

Catalyst 9000XシリーズスイッチでのIPsecの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[用語](#)

[設定](#)

[ネットワーク図](#)

[HSECライセンスのインストール](#)

[SVTIトンネル保護](#)

[確認](#)

[IPsecトンネル](#)

[IOSdコントロールプレーン](#)

[PDコントロールプレーン](#)

[トラブルシューティング](#)

[IOS](#)

[PDコントロールプレーン](#)

[PDデータプレーン](#)

[データプレーンパケットトレース](#)

[PDデータプレーンデバッグ](#)

[関連情報](#)

はじめに

このドキュメントでは、Catalyst 9300Xスイッチのインターネットプロトコルセキュリティ (IPSec)機能を確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPSec

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C9300x
- C9400x
- Cisco IOS® XE 17.6.4以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco IOS® XE 17.5.1以降、Catalyst 9300-XシリーズスイッチはIPsecをサポートしています。IPsecは、暗号化と認証を通じて高レベルのセキュリティを提供し、不正アクセスからデータを保護します。C9300XでのIPsecの実装では、sVTI(Static Virtual Tunnel Interface)設定を使用して2つのピア間に安全なトンネルを提供します。

Catalyst 9400-XシリーズスイッチでのIPsecサポートはCisco IOS® XE 17.10.1で導入されましたが、Catalyst 9500-Xのサポートは17.12.1で予定されています。

用語

IOS	IOSデーモン	これは Linux カーネル上で動作する Cisco IOS デーモンで、カーネル内のソフトウェアプロセスとして実行される。IOSdは、CLIコマンドと、ビルドアップ状態と設定を行うプロトコルを処理する。
PD	プラットフォーム依存	実行されているプラットフォームに固有のデータとコマンド
IPSec	インターネットプロトコルセキュリティ	データの認証と暗号化の両方式を実行して、インターネットプロトコルネットワーク上の2台のコンピュータ間で安全で暗号化された通信を提供する、安全なネットワークプロトコルスイート。
SVTI	スタティック仮想トンネルインターフェイス	セキュリティ機能を適用できる、静的に設定された仮想インターフェイス
SA	Security Association	SAは2つ以上のエンティティ間の関係であり、エンティティがセキュリティサービスを使用して安全に通信する方法を記述します

FED	転送エンジンドライバ	UADP ASICのハードウェアプログラミングを担当するスイッチコンポーネント
-----	------------	---

設定

ネットワーク図

この例では、Catalyst 9300XとASR1001-Xは、IPsec仮想トンネルインターフェイスを備えたIPsecピアとして機能します。



HSECライセンスのインストール

Catalyst 9300XプラットフォームでIPsec機能を有効にするには、HSECライセンス(C9000-HSEC)が必要です。これは、IPSecをサポートする他のCisco IOS XEベースのルーティングプラットフォームとは異なります。このようなプラットフォームでは、許可される暗号化スループットを増やすためだけにHSECライセンスが必要です。Catalyst 9300Xプラットフォームでは、HSECライセンスがインストールされていない場合、tunnel modeおよびtunnel protection CLIはブロックされます。

```
<#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
```

Smart Licensingを使用してスイッチをCSSMまたはCSLUに接続するときに、HSECライセンスをインストールします。

```
<#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
```

HSECライセンスが正しくインストールされていることを確認します。

```
<#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
```

トンネルインターフェイスでトンネルモードとしてIPsecを有効にします。

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

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

```
tunnel mode ipsec ipv4
```

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

```
end
```

IPsecを有効にすると、HSECライセンスは使用されます

```
<#root>
```

```
C9300X#
```

```
show license summ
```

```
Account Information:
```

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

```
Virtual Account: CORE TAC
```

```
License Usage:
```

```
License Entitlement Tag Count Status
```

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

```
IN USE
```

SVTIトンネル保護

C9300XのIPsec設定では、標準のCisco IOS XE IPsec設定を使用します。これは、[IKEv2スマートデフォルト](#)を使用した簡単なSVTI設定です。ここでは、デフォルトのIKEv2ポリシー、IKEv2プロポーザル、IPsecトランスフォーム、およびIKEv2のIPsecプロファイルを使用します。

C9300Xの設定

```
<#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:Catalyst 9300Xは本質的にはアクセスレイヤスイッチであるため、VTIなどのルーティングベースの機能が動作するには、ip routingを明示的に有効にする必要があります。

ピア設定

```
<#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
```

さまざまなIKEv2およびIPsec設定構造の詳細については、『[C9300X IPsecコンフィギュレーションガイド](#)』を参照してください。

確認

IPsecトンネル

C9300XプラットフォームでのIPsecの実装は、ルーティングプラットフォーム (ASR1000、ISR4000、Catalyst 8200/8300など) でのアーキテクチャとは異なります。ルーティングプラットフォームでは、IPsecの機能処理がQFP(Quantum Flow Processor)マイクロコードで実装されます。

C9300XのフォワーディングアーキテクチャはUADP ASICに基づいているため、QFP機能のFIA実装のほとんどは、ここでは適用されません。

主な違いは次のとおりです。

- show crypto ipsec sa peer x.x.x.x platform は、FMANからQFPまでのプラットフォームプロダクション情報を表示しません。
- パケットトレースも機能しません (詳細は後述) 。
- UADP ASICは暗号化トラフィックの分類をサポートしていないため、show crypto ruleset platformは適用されません

IOSdコントロールプレーン

IPsecコントロールプレーンの検証は、ルーティングプラットフォームの検証とまったく同じです。を参照してください。IOSdにインストールされているIPsec SAを表示するには、次のコマンドを実行します。

```
<#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:

出力のflow_idは、フォワーディングプレーンにインストールされたフローIDと一致している必要があります。

PDコントロールプレーン

IOSdとPDコントロールプレーン間の統計情報

<#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オブジェクトテーブル

<#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エントリ

<#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フロー情報

<#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
```

トラブルシューティング

IOS

次に示すdebugコマンドとshowコマンドは、一般に収集されます。

<#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コントロールプレーン

PDコントロールプレーンの動作を確認するには、前に示した確認手順を使用します。PDコントロールプレーンに関連する問題をデバッグするには、PDコントロールプレーンデバッグを有効にします。

1. btraceのログレベルをverboseに上げます。

<#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. PDコントロールプレーンの条件付きデバッグを有効にします。

<#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. fman_fp btrace出力からデバッグ出力を収集します。

<#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データプレーン

HMACやリプレイ障害などの一般的なIPsecドロップを含む、データプレーンIPsecトンネル統計情報の確認

```
<#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：フローidは、show crypto ipsec sa出力のフローidと一致します。個々のフロー統計情報は、コマンドshow platform software fed switch active ipsec counters sa <sa_id>でも取得できます。ここで、sa_idは、上記の出力のSAインデックスです。

データプレーンパケットトレーサ

UADP ASICプラットフォームのパケットトレーサは、QFPベースのシステムのパケットトレーサとは動作が大きく異なります。手動トリガーまたはPCAPベースのトリガーで有効にできます。次に、PCAP(EPC)ベースのトリガーの使用例を示します。

1. EPCを有効にし、キャプチャを開始します。

```
<#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. 残りを実行し、キャプチャを停止します。

<#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. キャプチャをフラッシュにエクスポートします

```
<#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. packet-tracerを実行します。

```
<#root>
```

```
C9300X#
```

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

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

```
C9300X#
```

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

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

```
C9300X#
```

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

```
Input Packet Details:
```

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

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

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

```
type     = 0x800
```

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

```
version  = 4
```

```
ihl      = 5
```

```
tos      = 0x0
```

```
len      = 100
```

```
id       = 15
```

```
flags    =
```

```
frag     = 0
```

```
ttl      = 255
```

```
proto    = icmp
```

```
chksum   = 0xa583
```

```
src=10.1.1.2
```

```
dst      = 10.2.1.2
```

```
options  = ''
```

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

```
type     = echo-request
```

```
code     = 0
```

```
chksum   = 0xae17
```

```
id       = 0x3
```

```
seq      = 0x0
```


###[Raw]###

load = '00 00 00 00 01 1B CF 14 AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD 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
  checksum = 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#
```

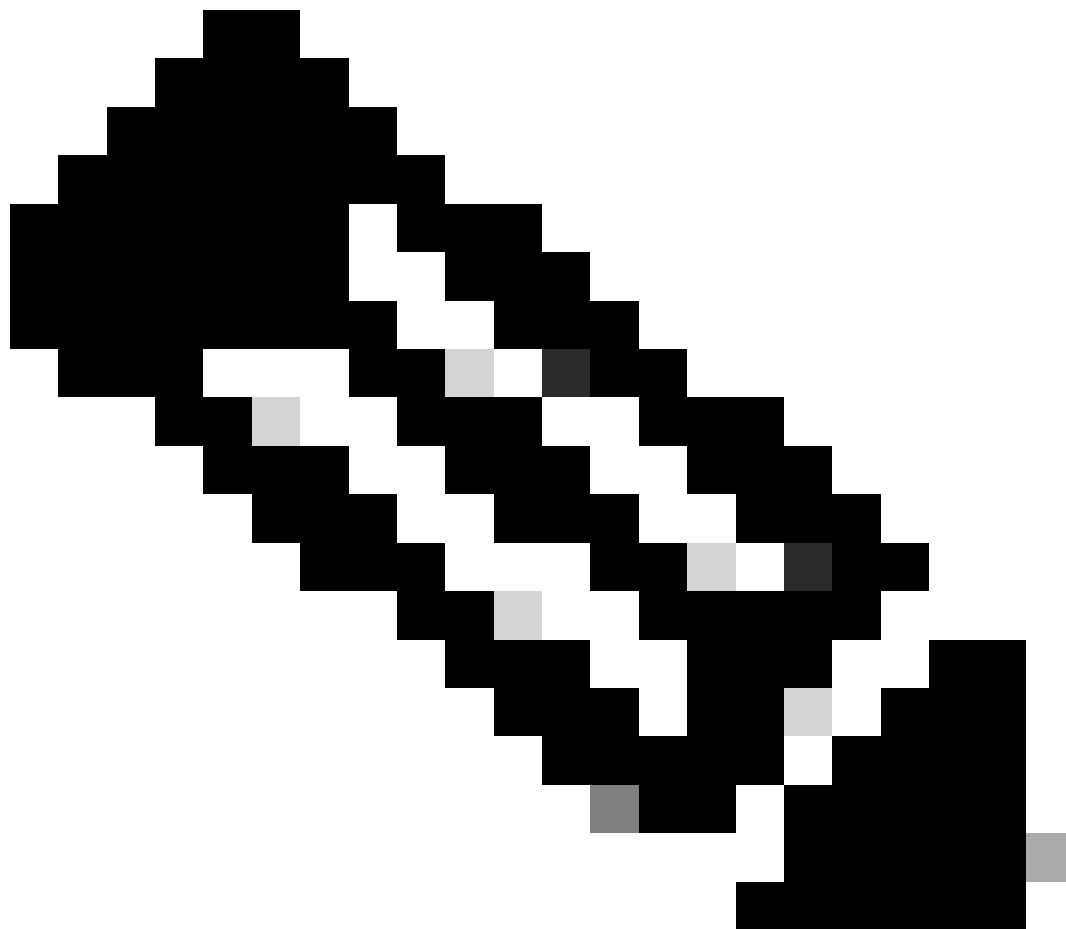
```
show crypto ipsec sa | in current outbound
```

```
current outbound spi:
```

```
0x6D1845C9
```

```
(1830307273)
```

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



注：上記の出力で、出力に転送されるパケットは、現在の発信SA SPIを持つESPパケットです。より詳細なFED転送決定分析を行うには、同じコマンドのdetailバリエーションを使用します。例：show plat hardware fed switch 1 forward last detail を使用できます。



注:PDデータプレーンのデバッグは、TACの支援がある場合にのみ有効にする必要があります。これらは、問題が通常のCLI/デバッグによって特定できない場合にエンジニアリング部門が必要とする、非常に低レベルのトレースです。

<#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のデバッグ

<#root>

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

関連情報

- [Catalyst 9300スイッチでのIPsecの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。