

# 排除IPsec反重播檢查故障

## 目錄

---

### [簡介](#)

### [背景資訊](#)

[重放攻擊概述](#)

[IPsec重播檢查保護](#)

### [可能導致IPsec重播丟棄的問題](#)

### [排除IPsec重播丟棄故障](#)

[使用Cisco IOS XE資料路徑資料包跟蹤功能](#)

[收集資料包捕獲](#)

[使用Wireshark序列號分析](#)

### [解決方案](#)

### [其他資訊](#)

[使用Cisco IOS Classic解決舊版路由器上的重播錯誤](#)

[使用早期的Cisco IOS XE軟體](#)

### [相關資訊](#)

---

## 簡介

本文描述與Internet協定安全(IPsec)防重播檢查失敗相關的問題，並提供可能的解決方案。

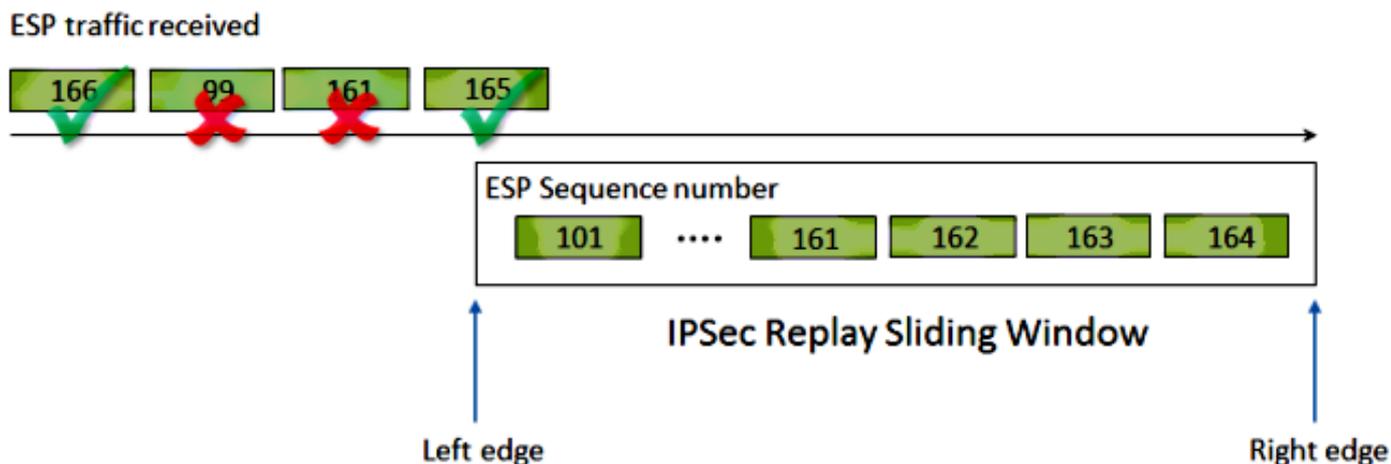
## 背景資訊

### 重放攻擊概述

重放攻擊是一種網路攻擊形式，其中惡意或欺詐性地記錄有效資料傳輸並在以後重複。某些人會記錄合法通訊並重複這些通訊，以便假冒有效使用者，從而中斷合法連線或對其造成負面影響，這是一種試圖破壞安全性的行為。

### IPsec重播檢查保護

IPsec將單調遞增的序列號分配給每個加密資料包，以提供針對攻擊者的反重播保護。接收IPsec端點會跟蹤當它使用這些編號時已處理過哪些資料包，以及可接受序列號的滑動視窗。Cisco IOS®實施中的預設反重播視窗大小為64個資料包，如下圖所示：



當IPsec隧道端點啟用了反重播保護時，傳入的IPsec流量按如下方式處理：

- 如果序列號位於視窗內且之前未收到，則檢查資料包的完整性。如果資料包通過完整性驗證檢查，則它被接受並且路由器標籤已收到此序列號。例如，封裝安全負載(ESP)序列號為162的資料包。
- 如果序列號位於視窗內，但之前已收到該資料包，則丟棄該資料包。這個重複的資料包將被丟棄，而且該丟棄將記錄在重放計數器中。
- 如果序列號大於視窗中的最高序列號，則會檢查資料包的完整性。如果資料包通過完整性驗證檢查，則滑動視窗將移動到右側。例如，如果接收到序列號為189的有效資料包，則視窗的新右邊緣設定為189，左邊緣為125 (  $189 - 64$  [視窗大小] )。
- 如果序列號小於左邊緣，則資料包將被丟棄，並記錄在重放計數器中。這被視為無序封包。

如果發生重播檢查失敗並且資料包被丟棄，路由器將生成類似於以下內容的Syslog消息：

```
%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
```

**注意：**重放檢測基於以下假設：IPsec安全關聯(SA)僅存在於兩個對等體之間。群組加密傳輸VPN(GETVPN)在許多對等點之間使用單個IPsec SA。因此，GETVPN使用一種完全不同的反重播檢查機制，稱為基於時間的反重播失敗。本文僅介紹點對點IPsec通道的基於計數器的反重放。

**注意：**反重播保護是IPsec協定提供的一項重要安全服務。禁用IPsec反重播具有安全影響，必須謹慎執行。

## 可能導致IPsec重播丟棄的問題

如前所述，重放檢查的目的是防止資料包的惡意重複。但是，在某些情況下，失敗的重播檢查可能不是由於惡意原因所致：

- 此錯誤可能是因為在通道端點之間的網路路徑中重新排序的封包數量充足。如果對等體之間存在多個網路路徑，則可能會發生這種情況。
  - 此錯誤可能是由於Cisco IOS內部的不對等封包處理路徑所導致。例如，需要IP重組才能解密的分段IPsec資料包可能會延遲足夠長，以至於在處理這些資料包時，它們已超出重播視窗的範圍。
  - 此錯誤可能是由在傳送IPsec端點上或網路路徑內啟用的服務品質(QoS)所導致。通過Cisco IOS實施，IPsec加密在出口方向的QoS之前進行。某些QoS功能(例如低延遲佇列(LLQ))可能會導致IPsec封包傳遞變得無序並被接收端點由於重新執行檢查失敗而捨棄。
  - 網路配置/運行問題可能會在資料包傳輸網路時重複這些資料包。
- 攻擊者(中間人)可能會延遲、丟棄和複製ESP流量。

## 排除IPsec重播丟棄故障

排除IPsec重播丟棄故障的關鍵是確定哪些資料包由於重播而被丟棄，並使用資料包捕獲來確定這些資料包是否確實是重播資料包或到達重播視窗以外的接收路由器的資料包。為了正確地將丟棄的資料包與監聽器跟蹤中捕獲的資料包相匹配，第一步是確定被丟棄的資料包所屬的對等體和IPsec流以及資料包的ESP序列號。

### 使用Cisco IOS XE資料路徑資料包跟蹤功能

在執行Cisco IOS® XE的路由器平台上，當發生捨棄時，有關對等體的資訊以及IPsec安全引數索引(SPI)會列在Syslog訊息中，以便協助排解反重新執行問題。但是，仍然遺漏的關鍵資訊是ESP序列號。ESP序列號用於唯一標識給定IPsec流中的IPsec資料包。如果沒有序列號，就很難準確識別資料包捕獲中丟棄了哪些資料包。

在此情況下，當觀察到重播丟棄時，可以使用Cisco IOS XE資料路徑資料包跟蹤功能，並顯示以下系統日誌消息：

```
%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
```

為了幫助識別丟棄的資料包的ESP序列號，請使用資料包跟蹤功能完成以下步驟：

1. 設定平台條件調試過濾器，以匹配來自對等裝置的流量：

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

1. 使用copy 選項啟用資料包跟蹤，以複製資料包報頭資訊：

```
debug platform packet enable
debug platform packet-trace packet 64
debug platform packet-trace copy packet input 13 size 100
```

1. 檢測到重放錯誤時，請使用資料包跟蹤緩衝區來標識由於重放而丟棄的資料包，並且可以在複製的資料包中找到ESP序列號：

<#root>

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

先前的輸出顯示第6和第7個封包已遭捨棄，因此現在可詳細檢查它們：

<#root>

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

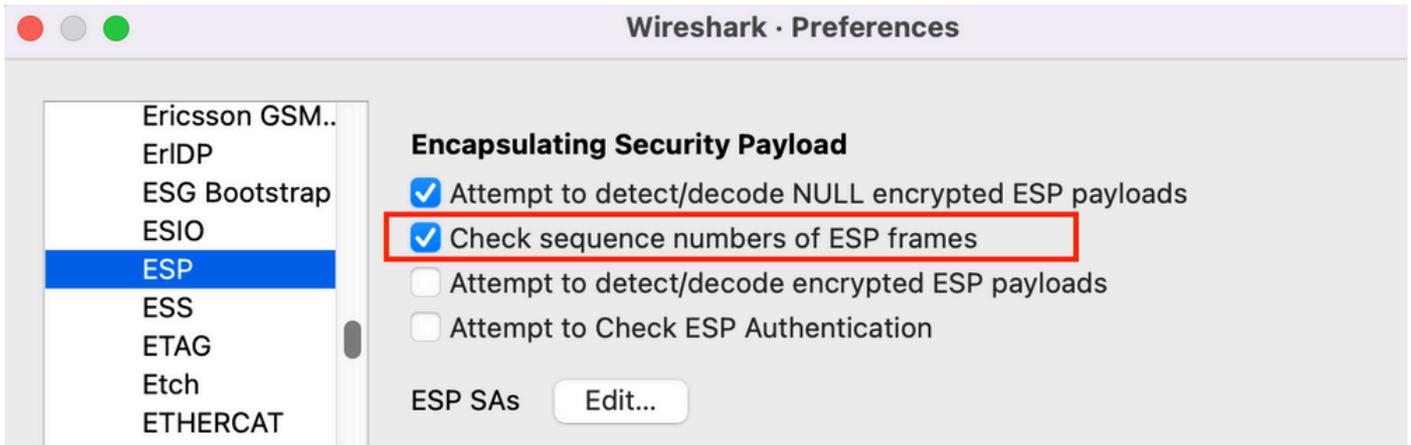
ESP序列號具有從IP報頭開始的24位元組的偏移量（或IP資料包的負載資料的4位元組），如前面的輸出中粗體所示。在此特定示例中，丟棄的資料包的ESP序列號為0x6。

## 收集資料包捕獲

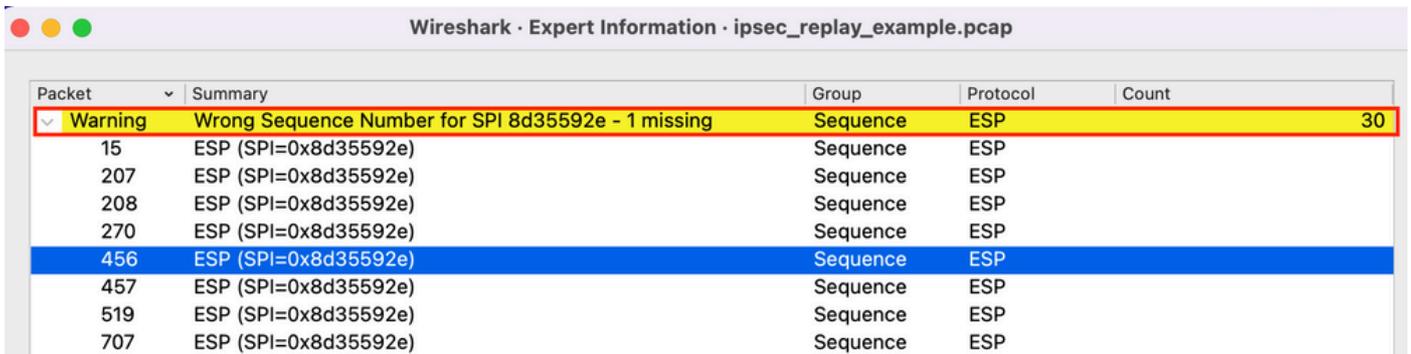
除了標識由於重放檢查失敗而丟棄的資料包的資訊包之外，還需要同時收集有關IPsec流的資料包捕獲。這有助於檢查同一IPsec流中的ESP序列號模式，以幫助確定重播丟棄的原因。有關如何在Cisco IOS XE路由器上使用嵌入式資料包捕獲(EPC)的詳細資訊，請參閱[適用於Cisco IOS和Cisco IOS XE的嵌入式資料包捕獲配置示例](#)。

## 使用Wireshark序列號分析

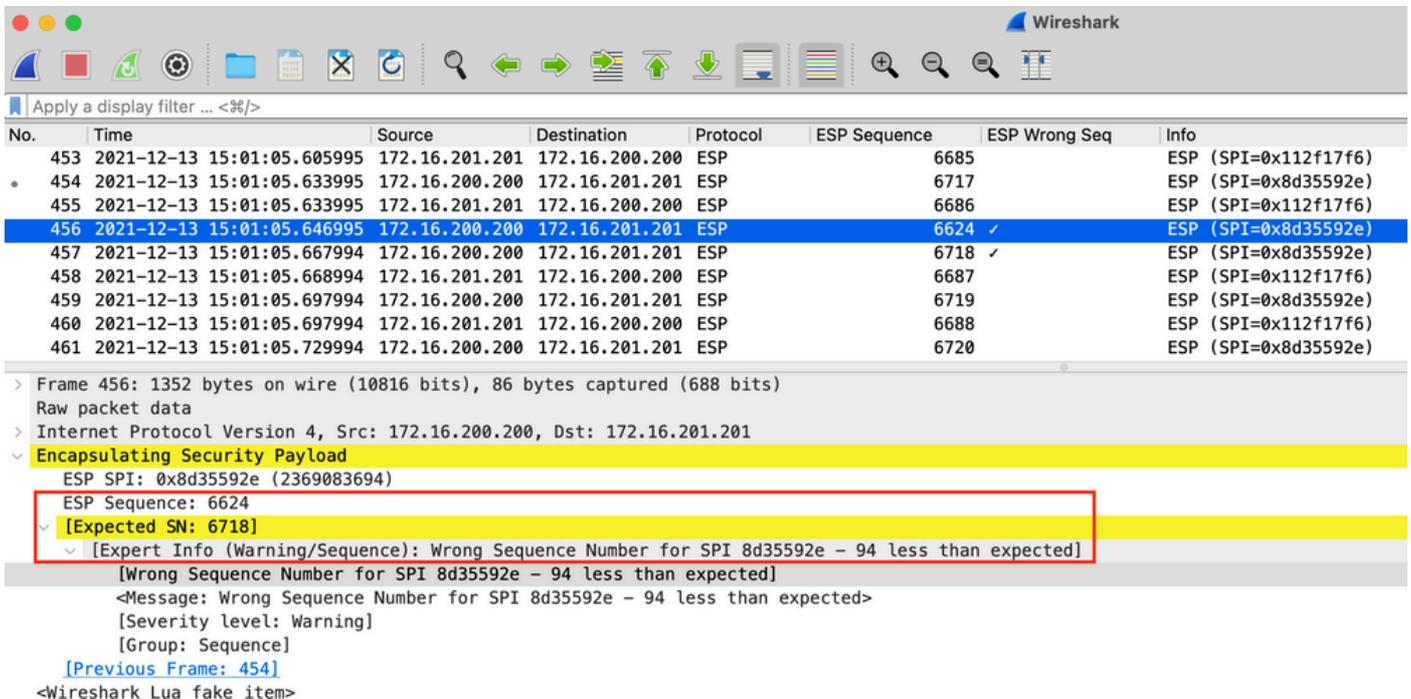
收集WAN介面上加密(ESP)資料包的資料包捕獲後，Wireshark可用於對任何序列號異常執行ESP序列號分析。首先，確保在Preferences > Protocols > ESP下啟用了Sequence Number Check，如下圖所示：



接下來檢查分析>專家資訊下的任何ESP序列號問題，如下所示：



按一下序號錯誤的任何封包可取得其他詳細資訊，如下所示：



## 解決方案

確定對等體並收集重放丟棄的資料包捕獲後，三種可能的情形可以解釋重放失敗：

### 1. 是已延遲的有效封包：

封包擷取有助於確認封包是否實際有效，以及問題是否不重大（由於網路延遲或傳輸路徑問題）或需要更深入的疑難排解。例如，捕獲顯示序列號為X的資料包無序到達，並且重放視窗大小當前設定為64。如果序列號為(X + 64)的有效資料包在資料包X之前到達，則視窗向右移動，然後由於重放失敗而丟棄資料包X。

在這些情況下，可以增加重放視窗的大小或禁用重放檢查以確保這樣的延遲是可接受的，並且合法的資料包不會被丟棄。預設情況下，重放視窗大小相當小（視窗大小為64）。如果增加大小，攻擊的風險不會大幅增加。有關如何配置IPsec反重放視窗的資訊，請參閱[如何配置IPsec反重放視窗：展開和禁用](#)文檔。



提示：如果在虛擬通道介面(VTI)上使用的IPSec配置檔案中禁用或更改了重放視窗，則在刪除並重新應用保護配置檔案或重置通道介面之前，更改不會生效。這是預期行為，因為IPsec配置檔案是一個模板，用於在啟動隧道介面時建立隧道配置檔案對映。如果介面已啟動，則重設介面之前，設定檔的變更不會影響通道。



註：早期聚合服務路由器(ASR)1000型號（例如帶有ESP5、ESP10、ESP20和ESP40以及ASR1001的ASR1000）不支援視窗大小1024，即使CLI允許該配置。因此，show crypto ipsec sa命令輸出中報告的視窗大小可能不正確。使用show crypto ipsec sa peer ip-address platform 命令驗證硬體反重播視窗大小。所有平台上的預設視窗大小為64個資料包。如需更多資訊，請參閱Cisco錯誤ID [CSCso45946](#)。較新版本的Cisco IOS XE路由平台(例如帶有ESP100和ESP200的ASR1K、ASR1001-X和ASR1002-X、整合服務路由器(ISR)4000系列路由器和Catalyst8000系列路由器)在15.2(2)S版及更新版本中支援大小為1024個資料包的視窗。

### 2. 這是因為傳送端點上的QoS配置：

這種情況需要仔細檢查並調整某些QoS以緩解狀況。有關此主題和潛在解決方案的更詳細說明，請參閱[啟用語音和影片的IPSec VPN\(V3PN\)中的防重放注意事項](#)。

### 3. 這是先前收到的重複封包：

如果是這種情況，則可以在資料包捕獲中觀察到同一IPsec流中具有相同ESP序列號的兩個或多個資料包。在這種情況下，丟包是預期的，因為IPsec重播保護旨在防止網路中的重播攻擊，而Syslog只是提供資訊。如果此情況持續出現，則必須將其作為潛在安全威脅進行調查。



注意：只有在IPsec轉換集中啟用身份驗證演算法時，才會出現重播檢查失敗。抑制此錯誤消息的另一種方法是禁用身份驗證並僅執行加密；但是，由於禁用身份驗證的安全影響，強烈建議不要這樣做。

## 其他資訊

使用Cisco IOS Classic解決舊版路由器上的重播錯誤

使用Cisco IOS的舊版ISR G2系列路由器上的IPsec重播丟棄與使用Cisco IOS XE的路由器不同，如下所示：

```
<#root>
```

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

請注意，消息輸出不提供對等IP地址或SPI資訊。若要在此平台上疑難排解，請使用錯誤訊息中的「conn-id」。識別錯誤訊息中的「conn-id」，然後在show crypto ipsec sa輸出中尋找它，因為重新執行是每SA檢查（而不是每對等）。Syslog消息還提供了ESP序列號，這有助於在資料包捕獲中唯一標識丟棄的資料包。

---

 註：對於不同版本的代碼，「conn-id」是入站SA的conn id或flow\_id。

---

以下圖示：

```
<#root>
```

```
%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 (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 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 (rcv) 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>

從該輸出中可以看到，重放丟棄來自具有入站ESP SA SPI 0xE7EDE943的10.2.0.200對等體地址。從日誌消息本身也可看出，丟棄的資料包的ESP序列號為13。對等體地址、SPI號和ESP序列號的組合可用於唯一標識資料包捕獲中丟棄的資料包。

---

 註：對於丟棄到每分鐘一分鐘的資料平面資料包，Cisco IOS系統日誌消息受速率限制。若要取得準確的封包捨棄次數的計數，請使用show crypto ipsec sa detail命令，如前所示。

---

## 使用早期的Cisco IOS XE軟體

在執行舊版Cisco IOS XE的路由器上，系統日誌中報告的「REPLAY\_ERROR」可能不會列印包含丟棄已重放資料包的對等體資訊的實際IPsec流，如下所示：

```
%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
```

若要識別正確的IPsec對等體和流資訊，請使用系統日誌消息中列印的資料平面(DP)控制代碼作為此命令中的輸入引數SA Handle，以便在Quantum流處理器(QFP)上檢索IPsec流資訊：

```
<#root>
```

```
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: 0x00000002e03bfff
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>
```

還可以使用嵌入式事件管理器(EEM)指令碼來自動進行資料收集：

```
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"
```

在本範例中，收集的輸出將重新導向到bootflash。若要看到此輸出，請使用命令more bootflash:replay-error.txt。

## 相關資訊

- [支援語音和影片的IPSec VPN\(V3PN\)解決方案參考網路設計](#)
- [如何配置IPsec Anti-Replay視窗：正在擴展和禁用。](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。