

# Dépannage des échecs de relecture de l'anti-IPsec cEdge SD-WAN

## 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 permettant d'afficher l'efficacité de la fenêtre de relecture 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](#)

## 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 Version 17.06.01
- 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 des paquets livrés dans le désordre en dehors de la fenêtre anti-relecture. Une approche générale de dépannage pour les abandons de l'anti-relecture IPsec peut être trouvée [dans les échecs de vérification de l'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 et envoie ces SA au contrôleur vSmart, qui à son tour propage la SA au reste des périphériques de périphérie dans le réseau 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. 6.12.1a/SD-WAN 19.2, les clés IPsec par paires 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. Avec SD-WAN, ce SPI entrant peut être identifié avec **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)

**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 :

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 de l'interface SPI pour SD-WAN sont codés avec des informations supplémentaires, et seuls les bits bas du champ SPI sont alloués pour l'interface SPI réelle.

### IPsec traditionnel :

```
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** (4 premiers bits, bits 0-3) : bits de contrôle 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, 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, veuillez voir [IPsec Anti Replay Mechanism for QoS](#).

Comme indiqué précédemment, cette implémentation de numéro de séquence multiple implique que la valeur SPI efficace qui 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 que la taille de fenêtre de relecture configurée est 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 la plate-forme logicielle 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 numéros 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** :

```
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
```

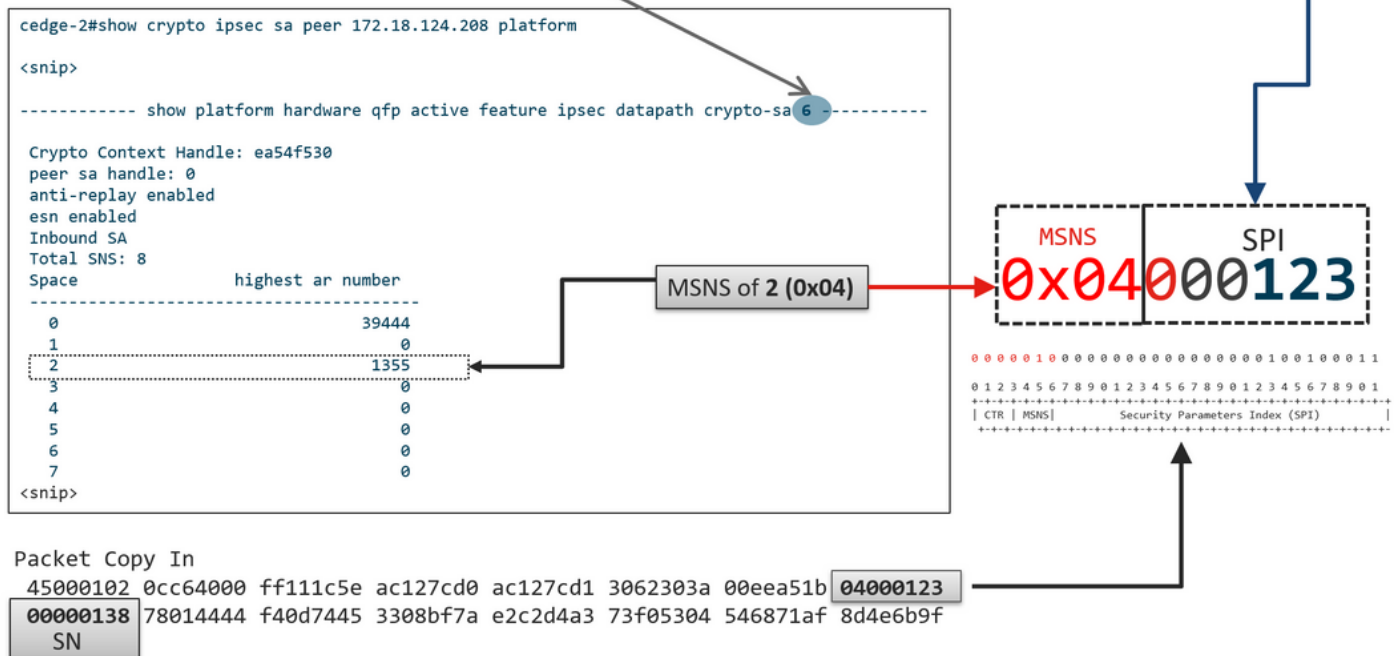
<snip>

Dans l'exemple, la fenêtre anti-relecture la plus élevée (bord droit de la fenêtre glissante anti-relecture) pour MSNS de 0 (0x00) est 3944, et celle pour MSNS de 2 (0x04) est 1355, 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.

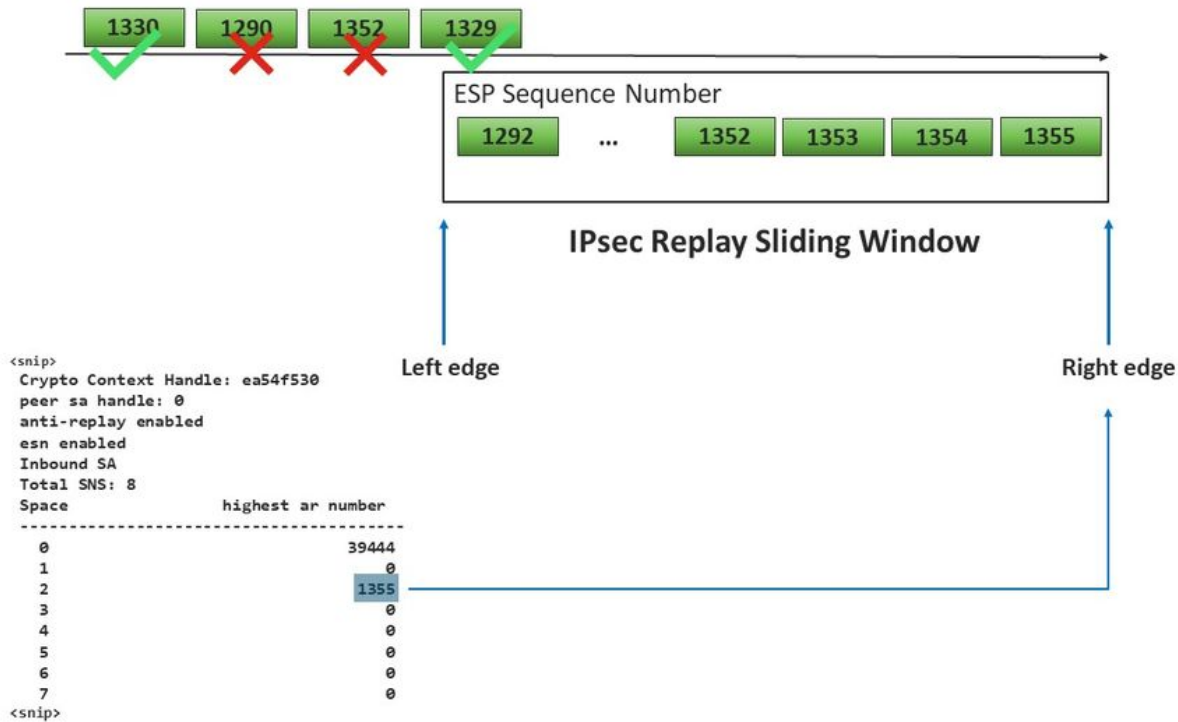
**Remarque :** il existe des différences de mise en oeuvre entre la plate-forme ASR1k et les autres plates-formes de routage Cisco IOS @XE (ISR4k, ISR1k, CSR1kv). Par conséquent, il y a des différences en termes de commandes show et de leurs résultats pour ces plates-formes.

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.

```
%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
```



Avec les informations précédentes obtenues le bord droit (fenêtre supérieure) et la fenêtre glissante ressemble comme indiqué dans l'image.



## Commandes permettant d'afficher l'efficacité de la fenêtre de relecture 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 que vous comprenez l'impact potentiel de toute commande, ils affectent les connexions de contrôle et le plan de données.

```
clear sdwan control connection
```

ou

```
request platform software sdwan port_hop <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.
- Tout modèle de la relecture baisse, par exemple., est-il sporadique ou constant ? Heure du problème et/ou de l'événement significatif, par exemple, cela se produit-il uniquement pendant les heures de pointe de production à fort trafic, ou uniquement pendant la retouche, et ainsi de suite ?

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 semblable à la façon dont elle est effectuée pour IPsec traditionnel, tenir 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 l'abandon de la relecture à partir du syslog et le taux d'abandon. 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 %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
```

**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, mais les pertes de relecture persistantes ont un impact sur le service et peuvent être analysées.

**Étape 2a.** Pour un débit de trafic relativement faible, prenez une trace de paquet avec la condition définie pour être l'adresse ipv4 homologue avec l'option **copy packet** et examinez les numéros de séquence pour le paquet abandonné par rapport au bord droit de la fenêtre de relecture actuelle et les numéros de séquence dans les paquets adjacents pour confirmer s'ils sont effectivement dupliqués ou en dehors de la fenêtre de relecture.

**Étape 2b.** Pour un débit de trafic élevé sans déclencheur prévisible, 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 plate-forme **show crypto ipsec sa peer x.x.x.x** sur le récepteur idéalement au moment où la capture de paquets ou la trace de paquets est collectée. Cette commande inclut les informations de la fenêtre de relecture du plan de données en temps réel pour l'association de sécurité entrante et sortante.

**Étape 4.** Si le paquet abandonné est en effet 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 alors qu'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 : 17.06.03a

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: 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
```

**Étape 1. Cochez la case Configured Anti Replay Window is 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"
```



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

**Étape2.** Vérifiez la taille de la fenêtre de relecture effective pour l'homologue 10.62.33.91 pour comparer et confirmer la valeur configurée.

```
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
```

Les **Taille de la fenêtre : 64** affiché dans le résultat ne correspond pas à la fenêtre de relecture configurée **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. Afin de s'assurer que la taille réelle de la fenêtre anti-relecture est la même que la taille configurée, appliquez l'une des commandes de la section pour mesurer l'efficacité de la fenêtre de relecture configurée.

**Étape 3.** Configurez et activez simultanément le suivi des paquets et 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 plat cond start
```

**Étape 4.** Récapitulatif du suivi des paquets :

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

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

(IpsecInput) Abandons de paquets :

```
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 1 0 0 1 0 0 0 1 1 1.**)

### Étape 6. Vérification de l'index 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: 0x000000000010dc0
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 fenêtre anti-relecture la plus élevée (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 :

```
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

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.** Collecter et obtenir 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: 00b6dfef DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

**Étape 9.** Convertissez en décimal le numéro de série et réorganisez-les en calcul simple :

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: 00b6dfef 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.** Convertissez en décimal le numéro de série et réorganisez-les en calcul simple :

Difference:

```
815 PKT: Decimal: 11984964 ***** Highest Value
```

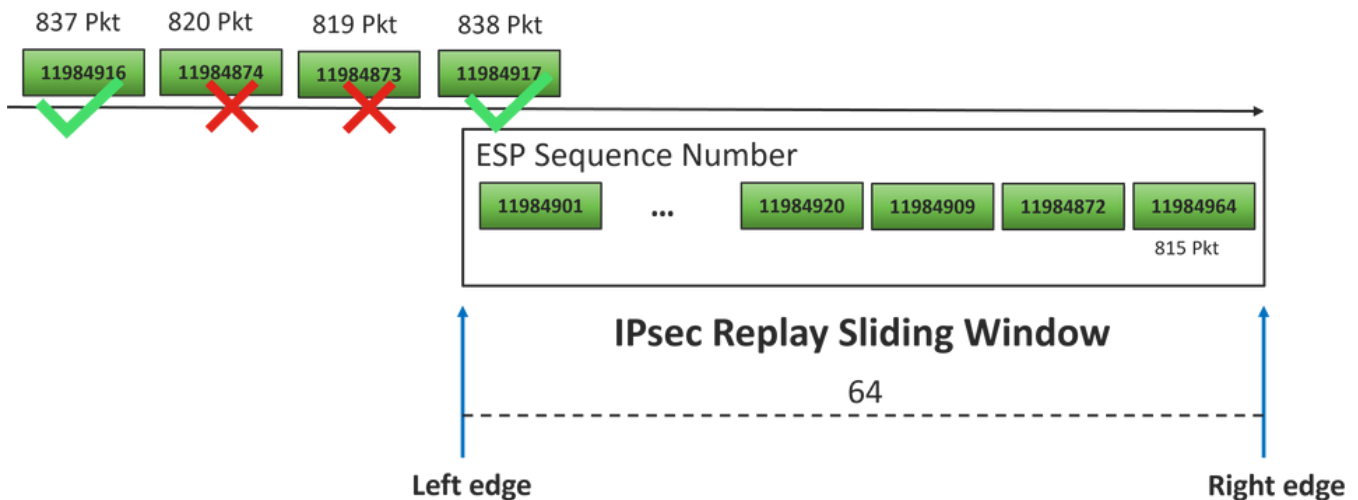
```
-----
815(Highest) - X PKT = Diff
```

```

-----
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, on peut visualiser la fenêtre glissante avec la **taille de fenêtre 64** et le **bord droit 11984964** comme représenté sur 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 le voit à l'étape 2, une des commandes de la section Commandes pour prendre effet de la fenêtre de relecture configurée doit être appliquée pour que la taille de fenêtre 1024 prenne effet.

## Outil de capture Wireshark supplémentaire

Le logiciel Wireshark est un autre outil utile permettant de corréliser 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

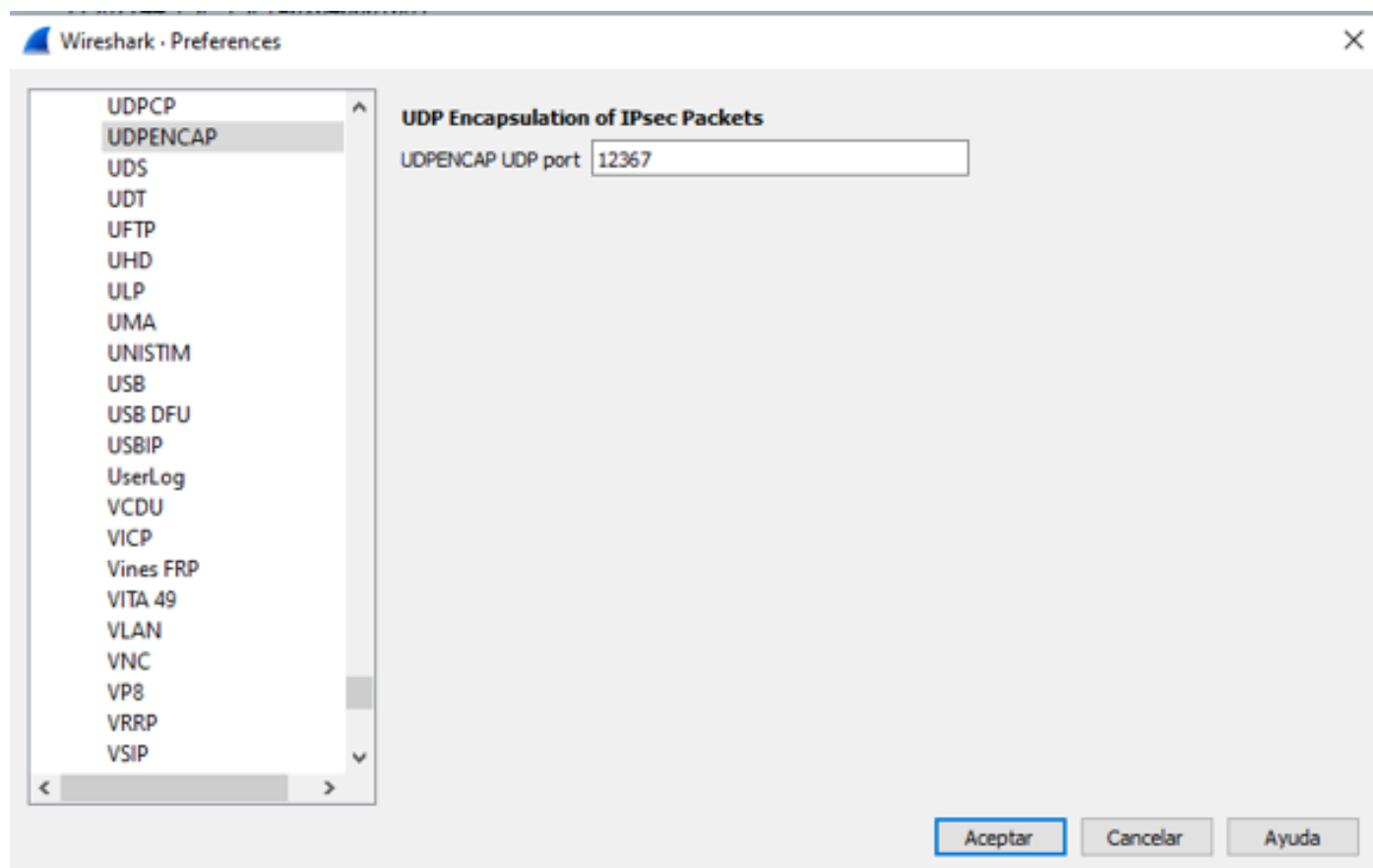
Configurez la capture de paquets pour la direction entrante et exportez-la vers le fichier pcap.

```

monitor capture CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TengigabitEthernet0/0/0 in
monitor capture CAP star
monitor capture CAP stop
monitor capture CAP export bootflash:Anti-replay.pca

```

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



Une fois UDPENCAP en place avec le port droit, les informations ESP s'affichent comme illustré dans l'image.

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	ESP Sequence	Info
17246	17.254037	10.62.33.91	10.62.63.251	ESP	11967739	ESP (SPI=0x04000106)
17247	17.254037	10.62.33.91	10.62.63.251	ESP	11967740	ESP (SPI=0x04000106)
17248	17.254037	10.62.33.91	10.62.63.251	ESP	11967741	ESP (SPI=0x04000106)
17249	17.254037	10.62.33.91	10.62.63.251	ESP	11967742	ESP (SPI=0x04000106)
17250	17.254037	10.62.33.91	10.62.63.251	ESP	11967743	ESP (SPI=0x04000106)
17251	17.255028	10.62.33.91	10.62.63.251	ESP	11967744	ESP (SPI=0x04000106)
17252	17.255028	10.62.33.91	10.62.63.251	ESP	11967745	ESP (SPI=0x04000106)
17253	17.255028	10.62.33.91	10.62.63.251	ESP	11967746	ESP (SPI=0x04000106)
17254	17.255028	10.62.33.91	10.62.63.251	ESP	11967747	ESP (SPI=0x04000106)
17255	17.255028	10.62.33.91	10.62.63.251	ESP	11967748	ESP (SPI=0x04000106)
17256	17.256035	10.62.33.91	10.62.63.251	ESP	11967750	ESP (SPI=0x04000106)
17257	17.257043	10.62.33.91	10.62.63.251	ESP	11967756	ESP (SPI=0x04000106)
17258	17.258034	10.62.33.91	10.62.63.251	ESP	11967762	ESP (SPI=0x04000106)

> Frame 84: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)

> Ethernet II, Src: Cisco\_99:bc:08 (7c:f8:80:99:bc:08), Dst: Cisco\_6b:20:00 (e0:69:ba:6b:20:00)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 972

> Internet Protocol Version 4, Src: 10.62.33.91, Dst: 10.62.63.251

> User Datagram Protocol, Src Port: 12367, Dst Port: 12347

UDP Encapsulation of IPsec Packets

Encapsulating Security Payload

ESP SPI: 0x04000106 (67109126)

ESP Sequence: 11929927

```

0000 e0 69 ba 6b 20 00 7c f8 80 99 bc 08 81 00 03 cc  ·i·k·|· ······
0010 08 00 45 54 00 72 ab 73 40 00 fd 11 5b e1 0a 3e  ··ET·r·s @··[·>
0020 21 5b 0a 3e 3f fb 30 4f 30 3b 00 5e 00 00 04 00  ![·>?·00 0;·^···
0030 01 06 00 b6 09 47 00 00 00 00 8c d2 66 f7 c0 8d  ··G· ···f·
0040 6c 97 57 8a fc d1 ff dc 33 a9 bb 22 0c de 5d 60  l·W· ··· 3·"·]·
0050 f3 e8 a3 83 49 d2 c7 59 b4 b2 92 b5 eb d0 e5 82  ···I·Y ······
0060 74 8c 88 52 30 32 8d db 66 ce c9 dc 2e d2 bc fc  t·R02· ·f· ···
0070 9c a8 07 1c 3e e1 8f 29 e1 ba a2 3a f8 c4 90 ea  ···>·) ···:·
0080 58 3c 82 72                                     X<·r

```

## Informations connexes

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

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.