瞭解安全Firepower 3100和4200中的IPsec和DTLS解除安裝並對其進行故障排除

目錄

簡介

本文檔介紹對負責處理流量分流的Firepower架構中的常見問題進行故障排除。

必要條件

IPSec配置基於路由或基於策略，或者兩者兼有。

需求

思科建議您瞭解以下主題：

- 站點到站點VPN
- 遠端存取VPN

採用元件

本檔案中的資訊是根據：

- 思科安全防火牆威脅防禦7.2.0+
- 思科安全防火牆3K/4K

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

功能資訊

支援裝置模型使用IPsec流量分流，其中，在IPsec站點到站點VPN或遠端訪問VPN安全關聯(SA)的初始協商之後，將IPsec連線分流到裝置中的現場可程式設計門陣列(FPGA)，從而提高裝置效能。

解除安裝操作與入口的預解密和解密處理以及出口的預加密和加密處理特別相關。系統軟體處理內部流以應用您的安全策略。

支援的平台

預設情況下，IPsec流量分流已啟用，到目前為止適用於以下裝置型別：

- 安全防火牆3100
- 安全防火牆4200

當VTI源自回送介面時，也會使用IPsec流量分流。

IPsec解除安裝在受支援的平台上可用，開始如下：

- 安全防火牆FTD 7.2
- 安全防火牆ASA 9.18

DTLS解除安裝在支援的平台上可用時，從以下開始：

- 安全防火牆FTD 7.6
- 安全防火牆ASA 9.22

限制

IPSec解除安裝

以下是IPsec解除安裝的限制：

- IKEv1
- 傳輸模式
- 壓縮
- 分段後
- 使用除64位以外的視窗大小的反重放
- 適用於通道化流量的防火牆過濾器
- 多情景

DTLS解除安裝

以下是DTLS解除安裝的限制：

- DTLS 1.0

- 壓縮
- 多情景
- 多例項
- 叢集

組態

預設情況下，在支援的IPSEC和DTLS平台上啟用流量分流。可使用CLI/flex-config啟用或禁用它。

<#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

疑難排解

在繼續操作之前，請瞭解解除安裝在協商完成並且已建立SA之前不會啟動。DTLS的情況也基本相同，因此初始握手或協商期間的問題可能與解除安裝無關，並且可以採用傳統的故障排除方法，包括調試和必要的捕獲。與流量分流相關的具體問題可能會以流量中斷的形式出現。

以下是幾個重要命令，在執行這些命令時，如果您已啟用流量分流，而且由於流量分流，資料包處理出現問題，則需進行確認。

- 驗證show crypto ipsec sa命令以檢查是否已啟用解除安裝。

<#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
```

- 也可以引用show ipsec stats命令來確認解除安裝。

<#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
```

- FTD 7.6 / ASA 9.22在引入DTLS解除安裝時，您可以使用show flow-offload info detail檢查DTLS和IPSEC解除安裝的狀態。

<#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輸出中檢查可能的丟棄/錯誤計數器。輸出可能因問題而異。在某些情況下，6元組的遺漏計數是非常高的。但最佳做法是在出現問題的過程中應多次收集這些輸出，以便對適當的計數器進行比較分析。CAM統計資訊計數器的最簡單解釋是每個計數

器都有其特定的用途，並且它們大多充當分類器，負責識別資料包並正確轉發資料包。兩組輸出代表IPSEC和DTLS統計資訊。

<#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命令也可以用於解除安裝計數器，並建議進行多次收集以進行比較分析。

<#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解除安裝捕獲，以確保在LINA捕獲中看不到任何內容時您正在接收加密資料包。LINA捕獲僅在FPGA正確處理傳入資料包並將其注入資料路徑時才列印輸出。如果

FPGA未正確處理資料包，則在LINA捕獲中可能看不到任何內容，但這並不意味著您根本沒有收到任何資料包。可以使用任何工具將轉儲還原為可讀格式。

<#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
```

- 您還可以選擇檢查交換機級別的捕獲，以確保正確接收和轉發到FPGA的流量。這些捕獲是從實驗室環境捕獲的，請確保應用適當的過濾器以最大程度地減少對生產環境的影響。詳細資訊可在安全防火牆捕獲中參考。

```
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
```

- 對於DTLS特定輸出以及前面的show輸出，可以針對會話特定資料驗證這一點。為了進行分析，也可以多次讀取這些資料包，尤其是標籤了用於確認資料包是否被正確處理和轉發的計數器。

<#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 <<<<<<<<<
```

- 可以根據要求執行一些額外的CLI。

<#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
```

- 除此之外，對於DTLS和IPSEC解除安裝，還可以在問題期間多次從fxos CLI收集show npu-accel統計資訊，以驗證幾個重要的計數器。此輸出因問題型別和環境而異。

<#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，建議同時從兩台裝置收集FXOS和FTD的疑難排解檔案以及FTD CLI的show tech support，以備它們在HA中執行分析時和之前的輸出使用。

結論

本文檔旨在深入解釋如何收集解除安裝特定輸出，因為由於基於FPGA的較新平台中進行的架構更改，這在可視性有限方面極具挑戰性。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。