Dépannage des échecs de vérification de l'anti-relecture IPsec

Table des matières

Introduction

Ce document décrit un problème lié aux échecs de vérification anti-relecture IPsec (Internet Protocol Security) et fournit des solutions possibles.

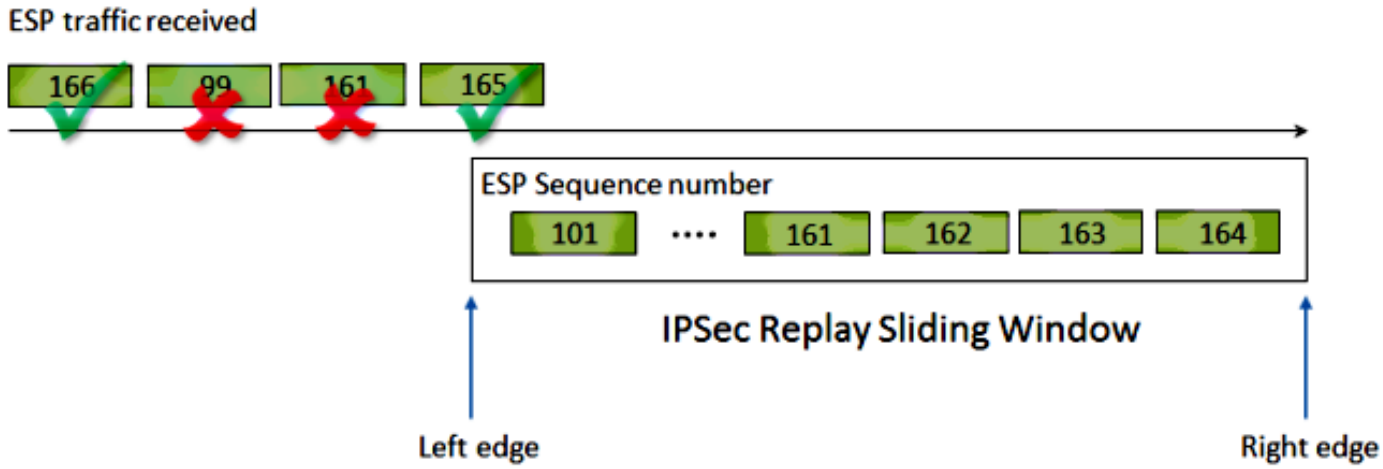
Informations générales

Présentation des attaques par relecture

Une attaque par relecture est une forme d'attaque réseau dans laquelle une transmission de données valide est enregistrée de manière malveillante ou frauduleuse, puis répétée. Il s'agit d'une tentative d'altération de la sécurité par une personne qui enregistre des communications légitimes et les répète afin d'usurper l'identité d'un utilisateur valide et d'interrompre ou de provoquer un impact négatif sur les connexions légitimes.

Protection de vérification de relecture IPsec

Un numéro de séquence qui augmente de façon monotone est attribué à chaque paquet chiffré par IPsec pour fournir une protection anti-relecture contre un attaquant. Le point d'extrémité IPsec récepteur garde une trace des paquets qu'il a déjà traités lorsqu'il utilise ces numéros et une fenêtre glissante de numéros de séquence acceptables. La taille de fenêtre anti-relecture par défaut dans l'implémentation de Cisco IOS® est de 64 paquets, comme illustré dans cette image :



Lorsque la protection anti-relecture est activée sur un point d'extrémité de tunnel IPsec, le trafic IPsec entrant est traité comme suit :

- Si le numéro d'ordre se trouve dans la fenêtre et n'a pas été reçu auparavant, l'intégrité du paquet est vérifiée. Si le paquet réussit la vérification d'intégrité, il est accepté et le routeur marque que ce numéro de séquence a été reçu. Par exemple, un paquet avec le numéro d'ordre ESP (Encapsulating Security Payload) 162.
- Si le numéro d'ordre se trouve dans la fenêtre, mais qu'il a déjà été reçu, le paquet est abandonné. Ce paquet dupliqué est rejeté et la suppression est enregistrée dans le compteur de relecture.

- 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. Par exemple, si un paquet valide avec un numéro de séquence de 189 est reçu, alors le nouveau bord droit de la fenêtre est défini sur 189, et le bord gauche est 125 (189 - 64 [taille de fenêtre]).
- Si le numéro de séquence est inférieur au bord gauche, le paquet est abandonné et enregistré dans le compteur de relecture. Il s'agit d'un paquet dans le désordre.

Dans les cas où un échec de vérification de relecture se produit et où le paquet est abandonné, le routeur génère un message Syslog semblable à ceci :

```
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle n, src_addr x.x.x.x, dest_addr y.
```

Remarque : la détection de relecture est basée sur l'hypothèse que l'association de sécurité IPsec existe entre deux homologues seulement. Le VPN de transport chiffré de groupe (GETVPN) utilise une seule SA IPsec entre plusieurs homologues. Par conséquent, GETVPN utilise un mécanisme de vérification anti-relecture entièrement différent appelé Time Based Anti-Replay Failure. Ce document couvre uniquement l'anti-relecture basée sur compteur pour les tunnels IPsec point à point.

Remarque : la protection anti-relecture est un service de sécurité important que le protocole IPsec offre. La désactivation de la fonction anti-relecture IPsec a des implications en matière de sécurité et doit être effectuée avec discrétion.

Problèmes pouvant entraîner des abandons de relecture IPsec

Comme décrit précédemment, les contrôles de relecture ont pour but de protéger contre les répétitions malveillantes de paquets. Cependant, dans certains cas, une vérification de relecture ayant échoué ne peut pas être due à une raison malveillante :

- L'erreur peut résulter d'un paquet suffisant qui est réorganisé dans le chemin réseau entre les points d'extrémité du tunnel. Cela peut se produire s'il existe plusieurs chemins réseau entre les homologues.
- L'erreur peut être causée par des chemins de traitement de paquets inégaux dans Cisco IOS. Par exemple, les paquets IPsec fragmentés qui nécessitent un réassemblage IP avant le déchiffrement peuvent être suffisamment retardés pour sortir de la fenêtre de relecture au moment où ils sont traités.
- L'erreur peut être causée par la qualité de service (QoS) activée sur le point d'extrémité IPsec émetteur ou dans le chemin d'accès réseau. Avec la mise en oeuvre de Cisco IOS, le chiffrement IPsec se produit avant la QoS dans le sens de la sortie. Certaines fonctionnalités de QoS, telles que la mise en file d'attente à faible latence (LLQ), peuvent entraîner le désordre de la livraison des paquets IPsec et leur abandon par le point d'extrémité récepteur en raison d'un échec de vérification de relecture.
- Un problème de configuration/d'exploitation du réseau peut dupliquer des paquets lorsqu'ils transitent sur le réseau.
- Un pirate (homme du milieu) peut potentiellement retarder, abandonner et dupliquer le trafic ESP.

Dépannage des abandons de relecture IPsec

La clé pour dépanner les abandons de relecture IPsec est d'identifier quels paquets sont abandonnés en raison de la relecture, et d'utiliser des captures de paquets pour déterminer si ces paquets sont effectivement relus des paquets ou des paquets qui sont arrivés sur le routeur récepteur en dehors de la fenêtre de relecture. Afin de faire correspondre correctement les paquets abandonnés à ce qui est capturé dans la trace de l'analyseur, la première étape consiste à identifier l'homologue et le flux IPsec auquel les paquets abandonnés appartiennent et le numéro de séquence ESP du paquet.

Utilisation de la fonction de suivi des paquets Cisco IOS XE Datapath

Sur les plates-formes de routeurs qui exécutent Cisco IOS® XE, des informations sur l'homologue ainsi que l'index de paramètres de sécurité IPsec (SPI) sont imprimées dans le message Syslog lorsqu'un abandon se produit, afin d'aider à résoudre les problèmes anti-relecture. Cependant, le

numéro de séquence ESP est un élément d'information clé qui n'est toujours pas détecté. Le numéro de séquence ESP est utilisé afin d'identifier de manière unique un paquet IPsec dans un flux IPsec donné. Sans le numéro de séquence, il devient difficile d'identifier exactement quel paquet est abandonné dans une capture de paquet.

La fonctionnalité de suivi de paquets de chemin de données de Cisco IOS XE peut être utilisée dans cette situation lorsque la perte de relecture est observée, avec ce message Syslog :

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:060 TS:00000001132883828011
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3, src_addr 10.2.0.200, dest_addr
```

Afin de faciliter l'identification du numéro de séquence ESP pour le paquet abandonné, complétez ces étapes avec la fonctionnalité de suivi de paquet :

Étape 1. Configurez le filtre de débogage conditionnel de la plate-forme afin de faire correspondre le trafic du périphérique homologue :

```
debug platform condition ipv4 10.2.0.200/32 ingress
debug platform condition start
```

Étape 2. Activez le suivi des paquets avec l'option copy afin de copier les informations d'en-tête de paquet :

```
debug platform packet enable
debug platform packet-trace packet 64
debug platform packet-trace copy packet input l3 size 100
```

Étape 3. Lorsque des erreurs de relecture sont détectées, utilisez le tampon de suivi des paquets afin d'identifier le paquet abandonné en raison de la relecture, et le numéro de séquence ESP peut être trouvé dans le paquet copié :

<#root>

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
```

Le résultat précédent montre que les paquets numéros 6 et 7 sont abandonnés, de sorte qu'ils peuvent être examinés en détail maintenant :

<#root>

```
Router#
```

show platform packet-trace packet 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
```

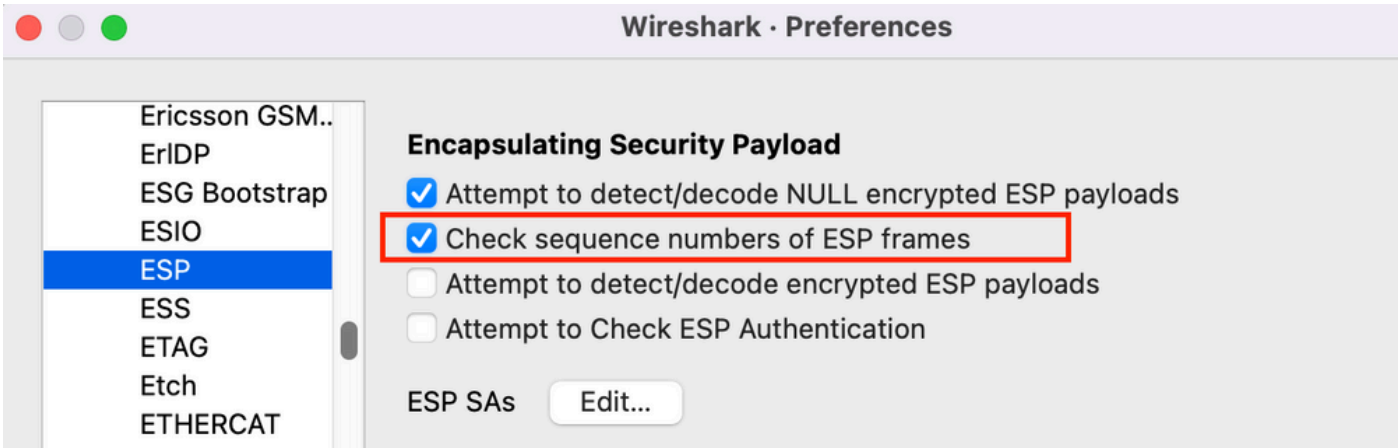
Le numéro de séquence ESP a un décalage de 24 octets qui commence par l'en-tête IP (ou 4 octets des données utiles du paquet IP), comme souligné en gras dans le résultat précédent. Dans cet exemple particulier, le numéro de séquence ESP du paquet abandonné est 0x6.

Collecter les captures de paquets

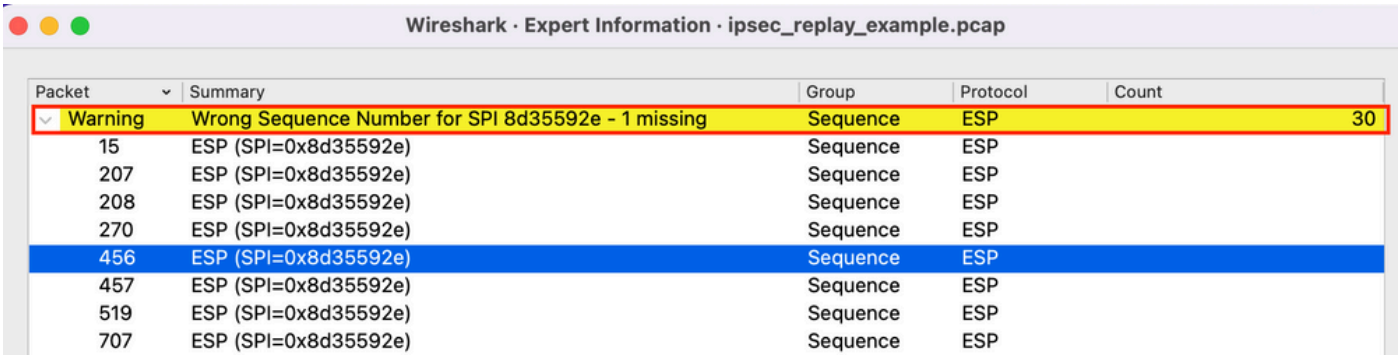
En plus de l'identification des informations de paquet pour le paquet abandonné en raison d'un échec de vérification de relecture, une capture de paquet pour le flux IPsec en question doit être collectée simultanément. Cela facilite l'examen du modèle de numéro de séquence ESP dans le même flux IPsec pour aider à déterminer la raison de la perte de relecture. Pour plus d'informations sur la façon d'utiliser la capture de paquets intégrée (EPC) sur les routeurs Cisco IOS XE, consultez Exemple de configuration de capture de paquets intégrée pour Cisco IOS et Cisco IOS XE.

Utiliser l'analyse de numéro de séquence Wireshark

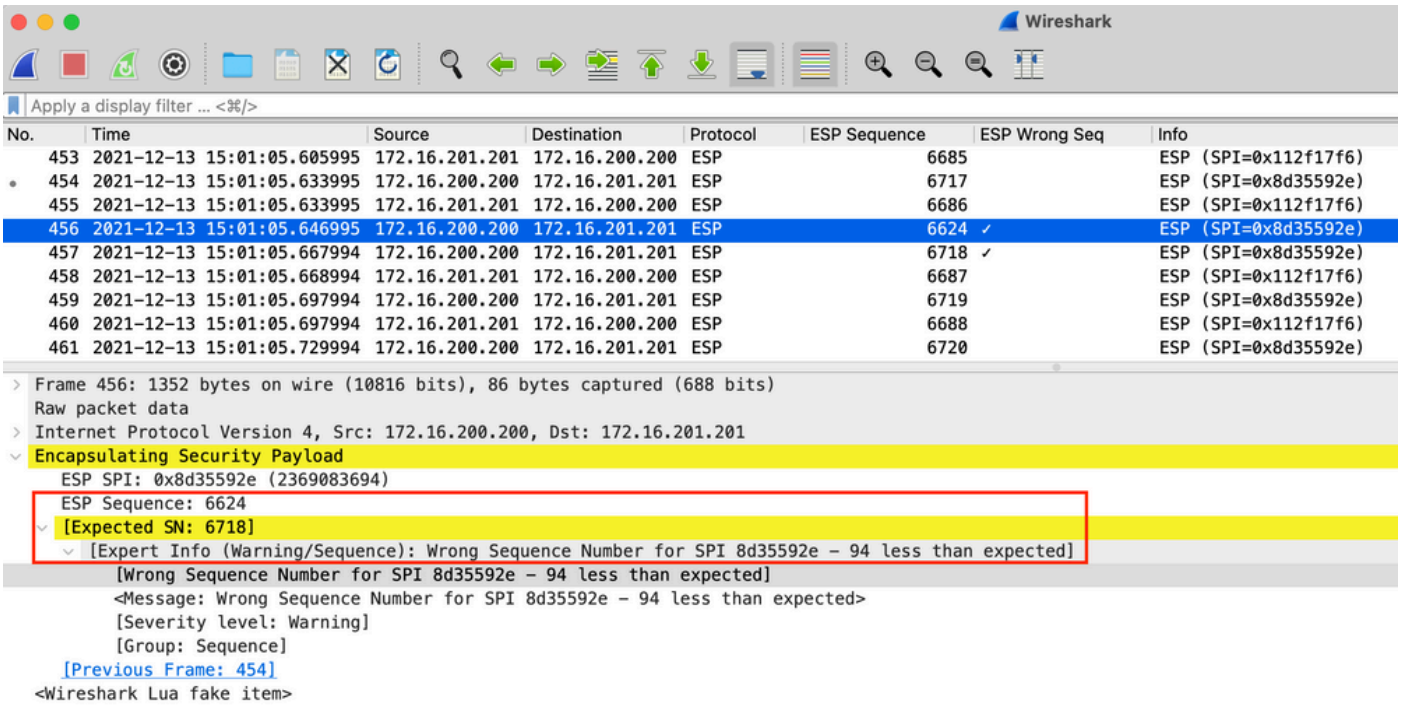
Une fois que la capture de paquets pour les paquets chiffrés (ESP) sur l'interface WAN a été collectée, Wireshark peut être utilisé pour effectuer une analyse de numéro de séquence ESP pour toute anomalie de numéro de séquence. Assurez-vous tout d'abord que la vérification du numéro de séquence est activée sous Préférences > Protocoles > ESP comme illustré dans l'image :



Vérifiez ensuite les problèmes de numéro de séquence ESP sous Analyze > Expert information comme suit :



Cliquez sur l'un des paquets dont le numéro d'ordre est incorrect pour obtenir des détails supplémentaires, comme suit :



Solution

Une fois que l'homologue est identifié et que la capture de paquets est collectée pour les abandons de relecture, trois scénarios possibles peuvent expliquer les échecs de relecture :

1. Il s'agit d'un paquet valide qui a été retardé :
   Les captures de paquets permettent de confirmer si le paquet est réellement valide et si le problème est insignifiant (en raison de la latence du réseau ou de problèmes de chemin de transmission) ou nécessite un dépannage plus approfondi. Par exemple, la capture montre un paquet avec un numéro de séquence de X qui arrive dans le désordre, et la taille de la fenêtre de relecture est actuellement définie sur 64. Si un paquet valide avec un numéro de séquence (X + 64) arrive avant le paquet X, la fenêtre est décalée vers la droite, puis le paquet X est abandonné en raison d'un échec de relecture.

Dans de tels scénarios, il est possible d'augmenter la taille de la fenêtre de relecture ou de désactiver le contrôle de relecture pour s'assurer que de tels retards sont considérés comme acceptables et que les paquets légitimes ne sont pas rejetés. Par défaut, la taille de la fenêtre de relecture est relativement petite (taille de fenêtre de 64). Si vous augmentez la taille, le risque d'attaque n'est pas beaucoup plus élevé. Pour plus d'informations sur la façon de configurer une fenêtre d'anti-relecture IPsec, référez-vous au document Comment configurer la fenêtre d'anti-relecture IPsec : développement et désactivation.

Conseil : si la fenêtre de relecture est désactivée ou modifiée dans le profil IPSec utilisé sur une interface de tunnel virtuelle (VTI), les modifications ne prennent pas effet tant que le profil de protection n'est pas supprimé et réappliqué ou que l'interface de tunnel n'est pas réinitialisée. Ce comportement est attendu, car les profils IPsec sont un modèle utilisé pour créer une carte de profil de tunnel lorsque l'interface de tunnel est activée. Si l'interface est déjà active, les modifications apportées au profil n'ont pas d'impact sur le tunnel tant que l'interface n'est pas réinitialisée.

Remarque : les premiers modèles ASR (Aggregation Services Router) 1000 (tels que l'ASR1000 avec ESP5, ESP10, ESP20 et ESP40, ainsi que l'ASR1001) ne prenaient pas en charge une taille de fenêtre de 1024, même si l'interface de ligne de commande autorisait cette configuration. Par conséquent, la taille de fenêtre qui est rapportée dans le résultat de la commande show crypto ipsec sa ne peut pas être correcte. Utilisez la commande show crypto ipsec sa peer ip-address platform afin de vérifier la taille de la fenêtre matérielle anti-replay. La taille de fenêtre par défaut est de 64 paquets sur toutes les plates-formes. Pour plus d'informations, référez-vous au bogue Cisco ID CSCso45946. Les plates-formes de routage Cisco IOS XE ultérieures (telles que ASR1K avec ESP100 et ESP200, ASR1001-X et ASR1002-X, les routeurs de la gamme ISR 4000 et les routeurs de la gamme Catalyst 8000) prennent en charge une taille de fenêtre de 1024 paquets dans les versions 15.2(2)S et ultérieures.

---

2. Elle est due à la configuration QoS sur le point d'extrémité expéditeur :
   Si la réorganisation des paquets après IPsec est provoquée par la configuration QoS sur le périphérique émetteur IPsec, une atténuation potentielle est d'utiliser l'espace de numéros de séquence multiples par SA IPsec disponible sur les plates-formes IOS XE.

3. Il s'agit d'un paquet dupliqué qui a été reçu précédemment :
   Si c'est le cas, alors deux paquets ou plus avec le même numéro de séquence ESP dans le même flux IPsec peuvent être observés dans la capture de paquets. Dans ce cas, la suppression de paquets est attendue car la protection de relecture IPsec fonctionne comme prévu pour empêcher les attaques de relecture sur le réseau, et le Syslog est juste informatif. Si cette situation persiste, elle doit être examinée en tant que menace potentielle pour la sécurité.

Remarque : les échecs de vérification de relecture ne sont visibles que lorsqu'un algorithme d'authentification est activé dans le jeu de transformation IPsec. Il est également possible de supprimer ce message d'erreur en désactivant l'authentification et en effectuant uniquement le cryptage. Toutefois, cela est fortement déconseillé en raison des implications de sécurité de l'authentification désactivée.

Additional Information

Dépannage des erreurs de relecture sur les anciens routeurs avec Cisco IOS Classic

Les abandons de relecture IPsec sur les anciens routeurs de la gamme ISR G2 qui utilisent Cisco IOS sont différents des routeurs qui utilisent Cisco IOS XE, comme illustré ici :

```
<#root>

%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed

connection id=529, sequence number=13
```

La sortie du message ne fournit pas l'adresse IP de l'homologue ni les informations SPI. Afin de dépanner sur cette plate-forme, utilisez le « conn-id » dans le message d'erreur. Identifiez le « conn-id » dans le message d'erreur et recherchez-le dans la sortie show crypto ipsec sa, puisque la relecture est une vérification par SA (par opposition à une vérification par homologue). Le message Syslog fournit également le numéro de séquence ESP, qui peut aider à identifier de manière unique le paquet abandonné dans la capture de paquets.

Remarque : avec différentes versions de code, le "conn-id" est soit l'ID de connexion soit l'ID de flux pour l'association de sécurité entrante.

Ceci est illustré ici :

```
<#root>

%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>
```

Comme vous pouvez le voir dans ce résultat, la perte de relecture provient de l'adresse d'homologue 10.2.0.200 avec un SPI SA ESP entrant de 0xE7EDE943. Le message de journal lui-même indique également que le numéro de séquence ESP du paquet abandonné est 13. La

combinaison de l’adresse homologue, du numéro SPI et du numéro de séquence ESP peut être utilisée afin d’identifier de manière unique le paquet abandonné dans la capture de paquets.

Remarque : le message Syslog de Cisco IOS est limité en débit pour le paquet de plan de données qui tombe à un par minute. Afin d'obtenir un compte précis du nombre exact de paquets abandonnés, utilisez la commande show crypto ipsec sa detail comme montré précédemment.

Utilisation du logiciel Cisco IOS XE antérieur

Sur les routeurs qui exécutent les versions précédentes de Cisco IOS XE, le message « REPLAY_ERROR » signalé dans le Syslog ne peut pas imprimer le flux IPsec réel avec les informations d'homologue où le paquet rejoué est abandonné, comme indiqué ici :

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread: 095 TS:00000000240306197890
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3
```

Afin d'identifier l'homologue IPsec correct et les informations de flux, utilisez le Handle du plan de données (DP) imprimé dans le message Syslog comme paramètre d'entrée SA Handle dans cette commande, afin de récupérer les informations de flux IPsec sur le Quantum Flow Processor (QFP) :

<#root>

```
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
                   : 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>
```

Un script EEM (Embedded Event Manager) peut également être utilisé pour automatiser la collecte de données :

```
event manager applet Replay-Error
 event syslog pattern "%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error"
 action 1.0 regexp "([0-9]+)$" "$_syslog_msg" dph
 action 2.0 cli command "enable"
 action 3.0 cli command "show platform hardware qfp active feature ipsec sa $dph |
 append bootflash:replay-error.txt"
```

Dans cet exemple, la sortie collectée est redirigée vers le bootflash. Afin de voir ce résultat, utilisez la commande more bootflash:replay-error.txt.

Informations connexes

- Conception du réseau de référence de la solution VPN IPSec (V3PN) compatible voix et vidéo
- Configuration de la fenêtre Anti-Replay d'IPsec : développement et désactivation.
- Assistance et documentation techniques - Cisco Systems

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.