排除IPsec反重播检查故障

目录

简介

背景信息

- 重放攻击概述
- IPsec重播检查保护

可能导致IPsec重播丢弃的问题

排除IPsec重播丢弃故障

- 使用Cisco IOS XE数据路径数据包跟踪功能
- 收集数据包捕获
- 使用Wireshark序列号分析

解决方案

Additional Information

- 使用Cisco IOS Classic对传统路由器上的重播错误进行故障排除
- 使用早期的Cisco IOS XE软件

相关信息

简介

本文档介绍与Internet协议安全(IPsec)防重播检查失败相关的问题，并提供可能的解决方案。

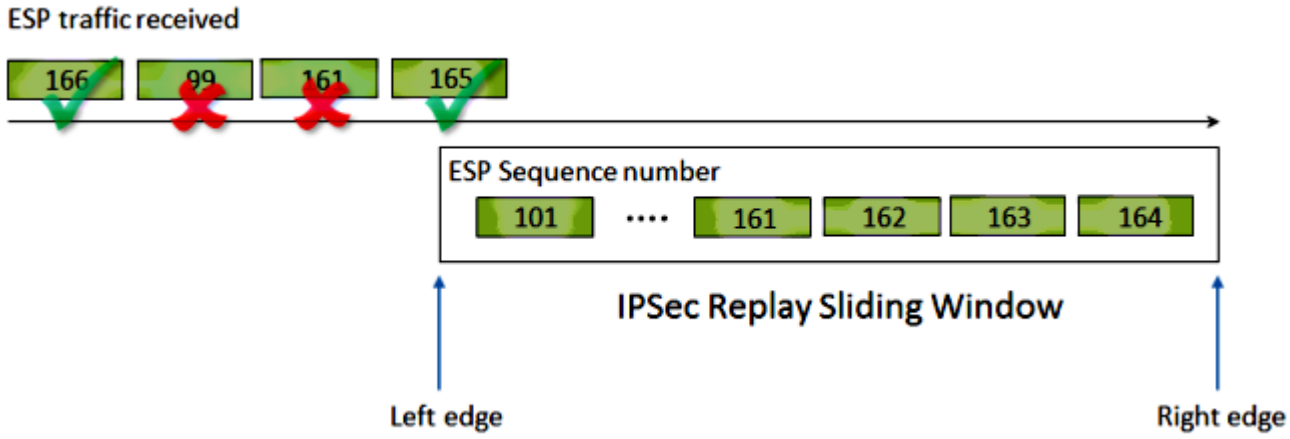
背景信息

重放攻击概述

重播攻击是一种网络攻击形式，其中恶意或欺诈性地记录有效数据传输并在以后重复。有人会记录合法通信并重复这些通信，以假冒有效用户，从而破坏合法连接或对合法连接造成负面影响，试图破坏安全性。

IPsec重播检查保护

IPsec会为每个加密数据包分配单调增加的序列号，以提供针对攻击者的反重播保护。接收方的IPsec端点会跟踪在使用这些编号和带有可接受序列号的滑动窗口时已处理的数据包。Cisco IOS®实施中的默认反重播窗口大小为64个数据包，如下图所示：



当IPsec隧道终端启用反重播保护时，传入的IPsec流量按如下方式处理：

- 如果序列号在窗口内且之前未收到，则检查数据包的完整性。如果数据包通过完整性验证检查，则会接受该数据包，并且路由器会标记已收到该序列号。例如，在前面的图中，封装安全负载(ESP)序列号为162的数据包位于重放窗口中。
- 如果序列号在窗口内，但之前已收到，则丢弃数据包。此重复的数据包将被丢弃，并在重放丢弃计数器中记录丢弃。

- 如果序列号大于窗口中的最高序列号，则检查数据包的完整性。如果数据包通过完整性验证检查，则滑动窗口将移至右侧。例如，如果收到序列号为189的有效数据包，则窗口的新右边设置为189，左边设置为125（189 - 64 [窗口大小]）。
- 如果序列号小于左边缘，则数据包将被丢弃，并记录在重放计数器中。这被视为无序数据包。

如果发生重播检查失败并且数据包被丢弃，路由器将生成类似于以下内容的系统日志消息：

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

注意：重播检测基于以下假设：IPsec安全关联(SA)仅存在于两个对等体之间。组加密传输VPN(GETVPN)在许多对等体之间使用单个IPsec SA。因此，GETVPN使用一种完全不同的反重播检查机制，称为基于时间的反重播失败。本文档仅介绍点对点IPsec隧道的基于计数器的反重放。

注意：反重播保护是IPsec协议提供的一项重要安全服务。禁用IPsec反重播会带来安全隐患，必须谨慎执行。

可能导致IPsec重播丢弃的问题

如前所述，重播检查的目的是防止合法数据包的恶意重复。可能导致失败的重播检查的一些常见条件包括：

- 此错误可能是由数据包在传输期间在隧道终端之间的网络路径中重新排序造成的。如果对等体之间存在多条网络路径，则可能会出现这种情况。

- 此错误可能是由于Cisco IOS内部数据包处理路径不均造成的。例如，需要IP重组才能解密的分段IPsec数据包可以延迟足够长的时间，以至于在处理这些数据包时，它们已超出重放窗口的范围。
- 此错误可能是由在发送IPsec终端上或网络路径内启用的服务质量(QoS)引起的。通过Cisco IOS实施，IPsec加密在出口方向的QoS之前进行。某些QoS功能(例如低延迟队列(LLQ))可能导致IPsec数据包传输因重播检查失败而变得无序并被接收终端丢弃。

- 网络配置/运行问题可能会在数据包通过网络时将其复制。
- 攻击者（中间人）可能会延迟、丢弃和复制ESP流量。

排除IPsec重播丢弃故障

排除IPsec重播丢弃故障的关键是确定哪些数据包因重播而丢弃，并使用数据包捕获来确定这些数据包是否确实是重播数据包或到达重播窗口以外的接收路由器的数据包。为了将丢弃的数据包与嗅探器跟踪中捕获的数据包正确匹配，第一步是标识对等体以及丢弃的数据包所属的IPsec流以及数据包的ESP序列号。

使用Cisco IOS XE数据路径数据包跟踪功能

在运行Cisco IOS® XE软件的路由器平台上，当发生重播丢弃时，系统日志消息中会打印有关对等体以及IPsec安全参数索引(SPI)的信息，以帮助识别被丢弃的数据包所属的对等体和特定隧道。但是，此输出中不显示ESP序列号。ESP序列号用于唯一标识给定IPsec流中的IPsec数据包。如果没有序列号，就很难准确识别数据包捕获中丢弃了哪些数据包。

在这种情况下，如果观察到重放丢弃，可以使用Cisco IOS® XE数据路径数据包跟踪功能，系统日志消息如下：

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:060 TS:00000011132883828011
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3, src_addr 10.2.0.200, dest_addr
```

为了帮助识别丢弃的数据包的ESP序列号，请使用数据包跟踪功能完成以下步骤：

步骤1.设置platform conditional debug 过滤器，以匹配来自对等设备的流量：

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

步骤2.使用copy选项启用数据包跟踪以复制数据包报头信息：

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

步骤3.当检测到重放错误时，请使用packet trace buffer确定由于重放而丢弃的数据包，并且可以在复制的数据包中找到ESP序列号：

```
<#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
```

前面的输出显示丢弃了编号6和7的数据包，因此现在可详细检查它们：

<#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
```

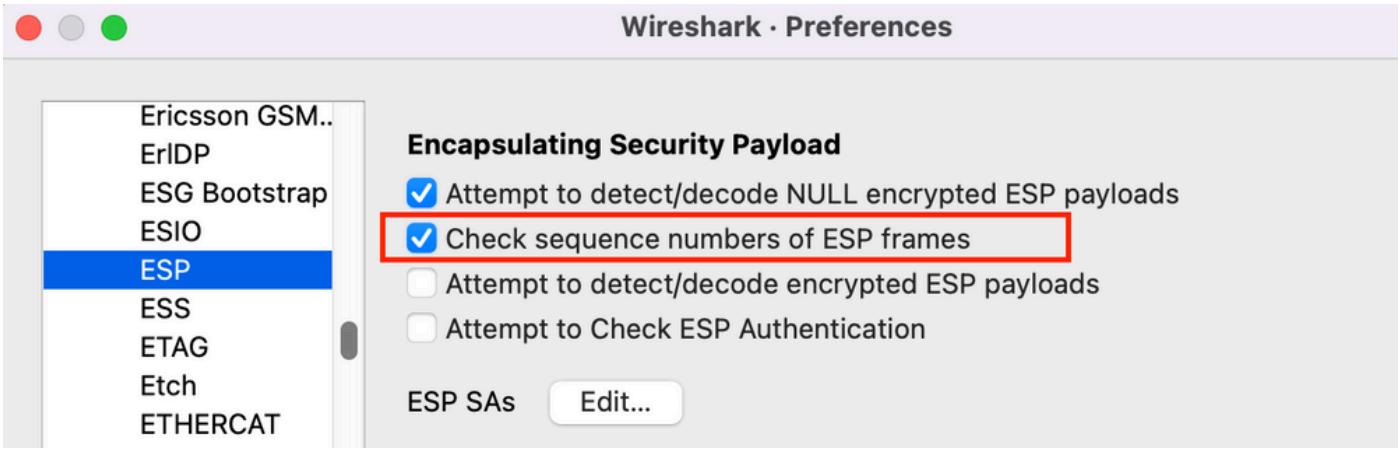
ESP序列号与IP报头起始位置的偏移量为24字节（或IP数据包负载数据的4字节），如前面的输出中粗体部分所强调。在此特定示例中，丢弃数据包的ESP序列号为0x6。

收集数据包捕获

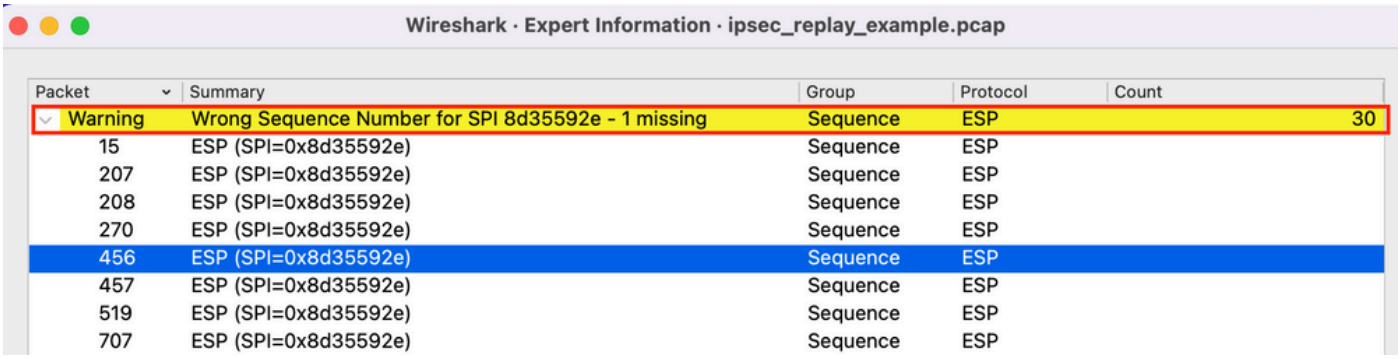
除了标识由于重放检查失败而丢弃的数据包的数据包信息外，需要同时收集有关IPsec流的数据包捕获。这有助于检查同一IPsec流中的ESP序列号模式，以帮助确定重播丢弃的原因。有关如何在Cisco IOS XE路由器上使用嵌入式数据包捕获(EPC)的详细信息，请参阅Cisco IOS和Cisco IOS XE的嵌入式数据包捕获配置示例。

使用Wireshark序列号分析

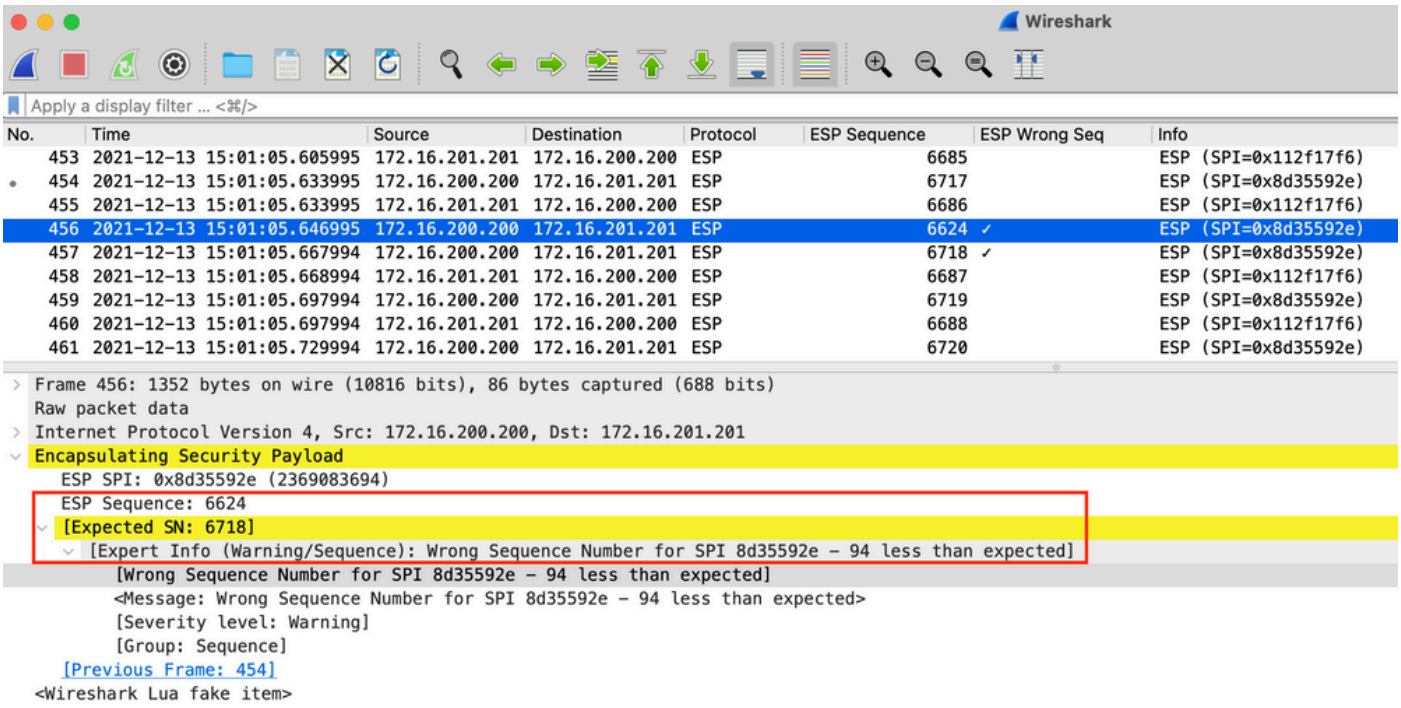
收集WAN接口上加密(ESP)数据包的数据包捕获后，Wireshark可用于对任何序列号异常执行ESP序列号分析。首先，确保在Preferences > Protocols > ESP下启用Sequence Number Check，如图所示：



接下来，在Analyze > Expert信息下检查任何ESP序列号问题，如下所示：



单击序列号错误的任何数据包，获取其他详细信息，如下所示：



解决方案

确定对等体并收集重放丢弃的数据包捕获后，三种可能的情况可以解释重放失败：

1. 它是已延迟的有效数据包：
   数据包捕获有助于确认数据包是否真正有效，以及问题是否不重要（由于网络延迟或传输路径问题）或需要更深入的故障排除。例如，捕获显示序列号为X的数据包顺序混乱，并且重放窗口大小当前设置为64。如果序列号为(X + 64)的有效数据包在数据包X之前到达，则窗口将移至右侧，然后数据包X由于重放失败而被丢弃。

   在这种情况下，可以增加重放窗口的大小或禁用重放检查以确保这样的延迟是可接受的，并且

合法的数据包不会被丢弃。默认情况下，重播窗口大小相当小（窗口大小为64）。 如果增加规模，攻击的风险不会大幅增加。有关如何配置IPsec防重播窗口的信息，请参阅如何配置IPsec防重播窗口：展开和禁用文档。

提示：如果在虚拟隧道接口(VTI)上使用的IPSec配置文件中禁用或更改了重播窗口，则更改在删除并重新应用保护配置文件或重置隧道接口后才会生效。这是预期行为，因为IPsec配置文件是一个模板，用于在启动隧道接口时创建隧道配置文件映射。如果接口已启动，则配置文件的更改不会影响隧道，直到重置接口。

注意：早期的聚合服务路由器(ASR)1000型号（例如带ESP5、ESP10、ESP20和ESP40以及ASR1001的ASR1000）不支持窗口大小为1024，即使CLI允许该配置。因此，show crypto ipsec sa命令输出中报告的窗口大小不正确。使用show crypto ipsec sa peer <ip-address> platform命令验证硬件反重播窗口大小。所有平台上的默认窗口大小为64个数据包。有关详细信息，请参阅Cisco Bug ID CSCso45946。较新版本的Cisco IOS XE路由平台(例如带ESP100和ESP200的ASR1K、ASR1001-X和ASR1002-X、集成服务路由器(ISR)4000系列路由器和Catalyst8000系列路由器)都支持1024数据包的窗口大小版本15.2(2)S及更高版本中。

2. 这是由于发送端点上的QoS配置造成的：
   如果IPsec发送设备上的QoS配置导致IPsec后的数据包重新排序，则可能的缓解措施是使用Cisco IOS XE平台上可用的每个IPsec SA的多序列号空间。

3. 它是先前收到的重复数据包：
   如果出现这种情况，则数据包捕获中可观察到同一IPsec流中具有相同ESP序列号的两个或多个数据包。在这种情况下，丢包是预期的，因为IPsec重播保护的工作方式是为了防止网络中的重播攻击，而系统日志只是提供信息。如果此情况持续出现，则必须将其作为潜在安全威胁进行调查。

注意：仅当在IPsec转换集中启用了身份验证算法时，才会出现重播检查失败。抑制此错误消息的另一种方法是禁用身份验证并仅执行加密；但是，由于禁用身份验证的安全影响，强烈建议不要这样做。

Additional Information

使用Cisco IOS Classic对传统路由器上的重播错误进行故障排除

使用Cisco IOS的传统ISR G2系列路由器上的IPsec重播丢弃与使用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
```

消息输出不提供对等体IP地址或SPI信息。要对此平台进行故障排除，请使用错误消息中的“conn-id”。识别错误消息中的“conn-id”，并在show crypto ipsec sa输出中查找它，因为重放是每SA检查（而不是每对等）。 系统日志消息还提供了ESP序列号，可帮助唯一识别数据包捕获中丢弃的数据包。

注意：对于不同版本的代码，“conn-id”是入站SA的conn id或flow_id。

下面对此进行了说明：

<#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 (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>
```

从此输出中可以看到，重播丢弃来自入站ESP SA SPI为0xE7EDE943的10.2.0.200对等体地址。也可以从日志消息本身注意到，已丢弃数据包的ESP序列号为13。可使用对等体地址、SPI号和ESP序列号的组合来唯一标识数据包捕获中丢弃的数据包。



注意：Cisco IOS系统日志消息对丢弃到每分钟一个的数据平面数据包进行速率限制。要获得确切的数据包丢弃数量的准确计数，请使用show crypto ipsec sa detail命令（如前所示）。

使用早期的Cisco IOS XE软件

在运行早期Cisco IOS XE版本的路由器上，系统日志中报告的“REPLAY_ERROR”无法打印包含丢弃已重播数据包的对等体信息的实际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
```

要识别正确的IPsec对等体和流信息，请使用系统日志消息中打印的数据平面(DP)句柄作为此命令中的输入参数SA句柄，以便在Quantum流处理器(QFP)上检索IPsec流信息：

<#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: 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>
```

嵌入式事件管理器(EEM)脚本还可用于自动化数据收集：

```
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"
```

在本示例中，收集的输出被重定向到bootflash。要查看此输出，请使用命令more bootflash:replay-error.txt。

相关信息

- 支持语音和视频的IPSec VPN(V3PN)解决方案参考网络设计
- 如何配置IPsec反重播窗口：正在扩展和正在禁用。
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。