Configurer IPsec sur les commutateurs de la gamme Catalyst 9000X

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Terminologie
- Configurer
  - Diagramme du réseau
  - Installer la licence HSEC
  - Protection du tunnel SVTI
- Vérifier
  - Tunnel IPsec
  - Plan de contrôle Cisco IOS
  - Plan de contrôle PD
- Dépannage
  - Cisco IOS
  - Plan de contrôle PD
  - Plan de données PD
  - Packet-Tracer de plan de données
  - Débogage du plan de données PD
- Informations connexes

Introduction

Ce document décrit comment vérifier la fonctionnalité IPsec (Internet Protocol Security) sur les commutateurs Catalyst 9300X.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IPsec

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C9300X
- C9400X
- Cisco IOS® XE 17.6.4 et versions ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Depuis la version 17.5.1 de Cisco IOS® XE, les commutateurs de la gamme Catalyst 9300-X prennent en charge IPsec. IPsec offre des niveaux élevés de sécurité grâce au chiffrement et à l'authentification, ainsi qu'une protection des données contre les accès non autorisés. L'implémentation IPsec sur le C9300X fournit des tunnels sécurisés entre deux homologues à l'aide de la configuration sVTI (Static Virtual Tunnel Interface).

La prise en charge IPsec sur les commutateurs de la gamme Catalyst 9400X a été introduite dans Cisco IOS® XE 17.10.1.

Terminologie

IOSd	Démon Cisco IOS	Il s'agit du démon Cisco IOS qui s'exécute sur le noyau Linux. Il est exécuté en tant que processus logiciel dans le noyau.IOSdtraite les commandes et les protocoles CLI qui créent l'état et la configuration.
PD	Dépendant De La Plateforme	Données et commandes spécifiques à la plate-forme sur laquelle elles sont exécutées
IPsec	Sécurité du protocole Internet	Suite de protocoles réseau sécurisés qui authentifie et crypte des paquets de données afin de fournir une communication chiffrée sécurisée entre deux ordinateurs sur un réseau à protocole Internet.
SVTI	Interface de tunnel virtuel statique	Une interface virtuelle configurée de manière statique à laquelle vous pouvez appliquer des fonctions de sécurité
SA	association de sécurité	Une association de sécurité est une relation entre deux entités ou plus qui décrit la manière dont les entités utilisent les services de sécurité pour communiquer de manière sécurisée
NOURRIR	Pilote du moteur de transfert	Composant de commutateur responsable de la programmation matérielle de l'ASIC UADP

Configurer

Diagramme du réseau

Pour les besoins de cet exemple, les Catalyst 9300X et ASR1001-X fonctionnent comme des homologues IPsec avec des interfaces de tunnel virtuel IPsec.



Installer la licence HSEC

Activez la fonctionnalité IPsec sur la plate-forme Catalyst 9300X. Deux licences sont requises : Licence HSEC (C9000-HSEC) et DNA-Advantage. Cette configuration est différente des autres plates-formes de routage basées sur Cisco IOS XE qui prennent en charge IPsec, où une licence HSEC est uniquement nécessaire pour augmenter le débit de cryptage autorisé. Sur la plate-forme Catalyst 9300X, le mode tunnel et la CLI de protection de tunnel sont bloqués si aucune licence HSEC n'est installée :

<#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
```

Installez la licence HSEC lorsque le commutateur est connecté à Cisco License Central ou CSLU à l'aide de 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

Vérifiez que la licence HSEC est correctement installée :

<#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

Activez IPsec comme mode de tunnel sur l'interface de tunnel :

<#root>

C9300X(config)#

interface tunnel1

C9300X(config-if)#

tunnel mode ipsec ipv4

C9300X(config-if)#

end

Une fois IPsec activé, la licence HSEC devient EN COURS D'UTILISATION

<#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
```

Protection du tunnel SVTI

La configuration IPsec sur le C9300X utilise la configuration IPsec Cisco IOS XE standard. Il s'agit d'une configuration SVTI simple utilisant les Smart Defaults IKEv2, où nous utilisons la stratégie IKEv2 par défaut, la proposition IKEv2, la transformation IPsec et le profil IPsec pour IKEv2.

Configuration 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
```

Remarque : Comme Catalyst 9300X est essentiellement un commutateur de couche d'accès, le routage ip doit être explicitement activé pour que les fonctionnalités basées sur le routage, telles que VTI, fonctionnent.

Configuration des homologues

<#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
```

Pour une discussion plus détaillée des différentes constructions de configuration IKEv2 et IPsec, veuillez consulter le Guide de configuration IPsec C9300X.

Vérifier

Tunnel IPsec

L'implémentation IPsec sur la plate-forme C9300X est architecturalement différente de celle sur les plates-formes de routage (ASR1000, ISR4000, Catalyst 8200/8300, etc.), où le traitement de la fonctionnalité IPsec est implémenté dans le microcode QFP (Quantum Flow Processor).

L'architecture de transfert C9300X est basée sur l'ASIC UADP, de sorte que la plupart de la mise en oeuvre FIA de la fonctionnalité QFP ne s'applique pas ici.

Voici quelques-unes des principales différences :

- show crypto ipsec sa peer x.x.x.x platform n'affiche pas les informations de programmation de la plate-forme du FMAN jusqu'au QFP.
- Packet-trace ne fonctionne pas non plus (plus sur ce point ci-dessous).
- L'ASIC UADP ne prend pas en charge la classification du trafic de chiffrement, donc show crypto ruleset platform ne s'applique pas

Plan de contrôle Cisco IOS

La vérification du plan de contrôle IPsec est exactement la même que celle des plates-formes de routage, voir . Pour afficher l'association de sécurité IPsec installée dans Cisco IOS :

<#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:
```

Notez flow_id dans la sortie, cela doit correspondre à l'id de flux installé dans le plan de transfert.

Plan de contrôle PD

Statistiques entre Cisco IOS et le plan de contrôle PD

<#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
```

Table d'objets 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
```

entrée 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
        ---------------------------------------
```

Informations de flux 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
```

Dépannage

Cisco IOS

Les commandes debug et show suivantes sont généralement collectées :

<#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
```

Plan de contrôle PD

Pour vérifier les opérations du plan de contrôle PD, suivez les étapes de vérification indiquées précédemment. Pour déboguer tout problème lié au plan de contrôle PD, activez les débogages du plan de contrôle PD :

1. Augmentez le niveau de journalisation btrace à verbeux :

```
<#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. Activer le débogage conditionnel du plan de contrôle 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. Collectez la sortie de débogage de la sortie 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
```

Plan de données PD

Vérifier les statistiques du tunnel IPsec du plan de données, y compris les abandons IPsec courants tels que les échecs HMAC ou de relecture

<#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
```



Remarque : l'id de flux correspond à l'id de flux dans la sortie show crypto ipsec sa. Des statistiques de flux individuelles peuvent également être obtenues avec la commande show platform software fed switch active ipsec counters sa <sa_id> où sa_id l'index SA dans la sortie précédente.

Packet-Tracer de plan de données

Le comportement de Packet-Tracer sur la plate-forme UADP ASIC est très différent de celui du système basé sur QFP. Il peut être activé avec un déclencheur manuel ou un déclencheur basé sur PCAP. Voici un exemple d'utilisation d'un déclencheur basé sur PCAP (EPC).

1. Activez EPC et lancez la capture :

<#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. Exécutez le reste et arrêtez la capture :

<#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. Exporter la capture dans la mémoire 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. Exécutez 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

Remarque : dans le résultat précédent, le paquet transféré en sortie est le paquet ESP avec le SA SPI sortant actuel. Pour une analyse plus détaillée de la décision de transmission FED, la variante detail de la même commande. Exemple : show plate hardware fed switch 1 forward last detail peut être utilisé.

Ceci est un exemple du traitement de décapsulation de paquet IPsec entrant après que le paquet a été déchiffré par le module de chiffrement. Remarque : dans le chemin de transfert d'entrée, après le déchiffrement, le paquet est redistribué vers l'UADP en tant que paquet encapsulé IPnIP.

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

Débogage du plan de données PD



Remarque : Le débogage du plan de données PD ne doit être activé qu'avec l'aide du TAC. Il s'agit de traces de très bas niveau dont l'ingénierie a besoin si le problème ne peut pas être identifié via des CLI/débogages normaux.

<#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

Débogages SHIM PD IPsec

<#root>

debug platform software ipsec info

debug platform software ipsec error

debug platform software ipsec verbose

```
debug platform software ipsec all
```

Informations connexes

- Configurer IPsec sur les commutateurs Catalyst 9300
- Configurer IPsec sur les commutateurs Catalyst 9400
- Cisco IOS XE 17.12.1 pour la commutation Catalyst

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.