EAP分段实施和行为

目录

简介

本文描述如何明白和排除故障可扩展的认证协议(EAP)会话。这些问题被讨论：

- 验证、授权和统计(AAA)服务器行为，当他们归还扩展验证传输层安全(EAP-TLS)会话的服务器证书
- 恳求者行为，当他们归还EAP-TLS会话的客户端证书
- 互通性，当使用Microsoft Windows本地请求方和思科AnyConnect网络访问管理器(NAM)
- 在IP、RADIUS和EAP-TLS和网络访问设备执行的重组进程的分段
- RADIUS成帧最大数量传输部件(MTU)属性
- AAA服务器的行为，当他们进行EAP-TLS数据包的分段

先决条件

要求

Cisco 建议您了解以下主题：

- EAP和EAP-TLS协议
- 思科身份服务引擎(ISE)的配置
- 思科Catalyst交换机的CLI配置

有一好了解EAP和EAP-TLS为了了解此条款是必要的。

服务器返回的证书链

AAA服务器(访问控制服务器(ACS)和ISE)总是返回EAP-TLS数据包的全双工一系列有服务器问候和服务器证书的：

ISE身份证书(共同名称(CN) =lise.example.com)与签署CN=win2012,dc=example,dc=com的Certificate Authority (CA)一起返回。行为是相同的为ACS和ISE。

请求方返回的证书链

Microsoft Windows本地请求方

配置的Microsoft Windows 7本地请求方为了使用EAP-TLS，有或没有“简单证书选择”，不发送客户端证书的全双工一系列。此行为出现，既使当客户端证书由不同的CA (另外一系列)签字比服务器证书。

此示例与在上一个屏幕画面和证书涉及提交的服务器问候。对于该方案， ISE证书由与使用的CA签字主题名称， CN=win2012,dc=example,dc=com。但是在Microsoft存储安装的用户证书由不同的CA签字， CN=CA， C=PL， S=Cisco CA， L=Cisco CA， O=Cisco CA。

结果， Microsoft Windows请求方回应仅客户端证书。CA (签署它的CN=CA、S=PL、S=Cisco CA、L=Cisco CA， O=Cisco CA)没有附加。

因此，当他们验证客户端证书时，行为， AAA服务器也许遇到问题。示例与Microsoft Windows 7 SP1专业人员关连。

解决方案

在ACS和ISE应该安装一条全双工证书链(签署客户端证书)的所有CA和子CA证书存储。

与证书确认的问题在ACS或ISE可以容易地检测。提交关于不信任证书的信息和ISE报告：

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

与证书确认的问题在请求方不容易地是可发现的。通常AAA服务器响应“终端放弃EAP会话”：

AnyConnect NAM

AnyConnect NAM没有此限制。在同一个方案中，它附加客户端证书的完整一系列(正确CA附加)：

与AnyConnect NAM一起的Microsoft Windows本地请求方

当两服务是UP时， AnyConnect NAM获得优先权。既使当NAM服务不运作，它在Microsoft Windows API仍然连接并且转发EAP数据包，能引起Microsoft Windows本地请求方的问题。这是这样失败示例。

您启用在Microsoft Windows的跟踪用此命令：

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

跟踪(**c:\windows\trace\svchost _RASTLS.LOG**)显示：

```
[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
```

最后数据包是Microsoft Windows本地请求方(与EAP大小1492)的EAP-TLS片段1发送的客户端证书。不幸地， Wireshark不显示该数据包：

并且该数据包确实没有发送(最后一个是EAP-TLS运载的服务器证书的第三个片段)。它由该AnyConnect NAM的模块消耗了在Microsoft Windows API的挂。

所以没有建议与Microsoft Windows本地请求方一起使用AnyConnect。当您使用所有AnyConnect服

务时，没有建议也使用NAM (当802.1x服务是需要的)时，没有Microsoft Windows本地请求方。

分段

分段在多层也许发生：

- IP
- RADIUS属性值对(AVP)
- EAP-TLS

Cisco IOS交换机非常智能。他们能了解EAP和EAP-TLS格式。虽然交换机不能解密TLS建立隧道，对分段负责和EAP数据包的装配和重新组装，当在LAN上的可扩展认证协议(EAPoL)时或RADIUS的封装。

EAP协议不支持分段。这是摘自RFC 3748 (EAP)的一个部分：

“分段不在EAP内支持;然而，各自的EAP方法可能支持此”。

EAP-TLS是这样示例。这是摘自RFC 5216 (EAP-TLS)的一个部分，第2.1.5部分(分段) ：

“当EAP-TLS对等体收到有M位集的时一EAP请求数据包，必须回应与EAP-Type=EAP-TLS和没有数据的一EAP答复。这担当片段ACK。**EAP服务器必须等待，直到在发送另一个片段前接收EAP答复**”。

最后句子描述AAA服务器一个非常重要功能。在他们能发送另一个EAP片段前，他们必须等待ACK。一个相似的规则使用请求方：

“EAP对等体必须等待，直到它在发送另一个片段前接收EAP请求”。

在IP层的分段

分段能仅发生在网络接入设备(纳季)和AAA服务器(作为传输使用的IP/UDP/RADIUS之间)。此情况发生，当纳季(Cisco IOS交换机)设法发送包含EAP有效负载，是接口的更大的然后MTU的RADIUS请求：

多数Cisco IOS版本不足够智能和不设法装配通过EAPoL接收的EAP数据包和结合他们在能适合物理接口MTU往AAA服务器的RADIUS信息包。

AAA服务器更加智能(如被提交在以下部分)。

在RADIUS的分段

这确实不是任何分段。根据RFC 2865，单个RADIUS属性能有253字节的数据。因此， EAP有效负载在多个EAP消息RADIUS属性总是传送：

那些EAP消息属性由Wireshark重新召集并且解释(“最后面几段”属性显示全部的EAP数据包的有效负载)。在EAP数据包的长度报头是相等的to1,012，并且四个RADIUS AVPs要求传输它。

在EAP-TLS的分段

从同样屏幕画面，您能看到那：

- EAP数据包长度是1,012
- EAP-TLS长度是2,342

这建议它是第一个EAP-TLS片段，并且请求方应该期待更多，可以被确认是否检查EAP-TLS标志：

这种分段频繁地发生在：

- RADIUS访问-查询由AAA服务器发送，运载与安全套接字协议层(SSL)服务器证书的EAP请求与全部的一系列。
- RADIUS Access-Request发送用纳季，运载与SSL客户端证书的EAP答复与全部的一系列。

EAP-TLS片段确认

如前所述，每个EAP-TLS片段，在随后的片段发送前，必须确认。

这是示例(EAPoL的数据包捕获在请求方和纳季之间)：

EAPoL帧和AAA服务器返回服务器证书：

- 该证书在EAP-TLS片段(数据包8)发送。
- 请求方确认该片段(数据包9)。
- 第二个EAP-TLS片段由纳季(数据包10)转发。
- 请求方确认该片段(数据包11)。
- 第三个EAP-TLS片段由纳季(数据包12)转发。
- 请求方不需要确认此;相反，它继续进行开始在数据包13的客户端证书。

这是详细信息数据包12 ：

您能看到Wireshark重新组装了数据包8， 10和12。EAP的大小分段is1,002， 1,002和338，带来EAP-TLS消息总大小到2342 (总EAP-TLS消息长度在每个片段宣布)。这可以被确认是否检查RADIUS信息包(在纳季和AAA服务器之间)：

RADIUS信息包4， 6和8运载那些三个EAP-TLS片段。前两个片段确认。Wireshark能引见关于EAP-TLS片段(大小的信息：1,002 + 1,002 + 338 = 2,342)。

此方案和示例是容易。Cisco IOS交换机没有需要更改EAP-TLS分段大小。

EAP-TLS片段重新组装与另外大小

请考虑发生了什么，当往AAA服务器的纳季MTU是9,000个字节(超大帧)，并且AAA服务器也连接与该使用的接口支持巨型帧。大多典型的恳求者连接与使用与MTU的一条1Gbit链路1,500。

在这种情况下， Cisco IOS交换机进行EAP-TLS “不对称”集合和重新组装并且更改EAP-TLS分段大小。这是AAA服务器发送的一个大EAP信息的一示例(SSL服务器证书)：

1. AAA服务器必须传送与SSL服务器证书的EAP-TLS信息。总大小该EAP数据包是3,000。在它在RADIUS访问Challenge/UDP/IP后被封装，比AAA服务器接口MTU仍然是较少。单个IP数据

包用12个RADIUS EAP消息属性传送。没有IP亦不EAP-TLS分段。

2. Cisco IOS交换机收到这样数据包，解封装它，并且决定EAP需要通过EAPoL发送到请求方。因为EAPoL不支持分段，交换机必须进行EAP-TLS分段。

3. Cisco IOS交换机准备能适合到接口MTU往请求方的第一个EAP-TLS片段(1,500)的。

4. 此片段由请求方确认。

5. 在确认接收后，另一个EAP-TLS片段发送。

6. 此片段由请求方确认。

7. 最后EAP-TLS片段由交换机发送。

此方案显示那：

- 在一些情况下，纳季必须创建EAP-TLS片段。
- 负责发送/确认那些片段的纳季。

同一个情况能为通过支持巨型帧的链路连接的请求方发生，当AAA服务器有更加小的MTU时(Cisco IOS交换机然后创建EAP-TLS片段，当发送往AAA服务器的EAP数据包)时。

RADIUS属性成帧MTU

RADIUS，有在RFC 2865定义的成帧MTU属性：

“此属性指示最大传输单元(MTU)为用户配置，当没有以某些其他方式时协商(例如PPP)。可能用于访问接受信息包。**也许用于访问请求信息包作为提示由对服务器的NAS将更喜欢该值，但是服务器没有要求尊敬提示”**。

ISE不尊敬提示。Access-Request的纳季发送的成帧MTU的值没有在ISE进行的分段的任何影响。

多个现代Cisco IOS交换机不允许对以太网接口的MTU的更改除了在交换机启用的全局巨型帧设置。巨型帧的配置影响在RADIUS Access-Request发送的成帧MTU属性的值。例如，您集：

```
Switch(config)#system mtu jumbo 9000
```

这强制交换机发送成帧MTU = 9000在所有RADIUS访问请求。同样没有巨型帧的系统MTU ：

```
Switch(config)#system mtu 1600
```

这强制交换机发送成帧MTU = 1600在所有RADIUS访问请求。

注意现代Cisco IOS交换机不允许您减少系统MTU值在1,500以下。

AAA服务器和请求方行为，当您发送EAP片段

ISE

ISE总是设法发送是长1,002个的字节的EAP-TLS片段(通常与证书的服务器问候) (虽然最后片段通常更加小)。它不尊敬RADIUS成帧MTU。重新配置它发送更大的EAP-TLS片段是不可能的。

Microsoft网络策略服务器(NP)

如果在NP，本地配置成帧MTU属性配置EAP-TLS片段的大小是可能的。

事件，虽然配置在Microsoft NP条款的EAP有效负载大小提及成帧的MTU的默认值NP RADIUS服务器的是1,500， Cisco技术支持中心(TAC)实验室显示发送2,000与默认设置(确认在Microsoft Windows 2012 Datacenter)。

测试设置**本地成帧MTU**根据以前被提及的指南由NP尊敬，并且分段EAP消息到在成帧MTU设置的大小的片段。但是没有使用在Access-Request接收的成帧MTU属性(同一样在ISE/ACS)。

设置此值是一有效应急方案为了调整问题在象这样的拓扑方面：

请求方[MTU 1500]--------[MTU 9000]Switch [MTU 9000]----------[MTU 9000]NPS

目前交换机不允许您设置MTU每个端口;对于6880交换机，此功能添加与Cisco Bug ID CSCuo26327 - 802.1x EAP-TLS不工作在FEX主机端口。

AnyConnect

AnyConnect发送是长1,486个的字节的EAP-TLS片段(通常客户端证书)。对于此值大小，以太网帧是1,500个字节。最后片段通常更加小。

Microsoft Windows本地请求方

Microsoft Windows发送是长1,486个或1,482个的字节的EAP-TLS片段(通常客户端证书)。对于此值大小，以太网帧是1,500个字节。最后片段通常更加小。

相关信息

- **配置基于 IEEE 802.1x 端口的身份验证**
- **技术支持和文档 - Cisco Systems**