

# Comprendre et dépanner le déchargement IPsec et DTLS dans Secure Firepower 3100 et 4200

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations sur les fonctionnalités](#)

[Plates-formes prises en charge](#)

[Limite](#)

[Déchargement IPsec](#)

[Déchargement DTLS](#)

[Configuration](#)

[Dépannage](#)

[Conclusion](#)

---

## Introduction

Ce document décrit le dépannage des problèmes courants dans l'architecture Firepower responsable de la gestion du déchargement de flux.

## Conditions préalables

La configuration IPsec est basée sur la route ou sur la stratégie, ou les deux.

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN de site à site
- VPN d'accès à distance

## Composants utilisés

Les informations contenues dans ce document sont basées sur :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations sur les fonctionnalités

Les modèles de périphériques de prise en charge utilisent le déchargement de flux IPsec où, après la négociation initiale d'un VPN site à site IPsec ou d'une association de sécurité VPN d'accès à distance (SA), les connexions IPsec sont déchargées vers la matrice de portes programmables sur site (FPGA) dans le périphérique, ce qui améliore les performances du périphérique.

Les opérations déchargées sont spécifiquement liées au traitement de pré-déchiffrement et de déchiffrement en entrée, et au traitement de pré-chiffrement et de chiffrement en sortie. Le logiciel système gère le flux interne pour appliquer vos stratégies de sécurité.

## Plates-formes prises en charge

Le déchargement de flux IPsec est activé par défaut et s'applique à ces types de périphériques jusqu'à présent :

- Pare-feu sécurisé 3100
- Pare-feu sécurisé 4200

Le déchargement de flux IPsec est également utilisé lorsque le VTI provient de l'interface de bouclage.

Le déchargement IPsec est disponible sur les plates-formes prises en charge à partir de :

- [Pare-feu sécurisé FTD 7.2](#)
- [Pare-feu sécurisé ASA 9.18](#)

Tandis que le déchargement DTLS est disponible sur les plates-formes prises en charge à partir de :

- [Pare-feu sécurisé FTD 7.6](#)
- [Pare-feu sécurisé ASA 9.22](#)

## Limite

### Déchargement IPsec

Voici les limites du déchargement IPsec :

- IKEv1
- Mode de transport
- Compression
- Post-fragmentation

- Anti-relecture avec une taille de fenêtre autre que 64 bits
- Filtres pare-feu pour le trafic tunnelisé
- Multi-contexte

## Déchargement DTLS

Voici les limites du déchargement DTLS :

- DTLS 1.0
- Compression
- Multi-contexte
- Multi-instance
- Grappe

## Configuration

Le déchargement de flux est activé par défaut sur les plates-formes prises en charge pour IPSEC et DTLS. Cli / flex-config peut être utilisé pour l'activer ou le désactiver.

```
<#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
```

## Dépannage

Avant de poursuivre, veuillez comprendre que le déchargement ne démarre pas tant que la négociation n'est pas terminée et que vous n'avez pas établi une SA. Le cas est à peu près le

même pour DTLS aussi, donc les problèmes lors des premiers échanges ou négociations ne sont peut-être pas liés au déchargement et peuvent avoir l'approche de dépannage traditionnelle avec des débogages et des captures nécessaires. Des problèmes spécifiques liés au déchargement du flux peuvent se produire sous la forme d'une interruption du trafic.

Voici quelques commandes importantes qui peuvent être exécutées pour obtenir une confirmation si vous avez activé le déchargement de flux et que le problème est la gestion des paquets due au déchargement de flux.

- Vérifiez la commande `show crypto ipsec sa` pour vérifier si le déchargement est activé.

<#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 192.0.2.0 255.255.255.252 192.0.2.4 255.255.255.252
    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: 0XXXXXXXX (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
```

- La commande show ipsec stats peut également être utilisée pour la confirmation du déchargement.

```
<#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
```





```
-----  
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

- La commande show counters peut également être utilisée pour les compteurs de déchargement et il est conseillé de les rassembler plusieurs fois dans un but d'analyse comparative.

<#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

- Les captures de déchargement IPSEC ou DTLS peuvent être regroupées pour s'assurer que vous recevez les paquets chiffrés si rien n'est vu dans les captures LINA. Les captures LINA impriment uniquement les sorties si FPGA a traité correctement le paquet entrant et l'a injecté dans le chemin de données. Si le paquet n'a pas été traité correctement par FPGA, il y a de fortes chances que rien ne soit visible dans les captures LINA, mais cela n'implique pas que vous n'avez reçu aucun paquet du tout. N'importe quel outil peut être utilisé pour restaurer les vidages au format lisible.

<#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
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

- Vous avez également la possibilité de vérifier les captures au niveau du commutateur pour vous assurer que le trafic est reçu et transféré correctement vers FPGA. Ces captures proviennent de l'environnement de laboratoire. Veillez à appliquer les filtres appropriés pour minimiser l'impact sur les environnements de production. Les détails peuvent être consultés dans [Captures de pare-feu sécurisées](#).

```
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 ae8a
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
0631 4b9d 0a08 52b5 d084 cb39 d55a ad91
777c cfe4 5555 5555
```

6 packets shown

- Pour les sorties spécifiques à DTLS, avec les sorties show précédentes, cela peut être vérifié pour les données spécifiques à la session. Ils peuvent également être lus plusieurs fois à des fins d'analyse, en particulier les compteurs marqués confirmant si les paquets sont traités et transférés correctement.

<#root>

```
firepower# show asp table socket offloaded
```

Protocol	Socket	State	Local Address	Foreign Address	IB-Pipe#
SVC_UDP	104d40e8	CONNECTED			
	<a href="#">203.0.113.5:443</a>		<a href="#">198.51.100.5:3875</a>	0 0	
SVC_UDP	0f435518	CONNECTED	<a href="#">203.0.113.5:443</a>	<a href="#">198.51.100.6:13265</a>	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 Hd1: 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-sessiondb

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

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

#send errors: 0, #rcv 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](http://203.0.113.5), Local port: 443

Foreign host: [198.51.100.5](http://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 <<<<<<<<

- Il existe peu d'interfaces de ligne de commande supplémentaires qui peuvent être exécutées en fonction des besoins.

<#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

- En plus de cela, pour le déchargement DTLS et IPSEC, les statistiques show npu-accel peuvent également être rassemblées à partir de l'interface de ligne de commande fxos plusieurs fois pendant le problème pour vérifier quelques compteurs importants. Ce résultat varie en fonction du type de problème et de l'environnement.

<#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 <<<<<<<<<

```

- Généralement, il est recommandé d'avoir un fichier de dépannage de FXOS et FTD tous les deux collectés avec show tech support de FTD CLI à partir des deux périphériques au cas où ils sont en cours d'exécution dans HA pour l'analyse avec les résultats précédents.

## Conclusion

L'objectif de ce document est d'expliquer en détail comment collecter des sorties spécifiques de déchargement, car cela est difficile en termes de visibilité limitée en raison des modifications architecturales apportées aux nouvelles plates-formes basées sur FPGA.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.