

Troubleshoot Firepower 1010 Continuous Reboot (Boot Loop) with Multiple AnyConnect Images after Software Upgrade

Contents

Issue

After software upgrade, Firepower 1010 continuously reboots (also known as the boot loop).

The terminal session shows the “**mmap64: Cannot allocate memory**” error messages and the Firepower eXtensible Operating System (FXOS) shutdown messages:

```
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
Rebooting ... (status 0x9)
```

```
Jun 24 08:25:48 root: FXOS shutdown log started: pid = 39475 cmdline = /bin/sh/sbin/fxos log_shutdown #
Jun 24 08:25:49 root: FXOS shutdown log completed: pid = 39475
The system is going down for reboot NOW!
```

Environment

- FMC-managed standalone Firepower 1010
- First seen after the software upgrade from version 7.4.2 to 7.6.4. Other versions can also be affected
- On the firewall, remote access virtual private network (RAVPN) is configured with multiple AnyConnect/Secure Client images

Resolution

Permanent resolution requires software upgrade to the version with the fix of Cisco bug ID [CSCwc82675](#).

As a workaround, reduce the number of AnyConnect/Secure Client images to prevent the firewall from continuous reboot.

These steps are verified on a standalone firewall:

1. Check if the system is in fail-safe mode. The fail-safe mode for the FTD/ASA application on Firepower 1000/2100 or Secure Firewall 3100 is activated due to continuous boot loop, traceback, and so on. If the firewall reboots 7 times within 7200 (increased from **3600** seconds with the fix of Cisco bug ID [CSCwj91341](#))seconds,the firewall enters the fail-safe mode and reboot stops. When the system is in the fail-safe mode:

- The system name is appended with the **-failed** string:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- The output of the **show failsafe-params** command in the FXOS **local-mgmt** command shell contains a warning message:

```
<#root>
```

```
firepower-1010-failed(local-mgmt)#
```

```
show failsafe-params
```

```
Max Restart: 1
```

```
Current Reboot Count: 1
```

```
Restart Time Interval(secs): 3600
```

```
WARNING: System in Failsafe mode. Applications are not running!
```

2. If the system is not in the fail-safe mode, then you can accelerate activation of the fail-safe mode by setting **Max Restart** to **Current Reboot Count + 1**:

```
<#root>
```

```
firepower-1010#
```

connect local-mgmt

firepower(local-mgmt)#

show failsafe-params

Max Restart: 7

Current Reboot Count: 2

Restart Time Interval(secs): 3600

firepower-1010(local-mgmt)#

config failsafe-max-restart

0 shall Disable Failsafe Mode!!!

Set a max_restart (0-8) value Or [x] to exit:

3

System may come up in Normal state post Reboot.

Configuration Successful

firepower-1010(local-mgmt)#

show failsafe-params

Max Restart:

3

Current Reboot Count:

2

Restart Time Interval(secs): 3600

3. Upon the next reboot, the firewall enters the fail-safe mode. Refer to step 1 for verification.

4. When the firewall boots, it enters the fail-safe mode. As soon as the login prompt appears, log in to the firewall, connect to the firewall using the **connect ftd** command and switch to the expert mode:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

```
firepower-1010:/$
```

5. In the expert mode, check AnyConnect/Secure Client images in startup config:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex "Mac OS"
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

6. Copy the file /mnt/disk0/.private/startup-config to the directory /ngfw/var/common. This step is important:

```
<#root>
```

```
firepower-1010:~$
```

```
cp /mnt/disk0/.private/startup-config /ngfw/var/common/
```

```
firepower-1010:~$
```

```
ls -l /ngfw/var/common/
```

```
total 12
```

```
...
```

```
-rwxr-xr-x 1 admin admin 11305 Jun 25 09:20
```

```
startup-config
```

7. Decide which images can be deleted.

8. Delete the lines with images from step 5 until there are a maximum of 2 images. Use **vim** or, alternatively, delete lines using the **sed** command as follows:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
```

```
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"
```

```
anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex "Mac OS"
```

```
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

```
firepower-1010:/$#
```

```
sudo sed -i '\#anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex
```

9. Confirm that the line is deleted:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
```

```
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"
```

```
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

10. Return to the FXOS local-mgmt shell and revert the fail-safe parameters to the original values from step 1, if changed. Then exit the fail-safe mode and reboot the firewall:

```
<#root>
```

```
firepower-1010:/$
```

```
exit
```

```
>
```

```
exit
```

```
firepower-1010#
```

```
connect local-mgmt
```

```
firepower-1010(local-mgmt)#
```

```
config failsafe-max-restart
```

```
0 shall Disable Failsafe Mode!!!
```

```
Set a max_restart (0-8) value Or [x] to exit:
```

```
7
```

```
System may come up in Normal state post Reboot.  
Configuration Successful
```

```
firepower-1010-failed(local-mgmt)#
```

```
show failsafe-params
```

```
Max Restart: 7
```

```
Current Reboot Count: 1
```

```
Restart Time Interval(secs): 3600
```

```
firepower-1010-failed(local-mgmt)#
```

```
failsafe-exit
```

```
System may reboot? (y/n)
```

```
y
```

Reset Successful

```
firepower-1010-failed(local-mgmt)#
```

```
exit
```

```
firepower-1010-failed#
```

```
scope chassis
```

```
KSEC-FPR1010-2 /chassis* #
```

```
reboot no-prompt
```

```
Broadcast message from root@KSEC-FPR1010-2 (Thu Jun 24 15:59:22 2026):  
All shells being terminated due to system /sbin/reboot
```

11. Monitor the session logs. The expected behavior is that after reboot, the firewall no longer continuously reboots.

12. If the firewall no longer continuously reboots, wait until the firewall is online, then ensure to delete the same AnyConnect/Secure Client images from step 8 from FMC/FDM UI, and deploy policies. Otherwise, the images are reapplied during the next policy deployment.

13. Ensure to upgrade software to the version with the fix of Cisco bug ID [CSCwc82675](#).

14. After software upgrade to the version with the fix of Cisco bug ID [CSCwc82675](#), add the AnyConnect/Secure Client images deleted at step 12 and deploy policies.

Cause

Multiple AnyConnect/Secure Client images result in elevated memory usage on Firepower 1010 due to the limited amount of memory available for the data plane (Lina engine). Due to limited amount of memory, the system can exhaust Lina engine memory, which usually results in Lina restarting and entering a continuous reboot loop. In some cases, different Lina processes can also trigger a traceback and generate core files.

This issue is tracked in Cisco bug ID [CSCwc82675](#). Additionally, the Remote Access VPN chapter in the Firewall Management Center Device Configuration Guide mentions “Using multiple Secure Client packages on threat defense devices can increase memory usage and affect the performance of the device. We recommend that you do not use multiple Secure Client packages on low-end threat defense devices to avoid

continuous reboots because of memory exhaustion. “

For more information refer to Cisco bug ID [CSCwj59682](#) and Cisco bug ID [CSCwm72469](#).

Related Content

- Cisco bug ID [CSCwm47108](#)
- Cisco bug ID [CSCwc82675](#)
- Cisco bug ID [CSCwm72469](#)
- Cisco bug ID [CSCwj59682](#)
- Cisco bug ID [CSCwj91341](#)
- [Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense](#)
- [Chapter: Remote Access VPN](#)