Falhas da verificação da Anti-repetição do IPsec

Índice

Introdução

Este documento descreve um problema que se refira a uma falha da verificação da anti-repetição da segurança de protocolo do Internet (IPsec), e fornece-o pesquisa defeitos procedimentos e soluções possíveis ao problema.

> Nota: A proteção anti-replay é um serviço de segurança importante que o protocolo IPSec ofereça. A incapacidade da anti-repetição do IPsec tem implicações de segurança, e deve somente ser usada com cuidado.

Informações de Apoio

Descrição do ataque de replay

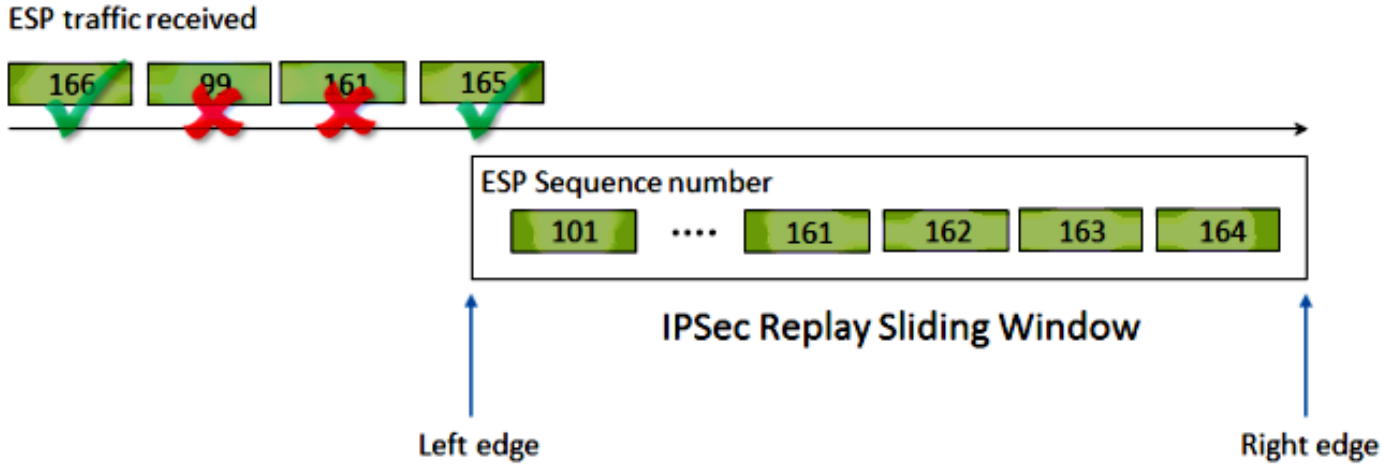
Um ataque de replay é um formulário do ataque de rede em que uma transmissão de dados válida é repetida maliciosamente ou fraudulentamente ou atrasa. É uma tentativa de subverter a Segurança por alguém que grava comunicações legítimas e as repete a fim encarnar um usuário válido, e interromper ou causar o impacto negativo para conexões legítimas.

Descrição da falha da verificação da repetição

O IPsec fornece a proteção anti-replay contra um atacante que duplique pacotes criptografado com a atribuição de um número de sequência monotonically crescente a cada pacote criptografado. O ponto final de IPSec de recepção mantém-se a par que os pacotes ele têm processado já com base nestes números com o uso de um indicador de deslizamento de todos os números de sequência aceitáveis. Atualmente, o tamanho da janela anti-resposta do padrão na aplicação do ® do Cisco IOS é 64 pacotes.

Nota: As requisições de aprimoramento CSCva65805 e CSCva65836 estiveram arquivadas aumentar o tamanho de janela da repetição do padrão a 512 enquanto 64 são considerados pouco pràtica pequenos para redes de modem.

Isto é ilustrado nesta figura:



Estão aqui as etapas para processar o tráfego de IPSec entrante que recebe no ponto final de túnel com a anti-repetição permitida:

1. Quando um pacote está recebido, se o número de sequência cai dentro do indicador e não esteve recebido previamente, o pacote está aceitado, e marcado como recebido antes que esteja enviado à verificação da integridade.

2. Se o número de sequência cai dentro do indicador e foi recebido previamente, o pacote está deixado cair, e o contador da repetição é incrementado.

3. Se o número de sequência é maior do que o número de sequência o mais alto no indicador, o pacote está aceitado, e marcado como recebido. O indicador de deslizamento é movido então para a direita.
   Nota: Isto somente ocorre se o pacote é válido e passa verificações de integridade.
4. Se o número de sequência é menos do que a mais baixa sequência no indicador, o pacote está deixado cair, e o contador da repetição é incrementado.

Nas segundas e quartas encenações, uma falha da verificação da repetição ocorre, e o roteador indica um Mensagem de Erro similar a este:

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

Nota: O transporte cifrado grupo VPN (GETVPN) tem uma falha baseada totalmente diferente da Anti-repetição do tempo chamado da verificação da anti-repetição. Este documento cobre somente a anti-repetição contador-baseada.

Problema

Como descrito anteriormente, a finalidade de verificações da repetição é proteger contra repetições maliciosas dos pacotes. Contudo, há algumas encenações onde uma verificação

falhada da repetição não pôde ser devido a uma razão maliciosa:

- O erro pôde resultar de um pacote requisita novamente no meio de transmissão. Isto é especialmente verdadeiro se os caminhos paralelos existem.
- O erro pôde ser causado por trajetos de processamento desiguais do pacote dentro do Cisco IOS. Por exemplo, grandes pacotes de IPsec que exigem a remontagem IP antes que a descriptografia puder ser atrasada bastante, em um sistema sob a carga, a fim cair fora do indicador da repetição antes que forem processados.
- O erro pôde ser causado pelo Qualidade de Serviço (QoS) permitido no ponto final de IPSec de emissão. Com o Cisco IOS aplicação, a criptografia IPSec acontece antes de QoS na direção de saída. Determinadas características de QoS, tais como o low latency queueing (LLQ), podem fazer com que a entrega do pacote de IPsec torne-se fora de serviço e deixada cair pelo valor-limite de recepção devido a uma falha da verificação da repetição.

Pesquise defeitos gotas da repetição do IPsec

A chave para pesquisar defeitos gotas da repetição do IPsec é identificar as quedas de pacote de informação devido à repetição, e capturas de pacote de informação do uso a fim confirmar se estes pacotes são certamente os pacotes replayed ou os pacotes que chegaram no roteador de recepção fora do indicador da repetição. A fim combinar corretamente os pacotes descartado ao que é capturado no farejador de rastreamento, a primeira etapa é identificar o par e o fluxo do IPsec a que os pacotes descartado pertencem. Isto é feito diferentemente baseou na plataforma de roteador.

Plataforma do roteador dos Serviços integrados de Cisco (ISR) /ISR G2 que executa o Cisco IOS clássico

A fim pesquisar defeitos nesta plataforma, use a CONN-**identificação no** Mensagem de Erro. Identifique a CONN-**identificação no** Mensagem de Erro, e procure-a na saída **cripto IPsec sa da mostra**, desde que a repetição é (associação de segurança) uma verificação por-**SA** (ao contrário de um por-**par**). O mensagem do syslog igualmente fornece o número de sequência do Encapsulating Security Payload (ESP), que pode ajudar excepcionalmente a identificar o pacote descartado na captura de pacote de informação.

> Nota: Com versões de código diferentes, a CONN-**identificação** é a **identificação conexão** ou **flow_id** para o SA de entrada.

Isto é ilustrado aqui:

```
%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>
```

Como pode ser visto desta saída, a gota da repetição é do endereço de peer de **10.2.0.200** com um Security Parameter Index de entrada ESP SA (SPI) de **0xE7EDE943**. Pode-se igualmente notar do mensagem de registro próprio que o número de sequência ESP para o pacote descartado é **13**. Assim, a combinação de endereço de peer, de número SPI, e do número de sequência ESP pode ser usada a fim identificar excepcionalmente o pacote deixado cair na captura de pacote de informação.

> Nota: O mensagem do syslog do Cisco IOS é limite de taxa para quedas de pacote de informação do dataplane. A fim obter uma contagem exata do número exato de pacotes deixou cair, usa o **comando show crypto ipsec sa detail** como mostrado previamente. Também, a nota no código mais cedo do que a versão do Cisco IOS 12.4(4)T, os contadores pôde ser atualizada incorretamente. Isto é fixado na identificação de bug Cisco CSCsa90034.

A agregação de Cisco presta serviços de manutenção ao roteador (ASR) esse Cisco IOS XE das corridas

Na plataforma ASR, o REPLAY_ERROR relatado em algumas das liberações mais adiantadas do Cisco IOS XE não pôde imprimir o fluxo real do IPsec onde o pacote replayed é deixado cair, como mostrado aqui:

```
%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>
```

A fim identificar o ipsec peer e a informação de fluxo corretos, use o punho do plano dos dados (DP) impresso no mensagem do syslog como o punho parâmetro de entrada SA neste comando a fim recuperar a informação de fluxo do IPsec no processador do fluxo do quantum (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>
```

Se a versão do Cisco IOS no ASR é a versão 3.7 PRE-XE, a seguir o Mensagem de Erro registra simplesmente a mensagem com **punho DP** e nenhuma informação sobre o peer/SPI a que o pacote do culpado pertence. Isto é o lugar onde a identificação de bug Cisco CSCtw69096 se torna relevante:

```
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>
```

Nesses casos, este script encaixado do gerente do evento (EEM) pode ser usado a fim ver que par e SPI provoca as mensagens da anti-repetição:

```
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>
```

A fim ver a saída no ASR própria, entre em **mais bootflash: comando replay-error.txt** periodicamente.

Trabalho com a característica de seguimento do pacote ASR Datapath

Com o Software Cisco IOS XE mais recente para o ASR1000, a informação sobre o par assim como o IPsec SPI são imprimidos igualmente a fim ajudar a pesquisar defeitos problemas da anti-repetição. Contudo, uma parte principal de informação que é ainda faltar comparada ao que é imprimido nas Plataformas ISR G2 que executam o clássico do Cisco IOS é o número de sequência ESP. O número de sequência ESP é usado a fim identificar excepcionalmente um pacote de IPsec dentro de um fluxo dado do IPsec. Sem o número de sequência, torna-se difícil identificar exatamente que o pacote obtém deixado cair em uma captura de pacote de informação.

Na versão 3.10 do Cisco IOS XE (15.3(3)S), uma infraestrutura de seguimento do pacote novo foi introduzida a fim ajudar a pesquisar defeitos a edição do encaminhamento de pacote do dataplane, e pode ser usada nesta situação de Troubleshooting particular onde esta gota da repetição é observada no 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>
```

A fim ajudar a identificar o número de sequência ESP para o pacote deixou cair, termina estas etapas com a característica de seguimento do pacote:

1. Estabelecer o filtro do debugging condicional da plataforma a fim combinar o tráfego do dispositivo de peer:

```
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. Permita o pacote que segue com a **opção de cópia** a fim copiar a informação de cabeçalho de pacote de informação:

```
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. Quando os erros da repetição são detectados, use o buffer do rastreamento de pacotes a fim identificar o deixado cair pacote devido à repetição, e o número de sequência ESP pode ser encontrado no pacote copiado:

```
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
```

A saída precedente mostra que os números **6** e **7 do** pacote estão deixados cair, assim que podem ser examinados em detalhe agora:

```
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
```

O número de sequência ESP tem um offset de **24** que parta do cabeçalho IP, como sublinhado em corajoso e em itálicos na saída precedente. Neste exemplo particular, o número de sequência ESP para o pacote descartado é **0x6**.

Solução

Depois que o par é identificado, há três cenários possíveis:

1. **É um pacote válido:** As capturas de pacote de informação ajudam a confirmar se o pacote é realmente válido, e se o problema é insignificante (devido às edições da latência da rede ou do caminho de transmissão) ou exige um mais detalhado pesquisa defeitos. Por exemplo, a captação mostra um pacote com um número de sequência de **X** que chega fora de serviço, e o tamanho de janela é ajustado a **64**. Se **X + 64** pacotes chega antes do pacote **X**, a seguir obtém deixado cair devido a uma falha da repetição (não é realmente um ataque).

   Em tais encenações, aumente o tamanho do indicador da repetição a fim assegurar-se de que tais atrasos estejam esclarecidos e impedir que os pacotes legítimos estejam deixados cair. À revelia, o tamanho de janela é razoavelmente pequeno (um tamanho de janela de **64**). Se você aumenta o tamanho, não aumenta extremamente o risco de um ataque. Para obter informações sobre de como configurar uma janela anti-resposta do IPsec, refira como configurar a janela anti-resposta do IPsec: Artigo de expansão e de desabilitação.

Dica: Se o indicador da repetição está desabilitado ou alterado no perfil IPSec e no perfil IPSec está usado com proteção do túnel em uma interface de túnel virtual (VTI), as mudanças não tomarão o efeito até que o perfil da proteção ou esteja removido e reaplicado ou a interface de túnel estiver restaurada. Este é comportamento esperado porque os perfis IPSec são apenas um molde para criar o mapa do perfil do túnel quando a interface de túnel é permitida (não fechado). Uma vez que a relação é já acima, as mudanças ao perfil não impactam o túnel até reaplicado ou a relação é restaurada.Nota: Um problema geralmente encontrado em ASR, no que diz respeito ao tamanho da janela anti-resposta, é que os modelos clássicos ASR1K (tais como o ASR1K com ESP5, ESP10, ESP20, e ESP40, junto com o ASR1001) não apoiam realmente um tamanho de janela de 1024. Mesmo que o comando permita que você ajuste este limite a 1024, o tamanho de janela é restaurado a 512 pelo hardware. Devido a isto, o tamanho de janela que é relatado na saída do **comando show crypto ipsec sa** não pôde estar correto. Incorpore o comando **cripto da plataforma do endereço IP do peer IPsec sa da mostra** a fim verificar o tamanho da janela anti-resposta do hardware. O tamanho de janela padrão é 64 pacotes em todas as Plataformas. Para mais informação, refira a identificação de bug Cisco CSCso45946. Uns modelos mais novos ASR1K (tais como o ASR1K com ESP100 e ESP200, o ASR1001-X e o ASR1002-X, e igualmente o ISR-4400) apoiam um tamanho de janela de 1024 pacotes nas versões 15.2(2)S e mais recente.

2. **É um pacote que caia fora da janela anti-resposta do receptor:** Caso que o ponto final de IPSec de recepção deixa cair os pacotes replayed (enquanto se supõe a), o sniffer simultâneo captura no lado WAN do remetente e da ajuda do receptor para seguir para baixo se este é causado pelo comportamento inadequado do remetente, ou por pacotes replayed no transit network.

3. **É devido à configuração de QoS na extremidade do remetente:** Esta situação exige o exame cuidadoso e algum o QoS que ajustam a fim abrandar a circunstância. Para uma descrição mais detalhada deste assunto e de uma solução potencial, refira as considerações da Anti-repetição em uma Voz e em um artigo permitido vídeo do IPSec VPN (V3PN).

Nota: As falhas da verificação da repetição são consideradas somente quando um algoritmo de autenticação é permitido no IPsec transforma o grupo. Uma outra maneira de suprimir este Mensagem de Erro é desabilitar a autenticação e executar a criptografia somente; contudo, este é fortemente desanimado devido às implicações de segurança da autenticação deficiente.

Informações Relacionadas

- **A Voz e o vídeo permitiram o projeto de rede da referência da solução do IPSec VPN (V3PN)**
- **Como configurar a janela anti-resposta do IPsec:** Expansão e desabilitação.
- **Suporte Técnico e Documentação - Cisco Systems**