Сбои антипроверки воспроизведения IPSec

Содержание

Введение

Этот документ описывает проблему, которая касается протокола IPSEC (Internet Protocol Security) (IPSec) сбой антипроверки воспроизведения и предоставляет процедуры устранения неполадок и возможные решения к проблеме.

> **Примечание:** Защита Антиответ является важным сервисом безопасности тот Протокол IPSec предложения. Выведение из строя антивоспроизведения IPSec имеет последствия для системы безопасности и должно только использоваться с осторожностью.

Общие сведения

Описание атаки с повторением пакетов

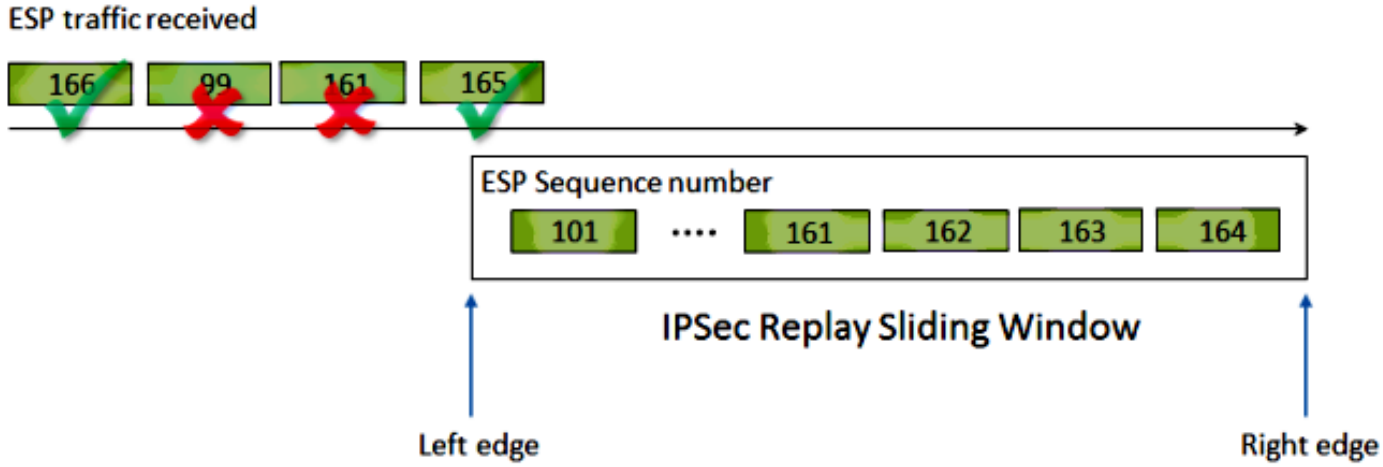
Атака с повторением пакетов является формой сетевой атаки, в которой допустимая передача данных злонамеренно или мошеннически повторена или задержана. Это - попытка ниспровергать безопасность кем-то, кто делает запись легитимной связи и повторяет их для исполнения роли допустимого пользователя, и разрушить или вызвать негативное воздействие для легитимных соединений.

Описание ошибки проверки воспроизведения

IPSec предоставляет защиту Антиответ против атакующего, который копирует зашифрованные пакеты с присвоением монотонно увеличивающегося порядкового номера к каждому зашифрованному пакету. Оконечная точка IPSec получения отслеживает, которых пакетов она уже обработала на основе этих номеров с использованием раздвижного окна всех приемлемых порядковых номеров. В настоящее время размер окна защиты Антиответ по умолчанию в реализации Cisco IOS® является 64 пакетами.

Примечание: Запросы на расширение CSCva65805 и CSCva65836 были поданы для увеличения размера окна воспроизведения по умолчанию до 512 как 64, считают непрактично маленькими для современных сетей.

Это проиллюстрировано на этом рисунке:



Вот шаги для обработки входящего Трафика IPSec на оконечной точке туннеля получения с включенным антивоспроизведением:

1. Когда пакет получен, если порядковый номер находится в пределах окна и не был ранее получен, пакет принят и отмечен, как получено, прежде чем это будет передано проверке целостности.

2. Если порядковый номер находится в пределах окна и был ранее получен, пакет отброшен, и счетчик воспроизведения инкрементно увеличен.

3. Если порядковый номер больше, чем самый высокий порядковый номер в окне, пакет принят и отмечен, как получено. Раздвижное окно тогда перемещено вправо.
   Примечание: Если пакет допустим и передает проверки целостности, это только происходит.
4. Если порядковый номер является меньше, чем самая низкая последовательность в окне, пакет отброшен, и счетчик воспроизведения инкрементно увеличен.

Во вторых и четвертых сценариях происходит сбой проверки воспроизведения, и маршрутизатор отображает сообщение об ошибках, подобное этому:

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

Примечание: У группы Зашифрованная Транспортная VPN (GETVPN) есть совершенно другая антипроверка воспроизведения под названием Время Базирующийся Сбой Антивоспроизведения. Этот документ только покрывает противооснованное антивоспроизведение.

Проблема

Как ранее описано, цель проверок воспроизведения состоит в том, чтобы защитить против

злонамеренных повторений пакетов. Однако существуют некоторые сценарии, где отказавшая проверка воспроизведения не могла бы произойти из-за злонамеренной причины:

- Ошибка могла бы следовать из пакетного переупорядочивания в средстве передачи. Если параллельные пути существуют, это особенно истинно.

- Ошибка могла бы быть вызвана неравным пакетом, обрабатывающим пути в Cisco IOS. Например, большие Пакеты ipsec, которые требуют повторной сборки IP перед расшифровкой, могли бы быть задержаны достаточно, в системе под загрузкой, для падения за пределами окна воспроизведения к тому времени, когда они обработаны.

- Ошибка могла бы быть вызвана Качеством обслуживания (QoS), включенным на Оконечной точке IPSec передачи. С реализацией Cisco IOS IP - безопасное шифрование происходит перед QoS в выходном направлении. Определенные Характеристики QoS, такие как очереди с низкой задержкой (LLQ), могут заставить доставку Пакета ipsec становиться неисправной и отброшенной оконечной точкой получения из-за сбоя проверки воспроизведения.

Отбрасывания воспроизведения IPSec устранения неполадок

Ключ для устранения проблем отбрасываний воспроизведения IPSec должен определить отбрасывание пакета, должное воспроизводить, и использовать захваты пакета, чтобы подтвердить, являются ли эти пакеты действительно воспроизводимыми пакетами или пакетами, которые поступили в принимающий маршрутизатор за пределами окна воспроизведения. Для корректного соответствия с отброшенными пакетами к тому, что перехвачено в отслеживании средств прослушивания, первый шаг должен определить узел и поток IPSec, которому принадлежат отброшенные пакеты. Это сделано по-другому на основе платформы маршрутизатора.

Cisco ISR (ISR) / ISR Платформа G2, который Классика Cisco IOS Выполнений

Для устранения проблем на этой платформе используйте **conn-id** в сообщении об ошибках. Определите **conn-id** в сообщении об ошибках и ищите его в **выходных данных show crypto ipsec sa**, так как воспроизведение является **на SA** (Сопоставление безопасности) проверка (в противоположность **на узел**). Сообщение системного журнала также предоставляет порядковый номер Безопасного закрытия полезной нагрузки (ESP), который может помочь однозначно определять отброшенный пакет в захвате пакета.

> **Примечание:** С другими версиями кода **conn-id** является или **conn id** или **flow_id** для входящего SA.

Это проиллюстрировано здесь:

```
%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>
```

Как видно из этих выходных данных отбрасывание воспроизведения от **10.2.0.200** адресов партнера (peer) с входящим индексом параметров безопасности (SPI) ESP SA **0xE7EDE943**. Можно также обратить внимание от самого сообщения журнала, что Порядковый номер ESP для отброшенного пакета равняется **13**. Так, комбинация адреса партнера (peer), номера SPI и Порядкового номера ESP может использоваться для однозначного определения пакета, заглядывал захвату пакета.

> **Примечание:** Сообщение системного журнала Cisco IOS с ограниченной скоростью для dataplane отбрасывания пакета. Для получения точного количества точного номера отброшенных пакетов используйте **подробную** команду **show crypto ipsec sa** как показано ранее. Кроме того, обратите внимание в коде ранее, чем версия Cisco IOS 12.4 (4) T, счетчики могли бы быть обновлены неправильно. Это исправлено в идентификаторе ошибки Cisco CSCsa90034.

Маршрутизатор агрегации (ASR) Cisco, который Cisco IOS XE Выполнений

На платформе ASR REPLAY_ERROR, о котором сообщают в некоторых более ранних версиях Cisco IOS XE, не мог бы распечатать фактический поток IPSec, где воспроизводимый пакет отброшен, как показано здесь:

```
%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>
```

Для определения корректного Узла IPsec и сведений о потоках, используйте Маркер Плоскости данных (DP), распечатанный в сообщении системного журнала как **Маркер SA** параметра ввода в этой команде для получения сведений о потоках IPSec на процессоре Quantum Flow (QFP):

```
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>
```

Если версией Cisco IOS на ASR является Версия 3.7 предXE, то сообщение об ошибках просто регистрирует сообщение с **Маркером DP** и никакой информацией об узле/SPI, которому принадлежит пакет преступника. Это - то, где идентификатор ошибки Cisco CSCtw69096 становится релевантным:

```
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>
```

В таких случаях этот сценарий встроенного диспетчера событий (EEM) может использоваться для наблюдения, какой узел и SPI инициируют сообщения антивоспроизведения:

```
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>
```

Для наблюдения выходных данных на самом ASR вводите **больше bootflash:replay-error.txt** команды периодически.

Работайте с пакетной функцией отслеживания канала передачи данных ASR

С более свежим программным обеспечением Cisco IOS XE для ASR1000 также распечатана информация об узле, а также SPI IPSec, чтобы помочь устранять проблемы антивоспроизведения. Однако одной важной частью информации, которая все еще отсутствует по сравнению с тем, что распечатано на платформах ISR G2, которые выполняют классику Cisco IOS, является Порядковый номер ESP. Порядковый номер ESP используется для однозначного определения Пакета ipsec в данном потоке IPSec. Без порядкового номера становится трудным определить точно, какому пакету заглядывают захват пакета.

В Версии 3.10 Cisco IOS XE (15.3 (3) S), новая пакетная инфраструктура отслеживания была представлена, чтобы помочь решать dataplane проблему пересылки пакетов, и она может использоваться в этом определенном состоянии устранения проблем, где это отбрасывание воспроизведения наблюдается относительно ASR:

```
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>
```

Чтобы помочь определять Порядковый номер ESP для отброшенного пакета, выполните эти шаги с пакетной функцией отслеживания:

1. Установите фильтр условной отладки платформы для соответствия с трафиком от однорангового устройства:

```
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. Включите пакетное отслеживание с **параметром копирования** для копирования информации о заголовке пакета:

```
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. То, когда ошибки воспроизведения обнаружены, используйте буфер трассировки пакетов, для определения пакета понизилось должный воспроизвести, и Порядковый номер ESP может быть найден в скопированном пакете:

```
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
```

Предыдущие выходные данные показывают, что пакет **номера 6 и 7** отброшен, таким образом, они могут быть исследованы подробно теперь:

```
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
```

Порядковый номер ESP имеет смещение **24**, который запускается с IP - заголовка, как подчеркнуто полужирным и курсива в предыдущих выходных данных. В этом конкретном примере Порядковый номер ESP для отброшенного пакета является **0x6**.

Решение

После того, как узел определен, существует три возможных сценария:

1. **Это - Допустимый пакет:** Захваты пакета помогают подтверждать, фактически допустим ли пакет, и если проблема незначительна (из-за задержки сети или проблем пути передачи) или требует более всестороннего устранения неполадок. Например, перехват показывает пакет с порядковым номером **X**, который поступает не в порядке, и размер окна установлен в **64**. Если **X + 64** пакета поступают перед пакетом **X**, то он отброшен из-за сбоя воспроизведения (это не действительно атака).

   В таких сценариях увеличьте размер окна воспроизведения, чтобы гарантировать, что

такие задержки составляются и препятствуют тому, чтобы были отброшены легитимные пакеты. По умолчанию размер окна является довольно маленьким (размер окна **64**). При увеличении размера он не значительно увеличивает риск атаки. Для получения информации о том, как настроить Окно защиты Антиответ IPsec, обратитесь к, Как Настроить Окно защиты Антиответ IPsec: статья Expanding и Disabling.
Совет: Если окно воспроизведения будет отключено или изменено в Профиле IPSEC, и Профиль IPSEC используется с tunnel protection в Виртуальном туннельном интерфейсе (VTI), то изменения не вступят в силу, пока профиль защиты или не удален и повторно применен или туннельный интерфейс, перезагружен. Это - нормальное поведение, потому что Профили IPSEC являются просто шаблоном для создания туннельной карты профиля, когда туннельный интерфейс включен (не закрытый). Как только интерфейс подключен уже, изменения к профилю не влияют на туннель, пока не повторно применено, или интерфейс перезагружен.**Примечание:** Обычно возникшая проблема на ASR, относительно размера окна защиты Антиответ, состоит в том, что классические модели ASR1K (такие как ASR1K с ESP5, ESP10, ESP20 и ESP40, наряду с ASR1001) фактически не поддерживают размер окна 1024. Даже при том, что команда позволяет вам устанавливать этот предел к 1024, размер окна перезагружен к 512 аппаратными средствами. Из-за этого размер окна, о котором сообщают в выходных данных **команды show crypto ipsec sa** , не мог бы быть корректным. Введите команду **платформы IP - адреса адресуемого точки show crypto ipsec sa** для проверки аппаратного размера окна защиты Антиответ. Стандартный размер окна является 64 пакетами на всех платформах. Для получения дополнительной информации обратитесь к идентификатору ошибки Cisco CSCso45946. Более новые модели ASR1K (такие как ASR1K с ESP100 и ESP200, ASR1001-X и ASR1002-X, и также ISR 4400) действительно поддерживают размер окна 1024 пакетов в Версиях 15.2 (2) S и позже.
2. **Это - пакет, который падает за пределами окна защиты Антиответ получателя:** В случае, если Оконечная точка IPSec получения отбрасывает воспроизводимые пакеты (как она предполагается к), одновременные перехваты анализатора на Стороне WAN и отправителя и получателя помогают отнести дорожку, если это вызвано неверным поведением отправителя, или пакетами, воспроизводимыми в транзитной сети.

3. **Это происходит из-за конфигурации QoS на конце отправителя:** Эта ситуация требует тщательного изучения и некоторой настройки QoS для смягчения условия. Для более всестороннего описания этой темы и возможного решения, обратитесь к Факторам Антивоспроизведения в статье Voice и Video Enabled IPSec VPN (V3PN).

Примечание: Когда алгоритм аутентификации включен в Команде IPsec transform set, сбои проверки воспроизведения только замечены. Другой способ подавить это сообщение об ошибках состоит в том, чтобы отключить аутентификацию и выполнить шифрование только; однако, этому строго обескураживают из-за последствий для системы безопасности отключенной аутентификации.

Дополнительные сведения

- Голос и видео включили IPSEC VPN (V3PN) ссылочная организация сети решения

- Как настроить окно защиты Антиответ IPsec: расширение и отключение.
- Cisco Systems – техническая поддержка и документация