EAP Fragmentation-implementaties en -gedrag

Inhoud

Inleiding

Dit document beschrijft hoe u EAP-sessies (Extensible Verification Protocol) kunt begrijpen en probleemoplossing kunt bieden.

Achtergrondinformatie

In de volgende delen van dit document wordt aandacht besteed aan deze gebieden:

- Gedrag van verificatie-, autorisatie- en accounting (AAA) servers wanneer deze het servercertificaat voor de EAP-TLS-sessie (Extensible Verification Protocol-Transport Layer Security) retourneren
- Gedrag van aanvragers wanneer zij het clientcertificaat voor de EAP-TLS-sessie retourneren
- Interoperabiliteit wanneer zowel de Microsoft Windows Native Supplicant als Cisco AnyConnect Network Access Manager (NAM) worden gebruikt
- Fragmentation in IP, RADIUS en EAP-TLS en opnieuw assemblageproces dat wordt uitgevoerd door netwerktoegangsapparaten
- Het kenmerk RADIUS framed-Maximum Transmission Unit (MTU)
- Het gedrag van AAA-servers bij het uitvoeren van fragmentatie van EAP-TLS-pakketten

Voorwaarden

Vereisten

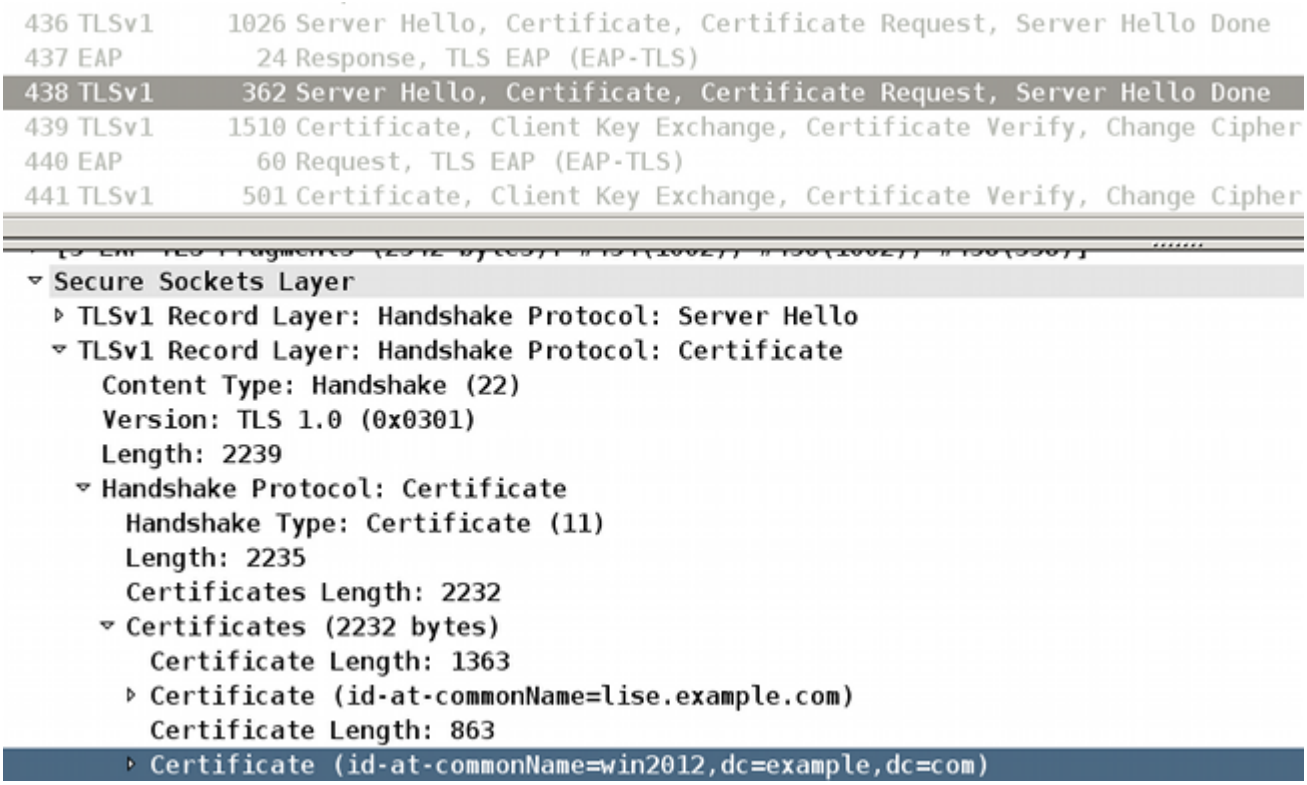
Cisco raadt kennis van de volgende onderwerpen aan:

- EAP- en EAP-TLS-protocollen
- Configuratie van Cisco Identity Services Engine (ISE)
- CLI-configuratie van Cisco Catalyst switches

Een goed begrip van EAP en EAP-TLS is noodzakelijk om dit artikel te kunnen begrijpen.

Certificaatketen teruggestuurd door de server

De AAA-server (Access Control Server (ACS) en ISE) retourneert altijd de volledige keten voor het EAP-TLS-pakket met de Server Hello en het Servercertificaat:



Het ISE-identiteitsbewijs (Common Name (CN)=lise.example.com) wordt teruggestuurd samen met de certificaatinstantie (CA) die het CN=win2012,dc=example,dc=com heeft ondertekend. Het gedrag is hetzelfde voor zowel ACS als ISE.

Certificaatketen teruggestuurd door de aanvrager

Microsoft Windows-native applicatie

Microsoft Windows 7 Native supplicant die is geconfigureerd voor het gebruik van EAP-TLS, met of zonder de "Eenvoudige certificaatselectie", stuurt niet de volledige keten van het clientcertificaat.

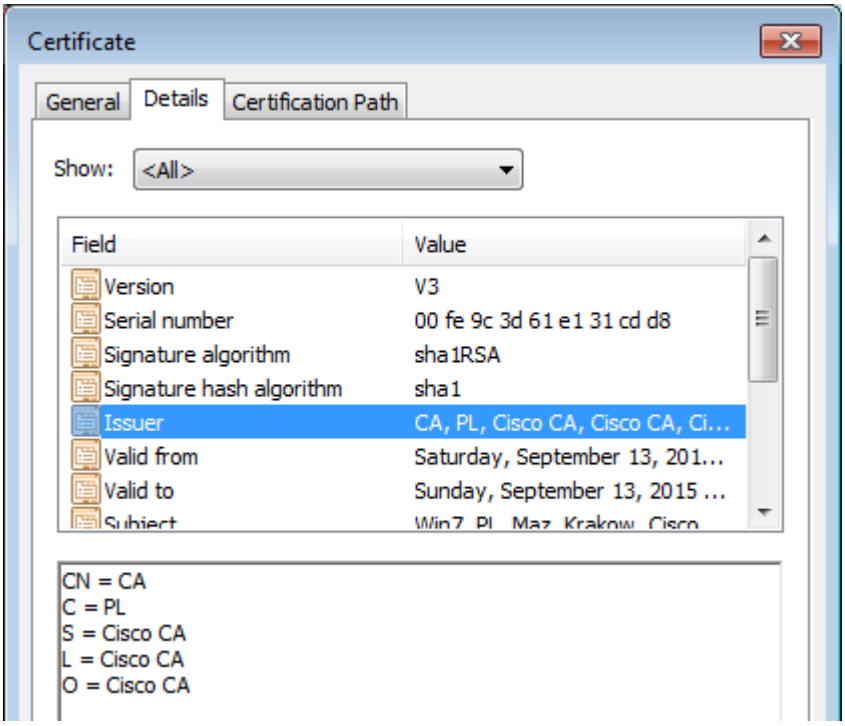
Dit gebeurt zelfs als het clientcertificaat is ondertekend door een andere CA (andere keten) dan het servercertificaat.

Dit voorbeeld heeft betrekking op de Server Hello en het Certificaat dat in de vorige screenshot wordt

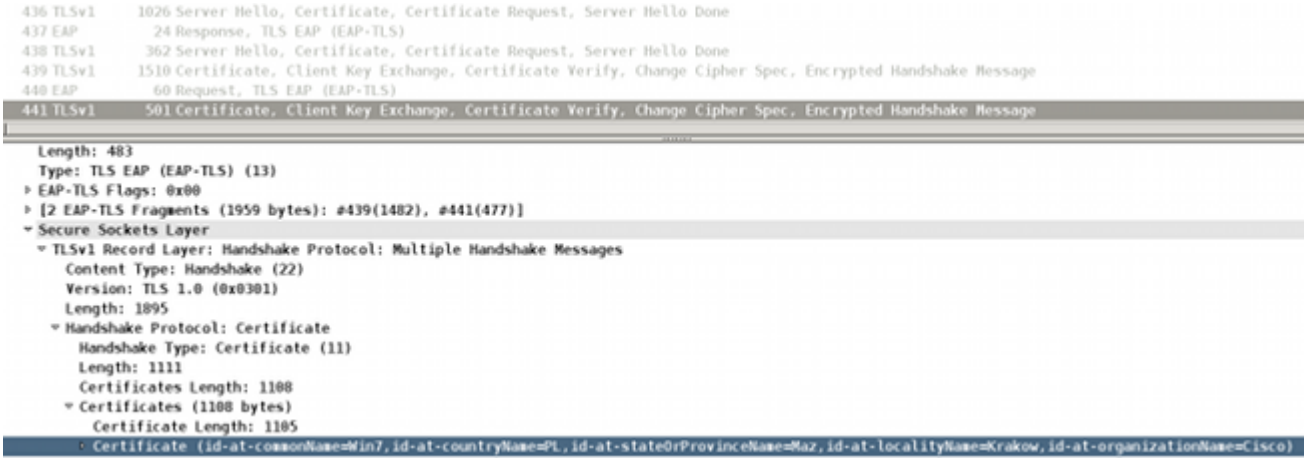
gepresenteerd.

Voor dat scenario wordt het ISE-certificaat ondertekend door de CA met het gebruik van een onderwerpnaam, CN=win2012,dc=example,dc=com.

Maar het gebruikerscertificaat dat in de Microsoft Store is geïnstalleerd, wordt ondertekend door een andere CA, CN=CA, C=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA.



Hierdoor reageert de Microsoft Windows-aanvrager alleen met het clientcertificaat. De CA die de overeenkomst ondertekent (CN=CA, S=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA) is niet aangesloten.



Door dit gedrag ondervinden de AAA-servers mogelijk problemen bij het valideren van clientcertificaten. Het voorbeeld heeft betrekking op Microsoft Windows 7 SP1 Professional.

Oplossing

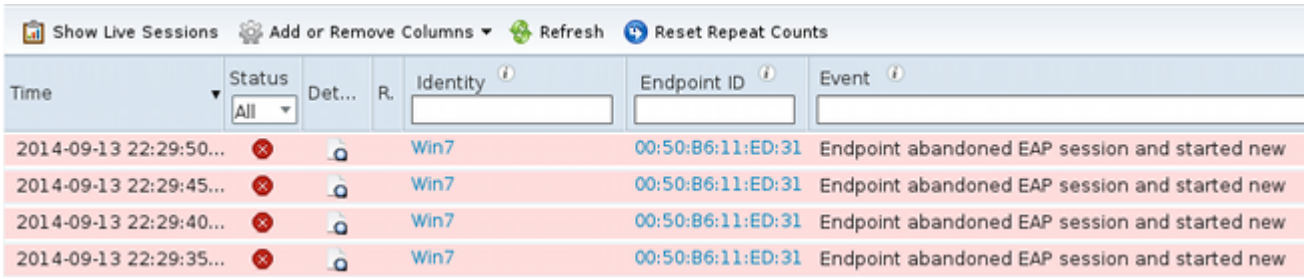
Een volledige certificaatketen moet worden geïnstalleerd op het certificaatarchief van ACS en ISE (alle CA en sub CA die clientcertificaten ondertekenen).

Problemen met de validatie van certificaten kunnen eenvoudig worden gedetecteerd op ACS of ISE. De

informatie over onbetrouwbaar certificaat wordt gepresenteerd en ISE-rapporten:

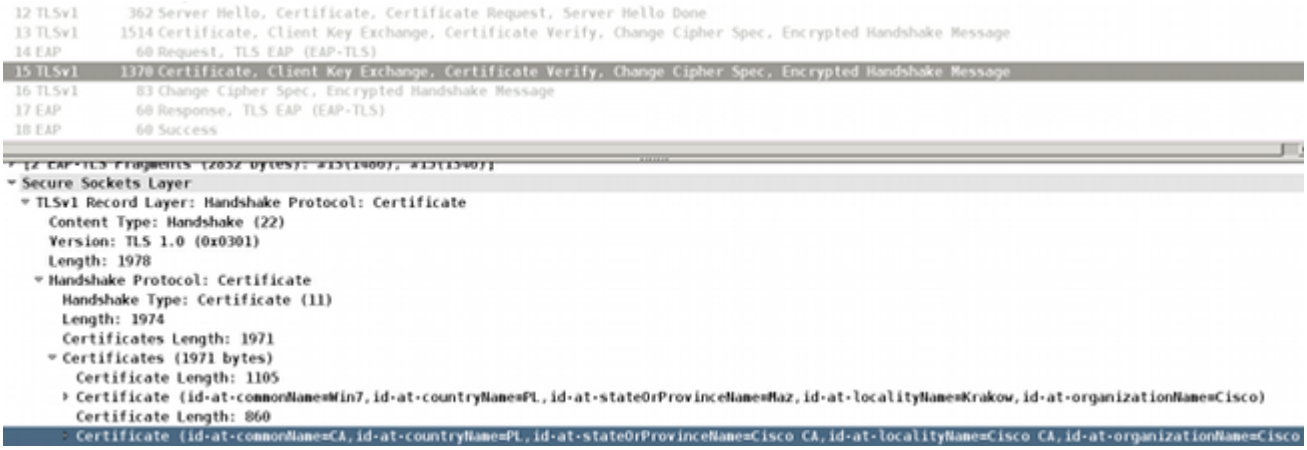
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Problemen met de validatie van het certificaat op de aanvrager zijn niet gemakkelijk op te sporen. Doorgaans reageert de AAA-server op de "Endpoint abondoned EAP Session":



AnyConnect NAM

Deze beperking is niet van toepassing op AnyConnect NAM. In hetzelfde scenario wordt de volledige keten van het clientcertificaat bijgevoegd (de juiste CA is bijgevoegd):



Microsoft Windows-native applicatie samen met AnyConnect NAM

Wanneer beide services zijn opgestart, heeft AnyConnect NAM voorrang.

Zelfs wanneer de NAM-service niet wordt uitgevoerd, sluit deze nog steeds aan op Microsoft Windows API en doorstuurt de EAP-pakketten, wat problemen kan opleveren voor de Microsoft Windows Native-applicatie.

Hier is een voorbeeld van zo'n mislukking.

U kunt overtrekken op Microsoft Windows inschakelen met deze opdracht:

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

De sporen (**c:\windows\trace\svchost_RASTLS.LOG**) tonen:

<#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)

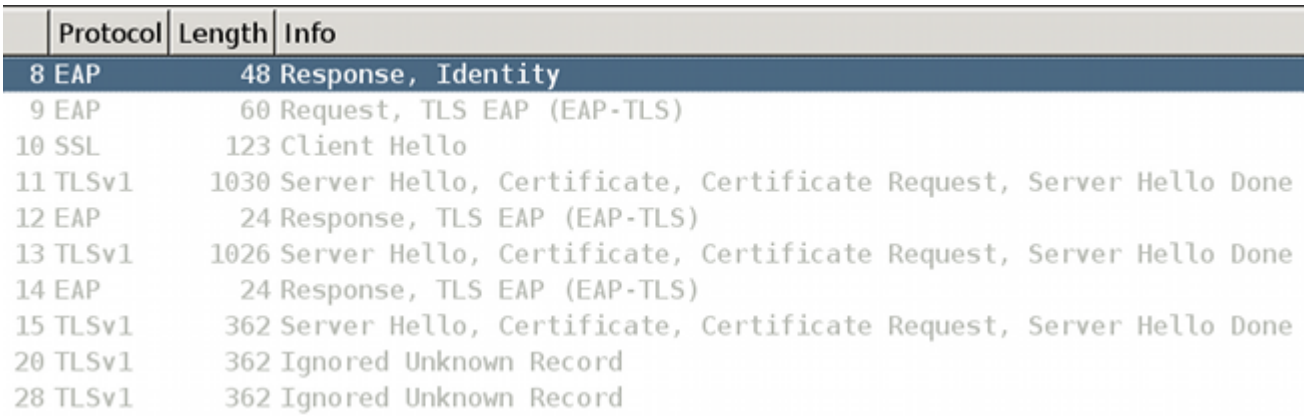
packet: Id: 125, Length:

1492

, Type: 13,

TLS blob length: 1819. Flags: LM

Het laatste pakket is een clientcertificaat (EAP-TLS-fragment 1 met EAP-grootte 1492) dat door de Microsoft Windows-native-aanvrager wordt verzonden. Helaas, Wireshark toont dat pakket niet:



	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

En dat pakket wordt niet echt verzonden; het laatste was het derde fragment van het EAP-TLS-servercertificaat dat gegevens bevatte.

Het is gebruikt door de AnyConnect NAM-module die aansluit op de Microsoft Windows API.

Daarom is het niet raadzaam AnyConnect samen met de Microsoft Windows Native Supplicant te gebruiken.

Wanneer u AnyConnect-services gebruikt, is het raadzaam de NAM ook te gebruiken (wanneer 802.1x-services nodig zijn) en niet de Microsoft Windows Native Supplicant.

Fragmentatie

De fragmentatie komt mogelijk op meerdere lagen voor:

- IP
- RADIUS-kenmerken als waardeparen (AVP)
- EAP-TLS

Cisco IOS® switches zijn zeer intelligent. Ze kunnen EAP- en EAP-TLS-formaten begrijpen.

Hoewel de switch de TLS-tunnel niet kan decoderen, is deze verantwoordelijk voor fragmentatie en assemblage en herassemblage van de EAP-pakketten bij insluiting in EAPoL of RADIUS.

Het EAP-protocol ondersteunt fragmentatie niet. Hier volgt een fragment van RFC 3748 (EAP):

"Fragmentation wordt niet ondersteund binnen EAP zelf; individuele EAP-methoden kunnen dit echter ondersteunen."

EAP-TLS is hiervan een voorbeeld. Hier volgt een fragment uit RFC 5216 (EAP-TLS), punt 2.1.5 (fragmentatie):

"Wanneer een EAP-TLS-peer een EAP-request-pakket ontvangt met de M-bitset, MOET hij met een EAP-Response reageren met EAP-Type=EAP-TLS en geen gegevens.

Dit dient als fragment ACK. **De EAP-server MOET wachten tot hij de EAP-Response ontvangt voordat hij een ander fragment kan verzenden**."

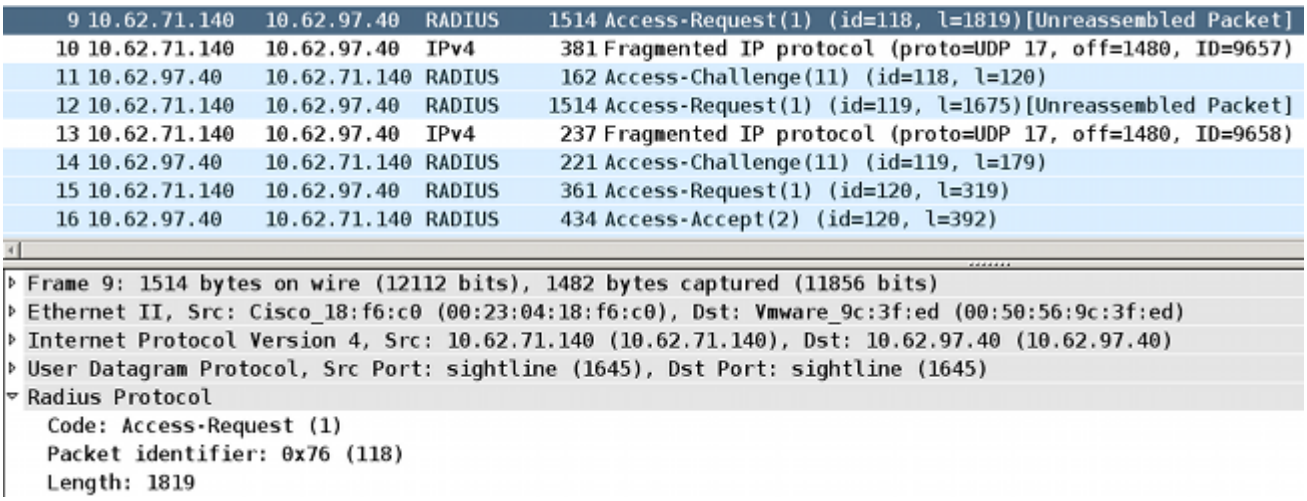
De laatste zin beschrijft een zeer belangrijke eigenschap van AAA-servers. Ze moeten wachten op de ACK voordat ze een ander EAP fragment kunnen verzenden. Voor de aanvrager wordt een soortgelijke regel gebruikt:

"De EAP-peer MOET wachten tot hij de EAP-aanvraag ontvangt voordat hij een ander fragment verstuurt."

Fragmentation in IP-laag

Fragmentation kan alleen optreden tussen het netwerktoegangsapparaat (NAD) en de AAA-server (IP/UDP/RADIUS gebruikt als transport).

Deze situatie doet zich voor wanneer NAD (Cisco IOS switch) probeert het RADIUS-verzoek te verzenden dat de EAP-payload bevat, die groter is dan MTU van de interface:

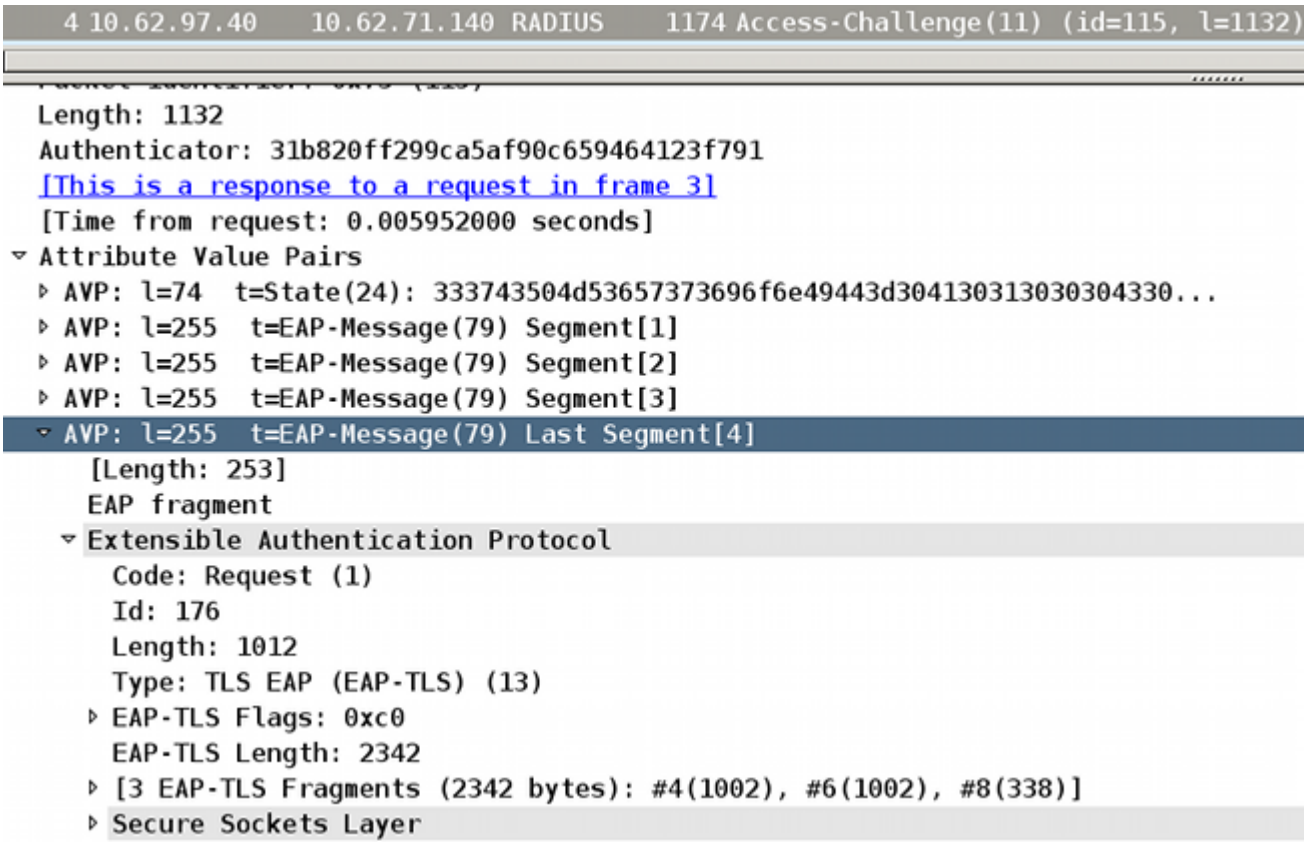


De meeste Cisco IOS-versies zijn niet intelligent genoeg en proberen geen EAP-pakketten te assembleren die via EAPoL worden ontvangen en deze te combineren in een RADIUS-pakket dat in de MTU van de fysieke interface naar de AAA-server kan passen.

AAA-servers zijn intelligenter (zoals in de volgende secties wordt getoond).

Fragmentatie in RADIUS

Dit is niet echt een soort fragmentatie. Zoals in RFC 2865 kan één RADIUS-kenmerk maximaal 253 bytes aan gegevens bevatten. Daarom wordt de EAP-payload altijd verzonden in meerdere EAP-Message RADIUS-kenmerken:



Deze EAP-Message-kenmerken worden opnieuw geassembleerd en geïnterpreteerd door Wireshark (het kenmerk "Laatste segment" toont de payload van het hele EAP-pakket).

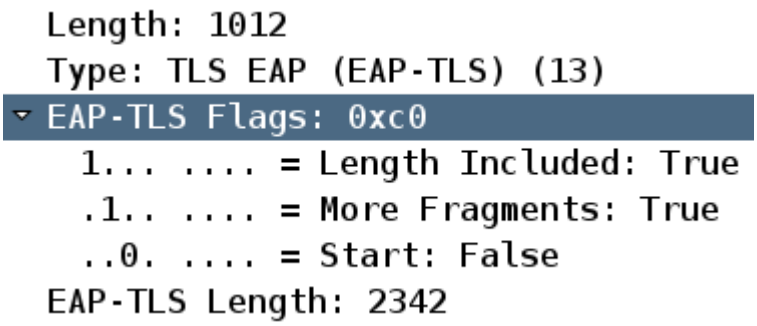
De kop Lengte in het EAP-pakket is gelijk aan 1,012 en er zijn vier RADIUS-AVP's nodig om het te transporteren.

Fragmentatie in EAP-TLS

Op dezelfde screenshot kunt u het volgende zien:

- EAP-pakketlengte is 1.012
- EAP-TLS-lengte is 2.342

Dit suggereert dat het het eerste EAP-TLS-fragment is en de aanvrager verwacht meer, wat kan worden bevestigd als u de EAP-TLS-vlaggen onderzoekt:



Dit type fragmentatie komt het meest voor in:

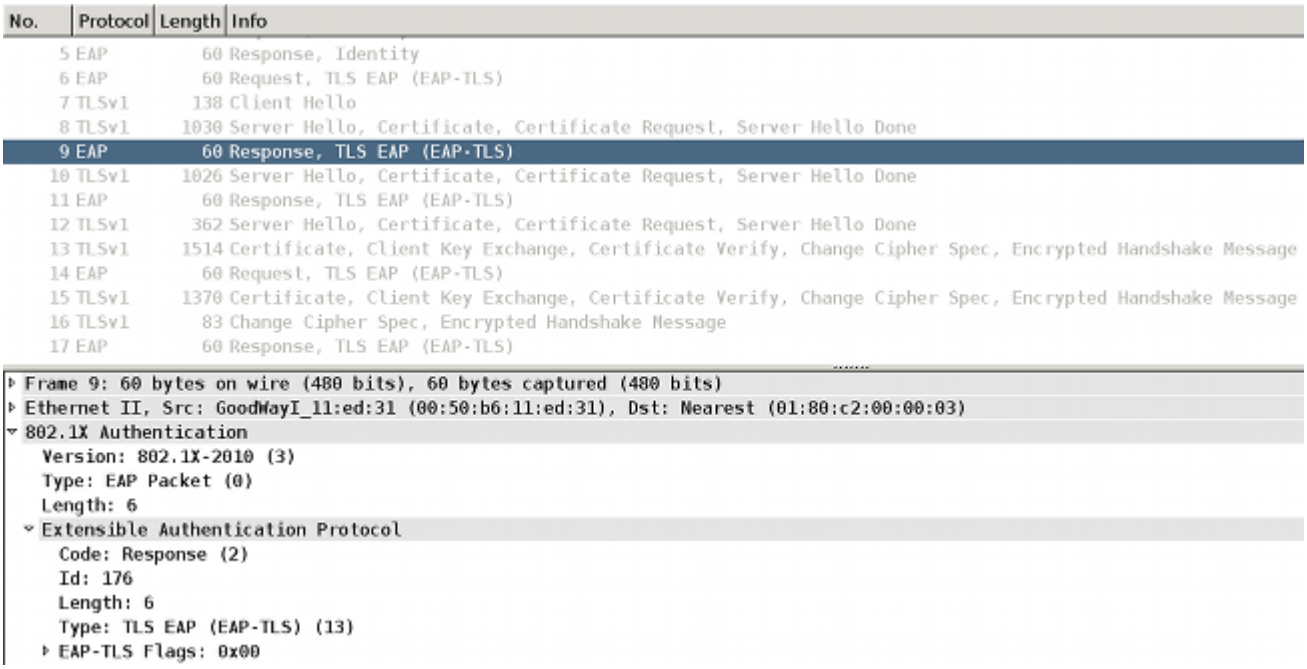
- RADIUS Access-Challenge verzonden door de AAA-server, die het EAP-Verzoek met het SSL-servercertificaat (Secure Sockets Layer) met de hele keten meedraagt.

- RADIUS-toegangsaanvraag verzenden door NAD, die de EAP-Response met het SSL-clientcertificaat met de hele keten meedraagt.

EAP-TLS-fragmentbevestiging

Zoals eerder is uitgelegd, moet elk EAP-TLS-fragment worden bevestigd voordat volgende fragmenten worden verzonden.

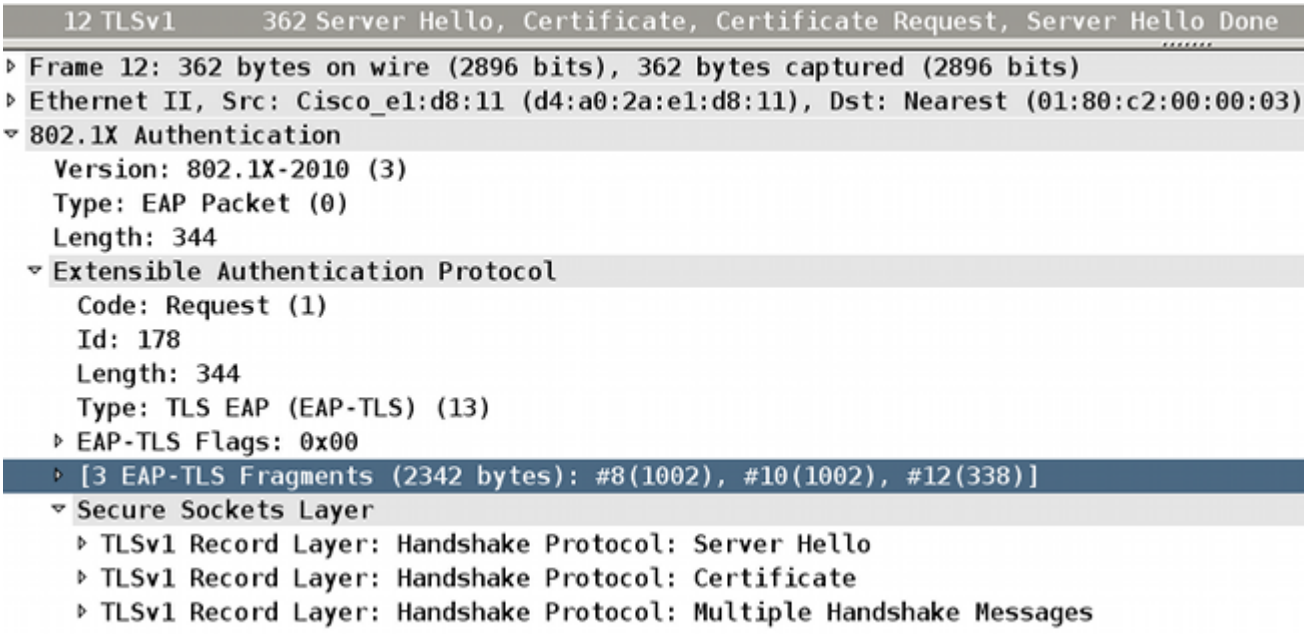
Hier is een voorbeeld (pakketopname voor EAPoL tussen de aanvrager en het NAD):



EAPoL-frames en de AAA-server geven het servercertificaat terug:

- Dat certificaat wordt verzonden in een EAP-TLS-fragment (pakket 8).
- De aanvrager erkent dat fragment (pakket 9).
- Het tweede EAP-TLS-fragment wordt doorgestuurd door NAD (pakket 10).
- De aanvrager erkent dat fragment (pakket 11).
- Het derde EAP-TLS-fragment wordt doorgestuurd door NAD (pakket 12).
- De aanvrager hoeft dit niet te erkennen, maar gaat verder met het clientcertificaat dat begint bij pakket 13.

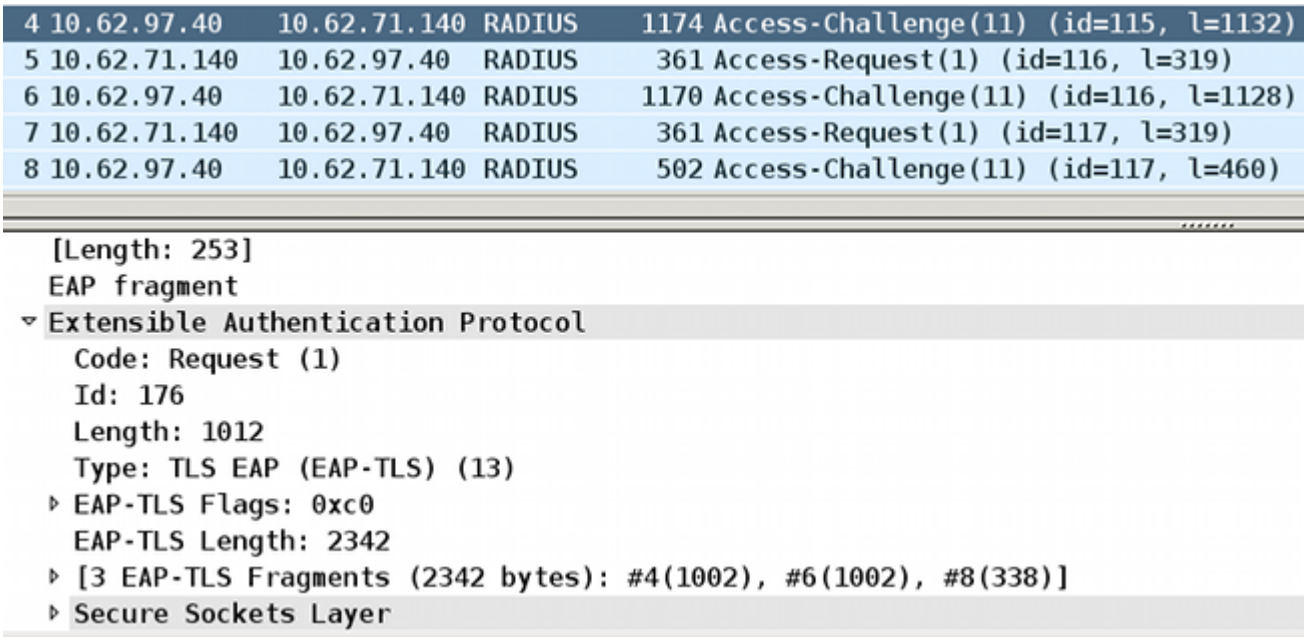
Hier zijn de details van pakket 12:



Je ziet dat Wireshark de pakketten 8, 10 en 12 opnieuw in elkaar heeft gezet.

De omvang van de EAP-fragmenten is 1,002, 1,002 en 338, wat de totale omvang van het EAP-TLS-bericht op 2342 brengt;

De totale lengte van EAP-TLS-berichten wordt in elk fragment aangekondigd. Dit kan worden bevestigd als u RADIUS-pakketten onderzoekt (tussen NAD en AAA-server):



RADIUS-pakketten 4, 6 en 8 bevatten deze drie EAP-TLS-fragmenten. De eerste twee fragmenten worden erkend.

Wireshark kan de informatie over de EAP-TLS-fragmenten presenteren (grootte: 1,002 + 1,002 + 338 = 2,342).

Dit scenario en voorbeeld was makkelijk. De Cisco IOS-switch hoefde de grootte van het EAP-TLS-fragment niet te wijzigen.

EAP-TLS-fragmenten opnieuw geassembleerd met verschillende afmetingen

Overweeg wat er gebeurt wanneer NAD MTU naar AAA-server 9000 bytes (jumboframe) is en de AAA-server ook is verbonden met het gebruik van de interface die jumboframes ondersteunt.

Het merendeel van de typische smeekbedes is verbonden met het gebruik van een 1Gbit link met een MTU van 1.500.

In een dergelijk scenario voert de Cisco IOS-switch EAP-TLS-"assymetrische" assemblage en herassemblage uit en wijzigt hij de grootte van EAP-TLS-fragmenten.

Hier is een voorbeeld voor een groot EAP-bericht dat door de AAA-server wordt verzonden (SSL-servercertificaat):

1. De AAA-server moet een EAP-TLS-bericht verzenden met een SSL-servercertificaat. De totale grootte van dat EAP-pakket is 3.000. Nadat het in RADIUS Access-Challenge/UDP/IP is ingesloten, is het nog steeds minder dan de AAA-serverinterface MTU. Eén IP-pakket wordt verzonden met 12 RADIUS EAP-Message-kenmerken. Er is geen IP- of EAP-TLS-fragmentatie.

2. De Cisco IOS-switch ontvangt een dergelijk pakket, decapsuleert het en besluit dat EAP via EAPoL naar de aanvrager moet worden verzonden. Aangezien EAPoL-fragmentatie niet ondersteunt, moet de switch EAP-TLS-fragmentatie uitvoeren.

3. De Cisco IOS-switch bereidt het eerste EAP-TLS-fragment voor dat in de MTU van de interface naar de aanvrager kan passen (1.500).

4. Dit fragment wordt bevestigd door de aanvrager.

5. Een ander EAP-TLS-fragment wordt verzonden nadat een bevestiging is ontvangen.

6. Dit fragment wordt bevestigd door de aanvrager.

7. Het laatste EAP-TLS-fragment wordt door de switch verzonden.

Dit scenario onthult dat:

- Onder bepaalde omstandigheden moet het NAD EAP-TLS-fragmenten aanmaken.
- Het NAD is verantwoordelijk voor het verzenden/erkennen van deze fragmenten.

Dezelfde situatie kan zich voordoen voor een aanvrager die is verbonden via een link die jumboframes ondersteunt, terwijl de AAA-server een kleinere MTU heeft (de Cisco IOS-switch maakt EAP-TLS-fragmenten aan wanneer het EAP-pakket naar de AAA-server wordt verzonden).

RADIUS-kenmerk framed-MTU

Voor RADIUS is er een framed-MTU-kenmerk dat in RFC 2865 is gedefinieerd:

"Deze eigenschap geeft de maximale transmissieeenheid aan die voor de gebruiker moet worden geconfigureerd, wanneer niet op een andere manier over deze eenheid wordt onderhandeld (zoals PPP). Het KAN worden gebruikt in access-acceptatiepakketten.

Het KAN worden gebruikt in een Access-request pakket als een hint door de NAS aan de server dat het de voorkeur zou geven aan die waarde, maar de server is niet nodig om de hint te honoreren."

ISE doet geen eer aan de hint. De waarde van framed-MTU verzonden door NAD in het access-request heeft geen invloed op de fragmentatie uitgevoerd door ISE.

Meerdere moderne Cisco IOS-switches staan geen wijzigingen in de MTU van de Ethernet-interface toe, behalve voor instellingen voor jumboframes die wereldwijd op de switch zijn ingeschakeld. De configuratie van jumboframes is van invloed op de waarde van het Framed-MTU-kenmerk dat in het RADIUS-toegangsverzoek is verzonden. U stelt bijvoorbeeld het volgende in:

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

Dit dwingt de switch om framed-MTU = 9000 in alle RADIUS-toegangsaanvragen te verzenden. Hetzelfde voor het systeem MTU zonder jumboframes:

```
<#root>

Switch(config)#

system mtu 1600
```

Dit dwingt de switch om framed-MTU = 1600 in alle RADIUS-toegangsaanvragen te verzenden.

Houd er rekening mee dat met moderne Cisco IOS-switches de MTU-waarde van het systeem niet lager kan worden dan 1.500.

AAA-servers en supplicant gedrag wanneer u EAP-fragmenten verzendt

ISE

ISE probeert altijd EAP-TLS-fragmenten (meestal Server Hello met certificaat) te verzenden die 1.002 bytes lang zijn (hoewel het laatste fragment meestal kleiner is).

Dit is geen eerbetoon aan de RADIUS Framed-MTU. Het is niet mogelijk om deze opnieuw te configureren om grotere EAP-TLS-fragmenten te verzenden.

Microsoft Network Policy Server (NPS)

Het is mogelijk om de grootte van de EAP-TLS-fragmenten te configureren als u het framed-MTU-kenmerk lokaal op NPS configureert.

Hoewel het artikel EAP Payload Size op Microsoft NPS configureren vermeldt dat de standaardwaarde van een framed MTU voor de NPS RADIUS-server 1.500 is, heeft het lab van Cisco Technical Assistance Center (TAC) aangetoond dat het 2.000 met de standaardinstellingen verzendt (bevestigd op een Microsoft Windows 2012 Datacenter).

Er wordt getest dat het **lokaal** instellen van **Framed-MTU** volgens de eerder genoemde gids gerespecteerd wordt door NPS en het fragmenteert de EAP-berichten in fragmenten van een grootte ingesteld in Framed-MTU. Maar het kenmerk Framed-MTU dat in het toegangsverzoek wordt ontvangen, wordt niet gebruikt

(hetzelfde als bij ISE/ACS).

Het instellen van deze waarde is een geldige tijdelijke oplossing om problemen in topologie als deze op te lossen:

Supplicant [MTU 1500] ---- ---- [MTU 9000]Switch [MTU 9000] ----- ----- [MTU 9000]NPS

Op dit moment kunt u met switches de MTU niet per poort instellen; voor 6880 switches wordt deze functie toegevoegd met Cisco bug-id CSCuo26327 - 802.1x EAP-TLS die niet werkt op FEX-hostpoorten.

AnyConnect

AnyConnect verzendt EAP-TLS-fragmenten (gewoonlijk clientcertificaat) met een lengte van 1.486 bytes. Voor deze waardegrootte is het Ethernet-frame 1500 bytes. Het laatste fragment is meestal kleiner.

Microsoft Windows-native applicatie

Microsoft Windows stuurt EAP-TLS-fragmenten (meestal clientcertificaat) met een lengte van 1.486 of 1.482 bytes. Voor deze waardegrootte is het Ethernet-frame 1500 bytes. Het laatste fragment is meestal kleiner.

Gerelateerde informatie

- **IEEE 802.1x-poortgebaseerde verificatie configureren**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.