FTD High CPU Core Alerts from Pruner.pl Process

Issue

FMC generates frequent high CPU utilization alerts for multiple managed FTD devices, and raise concerns about firewall performance and stability. Specifically, the FMC health monitor shows repeated CPU core spikes on specific cores over extended periods, with the internal Pruner.pl background process consistently consuming excessive CPU for the specified cores. Despite these critical CPU alerts appearing in FMC, no user-visible traffic impact is observed, and overall FTD stability remains unaffected.

Environment

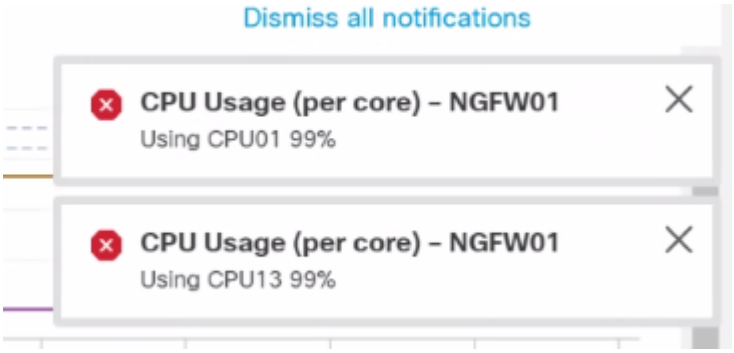
- FTD Software Version: 7.2.5 (affects both virtual and hardware models in all versions lesser than 7.2.6)
- Devices managed by Firepower Management Center (FMC)

Resolution

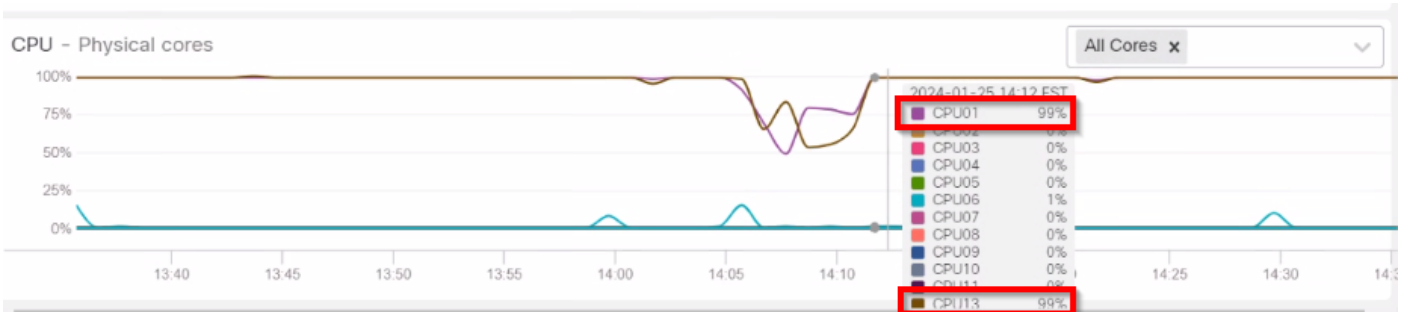
The resolution involves upgrading the affected FTD devices to a software version that contains the fix for the identified defect.

Troubleshooting and Analysis Steps

1: Examine the CPU utilization patterns in the FTD Health Monitor graphs over time to identify the scope and timing of the issue. The analysis reveals repeated CPU core spikes on specific cores occurring, while overall CPU and memory utilization remained within normal operating ranges.



inline_image_0.png



inline_image_1.png

```
Health Monitor Alert | Time: Mon Jul 24 06:34:20 2023 UTC | Severity: critical | Module: CPU Usage (per
Health Monitor Alert | Time: Mon Jul 24 04:24:20 2023 UTC | Severity: critical | Module: CPU Usage (per
```

2: Analyze FTD CLI and troubleshoot bundles from the affected FTD to identify the root cause of high CPU utilization.

3: Review the collected data to identify which processes are consuming excessive CPU resources. The analysis of top.log files confirmed that the Pruner.pl process was consistently using high CPU on certain cores, with the issue pattern starting around a specific timeframe.

```
root@FTDdevice:/home/admin# cd /ngfw/var/log/
root@FTDdevice:/ngfw/var/log# grep "Pruner.pl --persistent" top.log | grep -v "S   0.0"
 12341 root      20   0  458920 437816  10056 R 100.0   0.2   9452:10 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9453:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9454:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R  94.1   0.2   9455:15 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9456:18 /usr/bin/perl /ngfw/usr/local/sf/
```

The logs also show a high count of empty, 0-byte"*snort-unified.log" files which are the main reason for the Pruner.pl running so often.

```
root@FTDdevice:/home/admin# cd /ngfw/var/sf/detection_engines/FTD-UUID/
root@FTDdevice:/ngfw/var/sf/detection_engines/FTD-UUID# ls -l instance-* | grep -ri "root        0.snor
-rw-r--r--  1 root    root        0 Nov 12 19:47 snort-unified.log.1699818430
-rw-r--r--  1 root    root        0 Nov 12 19:41 snort-unified.log.1699818093
```

```
-rw-r--r--  1 root    root        0 Nov 12 19:35 snort-unified.log.1699817758
-rw-r--r--  1 root    root        0 Nov 12 17:13 snort-unified.log.1699809226
-rw-r--r--  1 root    root        0 Nov 12 17:08 snort-unified.log.1699808890
-rw-r--r--  1 root    root        0 Nov 12 17:02 snort-unified.log.1699808554
```

Software Upgrade Solution

1: Upgrade all affected FTD devices to a software version that contains the fix for CSCwh79095. The minimum recommended versions are:

- FTD 7.2.7 (minimum fix version in 7.2.x train)
- FTD 7.4.1 or later (recommended upgrade path)

2: After the upgrade, monitor FMC health alerts to confirm that:

- CPU utilization per core remains stable
- No new critical alarms are raised for Pruner.pl or similar background processes
- High CPU alerts for the Pruner.pl process no longer occur

Prevention and Best Practices

Implement these recommendations to prevent similar issues:

- Avoid running older code trains long-term and plan periodic upgrades to recommended releases to benefit from bug fixes and security updates
- Before major upgrades, review Cisco release notes and perform bug searches for known defects on current and target versions
- Continue monitoring FMC health alerts after upgrades to ensure system stability
- Review any special upgrade considerations documented in release notes

Cause

The high CPU alerts are caused by a software defect in FTD 7.2.5 identified as Cisco Bug ID CSCwh79095. This defect is due to empty, 0-byte snort-unified.log files which causes the internal Pruner.pl background process to consume excessive CPU on specific cores. This triggers persistent high-CPU alarms in FMC. Importantly, this condition does not affect data-plane traffic forwarding or overall device stability; it only generates critical CPU alerts in the management interface. The issue is related duplicate bugs including

CSCwe66384 (Pruner.pl and disk manager high CPU with no obvious disk issues) and CSCwf80946 (FTD: Pruner process using excessive System CPU cores and generating FMC HM alerts).

Related Content

- Cisco Bug ID CSCwh79095 - Snort generating an excessive number of snort-unified log files with zero bytes (Fixed in: 7.2.7, 7.4.1, 7.6.0)
- Cisco Bug ID CSCwf77994 - False critical high CPU alerts for FTD device system cores running instantaneous high usage (Fixed in: 7.2.9, 7.4.1, 7.6.0)
- FTD/FMC Release Notes and Recommended Releases documentation
- Cisco Technical Support & Downloads