Solucionar problemas de falhas de antireprodução de IPsec de borda SD-WAN

Contents

Introduction

Este documento descreve o comportamento antirrepetição de IPsec em roteadores SD-WAN IPsec para bordas e como solucionar problemas de antirrepetição.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Segurança de Protocolo Internet (IPsec)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C8000V Versão 17.06.01
- ASR1001-X Versão 17.06.03a
- vManage versão 20.7.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A autenticação IPsec fornece proteção antirreprodução integrada contra pacotes IPsec antigos ou duplicados com o número de sequência no cabeçalho ESP verificado no receptor. As quedas de pacotes de antirreprodução são um dos problemas de plano de dados mais comuns com o IPsec devido a pacotes entregues fora de ordem fora da janela de antirreprodução. Uma abordagem geral de solução de problemas para quedas de antirreprodução IPsec pode ser encontrada em IPsec Anti Replay Check Failures, e a técnica geral também se aplica a SD-WAN. No entanto, existem algumas diferenças de implementação entre o IPsec tradicional e o IPsec usado na solução SD-WAN da Cisco. O objetivo deste artigo é explicar essas diferenças e a abordagem nas plataformas cEdge com o Cisco IOS ®XE.

Considerações sobre a detecção de reprodução de SD-WAN

Chave de Grupo vs. Chave Pairwise

Diferentemente do IPsec tradicional, onde as SAs IPsec são negociadas entre dois peers com o uso do protocolo IKE, a SD-WAN usa um conceito de chave de grupo. Neste modelo, um dispositivo de borda SD-WAN gera periodicamente SA de entrada do plano de dados por TLOC e envia essas SAs para o controlador vSmart, que, por sua vez, propaga a SA para o restante dos dispositivos de borda na rede SD-WAN. Para obter uma descrição mais detalhada das operações do plano de dados da SD-WAN, consulte Visão geral da segurança do plano de dados da SD-WAN.

> **Observação**: desde o Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2, há suporte para chaves IPsec em pares. Consulte Visão Geral das Teclas de Interpolação IPsec. Com as teclas Pairwise, a proteção antirreprodução IPsec funciona exatamente como o IPsec tradicional. Este artigo concentra-se principalmente na verificação de repetição com o uso do modelo de chave de grupo.

SPI codificado

No cabeçalho ESP do IPsec, o SPI (Security Parameter Index) é um valor de 32 bits que o receptor usa para identificar a AS com a qual um pacote de entrada é descriptografado. Com a SD-WAN, esse SPI de entrada pode ser identificado com **show crypto ipsec sa**:

```
cedge-2#show crypto ipsec sa | se inbound
     inbound esp sas:
      spi: 0x123(291)
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2083, flow_id: CSR:83, sibling_flags FFFFFFFF80000008, crypto map: Tunnel1-
vesen-head-0
        sa timing: remaining key lifetime 9410 days, 4 hours, 6 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Observação: embora o SPI de entrada seja o mesmo para todos os túneis, o receptor tem um SA diferente e o objeto de janela de repetição correspondente associado ao SA para cada dispositivo de borda de peer, já que o SA é identificado pela origem, endereço IP de destino, origem, portas de destino 4-tupla e o número SPI. Essencialmente, cada par tem seu próprio objeto de janela antirreprodução.

No pacote real enviado pelo dispositivo par, observe que o valor SPI é diferente da saída anterior. Aqui está um exemplo da saída do packet-trace com a opção de cópia de pacote ativada:

```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

O SPI real no cabeçalho ESP é **0x04000123.** A razão para isso é que os primeiros bits no SPI para SD-WAN são codificados com informações adicionais e apenas os bits baixos do campo SPI são alocados para o SPI real.

IPsec tradicional:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SD-WAN:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  CTR  | MSNS|         Security Parameters Index (SPI)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- **CTR** (primeiros 4 bits, bits 0-3) - Bits de controle, usados para indicar o tipo específico de pacotes de controle. Por exemplo, o bit de controle 0x80000000 é usado para BFD.
- **MSNS** (próximos 3 bits, bits 4-6) - Índice de Espaço de Número de Sequência Múltipla. Isso é usado para localizar o contador de sequência correto na matriz de contadores de sequência para verificar a reprodução do pacote fornecido. Para SD-WAN, o 3-bit de MSNS permite que 8 classes de tráfego diferentes sejam mapeadas em seu próprio espaço de número de sequência. Isso implica que o valor SPI efetivo que pode ser usado para a seleção de SA é a ordem reduzida de 25 bits do valor completo de 32 bits do campo.

Espaço de número de sequência múltiplo para QoS

Écomum observar falhas de repetição de IPsec em um ambiente onde os pacotes são entregues fora de ordem devido à QoS, por exemplo, LLQ, já que a QoS é sempre executada após a criptografia e o encapsulamento de IPsec. A solução Multiple Sequence Number Space resolve esse problema com o uso de vários espaços de números de sequência mapeados para diferentes classes de tráfego de QoS para uma determinada associação de segurança. O espaço de número de sequência diferente é indexado pelos bits do MSNS codificados no campo SPI do

pacote ESP, conforme descrito. Para obter uma descrição mais detalhada, consulte Mecanismo antirreprodução IPsec para QoS.

Como observado anteriormente, essa implementação do Multiple Sequence Number implica que o valor SPI efetivo que pode ser usado para a seleção de SA é a ordem reduzida de 25 bits. Outra consideração prática quando o tamanho da janela de repetição é configurado com esta implementação é que o tamanho da janela de repetição configurada é para a janela de repetição agregada, portanto, o tamanho efetivo da janela de repetição para cada Espaço de Número de Sequência é 1/8 do agregado.

Exemplo de configuração:

```
config-t
Security
IPsec
replay-window 1024
Commit
```

> **Observação**: O tamanho da janela de repetição efetiva para cada Espaço de Número de Sequência é 1024/8 = 128!

> **Observação**: desde o Cisco IOS ®XE. 17.2.1, o tamanho da janela de repetição agregada foi aumentado para 8192 de modo que cada Espaço do Número de Sequência possa ter uma janela de repetição máxima de 8192/8 = 1024 pacotes.

Em um dispositivo cEdge, o último número de sequência recebido para cada espaço de número de sequência pode ser obtido da saída do dataplane IPsec **show crypto ipsec sa peer x.x.x.x platform**:

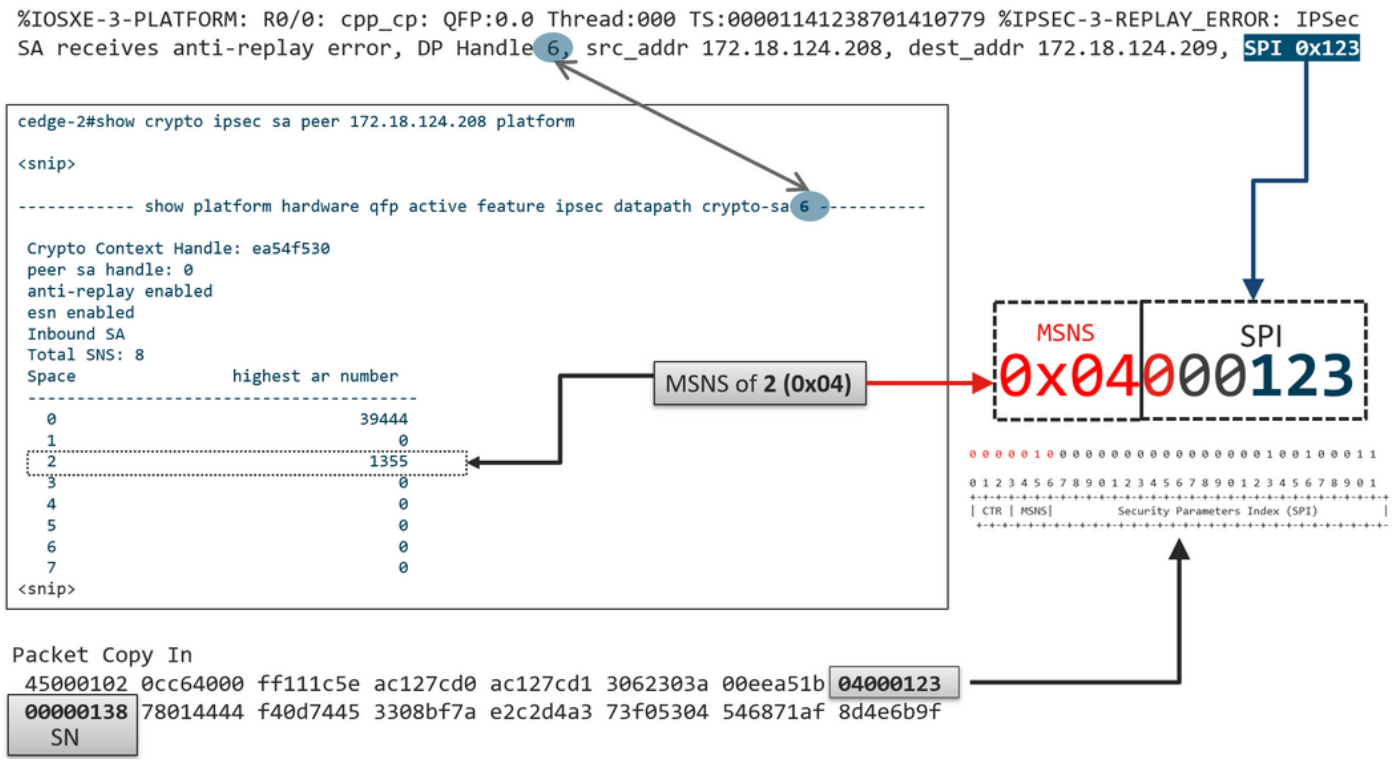
```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<snip>

------------------ show platform hardware qfp active feature ipsec datapath crypto-sa 5 --------
----------

 Crypto Context Handle: ea54f530
 peer sa handle: 0
 anti-replay enabled
 esn enabled
 Inbound SA
 Total SNS: 8
 Space                 highest ar number
 ----------------------------------------
   0                                39444
   1                                    0
   2                                 1355
   3                                    0
   4                                    0
   5                                    0
   6                                    0
   7                                    0
<snip>
```

No exemplo, a maior janela antirreprodução (Borda direita da janela móvel antirreprodução) para MSNS de 0 **(0x00)** é **3944**, e para MSNS de **2 (0x04)** é **1335**, e esses contadores são usados

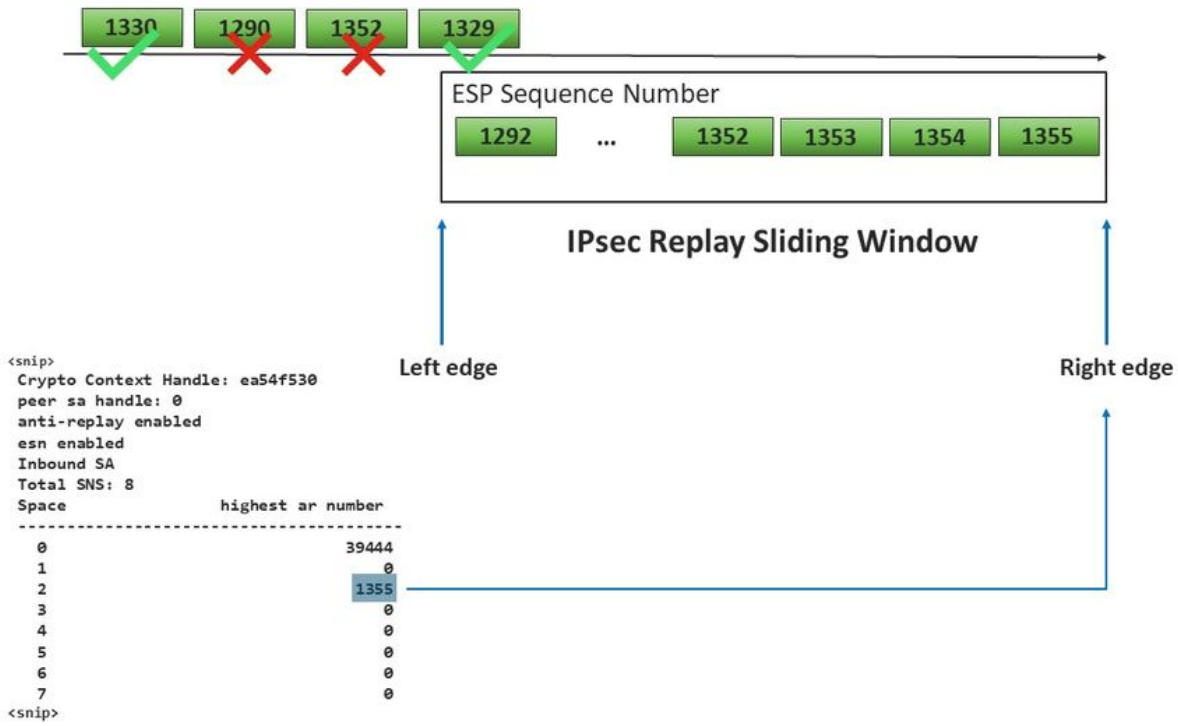
para verificar se o número de sequência está dentro da janela de repetição para pacotes no mesmo espaço de número de sequência.

> **Observação**: há diferenças de implementação entre a plataforma ASR1k e o resto das plataformas de roteamento Cisco IOS ®XE (ISR4k, ISR1k, CSR1kv). Como resultado, há algumas discrepâncias em termos dos comandos show e sua saída para essas plataformas.

Épossível correlacionar os erros Anti-Replay e as saídas show para encontrar o SPI e o índice do número de sequência como mostrado na imagem.



Com as informações anteriores obtidas, a borda direita (janela superior) e a janela deslizante se parecem com a imagem.



Comandos para a Eficácia da Janela de Repetição Configurada

Ao contrário do IPsec normal (não SD-WAN), o comando rekey não tem efeito para a janela anti replay.

```
request platform software sdwan security ipsec-rekey
```

Estes comandos acionam a janela de repetição configurada para entrar em vigor:

> **Aviso**: certifique-se de que você compreende o impacto potencial de qualquer comando, eles afetam as conexões de controle e plano de dados.

```
clear sdwan control connection
```

or

```
request platform software sdwan port_hop <color>
```

or

```
Interface Tunnelx
shutdown/ no shutdown
```

Solucionar Problemas de Falhas de Queda de Repetição

Solucionar problemas de coleta de dados

Para as quedas de antirreprodução do IPsec, é importante entender as condições e os possíveis desencadeadores do problema. No mínimo, colete o conjunto de informações para fornecer o

contexto:

- Informações de dispositivo para o remetente e o receptor para o pacote de repetição descartado, inclui tipo de dispositivo, cEdge vs. vEdge, versão de software e configuração.
- Histórico de problemas. Há quanto tempo a implantação está em vigor? Quando o problema começou? Quaisquer alterações recentes nas condições da rede ou do tráfego.
- Qualquer padrão para o replay cai, por exemplo., é esporádico ou constante? Hora do problema e/ou evento significativo, por exemplo, isso ocorre somente durante as horas de pico de produção de tráfego intenso ou somente durante a rechaveamento, etc.?

Com as informações coletadas anteriormente, continue com o fluxo de trabalho de solução de problemas.

Solucionar problemas de fluxo de trabalho

A abordagem geral de solução de problemas para problemas de repetição de IPsec é exatamente como ela é executada para o IPsec tradicional, leve em consideração o espaço de sequência SA por peer e o espaço de número de sequência múltipla, conforme explicado. Em seguida, siga estas etapas:

Etapa 1. Primeiro, identifique o peer para o descarte de repetição do syslog e a taxa de descarte. Para estatísticas de queda, sempre colete vários instantâneos de timestamp da saída para que a taxa de queda possa ser qualificada:

```
*Feb 19 21:28:25.006: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00001141238701410779 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 6,
src_addr 172.18.124.208, dest_addr 172.18.124.209, SPI 0x123

cedge-2#show platform hardware qfp active feature ipsec datapath drops
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
No time source, *11:25:53.524 EDT Wed Feb 26 2020
----------------------------------------------------------------------
Drop Type  Name                                        Packets
----------------------------------------------------------------------
        4  IN_US_V4_PKT_SA_NOT_FOUND_SPI                          30
       19  IN_CD_SW_IPSEC_ANTI_REPLAY_FAIL                        41
```

> **Observação**: não é raro ver quedas de repetição ocasionais devido à reordenação da entrega de pacotes na rede, mas quedas de repetição persistentes impactam o serviço e podem ser investigadas.

Passo 2a. Para uma taxa de tráfego relativamente baixa, considere um packet-trace com a condição definida para ser o endereço ipv4 do peer com a opção **copy packet** e examine os números de sequência do pacote descartado na borda direita da janela de repetição atual e os números de sequência nos pacotes adjacentes para confirmar se eles estão realmente duplicados ou fora da janela de repetição.

Passo 2b. Para alta taxa de tráfego sem acionador previsível, configure uma captura EPC com buffer circular e EEM para interromper a captura quando erros de repetição forem detectados. Como o EEM atualmente não é suportado no vManage a partir da versão 19.3, isso implica que o

cEdge teria que estar no modo CLI quando essa tarefa de solução de problemas for executada.

Etapa 3. Colete a plataforma **show crypto ipsec sa peer x.x.x.x** no receptor de forma ideal ao mesmo tempo em que a captura de pacotes ou o rastreamento de pacotes é coletado. Esse comando inclui as informações da janela de repetição do plano de dados em tempo real para SA de entrada e de saída.

Etapa 4. Se o pacote descartado estiver de fato fora de ordem, faça capturas simultâneas do remetente e do destinatário para identificar se o problema está na origem ou na camada de entrega da rede subjacente.

Etapa 5. Se os pacotes forem descartados mesmo que não estejam duplicados nem fora da janela de repetição, isso geralmente indica um problema de software no receptor.

Exemplo de Troubleshooting para ASR1001-x

Descrição do problema:

HW: ASR1001-X
SW: 17.06.03a

Vários erros de antirreprodução são recebidos para o peer de sessão 10.62.33.91, portanto, a sessão BFD oscila constantemente e o tráfego entre esses dois sites é afetado.

```
Jul 26 20:31:20.879: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:027 TS:00000093139972173042
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:32:23.567: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:009 TS:00000093202660128696
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:33:33.939: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:051 TS:00000093273031417384
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:34:34.407: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:020 TS:00000093333499638628
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
```

Etapa 1. A janela Verificar Anti Replay Configurado é 8192.

```
cEdge#sh sdwan security-info
security-info authentication-type deprecated
security-info rekey 86400
 security-info replay-window 8192
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
security-info extended-ar-window Disabled
security-info integrity-type "ip-udp-esp esp"
```

> **Observação**: O tamanho da janela de repetição efetiva para cada Espaço de Número de Sequência deve ser 8192/8= 1024 neste exemplo.

Etapa 2. Verifique o tamanho efetivo da janela de repetição para o peer 10.62.33.91 para comparar e confirmar o valor configurado.

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64                  <-- Effective Window Size
window base(ESN): 0
Multi-SNS window_top
---------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

O **Tamanho da janela: 64** exibido na saída não corresponde ao que a janela de repetição configurada **8 192 (8 192/8=1 024)**, o que significa que mesmo que ele tenha sido configurado, o comando não entrou em vigor.

> **Observação**: A janela de repetição efetiva é exibida apenas nas plataformas ASR. Para garantir que o tamanho real da janela de antireprodução seja igual ao tamanho configurado, aplique um dos comandos da seção para obter a eficácia da janela de reprodução configurada.

Etapa 3. Configure e habilite o rastreamento de pacotes e a captura de monitor (opcional) simultaneamente para o tráfego de entrada da sessão origem: 10.62.33.91, destino: 10.62.63.251

```
cEdge#debug platform packet-trace packet 2048 circular fia-trace data-size 2048
cEdge#debug platform packet-trace copy packet both size 2048 L3
cEdge#debug platform condition ipv4 10.62.33.91/32 in
cEdge#debug plat cond start
```

Etapa 4. Coletar resumo de rastreamento de pacote:

```
cEdge#show platform packet summay
```

Etapa 5. Expanda alguns pacotes descartados (IpsecInput) capturados.

(IpsecInput) Quedas de pacotes:

```
cEdge#sh platform pack pack 816
Packet: 816 CBUG ID: 973582
Summary
Input : TenGigabitEthernet0/0/0.972
Output : TenGigabitEthernet0/0/0.972
State : DROP 56 (IpsecInput)
Timestamp
Start : 97495234494754 ns (07/26/2022 21:43:56.25110 UTC)
Stop : 97495234610186 ns (07/26/2022 21:43:56.25225 UTC)
Path Trace
Feature: IPV4(Input)
Input : TenGigabitEthernet0/0/0.972
Output : <unknown>
Source : 10.62.33.91
Destination : 10.62.63.251
Protocol : 17 (UDP)
SrcPort : 12367
DstPort : 12347
<snip>

Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfed 00000000 d0a60d5b 6161b06e 453d0e3d 5ab694ce 5311bbb6 640ecd68
7ceb2726 80e39efd 70e5549e 57b24820 fb963be5 76d01ff8 273559b0 32382ab4
c601d886 da1b3b94 7a2826e2 ead8f308 c464

817 DROP:
--------------------------------
Packet: 817
<snip>
Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfec 00000000 cc72d5dd ef73fe25 2440bed6 31378b78 3c506ee5 98e3dba4
bc9e6aa0 50ea98f6 7dee25c8 c1579ce0 1212290c 650f5947 57b9bc04 97c7996c
d4dbf3e6 25b33684 a7129b67 141a5e73 8736
```

A SD-WAN usa ESP encapsulado em UDP:

- O cabeçalho UDP é 304f303b 00770000,
- O próximo é SPI (**04000106**)
- Portanto, **00b6e00d** é o número de segurança (SN).
- O índice MSNS é **2** (**x04**00106) devido a SPI de 32 bits (**0 0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 1.)

Etapa 6. Verificar o índice MSNS

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64
window base(ESN): 0
Multi-SNS window_top
-----------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
  index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

A maior janela antirreprodução (Borda direita da janela deslizante antirreprodução) para MSNS de 2 (0x04) é **0b65f00.**

Passo 7. Expanda alguns pacotes capturados encaminhados (FWD).

Pacotes encaminhados:

```
Packet: 838
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
 00b6e015 00000000 088bbd6a f4e4b35f b131143f ef1f91eb 659149f7 dbe6b025
be7fbfd0 5fad1c71 014321f1 3e0d38f2 cc8d0e5f 1494e4fa 097c7723 dfc7ceef
4a14f444 abcc1777 0bb9337f cd70c1da 01fc5262 848b657c 3a834680 b07b7092
81f07310 4eacd656 ed36894a e468
```

Pacote: 837

```
Packet: 837
<snip>
Packet Copy In
```

```
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
00b6e014 00000000 76b2a256 8e835507 13d14430 ae16d62c c152cdfd 2657c20c
01d7ce1d b3dfa451 a2cbf6e9 32f267f9 e10e9dec 395a0f9e 38589adb aad8dfb8
a3b72c8d a96f2dce 2a1557ab 67959b6e 94bbbb0a cfc4fc9e 391888da af0e492c
80bebb0e 9d7365a4 153117a6 4089
```

Etapa 8. Colete e obtenha as informações do número de sequência de vários pacotes encaminhados (FWD) antes, depois e depois dos descartes.

```
FWD:
839 PKT: 00b6e003 FWD
838 PKT: 00b6e001 FWD
837 PKT: 00b6e000 FWD
815 PKT: 00b6e044 FWD
814 PKT: 00b6dfe8 FWD
813 PKT: 00b6e00d FWD

DROP:
816 PKT: 00b6dfed DROP
817 PKT: 00b6dfec DROP
818 PKT: 00b6dfeb DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

Etapa 9. Converta o SN em decimal e reordene-o para um cálculo simples:

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

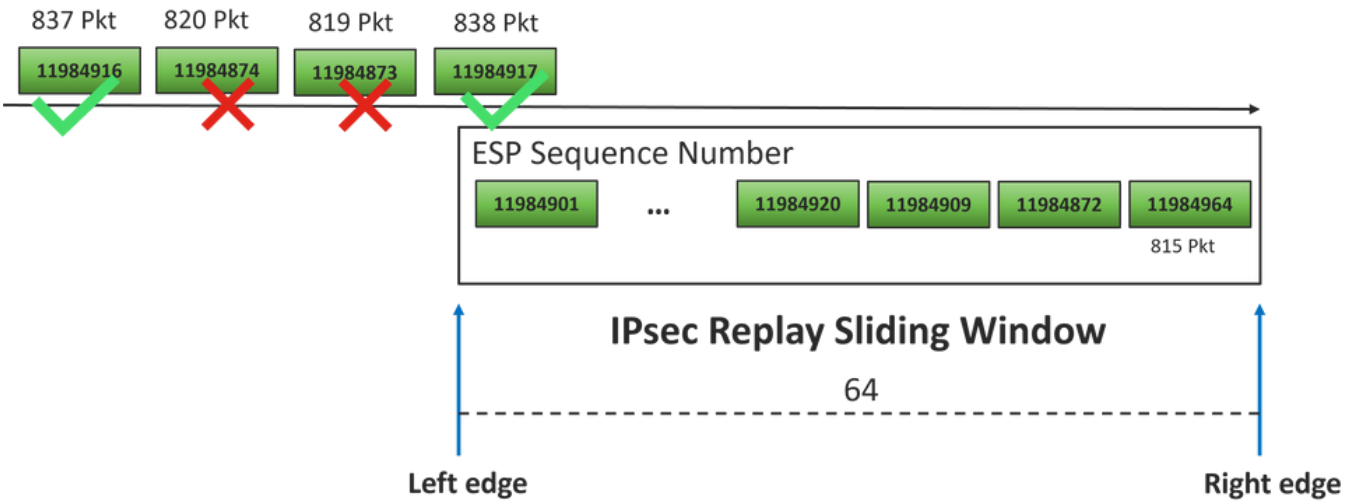
> **Observação**: se o número de sequência for maior que o número de sequência mais alto na janela, a integridade do pacote será verificada. Se o pacote passar na verificação de integridade, a janela deslizante será movida para a direita.

Etapa 10. Converta o SN em decimal e reordene-o para um cálculo simples:

```
Difference:

815 PKT: Decimal: 11984964 ***** Highest Value
--------------------------------------
815(Highest) - X PKT = Diff
--------------------------------------
816 PKT: 11984964 - 11984877 = 87 DROP
817 PKT: 11984964 - 11984876 = 88 DROP
818 PKT: 11984964 - 11984875 = 89 DROP
819 PKT: 11984964 - 11984873 = 91 DROP
820 PKT: 11984964 - 11984874 = 90 DROP
<snip>
```

```
837 PKT: 11984964 - 11984916 = 48 FWD
838 PKT: 11984964 - 11984917 = 47 FWD
839 PKT: 11984964 - 11984918 = 45 FWD
```

Para este exemplo, é possível visualizar a janela deslizante com o **tamanho de janela 64** e a **borda direita**11984964 como mostrado na imagem.



O número de sequência recebido para descartar pacotes está muito à frente da borda direita da janela de repetição para esse espaço de sequência.

Solução

Como o tamanho da janela ainda está no valor 64 anterior como visto na etapa 2, um dos comandos na seção Comandos para Aproveitar a Eficácia da Janela de Repetição Configurada precisa ser aplicado para que o tamanho da janela 1024 entre em vigor.

Ferramenta adicional de captura do Wireshark

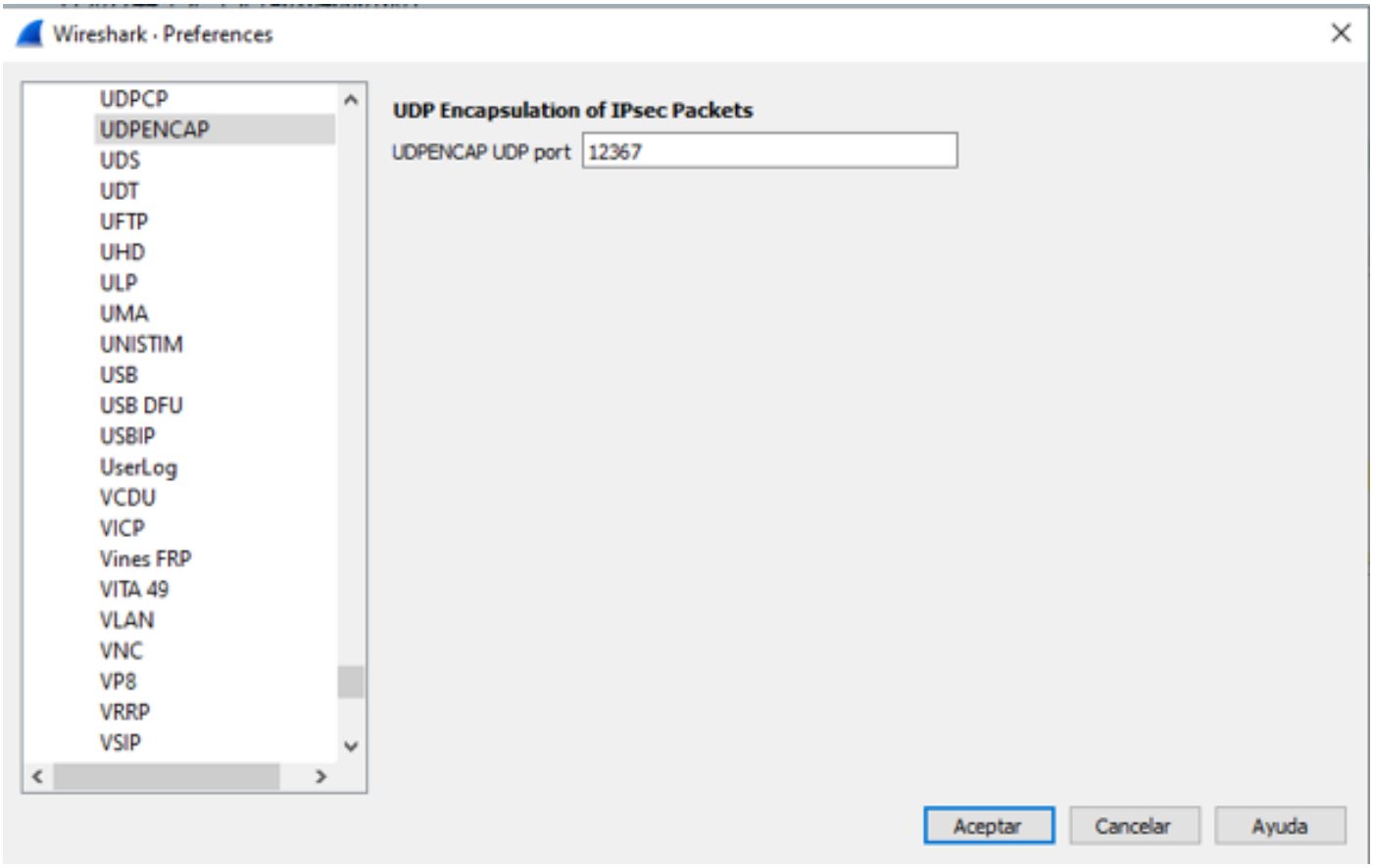
Outra ferramenta útil para ajudar a correlacionar o ESP SPI e o número de sequência é o software Wireshark.

> **Observação**: é importante coletar a captura de pacotes quando o problema ocorrer e se for possível ao mesmo tempo que o rastreamento fia é coletado conforme descrito anteriormente

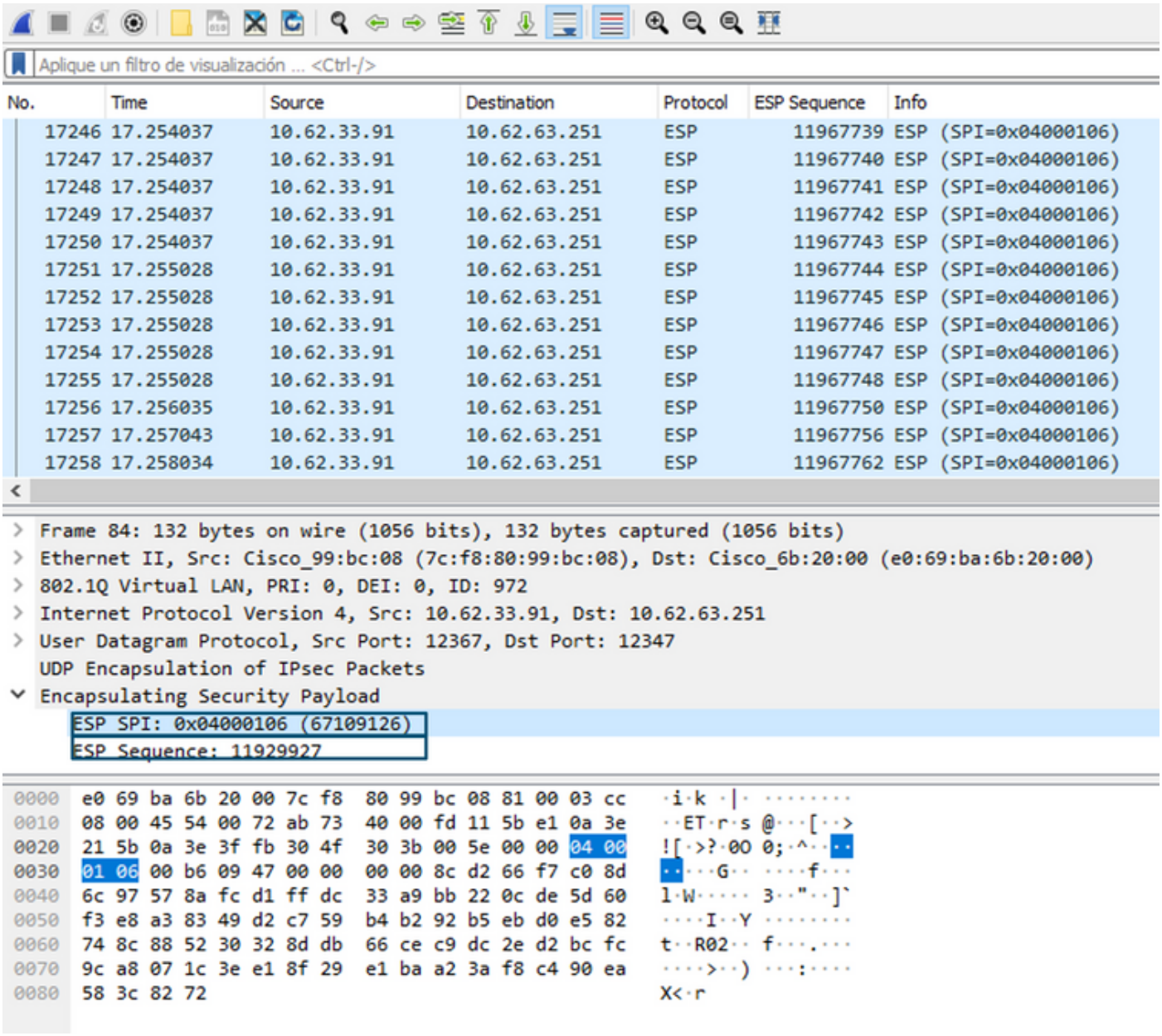
Configure a captura de pacote para a direção de entrada e exporte-a para o arquivo pcap.

```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Quando a captura de pcap é aberta no Wireshark, para poder ver o SPI ESP e o número de sequência, expanda um pacote, clique com o botão direito do mouse e selecione **preferências de protocolo**, procure **UDPENCAP** e altere a porta padrão para porta SD-WAN (porta de origem) como mostrado na figura.



Depois que UDPENCAP estiver no lugar com a porta direita, as informações de ESP são exibidas como mostrado na imagem.



Informações Relacionadas

- [Artigo IPsec Anti-Replay Check Failures TechZone (Falhas de verificação antirrepetição IPsec no TechZone)]
- [Expandindo e desativando a janela de antirreprodução IPsec]
- [Suporte técnico e downloads da Cisco]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.