

由于DTLS流量卸载问题，安全防火墙意外重新启动

目录

问题

思科安全防火墙威胁防御(FTD)会经历系统重新启动，反复导致服务中断，并且不会生成传统的crashinfo文件。在故障排除期间，会观察到重复生成crypto_eng0_arch_*文件以及重复出现的NPU加速器和FPGA致命错误消息，这些错误消息与重新启动事件同时出现。

- FTD目录确认重复生成crypto_eng0_arch_*文件，其时间戳与重新引导事件一致。

```
firepower# dir crypto_archive
-rwxr-xr-x 1 root root 55310816 Mar 12 01:22 crypto_eng0_arch_1.bin
-rwxr-xr-x 1 root root      869 Mar 12 01:22 crypto_eng0_arch_1.info
-rwxr-xr-x 1 root root  409235 Mar 12 01:22 crypto_eng0_arch_1.reg
-rwxr-xr-x 1 root root 55310816 Mar 12 04:25 crypto_eng0_arch_2.bin
-rwxr-xr-x 1 root root      869 Mar 12 04:25 crypto_eng0_arch_2.info
-rwxr-xr-x 1 root root  409111 Mar 12 04:25 crypto_eng0_arch_2.reg
-rwxr-xr-x 1 root root 55310816 Mar 12 09:45 crypto_eng0_arch_3.bin
-rwxr-xr-x 1 root root      869 Mar 12 09:45 crypto_eng0_arch_3.info
-rwxr-xr-x 1 root root  408688 Mar 12 09:44 crypto_eng0_arch_3.reg
-rwxr-xr-x 1 root root 55310816 Mar 11 18:48 crypto_eng0_arch_4.bin
-rwxr-xr-x 1 root root      869 Mar 11 18:48 crypto_eng0_arch_4.info
-rwxr-xr-x 1 root root  408895 Mar 11 18:48 crypto_eng0_arch_4.reg
-rwxr-xr-x 1 root root 55310816 Mar 11 21:11 crypto_eng0_arch_5.bin
-rwxr-xr-x 1 root root      869 Mar 11 21:11 crypto_eng0_arch_5.info
-rwxr-xr-x 1 root root  409136 Mar 11 21:11 crypto_eng0_arch_5.reg
```

- FTD日志显示重复出现的NPU加速器和FPGA致命错误消息，这些错误消息与意外重新启动和crypto_eng0_arch_*文件的计时匹配。

```
> expert
admin@device:~$ sudo su
Password: [enter admin password]
root@device:/Volume/home/admin# cat /opt/cisco/platform/logs/messages | grep -i npu
2026 Mar 11 07:11:42 KC FPGA: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
2026 Mar 11 07:11:42 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED
2026 Mar 11 07:11:42 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the device !!
```

```
2026 Mar 11 11:15:47 KC FPGA: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
2026 Mar 11 11:15:47 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED
2026 Mar 11 11:15:47 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the device !!
---
Mar 11 21:11:20 device kings-cross-fpga: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
Mar 11 21:11:20 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED
Mar 11 21:11:20 device FPRM: <<%FPRM-2-NPU_FPGA_FAILURE>> [F1418][critical][npu-fpga-failure][sha
Mar 11 21:11:20 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED - REBOOTING the de
Mar 12 01:22:53 device kings-cross-fpga: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
Mar 12 01:22:54 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED
Mar 12 01:22:54 device FPRM: <<%FPRM-2-NPU_FPGA_FAILURE>> [F1418][critical][npu-fpga-failure][sha
Mar 12 01:22:54 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED - REBOOTING the de
```

- FTD配置确认受影响的FTD上启用了DTLS流分流，这符合已知缺陷Cisco Bug ID CSCwq32085的条件。

```
firepower# show flow-offload-dtls info
DTLS offload: Enabled
Egress optimization: Enabled
```

环境

- 主要出现在Firepower 3100系列上，但会影响其他型号
- 影响未针对此问题使用固定版本的ASA和FTD。
- 由Firepower管理中心(FMC)管理
- 在受影响的设备上启用DTLS流分流

分辨率

将所有受影响的FTD/ASA设备升级到包含缺陷Cisco Bug ID [CSCwq32085](#)的修复程序的版本。

解决方法

- 1.转到Cisco安全防火墙管理中心中的Devices > FlexConfig。
- 2.创建或编辑FlexConfig对象。
- 3.插入命令行文本以通过FlexConfig禁用FTD设备的DTLS/IPSEC流量卸载。

```
no flow-offload-ipsec
no flow-offload-dtls
```

- 4.将FlexConfig Policy分配给目标FTD设备并部署配置。
- 5.更改需要重新启动FTD才能生效。

原因

意外重新启动是由FTD中的Cisco Bug ID CSCwq32085引起的。在Firepower 3100和4200系列设备上启用DTLS流量分流时，此已知软件缺陷可能会触发NPU/FPGA加速器故障和强制重启。该缺陷特别影响硬件加速功能，并在强制系统重新启动之前生成带有“检测到KC ILK问题”控制台错误消息的crypto_archive文件。

相关内容

- [了解安全Firepower 3100和4200中的IPsec和DTLS卸载并对其进行故障排除](#)
- [配置FlexConfig对象](#)
- [思科漏洞ID CSCwq32085](#)
- [思科安全防火墙威胁防御版本说明，版本7.6.x](#)
- [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）。