了解安全Firepower 3100和4200中的IPsec和DTLS卸载并对其进行故障排除

目录

简介

本文档介绍对负责处理流量分流的Firepower架构中的常见问题进行故障排除。

先决条件

IPSec配置要么基于路由，要么基于策略，要么二者兼有。

要求

Cisco 建议您了解以下主题：

- 站点到站点 VPN
- 远程访问 VPN

使用的组件

本文档中的信息基于：

- 思科安全防火墙威胁防御7.2.0+
- 思科安全防火墙3K/4K

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

功能信息

支持设备型号使用IPsec流量卸载，其中，在IPsec站点到站点VPN或远程访问VPN安全关联(SA)的初始协商之后，IPsec连接被卸载到设备中的现场可编程门阵列(FPGA)，从而提高设备性能。

卸载操作具体涉及入口的预解密和解密处理，以及出口的预加密和加密处理。系统软件处理内部流以应用安全策略。

支持的平台

默认情况下，IPsec流量分流已启用，并且到目前为止适用于以下设备类型：

- 安全防火墙3100
- 安全防火墙4200

当VTI源自环回接口时，也使用IPsec流量分流。

IPsec卸载在支持的平台上可用，从以下开始：

- 安全防火墙FTD 7.2
- 安全防火墙ASA 9.18

虽然DTLS卸载在支持的平台上可用，但从：

- 安全防火墙FTD 7.6
- 安全防火墙ASA 9.22

限制

IPSec卸载

以下是IPsec卸载的限制：

- IKEv1
- 传输模式
- 压缩
- 分片后
- 窗口大小不是64位的反重播
- 用于隧道流量的防火墙过滤器
- 多情景

DTLS卸载

以下是DTLS卸载的限制：

- DTLS 1.0

- 压缩
- 多情景
- 多实例
- 集群

配置

默认情况下，在支持IPSEC和DTLS的平台上启用流量分流。可以使用CLI/flex-config启用或禁用它。

<#root>

```
FPR(config)#flow-offload-ipsec
FPR(config)#no flow-offload-ipsec
```

<<<<<<< disable flow-offload for ipsec

```
FPR(config)#flow-offload-ipsec egress-optimization
FPR(config)#no flow-offload-ipsec egress-optimization
```

<<<<<<< disable egress optimization for ipsec

```
FPR(config)#flow-offload-dtls
FPR(config)#no flow-offload-dtls
```

<<<<<<< disable flow-offload for DTLS

```
FPR(config)#flow-offload-dtls egress-optimization
FPR(config)#no flow-offload-dtls egress-optimization
```

<<<<<<< disable egress optimization for DTLS

故障排除

在继续操作之前，请了解卸载在协商完成并且您已建立SA之前不会启动。DTLS的情况也基本相同，因此初始握手或协商期间的问题可能与卸载无关，并且可能具有传统的故障排除方法（包括调试和必要的捕获）。与流量分流相关的具体问题可能会以流量中断的形式出现。

下面是一些可以执行的重要命令，这些命令用于提示您是否启用了流量分流，以及由于流量分流导致的数据包处理出现问题。

- 验证show crypto ipsec sa命令以检查是否启用了卸载。

<#root>

firepower# show crypto ipsec sa peer 203.0.113.2

```
peer address: 203.0.113.2
    Crypto map tag: CSM_dmz_a_001_map, seq num: 1, local addr: 203.0.113.1

      access-list CSM_IPSEC_ACL_1 extended permit ip 192.0.2.0 255.255.255.252 192.0.2.4 255.255.255.25
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (192.0.2.0/255.255.255.252/0/0)
      remote ident (addr/mask/prot/port): (192.0.2.4/255.255.252.252/0/0)
      current_peer: 203.0.113.2


      #pkts encaps: 443, #pkts encrypt: 443, #pkts digest: 443
      #pkts decaps: 10254, #pkts decrypt: 10254, #pkts verify: 10254
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 443, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 886, #recv errors: 0

      local crypto endpt.: 203.0.113.1/500, remote crypto endpt.: 203.0.113.2/500
      path mtu 1500, ipsec overhead 86(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: XXXXXXXX
      current inbound spi : YYYYYYYY

    inbound esp sas:
      spi: 0xYYYYYYYY (YYYYYYYY)
        SA State: active
        transform: esp-aes-256 esp-sha-384-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 14, IKEv2,

CAN_BE_OFFLOADED, OFFLOADED, } <<<<<<<


        slot: 0, conn_id: 80438, crypto-map: CSM_cisco_map
        sa timing: remaining key lifetime (kB/sec): (32808888/26585)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xXXXXXXXX (XXXXXXXX)
        SA State: active
        transform: esp-aes-256 esp-sha-384-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 14, IKEv2,

CAN_BE_OFFLOADED, OFFLOADED, } <<<<<<<


        slot: 0, conn_id: 80438, crypto-map: CSM_cisco_map
        sa timing: remaining key lifetime (kB/sec): (34652026/26584)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

- show ipsec stats命令也可用于卸载确认。

<#root>

firepower# show ipsec stats

```
    IPsec Global Statistics
    -----------------------
    Active tunnels: 1
    Previous tunnels: 54
    Inbound
        Bytes: 3396848
        Decompressed bytes: 0
        Packets: 30329
        Dropped packets: 0
        Replay failures: 0
        Authentications: 30329
        Authentication failures: 0
        Decryptions: 30329
        Decryption failures: 0
        TFC Packets: 0
        Decapsulated fragments needing reassembly: 0
        Valid ICMP Errors rcvd: 0
        Invalid ICMP Errors rcvd: 0
     Outbound
        Bytes: 3431248
        Uncompressed bytes: 1837548
        Packets: 30585
        Dropped packets: 0
        Authentications: 30584
        Authentication failures: 0
        Encryptions: 30584
        Encryption failures: 0
        TFC Packets: 0
        Fragmentation successes: 0
            Pre-fragmentation successes: 0
            Post-fragmentation successes: 0
        Fragmentation failures: 0
            Pre-fragmentation failures: 0
            Post-fragmentation failures: 0
        Fragments created: 0
        PMTUs sent: 0
        PMTUs rcvd: 0
```

Offloaded Inbound, Pipe 0 <<<<<<<<<<<<<<<<

Bytes: 3336256

Packets: 29788

Authentications: 29788

Decryptions: 29788

Offloaded Outbound, Pipe 0 <<<<<<<<<<<<<<<<

```
      Bytes: 3358480

      Packets: 29918

      Authentications: 29918

      Encryptions: 29918

    Protocol failures: 0
    Missing SA failures: 0
    System capacity failures: 0
    Inbound SA delete requests: 89
    Outbound SA delete requests: 0
    Inbound SA destroy calls: 75
    Outbound SA destroy calls: 71
```

- 在同时引入DTLS卸载时，可以将FTD 7.6/ASA 9.22向前推进，您可以使用show flow-offload info detail检查DTLS和IPSEC卸载的状态。

<#root>

```
firepower# show flow-offload info detail



Current running state : Enabled


  Dynamic flow offload : Disabled
  flow table refresh count : 7866 [246]
  HW flow table refresh count : 246
  Invalid Precomputation Request: 2755106
  instance_id:2304 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:1 service_map: 0000000b
  instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:1 service_map: 0000000b
  ..........
  instance_id:256 interface_id:1011 action:0 logic_id_opt:0 subinterface_id_opt:1 service_map: 0000000b
  Services Registered:
  Flow_Offload: Registered

  IPSec Offload: Registered <<<<<<<<<<<


  DTLS Offload: Registered  <<<<<<<<<<<
```

- 在show flow-offload statistics输出中检查可能的丢弃/错误计数器。输出可能因问题而异。在某些情况下，6元组遗漏计数非常高。但最佳实践是在问题期间应多次收集这些输出，以便对适当的计数器进行比较分析。CAM统计信息计数器最简单的解释是每个计数器都有其特定的

用途，并且它们大多充当分类器，负责识别数据包并正确转发数据包。两组输出代表IPSEC和DTLS统计信息。

<#root>

These outputs can also be fetched separately for DTLS and IPSEC by

show flow-offload-ipsec statistics

and

show flow-offload-dtls statistics

.

firepower# show flow-offload info detail

```
  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 50736432
  Tx Packet count : 45999280
  Error Packet count : 0 <<<<<<<<<


  Drop Packet count : 0 <<<<<<<<<



  NOTE: The CAM counters displayed are cumulative counters
  for all offload applications and indicates the total packets offloaded

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 9675832699
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 74
  6-Tuple CAM Hit Count : 177440969
  6-Tuple CAM Miss Count : 9498391657

  NOTE: The counters displayed are cumulative counters
  for all offload applications and indicates the total packets offloaded

  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 48444809
  Tx Packet count : 44575287
  Error Packet count : 0 <<<<<<<<<


  Drop Packet count : 41 <<<<<<<<<



  NOTE: The CAM counters displayed are cumulative counters
```

```
  for all offload applications and indicates the total packets offloaded

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 9675832699
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 74
  6-Tuple CAM Hit Count : 177440969
  6-Tuple CAM Miss Count : 9498391657

  NOTE: The counters displayed are cumulative counters
  for all offload applications and indicates the total packets offloaded
```

- show counters命令也可用于卸载计数器，并建议进行多次收集，以便进行比较分析。

<#root>

For IPSEC offload

```
firepower# show counters
    IPSEC   OFFLOAD_IB_PKT_PROCESS                46201663    Summary
    IPSEC   OFFLOAD_IB_PKT_PROCESS_SUCCESS        46201663    Summary
    IPSEC   OFFLOAD_OB_PKT_PROCESS                44580990    Summary
    IPSEC   OFFLOAD_OB_PKT_PROCESS_SUCCESS        44580990    Summary
    IPSEC   OFFLOAD_EGRESS_OPTIMIZE_PKT           44580990    Summary
    IPSEC   OFFLOAD_FLOW_INBOUND_ADD_RULE         296         Summary
    IPSEC   OFFLOAD_FLOW_OUTBOUND_ADD_RULE        296         Summary
    IPSEC   OFFLOAD_FLOW_INBOUND_DEL_RULE         286         Summary
    IPSEC   OFFLOAD_FLOW_OUTBOUND_DEL_RULE        286         Summary
    IPSEC   OFFLOAD_FLOW_INBOUND_UPDATE_SUCCESS   253         Summary
```

For DTLS offload

```
firepower# show counters
    CRYPTO   DTLS_OFFLOAD_IB_PKT_PROCESS          11122701    Summary
    CRYPTO   DTLS_OFFLOAD_IB_PKT_SUCCESS          11122701    Summary
    CRYPTO   DTLS_OFFLOAD_OB_PKT_PROCESS          27269819    Summary
    CRYPTO   DTLS_OFFLOAD_OB_PKT_SUCCESS          27269819    Summary
    CRYPTO   DTLS_OFFLOAD_FLOW_IB_ADD_RULE        4189        Summary
    CRYPTO   DTLS_OFFLOAD_FLOW_OB_ADD_RULE        4189        Summary
    CRYPTO   DTLS_OFFLOAD_FLOW_IB_UPDATE_SUCCESS  3730        Summary
    CRYPTO   DTLS_OFFLOAD_RX_ALERT                621         Summary
    CRYPTO   DTLS_OFFLOAD_CONTROL_IN_PKT          226951      Summary
    CRYPTO   DTLS_OFFLOAD_EGRESS_OPTIMIZE_PKT     27269819    Summary
```

- 可以收集IPSEC或DTLS卸载捕获，以确保在LINA捕获中看不到任何内容时接收加密数据包。LINA捕获只在FPGA正确处理传入数据包并将其注入数据路径时打印输出。如果FPGA未正确

处理数据包，则在LINA捕获中可能看不到任何内容，但这并不意味着您根本没有收到任何数据包。可以使用任何工具将转储还原为可读格式。

<#root>

```
firepower# capture TAC ipsec-offload match spi 0x7XXXXXX9 203.0.113.1 203.0.113.2
```

<<< for IPSEC

```
firepower# capture TAC-DTLS dtls-offload match udp 203.0.113.1 eq <src port> 203.0.113.2 eq <dst port>
```

<<< for DTLS

```
firepower# show capture TAC
```

<<<< this is extracted for ipsec-offload

```
2 packets captured

   1: 13:54:40.883758       20db.ea88.ce95 c860.8f37.f614 0xc008 Length: 202

                         xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
                         xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
                         83a8 7c14 3c64 594f 951d ca36 0e4d ca7e
                         2d34 d4ea 3515 0202 ce36 ace9 59a5 6f69
                         04c6 8ff9 ddf7 9e82 f6c2 11c5
  2: 13:54:42.877014       20db.ea88.ce95 c860.8f37.f614 0xc008 Length: 202

                         xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
                         xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
                         3e83 a9b4 63b1 41cb 2408 0de1 4819 288b
                         9df8 fade 611e a338 98e5 74ec 552f c37d
                         8aa0 42d9 0b68 e5e7 7876 8bab
2 packets shown
```

- 您还可以选择检查交换机级别的捕获，以确保正确接收和转发流量到FPGA。这些捕获是从实验室环境中获取的，请确保应用适当的过滤器，以将对生产环境的影响降至最低。有关详细信息，请参阅安全防火墙捕获。

```
firepower# capture TAC switch interface <interface name> match ip 203.0.113.1 203.0.113.2
OR
firepower# capture TAC switch real-time
6 packets captured using switch real-time capture

    1: 09:10:29.298126 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150

               xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
               xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
               c685 5d8e c938 1617 c72e 7028 af65 aeba
               04b8 d2d5 db53 783f afed a8ee 9dcd 5938
               f198 e89f 5555 5555
    2: 09:10:39.298751 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150
```

```
            xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
            xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
            a340 8252 d626 6cd8 f16a c6f7 3460 0e5a
            290a 5ca7 8f9b 864c ef76 cdad 1839 8020
            2590 804b 5555 5555
    3: 09:10:49.298766 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150

            xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
            xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
            7ebc d4f3 c706 55ac 1358 ab7c 6363 9827
            ec29 47fe 4f91 4967 73a3 b646 7499 9269
            0816 f463 5555 5555

    4: 09:10:59.303405 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150

           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           d15c 1115 3042 72b4 3b81 88ea 7548 c7e4
           3401 b7ba 5555 5555
    5: 09:11:09.308165 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150

           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           752b 0ed4 1f2d 3429 0a09 bda5 2c68 1acd
           64e9 7e5e 5555 5555
    6: 09:11:19.313139 bc5a.56ac.6702 e4a4.0400.11bc 0x2057 Length: 150

           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
           0631 4b9d 0a08 52b5 d084 cb39 d55a ad91
           777c cfe4 5555 5555
    6 packets shown
```

- 对于DTLS特定输出以及前面的show输出，可以针对会话特定数据验证这一点。为了进行分析，也可以多次获取这些信息，尤其是已标记的计数器，用于确认是否正确处理和转发数据包。

<#root>

firepower# show asp table socket offloaded

```
Protocol    Socket    State      Local Address               Foreign Address               IB-Pipe#
SVC_UDP     104d40e8  CONNECTED
  203.0.113.5:443              198.51.100.5:3875             0            0
SVC_UDP     0f435518  CONNECTED  203.0.113.5:443             198.51.100.6:13265            0
```

firepower# show asp table socket 104d40e8 detail

```
Statistics for socket
0x104d40e8
:
```

```
3) AM Module
   Mod handle: 0x00000000104d40eb
   Rx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      1
   Tx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        App Flow-Ctrl Tx: 0
        Stack:         0x000014a89473bb80
        New Conn Cb:   0x00005559542f6130
        Notify   Cb:   0x00005559542f62a0
        App Hdl:       0x000000000549358a
        Shared  Lock:  0x000014a7e010d848
          Group Lock:  0x000014a7e010d848
          Async Lock:  0x000014a84a270b40
        Closed Mod Rx: -1, Tx: 4
        Push Module:   INVALID
        State:         CONNECTED
        Flags: 0x500003
          Inbound
          Accepted
          New Conn App Notify Success
          Stack Ref count

2) SVC_UDP Module
   Mod handle: 0x000014a8921aa180
   Rx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:      1
   Tx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:    785
        Idle (ms):              0
        DF-Bit Ignore:          Disable
        MTU:                    1150
        Fragmented Packets:     0
        Downstream:
           Data Pkts/Bytes:     768/481092


Drop Pkts/Bytes:     0/0


           Ctrl Pkts/Bytes:     15/10347
        Upstream:
           Data Pkts/Bytes:     1093/536093


Drop Pkts/Bytes:     0/0


           Ctrl Pkts/Bytes:     21/102
        Offload Stats:


#pkts in: 1093, #bytes in: 536093, #pkts decrypt: 1093 <<<<<<< this is expected to match with vpn-sessio


           #pkts out: 767, #bytes out: 480393, #pkts encrypt: 767


<<<<<<< this is expected to match with vpn-sessiondb det output counters


           #send errors: 0, #recv errors: 0
           #pkts failed (send): 0, #pkts failed (rcv): 0
           #pkts replay failed (rcv): 0
```

```
1) DTLS Module
   Mod handle: 0x000014a89030f300
   Rx:  0/128 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/128 ( 0 queued), Flow-Ctrl:      0,  Tot:    786
        Upstream Active/peak/total:     0/0/0
        Downstream Active/peak/total:   0/1/785
        Inbound bytes rx/tx:    303/0
        Inbound packets rx/tx:  2/0
        Inbound packets lost:   0
        Outbound bytes rx/tx:   427737/444392
        Outbound packets rx/tx: 785/786
        Outbound packets lost:  0
        Upstream Close Attempt:         0
        Upstream Close Forced:          0
        Upstream Close Next:            0
        Upstream Close Handshake:       0
        Downstream Close Attempt:       0
        Downstream Close Forced:        0
        Downstream Close Next:          0
        Inbound discard empty buf:      0
        Empty downstream buf:   0
        Encrypt call:           0
        Encrypt call error:     0
        Encrypt handoff:        0
        Encrypt CB success:     0
        Encrypt CB fail:        0
        Flowed Off:             0
        Stats Last State:       0x20 (TRFIN)
        Pending crypto cmds:    0
        Socket Last State:      0x1 (SSLOK )
        Socket Read State:      0xf0 (read header)
        Handle Read State:      0xf0 (read header)
        References:             2
        In Rekey:               0x0
        Flags:                  0x2000000
        Header Len:             13
        Record Type:            0x0
        Record Len:             0
        Queued Blocks:          0
        Queued Bytes:           0

0) TM Module
   Mod handle: 0x00000000104d40e8
   Rx:  0/1  (

0 queued

), Flow-Ctrl:      0,  Tot:      2
   Tx:  0/1  (

0 queued

), Flow-Ctrl:      0,  Tot:    786
        Transp Flow-Ctrl Rx: 0
        UDP handle: 0x000014a890217500
        Conn Timeout: 1800000 ms
        Local host: 203.0.113.5, Local port: 443
        Foreign host:198.51.100.5, Foreign port: 3875
          Rcvd:                 2
            with data:          2
            total data bytes:   303
          Sent:                 786
            with data:          786
```

```
            total data bytes:   444392
          Dropped:

            Rcv queue full:     0 <<<<<<<<<
```

- 根据要求，可以执行的附加CLI很少。

<#root>

Global stats

- show flow-offload-dtls statistics
- show crypto protocol ssl statistics

(aggregate of offloaded/ non-offloaded stats)

- show ssl mib

(aggregate of offloaded/ non-offloaded stats)

- show crypto accelerator statistics

(separate Offloaded statistics added)

Clearing stats

- clear flow-offload-dtls statistics

- 此外，对于DTLS和IPSEC卸载，还可以在问题期间从fxos CLI多次收集show npu-accel statistics，以验证几个重要计数器。此输出因问题类型和环境而异。

<#root>

>show npu-accel statistics

```
Output is cropped and gathered from one of the affected devices.

ilk_tx_good_pkt_cnt = 133997299
ilk_rx_good_pkt_cnt = 129123883
ilk_tx_err_pkt_cnt = 0 <<<<<<<<<<
```

ilk_tx_taildrop_pkt_cnt = 4867559   <<<<<<<<<<

ilk_tx_fifo_sbit_err_cnt = 0 <<<<<<<<<<

ilk_tx_fifo_dbit_err_cnt = 0 <<<<<<<<<<

ilk_rx_fifo_sbit_err_cnt = 0 <<<<<<<<<<

ilk_rx_fifo_dbit_err_cnt = 0 <<<<<<<<<<

ilk_rx_err_pkt_cnt = 0 <<<<<<<<<<

ilk_rx_seg_sop_cnt = 129123883
ilk_rx_seg_eop_cnt = 129123883

module: nvppu, pipe: 0
----
nvppu_ipsec_in_pkt_count = 46201704
nvppu_ipsec_in_byte_count = 5970198256
nvppu_ipsec_in_decrypt_pkt_count = 46201704
nvppu_ipsec_in_decrypt_byte_count = 4122130096
nvppu_ipsec_in_hash_pkt_count = 46201704
nvppu_ipsec_in_hash_byte_count = 5230970992
nvppu_ipsec_out_pkt_count = 44575287
nvppu_ipsec_out_byte_count = 31277069992
nvppu_ipsec_out_encrypt_pkt_count = 44575287
nvppu_ipsec_out_encrypt_byte_count = 29494058512
nvppu_ipsec_out_hash_pkt_count = 44575287
nvppu_ipsec_out_hash_byte_count = 30563865400

nvppu_ipsec_drop_pkt_count = 0 <<<<<<<<<<

nvppu_dtls_in_pkt_count = 11122815
nvppu_dtls_in_byte_count = 2810772142
nvppu_dtls_out_pkt_count = 27223995
nvppu_dtls_out_byte_count = 17111805764

nvppu_dtls_in_drop_pkt_count = 82   <<<<<<<<<<

nvppu_dtls_out_drop_pkt_count = 0 <<<<<<<<<<

nvppu_filtering_total_cnt = 46201704

nvppu_tfc_drop_cnt = 0 <<<<<<<<<<

nvppu_filtering_drop_cnt = 41   <<<<<<<<<<

nvppu_anti_drop_cnt = 0 <<<<<<<<<<

```
nvppu_dtls_anti_drop_cnt = 114 <<<<<<<<<<
```

- 通常，建议同时从两台设备收集FXOS和FTD的故障排除文件以及FTD CLI中的show tech support，以备它们在HA中运行以进行分析时和之前的输出时使用。

结论

本文档旨在深入解释如何收集卸载特定输出，因为由于基于FPGA的较新平台中所完成的架构更改，这对有限的可视性而言具有挑战性。

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）。