

Beveiligde firewall start onverwacht opnieuw op vanwege probleem met DTLS-flow-offload

Inhoud

uitgifte

Cisco Secure Firewall Threat Defense (FTD) herstart het systeem, waardoor de service herhaaldelijk wordt onderbroken en zonder traditionele crashinfo-bestanden te genereren. Tijdens het oplossen van problemen wordt een herhaalde generatie `crypto_eng0_arch_*`-bestanden waargenomen, samen met terugkerende NPU-accelerator en FPGA fatale foutmeldingen die samenvallen met de reboot-gebeurtenissen.

- FTD directory bevestigt herhaalde generatie van `crypto_eng0_arch_*` bestanden met tijdstempels die samenvallen met reboot gebeurtenissen.

```
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-logs tonen terugkerende NPU-accelerator en FPGA fatale foutmeldingen die overeenkomen met de timing van onverwachte herstart en `crypto_eng0_arch_*` bestanden.

```
> 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-configuratie bevestigt dat DTLS-flow offload is ingeschakeld op de betreffende FTD, wat overeenkomt met de voorwaarden voor bekende Cisco bug ID CSCwq32085.

```

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

```

milieu

- Voornamelijk te zien op de Firepower 3100-serie, maar heeft invloed op andere modellen
- Heeft invloed op ASA's en FTD's die niet op een vaste versie voor het probleem staan.
- Beheerd door Firepower Management Center (FMC)
- DTLS-flow offload ingeschakeld op getroffen apparaten

resolutie

Upgrade alle betrokken FTD/ASA-apparaten naar een versie met de oplossing voor het defect Cisco bug ID [CSCwq32085](#).

Tijdelijke oplossing

1. Ga naar Apparaten > FlexConfig in het Cisco Secure Firewall Management Center.
2. Een FlexConfig-object maken of bewerken.
3. Plaats de opdrachtregeltekst om DTLS/IPSEC Flow Offload voor het FTD-apparaat via FlexConfig uit te schakelen.

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

4. Wijs het FlexConfig-beleid toe aan het beoogde FTD-apparaat en implementeer de configuratie.
5. De wijziging vereist een FTD-reboot voor de wijzigingen die van invloed zijn.

Oorzaak

De onverwachte reboots werden veroorzaakt door Cisco bug ID CSCwq32085 in FTD. Dit bekende softwaredefect kan leiden tot NPU/FPGA-acceleratorstoringen en gedwongen herstart wanneer DTLS-flow offload is ingeschakeld op apparaten uit de Firepower 3100- en 4200-reeks. Het defect is specifiek van invloed op de hardwareversnellingsfuncties en genereert crypto_archive-bestanden met een "KCILK-probleem gedetecteerd" consolefoutberichten voordat het systeem opnieuw wordt opgestart.

Gerelateerde inhoud

- [IPsec en DTLS Offloading begrijpen en oplossen in Secure Firepower 3100 en 4200](#)
- [FlexConfig-objecten configureren](#)
- [Cisco bug ID CSCwq32085](#)
- [Cisco Secure Firewall Threat Defense Release Notes, versie 7.6.x](#)

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.