Configurazione di IPsec sugli switch Catalyst serie 9000X

Sommario

Introduzione

In questo documento viene descritto come verificare la funzionalità IPsec (Internet Protocol Security) sugli switch Catalyst 9300X.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IPSec

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9300X
- C9400X
- Cisco IOS® XE 17.6.4 e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

A partire da Cisco IOS® XE 17.5.1, gli switch Catalyst serie 9300-X supportano IPsec. IPsec fornisce elevati livelli di sicurezza tramite la crittografia e l'autenticazione, nonché la protezione dei dati dall'accesso non autorizzato. L'implementazione IPsec su C9300X fornisce tunnel sicuri tra due peer utilizzando la configurazione sVTI (Static Virtual Tunnel Interface).

Il supporto IPsec sugli switch Catalyst serie 9400-X è stato introdotto in Cisco IOS® XE 17.10.1, mentre il supporto per Catalyst 9500-X è previsto per la versione 17.12.1.

Terminologia

IOS d	daemon IOS	Questo è il daemon Cisco IOS che viene eseguito sul kernel Linux. Viene eseguito come processo software all'interno del kernel.IOSdelabora i comandi e i protocolli CLI che generano lo stato e la configurazione.
PD	Dipendente dalla piattaforma	Dati e comandi specifici della piattaforma su cui vengono eseguiti
IPSec	Internet Protocol Security	Suite di protocolli di rete sicuri che autentica e crittografa pacchetti di dati per garantire comunicazioni crittografate protette tra due computer su una rete IP.
SVTI	Interfaccia tunnel virtuale statica	Interfaccia virtuale configurata staticamente a cui è possibile applicare le funzionalità di sicurezza
SA	Associazione di protezione	Un'associazione di sicurezza è una relazione tra due o più entità che descrive il modo in cui le entità utilizzano i servizi di sicurezza per comunicare in modo sicuro

FED	Driver motore di inoltro	Il componente dello switch responsabile della programmazione hardware di UADP ASIC

Configurazione

Esempio di rete

In questo esempio, Catalyst 9300X e ASR1001-X funzionano come peer IPsec con interfacce tunnel virtuali IPsec.

Installa licenza HSEC

Abilitare la funzione IPsec sulla piattaforma Catalyst 9300X. È richiesta una licenza HSEC (C9000-HSEC). Ciò è diverso da altre piattaforme di routing basate su Cisco IOS XE che supportano IPsec, dove una licenza HSEC è necessaria solo per aumentare la velocità di crittografia consentita. Sulla piattaforma Catalyst 9300X, la modalità tunnel e la CLI di protezione tunnel sono bloccate se non è installata una licenza HSEC:

<#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
```

Installare la licenza HSEC quando lo switch è connesso a CSM o CSLU tramite 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
```

Verificare che la licenza HSEC sia installata correttamente:

```
<#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
```

Abilitare IPsec come modalità tunnel sull'interfaccia del tunnel:

```
<#root>

C9300X(config)#

int tunnel1


C9300X(config-if)#

tunnel mode ipsec ipv4


C9300X(config-if)#

end
```

Dopo aver abilitato IPsec, la licenza HSEC diventa IN USO

<#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

Protezione tunnel SVTI

La configurazione IPsec del C9300X utilizza la configurazione IPsec Cisco IOS XE standard. Si tratta di una configurazione SVTI semplice che utilizza IKEv2 Smart Defaults, in cui vengono utilizzati il criterio IKEv2 predefinito, la proposta IKEv2, la trasformazione IPSec e il profilo IPSec per IKEv2.

Configurazione C9300X

<#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

Nota: poiché Catalyst 9300X è essenzialmente uno switch a livello di accesso, il routing ip deve essere abilitato esplicitamente per il funzionamento di funzionalità basate sul routing come la VTI.

Configurazione peer

<#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
```

Per una descrizione più dettagliata dei vari costrutti di configurazione di IKEv2 e IPsec, vedere la Guida alla configurazione di IPsec per C9300X.

Verifica

Tunnel IPsec

L'implementazione di IPSec sulla piattaforma C9300X ha un'architettura diversa da quella delle piattaforme di routing (ASR1000, ISR4000, Catalyst 8200/8300, ecc.), in cui l'elaborazione delle funzioni IPSec viene implementata nel microcodice QFP (Quantum Flow Processor).

L'architettura di inoltro C9300X è basata sull'ASIC UADP, quindi la maggior parte dell'implementazione FIA della funzione QFP non è applicabile in questo caso.

Di seguito sono riportate alcune delle principali differenze:

- show crypto ipsec sa peer x.x.x.x la piattaforma non visualizza le informazioni di programmazione della piattaforma dal FMAN fino al QFP.
- Anche Packet-trace non funziona (per ulteriori informazioni, vedere di seguito).
- L'ASIC UADP non supporta la classificazione del traffico crittografico, quindi show crypto ruleset platform non è applicabile

IOSd Control Plane

La verifica del control plane IPsec è esattamente la stessa che si verifica per le piattaforme di routing, vedere . Per visualizzare l'associazione di protezione IPsec installata in IOSd:

<#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:
```

Notare il flow_id nell'output, deve corrispondere all'id di flusso installato nel piano di inoltro.

Piano di controllo PD

Statistiche tra IOSd e PD control plane

<#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
```

Tabella oggetti SADB

<#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
```

voce SADB

<#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
        ---------------------------------------
```

Informazioni sul flusso IPSec

<#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
```

Risoluzione dei problemi

IOS d

Di seguito vengono riportati i comandi debug e show comunemente raccolti:

<#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
```

Piano di controllo PD

Per verificare le operazioni del Piano di controllo PD, utilizzate le operazioni di verifica mostrate in precedenza. Per eseguire il debug di qualsiasi problema relativo al control plane PD, abilitare i debug del control plane PD:

1. Aumentare il livello di registrazione della traccia di blog in modo che sia dettagliato:

<#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. Abilitare il debug condizionale del control plane PD:

<#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. Raccogliere l'output del comando debug dall'output del comando btrace fman_fp:

<#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 Data Plane

Verificare le statistiche del tunnel IPsec della corsia di dati, incluse le cadute IPsec comuni, ad esempio gli errori HMAC o di riproduzione

<#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

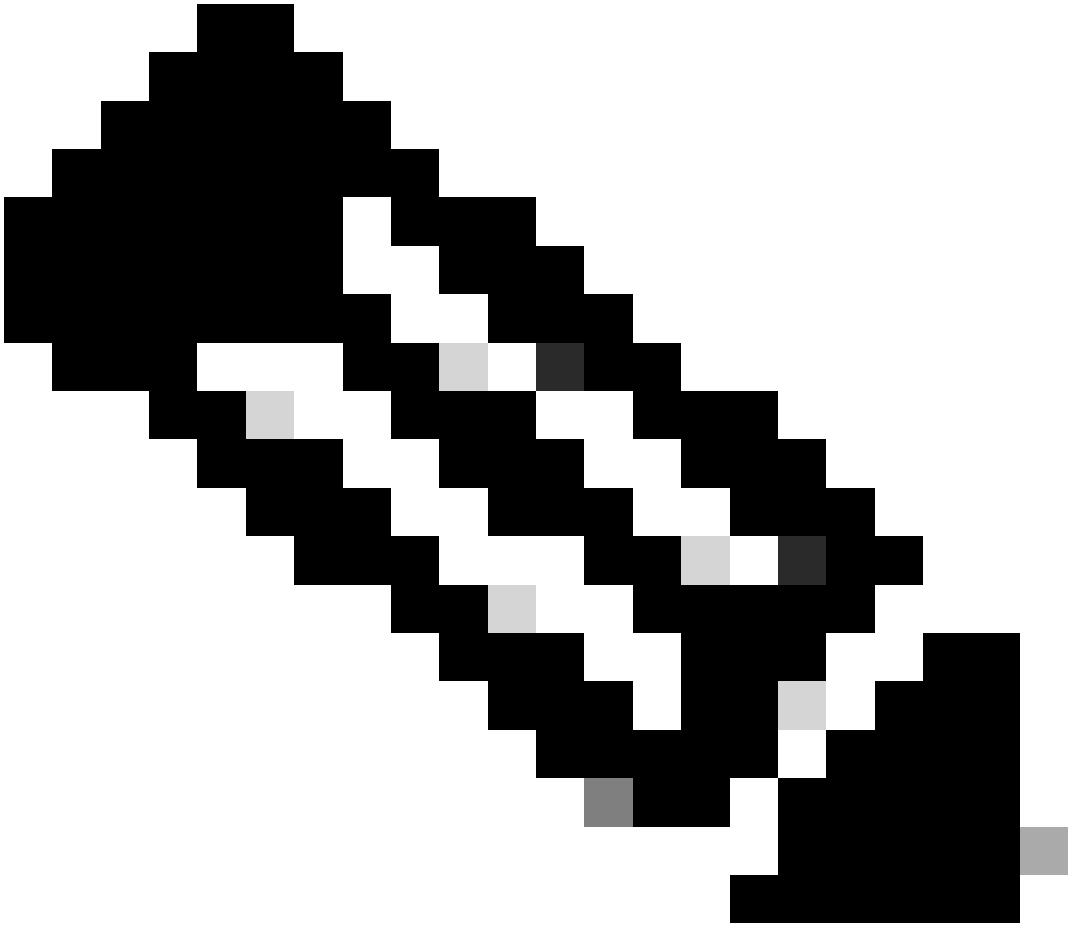
```
--------------------
Asic Instance 0: SA Stats
  Packet Format Check Error:    0
  Invalid SA:            0
  Auth Fail:            0
  Sequence Number Overflows:    0
  Anti-Replay Fail:        0
  Packet Count:            200
  Byte Count:            27600
---------------------------------
Outbound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



Nota: l'ID del flusso corrisponde all'ID del flusso nell'output show crypto ipsec sa. Le statistiche di flusso individuali possono essere ottenute anche con il comando show platform software fed switch active ipsec counters come <sa_id> dove sa_id rappresenta l'indice SA nell'output precedente.

Dataplane Packet-tracer

Il comportamento di Packet-tracer sulla piattaforma UADP ASIC è molto diverso da quello del sistema basato su QFP. Può essere attivato con un trigger manuale o basato su PCAP. Di seguito è riportato un esempio di utilizzo del trigger basato su PCAP (EPC).

1. Abilitare EPC e avviare l'acquisizione:

```
<#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. Eseguire il resto e interrompere la cattura:

```
<#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. Esportare l'acquisizione in memoria flash

<#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. Eseguire 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
```

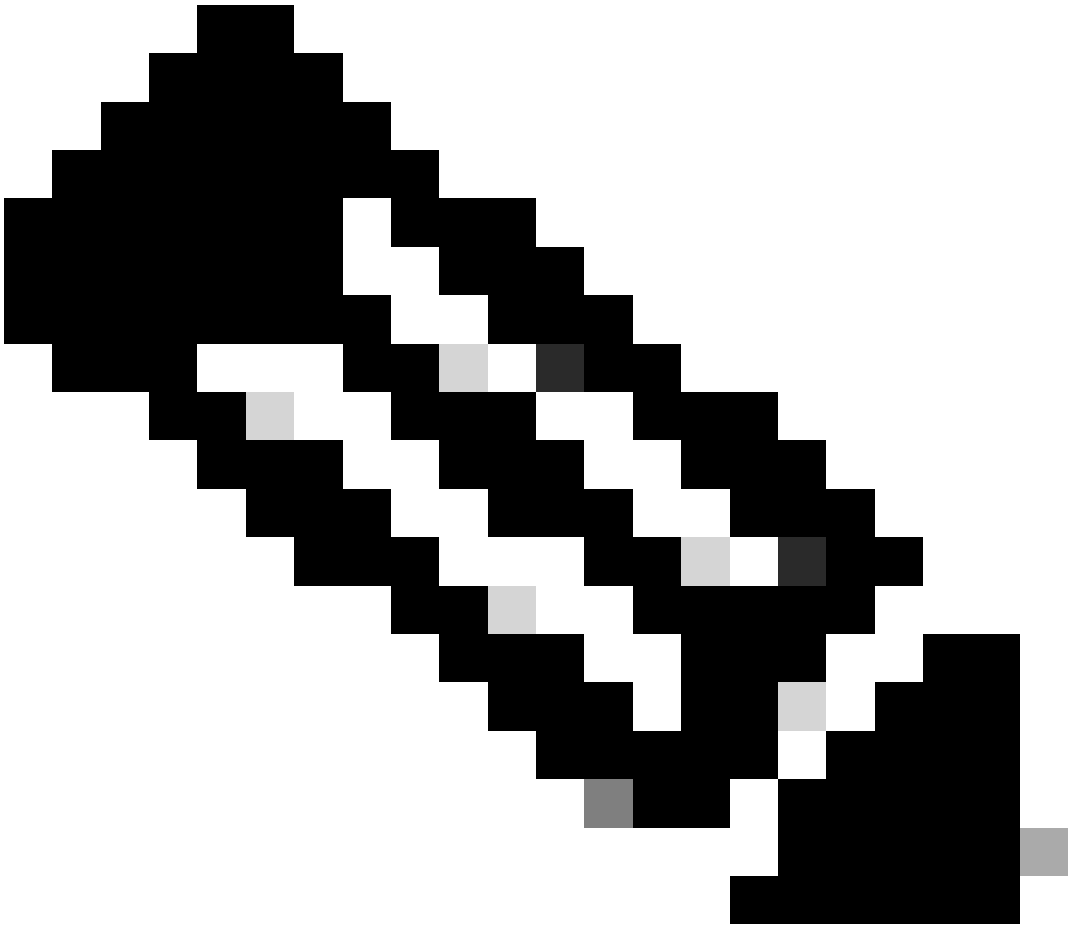
```
        chksum    = 0xae17
        id        = 0x3
        seq       = 0x0
###[ Raw ]###
           load      = '00 00 00 00 01 1B CF 14 AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD A
Ingress:
   Port                      : TwentyFiveGigE1/0/2
   Global Port Number        : 2
   Local Port Number         : 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

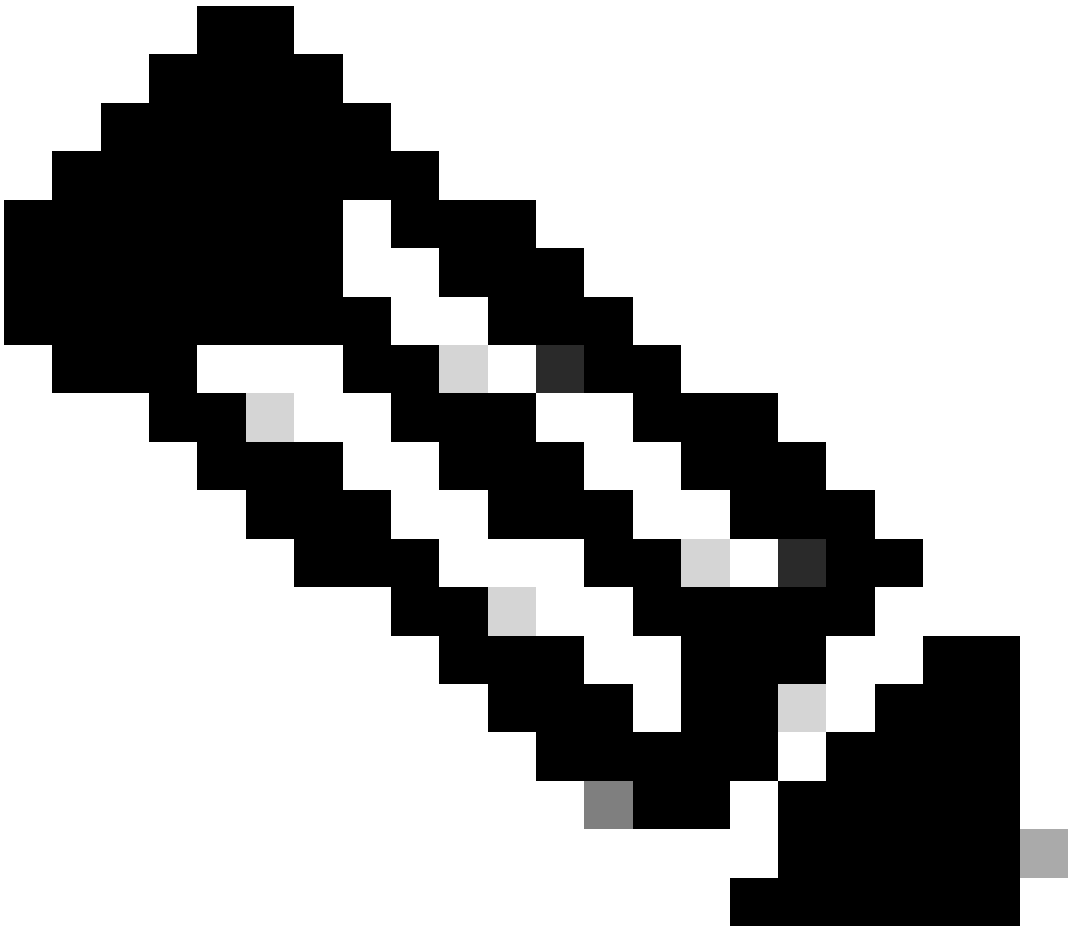
```
 00 00 00 06 09 B0 DC 13 11 FA DC F8 63 98 51 98 33 11 9C C0 D7 24 BF C2 1C 45 D3 1B 91 0B 5F B4 3A C0 A
```

```
********************************************************************************

C9300X#
show crypto ipsec sa | in current outbound

 current outbound spi:
0x6D1845C9
(1830307273)
<-- Matches the load result in packet trace
```



Nota: nell'output precedente, il pacchetto inoltrato in uscita è il pacchetto ESP con l'SPI SA in uscita corrente. Per un'analisi più dettagliata della decisione di inoltro FED, usare la variante detail dello stesso comando. Esempio: può essere utilizzato l'ultimo dettaglio dell'interruttore di alimentazione 1 del plat.

Debug del dataplane PD



Nota: il debug del piano dati PD deve essere abilitato solo con l'assistenza di TAC. Si tratta di tracce di livello molto basso necessarie ai tecnici se il problema non può essere identificato tramite CLI/Debug normali.

<#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

Debug SHIM IPsec PD

<#root>

debug platform software ipsec info

debug platform software ipsec error

debug platform software ipsec verbose

```
debug platform software ipsec all
```

Informazioni correlate

- Configurazione di IPsec sugli switch Catalyst 9300

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).