 1418 افتراضيا.
- يتم حساب TLS MTU من قيمة sysopt conn tcpmss (الافتراضي وه 1380). هذه هي الطريقة التي يتم بها اشتقاق وحدة الحد الأقصى للنقل (TLS) (كما وه موضح من إخراج Debug webVPN AnyConnect):

```
1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347
```

- يجلب AnyConnect محول الشبكة الخاصة الظاهرية (VPN) ويعين وحدة الحد الأقصى للنقل (DTLS) MTU له تحسبا لإمكانية توصيله عبر DTLS.
- يتم الآن توصيل عميل AnyConnect ويذهب المستخدم إلى موقع ويب معين.
- يرسل المستعرض نظام TCP ويعين MSS = 1418-40 = 1378 في النظام.
- يرسل خادم HTTP الموجود داخل ASA حزم بحجم 1418.
- ال يمكن أن يضعها ASA في النفق والـ يمكن أن يتجزئها حيث أنها لم تتفتت (DF) بت مجموعة.
- يقوم ASA بطباعة الحزم وإسقاطها باستخدام سبب إسقاط MP-SVC-no-fragment-ASP.

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347)
```

- وفي الوقت نفسه، يرسل ASA وجهة ICMP التي يتعذر الوصول إليها، والتجزئة المطلوبة، إلى المرسل:

```
%ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- إذا تم السماح ببروتوكول رسائل التحكم في الإنترنت (ICMP)، يرسل المرسل الحزم المسقطة ويبدأ كل شيء في العمل. إذا تم حظر بروتوكول ICMP، فسيتم حظر حركة المرور على ASA.
- بعد عمليات إرسال متعددة، تتفهم الشركة أنه لا يمكن إنشاء نفق DTLS وتحتاج إلى إعادة تعيين قيمة MTU جديدة لمهايئ الشبكة الخاصة الظاهرية (VPN).
- الغرض من عملية إعادة الاتصال هذه هو تخصيص وحدة الحد الأقصى للنقل (MTU) جديدة.

للحصول على مزيد من المعلومات حول سلوك إعادة الاتصال وأجهزة التوقيت، راجع [الأسئلة المتداولة حول AnyConnect: الأنفاق وسلوك إعادة الاتصال ومؤقت عدم النشاط](#).

معلومات ذات صلة

- [الدعم الفني والتنزيلات من Cisco](#)

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).