

# IPsec op Catalyst 9000X Series-Switches configureren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Terminologie](#)

[Configureren](#)

[Netwerkdigram](#)

[HSEC-licentie installeren](#)

[SVTI-tunnelbescherming](#)

[Verifiëren](#)

[IPsec-tunnel](#)

[IOSd-besturingsplane](#)

[PD-controlevlak](#)

[Problemen oplossen](#)

[IOSd](#)

[PD-controlevlak](#)

[PD-dataplane](#)

[Dataplane Packet-tracer](#)

[PDF-dataplane-debugging](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe de functie Internet Protocol Security (IPsec) op Catalyst 9300X switches moet worden geverifieerd.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IPSEC

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9300X switch
- C9400X switch
- Cisco IOS® XE 17.6.4 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Vanaf Cisco IOS® XE 17.5.1 ondersteunen Catalyst 9300-X Series-switches IPsec. IPsec biedt een hoge mate van beveiliging door middel van encryptie en verificatie en beschermt gegevens tegen toegang door onbevoegden. De IPsec-implementatie op de C9300X biedt beveiligde tunnels tussen twee peers met behulp van de sVTI-configuratie (Static Virtual Tunnel Interface).

IPsec-ondersteuning op de Catalyst 9400-X Series switches is geïntroduceerd in Cisco IOS® XE 17.10.1 terwijl ondersteuning voor Catalyst 9500-X is gepland voor 17.12.1.

## Terminologie

IOSd	IOS daemon	Dit is de Cisco IOS-daemon die op de Linux-kernel draait. Het wordt uitgevoerd als een softwareproces binnen de kernel.IOSdprocessing CLI commando's en protocollen die status en configuratie opbouwen.
PD	Platform-afhankelijk	Gegevens en opdrachten die specifiek zijn voor het platform waarop ze worden uitgevoerd
IPSEC	Internet Protocol Security Appliance	Een beveiligde netwerkprotocolreeks die spackets met gegevens verifieert en versleutelt om beveiligde versleutelde communicatie tussen twee computers te bieden via een Internet Protocol-netwerk.
SVTI	Statische virtuele tunnelinterface	Een statisch geconfigureerde virtuele interface waarop u beveiligingsfuncties kunt toepassen
SA	Security associatie	Een SA is een relatie tussen twee of meer entiteiten die beschrijft hoe de entiteiten beveiligingsdiensten gebruiken om veilig te communiceren

FED	Forwarding Engine Driver	De switch die verantwoordelijk is voor hardwareprogrammering van UADP ASIC
-----	--------------------------	--

## Configureren

### Netwerkdigram

In dit voorbeeld functioneren de Catalyst 9300X en ASR 1001-X als IPsec-peers met IPsec virtuele tunnelinterfaces.



### HSEC-licentie installeren

Schakel de functie IPsec op het Catalyst 9300X platform in en u hebt een HSEC-licentie (C9000-HSEC) nodig. Dit verschilt van andere op Cisco IOS XE gebaseerde routerplatforms die IPsec ondersteunen, waar een HSEC-licentie alleen nodig is om de toegestane doorvoersnelheid voor encryptie te verhogen. Op het Catalyst 9300X-platform worden de CLI voor tunnelmodus en tunnelbescherming geblokkeerd als er geen HSEC-licentie is geïnstalleerd:

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

```
C9300X(config-if)#
```

```
tunnel mode ipsec ipv4
```

```
%'tunnel mode' change not allowed
```

```
*Sep 19 20:54:41.068: %PLATFORM_IPSEC_HSEC-3-INVALID_HSEC: HSEC
```

```
license not present: IPSec mode configuration is rejected
```

Installeer de HSEC-licentie wanneer de switch is verbonden met CSM of CSLU met behulp van Smart Licensing:

```
<#root>
```

```
C9300X#
```

```
license smart authorization request add hseck9 local
```

```
*Oct 12 20:01:36.680: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
```

Controleer of de HSEC-licentie correct is geïnstalleerd:

```
<#root>
```

```
C9300X#
```

```
show license summ
```

Account Information:

Smart Account: Cisco Systems, TAC As of Oct 13 15:50:35 2022 UTC

Virtual Account: CORE TAC

License Usage:

License	Entitlement Tag	Count	Status
network-advantage	(C9300X-12Y Network Adv...)	1	IN USE
dna-advantage	(C9300X-12Y DNA Advantage)	1	IN USE
C9K HSEC	(Cat9K HSEC)	0	

NOT IN USE

Schakel IPsec als tunnelmodus in op de tunnelinterface:

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

```
C9300X(config-if)#
```

```
tunnel mode ipsec ipv4
```

```
C9300X(config-if)#
```

```
end
```

Als IPsec is ingeschakeld, wordt de HSEC-licentie IN GEBRUIK

```
<#root>
```

```
C9300X#
```

```
show license summ
```

```
Account Information:
```

```
Smart Account: Cisco Systems, TAC As of Oct 13 15:50:35 2022 UTC
```

```
Virtual Account: CORE TAC
```

```
License Usage:
```

```
License Entitlement Tag Count Status
```

```
-----  
network-advantage (C9300X-12Y Network Adv...) 1 IN USE  
dna-advantage (C9300X-12Y DNA Advantage) 1 IN USE  
C9K HSEC (Cat9K HSEC) 1
```

```
IN USE
```

## SVTI-tunnelbescherming

IPsec-configuratie op de C9300X maakt gebruik van de standaard Cisco IOS XE IPsec-configuratie. Dit is een eenvoudige SVTI-configuratie met [IKEv2 slimme standaardwaarden](#), waarbij we het standaard IKEv2-beleid, IKEv2-voorstel, IPsec-transformatie en IPsec-profiel voor IKEv2 gebruiken.

### C9300X configuratie

```
<#root>
```

```
ip routing
```

```
!
```

```
crypto ikev2 profile default
```

```
match identity remote address 192.0.2.2 255.255.255.255
```

```
authentication remote pre-share key cisco123
```

```
authentication local pre-share key cisco123
```

```
!
```

```
interface Tunnel1
```

```
ip address 192.168.1.1 255.255.255.252
```


```
tunnel source 198.51.100.1
```

```
tunnel mode ipsec ipv4
```

```
tunnel destination 192.0.2.2
```

```
tunnel protection ipsec profile default
```

---

 Opmerking: aangezien Catalyst 9300X in wezen een switch op de toegangslaag is, moet de IP-routing expliciet worden ingeschakeld voor de routing op basis van functies zoals VTI.

---

## Peer-configuratie

```
<#root>
```

```
crypto ikev2 profile default
```

```
match identity remote address 198.51.100.1 255.255.255.255
```

```
authentication remote pre-share key cisco123
```

```
authentication local pre-share key cisco123
```

```
!
```

```
interface Tunnel1
```

```
ip address 192.168.1.2 255.255.255.252
```

```
tunnel source 192.0.2.2
```

```
tunnel mode ipsec ipv4
```

```
tunnel destination 198.51.100.1
```

```
tunnel protection ipsec profile default
```

Raadpleeg de [Configuratiehandleiding](#) voor een meer gedetailleerde bespreking van de verschillende IKEv2- en IPsec-configuraties [C9300X IPsec](#).

## Verifiëren

### IPsec-tunnel

IPsec-implementatie op het C9300X-platform is architectonisch anders dan op de routingplatforms (ASR 1000, ISR 4000, Catalyst 8200/8300, enzovoort), waar de IPsec-functieverwerking wordt geïmplementeerd in de QFP-microcode (Quantum Flow Processor).

De C9300X Forwarding-architectuur is gebaseerd op de UADP ASIC, dus de meeste QFP-functie FIA-implementatie is hier niet van toepassing.

Hier zijn enkele van de belangrijkste verschillen:

- tonen crypto ipsec als peer x.x.x.x platform niet de platform programmering informatie van de FMAN tot QFP.
- Packet-trace werkt ook niet (meer hierover hieronder).
- UADP ASIC ondersteunt crypto traffic classificatie niet, dus toon crypto ruleset platform niet van toepassing

### IOSd-besturingsplane

IPsec-besturingsplane verificatie is precies hetzelfde als die voor de routeringsplatforms, zie . Zo toont u de IPsec SPA die in IOS is geïnstalleerd:

```
<#root>
```

```
C9300X#
```

```
show crypto ipsec sa
```

```
interface: Tunnel1
```

```
  Crypto map tag: Tunnel1-head-0, local addr 198.51.100.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer 192.0.2.2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 200, #pkts encrypt: 200, #pkts digest: 200
```

```
  #pkts decaps: 200, #pkts decrypt: 200, #pkts verify: 200
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

```
  #pkts not compressed: 0, #pkts compr.
```

```
failed: 0
```

```
  #pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 198.51.100.1, remote crypto endpt.: 192.0.2.2
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb TwentyFiveGigE1/0/1
```

```
current outbound spi: 0x42709657(1114674775)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0x4FE26715(1340237589)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 2098,
```

```
flow_id: CAT9K:98
```

```
, sibling_flags FFFFFFFF80000048, crypto map: Tunnel1-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (26/1605)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x42709657(1114674775)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 2097,
```

flow\_id: CAT9K:97

, sibling\_flags FFFFFFFF80000048, crypto map: Tunnel1-head-0  
sa timing: remaining key lifetime (k/sec): (32/1605)  
IV size: 16 bytes  
replay detection support: Y  
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Let op de flow\_id in de output, dit moet overeenkomen met de flow id geïnstalleerd in het voorwaartse vlak.

## PD-controlevlak

Statistieken tussen IOSd en PD besturingsplane

<#root>

C9300X#

show platfor software ipsec policy statistics

PAL CMD	REQUEST	REPLY OK	REPLY ERR	ABORT
SADB_INIT_START	3	3	0	0
SADB_INIT_COMPLETED	3	3	0	0
SADB_DELETE	2	2	0	0
SADB_ATTR_UPDATE	4	4	0	0
SADB_INTF_ATTACH	3	3	0	0
SADB_INTF_UPDATE	0	0	0	0
SADB_INTF_DETACH	2	2	0	0
ACL_INSERT	4	4	0	0
ACL_MODIFY	0	0	0	0
ACL_DELETE	3	3	0	0
PEER_INSERT	7	7	0	0
PEER_DELETE	6	6	0	0
SPI_INSERT	39	37	2	0
SPI_DELETE	36	36	0	0
CFLOW_INSERT	5	5	0	0
CFLOW_MODIFY	33	33	0	0
CFLOW_DELETE	4	4	0	0
IPSEC_SA_DELETE	76	76	0	0
TBAR_CREATE	0	0	0	0
TBAR_UPDATE	0	0	0	0
TBAR_REMOVE	0	0	0	0
	0	0	0	0
PAL NOTIFY	RECEIVE	COMPLETE	PROC ERR	IGNORE
NOTIFY_RP	0	0	0	0
SA_DEAD	0	0	0	0
SA_SOFT_LIFE	46	46	0	0
IDLE_TIMER	0	0	0	0
DPD_TIMER	0	0	0	0
INVALID_SPI	0	0	0	0
	0	5	0	0



VTI SADB	0	33	0	0
TP SADB	0	40	0	0

IPsec PAL database summary:

DB NAME	ENT ADD	ENT DEL	ABORT
PAL_SADB	3	2	0
PAL_SADB_ID	3	2	0
PAL_INTF	3	2	0
PAL_SA_ID	76	74	0
PAL_ACL	0	0	0
PAL_PEER	7	6	0
PAL_SPI	39	38	0
PAL_CFLOW	5	4	0
PAL_TBAR	0	0	0

SADB-objecttabel

<#root>

C9300X#

show plat software ipsec switch active f0 sadb all

IPsec SADB object table:

SADB-ID	Hint	Complete	#RefCnt	#CfgCnt	#ACL-Ref
3	vir-tun-int	true	2	0	0

SADB-vermelding

<#root>

C9300X#

show plat software ipsec switch active f0 sadb identifier 3

```

===== SADB id: 3
      hint: vir-tun-int
      completed: true
reference count: 2
configure count: 0
ACL reference: 0

```

SeqNo (Static/Dynamic)	ACL id
-----	

IPsec-stroominformatie

<#root>

C9300X#

```
show plat software ipsec switch active f0 flow all
```

```
=====
```

```
Flow id: 97
```

```
        mode: tunnel
        direction: outbound
        protocol: esp
           SPI: 0x42709657
    local IP addr: 198.51.100.1
    remote IP addr: 192.0.2.2
    crypto map id: 0
           SPD id: 3
        cpp SPD id: 0
    ACE line number: 0
        QFP SA handle: INVALID
    crypto device id: 0
IOS XE interface id: 65
    interface name: Tunnel1
        use path MTU: FALSE
        object state: active
    object bind state: new
```

```
=====
```

```
Flow id: 98
```

```
        mode: tunnel
        direction: inbound
        protocol: esp
           SPI: 0x4fe26715
    local IP addr: 198.51.100.1
    remote IP addr: 192.0.2.2
    crypto map id: 0
           SPD id: 3
        cpp SPD id: 0
    ACE line number: 0
        QFP SA handle: INVALID
    crypto device id: 0
IOS XE interface id: 65
    interface name: Tunnel1
        object state: active
```

## Problemen oplossen

### IOSd

Deze debug- en show-opdrachten worden vaak verzameld:

```
<#root>
```

```
show crypto eli all
```

```
show crypto socket
```

```
show crypto map
```

```
show crypto ikev2 sa detail
```

```
show crypto ipsec sa
```

```
show crypto ipsec internal
```

```
<#root>
```

```
debug crypto ikev2
```

```
debug crypto ikev2 error
```

```
debug crypto ikev2 packet
```

```
debug crypto ipsec
```

```
debug crypto ipsec error
```

```
debug crypto kmi
```

```
debug crypto socket
```

```
debug tunnel protection
```

## PD-controlevlak

Gebruik de eerder getoonde verificatiestappen om de werking van het PD-besturingsplane te verifiëren. Om eventuele problemen met betrekking tot het PD-besturingsplane op te sporen, kunt u PDF-besturingsplane debugs inschakelen:

1. Verhoog het logniveau naar breedspakig:

```
<#root>
```

C9300X#

```
set platform software trace forwarding-manager switch active f0 ipsec verbose
```

C9300X#

```
show platform software trace level forwarding-manager switch active f0 | in ipsec  
ipsec  
Verbose
```

## 2. Schakel voorwaardelijke debugging van PDF-besturingsplane in:

<#root>

C9300X#

```
debug platform condition feature ipsec controlplane submode level verbose
```

C9300X#

```
show platform conditions
```

Conditional Debug Global State: Stop

Feature	Type	Submode	Level
IPSEC			
	controlplane	N/A	

```
verbose
```

## 3. Verzamel de debug uitvoer van fman\_fp btrace uitvoer:

<#root>

C9300X#

```
show logging process fman_fp module ipsec internal
```

Logging display requested on 2022/10/19 20:57:52 (UTC) for Hostname: [C9300X], Model: [C9300X-24Y], Ver

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds  
executing cmd on chassis 1 ...

Unified Decoder Library Init .. DONE

Found 1 UTF Streams

2022/10/19 20:50:36.686071658 {fman\_fp\_F0-0}{1}: [ipsec] [22441]: (ERR): IPSEC-PAL-IB-Key::

2022/10/19 20:50:36.686073648 {fman\_fp\_F0-0}{1}: [ipsec] [22441]: (ERR): IPSEC-b0 d0 31 04 85 36 a6 08

## PD-dataplane

Controleer de IPsec-tunnelstatistieken van het dataplane, inclusief veelvoorkomende IPsec-druppels zoals HMAC- of replay-fouten

```
<#root>
```

```
C9300X#
```

```
show platform software fed sw active ipsec counters if-id all
```

```
#####
```

```
Flow Stats for if-id 0x41
```

```
#####
```

```
-----  
Inbound Flow Info for
```

```
flow id: 98
```

```
-----  
SA Index: 1
```

```
-----  
Asic Instance 0: SA Stats
```

Packet Format Check Error:	0
Invalid SA:	0
Auth Fail:	0
Sequence Number Overflows:	0
Anti-Replay Fail:	0
Packet Count:	200
Byte Count:	27600

```
-----  
Outbound Flow Info for
```

```
flow id: 97
```

```
-----  
SA Index: 1025
```

```
-----  
Asic Instance 0: SA Stats
```

Packet Format Check Error:	0
Invalid SA:	0
Auth Fail:	0
Sequence Number Overflows:	0
Anti-Replay Fail:	0
Packet Count:	200
Byte Count:	33600



Opmerking: de stroom-id komt overeen met de stroom-id in de show crypto ipsec als uitvoer. Individuele stroomstatistieken kunnen ook worden verkregen met de opdracht toon platformsoftware gevoede switch actieve ipsec tellers als <sa\_id> waar de sa\_id de SA Index in de vorige output.

---

## Dataplane Packet-tracer

Packet-tracer op het UADP ASIC-platform gedraagt zich heel anders dan op het QFP-gebaseerde systeem. Het kan worden ingeschakeld met een handmatige trigger of een PCAP-gebaseerde trigger. Hier is een voorbeeld van het gebruik van PCAP (EPC) gebaseerde trigger.

1. Schakel EPC in en start opname:

```
<#root>
```

```
C9300X#
```

```
monitor capture test interface twentyFiveGigE 1/0/2 in match ipv4 10.1.1.2/32 any
```

<#root>

C9300X#

show monitor capture test

Status Information for Capture test

Target Type:

Interface: TwentyFiveGigE1/0/2, Direction: IN

Status : Inactive

Filter Details:

IPv4

Source IP: 10.1.1.2/32

Destination IP: any

Protocol: any

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 10

File Details:

File not associated

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 0 (no limit)

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

## 2. Draai de rest en stop de opname:

<#root>

C9300X#

monitor capture test start

Started capture point : test

\*Oct 18 18:34:09.656: %BUFCAP-6-ENABLE: Capture Point test enabled.

<run traffic test>

C9300X#

monitor capture test stop

Capture statistics collected at software:

Capture duration - 23 seconds

Packets received - 5

Packets dropped - 0

Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : test

### 3. Exporteer de opname in de flitser

<#root>

C9300X#

```
show monitor capture test buff
```

```
*Oct 18 18:34:33.569: %BUFCAP-6-DISABLE
```

```
Starting the packet display ..... Press Ctrl + Shift + 6 to exit
```

```
 1  0.000000    10.1.1.2 -> 10.2.1.2    ICMP 114 Echo (ping) request  id=0x0003, seq=0/0, ttl=255
 2  0.000607    10.1.1.2 -> 10.2.1.2    ICMP 114 Echo (ping) request  id=0x0003, seq=1/256, ttl=2
 3  0.001191    10.1.1.2 -> 10.2.1.2    ICMP 114 Echo (ping) request  id=0x0003, seq=2/512, ttl=2
 4  0.001760    10.1.1.2 -> 10.2.1.2    ICMP 114 Echo (ping) request  id=0x0003, seq=3/768, ttl=2
 5  0.002336    10.1.1.2 -> 10.2.1.2    ICMP 114 Echo (ping) request  id=0x0003, seq=4/1024, ttl=
```

C9300X#

```
monitor capture test export location flash:test.pcap
```

### 4. Start pakkettracer:

<#root>

C9300X#

```
show platform hardware fed switch 1 forward interface TwentyFiveGigE 1/0/2 pcap flash:test.pcap number 1
```

Show forward is running in the background. After completion, syslog will be generated.

C9300X#

```
*Oct 18 18:36:56.288: %SHFWD-6-PACKET_TRACE_DONE: Switch 1 F0/0: fed: Packet Trace Complete: Execute (
```

```
*Oct 18 18:36:56.288: %SHFWD-6-PACKET_TRACE_FLOW_ID: Switch 1 F0/0: fed: Packet Trace Flow id is 131077
```

C9300X#

```
C9300X#show plat hardware fed switch 1 forward last summary
```

Input Packet Details:

```
###[ Ethernet ]###
```

```
dst      = b0:8b:d0:8d:6b:d6
```

```
src=78:ba:f9:ab:a7:03
```

```
type     = 0x800
```

```
###[ IP ]###
```

```
version  = 4
```

```
ihl      = 5
```

```
tos      = 0x0
```

```
len      = 100
```

```
id       = 15
```

```
flags    =
```

```
frag     = 0
```

```
ttl      = 255
```

```
proto    = icmp
```

```
chksum   = 0xa583
```

```
src=10.1.1.2
```

```
dst      = 10.2.1.2
```

```
options  = ''
```

```
###[ ICMP ]###
```

```
type     = echo-request
```

```
code     = 0
```



chksum = 0xae17  
id = 0x3  
seq = 0x0

###[ Raw ]###

load = '00 00 00 00 01 1B CF 14 AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD A

Ingress:

Port : TwentyFiveGigE1/0/2  
Global Port Number : 2  
Local Port Number : 2  
Asic Port Number : 1  
Asic Instance : 1  
Vlan : 4095  
Mapped Vlan ID : 1  
STP Instance : 1  
BlockForward : 0  
BlockLearn : 0  
L3 Interface : 38  
IPv4 Routing : enabled  
IPv6 Routing : enabled  
Vrf Id : 0

Adjacency:

Station Index : 179  
Destination Index : 20754  
Rewrite Index : 24  
Replication Bit Map : 0x1 ['remoteData']

Decision:

Destination Index : 20754 [DI\_RCP\_PORT3]  
Rewrite Index : 24  
Dest Mod Index : 0 [IGR\_FIXED\_DMI\_NULL\_VALUE]  
CPU Map Index : 0 [CMI\_NULL]  
Forwarding Mode : 3 [Other or Tunnel]  
Replication Bit Map : ['remoteData']  
Winner : L3FWDIPV4 LOOKUP  
Qos Label : 1  
SGT : 0  
DGTID : 0

Egress:

Possible Replication :  
Port : RCP  
Asic Instance : 0  
Asic Port Number : 0  
Output Port Data :  
Port : RCP  
Asic Instance : 0  
Asic Port Number : 90  
Unique RI : 0  
Rewrite Type : 0 [Unknown]  
Mapped Rewrite Type : 229 [IPSEC\_TUNNEL\_MODE\_ENCAP\_FIRSTPASS\_OUTERV4\_INNERV4]  
Vlan : 0  
Mapped Vlan ID : 0  
RCP, mappedRii.fdMuxProfileSet = 1 , get fdMuxProfile from MappedRii  
Qos Label : 1  
SGT : 0

\*\*\*\*\*

Input Packet Details:

N/A: Recirculated Packet

Ingress:

Port : Recirculation Port  
Asic Port Number : 90  
Asic Instance : 0  
Vlan : 0  
Mapped Vlan ID : 2

STP Instance : 0  
BlockForward : 0  
BlockLearn : 0  
L3 Interface : 38  
    IPv4 Routing : enabled  
    IPv6 Routing : enabled  
    Vrf Id : 0  
Adjacency:  
    Station Index : 177  
    Destination Index : 21304  
    Rewrite Index : 21  
    Replication Bit Map : 0x1 ['remoteData']  
Decision:  
    Destination Index : 21304  
    Rewrite Index : 21  
    Dest Mod Index : 0 [IGR\_FIXED\_DMI\_NULL\_VALUE]  
    CPU Map Index : 0 [CMI\_NULL]  
    Forwarding Mode : 3 [Other or Tunnel]  
    Replication Bit Map : ['remoteData']  
    Winner : L3FWDIPV4 LOOKUP  
    Qos Label : 1  
    SGT : 0  
    DGTID : 0

Egress:  
    Possible Replication :  
        Port : TwentyFiveGigE1/0/1  
    Output Port Data :  
        Port : TwentyFiveGigE1/0/1  
        Global Port Number : 1  
        Local Port Number : 1  
        Asic Port Number : 0  
        Asic Instance : 1  
        Unique RI : 0  
        Rewrite Type : 0 [Unknown]  
        Mapped Rewrite Type : 13 [L3\_UNICAST\_IPV4\_PARTIAL]  
        Vlan : 0  
        Mapped Vlan ID : 0

Output Packet Details:  
    Port : TwentyFiveGigE1/0/1

###[ Ethernet ]###  
    dst = 00:62:ec:da:e0:02  
    src=b0:8b:d0:8d:6b:e4  
    type = 0x800

###[ IP ]###  
    version = 4  
    ihl = 5  
    tos = 0x0  
    len = 168  
    id = 2114  
    flags = DF  
    frag = 0  
    ttl = 254  
    proto = ipv6\_crypt  
    chksum = 0x45db  
    src=198.51.100.1  
    dst = 192.0.2.2  
    options = ''

###[ Raw ]###      load = '

6D 18 45 C9

00 00 00 06 09 B0 DC 13 11 FA DC F8 63 98 51 98 33 11 9C C0 D7 24 BF C2 1C 45 D3 1B 91 0B 5F B4 3A C0

\*\*\*\*\*

C9300X#

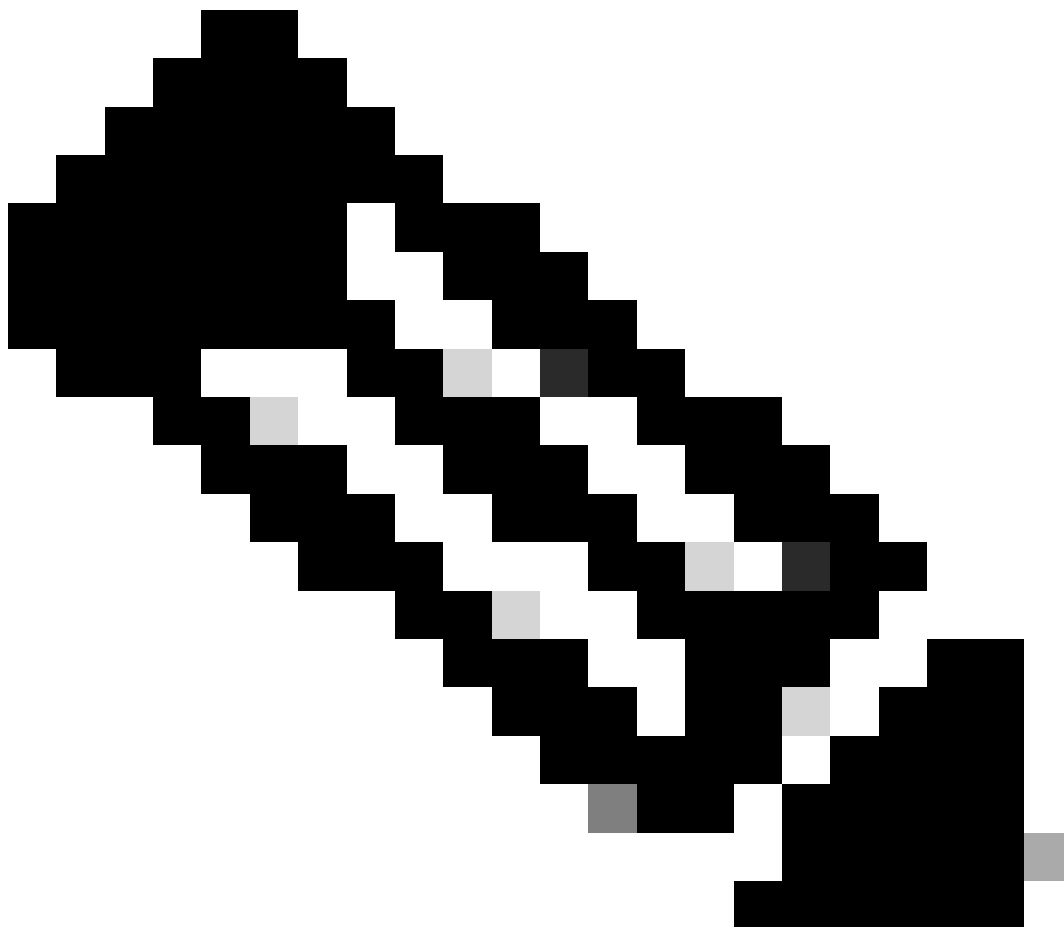
show crypto ipsec sa | in current outbound

current outbound spi:

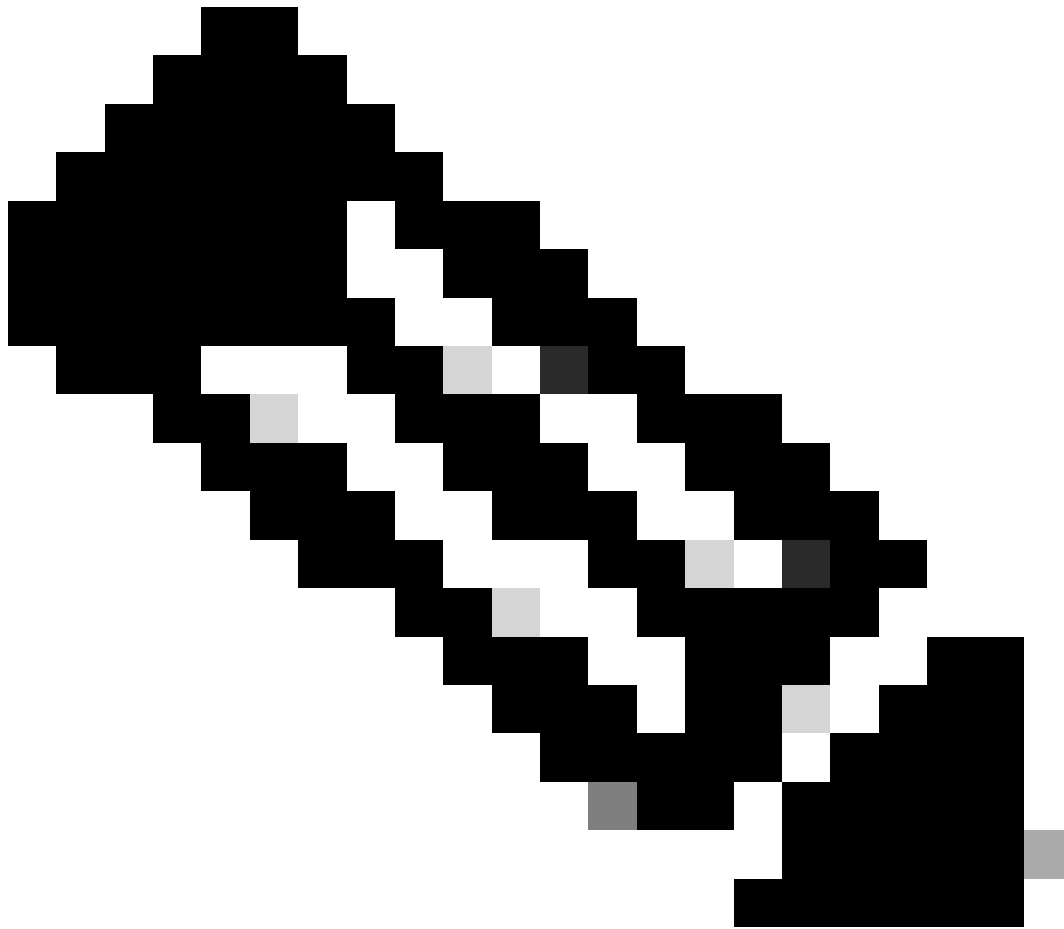
0x6D1845C9

(1830307273)

<-- Matches the load result in packet trace



Opmerking: in de vorige uitvoer is het pakket doorgestuurd uitgang het ESP-pakket met de huidige uitgaande SA SPI. Voor een gedetailleerdere FED-beleidsanalyse, de detailvariant van hetzelfde commando. Voorbeeld: toon plat hardware gevoed switch 1 voorwaartse laatste detail kan worden gebruikt.



**Opmerking:** PDF-dataplane debugging dient alleen mogelijk te zijn met ondersteuning van TAC. Dit zijn zeer lage sporen die de techniek nodig heeft als het probleem niet kan worden geïdentificeerd via normale CLI's/Debugs.

---

<#root>

C9300X#

```
set platform software trace fed switch active ipsec verbose
```

```
C9300X#
```

```
debug platform condition feature ipsec dataplane submode all level verbose
```

```
C9300X#
```

```
show logging process fed module ipsec internal
```

**IPsec PD/SHIM-debug**

```
<#root>
```

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

## Gerelateerde informatie

- [IPsec op Catalyst 9300 Switches configureren](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.