Dépannage des échecs de relecture de l'anti IPsec cEdge SDWAN

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Considérations relatives à la détection de relecture SD-WAN
  - Clé de groupe et clé par paire
  - SPI codé
  - Espace de numéros de séquence multiples pour QoS
- Commandes pour forcer l'entrée en vigueur de la fenêtre de relecture nouvellement configurée
- Dépannage des échecs de relecture/abandon
  - Dépannage de la collecte de données
  - Dépannage du workflow
- Exemple de dépannage pour ASR1001-x
  - Solution
  - Outil de capture Wireshark supplémentaire
- Informations connexes

Introduction

Ce document décrit le comportement d'anti-relecture IPsec dans SD-WAN IPsec pour les routeurs Edge et comment dépanner les problèmes d'anti-relecture.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) de Cisco
- Sécurité du protocole Internet (IPSec)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C8000V Version17.06.01
- ASR1001-X version 17.06.03a
- vManage Version 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'authentification IPsec fournit une protection intégrée contre la relecture contre les paquets IPsec anciens ou dupliqués avec le numéro de séquence dans l'en-tête ESP vérifié sur le récepteur. Les abandons de paquets anti-relecture sont l'un des problèmes de plan de données les plus courants avec IPsec en raison de paquets livrés dans le désordre, ou en dehors de la fenêtre anti-relecture. Une approche générale de dépannage pour les pertes d'anti-relecture IPsec peut être trouvée dans Dépannage des échecs de vérification d'anti-relecture IPsec, et la technique générale s'applique également à SD-WAN. Cependant, certaines différences d'implémentation existent entre IPsec traditionnel et IPsec utilisé dans la solution Cisco SD-WAN. Cet article a pour but d'expliquer ces différences et l'approche des plates-formes cEdge avec Cisco IOS ®XE.

Considérations relatives à la détection de relecture SD-WAN

Clé de groupe et clé par paire

Contrairement à IPsec traditionnel, où les SA IPsec sont négociées entre deux homologues à

l'aide du protocole IKE, SD-WAN utilise un concept de clé de groupe. Dans ce modèle, un périphérique de périphérie SD-WAN génère périodiquement des SA entrantes de plan de données par TLOC (Transport Locator) et envoie ces SA au contrôleur SD-WAN, qui à son tour propage la SA au reste des périphériques de périphérie dans le fabric SD-WAN.

Pour une description plus détaillée des opérations du plan de données SD-WAN, consultez Vue d'ensemble de la sécurité du plan de données SD-WAN.

Remarque : Depuis Cisco IOS ®XE 16.12.1b/SD-WAN 19.2, les clés par paires IPsec sont prises en charge ; voir Présentation des clés IPsec par paire. Avec les touches Pairwise, la protection anti-relecture IPsec fonctionne exactement comme IPsec traditionnel. Cet article se concentre principalement sur la vérification de relecture avec l'utilisation du modèle de clé de groupe.

SPI codé

Dans l'en-tête ESP IPsec, le SPI (Security Parameter Index) est une valeur de 32 bits que le récepteur utilise pour identifier l'association de sécurité avec laquelle un paquet entrant est décrypté. Dans SD-WAN, ce SPI entrant peut être identifié avec show crypto ipsec sa :

<#root>

```
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-
        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)
```

Remarque : même si le SPI entrant est le même pour tous les tunnels, le récepteur a un SA différent et l'objet de fenêtre de relecture correspondant associé au SA pour chaque périphérique de périphérie homologue puisque le SA est identifié par la source, l'adresse IP de destination, la source, les ports de destination 4-uplet et le numéro SPI. Donc essentiellement, chaque homologue a son propre objet fenêtre anti-replay.

Dans le paquet réel envoyé par le périphérique homologue, notez que la valeur SPI est différente de la sortie précédente. Voici un exemple du résultat de la commande packet-trace avec l'option de copie de paquet activée :

<#root>

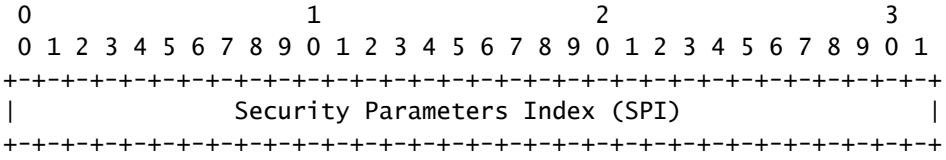
```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b

04000123

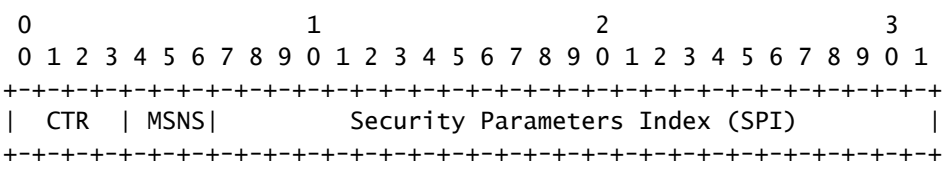
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

Le SPI réel dans l'en-tête ESP est 0x04000123. La raison en est que les premiers bits du SPI pour SD-WAN sont codés avec des informations supplémentaires, et que seuls les bits bas du champ SPI sont alloués pour le SPI réel.

IPsec traditionnel :



SD-WAN :



Where:

- CTR (4 premiers bits, bits 0-3) : les bits de contrôle sont utilisés pour indiquer le type spécifique de paquets de contrôle. Par exemple, le bit de contrôle 0x80000000 est utilisé pour BFD.
- MSNS (3 bits suivants, bits 4-6) - Multiple Sequence Number Space Index : Ceci est utilisé pour localiser le compteur de séquence correct dans le tableau de compteurs de séquence pour vérifier la relecture pour le paquet donné. Pour le SD-WAN, le 3 bits de MSNS permet

de mapper 8 classes de trafic différentes dans leur propre espace de numéros de séquence. Ceci implique que la valeur SPI efficace qui peut être utilisée pour la sélection SA est la valeur réduite de 25 bits d'ordre inférieur à la valeur complète de 32 bits du champ.

Espace de numéros de séquence multiples pour QoS

Il est courant d'observer des échecs de relecture IPsec dans un environnement où les paquets sont livrés dans le désordre en raison de la QoS, par exemple, LLQ (Low Latency Queuing), car la QoS est toujours exécutée après le chiffrement et l'encapsulation IPsec. La solution Multiple Sequence Number Space résout ce problème en utilisant plusieurs espaces de numéros de séquence mappés à différentes classes de trafic QoS pour une association de sécurité donnée. L'espace des différents numéros de séquence est indexé par les bits MSNS codés dans le champ SPI du paquet ESP comme illustré. Pour une description plus détaillée, consultez Mécanisme de reprise anti-IPsec pour QoS.

Comme indiqué précédemment, cette implémentation de numéro de séquence multiple implique que la valeur SPI effective peut être utilisée pour la sélection SA est la valeur réduite de 25 bits de poids faible. Une autre considération pratique lorsque la taille de fenêtre de relecture est configurée avec cette implémentation est la taille de fenêtre de relecture configurée pour la fenêtre de relecture agrégée, de sorte que la taille de fenêtre de relecture effective pour chaque espace de numéro de séquence est 1/8 de l'agrégat.

Exemple de configuration :

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



Remarque : La taille de fenêtre de relecture effective pour chaque espace de numéro de séquence est 1024/8 = 128 !



Remarque : Depuis le Cisco IOS ®XE. 17.2.1, la taille de la fenêtre de relecture agrégée a été augmentée à 8192, de sorte que chaque espace de numéro de séquence peut avoir une fenêtre de relecture maximale de 8192/8 = 1024 paquets.

Sur un périphérique cEdge, le dernier numéro de séquence reçu pour chaque espace de numéro de séquence peut être obtenu à partir de la sortie du plan de données show crypto ipsec sa peer x.x.x.x platform IPsec :

<#root>

```
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

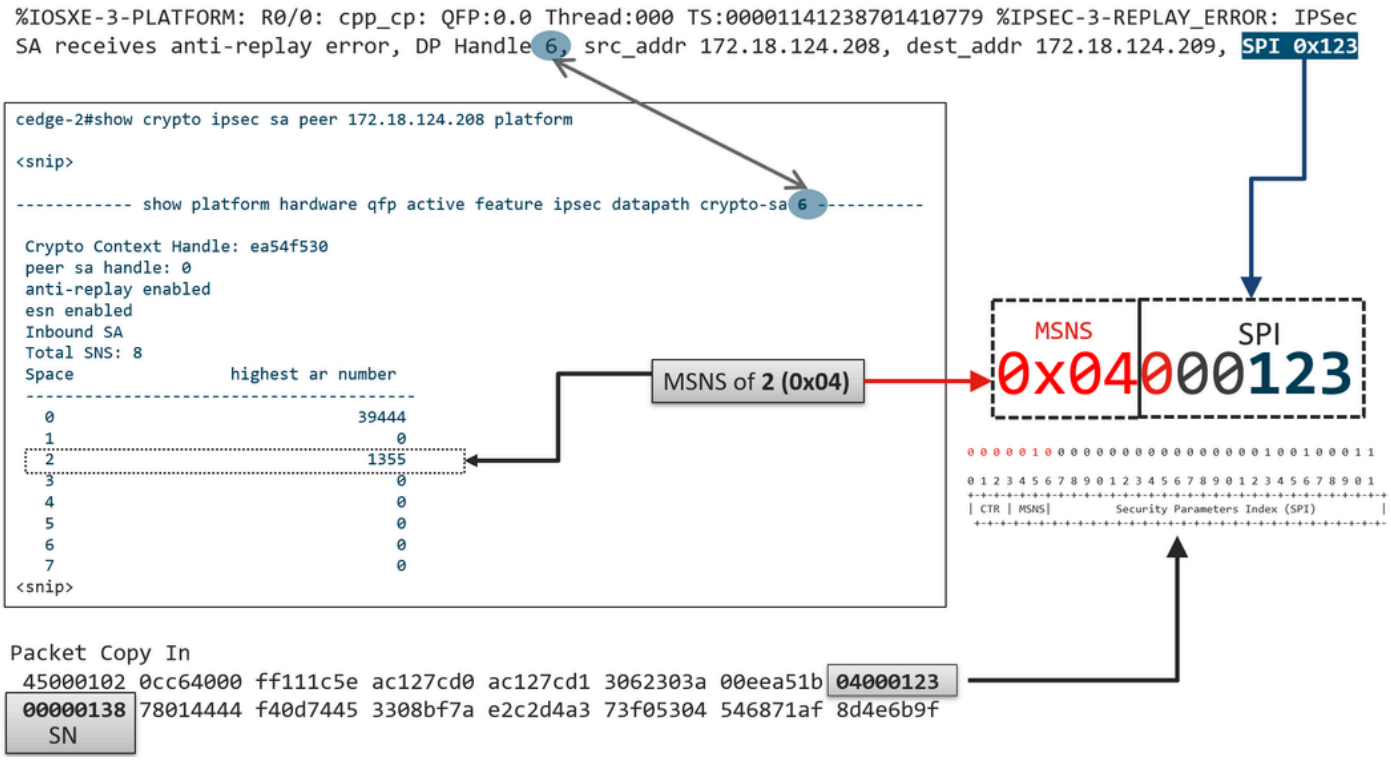

2                               1355

   3                                  0
   4                                  0
   5                                  0
   6                                  0
   7                                  0
<snip>
```

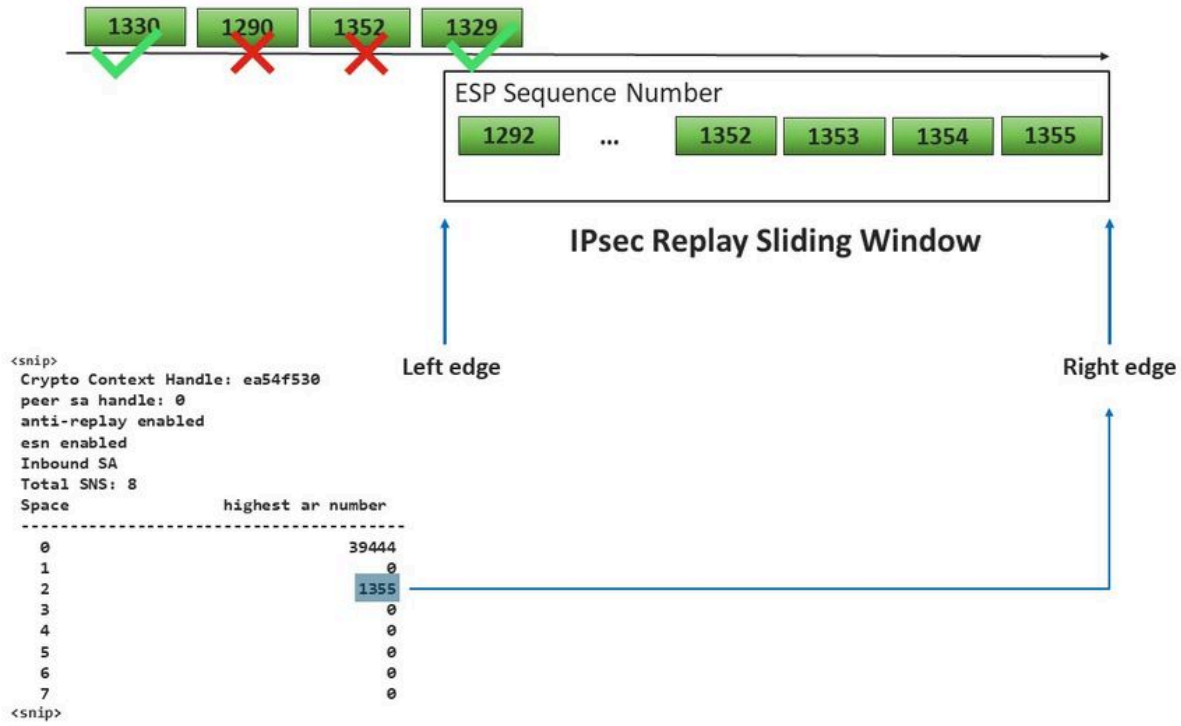
Dans l'exemple, le numéro de séquence de fenêtre anti-relecture le plus élevé (bord droit de la fenêtre glissante anti-relecture) pour MSNS de 0 (0x00) est 3944, et celui pour MSNS de 2 (0x04) est 1335, et ces compteurs sont utilisés pour vérifier si le numéro de séquence est à l'intérieur de la fenêtre de relecture pour les paquets dans le même espace de numéro de séquence.

Remarque : Il existe des différences de mise en oeuvre entre la plate-forme ASR1k et les autres plates-formes de routage Cisco IOS ®XE (routeurs ISR4k, ISR1k, CSR1kv, Catalyst 8000). Par conséquent, il y a des différences en termes de commandes show et de leurs résultats pour ces plates-formes.

Il est possible de corréler les erreurs Anti-Replay et les sorties show pour trouver le SPI, et l'index de numéro de séquence comme indiqué dans l'image.



Avec les informations précédentes obtenues, le bord droit (fenêtre supérieure) et la fenêtre coulissante ; comme illustré dans l'image.



Commandes pour forcer l'entrée en vigueur de la fenêtre de

relecture nouvellement configurée

Contrairement à l'IPsec normal (non SD-WAN), la commande rekey n'est pas appliquée à la fenêtre anti-replay.

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

Ces commandes déclenchent la prise d'effet de la fenêtre de relecture configurée :



Avertissement : Assurez-vous de comprendre l'impact potentiel de toute commande, car elle affecte les connexions de contrôle et le plan de données.

```
clear sdwan control connection
```

ou

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

ou

```
interface Tunnelx
 shutdown
 no shutdown
```

Dépannage des échecs de relecture/abandon

Dépannage de la collecte de données

Pour les abandons anti-relecture IPsec, il est important de comprendre les conditions et les déclencheurs potentiels du problème. Au minimum, collectez l'ensemble d'informations pour fournir le contexte :

- Informations sur le périphérique pour l'expéditeur et le destinataire pour les abandons de paquets de relecture, y compris le type de périphérique, cEdge et vEdge, la version du logiciel et la configuration.
- Historique des problèmes. Depuis combien de temps le déploiement est-il en place ? Quand le problème a-t-il commencé ? Toute modification récente des conditions du réseau ou du trafic.
- Un modèle pour les pertes de relecture, par exemple, est-il sporadique ou constant ? Heure du problème et/ou de l'événement significatif, cela se produit-il uniquement pendant les heures de pointe de production, ou uniquement pendant la retouche, etc.

Une fois les informations précédentes collectées, poursuivez le workflow de dépannage.

Dépannage du workflow

L'approche générale de dépannage pour les problèmes de relecture IPsec est identique à la façon dont elle est effectuée pour IPsec traditionnel. Tenez compte de l'espace de séquence SA par homologue et de l'espace de numéros de séquence multiples comme expliqué. Ensuite, procédez comme suit :

Étape 1. Identifiez d'abord l'homologue pour la suppression de relecture à partir du syslog et le taux de suppression. Pour les statistiques d'abandon, collectez toujours plusieurs instantanés horodatés de la sortie afin que le taux d'abandon puisse être quantifié :

```
*Feb 19 21:28:25.006: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001141238701410779 %IPSE

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
```

Remarque : Il n'est pas rare de voir des pertes de relecture occasionnelles dues à la

réorganisation de la livraison des paquets sur le réseau. Cependant, les pertes de relecture persistantes ont un impact sur le service et peuvent être analysées.

Étape 2a. Pour un débit de trafic relativement faible, effectuez un suivi de paquets en définissant la condition sur l'adresse IPv4 homologue avec l'option copy packet. Examinez les numéros de séquence du paquet abandonné par rapport à la fenêtre de relecture actuelle (bord droit) et les numéros de séquence des paquets adjacents. Vérifiez s'il s'agit bien de doublons ou de doublons en dehors de la fenêtre de relecture.

Étape 2b. Pour un débit de trafic élevé sans déclencheurs prévisibles, configurez une capture EPC avec tampon circulaire et EEM pour arrêter la capture lorsque des erreurs de relecture sont détectées. EEM n'étant pas pris en charge sur vManage à partir de la version 19.3, cela signifie que le serveur cEdge doit être en mode CLI lorsque cette tâche de dépannage est effectuée.

Étape 3 : collectez la sortie de la plate-forme show crypto ipsec sa peer x.x.x.x sur le récepteur, idéalement au moment de la capture du paquet ou lorsque la trace de paquet est collectée. Cette commande inclut les informations de la fenêtre de réexécution du plan de données en temps réel pour l'association de sécurité entrante et sortante.

Étape 4. Si le paquet abandonné est dans le désordre, effectuez des captures simultanées de l'expéditeur et du destinataire pour déterminer si le problème provient de la source ou de la couche de livraison réseau sous-jacente.

Étape 5. Si les paquets sont abandonnés même s'ils ne sont ni dupliqués ni en dehors de la fenêtre de relecture, cela indique généralement un problème logiciel sur le récepteur.

Exemple de dépannage pour ASR1001-x

Description du problème :

MATÉRIEL : ASR1001-X
Logiciel : 17.06.03 bis

Plusieurs erreurs d'anti-relecture sont reçues pour l'homologue de session 10.62.33.91. Par conséquent, la session BFD est constamment instable et le trafic entre ces deux sites est affecté.

```
Jul 26 20:31:20.879: %IOSXE-3-PLATFORM: RO/O: cpp_cp: QFP:0.0 Thread:027 TS:00000093139972173042 %IPSEC
Jul 26 20:32:23.567: %IOSXE-3-PLATFORM: RO/O: cpp_cp: QFP:0.0 Thread:009 TS:00000093202660128696 %IPSEC
Jul 26 20:33:33.939: %IOSXE-3-PLATFORM: RO/O: cpp_cp: QFP:0.0 Thread:051 TS:00000093273031417384 %IPSEC
Jul 26 20:34:34.407: %IOSXE-3-PLATFORM: RO/O: cpp_cp: QFP:0.0 Thread:020 TS:00000093333499638628 %IPSEC
```

Étape 1 : vérifiez que la fenêtre anti-relecture configurée est 8192.

<#root>

```
cEdge#show 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"
```

Remarque : Dans cet exemple, la taille effective de la fenêtre de relecture pour chaque espace de numéro de séquence doit être 8192/8= 1024.

Étape 2. Vérifiez la taille de la fenêtre de relecture effective pour l'homologue 10.62.33.91 afin de comparer et de confirmer la valeur configurée.

<#root>

```
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
```

La Taille De La Fenêtre : 64 affiché dans le résultat ne correspond pas à ce que la fenêtre de relecture configurée de 8192 (8192/8=1024), ce qui signifie que même si elle a été configurée, la commande n'a pas pris effet.

Remarque : La fenêtre de relecture effective s'affiche uniquement sur les plates-formes ASR. Pour vous assurer que la taille réelle de la fenêtre anti-relecture est identique à la taille configurée, appliquez l'une des commandes de la section précédente pour forcer la prise en compte de la taille de fenêtre configurée.

Étape 3 : configuration et activation simultanées du suivi des paquets et de la capture de surveillance (facultatif) pour le trafic entrant en provenance de la source de session : 10.62.33.91, destination : 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 platform condition start
```

Étape 4. Collecter le résumé du suivi des paquets :

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

```
811     Te0/0/0.972         Te0/0/1.301    FWD

812     Te0/0/0.972         Te0/0/1.301    FWD

813     Te0/0/0.972         Te0/0/1.301    FWD

814     Te0/0/0.972         Te0/0/1.301    FWD
```

```
815     Te0/0/0.972         Te0/0/1.301    FWD

816     Te0/0/0.972         Te0/0/0.972    DROP 56 (IpsecInput)

817     Te0/0/0.972         Te0/0/0.972    DROP 56 (IpsecInput)

818     Te0/0/0.972         Te0/0/0.972    DROP 56 (IpsecInput)

819     Te0/0/0.972         Te0/0/0.972    DROP 56 (IpsecInput)




837     Te0/0/0.972         Te0/0/1.301    FWD

838     Te0/0/0.972         Te0/0/1.301    FWD
```

Étape 5. Développez certains paquets abandonnés (IpsecInput) capturés.

(IpsecInput) Abandons de paquets :

<#root>

```
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
```

SD-WAN utilise ESP encapsulé UDP :

- L'en-tête UDP est 304f303b 00770000,
- La suivante est SPI (0400106)
- Par conséquent, 00b6e00d est le numéro de séquence (SN).
- L'index MSNS est 2 (x0400106) en raison de l'interface SPI 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 1 0 0 1 0 0 0 1 1 1.)

Étape 6. Vérification de l’index MSNS

<#root>

```
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
```

Le numéro de séquence de fenêtre anti-relecture le plus élevé (bord droit de la fenêtre glissante anti-relecture) pour MSNS de 2 (0x04) est 0b65f00.

Étape 7. Développez certains paquets transférés (FWD) capturés.

Paquets transférés :

<#root>

```
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
```

Paquet: 837

<#root>

```
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
```

Étape 8. Collectez et obtenez les informations de numéro de séquence à partir de plusieurs paquets transférés (FWD) avant, après et les abandons.

```
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
```

Étape 9. Convertissez le numéro d'ordre hexadécimal en décimal et réorganisez-les pour simplifier le calcul :

<#root>

```
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
```

Remarque : Si le numéro de séquence est supérieur au numéro de séquence le plus élevé dans la fenêtre, l'intégrité du paquet est vérifiée. Si le paquet réussit la vérification d'intégrité, la fenêtre glissante est déplacée vers la droite.

Étape 10. Calculez le delta entre le numéro de séquence le plus élevé et le numéro de séquence reçu pour chaque paquet :

<#root>

```
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:

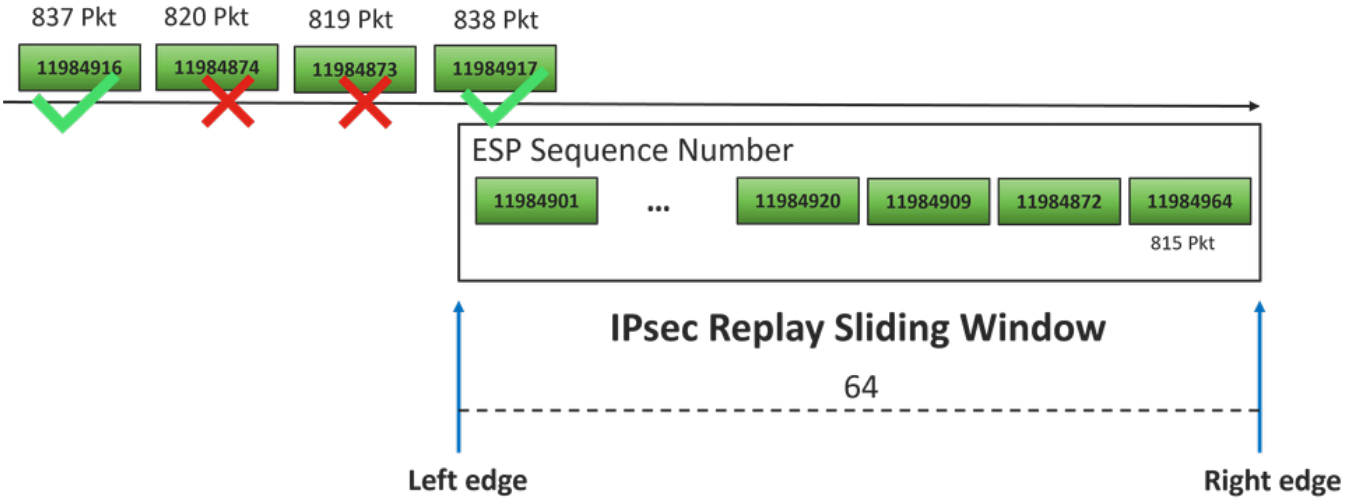
11984964

-

11984918 = 45

FWD

Pour cet exemple, il est possible de visualiser la fenêtre glissante avec la taille de fenêtre 64 et le bord droit 11984964 comme le montre l'image :



Le numéro de séquence reçu pour les paquets abandonnés se trouve bien en avant du bord droit de la fenêtre de relecture pour cet espace de séquence.

Solution

Comme la taille de fenêtre est toujours dans la valeur précédente 64, comme on l'a vu à l'étape 2, l'une des commandes de la section Commandes pour forcer l'entrée en vigueur de la fenêtre de relecture nouvellement configurée doit être appliquée pour que la taille de fenêtre augmentée 1024 prenne effet.

Outil de capture Wireshark supplémentaire

Wireshark est un autre outil utile permettant de corréler l'interface SPI ESP et le numéro de

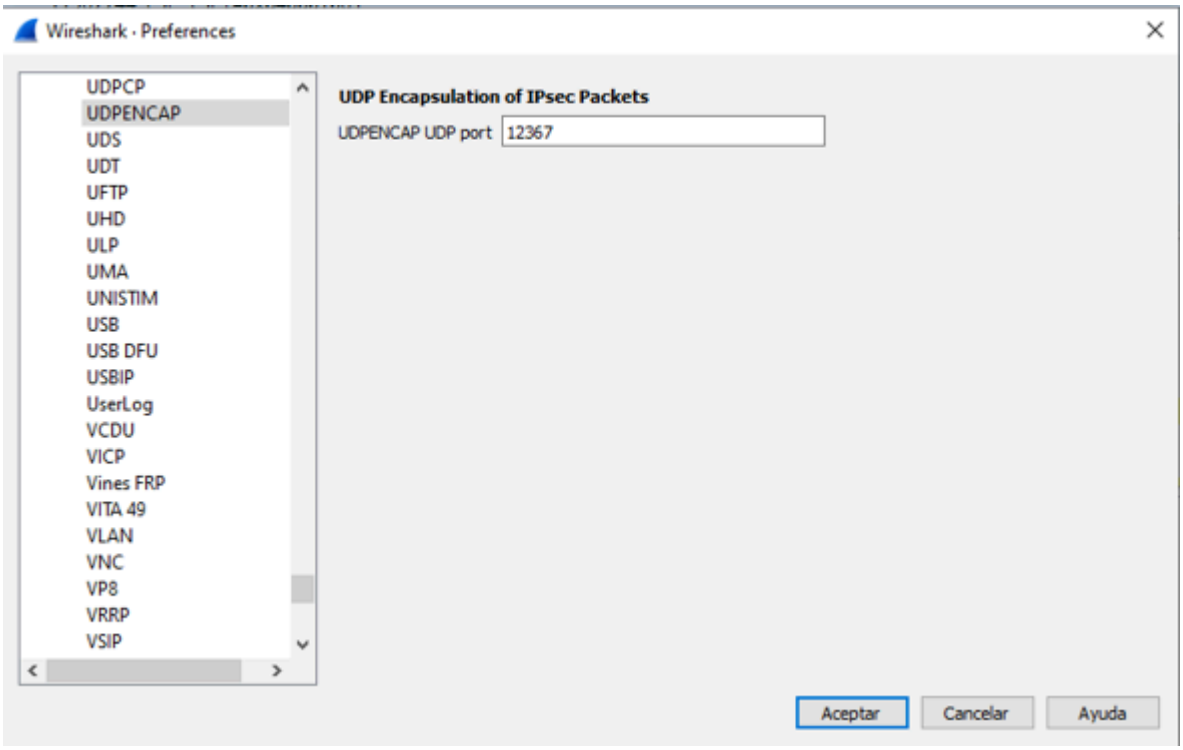
séquence.

> Remarque : Il est important de collecter la capture de paquets lorsque le problème se produit et si cela est possible en même temps, la trace fia est collectée comme décrit précédemment

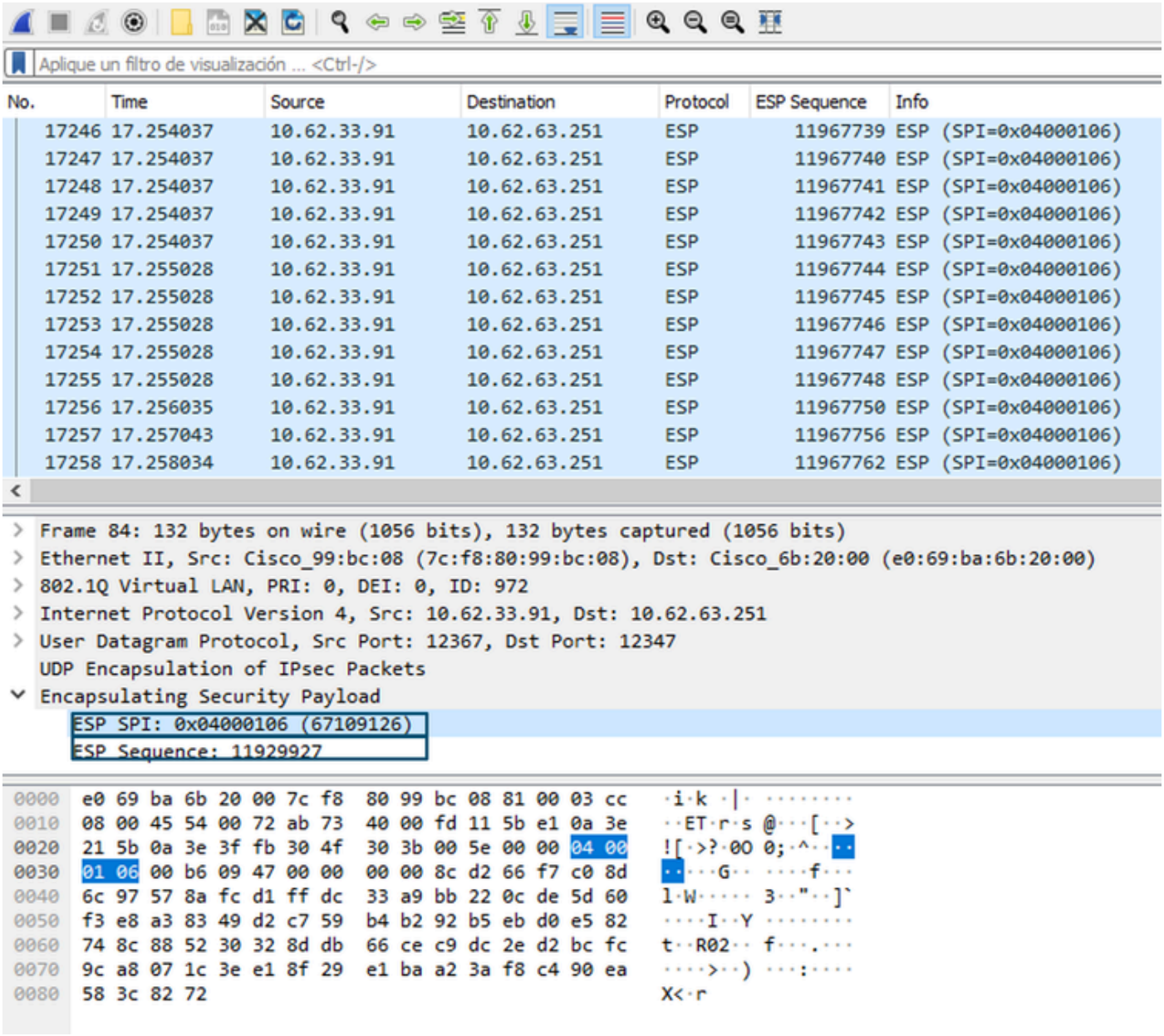
Configurez la capture de paquets pour la direction entrante et exportez-la vers le fichier pcap.

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

Lorsque la capture pcap est ouverte dans Wireshark, pour voir le SPI ESP et le numéro de séquence, développez un paquet en cliquant avec le bouton droit et sélectionnez les préférences de protocole. Recherchez UDPENCAP et remplacez le port par défaut par le port SD-WAN (port source), comme illustré dans l'image :



Une fois que UDPENCAP est en place avec le port correct, les informations ESP s'affichent, comme illustré dans l'image :



Informations connexes

- [Article TechZone sur les échecs de contrôle anti-relecture IPsec]
- [Extension et désactivation de la fenêtre IPsec Anti-Replay]
- [Assistance technique de Cisco et téléchargements]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.