High CPU on DATAPATH and Connectivity Issues on FTD Due to Excessive Embryonic Connections

Contents

Issue

High CPU utilization was observed on FTD devices, leading to connectivity problems and preventing users from acc

Environment

- Cisco Secure Firewall Firepower Threat Defense (FTD)
- Hardware: Cisco Firepower 1150
- Software Version: 7.4.2.3
- Managed by: Firepower Management Center (FMC)
- High Availability (HA) configuration
- Datapath and Snort CPU consistently at or near 100%
- High number of embryonic TCP connections due to internal scanners
- Recent changes: Log collector configurations applied and reverted; access rule deployment; observed failover event
- Systems generating high connections identified as internal Qualys scanners

Resolution

Identified High CPU Usage on DATAPATH used for traffic processing.

```
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
```

From the FTD CLI, an output of **show conn detail** was exported for review of Connection Statistics by internal auto

CAUTION: The output of **show conn detail** from the CLI can be extremely long if the connection count is over 100

The disk0 corresponds with /mnt/disk0/ directory in the FTD backend. Export the file accordingly.

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

Review the connection statistics from the results of the tool for embryonic connections in high amounts:

```
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%
```

After identifying the source IPs (in this case, internal security scanners), prevent the source from generating the traff

```
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
```

Monitor CPU Utilization After Mitigation to confirm that the cause was traffic-induced.

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

Traffic connectivity should return to normal, and latency should no longer be observed.

Cause

The root cause of high CPU and connectivity issues was excessive embryonic connections generated by internal secu
critical application access.

Related Content

- Cisco Technical Support & Downloads