# Fehlerbehebung bei IPsec-Anti-Replay-Überprüfungsfehlern

## Inhalt



## Einleitung

Dieses Dokument beschreibt ein Problem im Zusammenhang mit IPsec-Anti-Replay-Check-Fehlern (Internet Protocol Security) und stellt mögliche Lösungen vor.

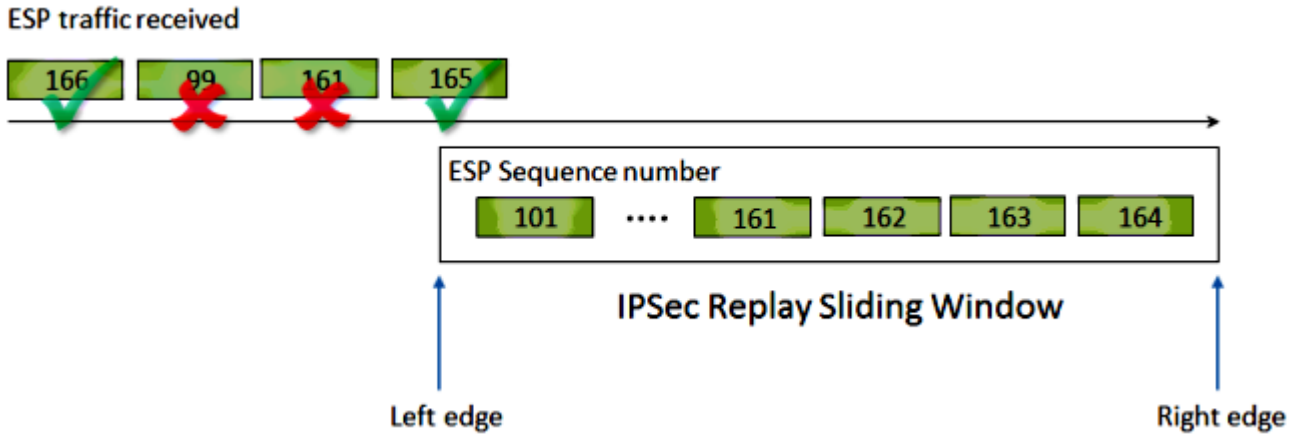
## Hintergrundinformationen

### Ein Überblick über Replay-Angriffe

Ein Replay-Angriff ist eine Form eines Netzwerkangriffs, bei dem eine gültige Datenübertragung auf böswillige oder betrügerische Weise aufgezeichnet und später wiederholt wird. Es handelt sich um einen Versuch, die Sicherheit durch eine Person zu untergraben, die legitime Kommunikation aufzeichnet und wiederholt, um die Identität eines gültigen Benutzers anzunehmen und legitime Verbindungen zu unterbrechen oder zu beeinträchtigen.

### Schutz für IPsec-Wiedergabeprüfung

Jedem verschlüsselten Paket wird über IPsec eine Sequenznummer zugewiesen, die sich monoton erhöht, um einen Anti-Replay-Schutz gegen einen Angreifer zu gewährleisten. Der empfangende IPsec-Endpunkt verfolgt, welche Pakete er bereits verarbeitet hat, wenn er diese Nummern verwendet, und ein gleitendes Fenster mit akzeptablen Sequenznummern. Die Standardgröße des Anti-Replay-Fensters in der Cisco IOS®-Implementierung beträgt 64 Pakete, wie in der Abbildung gezeigt:




Wenn für einen IPsec-Tunnelendpunkt der Anti-Replay-Schutz aktiviert ist, wird der eingehende IPsec-Datenverkehr wie folgt verarbeitet:

- Wenn die Sequenznummer in das Fenster fällt und noch nicht empfangen wurde, wird die Integrität des Pakets überprüft. Wenn das Paket die Integritätsprüfung besteht, wird es akzeptiert, und der Router markiert, dass diese Sequenznummer empfangen wurde. Beispiel: ein Paket mit der ESP-Sequenznummer 162 (Encapsulating Security Payload).
- Wenn die Sequenznummer in das Fenster fällt, aber zuvor empfangen wurde, wird das Paket verworfen. Dieses duplizierte Paket wird verworfen, und der Verwerfer wird im Wiedergabecunter aufgezeichnet.

- Wenn die Sequenznummer größer als die höchste Sequenznummer im Fenster ist, wird die Integrität des Pakets überprüft. Wenn das Paket die Integritätsprüfung besteht, wird das Schieberegler nach rechts verschoben. Wenn beispielsweise ein gültiges Paket mit der Sequenznummer 189 empfangen wird, wird der neue rechte Rand des Fensters auf 189 und der linke Rand auf 125 (189 - 64 [Fenstergröße]) gesetzt.

- Wenn die Sequenznummer niedriger als die linke Kante ist, wird das Paket verworfen und innerhalb des Wiedergabenzählers aufgezeichnet. Dies wird als fehlerhaftes Paket betrachtet.

In den Fällen, in denen eine Wiederholungsprüfung fehlschlägt und das Paket verworfen wird, generiert der Router eine Syslog-Meldung wie diese:

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

---

**Hinweis**: Die Wiedergabenerkennung basiert auf der Annahme, dass die IPsec-Sicherheitszuordnung (SA) nur zwischen zwei Peers besteht. GETVPN (Group Encrypted Transport VPN) verwendet eine einzelne IPsec-SA zwischen mehreren Peers. Daher verwendet GETVPN einen völlig anderen Anti-Replay-Prüfmechanismus, den Time Based Anti-Replay Failure (Zeitbasierter Anti-Replay-Fehler). In diesem Dokument wird nur die kontrabasierte Anti-Wiedergabe für Point-to-Point-IPsec-Tunnel behandelt.

---

**Hinweis**: Der Anti-Replay-Schutz ist ein wichtiger Sicherheitsdienst, den das IPsec-Protokoll bietet. Die Deaktivierung der IPsec-Anti-Replay hat Auswirkungen auf die Sicherheit und muss mit Diskretion durchgeführt werden.

---

# Probleme, die IPsec-Wiedergabeverringerungen verursachen können

Wie zuvor beschrieben, dient die Überprüfung von Wiederholungen dem Schutz vor böswilligen Wiederholungen von Paketen. Es gibt jedoch einige Szenarien, in denen eine fehlgeschlagene Überprüfung der Wiedergabe möglicherweise nicht auf einen böswilligen Grund zurückzuführen ist:

- Der Fehler kann durch ein ausreichendes Paket verursacht werden, das im Netzwerkpfad zwischen den Tunnelendpunkten neu angeordnet wird. Dies kann wahrscheinlich der Fall sein, wenn es mehrere Netzwerkpfade zwischen den Peers gibt.

- Der Fehler kann durch ungleiche Paketverarbeitungspfade im Cisco IOS verursacht werden. Fragmentierte IPsec-Pakete, die vor der Entschlüsselung erneut zusammengesetzt werden müssen, können so lange verzögert sein, dass sie bei der Verarbeitung aus dem Wiedergabefenster herausfallen.
- Der Fehler kann durch die QoS (Quality of Service) verursacht werden, die auf dem sendenden IPsec-Endpunkt oder im Netzwerkpfad aktiviert ist. Bei der Cisco IOS-Implementierung erfolgt die IPsec-Verschlüsselung vor QoS in Ausgangsrichtung. Bestimmte QoS-Funktionen wie Low Latency Queueing (LLQ) können dazu führen, dass die IPsec-Paketübermittlung aufgrund eines Fehlers bei der Wiederholungsprüfung außer Betrieb gerät und vom empfangenden Endpunkt verworfen wird.

- Ein Problem mit der Netzwerkkonfiguration oder dem Netzwerkbetrieb kann zu duplizierten Paketen führen, wenn diese das Netzwerk durchlaufen.

- Ein Angreifer (Man-in-the-Middle) könnte den ESP-Datenverkehr verzögern, verwerfen und duplizieren.

# Fehlerbehebung bei IPsec-Wiedergabeverwerfen

Der Schlüssel zur Fehlerbehebung bei IPsec-Replay-Drops besteht darin, zu ermitteln, welche Pakete aufgrund der Replay-Funktion verworfen werden, und anhand der Paketerfassung festzustellen, ob es sich bei diesen Paketen tatsächlich um replay-Pakete oder Pakete handelt, die auf dem empfangenden Router außerhalb des Replay-Fensters angekommen sind. Um die verworfenen Pakete den in der Sniffer-Ablaufverfolgung erfassten Paketen richtig zuzuordnen, müssen Sie im ersten Schritt den Peer und den IPsec-Fluss identifizieren, zu dem die verworfenen Pakete gehören, sowie die ESP-Sequenznummer des Pakets.

## Cisco IOS XE DataPath Packet Tracing-Funktion verwenden

Auf Routerplattformen, auf denen Cisco IOS® XE ausgeführt wird, werden Informationen über den Peer sowie der IPsec-Sicherheitsparameterindex (SPI) in der Syslog-Meldung ausgegeben, wenn ein Drop auftritt, um die Fehlerbehebung bei Anti-Replay-Problemen zu unterstützen. Eine wichtige Information, die jedoch immer noch fehlt, ist die ESP-Sequenznummer. Die ESP-Sequenznummer wird verwendet, um ein IPsec-Paket innerhalb eines bestimmten IPsec-Flusses eindeutig zu identifizieren. Ohne die Sequenznummer wird es schwierig, genau zu identifizieren, welches Paket bei einer Paketerfassung verworfen wird.

Die Funktion "Cisco IOS XE datapath packet-trace" kann in dieser Situation verwendet werden, wenn das Replay-Drop mit der folgenden Syslog-Meldung beobachtet wird:

```
%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
```

Um die ESP-Sequenznummer für das verworfene Paket zu identifizieren, führen Sie die folgenden Schritte mit der Paketablaufverfolgungsfunktion aus:

1. Richten Sie den bedingten Plattformdebugfilter ein, um den Datenverkehr vom Peer-Gerät abzugleichen:

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

1. Aktivieren Sie die Paketablaufverfolgung mit der **Kopieroption**, um die Paketkopfzeilen-Informationen zu kopieren:

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

1. Wenn Wiedergabefehler erkannt werden, verwenden Sie den Paketablaufverfolgungspuffer, um das Paket zu identifizieren, das aufgrund der Wiedergabe verworfen wurde. Die ESP-Sequenznummer kann in dem kopierten Paket gefunden werden:

<#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
```

Die vorherige Ausgabe zeigt, dass die Paketnummern 6 und 7 verworfen wurden, sodass sie jetzt im Detail untersucht werden können:

```
<#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
```

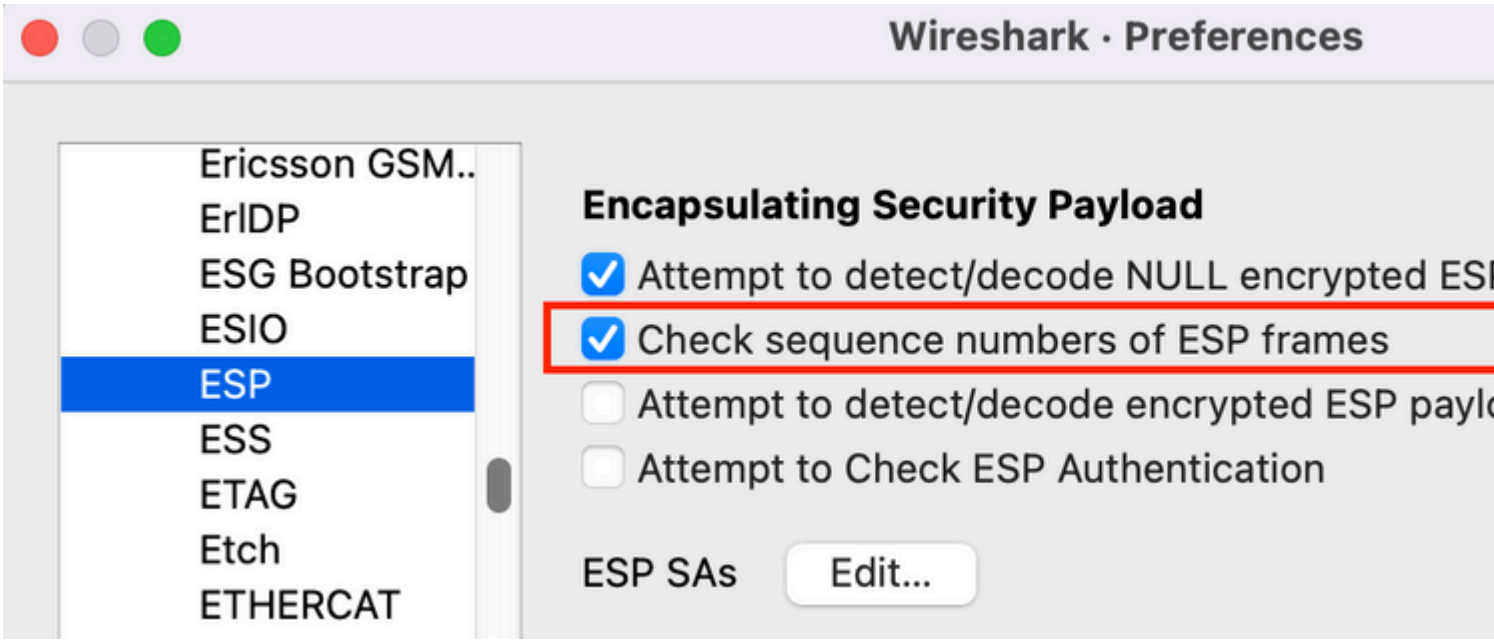
Die ESP-Sequenznummer hat einen Offset von 24 Byte, der vom IP-Header (oder 4 Byte der Nutzdaten des IP-Pakets) ausgeht, wie in der vorherigen Ausgabe fett hervorgehoben. In diesem Beispiel lautet die ESP-Sequenznummer für das verlorene Paket 0x6.

## Paketerfassungen erfassen

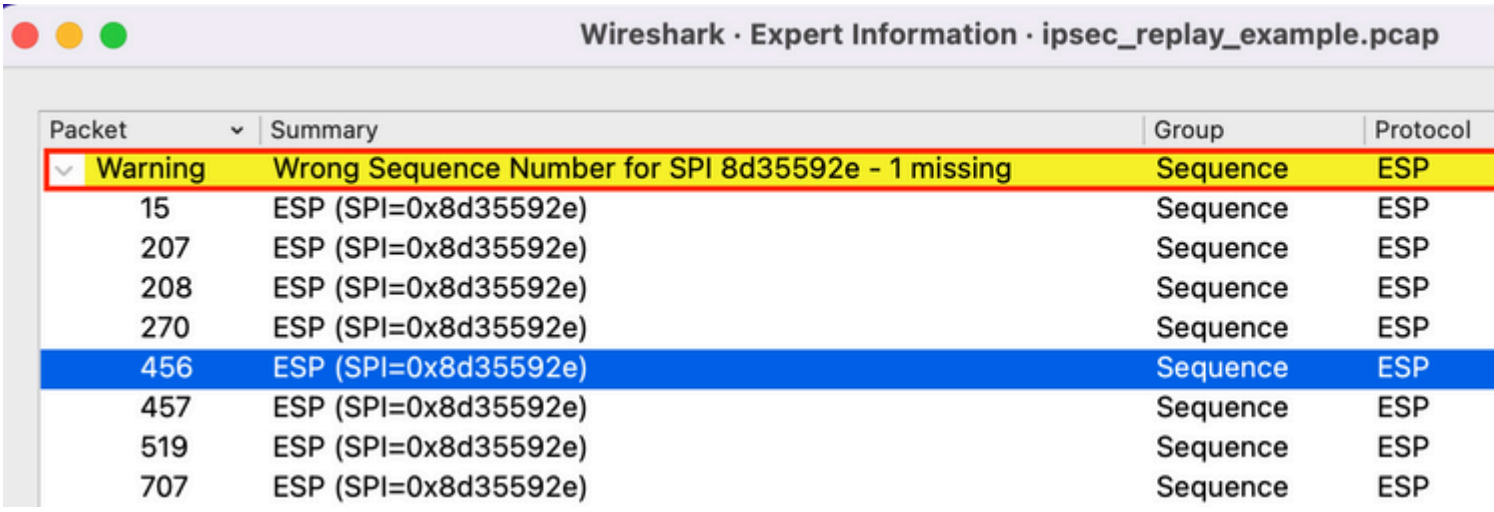
Zusätzlich zur Identifizierung der Paketinformationen für das aufgrund eines Fehlers bei der Wiederholungsprüfung verworfene Paket muss gleichzeitig eine Paketerfassung für den betreffenden IPsec-Fluss erfasst werden. Dies hilft bei der Untersuchung des ESP-Sequenznummernmusters innerhalb desselben IPsec-Flusses, um den Grund für den Replay-Abbruch zu ermitteln. Weitere Informationen zur Verwendung von Embedded Packet Capture (EPC) auf Cisco IOS XE-Routern finden Sie unter Embedded Packet Capture for Cisco IOS and Cisco IOS XE Configuration Example.

## Wireshark-Sequenznummernanalyse verwenden

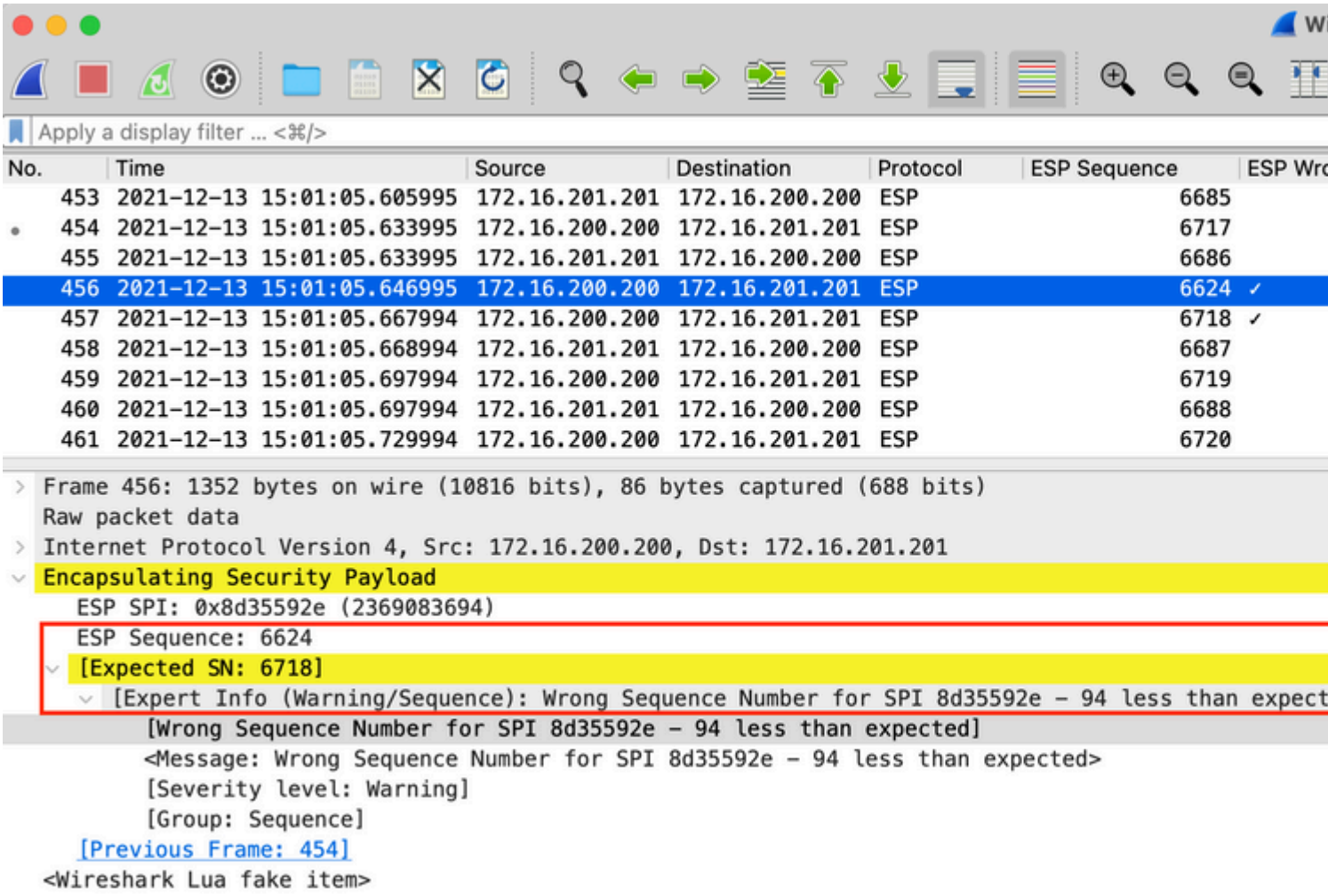
Nachdem die Paketerfassung für die verschlüsselten (ESP) Pakete an der WAN-Schnittstelle erfasst wurde, kann Wireshark verwendet werden, um ESP-Sequenznummernanalysen für Anomalien bei Sequenznummern durchzuführen. Stellen Sie zunächst sicher, dass die Überprüfung der Sequenznummer unter **Voreinstellungen > Protokolle > ESP** aktiviert ist, wie im Bild gezeigt:




Überprüfen Sie anschließend unter **Analyse > Experteninformationen** (**Analyze > Expert** Information) die ESP-Sequenznummer wie folgt:




Klicken Sie auf eines der Pakete mit der falschen Sequenznummer, um weitere Details zu erhalten:




# Lösung

Nachdem der Peer identifiziert und die Paketerfassung für die Wiedergabe-Löschungen erfasst wurde, können die Wiedergabefehler in drei möglichen Szenarien erklärt werden:

1. Es handelt sich um ein gültiges verzögertes Paket:
   Paketerfassungen helfen, zu bestätigen, ob das Paket tatsächlich gültig ist und ob das Problem unbedeutend ist (aufgrund von Netzwerklatenz oder Übertragungspfad-Problemen) oder eine eingehendere Fehlerbehebung erfordert. Die Erfassung zeigt beispielsweise ein Paket mit einer Sequenznummer von X, das nicht in der richtigen Reihenfolge ankommt, und die Größe des Wiedergabefensters ist derzeit auf 64 festgelegt. Wenn ein gültiges Paket mit der Sequenznummer (X + 64) vor dem Paket X eingeht, wird das Fenster nach rechts verschoben und dann das Paket X aufgrund eines Wiedergabefehlers verworfen.

   In solchen Szenarien ist es möglich, das Wiedergabefenster zu vergrößern oder die Wiedergabeprüfung zu deaktivieren, um sicherzustellen, dass solche Verzögerungen als akzeptabel angesehen werden und die legitimen Pakete nicht verworfen werden. Standardmäßig ist die Größe des Wiedergabefensters relativ klein (Fenstergröße 64). Wenn Sie die Größe erhöhen, erhöht sich das Risiko eines Angriffs nicht wesentlich. Weitere Informationen zum Konfigurieren eines IPsec-Anti-Replay-Fensters finden Sie im Dokument How to Configure IPsec Anti-Replay Window: Expanding and Disabling (So konfigurieren Sie IPsec-Anti-Replay-Fenster: Erweitern und Deaktivieren).

---

**Tipp:** Wenn das Wiedergabefenster in dem IPSec-Profil deaktiviert oder geändert wird, das auf

---

einer Virtual Tunnel Interface (VTI) verwendet wird, werden die Änderungen erst wirksam, wenn das Schutzprofil entweder entfernt und erneut angewendet oder die Tunnelschnittstelle zurückgesetzt wird. Dieses Verhalten wird erwartet, da IPsec-Profile eine Vorlage sind, die zum Erstellen einer Tunnelprofilzuordnung verwendet wird, wenn die Tunnelschnittstelle gestartet wird. Wenn die Schnittstelle bereits aktiv ist, wirken sich Änderungen am Profil erst auf den Tunnel aus, wenn die Schnittstelle zurückgesetzt wird.

**Hinweis**: Die früheren Aggregation Services Router (ASR) 1000-Modelle (wie ASR1000 mit ESP5, ESP10, ESP20 und ESP40 zusammen mit dem ASR1001) unterstützten keine Fenstergröße von 1024, obwohl die CLI zuließ, dass Konfiguration. Daher ist die Fenstergröße, die in der Ausgabe des Befehls **show crypto ipsec sa** gemeldet wird, möglicherweise nicht korrekt. Verwenden Sie den Befehl **show crypto ipsec sa peer ip-address platform**, um die Größe des Hardware-Anti-Replay-Fensters zu überprüfen. Die Standardfenstergröße beträgt 64 Pakete auf allen Plattformen. Weitere Informationen finden Sie unter Cisco Bug-ID CSCso45946. Die späteren Cisco IOS XE Routing-Plattformen (wie ASR1K mit ESP100 und ESP200, ASR1001-X und ASR1002-X, Integrated Service Router (ISR) der Serie 4000 und Catalyst 8000 Router) tun dies. unterstützen eine Fenstergröße von 1024 Paketen in Version 15.2(2)S und höher.

2. Der Grund hierfür ist die QoS-Konfiguration auf dem sendenden Endpunkt:
   Diese Situation erfordert eine sorgfältige Prüfung und eine gewisse QoS-Einstellung, um den Zustand zu mindern. Eine ausführlichere Beschreibung dieses Themas und einer möglichen Lösung finden Sie in dem Artikel Anti-Replay Considerations in a Voice and Video Enabled IPSec VPN (V3PN).

3. Es handelt sich um ein doppeltes Paket, das zuvor empfangen wurde:
   Wenn dies der Fall ist, können bei der Paketerfassung zwei oder mehr Pakete mit derselben ESP-Sequenznummer innerhalb desselben IPsec-Datenflusses beobachtet werden. In diesem Fall ist ein Paketverlust zu erwarten, da der IPsec-Wiedergabeschutz so funktioniert, dass Wiederholungsangriffe im Netzwerk verhindert werden. Das Syslog stellt lediglich Informationsmaterial dar. Wenn diese Bedingung weiterhin besteht, muss sie als potenzielles Sicherheitsrisiko untersucht werden.

**Hinweis**: Fehler bei der erneuten Überprüfung werden nur erkannt, wenn ein Authentifizierungsalgorithmus im IPsec-Transformationssatz aktiviert ist. Eine weitere Möglichkeit, diese Fehlermeldung zu unterdrücken, besteht darin, die Authentifizierung zu deaktivieren und nur die Verschlüsselung durchzuführen. Dies wird jedoch aufgrund der Sicherheitsauswirkungen einer deaktivierten Authentifizierung dringend empfohlen.

# Zusätzliche Informationen

## Fehlerbehebung bei Replay-Fehlern auf älteren Routern mit Cisco IOS Classic

Die IPsec-Wiedergabe wird auf den älteren Routern der ISR G2-Serie, die das Cisco IOS verwenden, nicht auf den Routern durchgeführt, die das Cisco IOS XE verwenden, wie hier gezeigt:

<#root>

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

**connection id=529, sequence number=13**

Beachten Sie, dass die Nachrichtenausgabe weder die Peer-IP-Adresse noch SPI-Informationen bereitstellt. Um auf dieser Plattform eine Fehlerbehebung durchzuführen, verwenden Sie die "conn-id" in der Fehlermeldung. Identifizieren Sie die "conn-id" in der Fehlermeldung, und suchen Sie sie in der Ausgabe von **show crypto ipsec sa,** da die Wiedergabe eine Per-SA-Prüfung ist (im Gegensatz zu einer Per-Peer-Prüfung). Die Syslog-Meldung enthält auch die ESP-Sequenznummer, anhand derer das verlorene Paket bei der Paketerfassung eindeutig identifiziert werden kann.

---

> **Hinweis**: Bei verschiedenen Codeversionen ist "conn-id" entweder die **conn-ID** oder **flow_id** für die eingehende SA.

---

Dies wird hier veranschaulicht:

<#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>
```

Wie aus dieser Ausgabe ersichtlich ist, stammt die Wiedergabeverweigerung von der 10.2.0.200-Peer-Adresse mit einem eingehenden ESP SA SPI von 0xE7EDE943. Aus der Protokollmeldung selbst kann auch hervorgehen, dass die ESP-Sequenznummer für das verlorene Paket 13 ist. Die Kombination aus Peer-Adresse, SPI-Nummer und ESP-Sequenznummer kann verwendet werden, um das bei der Paketerfassung verlorene Paket eindeutig zu identifizieren.

---

> **Hinweis**: Die Cisco IOS Syslog-Nachricht ist für das Datenpaket auf einem Datenflugzeug auf einen Wert pro Minute begrenzt. Um die genaue Anzahl der verworfenen Pakete zu ermitteln, verwenden Sie den Befehl **show crypto ipsec sa detail** wie oben gezeigt.

---

## Arbeiten mit älterer Cisco IOS XE Software

Auf Routern, auf denen frühere Cisco IOS XE-Versionen ausgeführt werden, druckt der Syslog-Eintrag "REPLAY_ERROR" möglicherweise nicht den tatsächlichen IPsec-Datenfluss mit den Peer-Informationen aus, an denen das wiedergegebene Paket verworfen wird, wie hier gezeigt:

```
%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
```

Um die richtigen IPsec-Peer- und Flow-Informationen zu identifizieren, verwenden Sie den in der Syslog-Meldung ausgedruckten Datenebenen-(DP)-Handle als Eingabeparameter "SA Handle" in diesem Befehl, um die IPsec-Flow-Informationen auf dem Quantum Flow Processor (QFP) abzurufen:

<#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>
```

Ein Embedded Event Manager (EEM)-Skript kann ebenfalls zur Automatisierung der Datenerfassung verwendet werden:

```
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 diesem Beispiel wird die erfasste Ausgabe an den **Bootflash** umgeleitet**.** Um diese Ausgabe anzuzeigen, verwenden Sie den Befehl **more bootflash:replay-error.txt**.

# Zugehörige Informationen

- Sprach- und videofähiges IPSec VPN (V3PN) Lösungsreferenznetzwerk
- So konfigurieren Sie das IPsec-Anti-Replay-Fenster: Erweitern und Deaktivieren.
- Technischer Support und Dokumentation für Cisco Systeme

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.