的通信流导致中断的AnyConnect客户端每分钟重新连接

目录

简介

本文讨论AnyConnect客户端也许重新连接到可适应安全工具的特定方案(ASA)在正确地一分钟之内。用户也许不能收到流量经过传输层安全(TLS)通道，直到AnyConnect重新连接。这取决于在本文讨论的一些个其他要素。

受影响的组件

- ASA版本9.0或版本9.1
- AnyConnect客户端版本3.0或版本3.1

症状

在本例中，当重新连接对ASA， AnyConnect客户端显示。

此Syslog在ASA被看到：

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

问题说明

这些诊断和报告工具(箭)日志在此问题看到：

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

Date         : 11/16/2013
Time         : 01:28:50
Type         : Warning
Source       : acvpnagent

Description : Reconfigure reason code 16:
New MTU configuration.

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

Date         : 11/16/2013
Time         : 01:28:50
Type         : Information
Source       : acvpnagent

Description : The entire VPN connection is being reconfigured.

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

Date         : 11/16/2013
Time         : 01:28:51
Type         : Information
Source       : acvpnui

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

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

Date         : 11/16/2013
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.


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

原因

此问题的原因是疏忽构建数据报传输传送层安全(DTL)通道。这能是由于两个原因：

- DTL在路径阻塞某处
- 使用一个非默认DTL端口

DTL在路径阻塞某处

自ASA版本9.x和AnyConnect版本3.x，优化介绍以为在client/ASA之间的TLS/DTLS协商的明显的最大转换单元(MTU)的形式。以前，客户端派生了明显地比最佳包括两个TLS/DTLS并且是的粗略估计MTU。现在， ASA计算两个TLS/DTLS的封装开销并且相应地得到MTU值。

只要DTL启用，客户端应用在的DTL MTU (在这种情况下1418)启用的VPN适配器(在DTL通道设立并且为路由/过滤器实施是需要的)前，保证最佳性能。如果DTL通道不可能设立或丢弃，客户端故障切换对TLS并且调节在虚拟适配器(VA)的MTU对TLS MTU值(这要求级别再接合)的会议。

解决方法

为了排除此可视转换DTL > TLS，管理员能配置仅TLS访问的一单独的隧道组有与DTL通道的建立的困难的用户的(例如由于防火墙限制)。

1. 最好的选项比TLS MTU是设置AnyConnect MTU值更低，然后协商。`group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect mtu 1300` 这做相等TLS和DTL MTU的值。再连接在这种情况下看不到。
2. 第二个选项是允许分段。 `group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect ssl df-bit-ignore enable`使用分段，大小超过MTU值)的大数据包(可以通过TLS被分段和被发送建立隧道。
3. 第三个选项是设置最大分段尺寸(MSS)到1460如下：`sysopt conn tcpmss 1460` 在这种情况下，大于DTL MTU 1418的TLS MTU将是1427 (RC4/SHA1) (AES/SHA1/LZS)。这应该解决与TCP的问题从ASA到AnyConnect客户端(由于MSS)，但是从ASA的大UDP流量到AnyConnect客户端也许遭受此，因为将由AnyConnect客户端丢弃由于更低AnyConnect客户端MTU 1418。如果**sysopt**修改**conn tcpmss**，它也许影响其它特性例如LAN对LAN (L2L) IPSec VPN通道。

使用非默认DTL波尔特

DTL失败的另一潜在原因启用在一个非默认端口的DTL，在WebVPN启用后(例如，当**WebVPN enable (event)外部**命令被输入)时。这归结于Cisco Bug ID CSCuh61321和被看到了在ASA推送非默认端口给客户端的版本9.x，但是继续听默认端口。结果， DTL没有被构件，并且AnyConnect重新连接。

```
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address             Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444           0.0.0.0:*

DTLS      00020dc8  LISTEN     172.16.11.1:443           0.0.0.0:*
```

在TLS通道设立后，客户端尝试设立DTL建立隧道到端口444正如所料：

导致打开的问题和加速的安全路径命令的顺序(ASP)表插槽是：

1. 从没启用的WebVPN插槽开始。`ciscoasa(config)# show run webvpn`
   `webvpn`
   `anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1`
   `anyconnect enable`

```
ciscoasa(config)# show asp table socket
Protocol  Socket    State      Local Address             Foreign Address
ciscoasa(config)#
```

2. 更换TLS端口到444并且启用WebVPN。`ciscoasa(config-webvpn)# show run webvpn`

```
webvpn
 port 444
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config-webvpn)# show asp tabl socket
Protocol  Socket    State      Local Address            Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444          0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443          0.0.0.0:*
```

3. 更换DTL端口到444。`ciscoasa(config-webvpn)# dtls port 444`

```
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address            Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444          0.0.0.0:*
DTLS      00020dc8  LISTEN     172.16.11.1:443          0.0.0.0:*
```

注意：DTL socket端口仍然是443。这时AnyConnect客户端虽则设立DTL到444!

解决方法

此问题的应急方案是遵从命令：

1. 禁用WebVPN。
2. 输入DTL端口。
3. 启用WebVPN。

此行为在版本8.4.x版本不存在， DTL插槽获得更新用配置端口，在配置被输入之后：

ASA版本8.4.6 ：

```
ciscoasa(config-webvpn)# port 444
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000d5df 172.16.11.1:443 0.0.0.0:* LISTEN

ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show asp table socket
```

```
Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000eb5f 172.16.11.1:444 0.0.0.0:* LISTEN << changed immediately
```

重新连接工作流

假设这些密码器配置：

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1
```

此事件顺序在这种情况下发生：

- AnyConnect设立一个parent通道，并且TLS数据建立隧道与RC4-SHA作为Ssl encryption。
- DTL在路径阻塞，并且DTL通道不可能设立。
- ASA宣布参数对AnyConnect，包括TLS和DTL MTU值，是两个独立的值。
- 默认情况下DTL MTU是1418。
- TLS MTU从**sysopt conn tcpmss**值计算(默认是1380)。这是TLS MTU如何派生(如被看到从输出的**调试WebVPN anyconnect**)：
  ```
  1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347
  ```
- AnyConnect提出VPN适配器并且分配在预期的**DTL** MTU到它能通过DTL连接。
- AnyConnect客户端当前连接，并且用户去一个特定的网站。
- 浏览器发送TCP SYN并且设置在它的MSS= 1418-40 = 1378。
- 在ASA的里面的Http服务器发送数据包大小1418。
- 因为他们安排不要分段(DF)位设置， ASA不放他们到通道，并且不能分段他们。
- ASA打印`%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111> Transmitting large packet 1418 (threshold 1347)`并且有MP svc没有片段ASP丢弃原因的丢包数据包。
- 同时ASA发送ICMP目的地不可达的，必要发送方的分段：
  ```
  %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
  ```
- 如果互联网控制消息协议(ICMP)允许，则发送方重传丢弃的数据包，并且一切开始工作。如果ICMP阻塞，则流量是在ASA的黑洞。
- 在数重新传输后它了解DTL通道不可能设立，并且需要重新指定一个新的MTU值到VPN适配器。
- 此的目的重新连接是分配每新的MTU。

关于的更多信息请重新连接行为，并且计时器，参见AnyConnect FAQ ：通道，重新连接行为和不活动计时器

警告

Cisco Bug ID CSCuh61321 AC 3.1:ASA把柄不正确地交替DTL端口，原因重新连接

相关信息

- **AnyConnect FAQ ：通道，重新连接行为和不活动计时器**
- **技术支持和文档 - Cisco Systems**