流量通过ASA时IPsec over TCP失败

目录

简介

使用IPsec over TCP连接到VPN前端的Cisco VPN客户端可能会连接到前端，但连接会在一段时间后失败。本文档介绍如何切换到IPsec over UDP或本机ESP IPsec封装以解决此问题。

开始使用前

要求

要遇到此特定问题，必须将Cisco VPN客户端配置为使用IPsec over TCP连接到VPN头端设备。在大多数情况下，网络管理员将ASA配置为接受通过TCP端口10000的Cisco VPN客户端连接。

使用的组件

本文档中的信息基于Cisco VPN客户端。

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客户端配置为IPsec over TCP(cTCP)时，如果收到重复的TCP ACK请求VPN客户端重新传输数据，VPN客户端软件将不会响应。如果VPN客户端和ASA头端之间有丢包，可能会生成重复的ACK。断断续续的丢包是Internet上比较常见的现实。但是，由于VPN终端未使用TCP协议（回想一下，它们正在使用cTCP），因此终端将继续传输并继续连接。

在此场景中，如果有其他设备（例如防火墙）有状态跟踪TCP连接，则会出现问题。由于cTCP协议未完全实现TCP客户端，且服务器重复的ACK未收到响应，这可能导致与此网络流一致的其他设备

丢弃TCP流量。必须在网络上丢包，导致TCP数据段丢失，从而触发问题。

这不是一个错误，而是网络上丢包和cTCP不是真实TCP的副作用。cTCP尝试通过在TCP报头中封装IPsec数据包来模拟TCP协议，但这是协议的范围。

当网络管理员实施具有IPS的ASA或在ASA上执行某种应用检查，导致防火墙充当连接的完整TCP代理时，通常会发生此问题。如果丢包，ASA将代表cTCP服务器或客户端确认丢失的数据，但VPN客户端永远不会响应。由于ASA从未收到其期望的数据，因此无法继续通信。因此，连接失败。

解决方案

要解决此问题，请执行以下任一操作：

- 从IPsec over TCP切换到IPsec over UDP，或使用ESP协议进行本地封装。
- 切换到AnyConnect客户端进行VPN终止，该客户端使用完全实施的TCP协议栈。
- 配置ASA以对这些特定IPsec/TCP流应用tcp-state-bypass。这实际上会禁用对匹配tcp-state-bypass策略的连接的所有安全检查，但允许连接工作，直到可以实施此列表中的其他解析。有关详细信息，请参阅TCP状态绕行指南和限制。
- 确定丢包的源，并采取纠正措施，防止IPsec/TCP数据包在网络中丢弃。这通常是不可能的，也是极其困难的，因为问题的触发因素通常是Internet上的数据包丢失，而且无法防止丢包。

相关信息

- 技术支持和文档 - Cisco Systems