由于初期连接过多，DATAPATH上的CPU使用率高和FTD上的连接问题

目录

问题

在FTD设备上观察到高的CPU利用率，导致连接问题并阻止用户访问关键业务应用程序。防火墙显示数据路径和Snort CPU使用率提高，用户遇到延迟和间歇性访问问题。调查显示大量初期的TCP连接，其中很大一部分来自内部安全扫描程序，导致资源耗尽和性能下降。

环境

- 思科安全防火墙Firepower威胁防御(FTD)
- Hardware:Cisco Firepower 1150
- 软件版本:7.4.2.3
- 管理者：Firepower Management Center (FMC)
- 高可用性(HA)配置
- 数据路径和Snort CPU始终保持在100%或接近100%
- 内部扫描器导致大量初始TCP连接
- 最近的更改:应用和恢复日志收集器配置；访问规则部署；观察到的故障切换事件
- 生成被识别为内部Qualys扫描器的高连接的系统

分辨率

已确定用于流量处理的DATAPATH上的CPU使用率较高。

```
device# show processes cpu-usage sorted non-zero
Hardware:   FPR-1150
Cisco Adaptive Security Appliance Software Version 9.20(2)43
ASLR enabled, text region 562a19048000-562a1e49126d
PC         Thread       5Sec     1Min     5Min   Process
   -          -        99.7%    99.7%    99.7%   DATAPATH-4-22658
   -          -        99.7%    99.7%    99.6%   DATAPATH-3-22657
   -          -        99.7%    99.6%    99.6%   DATAPATH-2-22656
   -          -        99.6%    99.7%    99.7%   DATAPATH-5-22659
   -          -        97.5%    97.1%    97.1%   DATAPATH-1-22655
   -          -        97.4%    97.1%    97.1%   DATAPATH-0-22654
0x0000562a1b8c55e3   0x0000151e97f523e0     1.1%     1.6%     1.6%   CP Processing
0x0000562a1d408771   0x0000151e97f434a0     0.4%     0.2%     0.0%   Unicorn Proxy Thread
0x0000562a1b6ba40a   0x0000151e97f3cb80     0.3%     0.3%     0.3%   appagent_async_client_receive_thre
0x0000562a1cfebc65   0x0000151e97f43f80     0.1%     0.1%     0.1%   IP SLA Mon Event Processor
0x0000562a1d328a89   0x0000151e97f64240     0.1%     0.1%     0.1%   lina logclient Rx data thread
0x0000562a1d72eb46   0x0000151e97f417a0     0.0%     0.1%     0.0%   cli_xml_request_process
```

```
0x0000562a1df983a5    0x0000151e97f69940      0.0%      0.1%      0.0%    Checkheaps
```

从FTD CLI中导出了show conn detail输出，供内部自动化工具查看连接统计信息。

注意：如果连接计数超过100,000，则CLI中的show conn detail输出可能会非常长。请确保为此集合分配了足够的时间。

disk0与FTD后端中的/mnt/disk0/目录对应。请相应地导出文件。

```
device# show conn detail | redirect disk0:/shconndetMMDDYY.txt
```

查看用于大量初期连接的工具结果的连接统计信息：

```
Total Emryonic Conns: 121611. This is 87.984% of the total conns (138219)
--
Top-5  Embryonic IPs (SYN, but not SYN/ACK - 'aA' flags) going through the device
IP                                                Count    Percent
-----------------------------------------------------------------
10.5.30.77                                        81519    33.517%
10.1.30.102                                       40042    16.463%
10.1.212.14                                         907     0.373%
10.1.204.4                                          837     0.344%
10.1.21.122                                         804     0.331%
```

确定源IP后（在本例中为内部安全扫描程序），阻止源生成流量并清除其与FTD的连接。

```
device# clear conn add 10.5.30.77
4563 connection(s) deleted.
device# show conn count
5936 in use, 465189 most used
Inspect Snort:
        preserve-connection: 4451 enabled, 0 in effect, 432406 most enabled, 0 most in effect
```

在缓解后监控CPU利用率，以确认原因是由流量引发的。

```
device# show cpu
CPU utilization for 5 seconds = 9%; 1 minute: 28%; 5 minutes: 70%
```

流量连接应恢复正常，并且不应再观察到延迟。

原因

高CPU和连接问题的根本原因是内部安全扫描仪生成的过多初期连接。这些连接（主要是没有相应SYN/ACK响应的SYN数据包）不堪重负FTD数据路径和Snort进程。大量不完整连接导致资源耗尽，导致CPU使用率持续较高、连接间歇性以及对关键业务应用程序访问的影响。

相关内容

- 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）。