

在Catalyst 9000X系列交換機上配置IPsec

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[技術](#)

[設定](#)

[網路圖表](#)

[安裝HSEC許可證](#)

[SVTI通道保護](#)

[驗證](#)

[IPsec通道](#)

[IOSd控制平面](#)

[PD控制平面](#)

[疑難排解](#)

[IOSd](#)

[PD控制平面](#)

[PD資料平面](#)

[資料平面Packet Tracer](#)

[PD資料平面調試](#)

[相關資訊](#)

簡介

本檔案介紹如何驗證Catalyst 9300X交換器上的網際網路通訊協定安全(IPsec)功能。

必要條件

需求

思科建議您瞭解以下主題：

- IPsec

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C9300

- C9400
- Cisco IOS® XE 17.6.4及更高版本

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。

背景資訊

從Cisco IOS® XE 17.5.1開始，Catalyst 9300-X系列交換機支援IPsec。IPsec透過加密和身份驗證提供高級別的安全性，並保護資料免遭未經授權的訪問。C9300X上的IPsec實施使用sVTI（靜態虛擬隧道介面）配置在兩個對等體之間提供安全隧道。

Cisco IOS® XE 17.10.1中引入了Catalyst 9400-X系列交換機上的IPsec支援，而Catalyst 9500-X的支援預定為17.12.1。

技術

IOSd	IOS守護程式	這是在Linux核心上運行的Cisco IOS守護程式。它在核心中作為軟體進程運行。IOSdprocesses CLI命令和協定，用於建立狀態和配置。
PD	視平台而定	運行平台的特定資料和命令
IPsec	網際網路通訊協定安全性	一種安全網路協定簇，它驗證和加密資料的間隔，以便透過Internet協定網路在兩台電腦之間提供安全的加密通訊。
SVTI	靜態虛擬通道介面	靜態配置的虛擬介面，您可以對其應用安全功能
SA	安全性關聯	SA是兩個或多個實體之間的關係，描述實體如何使用安全服務進行安全通訊
FED	轉發引擎驅動程式	負責UADP ASIC硬體程式設計的交換機元件

設定

網路圖表

在本示例中，Catalyst 9300X和ASR1001-X作為IPsec對等體與IPsec虛擬隧道介面起作用。



安裝HSEC許可證

在Catalyst 9300X平台上啟用IPSec功能，需要HSEC許可證(C9000-HSEC)。這與支援IPSec的基於Cisco IOS XE的其他路由平台不同，在該平台中，僅需要使用HSEC許可證來增加允許的加密吞吐量。在Catalyst 9300X平台上，如果未安裝HSEC許可證，則隧道模式和隧道保護 CLI將被阻止：

```
<#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
```

使用智慧許可在交換機連線到CSSM或CSLU時安裝HSEC許可證：

```
<#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
```

驗證已正確安裝HSEC許可證：

```
<#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
```

在隧道介面上啟用IPsec作為隧道模式：

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

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

```
tunnel mode ipsec ipv4
```

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

```
end
```

一旦啟用IPSec，HSEC許可證就會被使用

```
<#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

IN USE

SVTI通道保護

C9300X上的IPsec配置使用標準Cisco IOS XE IPsec配置。這是使用[IKEv2 Smart Defaults](#)的簡單SVTI配置，其中我們使用IKEv2的預設IKEv2策略、IKEv2方案、IPsec轉換和IKEv2的IPsec配置檔案。

C9300X配置

```
<#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
```

 注意：由於Catalyst 9300X基本上是接入層交換機，因此必須明確啟用ip routing，才能使基於路由的功能（如VTI）正常工作。

對等配置

```
<#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
```

有關各種IKEv2和IPsec配置結構的更詳細討論，請參閱[C9300X IPsec配置指南](#)。

驗證

IPsec通道

C9300X平台上的IPsec實施在架構上不同於路由平台（ASR1000、ISR4000、Catalyst 8200/8300等），其中IPsec功能處理在QFP（量子流處理器）微碼中實現。

C9300X轉發架構基於UADP ASIC，因此大多數QFP功能FIA實施不適用於此處。

以下是一些主要區別：

- show crypto ipsec sa peer x.x.x.x platform不顯示從FMAN到QFP的平台程式設計資訊。
- Packet-trace也不起作用（有關以下內容的詳細資訊）。
- UADP ASIC不支援加密流量分類，因此show crypto ruleset platform不適用

IOSd控制平面

IPsec控制平面驗證與路由平台的驗證完全相同，請參閱。要顯示IOSd中安裝的IPsec SA，請執行以下操作：

```
<#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:
```

注意輸出中的flow_id，它必須與轉發平面中安裝的流id匹配。

PD控制平面

IOSd和PD控制平面之間的統計資訊

```
<#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物件表格

<#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條目

<#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流資訊

<#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
```

疑難排解

IOSd

通常會收集以下debug和show命令：

```
<#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控制平面

要檢驗PD控制平面操作，請使用前面顯示的檢驗步驟。要調試與PD控制平面相關的所有問題，請啟用PD控制平面調試：

1. 將btrace日誌記錄級別提升至詳細：

```
<#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. 啟用PD控制平面條件調試：

```
<#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. 收集 fman_fp btrace 輸出的調試輸出：

<#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資料平面

驗證資料層面IPsec隧道統計資訊，包括常見IPsec丟棄（例如HMAC或重播故障）

<#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

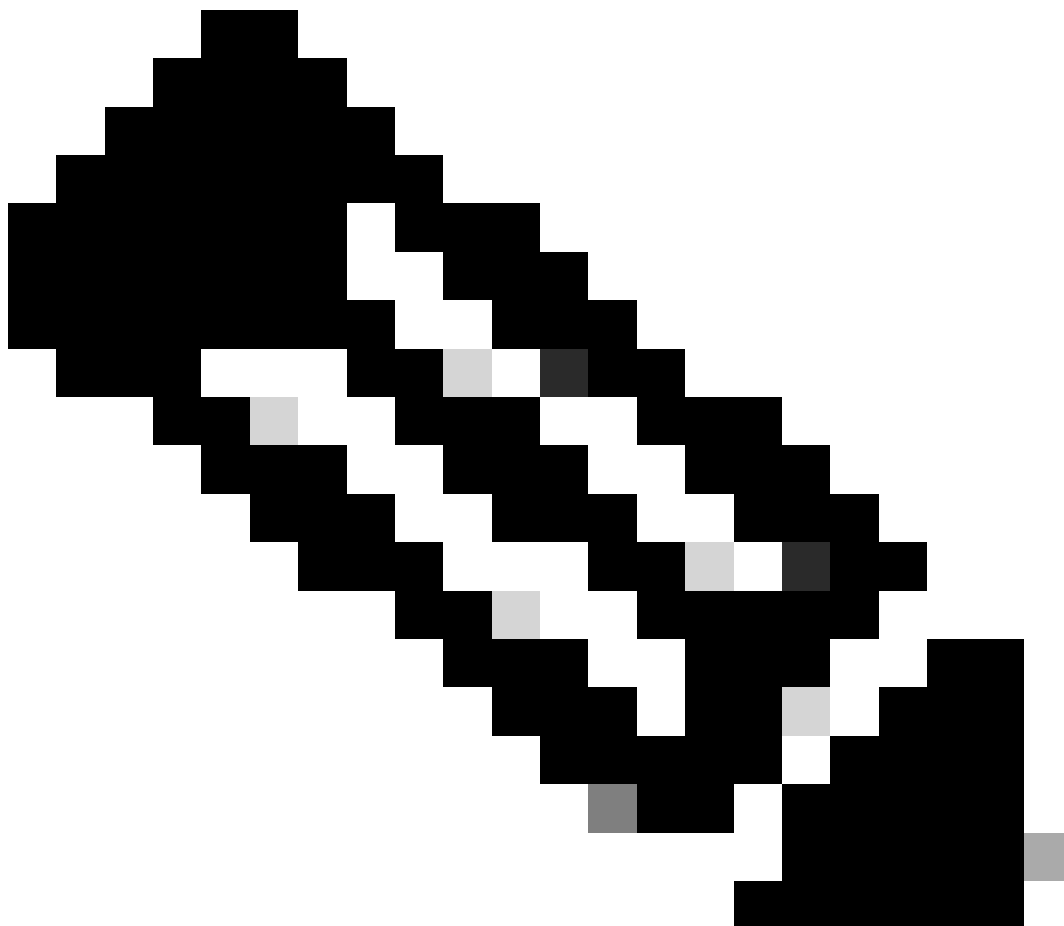
Outbound Flow Info for

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



注意：流ID與show crypto ipsec sa輸出中的流ID匹配。使用show platform software fed

switch active ipsec counters sa <sa_id>命令還可以獲取單個流統計資料，其中sa_id是前面輸出中的SA索引。

資料平面Packet Tracer

UADP ASIC平台上的Packet Tracer與基於QFP的系統上的Packet Tracer的行為完全不同。可以使用手動觸發器或基於PCAP的觸發器啟用它。以下是使用基於PCAP (EPC)的觸發器的示例。

1. 啟用EPC並開始捕獲：

```
<#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. 執行其餘專案並停止擷取：

```
<#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 exist till exported or cleared
```

```
Stopped capture point : test
```

3. 將擷取匯出至快閃記憶體

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

```
C9300X#
```

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

4. 運行Packet Tracer :

```
<#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
```


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:
```

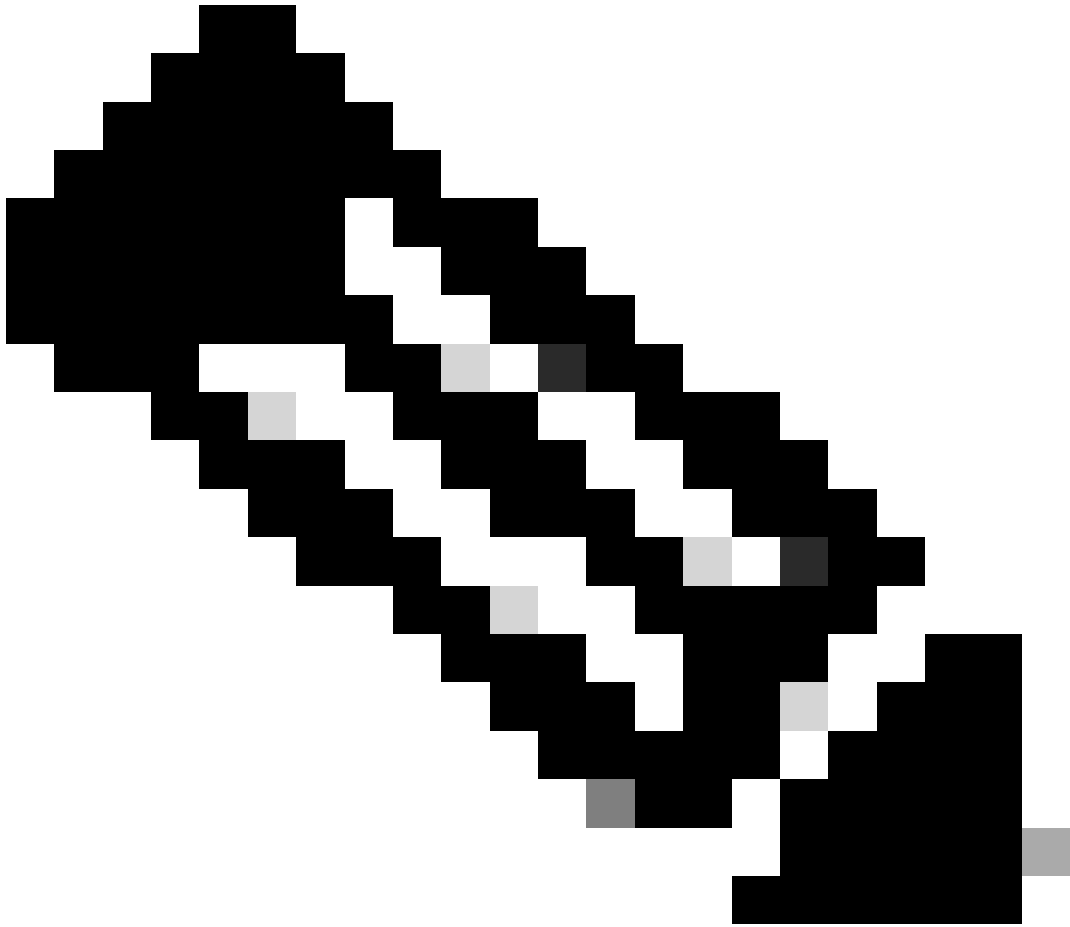
```
0x6D1845C9
```

```
(1830307273)
```

```
<-- Matches the load result in packet trace
```



注意：在前面的輸出中，轉發到出口的資料包是具有當前出站SA SPI的ESP資料包。要獲得更詳細的FED轉發決策分析，可使用同一命令的detail變體。示例：可以使用show plat hardware fed switch 1 forward last detail。



注意：只能在TAC的幫助下啟用PD資料平面調試。如果無法通過常規CLI/調試辨識問題，則工程需要這些非常低級別的跟蹤。

```
<#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調試

<#root>

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

相關資訊

- [在Catalyst 9300交換機上配置IPsec](#)

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）。