보안 Firepower 3100 및 4200에서 IPsec 및 DTLS 오프로드 이해 및 문제 해결

목차

소개

이 문서에서는 플로우 오프로드 처리를 담당하는 Firepower 아키텍처의 일반적인 문제를 해결하는 방법을 설명합니다.

사전 요구 사항

IPSec 컨피그레이션은 경로 기반 또는 정책 기반 중 하나 또는 둘 다입니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 사이트 대 사이트 VPN
- 원격 액세스 VPN

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Cisco Secure Firewall Threat Defense 7.2.0+
- Cisco Secure Firewall 3K/4K

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 정보

지원 디바이스 모델은 IPsec 플로우 오프로드를 사용합니다. IPsec 사이트 대 사이트 VPN 또는 원격 액세스 VPN SA(보안 연결)의 초기 협상 이후에 IPsec 연결이 디바이스의 FPGA(Field-Programmable Gate Array)로 오프로드되므로 디바이스 성능이 향상됩니다.

오프로드된 작업은 특히 인그레스(ingress)의 사전 암호 해독 및 암호 해독 처리, 이그레스(egress)의 사전 암호화 및 암호화 처리와 관련이 있습니다. 시스템 소프트웨어는 보안 정책을 적용하기 위해 내부 흐름을 처리합니다.

지원되는 플랫폼

IPsec 흐름 오프로드는 기본적으로 활성화되어 있으며 지금까지 이러한 디바이스 유형에 적용됩니다.

- 보안 방화벽 3100
- 보안 방화벽 4200

VTI가 루프백 인터페이스에서 소싱되는 경우에도 IPsec 흐름 오프로드가 사용됩니다.

IPsec 오프로딩은 다음과 같이 지원되는 플랫폼에서 사용할 수 있습니다.

- Secure Firewall FTD 7.2
- Secure Firewall ASA 9.18

지원되는 플랫폼에서 DTLS 오프로드를 사용할 수 있는 경우

- Secure Firewall FTD 7.6
- 보안 방화벽 ASA 9.22

제한

IPSec 오프로딩

다음은 IPsec 오프로딩의 제한 사항입니다.

- IKEv1
- 전송 모드
- 압축
- 사후 조각화
- 윈도우 크기가 64비트가 아닌 재전송 방지
- 터널링 트래픽용 방화벽 필터
- 다중 컨텍스트

DTLS 오프로딩

다음은 DTLS 오프로드의 제한입니다.

- DTLS 1.0
- 압축
- 다중 컨텍스트
- 다중 인스턴스
- 클러스터

설정

플로우 오프로드는 IPSEC과 DTLS 모두에 지원되는 플랫폼에서 기본적으로 활성화됩니다. Cli/flex-config를 활성화하거나 비활성화하는 데 활용할 수 있습니다.

<#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

문제 해결

더 진행하기 전에 협상이 완료되고 SA가 설정되기 전까지 오프로드가 시작되지 않는다는 점을 이해해주십시오. DTLS의 경우도 마찬가지이므로 초기 악수나 협상 중 발생한 문제는 오프로드와 관련이 없을 수 있으며, 기존의 트러블슈팅 방식인 디버그 및 필요한 캡처를 사용할 수 있습니다. 플로우 오프로딩과 관련된 특정 문제는 트래픽 중단 형태로 발생할 수 있습니다.

플로우 오프로드가 활성화되었고 플로우 오프로드로 인한 패킷 처리에 문제가 있는 경우 확인을 유

도하기 위해 실행할 수 있는 몇 가지 중요한 명령이 있습니다.

- show crypto ipsec sa 명령을 확인하여 오프로드가 활성화되었는지 확인합니다.

<#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
```

- 오프로딩 확인을 위해 show ipsec stats 명령도 참조할 수 있습니다.

<#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 9.22로 진행하면서 DTLS 오프로드도 도입했습니다. show flow-offload info detail을 사용하여 DTLS와 IPSEC 오프로드의 상태를 모두 확인할 수 있습니다.

<#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 출력에서 가능한 삭제/오류 카운터를 확인합니다. 출력은 문제에 따라 달라질 수 있습니다. 경우에 따라 6튜플의 miss count가 매우 높게 나타났다. 그러나 모범 사례는 이러한 출력은 적절한 카운터에 대한 비교 분석을 위해 문제 발생 시 여러 번 수집되어야 한다는 것입니다. CAM 통계 카운터에 대한 간단한 설명은 각 카운터가 특정 목적을 가지고 있으며, 주로 패킷을 식별하고 올바르게 전달하는 분류자 역할을 합니다. 두 출력 세트는 IPSEC 및 DTLS 통계를 나타냅니다.

<#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 명령은 오프로드 카운터에도 참조될 수 있으며 비교 분석을 위해 여러 번 수집해야 합니다.

<#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 캡처에 아무것도 표시되지 않으면 암호화된 패킷을 수신하도록 IPSEC 또는 DTLS 오프로드 캡처를 수집할 수 있습니다. LINA는 FPGA가 수신 패킷을 올바르게 처리하여 데이터경로에 삽입한 경우에만 출력을 캡처합니다. 패킷이 FPGA에서 올바르게 처리되지 않은 경우 LINA 캡처에 아무것도 표시되지 않을 가능성이 있지만, 이는 패킷을 전혀 수신하지 않았음을 의미하지는 않습니다. 모든 도구를 사용하여 덤프를 읽기 가능한 형식으로 복원할 수 있습니다.

<#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
```

- 또한 스위치 레벨 캡처를 확인하여 트래픽이 FPGA에 올바르게 수신되고 전달되는지 확인하는 옵션도 있습니다. 이러한 캡처는 랩 환경에서 가져온 것이므로 프로덕션 환경에 미치는 영향을 최소화하기 위해 적절한 필터를 적용해야 합니다. 자세한 내용은 Secure Firewall Captures에서 참조할 수 있습니다.

```
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
```

- DTLS별 출력의 경우 이전 show 출력과 함께 세션별 데이터에 대해 확인할 수 있습니다. 또한 분석을 위해 여러 번 가져올 수 있으며, 특히 패킷이 올바르게 처리 및 전달되는지 여부를 확인하는 표시된 카운터를 사용할 수 있습니다.

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

- 요구 사항에 따라 실행할 수 있는 추가 CLI는 거의 없습니다.

<#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
```

- 이와 함께 DTLS와 IPSEC 오프로드 모두에 대해 몇 가지 중요한 카운터를 확인하기 위해 문제가 발생하는 동안 fxos CLI에서 show npu-accel statistics를 여러 번 수집할 수도 있습니다. 이 출력은 문제 유형 및 환경에 따라 달라집니다.

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

- 일반적으로, FXOS 및 FTD의 문제 해결 파일이 이전 출력과 함께 분석을 위해 HA에서 실행 중인 경우 두 디바이스에서 모두 FTD CLI의 show tech 지원과 함께 수집되는 것이 좋습니다.

결론

이 문서의 목적은 새로운 FPGA 기반 플랫폼에서 수행되는 아키텍처 변경으로 인해 제한된 가시성 측면에서 어려운 상황에서 오프로드 특정 출력을 수집하는 방법을 자세히 설명하는 것입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.