在Catalyst 9000X系列交换机上配置IPsec

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 术语

配置

- 网络图
- 安装HSEC许可证
- SVTI隧道保护

验证

- IPSec 隧道
- Cisco IOS控制平面
- PD控制平面

故障排除

- Cisco IOS
- PD控制平面
- PD数据平面
- 数据平面Packet-tracer
- PD数据平面调试

相关信息

简介

本文档介绍如何验证Catalyst 9300X交换机上的互联网协议安全(IPsec)功能。

先决条件

要求

Cisco 建议您了解以下主题：

- IPsec

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C9300X
- C9400X
- Cisco IOS® XE 17.6.4及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

从Cisco IOS® XE 17.5.1开始，Catalyst 9300-X系列交换机支持IPsec。IPsec通过加密和身份验证提供高级别的安全性，并保护数据免遭未经授权的访问。C9300X上的IPsec实施使用sVTI（静态虚拟隧道接口）配置在两个对等体之间提供安全隧道。

Cisco IOS® XE 17.10.1中引入了Catalyst 9400X系列交换机上的IPsec支持。

术语

IOSd	Cisco IOS后台守护程序	Linux 内核上运行的 Cisco IOS 后台守护程序，它在内核中作为软件进程运行。IOS处理用于建立状态和配置的CLI命令和协议。
PD	平台相关	特定于运行这些数据的平台的数据和命令
IPsec	Internet 协议安全性	一种安全网络协议簇,验证并对数据空间进行加密，以便在两台计算机之间通过Internet Protocol网络提供安全加密通信。

SVTI	静态虚拟隧道接口	可以应用安全功能的静态配置的虚拟接口
SA	安全关联	SA是两个或多个实体之间的关系，用于描述实体如何使用安全服务进行安全通信
美联储	转发引擎驱动程序	交换机组件负责UADP ASIC的硬件编程。

配置

网络图

在本例中，Catalyst 9300X和ASR1001-X用作具有IPsec虚拟隧道接口的IPsec对等体。



安装HSEC许可证

在Catalyst 9300X平台上启用IPsec功能，需要两个许可证：HSEC许可证(C9000-HSEC)和DNA优势。这与支持IPsec的其他基于Cisco IOS XE的路由平台不同，在支持IPsec的路由平台中，仅需要使用HSEC许可证来增加允许的加密吞吐量。在Catalyst 9300X平台上，如果未安装HSEC许可证，则阻止tunnel mode和tunnel protection CLI:

```
<#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
```

当交换机使用智能许可连接到思科许可中心或CSLU时，安装HSEC许可证：

```
<#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
```

验证HSEC许可证已正确安装：

```
<#root>
C9300X#
show license summary

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
```

在隧道接口上启用IPsec作为隧道模式：

```
<#root>

C9300X(config)#

interface tunnel1


C9300X(config-if)#

tunnel mode ipsec ipv4


C9300X(config-if)#

end
```

启用IPsec后，HSEC许可证即会使用

```
<#root>

C9300X#

show license summary


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隧道保护

C9300X上的IPsec配置使用标准的Cisco IOS XE IPsec配置。这是使用IKEv2 Smart Defaults的简单SVTI配置，其中我们使用IKEv2的默认IKEv2策略、IKEv2提议、IPsec转换和IPsec配置文件进行IKEv2。

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：由于Catalyst 9300X本质上是接入层交换机，因此必须明确启用ip路由，才能使VTI等基于路由的功能发挥作用。

对等体配置

<#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
```

有关各种IKEv2和IPsec配置结构的更详细讨论，请参阅C9300X IPsec配置指南。

验证

IPSec 隧道

C9300X平台上的IPsec实施在架构上不同于路由平台（ASR1000、ISR4000、Catalyst 8200/8300等），其中IPsec功能处理在QFP（量子流处理器）微码中实现。

C9300X转发架构基于UADP ASIC，因此大多数QFP功能FIA实施在此不适用。

以下是一些主要区别：

- show crypto ipsec sa peer x.x.x.x platform 不显示从FMAN到QFP的平台编程信息。
- Packet-trace也不起作用（有关以下内容的详细信息）。
- UADP ASIC不支持加密流量分类，因此show crypto ruleset platform不适用

Cisco IOS控制平面

IPsec控制平面验证与路由平台的验证完全相同，请参阅。要显示Cisco IOS中安装的IPsec SA，请执行以下操作：

```
<#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:
```

请注意，输出中的flow_id必须与转发平面中安装的流id匹配。

PD控制平面

Cisco IOS和PD控制平面之间的统计信息

<#root>

C9300X#

show platform 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对象表

<#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条目

<#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流信息

<#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
```

故障排除

Cisco IOS

通常收集以下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

要验证PD控制平面操作，请使用前面显示的验证步骤。要调试与PD控制平面相关的任何问题，请启用PD控制平面调试：

1.将btrace logging级别增加至verbose:

```
<#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.启用PD控制平面条件调试：

<#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输出的调试输出：

<#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数据平面

验证数据平面IPsec隧道统计信息，包括常见IPsec丢弃（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与show crypto ipsec sa输出中的流id匹配。也可以使用show platform software fed switch active ipsec counters sa <sa_id>命令获取单个流统计信息，其中sa_id是上一个

输出中的SA Index。

数据平面Packet-tracer

UADP ASIC平台上的Packet Tracer与基于QFP的系统上的Packet Tracer的行为截然不同。可以使用手动触发器或基于PCAP的触发器启用它。以下是使用基于PCAP(EPC)的触发器的示例。

1.启用EPC并开始捕获：

<#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.运行其余操作并停止捕获：

<#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.将捕获导出到闪存中

<#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.运行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
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 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 A
********************************************************************************
```

C9300X#

show crypto ipsec sa | in current outbound

```
 current outbound spi:
```

0x6D1845C9

(1830307273)

<-- Matches the load result in packet trace

注意：在前面的输出中，转发的数据包出口是具有当前出站SA SPI的ESP数据包。有关更详细的FED转发决策分析，请参阅同一命令的detail变体。示例：可使用show plat

---

hardware fed switch 1 forward last detail。

这是加密模块解密数据包后入站IPsec数据包解封处理的示例。请注意，在入口转发路径中，解密后，数据包将作为IPnIP封装数据包重新循环到UADP。

```
C9300X#show plat hardware fed switch 1 forward last summary
Input Packet Details:
###[ Ethernet ]###
  dst       = 8c:94:61:17:95:e4
  src=00:c1:64:c3:d5:d0
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 120
     id        = 34
     flags     =
     frag      = 0
     ttl       = 254
     proto     = ipencap
     chksum    = 0x5038
     src=192.0.2.2
     dst       = 198.51.100.1
     options   = ''
###[ IP ]###
        version   = 4
        ihl       = 5
        tos       = 0x0
        len       = 100
        id        = 23
        flags     =
        frag      = 0
        ttl       = 255
        proto     = icmp
        chksum    = 0xa7e8
        src=10.2.1.2
        dst       = 10.1.1.2
        options   = ''
###[ ICMP ]###
           type      = echo-reply
           code      = 0
           chksum    = 0xa60e
           id        = 0x6
           seq       = 0x0
###[ Raw ]###
              load      = '00 00 00 00 00 42 DF F3 AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB C
Ingress:
   Port                     : TwentyFiveGigE1/0/1
   Global Port Number       : 1
   Local Port Number        : 1
   Asic Port Number         : 0
   Asic Instance            : 0
   Vlan                     : 4095
```

```
   Mapped Vlan ID            : 1
   STP Instance              : 1
   BlockForward              : 0
   BlockLearn                : 0
   L3 Interface              : 37
       IPv4 Routing          : enabled
       IPv6 Routing          : enabled
       Vrf Id                : 0
   Adjacency:
       Station Index         : 187
       Destination Index     : 20498
       Rewrite Index         : 28
       Replication Bit Map   : 0x4    ['localData']
   Decision:
       Destination Index     : 20498  [DI_RCP_PORT1]
       Rewrite Index         : 28
       Dest Mod Index        : 0      [IGR_FIXED_DMI_NULL_VALUE]
       CPU Map Index         : 0      [CMI_NULL]
       Forwarding Mode       : 3      [Other or Tunnel]
       Replication Bit Map   :        ['localData']
       Winner                :        IPSECINSSECDECAP LOOKUPV4
       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      : 88
       Unique RI             : 0
       Rewrite Type          : 0      [Unknown]
       Mapped Rewrite Type   : 262    [IPSEC_TUNNEL_MODE_DECAP_SECONDPASS_INNERV4]
       Vlan                  : 4095
       Mapped Vlan ID        : 1
        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          : 88
   Asic Instance             : 0
   Vlan                      : 0
   Mapped Vlan ID            : 2
   STP Instance              : 0
   BlockForward              : 0
   BlockLearn                : 0
   L3 Interface              : 39
       IPv4 Routing          : enabled
       IPv6 Routing          : enabled
       Vrf Id                : 0
   Adjacency:
       Station Index         : 117    [SI_CPUQ_FORUS_TRAFFIC]
       Destination Index     : 21116
       Rewrite Index         : 1
       Replication Bit Map   : 0x8    ['localCpu']
```

```
   Decision:
       Destination Index     : 21116  [DI_CPUQ_FORUS_TRAFFIC]
       Rewrite Index         : 1      [RI_CPU]
       Dest Mod Index        : 0      [IGR_FIXED_DMI_NULL_VALUE]
       CPU Map Index         : 0      [CMI_NULL]
       Forwarding Mode       : 3      [Other or Tunnel]
       Replication Bit Map   :        ['localCpu']
       Winner                :        L3FWDIPV4 LOOKUP
       Qos Label             : 1
       SGT                   : 0
       DGTID                 : 0
Egress:
   Possible Replication      :
       Port                  : CPU_Q_FORUS_TRAFFIC
   Output Port Data          :
     Port                    : CPU
       Asic Instance         : 0
       CPU Queue             :      2 [CPU_Q_FORUS_TRAFFIC]
       Unique RI             : 0
       Rewrite Type          : 0      [Unknown]
       Mapped Rewrite Type   : 17     [CPU_ENCAP]
       Vlan                  : 0
       Mapped Vlan ID        : 2
*****************************************************************************
```

PD数据平面调试



注意：PD数据平面调试只能在TAC的帮助下启用。如果无法通过常规CLI/调试识别问题，则工程需要这些非常低级别的跟踪。

<#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调试

<#root>

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

相关信息

- 在Catalyst 9300交换机上配置IPsec
- 在Catalyst 9400交换机上配置IPsec
- 适用于Catalyst交换的思科IOS XE 17.12.1

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。