سلوك وتنفيذ تجزئة EAP

المحتويات

المقدمة

معلومات أساسية

المتطلبات الأساسية

المتطلبات

تم إرجاع سلسلة الشهادات بواسطة الخادم

سلسلة الشهادات التي تم إرجاعها من قبل المتلقي

مدمج Microsoft Windows الأصلي

الحل

AnyConnect NAM

عميل Microsoft Windows الأصلي مع AnyConnect NAM

تشفير

التجزئة في طبقة IP

التجزئة في RADIUS

التجزئة في EAP-TLS

تأكيد جزء EAP-TLS

أجزاء EAP-TLS يعاد تجميعها بحجم مختلف

سمة RADIUS Framed-MTU

خوادم AAA وسلوك العميل عند إرسال أجزاء EAP

محرك خدمات كشف الهوية (ISE)

خادم نهج شبكة Microsoft (NPS)

AnyConnect

مدمج Microsoft Windows الأصلي

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية فهم جلسات عمل بروتوكول المصادقة الموسع (EAP) واستكشاف أخطائها وإصلاحها.

معلومات أساسية

تم تخصيص أقسام من هذا المستند للتغطية في هذه المجالات:

- سلوك خوادم المصادقة والتفويض والمحاسبة (AAA) عند إرجاع شهادة الخادم لجلسة عمل أمان طبقة النقل - بروتوكول المصادقة الموسع (EAP-TLS)
- سلوك المتضامنين عندما يرجعون شهادة العميل لجلسة EAP-TLS
- قابلية التشغيل البيني عند إستخدام كل من مدمج Microsoft Windows الأصلي ومدير الوصول إلى الشبكة (NAM) من Cisco AnyConnect
- التجزئة في عملية IP و RADIUS و EAP-TLS وإعادة التجميع التي يتم تنفيذها

بواسطة أجهزة الوصول إلى الشبكة
- سمة وحدة الإرسال القصوى ذات الإطار RADIUS (MTU)
- سلوك خوادم AAA عند إجراء تجزئة حزم EAP-TLS

المتطلبات الأساسية

المتطلبات

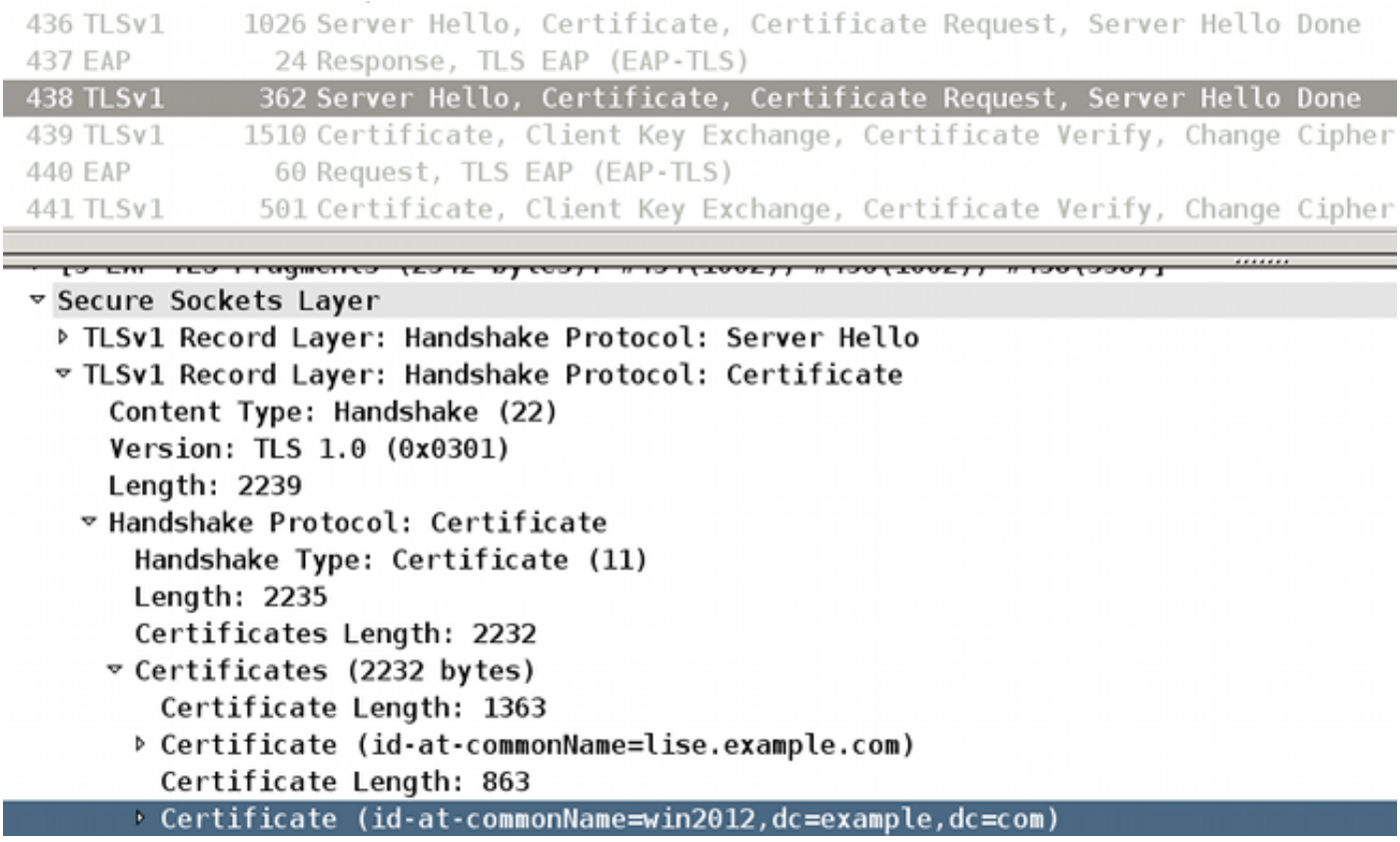
توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- برروتوكولات EAP و EAP-TLS
- تكوين محرك خدمات الهوية من Cisco (ISE)
- CLI تشكيل من cisco مادة حفازة مفتاح

من الضروري فهم EAP و EAP-TLS فهما جيدا من أجل فهم هذه المقالة.

تم إرجاع سلسلة الشهادات بواسطة الخادم

يرجع خادم AAA (خادم التحكم في الوصول (ACS) و ISE) دائما السلسلة الكاملة لحزمة EAP-TLS مع Server Hello وشهادة الخادم:



يتم إرجاع شهادة هوية ISE (الاسم الشائع (CN)=lise.example.com) مع المرجع المصدق (CA) الذي وقع على CN=win2012،dc=example،dc=com. والاختلاف السلوك بالنسبة لكل من ACS و ISE.

سلسلة الشهادات التي تم إرجاعها من قبل المتلقي

ملتمس Microsoft Windows الأصلي

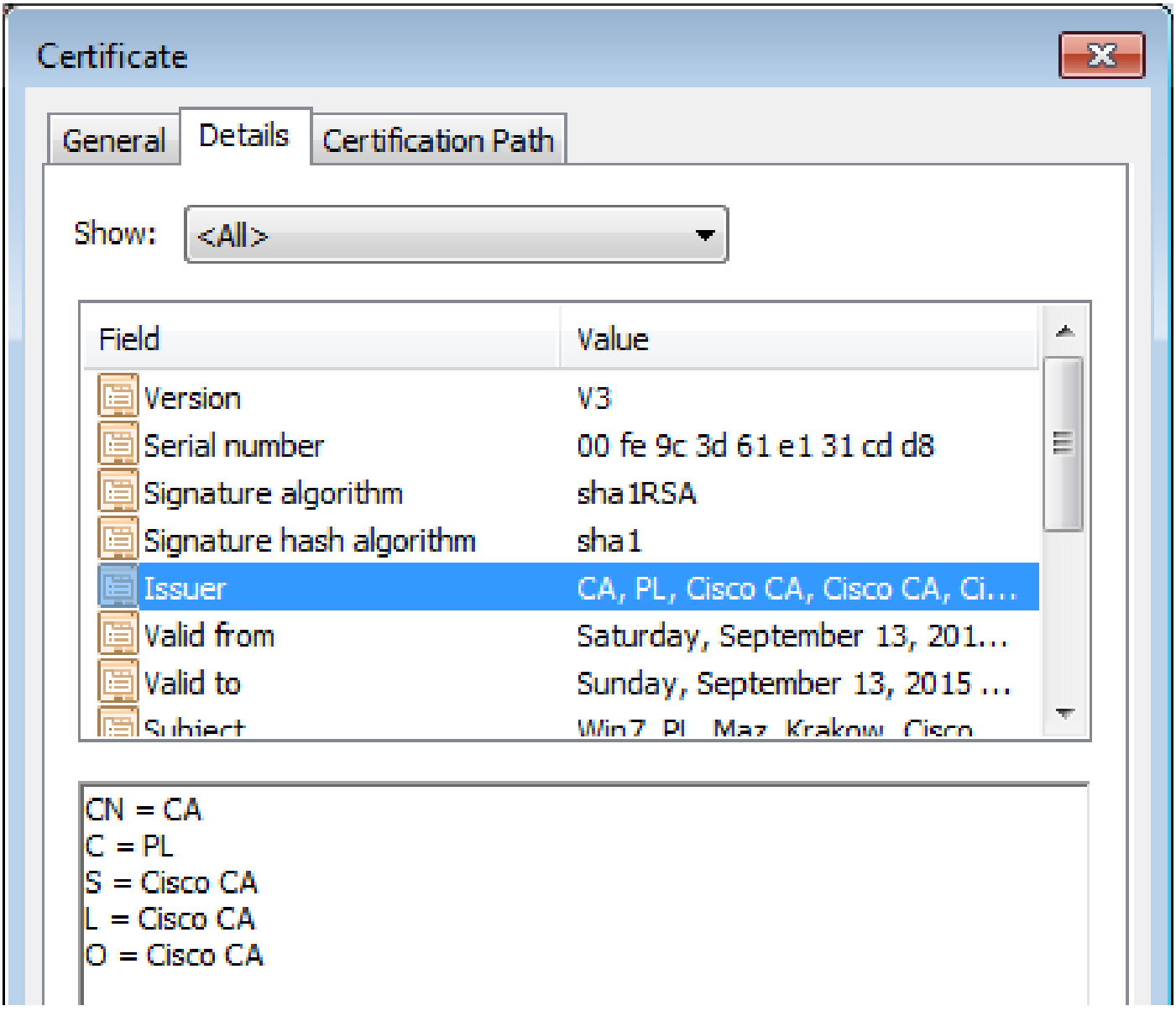
ال يرسل المهالحق الأصلي ل Microsoft Windows 7 الذي تم تكوينه لاستخدام EAP-TLS، مع أو بدون "تحديد الشهادة البسيط"، السلسلة الكاملة لشهادة العميل.

يحدث هذا السلوك حتى عندما تكون شهادة العميل موقعة من مرجع مصدق (سلسلة مختلفة) مختلف عن شهادة الخادم.

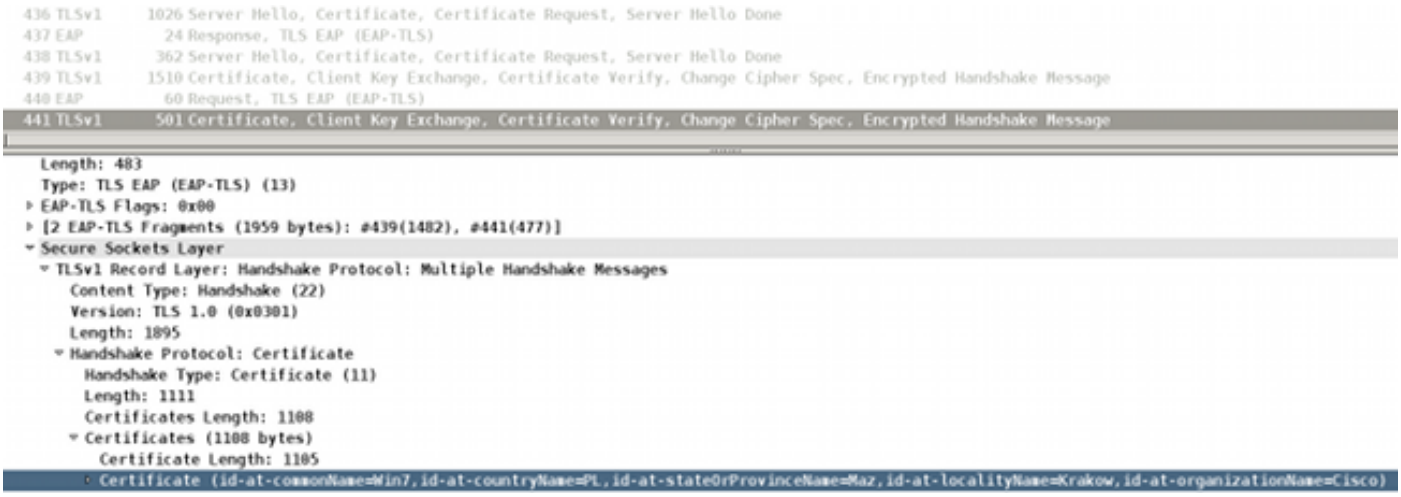
هذا المثال متعلق ب Server Hello و Certificate المقدمين في لقطة الشاشة السابقة.

بالنسبة لذلك السيناريو، يتم توقيع شهادة ISE من قبل CA باستخدام اسم الموضوع، CN=win2012،dc=example،dc=com.

غير أن شهادة المستخدم المثبتة في مخزن Microsoft موقعة من مرجع مصدق مختلف، CN=CA،C=PL،S=Cisco CA،L=Cisco CA، o=Cisco CA.



ونتيجة لذلك، يستجيب طالب Microsoft Windows لشهادة العميل فقط. CA الذي يوقع عليه (CN=CA،S=PL،S=Cisco CA، L=Cisco CA، o=Cisco CA) غير مرفق.



وبسبب هذا السلوك، من المحتمل أن تواجه خوادم AAA مشاكل عند التحقق من شهادات العميل. يتعلق المثال بنظام التشغيل Microsoft Windows 7 SP1 Professional.

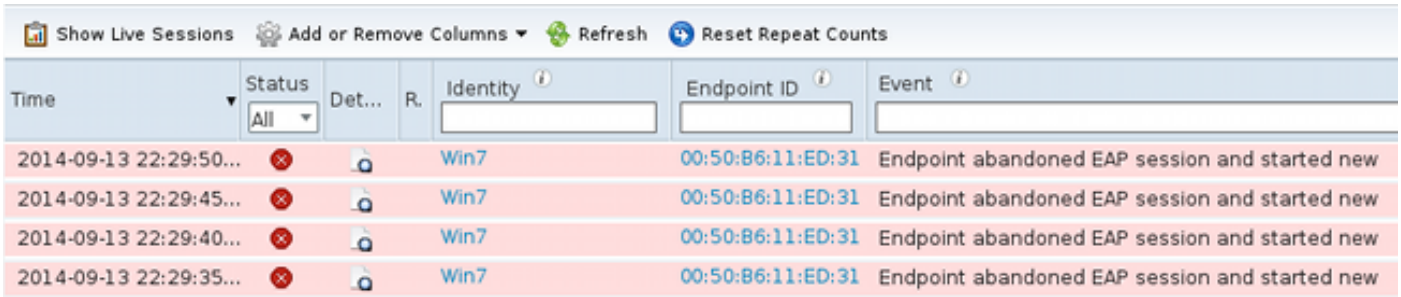
الحل

يجب تثبيت سلسلة شهادات كاملة على مخزن شهادات ACS و ISE (كافة شهادات عميل توقيع CA و CA الفرعي).

يمكن اكتشاف مشكلات التحقق من صحة الشهادة بسهولة على ACS أو ISE. يتم تقديم المعلومات حول الشهادة غير الموثوق بها وتقارير ISE:

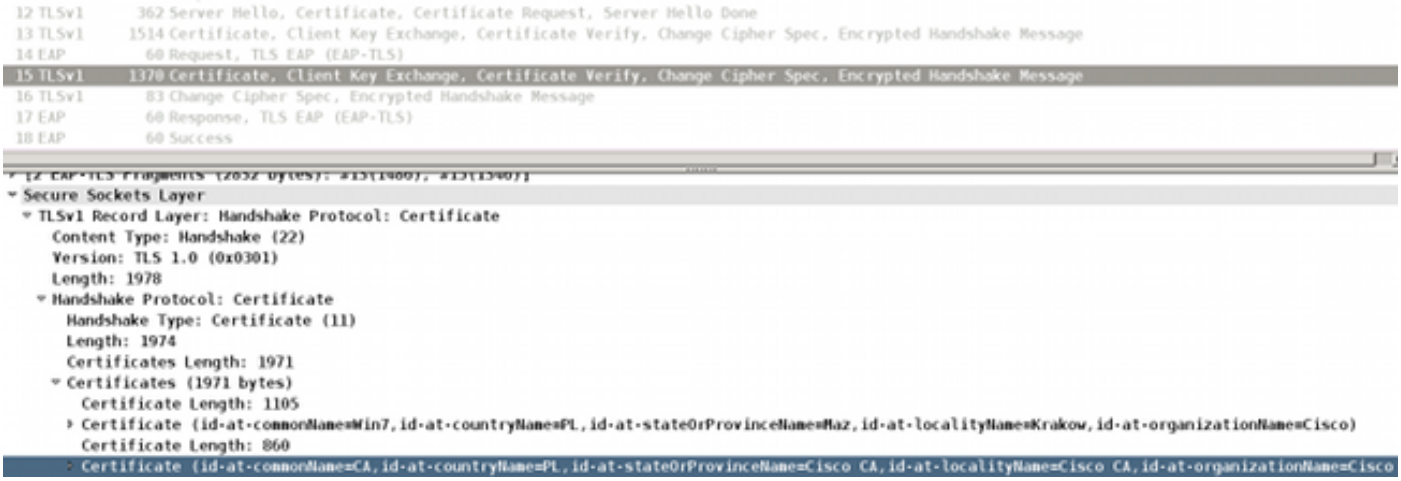
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

لا يمكن بسهولة اكتشاف المشاكل المتعلقة بالتحقق من صحة الشهادة على مقدم الطلب. يستجيب خادم AAA عادة بأن "نقطة النهاية لجلسة EAP":



AnyConnect NAM

لا تحتوي AnyConnect NAM على هذا الحد. وفي السيناريو نفسه، تقوم بإرفاق السلسلة الكاملة لشهادة العميل (يتم إرفاق المرجع المصدق الصحيح):



عميل Microsoft Windows الأصلي مع AnyConnect NAM

عندما تكون كلتا الخدمتين قيد التشغيل، تكون الأولوية لـ AnyConnect NAM.

حتى في حالة عدم تشغيل خدمة NAM، فإنها تظل متصلة بـ Microsoft Windows API وتعيد حزم EAP، مما قد يسبب مشاكل للمطالب الأصلي لـ Microsoft Windows.

وإليكم مثال على مثل هذا الفشل.

يمكنك تمكين التتبع على Microsoft Windows باستخدام هذا الأمر:

```
C:\netsh ras set tracing * enable
```

تظهر الآثار (c:\windows\trace\svchost_RASTLS.LOG):

<#root>

```
[2916] 09-14 21:29:11:254: >> Received Request (Code: 1) packet: Id: 55, Length:
6, Type: 13, TLS blob length: 0. Flags: S
[2916] 09-14 21:29:11:254: << Sending Response (Code: 2) packet: Id: 55, Length:
105, Type: 13, TLS blob length: 95. Flags: L
[1804] 09-14 21:29:11:301: >> Received Request (Code: 1) packet: Id: 56, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[1804] 09-14 21:29:11:301: << Sending Response (Code: 2) packet: Id: 56, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:348: >> Received Request (Code: 1) packet: Id: 57, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[1804] 09-14 21:29:11:348: << Sending Response (Code: 2) packet: Id: 57, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: >> Received Request (Code: 1) packet: Id: 58, Length:
344, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: << Sending Response (Code: 2) packet: Id: 58, Length:
1492, Type: 13, TLS blob length: 1819. Flags: LM
[3084] 09-14 21:31:11:203: >> Received Request (Code: 1) packet: Id: 122, Length:
6, Type: 13, TLS blob length: 0. Flags: S
[3084] 09-14 21:31:11:218: << Sending Response (Code: 2) packet: Id: 122, Length:
105, Type: 13, TLS blob length: 95. Flags: L
```

```
[3420] 09-14 21:31:11:249: >> Received Request (Code: 1) packet: Id: 123, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[3420] 09-14 21:31:11:249: << Sending Response (Code: 2) packet: Id: 123, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 124, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[3420] 09-14 21:31:11:281: << Sending Response (Code: 2) packet: Id: 124, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 125, Length:
344, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:296: <<

Sending Response (Code: 2)

 packet: Id: 125, Length:

1492

, Type: 13,

TLS blob length: 1819. Flags: LM
```

الحزمة الأخيرة هي شهادة عميل (EAP-TLS جزء 1 بحجم EAP 1492) مرسلة من قبل طالب Microsoft Windows الأصلي. لسوء الحظ، لا يعرض Wireshark هذه الحزمة:

	Protocol	Length	Info
8	EAP	48	Response, Identity
9	EAP	60	Request, TLS EAP (EAP-TLS)
10	SSL	123	Client Hello
11	TLSv1	1030	Server Hello, Certificate, Certificate Request, Server Hello Done
12	EAP	24	Response, TLS EAP (EAP-TLS)
13	TLSv1	1026	Server Hello, Certificate, Certificate Request, Server Hello Done
14	EAP	24	Response, TLS EAP (EAP-TLS)
15	TLSv1	362	Server Hello, Certificate, Certificate Request, Server Hello Done
20	TLSv1	362	Ignored Unknown Record
28	TLSv1	362	Ignored Unknown Record

وهذه الحزمة التي تم إرسالها حقا، أما الجزء الأخير فكان الجزء الثالث من EAP-TLS الذي يحمل شهادة خادم.

تم إستهلاكه من قبل وحدة AnyConnect NAM المتصلة بواجهة برمجة تطبيقات Microsoft Windows.

ولهذا السبب لا يوصى باستخدام AnyConnect مع طالب Microsoft Windows الأصلي.

عند إستخدام أي خدمات AnyConnect، يوصى باستخدام NAM أيضا (عند الحاجة إلى خدمات 802.1x)، وليس مدمج Microsoft Windows الأصلي.

تشظية

من المحتمل أن يحدث التجزئة على طبقات متعددة:

- IP

- أزواج قيمة سمة RADIUS (AVP)
- EAP-TLS

محولات Cisco IOS® ذكية جدا. يمكنهم فهم تنسيقات EAP و EAP-TLS.

وعلى الرغم من أن المحول غير قادر على فك تشفير نفق TLS، فإنه مسؤول عن التجزئة، وتجميع وإعادة تجميع حزم EAP عند التضمين في بروتوكول المصادقة المتوسع عبر الشبكة المحلية (LAN) أو RADIUS.

ال يدعم بروتوكول EAP التجزئة. فيما يلي مقتطف من RFC 3748 (EAP):

"ال يتم دعم التجزئة داخل EAP نفسه، ومع ذلك، قد تدعم أساليب EAP الفردية هذا الأمر."

EAP-TLS هو مثال. فيما يلي مقتطف من RFC 5216 (EAP-TLS)، القسم 2.1.5 (التجزئة):

"عندما يستلم نظير EAP-TLS حزمة EAP-Request مع مجموعة بت M، يجب أن يستجيب مع EAP-Response باستخدام EAP-type=EAP-TLS وبدون بيانات.

هذا يعمل كخاتم. يجب أن ينتظر خادم EAP حتى يستلم إستجابة EAP قبل إرسال جزء آخر.

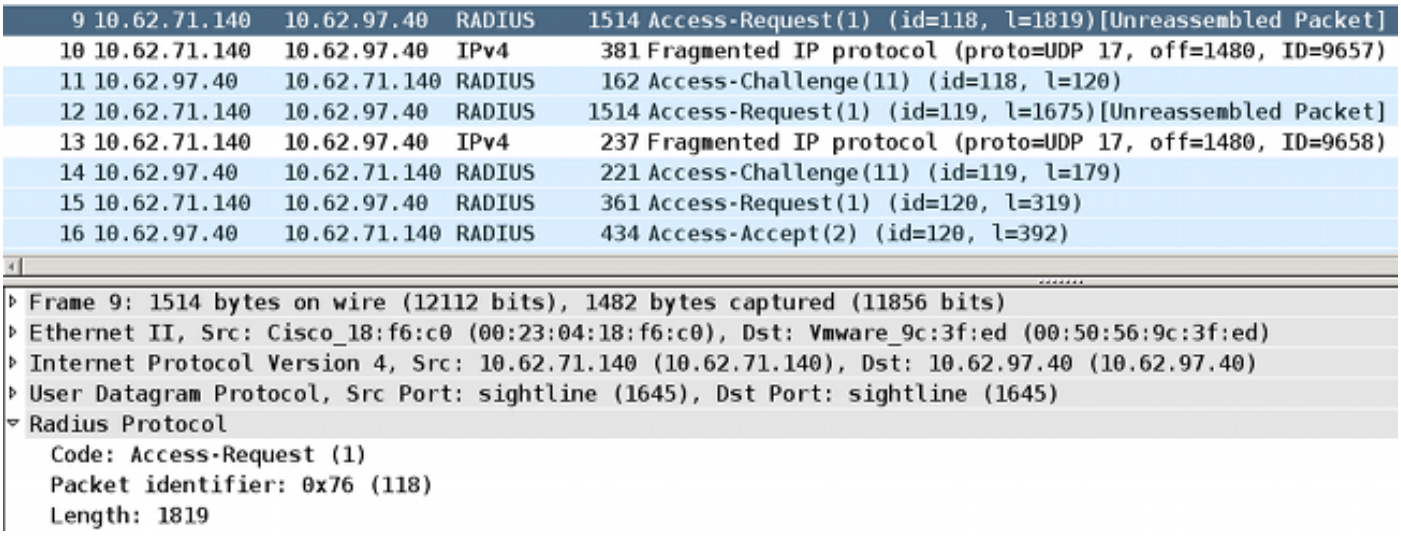
تصف الجملة الأخيرة ميزة مهمة للغاية لخوادم AAA. ويجب عليهم انتظار ACK قبل أن يتمكنوا من إرسال جزء EAP آخر. وتستخدم قاعدة مماثلة للمطالب:

"يجب أن ينتظر نظير EAP حتى يستلم طلب EAP قبل إرسال جزء آخر."

التجزئة في طبقة IP

يمكن أن يحدث التجزئة فقط بين جهاز الوصول إلى الشبكة (NAD) وخادم AAA (IP/UDP/RADIUS المستخدم كنقل).

ويحدث هذا الموقف عندما يحاول NAD (محول Cisco IOS) إرسال طلب RADIUS الذي يحتوي على حمولة EAP، والتي تكون أكبر من MTU للواجهة:

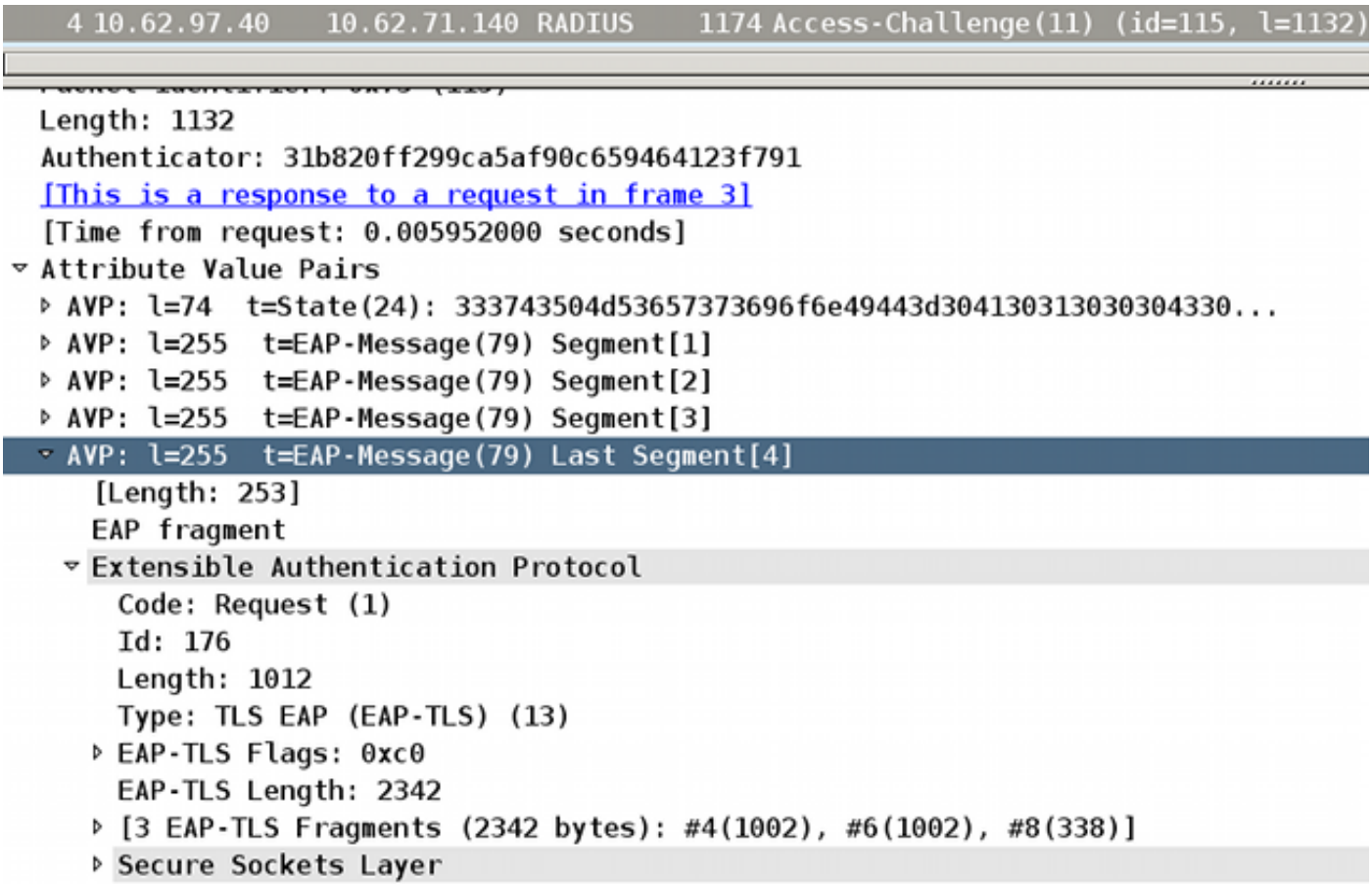


معظم إصدارات Cisco IOS ليست ذكية بشكل كاف والا تحاول تجميع حزم EAP المستلمة عبر EAPoL وتجميعها في حزمة RADIUS التي يمكن أن تلائم في وحدة الحد الأقصى للنقل (MTU) للواجهة المادية تجاه خادم AAA.

خوادم AAA أكثر ذكاء (كما هو موضح في الأقسام التالية).

التجزئة في RADIUS

هذا ليس حقا أي نوع من التجزئة. طبقا ل RFC 2865، يمكن أن يكون لسمة RADIUS واحدة ما يصل إلى 253 بايت من البيانات.ولهذا السبب، فإن حمولة EAP تنتقل دائما في سمات RADIUS متعددة لرسالة EAP:



يعاد تجميع سمات رسالة EAP هذه وتفسيرها بواسطة Wireshark (تكشف سمة "Last Segment" حمولة حزمة EAP بأكملها).

رأس الطول في حزمة EAP يساوي 1،012، ويتطلب أربعة RADIUS AVPs لنقله.

التجزئة في EAP-TLS

من لقطة الشاشة نفسها، يمكنك أن ترى ما يلي:

- طول حزمة EAP هو 1،012
- يبلغ طول EAP-TLS 2،342

وهذا يشير إلى أنها أول جزء من EAP-TLS ويتوقع المطالب المزيد، والذي يمكن تأكيده إذا فحصت عالمات EAP-TLS:

```
Length: 1012
Type: TLS EAP (EAP-TLS) (13)
▾ EAP-TLS Flags: 0xc0
    1... .... = Length Included: True
    .1.. .... = More Fragments: True
    ..0. .... = Start: False
EAP-TLS Length: 2342
```

يحدث هذا النوع من التجزئة غالبا في:

- تحدي الوصول إلى RADIUS الذي يتم إرساله بواسطة خادم AAA، والذي يحمل طلب EAP مع شهادة خادم طبقة مآخذ التوصيل الآمنة (SSL) مع السلسلة بأكملها.
- يرسل RADIUS Access-Request بواسطة NAD، الذي يحمل إستجابة EAP مع شهادة عميل SSL مع السلسلة بأكملها.

تأكيد جزء EAP-TLS

وكما أوضح سابقا، يجب الاعتراف بكل جزء من EAP-TLS قبل إرسال الأجزاء اللاحقة.

وفيما يلي مثال (التقاط الحزم ل EAPoL بين المتلقي و NAD):

No.	Protocol	Length	Info
5	EAP	60	Response, Identity
6	EAP	60	Request, TLS EAP (EAP-TLS)
7	TLSv1	138	Client Hello
8	TLSv1	1030	Server Hello, Certificate, Certificate Request, Server Hello Done
9	EAP	60	Response, TLS EAP (EAP-TLS)
10	TLSv1	1026	Server Hello, Certificate, Certificate Request, Server Hello Done
11	EAP	60	Response, TLS EAP (EAP-TLS)
12	TLSv1	362	Server Hello, Certificate, Certificate Request, Server Hello Done
13	TLSv1	1514	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
14	EAP	60	Request, TLS EAP (EAP-TLS)
15	TLSv1	1370	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
16	TLSv1	83	Change Cipher Spec, Encrypted Handshake Message
17	EAP	60	Response, TLS EAP (EAP-TLS)

```
▸ Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: GoodWayI_11:ed:31 (00:50:b6:11:ed:31), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 6
  ▾ Extensible Authentication Protocol
      Code: Response (2)
      Id: 176
      Length: 6
      Type: TLS EAP (EAP-TLS) (13)
    ▸ EAP-TLS Flags: 0x00
```

ترجع إطارات EAPoL وخادم AAA شهادة الخادم:

- يتم إرسال هذه الشهادة في جزء EAP-TLS (الحزمة 8).
- يتعرف الطالب على هذا الجزء (الحزمة 9).
- ويرسل الجزء الثاني من EAP-TLS بواسطة NAD (الحزمة 10).
- يتعرف الطالب على هذا الجزء (الحزمة 11).
- تتم إعادة توجيه الجزء الثالث من EAP-TLS بواسطة NAD (الحزمة 12).
- والي يلزم أن يقر الملتمس بذلك؛ بل إنه يتقدم بشهادة العميل التي تبدأ في الحزمة 13.

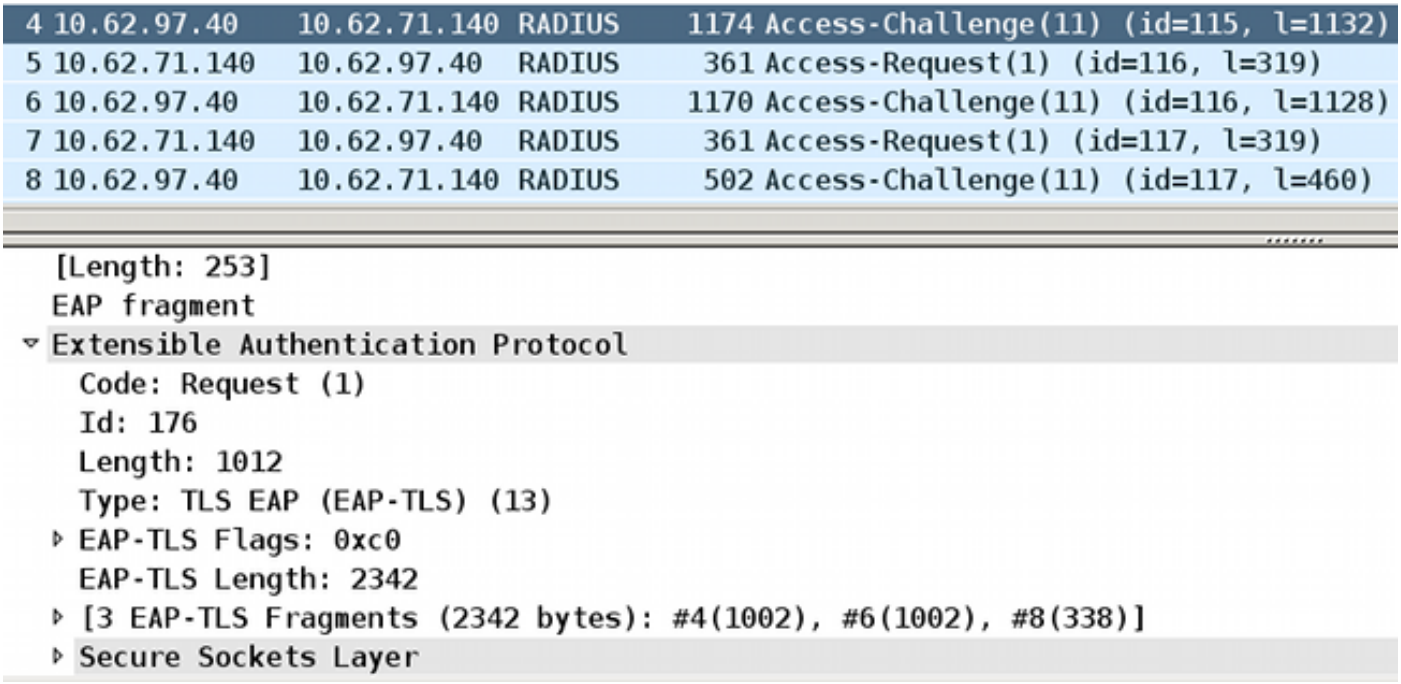
فيما يلي تفاصيل الحزمة 12:

```
   12 TLSv1      362 Server Hello, Certificate, Certificate Request, Server Hello Done
▸ Frame 12: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits)
▸ Ethernet II, Src: Cisco_e1:d8:11 (d4:a0:2a:e1:d8:11), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 344
  ▾ Extensible Authentication Protocol
      Code: Request (1)
      Id: 178
      Length: 344
      Type: TLS EAP (EAP-TLS) (13)
    ▸ EAP-TLS Flags: 0x00
    ▸ [3 EAP-TLS Fragments (2342 bytes): #8(1002), #10(1002), #12(338)]
    ▾ Secure Sockets Layer
      ▸ TLSv1 Record Layer: Handshake Protocol: Server Hello
      ▸ TLSv1 Record Layer: Handshake Protocol: Certificate
      ▸ TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
```

يمكنك أن ترى أن Wireshark أعاد تجميع الحزم 8، 10، و 12.

وحجم أجزاء EAP هو 1،002 و 1،002 و 338، مما يجعل الحجم الإجمالي لرسالة EAP-TLS يبلغ 2342؛

يتم الإعلان عن إجمالي طول رسالة EAP-TLS في كل جزء. ويمكن تأكيد ذلك إذا قمت بفحص حزم RADIUS (بين NAD وخادم AAA):



يحمل حزم RADIUS أرقام 4 و 6 و 8 هذه الأجزاء الثلاثة من EAP-TLS. ويتم الاعتراف بالجزأين الأولين.

يستطيع Wireshark تقديم المعلومات حول أجزاء EAP-TLS (الحجم: 1،002 + 1،002 + 338 = 2،342).

كان هذا السيناريو والمثال سهلا. لم يكن محول Cisco IOS بحاجة إلى تغيير حجم جزء EAP-TLS.

إعادة تجميع أجزاء EAP-TLS بحجم مختلف

ضع في الاعتبار ما يحدث عندما يكون NAD MTU تجاه خادم AAA 9000 بايت (إطار كبير) ويكون خادم AAA أيضا متصلا باستخدام الواجهة التي تدعم الإطارات كبيرة الحجم.

يرتبط معظم المقلمات النموذجية باستخدام إرتباط بسرعة 1 جيجابت ذي وحدة الحد الأقصى للنقل (MTU) تبلغ 1500.

في مثل هذا السيناريو، يتجز محول Cisco IOS تجميع EAP-TLS "assymetric" وإعادة تجميعه ويغير أحجام أجزاء EAP-TLS.

وفيما يلي مثال على رسالة EAP كبيرة الحجم مرسلة من خادم AAA (شهادة خادم SSL):

1. يجب أن يرسل خادم AAA رسالة EAP-TLS مع شهادة خادم SSL. يبلغ الحجم الإجمالي لحزمة EAP هذه 3000. بعد تضمينها في RADIUS Access-Challenge/UDP/IP، فإنها لا تزال أقل من وحدة الحد الأقصى للنقل (MTU) لواجهة خادم AAA. يتم إرسال حزمة IP واحدة مع سمات رسالة EAP ل 12 RADIUS. لا يوجد تجزئة IP أو EAP-TLS.

2. يتلقى محول Cisco IOS هذه الحزمة، ويفصل بينها، ويقرر أن EAP يحتاج أن يكون أرسلت عن طريق EAPoL إلى الطالب. بما أن EAPoL لا يدعم التجزئة، فيجب على المحول إجراء تجزئة EAP-TLS.

3. يقوم محول Cisco IOS بتجميع أول جزء من EAP-TLS يمكن وضعه في وحدة الحد الأقصى للنقل (MTU) للواجهة باتجاه الموجه (1500).

4. يتم تأكيد هذه القطعة بواسطة الطالب.

5. يتم إرسال جزء EAP-TLS آخر بعد تلقي الإقرار.

6. يتم تأكيد هذه القطعة بواسطة الطالب.

7. يتم إرسال الجزء الأخير من EAP-TLS بواسطة المحول.

ويكشف هذا السيناريو عن ما يلي:

- في بعض الظروف، يجب أن يقوم NAD بإنشاء أجزاء EAP-TLS.
- ويضطلع المعهد الوطني لإزالة الألغام بمسؤولية إرسال/إقرار تلك الأجزاء.

وقد يحدث نفس الموقف لمطلب متصل عبر إرتباط يدعم إطارات Jumbo بينما يحتوي خادم AAA على وحدة الحد الأقصى للنقل (MTU) أصغر (ثم يقوم محول Cisco IOS بإنشاء أجزاء EAP-TLS عندما يرسل حزمة EAP نحو خادم AAA).

سمة RADIUS Framed-MTU

بالنسبة ل RADIUS، هناك سمة MTU ذات إطار محدد في RFC 2865:

"تشير هذه السمة إلى الحد الأقصى لوحدة الإرسال التي ستتم تكوينها للمستخدم، في حالة عدم التفاوض بشأنها بواسطة وسائل أخرى (مثل PPP). وقد يتم إستخدامه في حزم قبول الوصول.

وقد يتم إستخدامه في حزمة طلب الوصول كتلميح من قبل NAS للخادم بأنه يفضل هذه القيمة، ولكن الخادم غير مطلوب لتكريم التلميح."

ال يحترم ISE التلميح. ال تؤثر قيمة وحدة الحد الأقصى للنقل (MTU) التي تم إرسالها بواسطة ISE. يتم إستخدام NAD في طلب الوصول على التجزئة التي تم إجراؤها بواسطة ISE.

ال تسمح محولات Cisco IOS المتعددة الحديثة بإجراء تغييرات على وحدة الحد الأقصى للنقل لكل واجهة (MTU) باستثناء إعدادات الإطارات كبيرة الحجم التي تم تمكينها بشكل عام على المحول. يؤثر تكوين الإطارات كبيرة الحجم على قيمة سمة Framed-MTU التي يتم إرسالها في طلب وصول RADIUS. على سبيل المثال، تقوم بضبط:

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

هذا يجبر المفتاح على إرسال Framed-MTU = 9000 في كل RADIUS منفذ يطلب. نفس الشيء بالنسبة لوحدة الحد الأقصى للنقل (MTU) للنظام دون إطارات ضخمة:

```
<#root>

Switch(config)#

system mtu 1600
```

وهذا يفرض على المحول إرسال وحدة الحد الأقصى للنقل (MTU) في إطار FRAMED = 1600 في جميع طلبات وصول RADIUS.

لاحظ أن محولات Cisco IOS الحديثة تسمح لك بتقليل قيمة وحدة الحد الأقصى للنقل (MTU) للنظام إلى ما دون 1500.

خوادم AAA وسلوك المكمل عند إرسال أجزاء EAP

محرك خدمات كشف الهوية (ISE)

يحاول ISE دائما إرسال أجزاء EAP-TLS (عادة ما يكون Server Hello with Certificate) التي يبلغ طولها 1002 بايت (على الرغم من أن الجزء الأخير يكون عادة أصغر).

وهو ال في باإلطار RADIUS-MTU. ال يمكن إعادة تكوينه لإرسال أجزاء EAP-TLS أكبر.

خادم نهج شبكة Microsoft (NPS)

من الممكن تكوين حجم أجزاء EAP-TLS إذا قمت بتكوين سمة Framed-MTU محليا على NPS.

حدث رغم أن المقال لتكوين حجم حمولة EAP على Microsoft NPS يشير إلى أن القيمة الافتراضية لوحدة الحد الأقصى للنقل (MTU) في إطار لخادم NPS RADIUS هي 1500، فقد أظهر مختبر مركز المساعدة التقنية (TAC) من Cisco أنه يرسل 2000 مع الإعدادات الافتراضية (التي تم تأكيدها على مركز بيانات Microsoft Windows 2012).

وقد تم إختبار أن إعداد MTU في إطار محلي وفقا للدليل المذكور سابقا يتم إحترامه من قبل مصادر الشبكة، ويقسم رسائل EAP إلى أجزاء من حجم مضبوط في إطار-MTU. ولكن ال يتم إستخدام سمة Framed-MTU التي تم تلقيها في طلب الوصول (نفس السمة الموجودة على ISE/ACS).

تعيين هذه القيمة هو حل بديل صالح إلصالح المشاكل في المخطط مثل هذا:

مصدر [MTU 1500] — — [MTU 9000]محول [MTU 9000] — [MTU 9000]مصادر الشبكة

ال تسمح لك المحولات حاليا بتعيين MTU لكل منفذ؛ بالنسبة لمحولات 6880، تتم إضافة هذه الميزة باستخدام معرف تصحيح الأخطاء من Cisco CSCuo26327 - 802.1x EAP-TLS ال تعمل على منافذ مضيف FEX.

AnyConnect

يرسل AnyConnect أجزاء EAP-TLS (عادة شهادة العميل) التي يبلغ طولها 1486 بايت. لحجم القيمة هذا، يكون إطار الإيثرنت 1500 بايت. آخر جزء هو عادة أصغر.

ملتمس Microsoft Windows الأصلي

يرسل Microsoft Windows أجزاء EAP-TLS (عادة شهادة العميل) التي يبلغ طولها 1،482 أو 1،486 بايت. لحجم القيمة هذا، يكون إطار الإيثرنت 1500 بايت. آخر جزء هو عادة أصغر.

معلومات ذات صلة

- تكوين المصادقة المستندة إلى المنفذ IEEE 802.1x
- 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).