Fehlerbehebung bei Fehlern bei der IPsec-Anti-Replay-Prüfung

Inhalt

Einleitung

In diesem Dokument wird ein Problem im Zusammenhang mit IPsec-Anti-Wiederholungsprüffehlern (Internet Protocol Security) und die Fehlerbehebung bei möglichen Lösungen beschrieben.

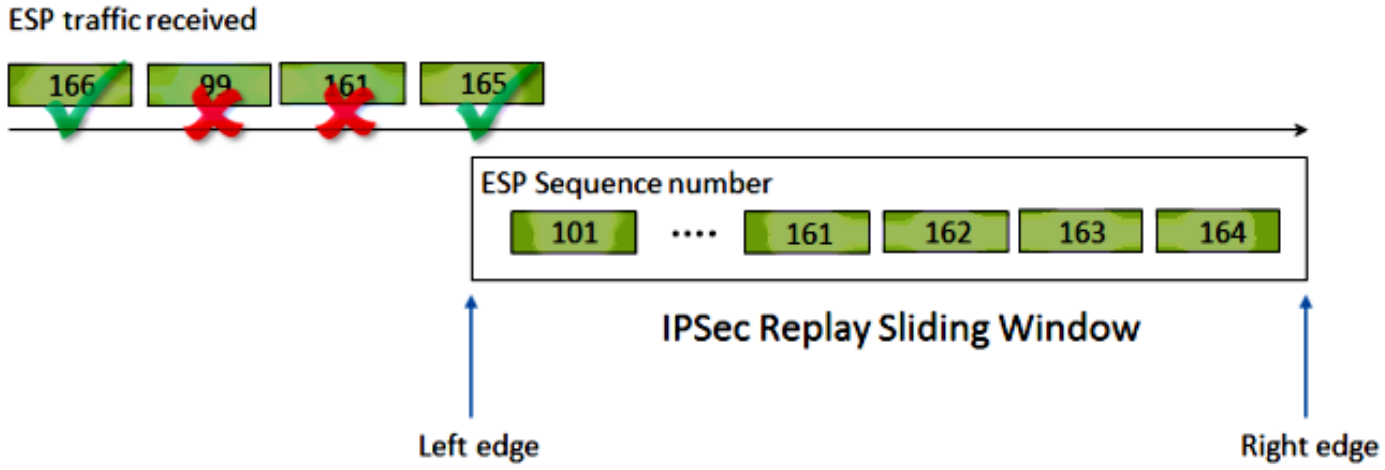
Hintergrundinformationen

Übersicht über Wiederholungsangriffe

Ein Wiederholungsangriff ist eine Form von Netzwerkangriffen, bei der eine gültige Datenübertragung böswillig oder betrügerisch aufgezeichnet und später wiederholt wird. Es handelt sich um den Versuch, die Sicherheit durch eine Person zu untergraben, die legitime Kommunikation aufzeichnet und wiederholt, um einen gültigen Benutzer zu imitieren und legitime Verbindungen zu stören oder zu beeinträchtigen.

IPsec-Replay-Prüfschutz

Eine Sequenznummer, die monoton zunimmt, wird jedem verschlüsselten Paket per IPsec zugewiesen, um einen Anti-Replay-Schutz gegen einen Angreifer zu bieten. Der empfangende IPsec-Endpunkt überwacht, welche Pakete er bereits verarbeitet hat, wenn er diese Zahlen verwendet, und zeigt ein gleitendes Fenster mit zulässigen Sequenznummern an. Die Standardgröße des Anti-Replay-Fensters in der Cisco IOS®-Implementierung beträgt 64 Pakete, wie in diesem Bild gezeigt:



Wenn ein IPsec-Tunnelendpunkt über aktivierten Anti-Replay-Schutz verfügt, wird der eingehende IPsec-Datenverkehr wie folgt verarbeitet:

- Wenn die Sequenznummer in das Fenster fällt und nicht zuvor empfangen wurde, wird die Integrität des Pakets überprüft. Wenn das Paket die Integritätsprüfung besteht, wird es akzeptiert, und der Router gibt an, dass diese Sequenznummer empfangen wurde. Beispielsweise ein Paket mit der ESP-Folgenummer 162 (Encapsulating Security Payload).
- Wenn die Sequenznummer in das Fenster fällt, aber bereits empfangen wurde, wird das Paket verworfen. Dieses duplizierte Paket wird verworfen, und der Drop wird im Wiederholungszähler 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 Schiebefenster nach rechts verschoben. Wenn beispielsweise ein gültiges Paket mit einer Folgenummer von 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 der linke Rand ist, wird das Paket verworfen und im Wiederholungszähler aufgezeichnet. Dies wird als Out-of-Order-Paket angesehen.

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

```
%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
```

Anmerkung: Die Wiederholungserkennung basiert auf der Annahme, dass die IPsec Security Association (SA) nur zwischen zwei Peers existiert. Group Encrypted Transport VPN (GETVPN) verwendet eine einzelne IPsec-SA zwischen mehreren Peers. Aus diesem Grund verwendet GETVPN einen völlig anderen Anti-Replay-Überprüfungsmechanismus, den Time Based Anti-Replay Failure (Time Based Anti-Replay Failure). Dieses Dokument behandelt nur die kontrabasierte Anti-Replay-Funktion für Point-to-Point-IPsec-Tunnel.

Anmerkung: Anti-Replay-Schutz ist ein wichtiger Sicherheitsdienst, den das IPsec-Protokoll bietet. IPsec Anti-Replay deaktiviert hat Sicherheitsauswirkungen und muss mit Diskretion getan werden.

Probleme, die IPsec-Replay-Verluste verursachen können

Wie bereits beschrieben, dienen Wiederholungsprüfungen dem Schutz vor bösartigen Paketwiederholungen. In einigen Fällen kann es jedoch vorkommen, dass eine Wiederholungsprüfung fehlschlägt, wenn dies auf einen bösartigen Grund zurückzuführen ist:

- Der Fehler kann auf ein ausreichendes Paket zurückzuführen sein, das im Netzwerkpfad zwischen den Tunnelendpunkten neu sortiert wird. Dies kann wahrscheinlich auftreten, wenn mehrere Netzwerkpfade zwischen den Peers vorhanden sind.
- Der Fehler kann durch ungleiche Paketverarbeitungswege innerhalb des Cisco IOS verursacht werden. So können beispielsweise fragmentierte IPsec-Pakete, die vor der Entschlüsselung eine IP-Reassemblierung erfordern, verzögert werden, sodass sie bei der Verarbeitung aus dem Replay-Fenster 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 ausgehende Richtung. Bestimmte QoS-Funktionen wie Low Latency Queueing (LLQ) können dazu führen, dass die IPsec-Paketübermittlung aufgrund eines Replay Check-Fehlers außer Betrieb genommen und vom empfangenden Endpunkt verworfen wird.
- Ein Problem mit der Netzwerkkonfiguration/dem Betrieb kann Pakete beim Durchlaufen des Netzwerks duplizieren.
- Ein Angreifer (Man-in-the-Middle) könnte den ESP-Datenverkehr möglicherweise verzögern, verwerfen und duplizieren.

Fehlerbehebung bei IPsec-Replay-Verlusten

Der Schlüssel zur Fehlerbehebung bei Verwerfen von IPsec-Wiederholungen besteht darin, festzustellen, welche Pakete aufgrund von Wiederholungen verworfen werden. Mithilfe von Paketerfassungen kann festgestellt werden, ob diese Pakete tatsächlich wiedergegeben werden oder Pakete, die außerhalb des Wiedergabe-Fensters auf dem empfangenden Router eintreffen. Um die verworfenen Pakete korrekt mit dem abzugleichen, was in der Sniffer-Trace erfasst wird, müssen zuerst der Peer und der IPsec-Fluss identifiziert werden, zu dem die verworfenen Pakete gehören, und die ESP-Sequenznummer des Pakets.

Verwenden der Cisco IOS XE Datapath Packracing-Funktion

Auf Routerplattformen, auf denen Cisco IOS® XE ausgeführt wird, werden Informationen über den Peer sowie den IPsec Security Parameter Index (SPI) in der Syslog-Meldung ausgegeben, wenn ein Datenverlust auftritt, um bei der Behebung von Problemen mit der Wiedergabe zu helfen. 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-Datenflusses eindeutig zu identifizieren. Ohne die Sequenznummer ist es schwierig, genau zu bestimmen, welches Paket bei der Paketerfassung verworfen wird.

In dieser Situation, in der die Wiedergabe-Drop-Funktion mit dieser Syslog-Meldung beobachtet wird, kann die Funktion "Packet-Trace" des Cisco IOS XE-Datenpakets verwendet werden:

```
%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
```

Führen Sie die folgenden Schritte mit der Paketverfolgungsfunktion aus, um die ESP-Sequenznummer für das verworfene Paket zu identifizieren:

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

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

2. Aktivieren Sie die Paket-Ablaufverfolgung mit der **Kopieroption**, um die Paketkopf-Informationen zu kopieren:

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

3. Wenn Fehler bei der erneuten Wiedergabe erkannt werden, verwenden Sie den Paket-Ablaufverfolgungspuffer, um das aufgrund der erneuten Wiedergabe verworfene Paket zu identifizieren. Die ESP-Sequenznummer befindet sich im kopierten Paket:

```
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 werden, sodass sie jetzt im Detail untersucht werden können:

```
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
```

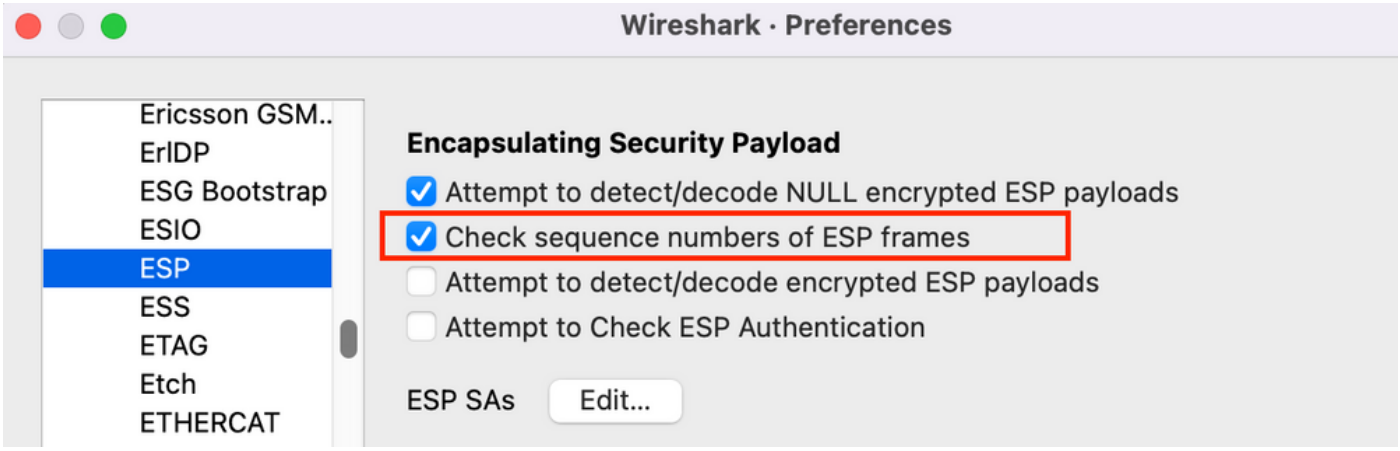
Die ESP-Sequenznummer hat einen Offset von 24 Byte, der vom IP-Header (oder 4 Byte der Payload-Daten des IP-Pakets) beginnt, wie in der vorherigen Ausgabe fett hervorgehoben. In diesem Beispiel lautet die ESP-Sequenznummer für das verworfene Paket 0x6.

Paketerfassung erfassen

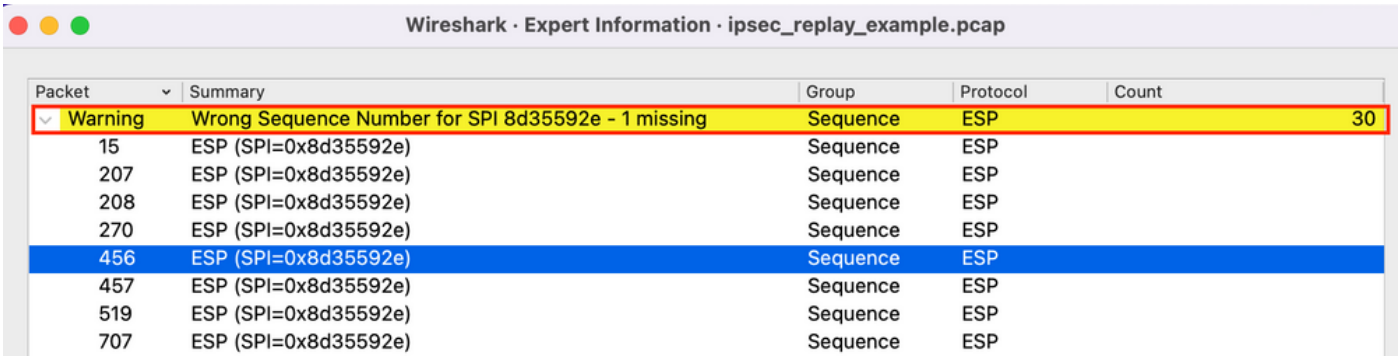
Zusätzlich zur Identifizierung der Paketinformationen für das aufgrund eines Replay-Check-Fehlers verworfene Paket muss eine Paketerfassung für den betreffenden IPsec-Fluss gleichzeitig erfasst werden. Dies hilft bei der Untersuchung des ESP-Sequenzzahlmusters innerhalb desselben IPsec-Datenflusses, um den Grund für den Abbruch der Wiedergabe zu ermitteln. Ausführliche Informationen zur Verwendung der Embedded Packet Capture (EPC) auf Cisco IOS XE-Routern finden Sie unter Konfigurationsbeispiel für die integrierte Paketerfassung für Cisco IOS und Cisco IOS XE.

Wireshark-Sequenzzahlanalyse verwenden

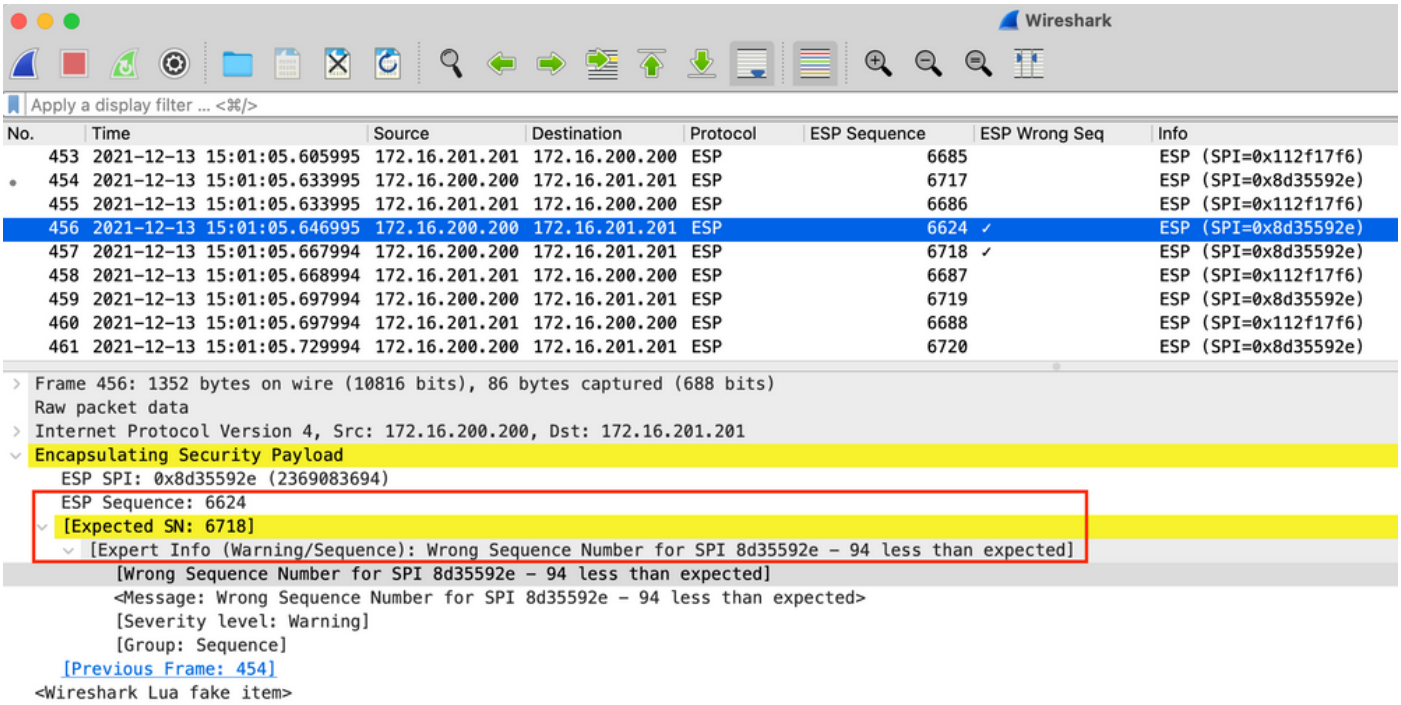
Nachdem die Paketerfassung für die verschlüsselten (ESP-)Pakete auf der WAN-Schnittstelle erfasst wurde, kann Wireshark zur Ausführung einer ESP-Sequenzzahlanalyse für alle Sequenznummern-Anomalien verwendet werden. Stellen Sie zunächst sicher, dass die Überprüfung der Sequenznummer unter **Voreinstellungen > Protokolle > ESP** aktiviert ist, wie im Bild gezeigt:



Prüfen Sie anschließend unter **Analyze > Expert** wie folgt auf Probleme mit ESP-Sequenznummern:



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



Lösung

Nachdem der Peer identifiziert und die Paketerfassung für die Wiederholungsversuche erfasst wurde, können die Wiederholungsfehler in drei möglichen Szenarien erklärt werden:

1. Es handelt sich um ein gültiges Paket, das sich verzögert hat:
   Mithilfe der Paketerfassungen kann überprüft werden, ob das Paket tatsächlich gültig ist und ob das Problem unerheblich ist (aufgrund von Netzwerklatenz oder Problemen mit dem Übertragungspfad) oder eine eingehendere Fehlerbehebung erforderlich ist. Beispielsweise zeigt die Erfassung ein Paket mit der Sequenznummer X an, das in der falschen Reihenfolge ankommt, und die Größe des Replay-Fensters ist derzeit auf 64 festgelegt. Wenn ein gültiges Paket mit einer Sequenznummer (X + 64) vor Paket X eingeht, wird das Fenster nach rechts verschoben und anschließend Paket X aufgrund eines Wiederholfehlers verworfen.

   In solchen Szenarien ist es möglich, die Größe des Replay-Fensters zu erhöhen oder die Replay-Prüfung zu deaktivieren, um sicherzustellen, dass solche Verzögerungen als akzeptabel angesehen werden und die legitimen Pakete nicht verworfen werden. Standardmäßig ist die Größe des Replay-Fensters recht klein (Fenstergröße 64). Wenn Sie die Größe erhöhen, erhöht dies das Risiko eines Angriffs nicht erheblich. Weitere Informationen zum Konfigurieren eines IPsec Anti-Replay-Fensters finden Sie im Fenster Konfigurieren von IPsec Anti-Replay: Erweitern und Deaktivieren von Dokumenten.

   Tipp: Wenn das Replay-Fenster im IPSec-Profil, das auf einer Virtual Tunnel Interface (VTI) verwendet wird, deaktiviert oder geändert ist, werden die Änderungen erst wirksam, wenn das Schutzprofil entfernt und erneut angewendet oder die Tunnelschnittstelle zurückgesetzt wurde. Dieses Verhalten wird erwartet, da IPsec-Profile eine Vorlage sind, die zum Erstellen einer Tunnelprofilzuordnung verwendet wird, wenn die Tunnelschnittstelle aktiviert wird. Wenn die Schnittstelle bereits aktiv ist, wirken sich Änderungen am Profil erst auf den Tunnel aus, wenn die Schnittstelle zurückgesetzt wurde.**Anmerkung:** Die ersten ASR 1000-Modelle (z. B. ASR1000 mit ESP5, ESP10, ESP20 und ESP40 zusammen mit dem ASR1001) unterstützten die Fenstergröße 1024 nicht, obwohl die CLI diese Konfiguration ermöglichte. Infolgedessen ist die Fenstergröße, die in der Ausgabe des Befehls **show crypto ipsec sa** angezeigt wird, möglicherweise nicht korrekt. Verwenden Sie den Befehl **show crypto ipsec als Peer-IP-Adresse-Plattform**, um die Größe des Hardware-Anti-Replay-Fensters zu überprüfen. Die Standard-Fenstergröße 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) Router der Serie 4000 und Catalyst Router der Serie 8000) erfüllen die Anforderungen unterstützt eine Fenstergröße von 1024 Paketen in Version 15.2(2)S und höher.
2. Die Ursache hierfür ist die QoS-Konfiguration auf dem sendenden Endpunkt:
   Diese Situation erfordert eine sorgfältige Prüfung und Abstimmung einiger QoS, um den Zustand abzumildern. Eine ausführliche Beschreibung dieses Themas und einer potenziellen Lösung finden Sie im Artikel Anti-Replay Considerations in a Voice and Video Enabled IPSec VPN (V3PN).

3. Es handelt sich um ein Duplikat des zuvor empfangenen Pakets:
   In diesem Fall 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-Replay-Schutz wie vorgesehen funktioniert, um Wiederholungsangriffe im Netzwerk zu verhindern. Das Syslog dient lediglich als Informationsquelle. Wenn diese Bedingung weiterhin besteht, muss sie als potenzielle Sicherheitsbedrohung untersucht werden.

   Anmerkung: Fehler bei der Wiederholungsprüfung werden nur angezeigt, wenn im IPsec-Transformationssatz ein Authentifizierungsalgorithmus aktiviert ist. Eine andere Möglichkeit, diese Fehlermeldung zu unterdrücken, besteht darin, die Authentifizierung zu deaktivieren und nur die Verschlüsselung auszuführen. Dies wird jedoch aufgrund der Sicherheitsauswirkungen einer deaktivierten Authentifizierung nachdrücklich abgeraten.

Zusätzliche Informationen

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

Die IPsec-Replay-Drops auf den älteren Routern der ISR G2-Serie, die Cisco IOS verwenden, unterscheiden sich von Routern, die Cisco IOS XE verwenden, wie hier gezeigt:

```
%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 die SPI-Informationen bereitstellt. Verwenden Sie zur Fehlerbehebung auf dieser Plattform die "conn-id" in der Fehlermeldung. Identifizieren Sie die "conn-id" in der Fehlermeldung und suchen Sie sie in der **show crypto ipsec als** Ausgabe, da die Wiederholung eine Prüfung pro SA ist (im Gegensatz zu einer Pro-Peer-Prüfung). Die Syslog-Meldung enthält auch die ESP-Sequenznummer, die bei der eindeutigen Identifizierung des in der Paketerfassung verworfenen Pakets helfen kann.

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

Dies wird hier veranschaulicht:

```
%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 der Wiederholungsverlust 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 verworfene Paket 13 lautet. Die Kombination aus Peer-Adresse, SPI-Nummer und ESP-Sequenznummer kann verwendet werden, um das in der Paketerfassung verworfene Paket eindeutig zu identifizieren.

> **Anmerkung:** Die Cisco IOS-Syslog-Meldung ist für das Datenaplane-Paket, das pro Minute auf einen Wert sinkt, ratenlimitiert. Um eine genaue Anzahl der verworfenen Pakete zu erhalten, verwenden Sie den Befehl **show crypto ipsec als Detail**, wie zuvor gezeigt.

Arbeiten mit früherer Cisco IOS XE-Software

Auf Routern, die die früheren Cisco IOS XE-Versionen ausführen, wird der im Syslog gemeldete "REPLAY_ERROR" den tatsächlichen IPsec-Fluss möglicherweise nicht mit den Peer-Informationen drucken, bei denen das wiedergegebene Paket verworfen wird. Dies ist der folgende Beispiel:

```
%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 das in der Syslog-Meldung ausgedruckte Data Plane (DP) Handle als Eingabeparameter SA Handle in diesem Befehl, um die IPsec-Flow-Informationen auf dem Quantum Flow Processor (QFP) abzurufen:

```
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 auch zum Automatisieren 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 gesammelte Ausgabe an den **Bootflash** umgeleitet**.** Um diese Ausgabe anzuzeigen, verwenden Sie den Befehl **more bootflash:replay-error.txt**.

Zugehörige Informationen

- Referenznetzwerk-Design für Sprach- und Videolösungen mit IPSec VPN (V3PN)
- Konfigurieren des IPsec Anti-Replay-Fensters: Erweitern und Deaktivieren.
- Technischer Support und Dokumentation für Cisco Systeme