

Configurar o IPsec nos switches Catalyst 9000X Series

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Terminologia](#)

[Configurar](#)

[Diagrama de Rede](#)

[Instalar licença HSEC](#)

[Proteção de túnel SVTI](#)

[Verificar](#)

[Túnel IPsec](#)

[Plano de controle IOSd](#)

[Plano de controle PD](#)

[Troubleshooting](#)

[IOSd](#)

[Plano de controle PD](#)

[Plano de dados PD](#)

[Packet Tracer do Dataplane](#)

[Depuração de Dataplane PD](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como verificar o recurso Internet Protocol Security (IPsec) nos switches Catalyst 9300X.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IPsec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9300X
- C9400X
- Cisco IOS® XE 17.6.4 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A partir do Cisco IOS® XE 17.5.1, os switches da série Catalyst 9300-X suportam IPsec. O IPsec fornece altos níveis de segurança por meio de criptografia e autenticação, além de proteger os dados contra acesso não autorizado. A implementação IPsec no C9300X fornece túneis seguros entre dois pares usando a configuração sVTI (Static Virtual Tunnel Interface).

O suporte a IPsec nos switches da série Catalyst 9400-X foi introduzido no Cisco IOS® XE 17.10.1, enquanto o suporte para o Catalyst 9500-X está programado para 17.12.1.

Terminologia

IOSd	daemon IOS	Este é o daemon do Cisco IOS executado no kernel do Linux. Ele é executado como um processo de software dentro do kernel. IOSd processa comandos e protocolos CLI que criam o estado e a configuração.
PD	Dependente da plataforma	Dados e comandos específicos da plataforma em que são executados
IPsec	Segurança de protocolo de Internet	Um conjunto de protocolos de rede segura que autentica e criptografa pacotes de dados para fornecer comunicação criptografada segura entre dois computadores em uma rede Internet Protocol.
sVTI	Interface de túnel virtual estático	Uma interface virtual configurada estaticamente à qual você pode aplicar recursos de segurança
SA	Associação de segurança	Um SA é um relacionamento entre duas ou mais entidades que descreve como as entidades usam serviços de segurança para se comunicar com segurança

FED	Driver do mecanismo de encaminhamento	O componente de switch responsável pela programação de hardware do UADP ASIC
-----	---------------------------------------	--

Configurar

Diagrama de Rede

Neste exemplo, o Catalyst 9300X e o ASR1001-X funcionam como pares IPsec com interfaces de túnel virtual IPsec.



Instalar licença HSEC

Habilite o recurso IPsec na plataforma Catalyst 9300X. É necessária uma licença HSEC (C9000-HSEC). Isso é diferente de outras plataformas de roteamento baseadas no Cisco IOS XE que suportam IPsec, em que uma licença HSEC é necessária apenas para aumentar o throughput de criptografia permitido. Na plataforma Catalyst 9300X, o modo de túnel e a CLI de proteção de túnel são bloqueados se uma licença HSEC não estiver instalada:

```
<#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
```

Instale a licença HSEC quando o switch estiver conectado ao CSSM ou CSLU usando o 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
```

Verifique se a licença HSEC está instalada corretamente:

```
<#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

Habilite IPsec como o modo de túnel na interface de túnel:

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

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

```
tunnel mode ipsec ipv4
```

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

```
end
```

Depois que o IPsec é habilitado, a licença HSEC se torna EM 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
```

Proteção de túnel SVTI

A configuração de IPsec no C9300X usa a configuração padrão de IPsec do Cisco IOS XE. Esta é uma configuração SVTI simples usando [Padrões Inteligentes IKEv2](#), onde estamos usando a política IKEv2 padrão, proposta IKEv2, transformação IPsec e perfil IPsec para IKEv2.

Configuração do 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
```

 Observação: como o Catalyst 9300X é essencialmente um switch de camada de acesso, o IP routing precisa ser explicitamente habilitado para que os recursos baseados em roteamento, como o VTI, funcionem.

Configuração de Par

```
<#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
```

Para uma discussão mais detalhada das várias construções de configuração IKEv2 e IPsec, consulte o [Guia de configuração do C9300X IPsec](#).

Verificar

Túnel IPsec

A implementação de IPsec na plataforma C9300X é arquitetonicamente diferente que nas plataformas de roteamento (ASR1000, ISR4000, Catalyst 8200/8300, etc.), onde o processamento de recursos de IPsec é implementado no microcódigo QFP (Quantum Flow Processor).

A arquitetura de encaminhamento do C9300X é baseada no ASIC UADP, portanto, a maior parte da implementação do FIA de recursos QFP não se aplica aqui.

Aqui estão algumas das principais diferenças:

- `show crypto ipsec sa peer x.x.x.x platform` não mostra as informações de programação da plataforma do FMAN até o QFP.
- O rastreamento de pacotes também não funciona (mais sobre isso abaixo).
- O UADP ASIC não oferece suporte à classificação de tráfego de criptografia, portanto, `show crypto rule platform` não se aplica

Plano de controle IOSd

A verificação do plano de controle IPsec é exatamente a mesma que a das plataformas de roteamento, consulte . Para exibir o SA IPsec instalado no 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:
```

Observe o flow_id na saída; ele deve corresponder ao id de fluxo instalado no plano de encaminhamento.

Plano de controle PD

Estatísticas entre IOSd e plano de controle PD

```
<#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

Tabela de objetos 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

entrada 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
-----
```

Informações de fluxo de 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
```

Troubleshooting

IOSd

Esses comandos debug e show são normalmente coletados:

<#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
```

Plano de controle PD

Para verificar as operações do Plano de controle PD, use as etapas de verificação mostradas anteriormente. Para depurar quaisquer problemas relacionados ao plano de controle PD, ative as depurações do plano de controle PD:

1. Aumente o nível de log do btrace para detalhado:

<#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. Ativar a depuração condicional do painel de controle 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. Colete a saída de depuração da saída de 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

Plano de dados PD

Verificar as estatísticas de túnel IPsec do dataplane, incluindo quedas de IPsec comuns, como falhas de HMAC ou de reprodução

```
<#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
```



Observação: o id de fluxo corresponde ao id de fluxo na saída show crypto ipsec sa. As estatísticas de fluxo individuais também podem ser obtidas com o comando show platform software fed switch active ipsec counters sa <sa_id> onde sa_id representa o índice SA na saída anterior.

Packet Tracer do Dataplane

O Packet Tracer na plataforma UADP ASIC se comporta de forma muito diferente do sistema baseado em QFP. Ele pode ser ativado com um acionador manual ou um acionador baseado em PCAP. Este é um exemplo do uso do acionador baseado em PCAP (EPC).

1. Habilitar EPC e iniciar captura:

```
<#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. Execute o resto e pare a captura:

<#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. Exportar a captura para 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. Executar 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 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#

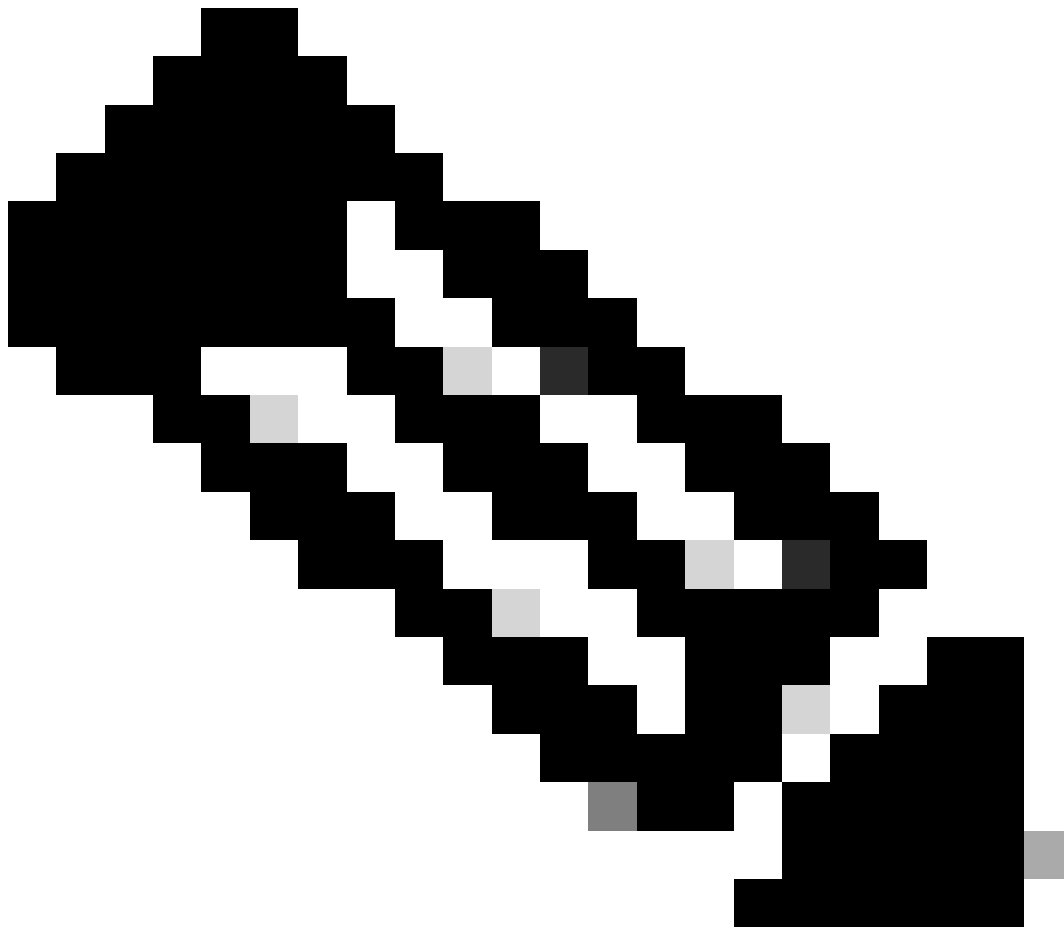
show crypto ipsec sa | in current outbound

current outbound spi:

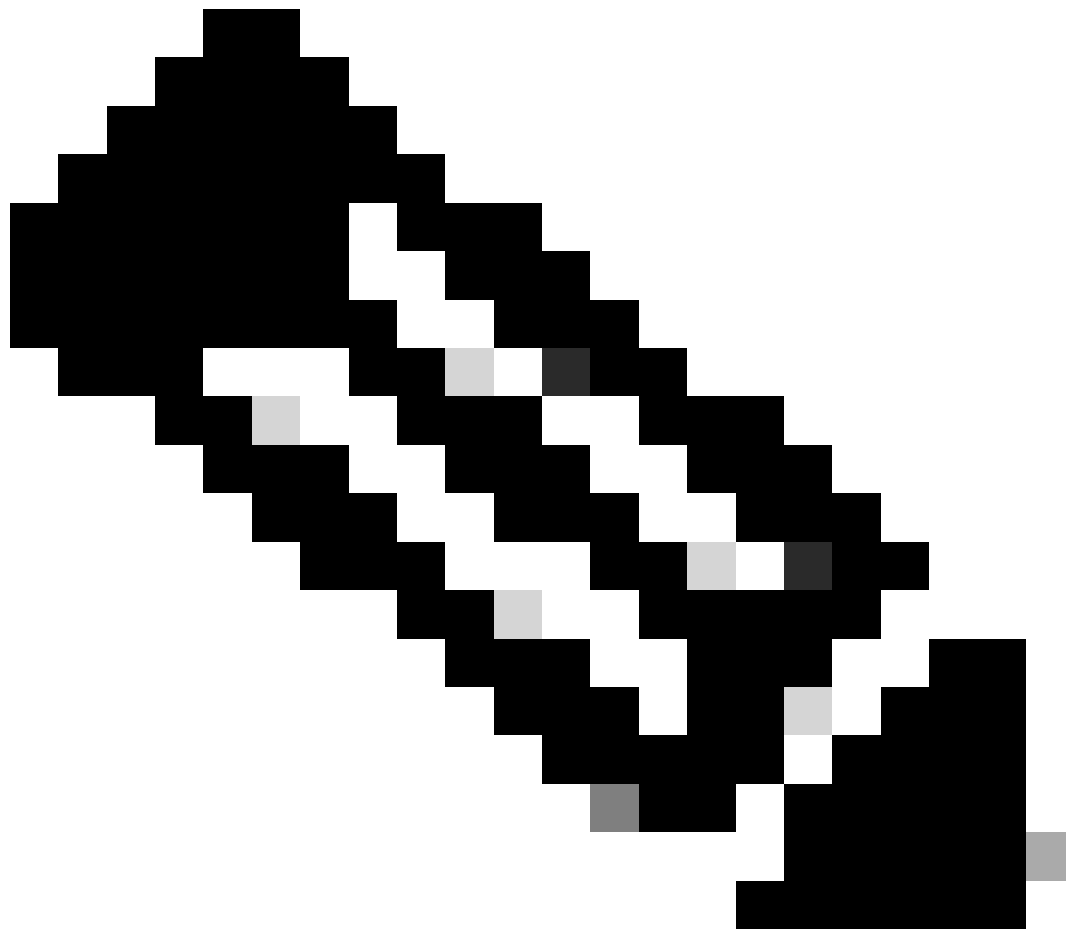
0x6D1845C9

(1830307273)

<-- Matches the load result in packet trace



Observação: na saída anterior, o pacote encaminhado é o pacote ESP com o SA SPI de saída atual. Para uma análise de decisão de encaminhamento de FED mais detalhada, a variante detail do mesmo comando. Exemplo: show plat hardware fed switch 1 forward last detail pode ser usado.



Observação: a depuração do plano de dados PD só deve ser habilitada com a assistência do TAC. Esses são rastreamentos de nível muito baixo que a engenharia precisa se o problema não puder ser identificado através de CLIs/depurações normais.

<#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
```

Depurações IPsec PD SHIM

```
<#root>
```

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

Informações Relacionadas

- [Configurar o IPsec em Switches Catalyst 9300](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.