修复AnyConnect重新连接导致的流量中断

目录

简介

本文档介绍当AnyConnect客户端在整整一分钟内重新连接到自适应安全设备(ASA)时发生的情况。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

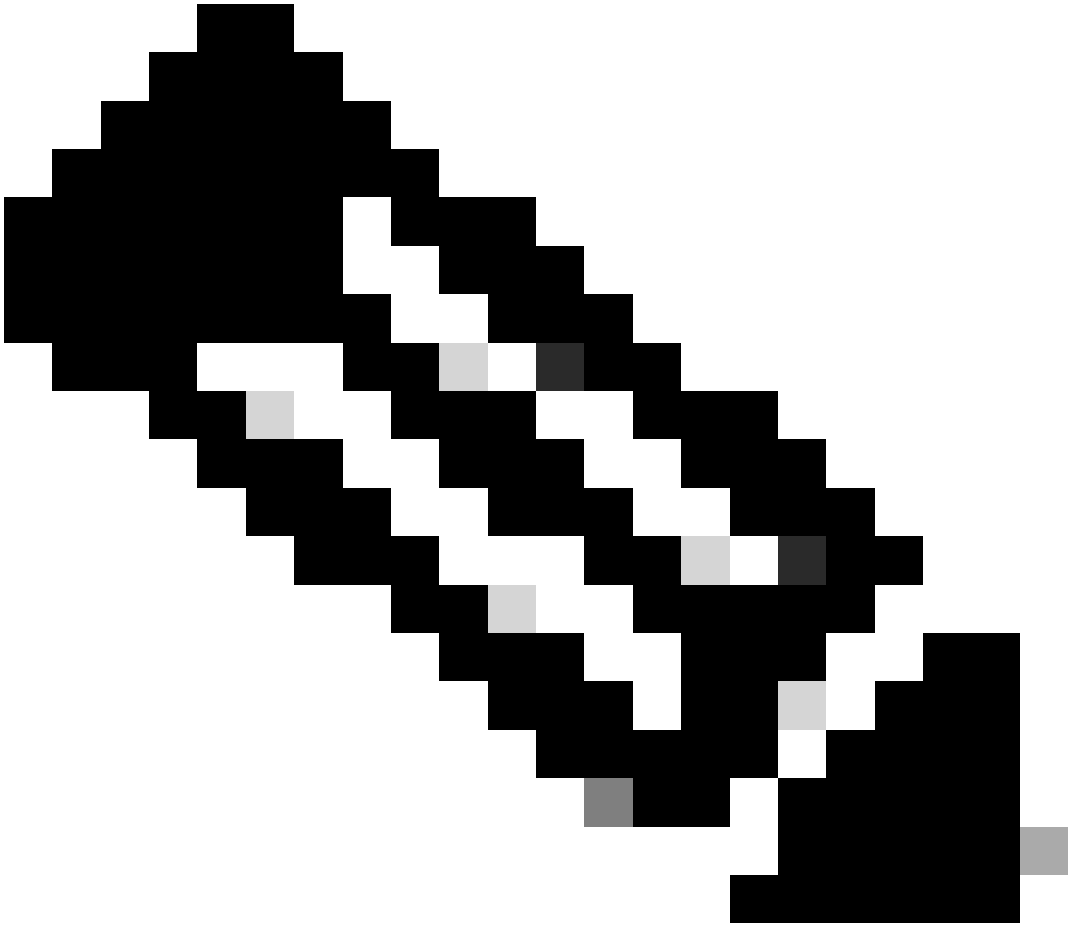
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

以下产品受此问题影响：

- ASA版本9.17
- AnyConnect客户端版本4.10

背景信息

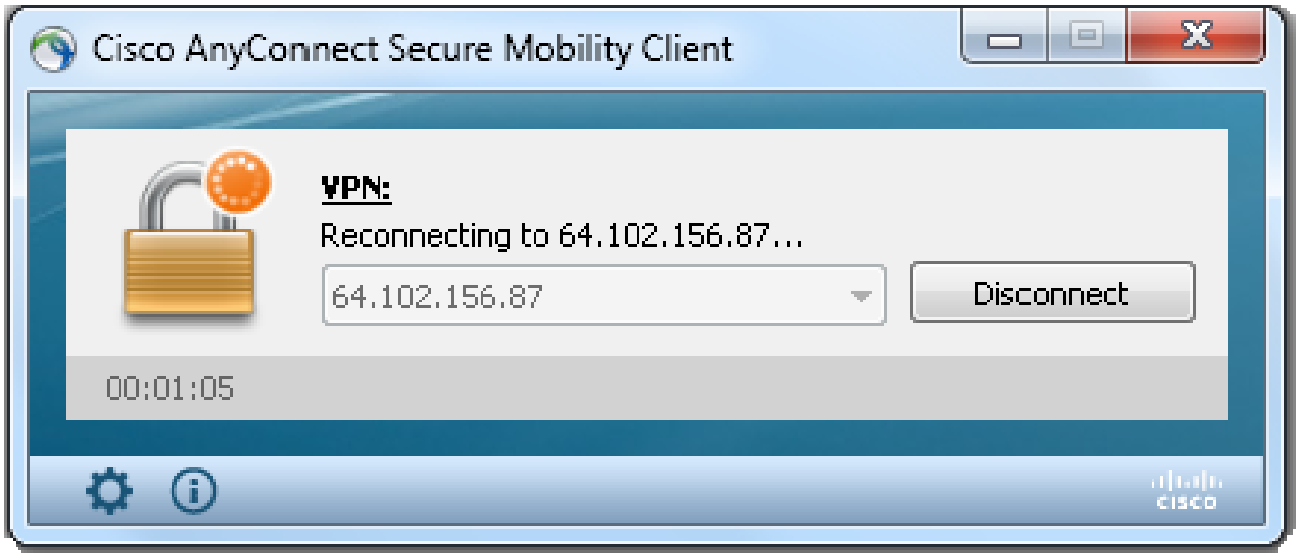


注意：AnyConnect已更名为Cisco Secure Client。没有其他任何更改，只有名称，并且安装过程是相同的。

如果AnyConnect客户端在一分钟内重新连接到自适应安全设备(ASA)，则在AnyConnect重新连接之前，用户无法通过传输层安全(TLS)隧道接收流量。这取决于本文档中讨论的几个其他因素。

症状

在本示例中，AnyConnect客户端在重新连接到ASA时显示。



在ASA上看到以下系统日志：

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

问题说明

出现此问题的诊断和Reporting工具(DART)日志如下：

<#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.

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

原因

此问题的原因是无法构建数据报传输层安全(DTLS)隧道。这可能是因为两个原因：

- DTLS在路径中的某个位置被阻止。
- 使用非默认DTLS端口。

DTLS在路径中的某个位置被阻止

从ASA版本9.x和AnyConnect版本4.x开始，已引入针对客户端/ASA之间的TLS/DTLS协商的不同最大过渡单元(MTU)形式的优化。以前，客户端推导出了涵盖TLS/DTLS的粗略估计MTU，并且明显低于最优估计MTU。现在，ASA会计算两种TLS/DTLS的封装开销并相应地获取MTU值。

只要启用DTLS，客户端就会在VPN适配器（在建立DTLS隧道之前启用并且需要路由/过滤器实施）上应用DTLS MTU（在本例中为1418），以确保最佳性能。如果DTLS隧道无法建立或某个点被丢弃，则客户端会故障切换到TLS，并将虚拟适配器(VA)上的MTU调整为TLS MTU值（这需要重新连接会话级别）。

分辨率

为了消除DTLS > TLS的这一可见转换，管理员可以为无法建立DTLS隧道（例如由于防火墙限制

）的用户配置一个单独的隧道组，使其只进行TLS访问。

1. 最佳选项是将AnyConnect MTU值设置为低于TLS MTU，然后协商。

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

这使TLS和DTLS MTU值相等。在这种情况下，看不到重新连接。

2. 第二个选项是允许分段。

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

使用分段时，大型数据包（其大小超过MTU值）可以分段并通过TLS隧道发送。

3. 第三个选项是将Maximum Segment Size (MSS)设置为1460，如下所示：

```
sysopt conn tcpmss 1460
```

在这种情况下，TLS MTU可以是1427 (RC4/SHA1)，大于DTLS MTU 1418 (AES/SHA1/LZS)。这解决了从ASA到AnyConnect客户端的TCP问题（得益于MSS），但是从ASA到AnyConnect客户端的大量UDP流量可能会受到此问题的影响，因为AnyConnect客户端MTU 1418较低，所以它可以被AnyConnect客户端丢弃。如果sysopt conn tcpmss被修改，可能会影响其他功能，例如LAN到LAN (L2L) IPSec VPN隧道。

重新连接工作流

假设配置了以下密码：

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

这种情况下会发生以下一系列事件：

- AnyConnect建立父隧道和TLS数据隧道，使用AES256-SHA256作为SSL加密。

- 路径中阻止了DTLS，因此无法建立DTLS隧道。
- ASA向AnyConnect通告参数，其中包括TLS和DTLS MTU值，这是两个独立的值。
- 默认情况下，DTLS MTU为1418。
- TLS MTU根据sysopt conn tcpmss值计算（默认值为1380）。以下是TLS MTU的生成方式（如debug webvpn anyconnect输出所示）：

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

- AnyConnect启动VPN适配器并向其分配DTLS MTU，以预测其可以通过DTLS进行连接。
- AnyConnect客户端现在已连接，用户将访问特定网站。
- 浏览器发送TCP SYN并在其中设置MSS = 1418-40 = 1378。
- ASA内部的HTTP服务器发送大小为1418的数据包。
- ASA无法将它们放入隧道中，并且无法对其进行分段，因为它们已设置不分段(DF)位。
- ASA打印并丢弃具有mp-svc-no-fragment-ASP丢弃原因的数据包。

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

- 同时，ASA会将ICMP Destination Unreachable， Fragmentation Needed发送给发送方：

```
%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
```

- 如果允许Internet控制消息协议(ICMP)，则发送方重新传输丢弃的数据包，一切开始工作。如果ICMP被阻止，则流量会在ASA上进入黑洞。
- 经过多次重新传输后，它知道无法建立DTLS隧道，需要为VPN适配器重新分配新的MTU值。
- 重新连接的目的是分配新的MTU。

有关重新连接行为和计时器的详细信息，请参阅AnyConnect常见问题：隧道、重新连接行为和非活动计时器

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。