当流量流经ASA， IPSec over TCP发生故障

目录

简介

连接对VPN头端使用IPSec over TCP另一方面的Cisco VPN Client也许连接到头端罚款，但是连接在一些时间以后失效。本文描述如何换成UDP的IPSec或本地ESP IPSec封装为了解决问题。

开始使用前

要求

使用IPSec over TCP，为了遇到此特定问题， Cisco VPN Client必须配置连接到VPN数据转发设备。在多数实例，网络管理员配置ASA接受在TCP端口10000的Cisco VPN Client连接。

使用的组件

本文档中的信息根据Cisco VPN Client。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

当VPN客户端为IPSec over TCP (cTCP)配置， VPN客户端软件不会响应，如果重复项TCP ACK是接收的询问VPN客户端的能重新传输数据。如果有包丢失在VPN客户端和ASA头端之间，复制确认也许生成。断断续续包丢失是在互联网的一相当普遍的实际情况。然而，因为VPN终端不使用TCP协议(收回他们使用cTCP)，终端将持续传送，并且连接将继续。

在此方案中，如果有另一个设备例如跟踪TCP连接的防火墙statefully，问题发生。因为cTCP协议不充分地实现复制确认不收到答复的TCP客户端和服务器，这能根据此网络数据流促成其它设备下降

TCP数据流。包丢失在造成TCP分段的网络必须发生失踪，触发问题。

这是没有bug，然而包丢失对网络和事实副作用cTCP不是实时TCP。cTCP设法通过包裹在TCP报头内的IPSec信息包模拟TCP协议，但是那是协议的范围。

此问题典型地发生，当网络管理员实现与IPS时的ASA，或者执行造成防火墙作为连接的一个全双工TCP代理的某类在ASA的应用检查。如果有包丢失， ASA代表cTCP服务器或客户端缺少数据的ACK，但是VPN客户端不会响应。因为预计的ASA从未接收数据，通信不能继续。结果，连接发生故障。

解决方案

为了解决此问题，请进行这些操作中的任一：

- 交换机从IPSec over TCP到UDP的IPSec或者与ESP协议的本地封装。
- 对AnyConnect客户端的交换机VPN终端的，使用充分地被实施的TCP协议栈。
- 配置ASA申请TCP状态旁路这些特定IPsec/TCP流。这根本禁用匹配TCP状态旁路策略的连接的所有安全性检查，但是允许连接工作直到从此列表的另一解决方法可以实现。欲知更多信息、参考的TCP状态旁路指南和限制。
- 识别包丢失的来源，并且采取纠正措施为了防止IPsec/TCP数据包丢弃在网络。这通常是不可能或非常困难，因为对问题的触发通常是在互联网的包丢失，并且丢包不可能被防止。

相关信息

- 技术支持和文档 - Cisco Systems