

ASA吞吐量和连接速度故障排除和分析数据包捕获

摘要

简介

本文描述如何排除故障思科可适应安全工具(ASA)吞吐量和连接速度问题。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据思科可适应安全工具(ASA)。

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

一些客户也许遇到问题,当他们首先部署ASA时或,当他们测试新的连接时。问题是流经ASA是更低的比的连接的TCP吞吐量,当ASA不在连接路径时(或连接慢比,在ASA在网络实现)前。

例如,客户也许用ASA 5505或ASA 5510替换一个低端D林克路由器(或其他路由设备);然而,一旦路由器替换,非常地减少连接速度。客户也许提出有Cisco TAC的一个案件,因为他们相信ASA导致对连接速度的减少。

功能信息

故障排除方法

当有包丢失或信息包延迟在网络,TCP流减速。为了了解问题的确切的原因,数据必须显示在电线的实际TCP信息包该连接的,并且网络如何也许影响他们。通常网络管理员警告对问题,当他们进行一特定操作时,例如FTP文件传输或联机速度测试。问题可以经常被再次产生。所以,管理员能收集所需的数据为了查找根本原因。

在测验前后,为了收集所需的数据,应该从ASA运行**show tech**命令。此命令显示配置和信息包统计数据(主要从**show service策略**)并且显示,如果接口错误增加。

双向，同时数据包捕获(采取从受影响的两个ASA接口连接横断)要求充分地诊断问题的原因。

参考这些文档以如何应用数据包捕获为例到ASA：

- [排除通过 PIX 和 ASA 的连接故障](#)
- [TAC安全播客情节#1 -使用排除故障的ASA数据包捕获工具](#)

数据分析

一旦收集所需的数据，您能使用数据包捕获为了确定哪些问题也许已经出现：

- 在他们到达ASA的外部接口前，从外部主机的数据包丢弃或延迟。
- 数据包由ASA延迟或丢弃。
- 数据包在网络内部延迟或丢弃某处。

注意：此分析假设数据从在外部接口的一台主机发送到在内部接口的一台主机。

此视频显示示例如何执行在数据包捕获的分析：

联合TCP的数据流是技术考虑事项特定对此问题，因为，当您从事在ASA时的某些功能，防火墙充分地联合穿过它的TCP数据流。

例如，如果ASA发现在网络的一个丢失的信息包(因为没有接收在ASA)，它代表缺少数据的另一个TCP终端发送ACK。此方案最普通。如果ASA发现到达故障中的数据包，ASA重新排序数据包并且通过他们到接收方按适当的顺序。如果没有重拨网络的丢包或的数据包，没有副作用对启用此功能。如果由通过网络和ASA顺利地通过的任一个TCP终端的所有发送的数据包，您不会知道此功能启用，因为不采取在数据包流的行动。只有当有时与TCP连接的麻烦在网络进一步启用此功能减速网络流量。操作联合TCP数据流是非常资源密集为ASA。对于在网络丢弃的每数据包ASA必须不仅发送TCP数据包请求该数据包重新传输，但是必须也缓冲数据包发送方继续发送，在数据包失踪了后。

常见问题

在连接ASA到邻接设备的接口的不正确的配置的速度和双工值

当设备由ASA时，替换此问题经常出现。如果在ASA接口的速度和双工值不是相同的象在邻接设备的值，丢包在该接口发生。检查在ASA接口以及相邻接口的速度和双工值。

检查ASA的show interface输出是此问题症状的明显的错误：

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
```

```
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

发送流量到IPS模块

当ASA配置发送流量到IPS模块时，TCP数据流联合的功能在ASA从事。参考本文的[数据分析部分](#)关于TCP数据流联合的功能的更多信息。

TCP MSS选项的ASA修改导致轻微的性能降低

默认情况下ASA设置在SYN数据包的TCP MSS选项到1380。所以，TCP终端不应该传送TCP数据段大于1380个字节。此值比经常DEFAULT值更低1460个字节并且代表一TCP性能下降大约六百分比(6%)。性能也许改善是您增加设置在ASA的最大MSS或禁用MSS调整。在您修改default命令在ASA前，请了解风险介入关于潜在的分段，如果数据包在路径进一步被封装某处。

欲知更多信息，参考Cisco ASA 5500系列命令参考的[sysopt连接tcpmss](#)部分。

FAQ

相关信息

- [Cisco ASA 5500系列命令参考， 8.2](#)
- [技术支持和文档 - Cisco Systems](#)