Secure Firepower 3100および4200のIPSecおよびDTLSオフロードの説明とトラブルシューティング

内容

はじめに

このドキュメントでは、フローオフロードを処理するFirepowerアーキテクチャの一般的な問題のトラブルシューティングについて説明します。

前提条件

IPSec設定は、ルートベースかポリシーベース、またはその両方です。

要件

次の項目に関する知識があることが推奨されます。

- サイト間VPN
- リモート アクセス VPN

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Firewall Threat Defense 7.2.0+
- Cisco Secure Firewall 3000/4000

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能情報

サポートするデバイスモデルでは、IPSecサイト間VPNまたはリモートアクセスVPNセキュリティアソシエーション(SA)の最初のネゴシエーションの後に、IPSec接続がデバイスのField-Programmable Gate Array(FPGA)にオフロードされるIPSecフローオフロードが使用されます。これにより、デバイスのパフォーマンスが向上します。

オフロードされる操作は、入力での復号化前および復号化処理、および出力での暗号化前および暗号化処理に特に関連します。システムソフトウェアが内部フローを処理し、セキュリティポリシーを適用します。

対応プラットフォーム

IPSecフローオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

VTIがループバックインターフェイスから発信される場合にも、IPsecフローオフロードが使用されます。

IPSecオフロードは、次のプラットフォームでサポートされています。

- セキュアファイアウォールFTD 7.2
- セキュアファイアウォールASA 9.18

DTLSオフロードは、次のプラットフォーム以降のサポート対象プラットフォームで使用できます。

- セキュアファイアウォールFTD 7.6
- セキュアファイアウォールASA 9.22

制限

IPSecオフロード

IPSecオフロードには次の制限事項があります。

- IKEv1
- 転送モード（Transport Mode）

- 圧縮
- フラグメンテーション後
- 64ビット以外のウィンドウサイズでのアンチリプレイ
- トンネリングトラフィック用のファイアウォールフィルタ
- マルチコンテキスト

DTLSオフロード

DTLSオフロードには次の制限事項があります。

- DTLS 1.0
- 圧縮
- マルチコンテキスト
- マルチインスタンス
- クラスタ

コンフィギュレーション

IPSECとDTLSの両方でサポートされるプラットフォームでは、デフォルトでフローオフロードが有効になっています。Cli/flex-configを有効または無効にするために利用できます。

<#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

トラブルシューティング

先に進む前に、ネゴシエーションが完了してSAが確立されるまで、オフロードが開始されないことに注意してください。このケースはDTLSの場合もほとんど同じであるため、初期ハンドシェイクまたはネゴシエーション時の問題はオフロードとは無関係である可能性があり、デバッグおよび必要なキャプチャを含む従来のトラブルシューティング手法を使用できます。フローオフロードに関連する特定の問題が、トラフィックの中断という形で発生する可能性があります。

フローオフロードを有効にしており、問題がフローオフロードによるパケット処理にある場合に、確認を促すために実行できる重要なコマンドがいくつかあります。

- show crypto ipsec saコマンドを確認して、オフロードが有効になっているかどうかを確認します。

<#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
```

- オフロードを確認するには、show ipsec statsコマンドも使用できます。

<#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への移行では、DTLSオフロードも導入されている場合、show flow-offload info detailを使用してDTLSとIPSECの両方のオフロードのステータスを確認できます。

<#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 <<<<<<<<<<<

- show flow-offload statisticsの出力で廃棄またはエラーカウンタの可能性を確認します。出力は問題によって異なる場合があります。場合によっては、6タプルミス数が非常に高くなることがあります。ただし、ベストプラクティスは、適切なカウンタの比較分析を行うために、これらの出力が問題中に複数回収集されることです。CAM統計カウンタに関する最も単純な説明は、各カウンタが特定の目的を持ち、主にパケットを識別して正しく転送する分類子として機能することです。2つの出力セットは、IPSECおよびDTLSの統計情報を表します。

<#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
```

- また、比較分析のために、show countersコマンドをオフロードカウンタで参照し、複数回の収集を推奨できます。

<#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
```

- LINAキャプチャに何も表示されない場合に暗号化パケットを受信していることを確認するために、IPSECまたはDTLSオフロードキャプチャを収集できます。LINAキャプチャでは、FPGAが着信パケットを正しく処理してデータパスに挿入した場合にのみ、出力が出力されます。パケットがFPGAによって正しく処理されなかった場合、LINAキャプチャには何も表示されない可能性がありますが、これはパケットをまったく受信していないことを意味するものではありません。ダンプを読み取り可能な形式に復元するには、任意のツールを使用できます。

<#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
```

- また、スイッチレベルのキャプチャをチェックして、トラフィックが受信され、FPGAに正しく転送されていることを確認するオプションもあります。これらのキャプチャはラボ環境から取得したものです。実稼働環境への影響を最小限に抑えるために、適切なフィルタを必ず適用してください。詳細は、「セキュアなファイアウォールキャプチャ」で参照できます。

```
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
```

- DTLS固有の出力の場合、前述のshow出力とともに、セッション固有のデータについてこれを確認できます。また、分析のために複数回フェッチすることもできます。特に、パケットが正しく処理され、転送されているかどうかを確認するマーク付きカウンタが必要です。

<#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 <<<<<<<<<

- 要件に応じて実行できる追加のCLIがいくつかあります。

<#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

- また、DTLSとIPSECの両方のオフロードについて、問題の発生中にfxos CLIからshow npu-accel statisticsを複数回収集して、いくつかの重要なカウンタを確認できます。この出力は、問題のタイプや環境によって異なります。

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

- 通常は、分析のために前の出力とともにHAで実行されている場合に備えて、両方のデバイスからFTD CLIからのshow tech supportとともにFXOSとFTDのトラブルシューティングファイルを収集することをお勧めします。

結論

このドキュメントの目的は、オフロード固有の出力を収集する方法を詳細に説明することです。これは、新しいFPGAベースのプラットフォームではアーキテクチャの変更が行われるため、可視性の制限という点で困難であるためです。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。