IPSec アンチ リプレイ チェックの失敗

目次

概要

この資料は問題にインターネット プロトコル セキュリティ（IPSec）再生防止 チェック失敗にかかわる記述し、解決します手順および可能 な 解決策を提供したものです問題を。

> **注:** アンチリプレイ保護は、IPSec プロトコルが提供する重要なセキュリティ サービスです。 IPSec アンチリプレイのディセーブル化はセキュリティに影響するため、注意して使用する必要があります。

背景説明

リプレイ アタックの説明

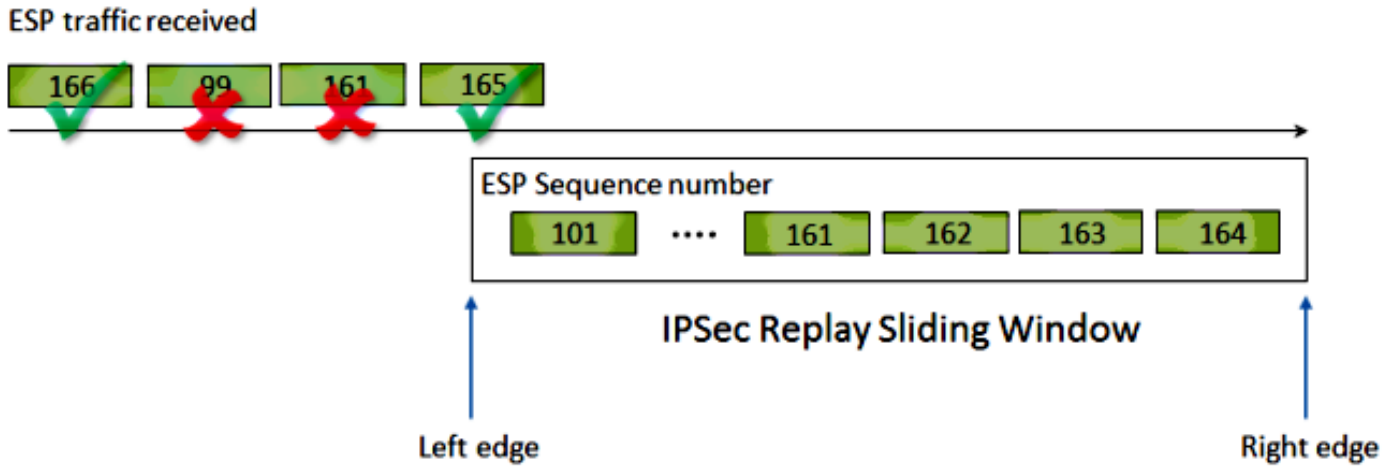
リプレイ アタックは、有効なデータ送信が悪意をもって、または不正に繰り返して返されたり、遅延したりするネットワーク攻撃の一種です。 これは、有効なユーザになりすまして正当な接続を中断したり、その接続に悪影響与えたりするために正当な通信を記録し、それらの通信を繰り返す他者がセキュリティを弱体化させる試みです。

リプレイ チェック障害の説明

IPSec により、それぞれに単調に増加するシーケンス番号を割り当てた暗号化パケットを複製する攻撃者に対するアンチリプレイ保護が提供されます。 受信側の IPsec エンドポイントでは、受け入れ可能なすべてのシーケンス番号のスライディング ウィンドウを使用して、これらの番号に基づいてすでに処理しているパケットを追跡します。 現在、Cisco IOS® 実装のデフォルトのアンチリプレイ ウィンドウ サイズは 64 パケットです。

> **注:** 64 が現代のネットワークのために実際的でなく小さい考慮されると同時に機能拡張要求 CSCva65805 および CSCva65836 は 512 にデフォルト リプレイ ウィンドウ サイズを増加するファイルされました。

これを次の図に示します。



アンチリプレイがイネーブルになっている受信側のトンネル エンドポイントで着信 IPsec トラフィックを処理する手順を次に示します。

1. パケットを受信する際にシーケンス番号がウィンドウ内にあり、以前に受信されなかった場合、パケットは受け入れられ、整合性の確認に送信される前に受信済みとマークされます。

2. シーケンス番号がウィンドウ内にあり、以前に受信した場合、パケットはドロップされ、リプレイのカウンタが増分されます。

3. シーケンス番号がウィンドウで最も大きいシーケンス番号を超える場合、パケットは受け入れられ、受信済みとマークされます。 スライディング ウィンドウが右側に移動します。
   注: これが発生するのは、パケットが有効で、整合性チェックをパスした場合だけです。
4. シーケンス番号がウィンドウで最も小さいシーケンス番号より小さい場合、パケットはドロップされ、リプレイのカウンタが増分されます。

2 番目と 4 番目のシナリオでは、リプレイ チェック障害が発生し、ルータで次のようなエラー メッセージが表示されます。

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

> **注:** Group Encrypted Transport VPN（GETVPN）には、時間ベースのアンチリプレイ障害と呼ばれるまったく異なるアンチリプレイ チェックがあります。 このドキュメントでは、カウンタベースのアンチリプレイのみを取り上げます。

問題

すでに説明したように、リプレイ チェックの目的は、パケットの悪意のある繰り返しから保護することです。 ただし、以下のように失敗したリプレイのチェックが悪意のある理由によるものではない可能性があるシナリオがあります。

- 伝送メディアでのパケット順序の入れ替えによって エラーが発生する可能性があります。 これは特にパラレル パスが存在する場合に当てはまります。

- Cisco IOS 内の不均等なパケット処理パスよって エラーが発生する可能性があります。 たとえば、負荷がかかったシステムでは、大きい IPsec パケットが処理されるまでリプレイ ウィ

ンドウ外にするために、復号化の前に IP 再構成を必要とする大きい IPsec パケットが大幅に遅延する可能性があります。

- エラーは送信 IPsecエンドポイントで有効に なる Quality of Service （ QoS ）によって引き起こされるかもしれません。 Cisco IOS 実装では、出力方向の QoS の前に IPsec 暗号化が行われます。 低遅延キューイング（ LLQ ）などの特定の QoS 機能により、IPSec パケット配信が不正になり、リプレイ チェック障害による受信側のエンドポイントでドロップされる可能性があります。

IPSec リプレイ ドロップのトラブルシューティング

IPSec リプレイ ドロップのトラブルシューティングで重要となるのは、これらのパケットが実際にリプレイされたパケットであるか、リプレイ ウィンドウ外のルータに到着したパケットであるかを確認するために、リプレイによるパケット ドロップを特定し、パケット キャプチャを使用することです。 ドロップされたパケットをスニファ トレースでキャプチャされたものと照合するには、まずドロップされたパケットが属するピアと IPSec フローを特定します。 この手順は、ルータ プラットフォームによって異なります。

Cisco IOS Classic を実行するシスコ サービス統合型ルータ（ ISR ）/ISR G2 プラットフォーム

このプラットフォームでトラブルシューティングを行うには、エラー メッセージで **conn-id** を使用します。 リプレイは **SA ごとの**（セキュリティ アソシエーション）チェック（as opposed to a **ピアごと**とは異なる）であるため、エラー メッセージで **conn-id** を特定し、**show crypto ipsec sa** 出力でそれを探します。 syslog メッセージでも Encapsulating Security Payload （ ESP ）のシーケンス番号が提供され、パケット キャプチャでドロップされたパケットを一意に識別することができます。

> **注:** コードのバージョンによって、**conn-id** は着信 SA の **conn id** または **flow_id** になります。

これを以下に示します。

```
%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>
```

この出力からわかるように、リプレイ ドロップは、0xE7EDE943 のインバウンド方向の ESP SA の Security Parameter Index (SPI) を使用した 10.2.0.200 ピア アドレスによるものです。 また、ログ メッセージ自体からもドロップされたパケットの ESP のシーケンス番号が 13 であることがわかります。 したがって、ピア アドレス、SPI 番号、および ESP の組み合わせを使用して、パケット キャプチャでドロップされたパケットを一意に識別することができます。

> **注:** Cisco IOS Syslog メッセージには、データプレーンのパケット ドロップのレート制限があります。 ドロップされたパケットの実際な数の正確なカウントを取得するには、前に示したように **show crypto ipsec sa detail コマンド**を使用します。 また、宛先のコード Cisco IOS バージョン 12.4(4) T 以前のコードでは、カウンタが正しく更新されない場合があります。 これは、Cisco bug ID CSCsa90034 で修正されています。

Cisco IOS XE を実行する Cisco アグリゲーション サービス ルータ (ASR)

ASR プラットフォームでは、次に示すように、以前の Cisco IOS XE リリースの一部で報告されている REPLAY_ERROR がリプレイされたパケットがドロップされた実際の IPSec フローを出力しない可能性があります。

```
%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>
```

正しい IPSec ピアとフロー情報を特定するには、syslog メッセージに出力されたデータ プレーン（DP）ハンドルをこのコマンドで入力パラメータ SA Handle として使用し、Quantum Flow Processor（QFP）の IPSec フロー情報を取得します。

```
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>
```

ASR の Cisco IOS バージョンが XE バージョン 3.7 以前である場合、エラー メッセージには、**DP ハンドル**を含むメッセージが出力されるだけで、問題となっているパケットが属するピア/SPI に関する情報はありません。 これは、Cisco bug ID CSCtw69096 に関連しています。

```
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>
```

このような場合、次の組み込みイベント マネージャ（EEM）のスクリプトを使用すると、アンチリプレイ メッセージをトリガーするピアおよび SPI を確認できます。

```
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>
```

ASR の出力自体を表示するには、more bootflash:replay-error.txt コマンドを定期的に入力します。

ASR データパスのパケットトレース機能の使用

ASR1000 向けの最新の Cisco IOS XE ソフトウェアでは、アンチリプレイ問題のトラブルシューティングを行うために、IPSec SPI に加え、ピアに関する情報も出力されます。 ただし、ISR G2 プラットフォームで出力される内容と比較した場合に、依然として不足している重要な情報は ESP シーケンス番号です。 ESP のシーケンス番号は、特定の IPSec フロー内で IPsec パケットを一意に識別するのに使用されます。 シーケンス番号がないと、パケット キャプチャでどのパケットがドロップされたかを識別することが困難になります。

Cisco IOS XE バージョン 3.10（15.3(3)S）では、データプレーンのパケット転送のトラブルシューティングを行うために新しいパケット トレース インフラストラクチャが導入されており、このリプレイ ドロップが ASR で発生するこの特定のトラブルシューティング状況でそのインフラストラクチャを使用できます。

```
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>
```

ドロップされたパケットの ESP シーケンス番号を識別するには、パケット トレース機能で次の手順を実行します。

1. ピア デバイスからのトラフィックと照合するためにプラットフォームの条件付きデバッグ フィルタを設定します。

```
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. パケット ヘッダー情報をコピーするために copy option を使用してパケット トレースをイネーブルにします。

```
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. リプレイ エラーが検出されたら、パケット トレース バッファを使用してリプレイによってドロップされたパケットを識別します。コピーされたパケットに ESP シーケンス番号があります。

```
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
```

上記の出力は、パケット番号 6 と 7 がドロップされていることを示すため、これで詳細に調べることができます。

```
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
```

上記の出力でボールドとイタリックで強調されているように、ESP シーケンス番号のオフセットは、IP ヘッダーで始まる 24 です。 この例では、ドロップされたパケットの ESP シーケンス番号は 0x6 です。

解決策

ピアが識別された後、次の 3 つのシナリオが考えられます。

1. **有効なパケットである場合:** パケット キャプチャは、パケットが実際に有効であるか、問題が重大ではないか（ネットワーク遅延または伝送パスの問題による）、またはより詳細なトラブルシューティングが必要であるかを確認するのに役立ちます。 たとえば、キャプチャは、誤った順序で到着する X のシーケンス番号が付いたパケットを示し、ウィンドウ サイズが 64 に設定されています。 パケット X の前には、X + 64 パケットが到着すると、リプレイ障害（実際には攻撃ではありません）が原因でドロップされます。

   このようなシナリオでは、この遅延が考慮されることを確認し、正当なパケットがドロップされないようにリプレイ ウィンドウのサイズを増やします。 デフォルトでは、ウィンドウ サイズは非常に小さくなっています（64 のウィンドウ サイズ）。 サイズを増やしても、攻撃のリスクは大きくなりません。 IPSec アンチリプレイ ウィンドウの設定方法については、IPSec アンチリプレイ ウィンドウの設定方法： 拡張とディセーブルの記事を参照してください。
   ヒント： リプレイ ウィンドウが無効であるか、または IPSec プロファイルおよび IPSec プロファイルで変えられて仮想 な トンネルインターフェイス（VTI）のトンネル 保護と使用されれば、変更は保護 プロファイルがまたはトンネルインターフェイスがリセットされる取除かれか、再適用されるまで実施されません。 これはトンネルインターフェイスが有効に なるとき IPSec プロファイルがトンネル プロファイル マップを作成するちょうどテンプレートであるので予期された動作です（締められない）。 インターフェイスが既にあっていれば、プロファイルへの変更は再適用されるまでのトンネルに影響を与えませんまたはインターフェイスはリセットされます。**注:** アンチリプレイ ウィンドウのサイズに関して ASR でよく発生する問題は、従来の ASR1K モデル（ASR1001 のほか、ESP5、ESP10、ESP20、ESP40 の ASR1K など）で実際に 1024 のウィンドウ サイズをサポートしないことです。 コマンドを使用してこの制限を 1024 に設定できても、ウィンドウ サイズはハー

ドウェアによって 512 にリセットされます。 このため、**show crypto ipsec sa コマンド**の出力でレポートされるウィンドウ サイズは正しくないことがあります。 ハードウェアのアンチリプレイ ウィンドウのサイズを確認するには、**show crypto ipsec sa peer ip-address platform** コマンドを入力します。 デフォルトのウィンドウ サイズは、すべてのプラットフォームで 64 パケットです。 詳細は、Cisco Bug ID CSCso45946 を参照してください。 新しい ASR1K モデル（ESP100 および ESP200 の ASR1K、ASR1001-X、ASR1002-X、ISR-4400 など）のバージョン 15.2(2)S 以降では、1024 パケットのウィンドウ サイズをサポートしています。

2. **受信側のアンチリプレイ ウィンドウ外のパケットである場合:** 受信側の IPsec エンドポイントがリプレイされたパケットをドロップした場合（想定されているように）、この原因が送信側の誤動作または中継ネットワークでリプレイされたパケットであるときは、送信側および受信側の WAN 側の同時スニファ キャプチャが追跡します。

3. **送信側のエンド上の QoS 設定が原因である場合:** この状況では、状況を緩和するために入念に調べ、QoS を調整する必要があります。 このトピックの詳細と考えられる解決策については、Voice and Video Enabled IPSec VPN（V3PN）に関するアンチリプレイの考慮事項を参照してください。

注: リプレイ チェック障害が表示されるのは、IPSec トランスフォーム セットで認証アルゴリズムがイネーブルになっている場合だけです。 このエラー メッセージを抑制するもう 1 つの方法は、認証をディセーブルにして暗号化のみを実行することです。 ただし、これは、ディセーブルにした認証がセキュリティに影響するため、強く推奨しません。

関連情報

- Voice and Video Enabled IPsec VPN（V3PN）ソリューション参照ネットワーク設計
- IPsec アンチリプレイの設定方法： 拡張とディセーブル化
- テクニカルサポートとドキュメント - Cisco Systems