

Konfigurieren von IPsec auf Catalyst Switches der Serie 9000X

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Terminologie](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Installieren der HSEC-Lizenz](#)

[SVTI-Tunnelschutz](#)

[Überprüfung](#)

[IPsec-Tunnel](#)

[IOSd-Kontrollebene](#)

[PD-Kontrollebene](#)

[Fehlerbehebung](#)

[IOSd](#)

[PD-Kontrollebene](#)

[PD-Datenebene](#)

[Datenflugzeug-Paketverfolgungssystem](#)

[Debuggen von PD-Datenfeldern](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die IPsec-Funktion (Internet Protocol Security) auf Catalyst 9300X-Switches überprüfen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IPsec

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9300X
- C9400X
- Cisco IOS® XE 17.6.4 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ab Cisco IOS® XE 17.5.1 unterstützen Catalyst Switches der Serie 9300-X IPsec. IPsec bietet ein hohes Maß an Sicherheit durch Verschlüsselung und Authentifizierung sowie Schutz von Daten vor unbefugtem Zugriff. Die IPsec-Implementierung auf dem C9300X bietet sichere Tunnel zwischen zwei Peers mithilfe der sVTI-Konfiguration (Static Virtual Tunnel Interface).

Die IPsec-Unterstützung für Switches der Catalyst 9400-X-Serie wurde in Cisco IOS® XE 17.10.1 eingeführt, während die Unterstützung für Catalyst 9500-X für 17.12.1 geplant ist.

Terminologie

IOSd	IOS-Daemon	Dies ist der Cisco IOS-Daemon, der auf dem Linux-Kernel ausgeführt wird. Er wird als Softwareprozess im Kernel ausgeführt. IOSdprozessiert CLI-Befehle und -Protokolle, die Status und Konfiguration aufbauen.
PD	Plattformabhängig	plattformspezifische Daten und Befehle
IPsec	Internetprotokoll-Sicherheit	Eine sichere Netzwerkprotokoll-Suite, die Datenpakete authentifiziert und verschlüsselt, um eine sichere verschlüsselte Kommunikation zwischen zwei Computern über ein Internetprotokoll-Netzwerk bereitzustellen.
sVTI	Statische virtuelle Tunnelschnittstelle	Eine statisch konfigurierte virtuelle Schnittstelle, auf die Sie Sicherheitsfunktionen anwenden können
SA	Sicherheitszuordnung	Ein SA ist eine Beziehung zwischen zwei oder mehr Einheiten, die beschreibt, wie die Einheiten Sicherheitsdienste nutzen, um sicher zu kommunizieren

FED	Forwarding-Engine-Treiber	Die Switch-Komponente, die für die Hardwareprogrammierung des UADP ASIC verantwortlich ist
-----	---------------------------	--

Konfigurieren

Netzwerkdiagramm

Für dieses Beispiel fungieren der Catalyst 9300X und der ASR1001-X als IPsec-Peers mit virtuellen IPsec-Tunnelschnittstellen.



Installieren der HSEC-Lizenz

Aktivieren Sie die IPsec-Funktion auf der Catalyst 9300X-Plattform. Eine HSEC-Lizenz (C9000-HSEC) ist erforderlich. Dies unterscheidet sich von anderen Cisco IOS XE-basierten Routing-Plattformen, die IPsec unterstützen, wobei eine HSEC-Lizenz nur erforderlich ist, um den zulässigen Verschlüsselungsdurchsatz zu erhöhen. Auf der Catalyst 9300X-Plattform werden der Tunnelmodus und die Tunnelschutz-CLI blockiert, wenn keine HSEC-Lizenz installiert ist:

```
<#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
```

Installieren Sie die HSEC-Lizenz, wenn der Switch über Smart Licensing mit CSSM oder CSLU verbunden ist:

```
<#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
```

Überprüfen Sie, ob die HSEC-Lizenz ordnungsgemäß installiert ist:

```
<#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
```

Aktivieren Sie IPsec als Tunnelmodus auf der Tunnelschnittstelle:

```
<#root>
```

```
C9300X(config)#
```

```
int tunnel1
```

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

```
tunnel mode ipsec ipv4
```

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

```
end
```

Sobald IPsec aktiviert ist, wird die HSEC-Lizenz IN USE

```
<#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-Tunnelschutz

Die IPsec-Konfiguration auf dem C9300X verwendet die Cisco IOS XE IPsec-Standardkonfiguration. Hierbei handelt es sich um eine einfache SVTI-Konfiguration mit [IKEv2 Smart Defaults](#), bei der die IKEv2-Standardrichtlinie, das IKEv2-Angebot, die IPsec-Transformation und das IPsec-Profil für IKEv2 verwendet werden.

Konfiguration des 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
```

 Hinweis: Da es sich bei Catalyst 9300X im Wesentlichen um einen Access Layer-Switch handelt, muss IP-Routing explizit aktiviert werden, damit Routing-basierte Funktionen wie VTI funktionieren.

Peer-Konfiguration

<#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
```

Eine ausführlichere Erläuterung der verschiedenen IKEv2- und IPsec-Konfigurationskonstrukte finden Sie im [C9300X IPsec-Konfigurationsleitfaden](#).

Überprüfung

IPsec-Tunnel

Die IPsec-Implementierung auf der C9300X-Plattform unterscheidet sich von der Architektur auf Routing-Plattformen (ASR1000, ISR4000, Catalyst 8200/8300 usw.), bei denen die IPsec-Funktionsverarbeitung im QFP-Mikrocode (Quantum Flow Processor) implementiert ist.

Die C9300X-Weiterleitungsarchitektur basiert auf der UADP-ASIC, sodass die meisten QFP-Funktionen der FIA-Implementierung hier nicht zur Anwendung kommen.

Hier einige der wichtigsten Unterschiede:

- show crypto ipsec sa peer x.x.x.x-Plattform zeigt keine Plattformprogrammierungsinformationen vom FMAN bis zum QFP an.
- Packet-trace funktioniert ebenfalls nicht (mehr dazu weiter unten).
- UADP ASIC unterstützt keine Klassifizierung des Krypto-Datenverkehrs, daher gilt die Plattform für den Krypto-Regelsatz nicht

IOSd-Kontrollebene

Die Verifizierung der IPsec-Kontrollebene entspricht exakt der Verifizierung für die Routing-Plattformen, siehe . So zeigen Sie die in IOSd installierte IPsec-SA an:

```
<#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:

Beachten Sie die flow_id in der Ausgabe. Diese muss mit der auf der Weiterleitungsebene installierten Fluss-ID übereinstimmen.

PD-Kontrollebene

Statistiken zwischen IOSd- und PD-Kontrollebene

<#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-Objekttabelle

<#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-Eintrag

<#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-Flow-Informationen

<#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
```

Fehlerbehebung

IOSd

Diese Befehle debug und show werden in der Regel wie folgt zusammengefasst:

```
<#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-Kontrollebene

Verwenden Sie zur Verifizierung der Bedienung der PD-Kontrollebene die oben aufgeführten Verifizierungsschritte. Aktivieren Sie die Debug-Funktion für die PD-Kontrollebene, um alle mit der PD-Kontrollebene zusammenhängenden Probleme zu beheben:

1. Erhöhen Sie die Protokollierungsebene für "btrace" auf "verbose":

```
<#root>
```

C9300X#

```
set platform software trace forwarding-manager switch active f0 ipsec verbose
```

C9300X#

```
show platform software trace level forwarding-manager switch active f0 | in ipsec
```

```
ipsec
```

```
Verbose
```

2. Aktivieren Sie das bedingte Debuggen der PD-Kontrollebene:

<#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. Sammeln Sie die Debug-Ausgabe von fman_fp btrace:

<#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-Datenebene

Überprüfen der IPsec-Tunnelstatistik des Datenbereichs, einschließlich häufiger IPsec-Drops wie HMAC oder Wiedergabefehler

```
<#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



Hinweis: Die Flow-ID stimmt mit der Flow-ID in der Ausgabe `show crypto ipsec sa` überein. Einzelne Flow-Statistiken können auch mit dem Befehl `show platform software fed switch active ipsec counters sa <sa_id>` abgerufen werden, wobei `sa_id` den SA-Index in der vorherigen Ausgabe darstellt.

Datenflugzeug-Paketverfolgungssystem

Packet-Tracer verhält sich auf der UADP ASIC-Plattform ganz anders als auf dem QFP-basierten System. Sie kann entweder mit einem manuellen oder einem PCAP-basierten Trigger aktiviert werden. Hier ist ein Beispiel für die Verwendung von PCAP (EPC)-basierten Triggern.

1. Aktivieren Sie EPC und fangen Sie an:

```
<#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. Führen Sie den Rest aus und stoppen Sie die Erfassung:

<#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. Exportieren der Erfassung in 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. Ausführen der Paketverfolgung:

<#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
```



```

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#

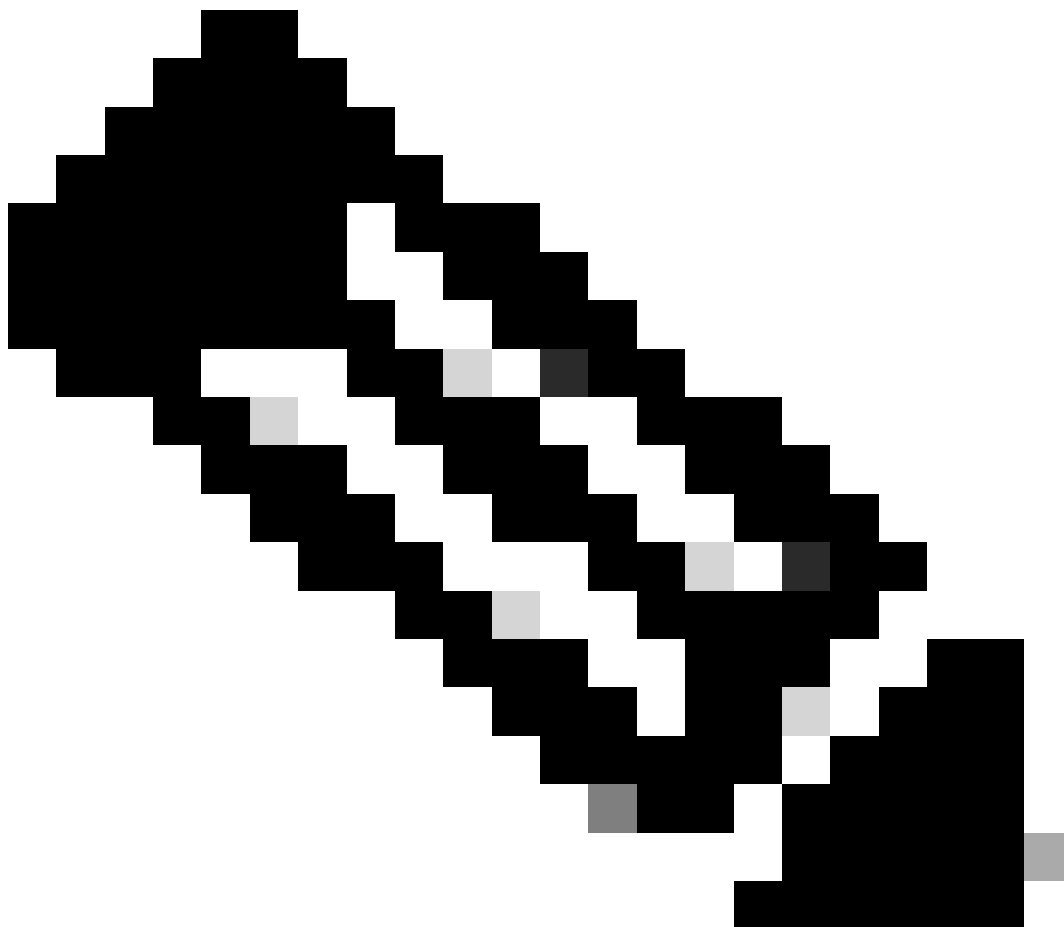
show crypto ipsec sa | in current outbound

current outbound spi:

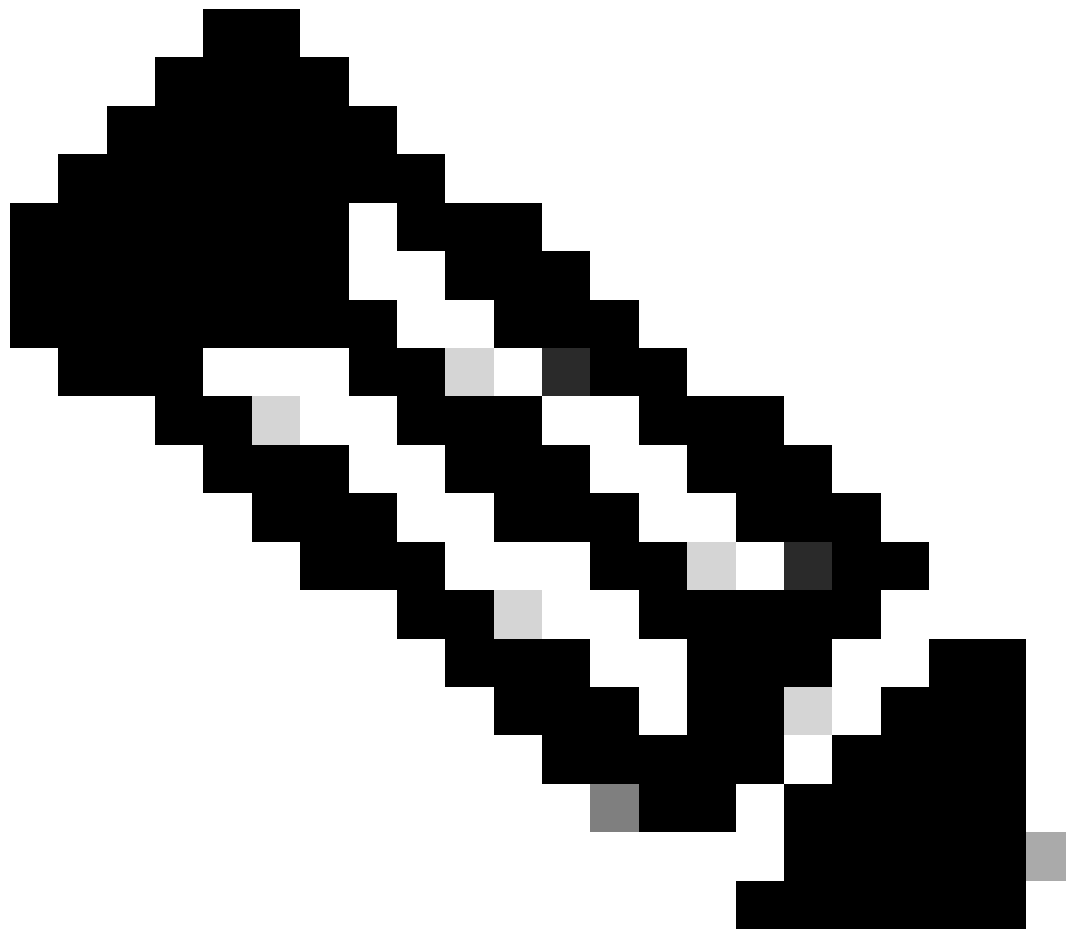
0x6D1845C9

(1830307273)

<-- Matches the load result in packet trace



Hinweis: In der vorherigen Ausgabe ist der Paketweiterleitungsausgang das ESP-Paket mit dem aktuellen ausgehenden SA SPI. Für eine detailliertere FED-Weiterleitungsentscheidungsanalyse die Detailvariante desselben Befehls. Beispiel: show plat hardware fed switch 1 vorwärts letzte details kann verwendet werden.



Hinweis: Das Debuggen von PD-Datenblättern sollte nur mit Unterstützung durch das TAC aktiviert werden. Dies sind Traces auf sehr niedriger Ebene, die vom Engineering benötigt werden, wenn das Problem nicht über normale CLIs/Debugs identifiziert werden kann.

<#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-Debugs

```
<#root>
```

```
debug platform software ipsec info
```

```
debug platform software ipsec error
```

```
debug platform software ipsec verbose
```

```
debug platform software ipsec all
```

Zugehörige Informationen

- [Konfigurieren von IPsec auf Catalyst Switches der Serie 9300](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.