Troubleshoot an Unresponsive Cisco Secure Firewall

Contents

Introduction

This document describes the recommended steps to troubleshoot a Cisco Secure Firewall Threat Defense (FTD) that is unresponsive on 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx, and 93xx hardware platforms.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco Secure FTD basics (installation/configuration).

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Cisco Firepower eXtensible Operating System (FXOS)

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In some cases, a Cisco FTD device can become unresponsive. Typical symptoms include:

- No SSH access.
- No console access.
- Console access is working, but login credentials are not.
- Transit traffic is not going through the device.
- Interfaces are down (data and or management).
- LEDs are off or amber (blinking or solid).
- Secure module (4100, 9300) becomes unresponsive.

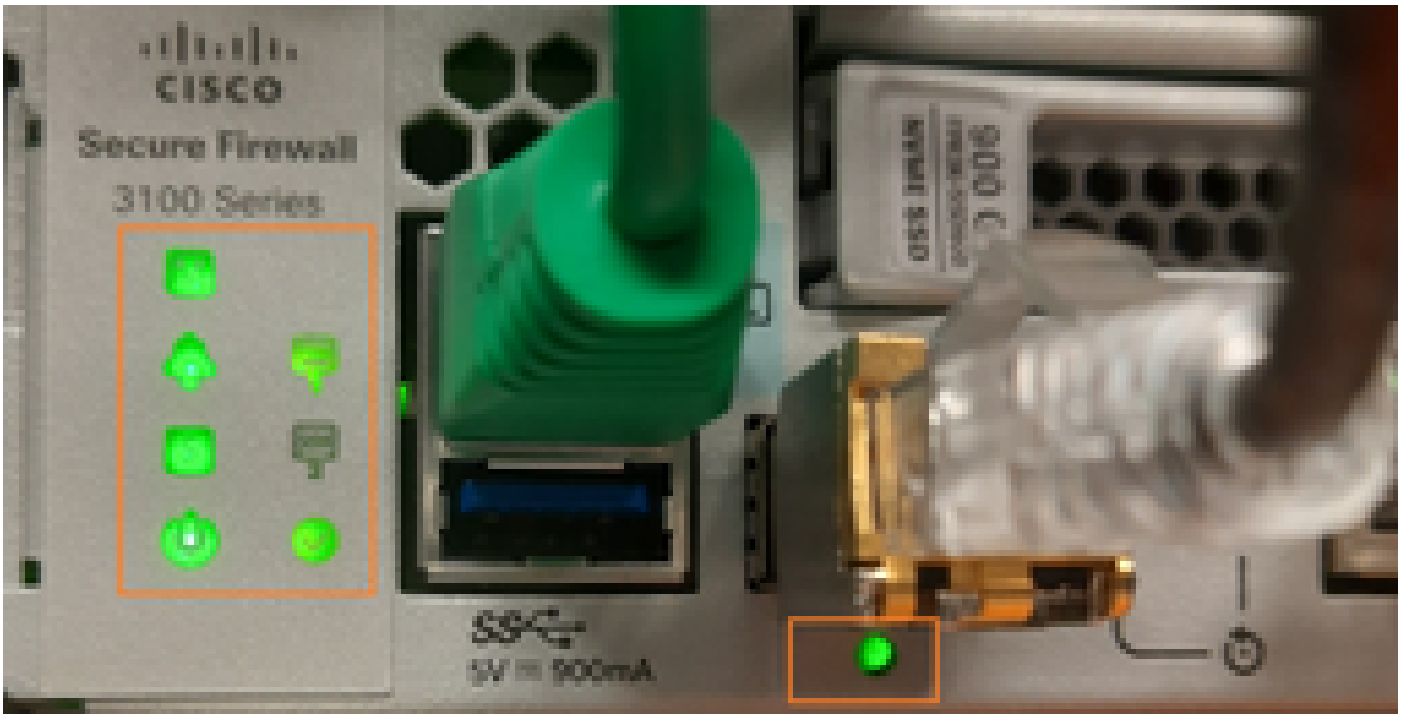
Note that, depending on the situation, some of them are not going to be present. For example, you could have transit traffic going through, but only management access is not working.

Troubleshoot

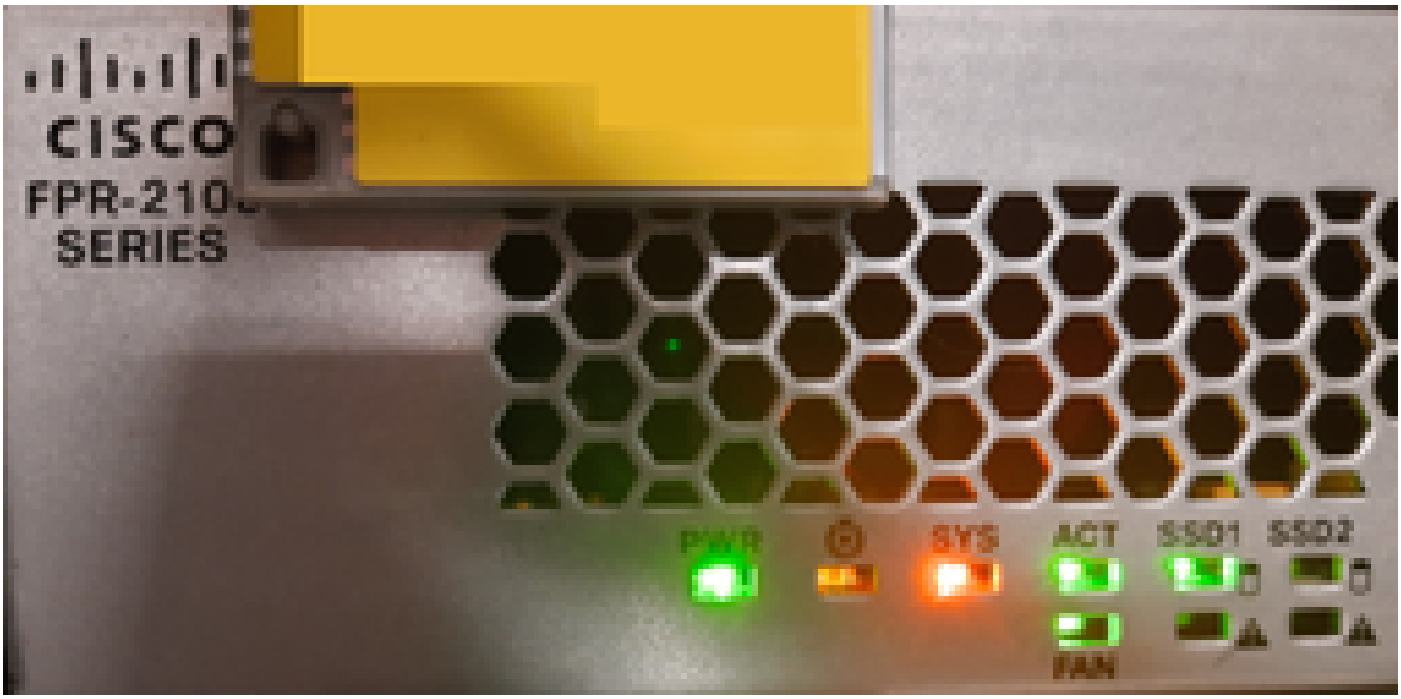
This section covers the recommended steps and actions that you need to take. You can provide this information to Cisco TAC for further analysis.

Step 1: Visual Inspection (Front Panel)

Take a video or a picture of the front panel LEDs. Here are some examples where all the LEDs are clearly visible:



In the next photo, the SYS LED indicates a device problem:



You can consult the hardware guide of your device model to get additional information about the LED, for example:

Model	LED info
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overview.html#
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/overview.html#
1210CE, 1210CP, 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-1210-20/m_o
1230, 1240, 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-1230-40-5
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/overview.l
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/m-overview
4110, 4120, 4140, 4150	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/overview.l

4112, 4115, 4125, 4145	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.html#conc
4200	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200-install/m-overview
9300	https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300/b_install_g

Step 2: Visual Inspection (Rear Panel)

Take a video or a picture of the LEDs at the rear panel, for example:

If you don't see any power LEDs on:

- Try to reseat the power supplies (whenever applicable).
- If possible, try to replace the power supply.

Step 3: Fan Checks

Verify if the fans in the back of the appliance are running.

Step 4: Physical Environment Checks

Verify if there is any noise or smell coming from the device.

Step 5: Console and Management Ports Checks

Make sure that the console and management ports are properly connected. If the problem is only on the management port, try to change the SFP (whenever applicable) and the network cable.

Step 6: Management IP Connectivity Test

Try to ping (ICMP) the management IP of the device.

Step 7: Adjacent Devices Checks

Check the port status of the adjacent devices, for example:

<#root>

```
switch#
```

```
show interface description | i FW-4215-1
```

```
Gi7/1                          up             up       FW-4215-1 ETH1/1
Gi7/2                          up             up       FW-4215-1 ETH1/2
Gi7/3                          up             up       FW-4215-1 MGMT
```

Step 8: HA/Cluster Device Checks

In case of a high availability (HA) or a cluster setup, collect a troubleshoot bundle from the peer device(s).

Step 9: Collect Console Logs

Attach a laptop to the console port and copy any messages shown. Try to press the up/down keyboard keys or the PageUp to see all the messages on the screen.

Step 10: Perform a Cold Reboot

With a laptop attached to the console port:

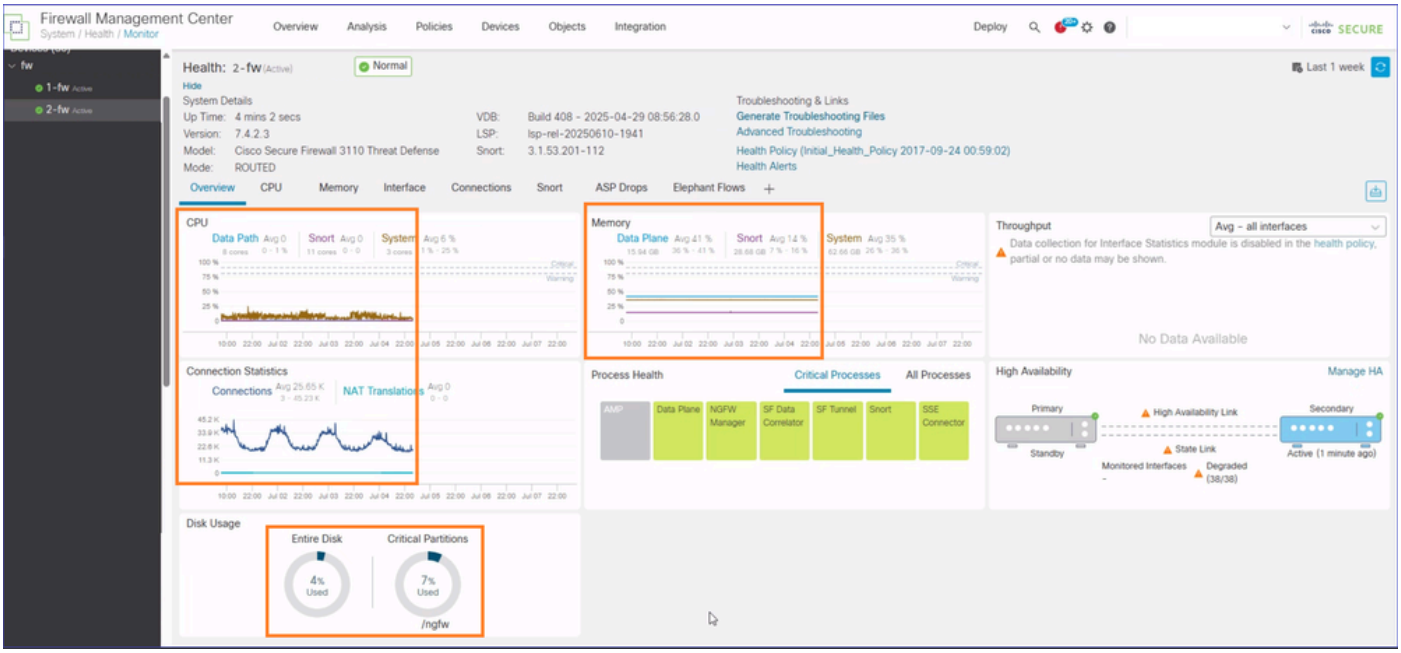
1. Unplug all power cables and wait a couple of minutes before plugging them back.
2. In case of a failover setup or a cluster setup, to minimize any risk of Active/Active or Cluster instability, you can unplug or shutdown from the adjacent switch device all the data interfaces of the affected unit including the HA or CCL links.
3. Then, re-plug the power cables and power on the device.
4. Wait ~5 minutes.

5. Collect the console output.

Note that if the device was not gracefully shut down and the device was operational (the front panel LEDs were on), the cold reboot can cause a database corruption. If the cold reboot brings up the device, collect a troubleshoot bundle and contact Cisco TAC.

Step 11: Collect Health Monitor graphs from FMC

If the device recovers and is managed by an FMC, navigate to **System> Health > Monitor**, and select the device. Focus on the highlighted graphs to understand what the status of the device was before getting unresponsive (for example, high memory, high CPU, high disk utilization, and so on).



Step 12: Check for disk issues

Non-working scenario (4100):

<#root>

FW4100#

show server storage

```
Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD12345678
        HW Revision:
        PCI Addr: 00:31.2
```

```
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
           Vendor: Micron
           Model: 5300 MTFD
           Serial: MSA123456AB
           HW Rev:
           Operability: N/A


       Presence: Missing <-----


           Size (MB): 200000
           Drive State: Online
           Power State: Active
           Link Speed: 6 Gbps
           Device Type: SSD

         Local Disk Config Definition:
            Mode: NO RAID
            Description:
            Protect Configuration: No
```

Sample output from 3100 where disk is operational:

<#root>

```
FW3105#
```

show server storage

```
Server 1/1:
    Disk Controller 1:
        Type: SOFTRAID
        Vendor: Cisco Systems Inc
        Model: FPR_SOFTRAID
        HW Revision:
        PCI Addr:
        Raid Support: raid1
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Optimal

        Local Disk 1:
            Presence: Equipped
            Model: SAMSUNG MZQL2960HCJR-00A07
            Serial: S64FNT0AB12345
```

Operability: Operable   <---

```
            Size (MB): 858306
            Device Type: SSD
            Firmware Version: GDC5A02Q
```

```
        Virtual Drive 1:
            Type: Raid
            Blocks: 878906048
            Operability: Degraded
            Presence: Equipped
            Size (MB): 858306
            Drive State: Degraded
```

Sample output from 4100 where disk is operational:

<#root>

FW4125#

show server storage

```
Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD1234567
        HW Revision:
        PCI Addr: 00:31.2
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
            Vendor: TOSHIBA
            Model: KHK61RSE
            Serial: 11BS1234567AB
            HW Rev: 0
```

Operability: Operable

```
            Presence: Equipped
            Size (MB): 800000
            Drive State: Online
            Power State: Active
            Link Speed: 6 Gbps
            Device Type: SSD

        Local Disk Config Definition:
            Mode: No RAID
            Description:
            Protect Configuration: No
```

Step 13: Log analysis

If the firewall device recovers and you would like to analyze the backend logs, generate a troubleshoot bundle and check the files mentioned in the table. Note that:

- On 1xxx, 12xx, 21xx (appliance mode), 31xx, 42xx platforms, the FTD troubleshoot bundle also contains the chassis (FPRM) bundle from FXOS in the \dir-archives\var-common-platform_ts\ path. You have to extract the contents of the FPRM bundle.
- On 3100/4200 in Multi-Instance (MI) mode collect chassis TS file from FMC UI or the chassis CLI (**show tech-support fprm detail** from the **local-mgmt** command scope) as described in https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400.
- On 41xx, 93xx platforms, you have to generate the chassis bundle separately either from the chassis UI, or the FXOS CLI as described in https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400
- For 4100 and 9300 device platforms, you need to collect **FXOS** and **FTD** troubleshoot bundles. For all the other platforms, the FTD troubleshoot bundle is enough since it also contains the FXOS troubleshoot bundle.
- For ASA the '**show tech-support**' command output after the recovery is not be very helpful. You have to rely on the FXOS troubleshoot bundle.
- Compared to other platforms, on 41xx, 93xx you have two troubleshooting bundles: **chassis** (BC1) and **module** bundle.
- The chassis bundle (BC1) on 41xx, 93xx, contains among others the FPRM and CIMC bundles.
- The module bundle on 41xx, 93xx contains mainly FXOS logs from the blade.
- If you have an ASA installed, you have to rely only on the chassis, FPRM and module bundles (whenever applicable) and the '**show tech-support'** command output from ASA.
- Depending on the platform and incident, not all files are going to be present.

File Path in the Troubleshoot Bundle	**Description/Ti**
FTD TS bundle: /dir-archives/var-log/messages*	The string 'sysl shutting down' shown during a graceful shutdo The string 'sysl starting up' is s when the devic starts.
FTD TS bundle: /dir-archives/var-log/ASAconsole.log In case of ASA on 4100/9300, you can also find the file in the Module bundle under /opt/cisco/platform/logs/ASAconsole.log	Look for errors failures, and so
FTD TS bundle: /dir-archives/var-log/dmesg.log	Look for errors failures, and so
FTD TS bundle: /dir-archives/var/log/ngfwManager.log*	Look for errors failures, and so

	This file also co information abo HA/Cluster eve
FTD TS bundle: /command-outputs/LINA_troubleshoot/show_tech_output.txt	The output of th '**show failover history**' and '**sh cluster' history** provide additio insights of the sequence of the events.
FTD TS bundle: /command-outputs/ Filenames: · for CORE in `ls opt-cisco-csp-cores _ grep core`_ do file -opt-cisco-csp-cores-_{CORE}_ done.output · for CORE in `ls var-common _ grep core`_ do file var-common-_{CORE}_ done.output · for CORE in `ls var-data-cores _ grep core`_ do file -var-data-cores-_{CORE}_ done.output	Check for poten core files (trace
FTD TS bundle: /dir-archives/var/log/crashinfo/snort3-crashinfo.*	Check for Snor crashinfo files.
FTD TS bundle: /dir-archives/var/log/process_stderr.log*	Check for Back (for example C bug ID CSCwh
FTD TS bundle: /dir-archives/var/log/periodic_stats/	The directory c multiple files th provide insight the time of the incident.
FPRM bundle: tech_support_brief	Check the 'sho detail' outputs.
FPRM bundle: /opt/cisco/platform/logs/kern.log	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/messages*	Look for errors failures, and so

FPRM bundle: /opt/cisco/platform/logs/mce.log The same file also exists in the module bundle (41xx, 93xx).	This is the Mac Check Exceptio (mce) file. Loo errors, faults, fa and so on.
FPRM bundle: /opt/cisco/platform/logs/portmgr.out	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/ssp-pm.log The same file also exists in the module bundle (41xx, 93xx).	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/sma.log The same file also exists in the module bundle (41xx, 93xx).	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/heimdall.log	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/ssp-shutdown.log The same file also exists in the module bundle (41xx, 93xx).	It contains the of **ps**, **top** and f lines from **dme** when reboot or shutdown is ini Available on 1000/2100/310
FPRM bundle: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	Look for errors failures, and so
FPRM bundle: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	Look for errors failures, and so
CIMC bundle (41xx, 93xx): /obfl/obfl-log*	Look for errors failures, and so
CIMC bundle (41xx, 93xx): /CIMC1_TechSupport.tar.gz/CIMC1_TechSupport.tar/tmp/techsupport_pid*/CIMC1_TechSupport-	Look for errors failures, and so

nvram.tar.gz/CIMC1_TechSupport-nvram.tar/nv/etc/log/eng-repo/messages*	Especially for CATERR
Module bundle (41xx, 93xx): /tmp/mount_media.log/mount_media.log	Look for errors failures, and so

Step 14: Captures

If a specific interface becomes unresponsive take captures on the firewall and the adjacent device. You can refer to this document for details:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Additionally, ensure that the ARP and CAM tables of the adjacent devices are properly populated.

Step 15: Additional Information to Provide to Cisco TAC

In addition to the items mentioned above, it is highly recommended to also provide this information:

15a. If the device recovered collect a troubleshoot bundle (check step 13 for details).

15b. If the device is still unresponsive provide the this information:

- Hardware information (model).
- Software information.
- FMC software information (if applicable).
- Deployment (Standalone/HA/Cluster).

15c. Approximate time (date/time) when the device became unresponsive.

15d. Approximate uptime of the device before it became unresponsive.

15e. Is this a new setup or an existing one?

15f. What was the last action performed before the device becoming unresponsive?

15g. Firewall data plane (LINA) syslogs from the time the device got unresponsive (try to get logs starting ~5 minutes before the incident). As a best practice, it is recommended to configure syslogs at level 6 (Informational).

15h. In case you have configured a syslog server on the chassis (FXOS on 4100/9300) provide the logs (starting ~5 minutes before the incident).

15i. Syslogs from the adjacent devices from the time of the incident.

15j. Topology diagram that shows the physical connections between the firewall device and the adjacent devices.

Common Issues

Error: Timed out communicating with DME

If you connect to the console and see:

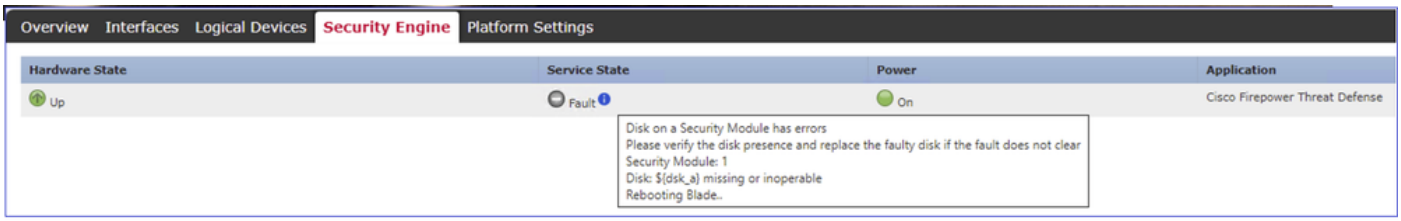
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

Most of the times, this indicates a software problem.

Recommended Action: Contact Cisco TAC

Disk error: missing or inoperable

This output is from a 4100/9300 hardware appliance where a disk-related fault is generated:



Recommended Action: Try reseating the SSD disk. If it does not help, collect chassis troubleshoot bundle and contact Cisco TAC.

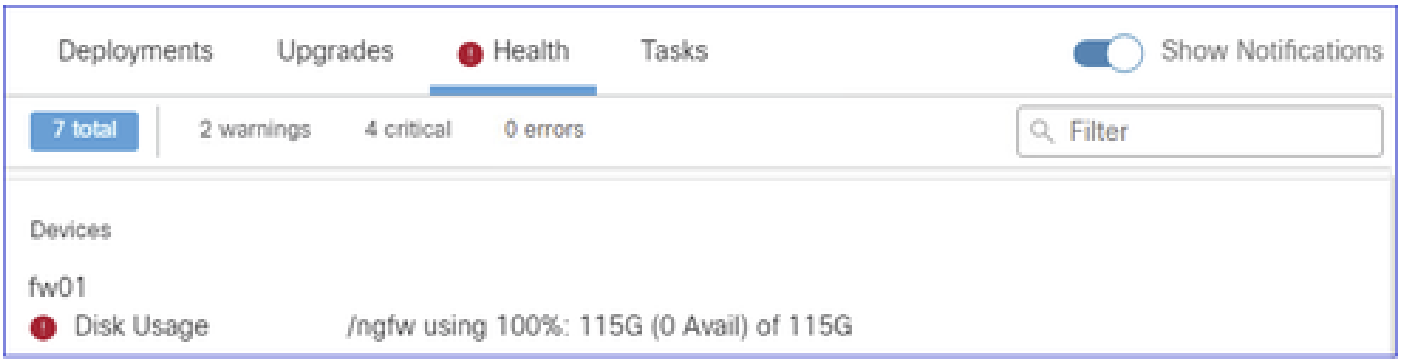
Field Notice: FN72077 - FPR9300 and FPR4100

- The FPR9300 and FPR4100 Series security appliances no longer pass network traffic.
- Users with valid credentials are not able to log in to the management console.
- CLI shows error message: "Software Error: Exception during execution: [Error: Timed out communicating with DME]

Recommended Action: A power-cycle of the 4100/9300 chassis is required in order to temporarily recover from this issue. Check Cisco bug ID CSCvx99172 for details and a version that has a fix.
(Field Notice: FN72077 - FPR9300 and FPR4100 Series Security Appliances - Some Appliances Might Fail to Pass Traffic After 3.2 Years of Uptime).

Disk Utilization 100%

Low disk space on the firewall can render the device unresponsive. If the device is managed by FMC you can get health alerts like this:



Recommended Action: If you have FMC and FTD running on software 7.7.0 and higher, try to clear some disk space using the procedure documented at https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space

If this is not feasible or does not help, contact Cisco TAC.

CSF 3100 does not come up after a power outage

Recommended Action: Upgrade to a software release that has a fix for:

Cisco bug ID CSCwm14729
CSF 3100 series not rebooting after power outage, requiring manual power cycle.

Cisco Firepower 2100 Series Security Appliances: Some Units Can Experience

Memory Failures

- DIMM failures within 5 years of service due to component process issues
- Related FN: https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html
- Related Cisco bug ID CSCwb74948

Recommended Action: Replacement of DIMM components or replacement of the security appliance

References

- https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html
- https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#
- https://www.cisco.com/c/en/us/support/docs/field-notices/720/fn72077.html
- https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/216245-collection-of-core-files-from-a-firepowe.html#anc6
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html