# Probleemoplossing voor IPsec Anti-Replay-controles

## Inhoud



## Inleiding

Dit document beschrijft een probleem dat te maken heeft met IPsec-beveiliging (Internet Protocol Security), tekortkomingen in de controle en hoe u problemen kunt oplossen met mogelijke oplossingen.

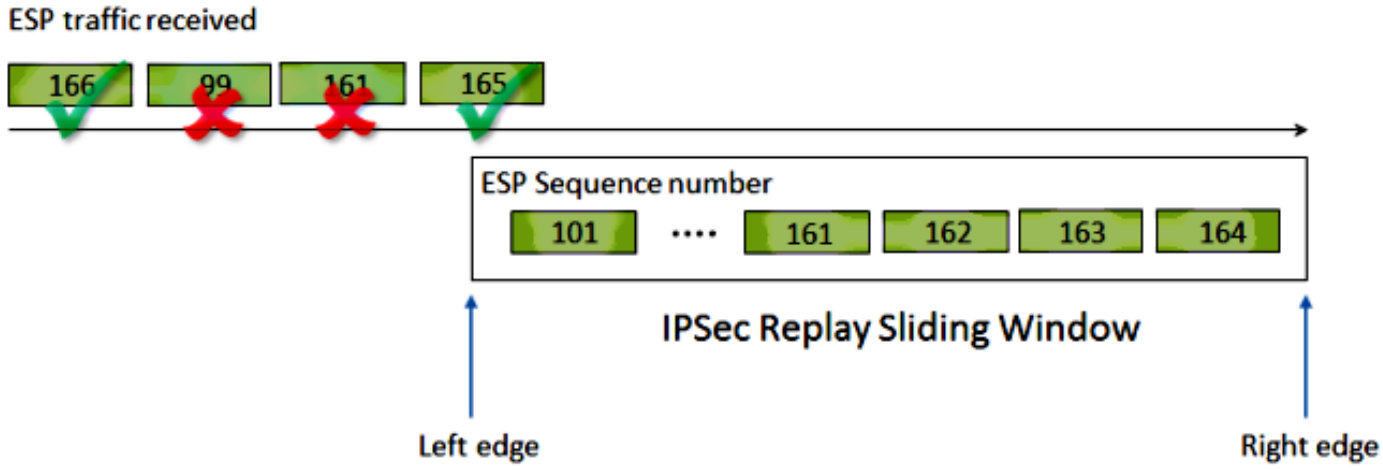
## Achtergrondinformatie

### Een overzicht van terugspeelaanvallen

Een replay-aanval is een vorm van netwerkaanval waarbij geldige data-transmissie op malicieuze of frauduleuze wijze wordt vastgelegd en later wordt herhaald. Het is een poging om de veiligheid te ondermijnen door iemand die rechtmatige communicatie registreert en deze herhaalt om zich te imiteren tot een geldige gebruiker en de legitieme connecties te ontwrichten of er een negatieve impact op te geven.

### IPsec Replay Control-bescherming

Een sequentienummer dat automatisch wordt verhoogd wordt aan elk versleuteld pakket door IPsec toegewezen om bescherming tegen terugspelen tegen een aanvaller te bieden. Het ontvangende IPsec-eindpunt houdt bij welke pakketten het al heeft verwerkt wanneer het deze getallen en een schuivend venster met aanvaardbare sequentienummers gebruikt. De standaard anti-replay venstergrootte in de Cisco IOS® implementatie is 64 pakketten, zoals getoond in deze afbeelding:




Wanneer een IPsec-tunneleindpunt anti-replay beveiliging heeft ingeschakeld, wordt het inkomende IPsec-verkeer als volgt verwerkt:

- Als het sequentienummer binnen het venster valt en niet eerder is ontvangen, is de integriteit van het pakket gecontroleerd. Als het pakket de controle van de integriteit overgaat, wordt het aanvaard en de router merkt op dat dit volgnummer is ontvangen. Bijvoorbeeld, een pakket met het Encapsulating Security Payload (ESP) volgnummer 162.
- Als het sequentienummer binnen het venster valt maar eerder ontvangen is, wordt het pakje ingetrokken. Dit gedupliceerde pakket wordt weggegooid en de druppel wordt in de terugspeelteller opgenomen.
- Als het sequentienummer groter is dan het hoogste sequentienummer in het venster, wordt de integriteit van het pakket gecontroleerd. Als het pakket de controle op de integriteit passeert, wordt het schuifvenster naar rechts verplaatst. Als bijvoorbeeld een geldig pakket met een volgnummer van 189 wordt ontvangen, is de nieuwe rechterrand van het venster ingesteld op 189 en de linkerrand is 125 (189-64 [venstergrootte]).
- Als het sequentienummer lager is dan de linkerrand, wordt het pakje ingetrokken en in de terugspeelteller opgenomen. Dit wordt beschouwd als een out-of-order pakje.

In de gevallen waar een fout bij de terugspeelcontrole optreedt en het pakje wordt ingetrokken, genereert de router een gelijkaardig slogbericht:

```
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle n, src_addr x.x.x.x,
dest_addr y.y.y.y, SPI 0xzzzzzzzz
```

**Opmerking:** De herspeeldetectie is gebaseerd op de aanname dat de IPsec Security Association (SA) tussen slechts twee peers bestaat. Group Encrypted Transport VPN (GETVPN) gebruikt één IPsec SA tussen vele peers. Als resultaat hiervan gebruikt GETVPN een totaal ander anti-replay controle mechanisme dat Time-Based Anti-Replay defect heet. Dit document heeft alleen betrekking op contra-gebaseerde anti-replay voor IPsec-tunnels van punt tot punt.

**Opmerking:** Anti-replay bescherming is een belangrijke veiligheidsservice die het IPsec-protocol biedt. IPsec anti-replay-uitgeschakeld heeft gevolgen voor de beveiliging en moet uitgevoerd worden met discretie.

# Problemen die een terugspeeldaling van IPsec kunnen veroorzaken

Zoals eerder beschreven, is het doel van terugspeelcontroles om tegen kwaadwillige herhalingen van pakketten te beschermen. Er zijn echter enkele scenario's waarbij een mislukte replay-controle mogelijk niet te wijten is aan een kwaadaardige reden:

- De fout kan resulteren uit een voldoende pakje dat in het netwerkpad tussen de eindpunten van de tunnel opnieuw wordt geordend. Dit kan waarschijnlijk voorkomen als er meerdere netwerkpaden tussen de peers zijn.
- De fout kan worden veroorzaakt door ongelijke paden voor pakketverwerking binnen Cisco IOS. Bijvoorbeeld, gefragmenteerde IPsec pakketten die IP reassembleren vóór decryptie zouden genoeg vertraagd kunnen zijn, dat zij buiten het terugspeelvenster vallen tegen de tijd dat zij worden verwerkt.
- De fout kan veroorzaakt zijn door QoS (Quality of Service) dat ingeschakeld is op het verzenden van IPsec-eindpunt of in het netwerkpad. Met de Cisco IOS-implementatie komt IPsec-encryptie voor vóór QoS in de egress-richting. Bepaalde QoS-functies, zoals LLQ (Low Latency Queueing), kunnen ervoor zorgen dat de levering van IPsec-pakketten op den duur is en door het ontvangende eindpunt is gedaald wegens een storing in de terugspeelcontrole.
- Een probleem met de netwerkconfiguratie/het operationele probleem kan pakketten dupliceren terwijl ze het netwerk doorvoeren.
- Een aanvaller (man-in-het-midden) kan het ESP-verkeer vertragen, laten vallen en dupliceren.

# Terugspelen van IPsec-probleemoplossing

De sleutel tot het oplossen van IPsec replay drups is om te identificeren welke pakketten wegens het opnieuw afspelen worden gedropt, en te gebruiken pakketheken om te bepalen of deze pakketten inderdaad worden weergegeven of pakketten die op de ontvangende router buiten het replay venster zijn gearriveerd. Om de gedropt pakketten correct aan te passen aan wat in het snuffelspoor wordt opgenomen, is de eerste stap om de peer en de stroom IPsec te identificeren waartoe de gedropt pakketten behoren en het ESP sequentienummer van het pakket.

## Gebruik Cisco IOS XE Datapath Packet Tracing-functie

Op routerplatforms die Cisco IOS® XE uitvoeren, wordt informatie over de peer zowel als de IPsec Security Parameter Index (SPI) afgedrukt in het Syrische bericht wanneer er een daling optreedt, om problemen met betrekking tot de oplossing te helpen oplossen. Een belangrijk element dat nog ontbreekt, is het ESP-volgnummer. Het ESP sequentienummer wordt gebruikt om een IPsec-pakket binnen een bepaalde IPsec-stroom uniek te identificeren. Zonder het sequentienummer wordt het moeilijk om precies te bepalen welk pakket in een pakketvastlegging wordt gedropt.

De Cisco IOS XE datapath-pakketsporenfunctie kan in deze situatie worden gebruikt wanneer de terugspeelval wordt waargenomen, met dit Syrische bericht:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:060 TS:00000001132883828011
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3, src_addr 10.2.0.200,
dest_addr 10.1.0.100, SPI 0x4c1d1e90
```

Om het ESP sequentienummer voor het ingetrokken pakket te helpen identificeren, vult u deze

stappen met de pakkettraceringsfunctie in:

1. Stel het platform voorwaardelijke debug filter in om verkeer van het peer apparaat aan te passen:

```
debug platform condition ipv4 10.2.0.200/32 ingress
debug platform condition start
```

2. Schakel pakkettracering met de optie **kopiëren** in om de informatie over de pakketheader te kopiëren:

```
debug platform packet enable
debug platform packet-trace packet 64
debug platform packet-trace copy packet input l3 size 100
```

3. Wanneer terugspeelfouten worden gedetecteerd, gebruikt u de buffer van de pakketsporen om het ingesloten pakket te identificeren om terug te spelen, en het ESP sequentienummer kan in het gekopieerde pakket worden gevonden:

```
Router#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi4/0/0 Tu1 CONS Packet Consumed
1 Gi4/0/0 Tu1 CONS Packet Consumed
2 Gi4/0/0 Tu1 CONS Packet Consumed
3 Gi4/0/0 Tu1 CONS Packet Consumed
4 Gi4/0/0 Tu1 CONS Packet Consumed
5 Gi4/0/0 Tu1 CONS Packet Consumed
6     Gi4/0/0          Tu1              DROP   053 (IpsecInput)
7     Gi4/0/0          Tu1              DROP   053 (IpsecInput)
8 Gi4/0/0 Tu1 CONS Packet Consumed
9 Gi4/0/0 Tu1 CONS Packet Consumed
10 Gi4/0/0 Tu1 CONS Packet Consumed
11 Gi4/0/0 Tu1 CONS Packet Consumed
12 Gi4/0/0 Tu1 CONS Packet Consumed
13 Gi4/0/0 Tu1 CONS Packet Consumed
```

De vorige uitvoer toont dat de pakketnummers 6 en 7 worden ingetrokken, zodat ze nu in detail kunnen worden bekeken:

```
Router#show platform packet-trace packet 6
Packet: 6 CBUG ID: 6
Summary
Input : GigabitEthernet4/0/0
Output : Tunnel1
State : DROP 053 (IpsecInput)
Timestamp : 3233497953773
Path Trace
Feature: IPV4
Source : 10.2.0.200
Destination : 10.1.0.100
Protocol : 50 (ESP)
Feature: IPSec
Action : DECRYPT
SA Handle : 3
SPI : 0x4c1d1e90
```

```
Peer Addr : 10.2.0.200
Local Addr: 10.1.0.100
Feature: IPSec
Action : DROP
Sub-code : 019 - CD_IN_ANTI_REPLAY_FAIL
Packet Copy In
45000428 00110000 fc329575 0a0200c8 0a010064 4c1d1e90 00000006 790aa252
e9951cd9 57024433 d97c7cb8 58e0c869 2101f1ef 148c2a12 f309171d 1b7a4771
d8868af7 7bae9967 7d880197 46c6a079 d0143e43 c9024c61 0045280a d57b2f5e
23f06bc3 ab6b6b81 c1b17936 98939509 7aec966e 4dd848d2 60517162 9308ba5d
```

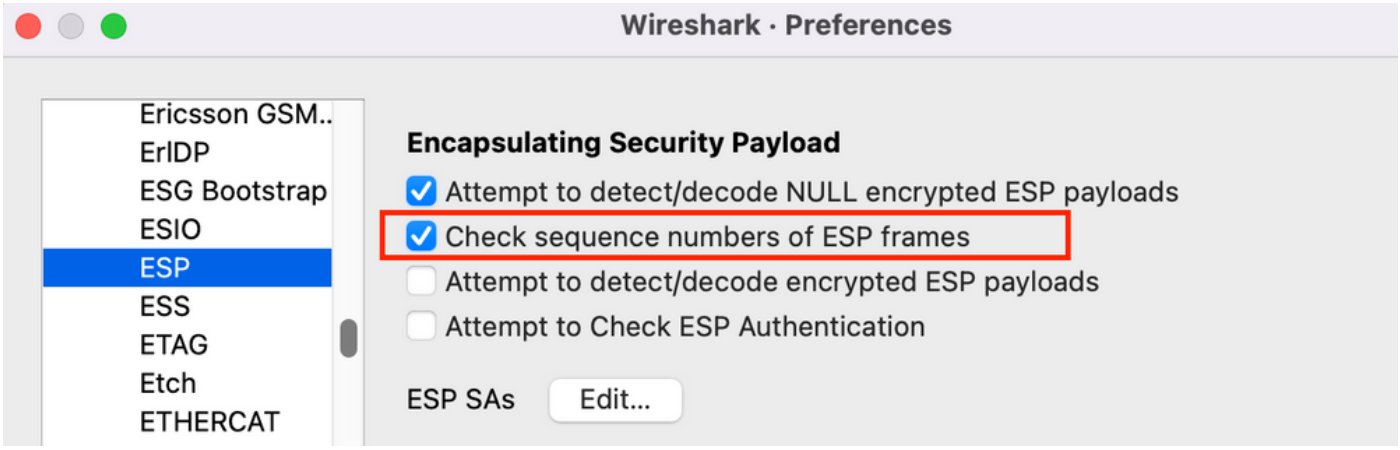
Het ESP-sequentienummer heeft een offset van 24 bytes die van de IP-header (of 4 bytes van de payload-gegevens van het IP-pakket) begint, zoals vet in de vorige uitvoer wordt benadrukt. In dit specifieke voorbeeld, is het ESP opeenvolgingsnummer voor het ingetrokken pakket 0x6.

## Verzamelen pakketvastlegging

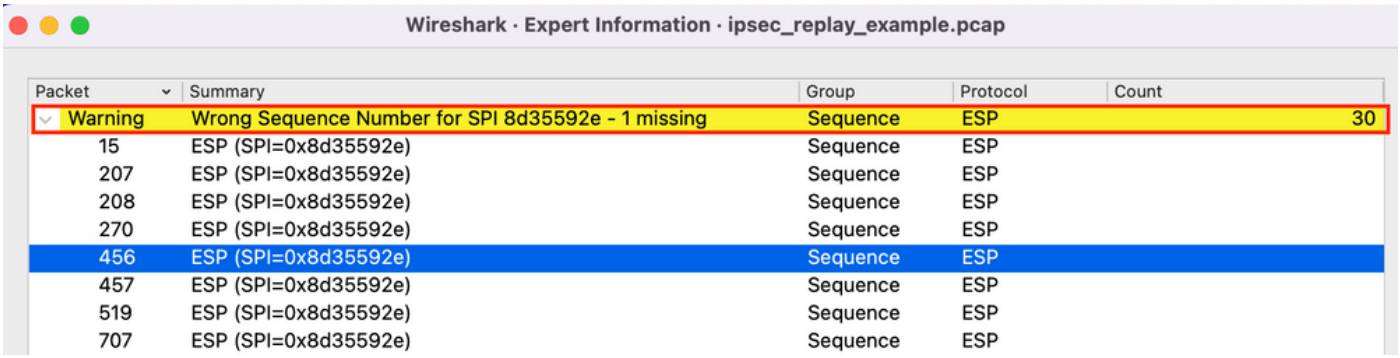
Naast de identificatie van de pakketinformatie voor het pakket dat is ingetrokken omdat de controle is mislukt, moet er tegelijkertijd een pakketvastlegging voor de betrokken IPsec-stroom worden verzameld. Dit helpt bij het onderzoek van het ESP sequentienummer patroon binnen dezelfde IPsec-stroom om de reden voor de terugspeelval te bepalen. Zie Ingesloten pakketvastlegging voor Cisco IOS XE-routers voor meer informatie over het gebruik van de ingesloten pakketvastlegging voor Cisco IOS en Cisco IOS XE-configuratievoorbeeld.

## Gebruik van Wireless-haai sequentienummer analyse

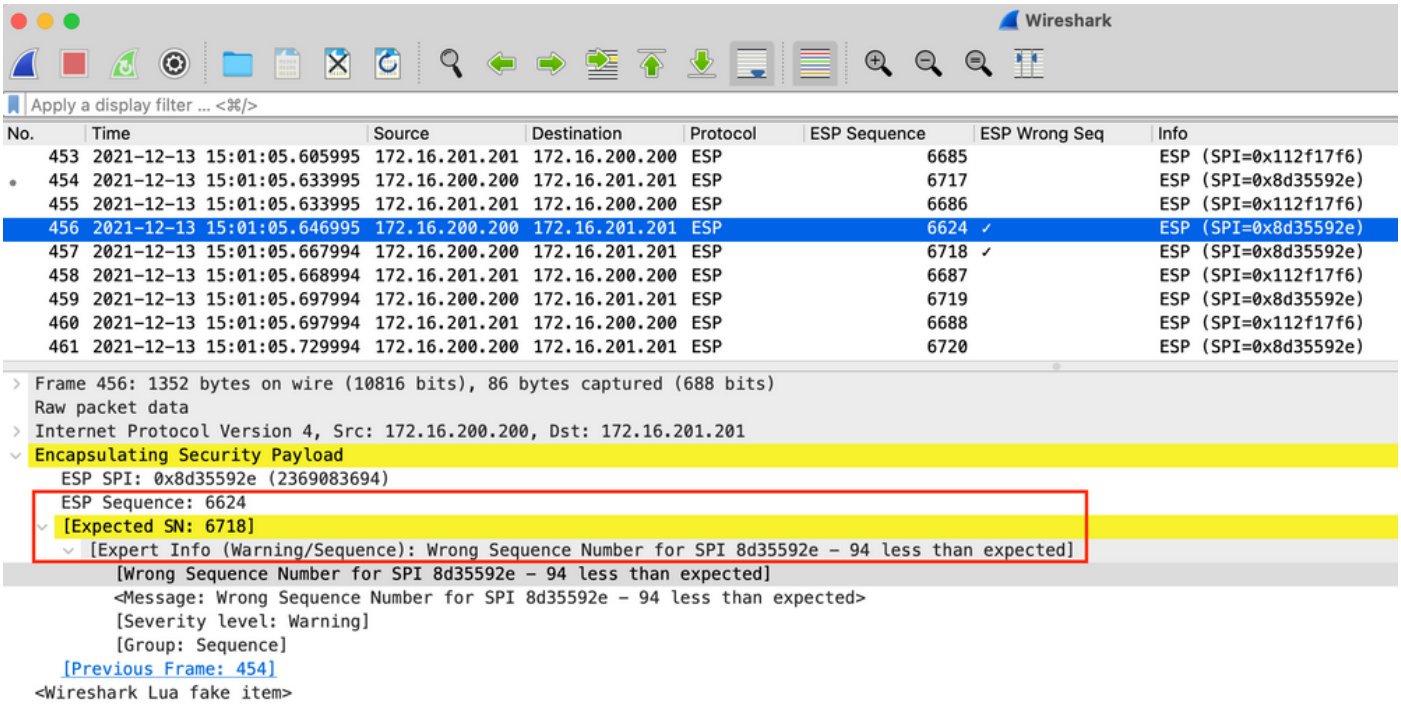
Nadat de pakketvastlegging voor de gecodeerde (ESP) pakketten op de WAN-interface is verzameld, kan Wireshark worden gebruikt om ESP sequentienummer analyse uit te voeren voor elke anomalie van het sequentienummer. Zorg er eerst voor dat de optie Volgnummer controleren is ingeschakeld onder **Voorkeuren > Protocols > ESP** zoals in de afbeelding:



Volgende controle op eventuele ESP-sequentienummer-kwesties bij **analyse >** als volgt informatie van **deskundigen**:




Klik op een van de pakketten met het verkeerde Volgnummer om de volgende aanvullende informatie te krijgen:




# Oplossing

Nadat de peer wordt geïdentificeerd en pakketvastlegging wordt verzameld voor de

terugspeeldruppels, zouden drie mogelijke scenario's de terugspeelfouten kunnen verklaren:

1. Dit is een geldig pakje dat is vertraagd:
   Packet Captures helpen bevestigen als het pakket feitelijk geldig is, en als het probleem onbetekenend is (door problemen met netwerkvertraging of transmissiepad) of een grondiger probleemoplossing vereist. De opname toont bijvoorbeeld een pakje met een volgnummer van X dat uit bestelling komt en de grootte van het terugspeelvenster is op dit moment ingesteld op 64. Als een geldig pakket met volgnummer (X + 64) arriveert vóór pakje X, wordt het venster naar rechts verschoven en wordt pakket X ingetrokken vanwege een storing.

   In dergelijke scenario's is het mogelijk om de grootte van het terugspeelvenster te vergroten of de terugspeelcontrole uit te schakelen om ervoor te zorgen dat dergelijke vertragingen als acceptabel worden beschouwd en dat de legitieme pakketten niet worden weggegooid. Standaard is de grootte van het terugspeelvenster tamelijk klein (venstergrootte van 64). Als u de omvang verhoogt, verhoogt dit het risico op een aanval niet enorm. Raadpleeg voor informatie over het configureren van een IPsec Anti-Replay-venster de manier waarop u IPsec Anti-Replay-venster kunt configureren: Document uitvouwen en uitschakelen.

   **Tip:** Als het terugspeelvenster is uitgeschakeld of gewijzigd in het IPSec-profiel dat op een Virtual Tunnel Interface (VTI) wordt gebruikt, worden de wijzigingen niet uitgevoerd totdat het beveiligingsprofiel is verwijderd en opnieuw wordt toegepast of de tunnelinterface is gereset. Dit is verwacht gedrag omdat IPsec-profielen een sjabloon zijn die wordt gebruikt om een tunnelprofielkaart te maken wanneer de tunnelinterface wordt verhoogd. Als de interface al is geactiveerd, hebben wijzigingen in het profiel geen invloed op de tunnel totdat de interface is hersteld.**Opmerking:** De vroege modellen van Aggregation Services Router (ASR) 1000 (zoals de ASR1000 met ESP5, ESP10, ESP20 en ESP40, samen met de ASR1001) hebben geen venstergrootte van 1024 ondersteund, ook al heeft de CLI die configuratie toegestaan. Als resultaat hiervan is de venstergrootte die in de **show crypto ipsec als** opdrachtoutput wordt gemeld wellicht niet correct. Gebruik de **show crypto ipsec als peer-ip-adresplatform** opdracht om de hardware anti-replay venstergrootte te controleren. De standaardvenstergrootte is 64 pakketten op alle platforms. Raadpleeg voor meer informatie Cisco bug-ID CSCso45946. De latere Cisco IOS XE-routingplatforms (zoals de ASR1K met ESP100 en ESP200, de ASR1001-X en ASR1002-X, geïntegreerde services router (ISR 4) Routers, en Catalyst 8000 Series routers) ondersteunen een venstergrootte van 1024 pakketten in versies 15.2(2)S en later.
2. Dit is het gevolg van de QoS-configuratie op het verzendendpoints:
   Deze situatie vereist een zorgvuldig onderzoek en het afstemmen van een aantal QoS om de aandoening te verzachten. Voor een grondiger beschrijving van dit onderwerp en een mogelijke oplossing, raadpleeg de Anti-Replay Aandacht in een spraak- en video-enabled IPSec VPN (V3PN) artikel.

3. Dit is een tweevoudig pakket dat eerder is ontvangen:
   Als dit zich voordoet, kunnen twee of meer pakketten met hetzelfde ESP-sequentienummer binnen dezelfde IPsec-stroom worden waargenomen bij de pakketvastlegging. In dit geval wordt de pakketdaling verwacht wanneer de IPsec-bescherming voor herafspelen werkt zoals bedoeld om herhalingsaanvallen in het netwerk te voorkomen en het formulier is slechts informatie. Als deze conditie aanhoudt moet deze onderzocht worden als een

potentiele veiligheidsbedreiging.

**Opmerking:** Controle terugspelen mislukkingen worden slechts gezien wanneer een authenticatiealgoritme in de IPsec transformatie set wordt geactiveerd. Een andere manier om deze foutmelding te onderdrukken is om alleen verificatie uit te schakelen en encryptie uit te voeren; dit wordt echter sterk ontmoedigd door de veiligheidsimplicaties van gehandicapte authenticatie .

# Aanvullende informatie

## Probleemoplossing voor herspelen van fouten op oudere routers met Cisco IOS klassieke netwerkmodule

De terugspeeldruppels van IPsec op de oudere ISR G2 Series routers die Cisco IOS gebruiken zijn anders dan routers die Cisco IOS XE gebruiken, zoals hier wordt getoond:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=529, sequence number=13
```

Merk op dat de berichtoutput noch het peer IP adres noch de SPI informatie verstrekt. Om een oplossing voor dit platform te vinden, gebruikt u de "conn-id" in de foutmelding. Identificeer de "conn-id" in de foutmelding en kijk ernaar in de **show crypto ipsec als** output, omdat replay een per-SA controle is (in tegenstelling tot een per-peer). Het Syrische bericht geeft ook het ESP sequentienummer, dat uniek kan helpen om het gedemonteerde pakket in de pakketvastlegging te identificeren.

**Opmerking:** Met verschillende versies van code is "conn-id" ofwel de **conn id** of **flow_id** voor de inkomende SA.

Dit wordt hier geïllustreerd:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=529, sequence number=13

Router#show crypto ipsec sa | in peer|conn id
current_peer 10.2.0.200 port 500
conn id: 529, flow_id: SW:529, sibling_flags 80000046, crypto map: Tunnel0-head-0
conn id: 530, flow_id: SW:530, sibling_flags 80000046, crypto map: Tunnel0-head-0
Router#

Router#show crypto ipsec sa peer 10.2.0.200 detail

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.1.0.100

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 10.2.0.200 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
#pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 21
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 10.1.0.100, remote crypto endpt.: 10.2.0.200
path mtu 2000, ip mtu 2000, ip mtu idb Serial2/0
current outbound spi: 0x8B087377(2332586871)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xE7EDE943(3891128643)
transform: esp-gcm ,
in use settings ={Tunnel, }
conn id: 529, flow_id: SW:529, sibling_flags 80000046, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4509600/3223)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

<SNIP>
```

Zoals je op deze uitvoer kunt zien, is de terugspeelval vanaf het 10.2.0.200 Peeradres met een inkomende ESP SA SPI van 0xE7EDE943. Van het logbericht zelf kan ook worden opgemerkt dat het ESP sequentienummer voor het ingetrokken pakket 13 is. De combinatie van peer adres, SPI nummer en het ESP sequentienummer kan worden gebruikt om het pakket dat in de pakketvastlegging is gevallen, uniek te identificeren.

> **Opmerking:** Het Cisco IOS SLUG-bericht is snelheidsbeperkt voor het dataplatform dat per minuut daalt. Om een nauwkeurige telling van het nauwkeurige aantal gedropte pakketten te krijgen, gebruik de **show crypto ipsec als detail** opdracht zoals eerder getoond.

## Werk met eerdere Cisco IOS XE-software

Op routers die de eerdere Cisco IOS XE-releases uitvoeren, kan de "REPLAY_FOUT" die in het systeem is gemeld, de eigenlijke IPsec-stroom niet afdrukken met de peer-informatie waar het afgespeeld pakket is gevallen, zoals hier wordt getoond:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread: 095 TS:00000000240306197890
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3
```

Om de juiste IPsec-peer- en stroominformatie te identificeren, gebruikt u de Data Plane (DP) Handle die in het Syrische bericht is afgedrukt als de invoerparameter SA Handle in deze opdracht, om de IPsec-stroominformatie over de Quantum Flow Processor (QFP) te herstellen:

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
```

```
crypto ctx: 0x000000002e03bfff
flags: 0xc000800
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

Een Embedded Event Manager (EEM) script kan ook gebruikt worden om de gegevensverzameling te automatiseren:

```
event manager applet Replay-Error
 event syslog pattern "%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error"
 action 1.0 regexp "([0-9]+)$" "$_syslog_msg" dph
 action 2.0 cli command "enable"
 action 3.0 cli command "show platform hardware qfp active feature ipsec sa $dph |
append bootflash:replay-error.txt"
```

In dit voorbeeld wordt de verzamelde uitvoer opnieuw naar de **flitser** gericht. Om deze uitvoer te zien, gebruikt u de opdracht **meer flitser:replay-error.txt**.

# Gerelateerde informatie

- Spraak en video-enabled IPSec VPN (V3PN) oplossing Referentienetwerk
- Zo configureren u een IPsec-venster met een replay: Uitvouwen en uitschakelen.
- Technische ondersteuning en documentatie – Cisco Systems