ASA吞吐量和连接速度故障排除和分析数据包捕获

目录

简介

本文档介绍如何排除思科自适应安全设备(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

本文档中的信息基于思科自适应安全设备(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

一些客户在首次部署ASA或测试新连接时可能遇到问题。问题是，流经ASA的连接的TCP吞吐量比ASA不在连接路径中时要低得多（或连接比在网络中实施ASA之前慢得多）。

例如，客户可以用ASA 5505或ASA 5510替换低端D-Link路由器（或其他路由设备）；但是，更换路由器后，连接速度会大大降低。客户可能会向Cisco TAC提出问题，因为他们认为ASA导致连接速度降低。

故障排除方法

当网络中出现丢包或数据包延迟时，TCP流速会减慢。为了了解问题的确切原因，数据必须显示该连接线上实际的TCP数据包以及网络可能对它们产生的影响。通常，网络管理员在执行特定操作（如FTP文件传输或在线速度测试）时会收到问题警报。大多数情况下，问题是可以重现的。因此，管理员可以收集所需数据以查找根本原因。

为了收集所需数据，应在测试前后从ASA运行**show tech**命令。此命令显示配置和数据包统计信息(主**要来自show service-policy**)，还显示接口错误是否增加。

要完全诊断问题的原因，需要同时进行双向数据包捕获（从连接经过的两个受影响的ASA接口获取）。

有关如何将数据包捕获应用到ASA的示例，请参阅以下文档：

- 排除通过 PIX 和 ASA 的连接故障
- TAC安全播客第#1集 — 使用ASA数据包捕获实用程序进行故障排除

数据分析

收集所需数据后，可以使用数据包捕获来确定可能发生的以下问题：

- 来自外部主机的数据包在到达ASA的外部接口之前会被丢弃或延迟。
- 数据包被ASA延迟或丢弃。
- 数据包在内部网络的某个位置被延迟或丢弃。

注意：此分析假设数据是从外部接口上的主机发送到内部接口上的主机。

此视频显示如何对数据包捕获执行分析的示例：

*TCP数据流合*并是此问题特有的技术考虑因素，因为当您在ASA上使用某些功能时，防火墙会完全合并通过它的TCP数据流。

例如，如果ASA发现网络上缺少数据包（因为未在ASA处接收），它会代表其他TCP终端发送ACK来查找缺失的数据。这种情况最常见。如果ASA发现到达的数据包顺序混乱，ASA会重新排序数据包，并按正确顺序将其传递给接收方。如果没有网络丢包或数据包重新排序，则启用此功能不会产生任何副作用。如果任一TCP终端发送的所有数据包都成功通过网络和ASA，则您不会知道此功能已启用，因为它不对数据包流采取操作。只有当网络上的TCP连接出现故障时，此功能才会进一步降低网络流量。合并TCP流的操作对ASA而言非常占用资源。对于网络中丢弃的每个数据包，ASA不仅必须发送TCP数据包请求重新传输该数据包，还必须缓冲发送方在数据包丢失后继续发送的数据包。

常见问题

将ASA连接到相邻设备的接口上的速度和双工值配置错误

当设备被ASA替换时，通常会发生此问题。如果ASA接口上的速度和双工值与相邻设备上的值不同，则该接口上会发生丢包。检查ASA接口以及相邻接口上的速度和双工值。

检查ASA的**show interface**输出，以找出导致此问题的症状的明显错误：

```
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
```

将流量发送到IPS模块

当ASA配置为将流量发送到IPS模块时，ASA上会启用TCP流合并功能。有关TCP数据流合并功*能的详细*信息，请参阅本文档的数据分析部分。

ASA修改TCP MSS选项导致性能轻微下降

默认情况下，ASA将SYN数据包中的TCP MSS选项设置为1380。因此，TCP终端不应传输大于1380字节的TCP数据段。此值低于通常默认值1460字节，表示TCP性能下降约6%(6%)。 如果增加ASA上的最大MSS设置或禁用MSS调整，性能可能会提高。在ASA上修改默认命令之前，请了解如果数据包进一步封装在路径中某处，则可能的分段所涉及的风险。

有关详细信息，请参阅《Cisco ASA 5500系列命令参考》的*sysopt connection tcpmss部分*。

相关信息

- Cisco ASA 5500系列命令参考，8.2
- 技术支持和文档 - Cisco Systems