IPSec反重放检查失败

目录

简介

本文描述关系到一Internet协议安全性的问题(IPSec)反重放检查失败，并且提供排除故障步骤和可能的解决方案对问题。

> **注意**：反重放保护是IPSec协议提供的重要安全性服务。IPSec反重放不合格有安全影响，并且应该小心地只使用。

背景信息

重放攻击说明

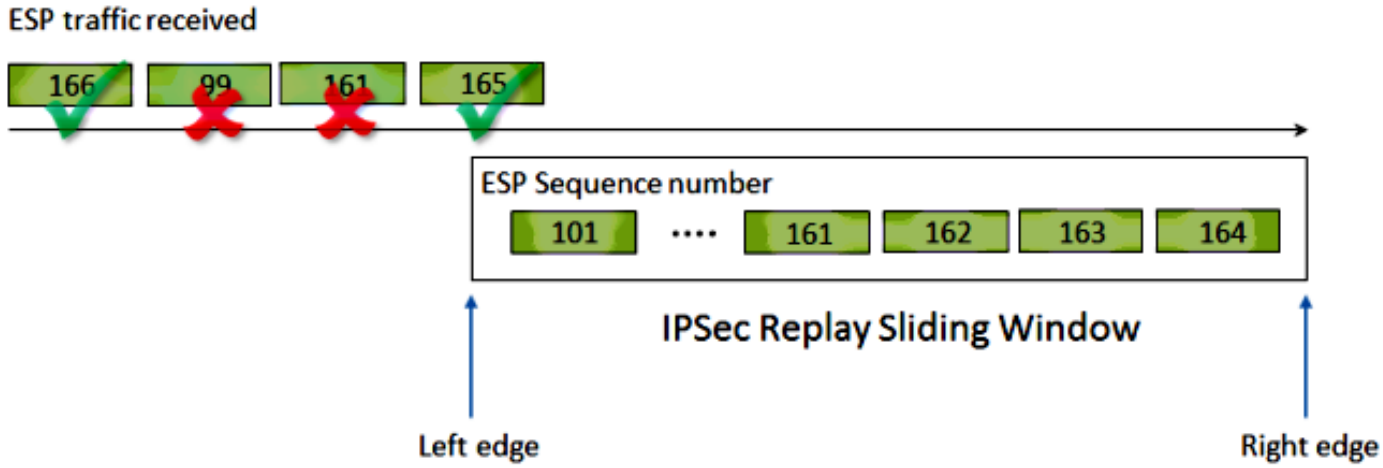
重放攻击是有效数据传输有恶意或欺骗性地被重复或延迟网络攻击的表。它是尝试由记录合法通信并且重复他们为了扮演有效用户的人推翻安全和打乱或者导致合法连接的负面影响。

重播检查失败说明

IPSec提供反重放保护复制有一个单调地增加的序号分配的加密的信息包到每加密的信息包的攻击者。数据包它根据有使用的这些编号已经处理一个滑动窗口所有可接受序号的接收的IPSec终点记录。目前，在Cisco IOS实施的默认反重放窗口大小是64数据包。

> **注意**：当64被认为不切实际小为流行网络，增强请求CSCva65805和CSCva65836提出了增加默认重播窗口大小到512。

这在此图说明：



这是处理在接收的隧道终点的流入IPSec数据流的步骤有反重放已启用的：

1. 当数据包接收时，如果序号在窗口内下降和以前未接收，数据包接受，并且被标记作为已接收，在发送对完整性验证前。

2. 如果序号在窗口内下降和以前接收，数据包丢弃，并且重播计数器被增加。

3. 如果序号比在窗口的最高的序号极大，数据包接受，并且被标记作为已接收。滑动窗口然后移动在右边。
   注意：这只发生，如果数据包有效并且通过完整性检查。
4. 如果序号比在窗口的最低的顺序是较少，数据包丢弃，并且重播计数器被增加。

在第二个和第四个方案中，重播检查失败发生，并且路由器显示错误消息类似于此：

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

> **注意**：分组加密传输VPN (GETVPN)有呼叫Time Based反重放失败的一完全不同的反重放检查。本文只包括基于反的反重放。

问题

如前所述，重播检查目的将防止受到数据包的有恶意的重复。然而，有一失败的重播检查也许不归结于一个有恶意的原因的一些方案：

- 错误在传输介质也许起因于数据包重拨。如果并行路径存在，这是准确无误的。

- 错误也许由不同等的数据包处理路径造成在Cisco IOS里面。例如，要求IP重组的大IPSec信息包，在解密在负载的一个系统也许延迟足够，为了落在重播窗口外面下前，当他们处理的时候。

- 错误也许由在发送的IPSec终点启用的服务质量(QoS)造成。使用Cisco IOS实施， IPSec加密在输出方向的QoS前发生。某些QoS功能，例如低延迟队列(LLQ)，能造成IPSec信息包交付变得有故障和已丢失由接收的终端由于重播检查失败。

排除故障IPSec重播丢包

排除故障IPSec重播丢包的密钥是识别由于的丢包重赛，并且使用数据包捕获为了确认这些数据包是否的确是在接收路由器到达在重播窗口外面的被重赛的数据包或数据包。为了正确地匹配对什么的丢弃的数据包在嗅探器跟踪捕获，第一步将识别丢弃的数据包属于的对等体和IPSec流。这不同地执行根据路由器平台。

思科运行经典的Cisco IOS的集成业务路由器(ISR) /ISR G2平台

为了排除故障在此平台，请使用**conn-id**在错误消息。识别在错误消息的**conn-id**，并且寻找它在**show crypto ipsec sa**输出中，因为重播是每**SA** (安全关联)检查(与**每对等相对**)。系统消息也提供封装安全有效载荷(ESP)序号，可独特帮助识别在数据包捕获的丢弃的数据包。

注意：用不同的编码版本， **conn-id**是**conn id**或**flow_id**入站SA的。

这说明得此处：

```
%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>
```

和能从此输出被看到，重播丢弃是从与一个入站ESP SA安全参数索引(SPI)的**10.2.0.200**对等地址**0xE7EDE943**。它可以也是要注意的从日志消息丢弃的数据包的ESP序号是**13**。因此，对等地址、SPI编号和ESP序号的组合可以用于为了独特识别在数据包捕获丢弃的数据包。

> **注意**：Cisco IOS系统消息为dataplane丢包是速率限制。为了获得被丢弃的数据包确切的数字的准确计数，请使用**show crypto ipsec sa detail命令**如以前显示。并且，注意用代码早于Cisco IOS版本12.4(4)T，计数器也许不正确地更新。这在Cisco Bug ID CSCsa90034修复。

思科聚合服务路由器(ASR)该运行Cisco IOS XE

在ASR平台上，在某些报告的REPLAY_ERROR初期的Cisco IOS XE版本也许不打印被重赛的数据包丢弃的实际IPSec流，如显示此处：

```
%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>
```

为了识别正确IPSec对等体和流信息，请使用打印的数据层面(DP)把柄在系统消息，在此命令的**SA**输入参数**把柄**为了获取关于Quantum流处理器(QFP)的IPSec流信息：

```
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 (Details below)
: 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>
```

如果在ASR的Cisco IOS版本是PRE XE版本3.7，则错误消息记录与**DP把柄**和没有信息的消息关于罪犯数据包属于的peer/SPI。这是Cisco Bug ID CSCtw69096变得相关的地方：

```
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 (Details below)
: 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>
```

在这类情况下，这被嵌入的活动管理器(EEM)脚本可以用于为了发现哪对等体和SPI触发反重放消息：

```
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 (Details below)
: 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>
```

为了看到在ASR的输出，请输入**更多Bootflash ：周期地重播error.txt命令。**

与ASR数据路径包跟踪功能一起使用

使用ASR1000的更加最近的Cisco IOS XE软件，关于对等体的信息以及IPSec SPI也打印为了帮助排除故障反重放问题。然而，仍然失踪与的一个关键信息什么比较在运行Cisco IOS经典之作的ISR G2平台打印是ESP序号。ESP序号用于为了独特识别在一个给的IPSec流内的一个IPSec信息包。没有序号，正确地识别数据包在数据包捕获被撤销的变得难。

在Cisco IOS XE版本3.10 (15.3(3)S)中，跟踪基础设施的新的数据包介绍为了帮助排除故障dataplane信息包转发问题，并且可以用于此重播丢弃在ASR被观察的此特定的故障排除情况：

```
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 (Details below)
: 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>
```

为了帮助确定丢弃的数据包的ESP序号，请完成与包跟踪功能的这些步骤：

1. 设置平台条件调试过滤器为了匹配从对等设备的流量：

   ```
   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 (Details below)
   : 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>
```

2. 使包跟踪以**Copy选项**为了复制信息包报头题头信息：

```
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 (Details below)
: 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>
```

3. 当重播错误检测时，请使用数据包踪迹缓冲区为了识别数据包丢弃的由于重赛，并且ESP序号可以在数据包找到复制：

```
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
```

上一个输出显示数据包第6和7丢弃，因此他们可以当前详细被检查：

```
Router#show platform packet-trace  pac 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
```

从IP报头开始的ESP序号有偏移量24，如强调在粗体和斜体字在上一个输出中。在本例中特定的示例，丢弃的数据包的ESP序号是0x6。

解决方案

在对等体识别后，有三个可能的情况：

1. **它是有效信息包：**数据包捕获帮助确认数据包是否实际上有效和，如果问题是可忽略的(由于网络延迟或传输路径问题)或要求一更加详细排除故障。例如，捕获显示一数据包用到达故障中X的序号，并且窗口大小设置到64。如果X + 64数据包在数据包x前到达，则被撤销由于重播失败(它确实不是攻击)。

   在这样方案中，请增加重播窗口的大小为了保证这样延迟占和防止合法数据包丢弃。默认情况下，窗口大小相当小(窗口大小64)。如果增加大小，不非常地增加攻击的风险。关于如何配置IPsec反重放窗口的信息，参考如何配置IPsec反重放窗口：展开和禁用的条款。
   提示：如果重播窗口禁用或修改在IPSec简档和IPSec简档与在一个虚拟隧道接口(VTI)的通道保护一起使用，更改不会生效，直到保护配置文件或者删除并且重新应用或者隧道接口重置。这是预料之中的行为，因为IPSec简档是创建通道配置文件地图的模板，当隧道接口启用时(没关闭)。一旦接口已经是，对配置文件的更改不影响直到重新应用的通道或接口重置。**注意**

：在ASR的一通常遇到的问题，关于反重放窗口大小，是经典ASR1K型号(例如与ESP5的ASR1K， ESP10、ESP20和ESP40，与ASR1001一起)实际上不支持窗口大小1024。即使命令允许您定此限制到1024，窗口大小重置到512由硬件。因此，在**show crypto ipsec sa命令**输出中报告的窗口大小也许不正确。输入**show crypto ipsec sa对端IP地址平台**命令为了验证硬件反重放窗口大小。默认窗口尺寸是在所有平台的64数据包。欲知更多信息，参考Cisco Bug ID CSCso45946。更新的ASR1K型号(例如与ESP100的ASR1K和ESP200， ASR1001-X和ASR1002-X并且ISR-4400)支持窗口大小在版本15.2(2)S和以上的1024数据包。

2. **它是落在接收方的反重放窗口外面的数据包：**万一接收的IPSec终点丢弃被重赛的数据包(当是推测的对)，在发送方广域网端的同时嗅探器捕获，并且接收方帮助由在转接网络重赛的数据包搜寻，如果这造成由发送方的行为不端，或者。

3. **它归结于在发送方的末端的QoS配置：**此情况要求仔细调整考试和某的QoS为了缓和情况。对于此主题和潜在解决方案的一更加详细的说明，参考在语音的反重放考虑事项，并且视频启用IPSec VPN (V3PN)条款。

注意：当验证算法在IPSec转换集时，启用重播检查失败只看到。另一个方式抑制此错误消息将禁用验证和进行仅加密;然而，这严格被劝阻的归结于已禁用验证安全影响。

相关信息

- **语音和视频启用的IPSec VPN (V3PN)解决方案参考网络设计**
- **如何配置IPsec反重放窗口：展开和禁用**。
- **技术支持和文档 - Cisco Systems**