Pannes de contrôle d'anti-relecture d'IPSec

Contenu

Introduction

Ce document décrit un problème qui concerne une panne de contrôle d'anti-relecture d'IPSec (IPSec), et fournit dépannent des procédures et des solutions possibles au problème.

> **Note**: La protection d'anti-relecture est un important service de sécurité que le protocole IPsec offre. La désactivation d'anti-relecture d'IPSec a des implications en matière de sécurité, et devrait seulement être utilisée avec prudence.

Informations générales

Description d'attaque par relecture

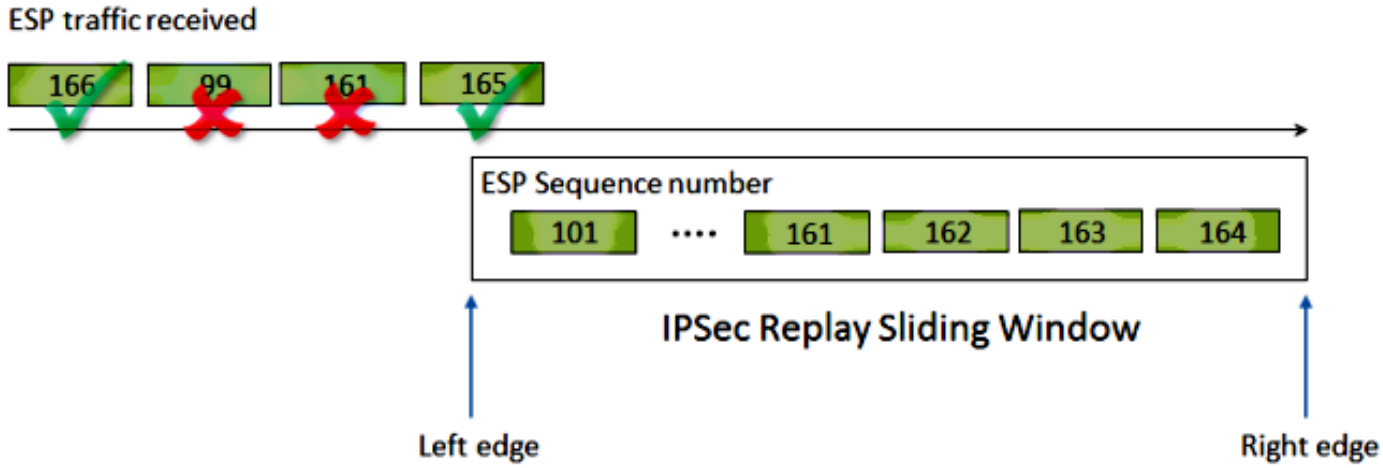
Une attaque par relecture est une forme d'attaque réseau dans laquelle une transmission de données valide avec malveillance ou frauduleux est répétée ou retardee. C'est une tentative de renverser la Sécurité par quelqu'un qui enregistre des transmissions légitimes et les répète afin de personnifier un utilisateur valide, et de perturber ou entraîner l'incidence négative pour les connexions légitimes.

Description de panne de contrôle de rediffusion

IPSec assure la protection d'anti-relecture contre un attaquant qui reproduit les paquets chiffrés avec l'attribution d'un numéro de séquence monotoniquement croissant à chaque paquet chiffré. Le point final de réception d'IPSec maintient que les paquets il a déjà traité sur la base de ces nombres avec l'utilisation d'une fenêtre glissante de tous les numéros de séquence acceptables. Actuellement, la taille de la fenêtre par défaut d'anti-relecture dans l'implémentation de Cisco IOS® est 64 paquets.

Note: Les demandes d'amélioration CSCva65805 et CSCva65836 ont été classées d'augmenter la taille de la fenêtre par défaut de rediffusion à 512 pendant que 64 est considérés impraticable petits pour les réseaux modernes.

Ceci est illustré dans cette figure :



Voici les étapes pour traiter le trafic entrant d'IPSec sur recevant le périphérique du tunnel avec l'anti-relecture activée :

1. Quand un paquet est reçu, si le numéro de séquence fait partie de la fenêtre et n'était pas précédemment reçu, le paquet est reçu, et marqué en tant que reçu avant qu'il soit envoyé à la vérification d'intégrité.

2. Si le numéro de séquence fait partie de la fenêtre et était précédemment reçu, le paquet est lâché, et le compteur de rediffusion est incrémenté.

3. Si le numéro de séquence est plus grand que le numéro de séquence le plus élevé dans la fenêtre, le paquet est reçu, et marqué en tant que reçu. La fenêtre glissante est alors déplacée vers la droite.
   Note: Ceci seulement se produit si le paquet est valide et passe des contrôles d'intégrité.
4. Si le numéro de séquence est moins que le plus bas ordre dans la fenêtre, le paquet est lâché, et le compteur de rediffusion est incrémenté.

Dans les deuxièmes et quatrièmes scénarios, une panne de contrôle de rediffusion se produit, et le routeur affiche un message d'erreur semblable à ceci :

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

Note: Le Group Encrypted Transport VPN (GETVPN) a une panne basée entièrement différente d'anti-relecture de temps appelé de contrôle d'anti-relecture. Ce document couvre seulement l'anti-relecture basée sur compteur.

Problème

Comme décrit précédemment, le but des contrôles de rediffusion est de se protéger contre des

répétitions malveillantes des paquets. Cependant, il y a quelques scénarios où un contrôle défectueux de rediffusion ne pourrait pas être dû à une raison malveillante :

- L'erreur pourrait résulter d'un paquet commandent à nouveau dans le support de transmission. C'est particulièrement vrai si les chemins parallèles existent.

- L'erreur pourrait sont provoqué par par les chemins inégaux de traitement de paquets à l'intérieur du Cisco IOS. Par exemple, grands paquets d'IPSec qui exigent le réassemblage IP avant que le déchiffrement pourrait être retardé assez, dans un système sous le chargement, afin de tomber en dehors de la fenêtre de rediffusion avant qu'ils soient traités.

- L'erreur pourrait sont provoqué par par le Qualité de service (QoS) activé sur le point final de envoi d'IPSec. Avec le Cisco IOS implémentation, le chiffrement IPSec se produit avant QoS dans la direction de sortie. Certaines caractéristiques de QoS, telles que la basse latence s'alignant (LLQ), peuvent faire devenir la livraison de paquet d'IPSec en panne et chutée par le point final de réception dû à une panne de contrôle de rediffusion.

Dépannez les baisses de rediffusion d'IPSec

La clé pour dépanner des baisses de rediffusion d'IPSec est d'identifier les pertes de paquets devant rejouer, et utilise des captures de paquet afin de confirmer si ces paquets sont en effet des paquets rejoués ou des paquets qui sont arrivés sur le routeur récepteur en dehors de la fenêtre de rediffusion. Afin d'apparier correctement les paquets abandonnés à ce qui est capturé dans le tracé de renifleur, la première étape est d'identifier le pair et l'écoulement d'IPSec auxquels les paquets lâchés appartiennent. Ceci est fait différemment a basé sur la plate-forme de routeur.

Plate-forme de l'Integrated Services Router de Cisco (ISR) /ISR G2 qui exécute le Cisco IOS classique

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 de **show crypto ipsec sa**, puisque la rediffusion est un contrôle par-**SA** (association de sécurité) (par opposition à un par-**pair**). Le message de Syslog fournit également le numéro de séquence de Protocole ESP (Encapsulating Security Payload), qui peut aider seulement à identifier le paquet abandonné dans la capture de paquet.

> **Note**: Avec des différentes versions de code, le conn.-**id** est l'**id** ou **flow_id conn.** pour SA d'arrivée.

Ceci est illustré ici :

```
%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 peut être vu de cette sortie, la baisse de rediffusion est de l'adresse de pair de **10.2.0.200** avec un index d'arrivée de paramètre de Sécurité de ESP SA (SPI) de **0xE7EDE943**. Il peut également noter du message de log lui-même que le numéro de séquence de l'ESP pour le paquet abandonné est **13**. Ainsi, la combinaison de l'adresse de pair, du nombre SPI, et du numéro de séquence de l'ESP peut être utilisée afin d'identifier seulement le paquet abandonné dans la capture de paquet.

> **Note**: Le message de Syslog de Cisco IOS est débit-limité pour des pertes de paquets de dataplane. Afin d'obtenir un compte précis du numéro exact de paquets a relâché, utilise la commande de **détail de show crypto ipsec sa** comme affiché précédemment. En outre, la note en code plus tôt que la version 12.4(4)T de Cisco IOS, les compteurs pourrait être mise à jour inexactement. Ceci est réparé dans l'ID de bogue Cisco CSCsa90034.

L'agrégation de Cisco entretient le routeur (ASR) ce Cisco IOS XE de passages

Sur la plate-forme ASR, le REPLAY_ERROR signalé dans certaines des releases plus tôt de Cisco IOS XE ne pourrait pas imprimer l'écoulement réel d'IPSec où le paquet rejoué est lâché, comme affiché ici :

```
%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>
```

Afin d'identifier l'IPSec correct scrutez et circulez les informations, utilisent le traitement du plan de données (DP) imprimé dans le message de Syslog comme le **traitement de** paramètre d'entrée **SA** dans cette commande afin de récupérer les informations d'écoulement d'IPSec sur le processeur d'écoulement de Quantum (QFP) :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

Si la version de Cisco IOS sur l'ASR est version 3.7 de pre-XE, alors le message d'erreur se connecte simplement le message avec le **traitement DP** et aucune informations sur le peer/SPI auquel le paquet de coupable appartient. C'est où l'ID de bogue Cisco CSCtw69096 devient approprié :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
```

```
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

En pareil cas, ce script inclus du gestionnaire d'événement (EEM) peut être utilisé afin de voir quels pair et SPI déclenche les messages d'anti-relecture :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

Afin de voir la sortie sur l'ASR elle-même, écrivez **plus de bootflash : commande replay-error.txt** périodiquement.

Travail avec la configuration de suivi de paquet ASR Datapath

Avec le Logiciel Cisco IOS XE version 2 plus récent pour l'ASR1000, des informations sur le pair aussi bien que l'IPSec SPI sont également imprimés afin d'aider à dépanner des problèmes d'anti-relecture. Cependant, une information principale qui est toujours manquer comparé à ce qui est imprimé sur les Plateformes d'ISR G2 que le classique de Cisco IOS de passage est le numéro de séquence de l'ESP. Le numéro de séquence de l'ESP est utilisé afin d'identifier seulement un paquet d'IPSec dans un écoulement indiqué d'IPSec. Sans numéro de séquence, il devient difficile de l'identifier exactement que le paquet obtient relâché dans une capture de paquet.

Dans la version 3.10 (15.3(3)S) de Cisco IOS XE, une nouvelle infrastructure de suivi de paquet a été introduite afin d'aider à dépanner la question de transfert de paquet de dataplane, et elle peut être utilisée dans cette situation particulière de dépannage où on observe cette baisse de rediffusion sur l'ASR :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

Afin d'aider à identifier le numéro de séquence de l'ESP pour le paquet relâché, terminez-vous ces étapes avec la configuration de suivi de paquet :

1. Installez le filtre conditionnel d'élimination des imperfections de plate-forme afin d'apparier le trafic du périphérique de pair :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
```

```
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

2. Permettez au suivi de paquet avec l'option de **copie** afin de copier les informations d'en-tête de paquet :

```
Router#show platform hardware qfp active feature ipsec sa 3
QFP ipsec sa Information

QFP sa id: 3
pal sa id: 2
QFP spd id: 1
QFP sp id: 2
QFP spi: 0x4c1d1e90(1276976784)
crypto ctx: 0x000000002e03bfff
flags: 0xc000800 (Details below)
: src:IKE valid:Yes soft-life-expired:No hard-life-expired:No
: replay-check:Yes  proto:0  mode:0  direction:0
: qos_preclassify:No qos_group:No
: frag_type:BEFORE_ENCRYPT df_bit_type:COPY
: sar_enable:No getvpn_mode:SNDRCV_SA
: doing_translation:No assigned_outside_rport:No
: inline_tagging_enabled:No
qos_group: 0x0
mtu: 0x0=0
sar_delta: 0
sar_window: 0x0
sibling_sa: 0x0
sp_ptr: 0x8c392000
sbs_ptr: 0x8bfbf810
 local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200
cgid.cid.fid.rid: 0.0.0.0
ivrf: 0
fvrf: 0
trans udp sport: 0
trans udp dport: 0
first intf name: Tunnel1
<SNIP>
```

3. Quand des erreurs de rediffusion sont détectées, employez la mémoire tampon de tracé de paquets afin d'identifier le dû relâché par paquet pour rejouer, et le numéro de séquence de l'ESP peut être trouvé dans le paquet copié :

```
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
```

La sortie précédente prouve que les numéros **6** et **7 de** paquet sont abandonnés, ainsi ils peuvent être maintenant examinés en détail :

```
Router#show platform packet-trace  pac 6
Packet: 6 CBUG ID: 6
Summary
Input : GigabitEthernet4/0/0
Output : Tunnel1
State : DROP 053 (IpsecInput)
Timestamp : 3233497953773
Path Trace
Feature: IPV4
Source : 10.2.0.200
Destination : 10.1.0.100
Protocol : 50 (ESP)
Feature: IPSec
Action : DECRYPT
SA Handle : 3
SPI : 0x4c1d1e90
Peer Addr : 10.2.0.200
Local Addr: 10.1.0.100
Feature: IPSec
Action : DROP
Sub-code : 019 - CD_IN_ANTI_REPLAY_FAIL
Packet Copy In
45000428 00110000 fc329575 0a0200c8 0a010064 4c1d1e90 00000006 790aa252
e9951cd9 57024433 d97c7cb8 58e0c869 2101f1ef 148c2a12 f309171d 1b7a4771
d8868af7 7bae9967 7d880197 46c6a079 d0143e43 c9024c61 0045280a d57b2f5e
23f06bc3 ab6b6b81 c1b17936 98939509 7aec966e 4dd848d2 60517162 9308ba5d
```

Le numéro de séquence de l'ESP a un décalage de **24** qui commence à partir de l'en-tête IP, comme souligné en gras et italique dans la sortie précédente. Dans cet exemple particulier, le numéro de séquence de l'ESP pour le paquet abandonné est **0x6**.

Solution

Après que le pair soit identifié, il y a trois scénarios possibles :

1. **C'est un paquet valide :** Les captures de paquet aident à confirmer si le paquet est réellement valide, et si le problème est non significatif (en raison des questions de latence de

réseau ou de chemin de transmission) ou exige un plus en profondeur dépannent. Par exemple, la capture affiche un paquet avec un numéro de séquence de **X** qui arrive en panne, et la taille de la fenêtre est fixée à **64**. Si **X + 64** paquets arrivent avant le paquet **X**, alors il obtient en raison abandonné d'une panne de rediffusion (ce n'est pas vraiment une attaque).

Dans de tels scénarios, augmentez la taille de la fenêtre de rediffusion afin de s'assurer que de tels retards sont expliqués et empêcher les paquets légitimes d'être abandonné. Par défaut, la taille de la fenêtre est assez petite (taille de la fenêtre de **64**). Si vous augmentez la taille, elle n'augmente pas considérablement le risque d'une attaque. Pour les informations sur la façon dont configurer une fenêtre d'anti-relecture d'IPsec, référez-vous le comment configurer la fenêtre d'anti-relecture d'IPsec : Développant et désactivant l'article.
Conseil : Si la fenêtre de rediffusion est désactivée ou modifié dans le profil IPSec et le profil IPSec est utilisé avec le tunnel protection sur une interface de tunnel virtuelle (VTI), les modifications ne les prendront pas effet jusqu'à ce que le profil de protection ou soit retiré et réappliqué ou l'interface de tunnel est remise à l'état initial. C'est comportement prévu parce que les profils IPSecs sont juste un modèle pour créer la carte de profil de tunnel quand l'interface de tunnel est activée (non fermé). Une fois que l'interface est déjà, les modifications au profil n'affectent pas le tunnel jusqu'à réappliquer ou l'interface est remise à l'état initial.**Note**: Un problème généralement produit sur des ASR, en ce qui concerne la taille de la fenêtre d'anti-relecture, est que les modèles classiques ASR1K (tels que l'ASR1K avec ESP5, ESP10, ESP20, et ESP40, avec l'ASR1001) ne prennent en charge pas réellement une taille de la fenêtre de 1024. Quoique la commande te permette pour fixer cette limite à 1024, la taille de la fenêtre est remise à l'état initial à 512 par le matériel. Pour cette raison, la taille de la fenêtre qui est signalée dans la sortie de commande de **show crypto ipsec sa** ne pourrait pas être correcte. Sélectionnez la commande de **plate-forme d'adresse IP homologue de show crypto ipsec sa** afin de vérifier la taille de la fenêtre d'anti-relecture de matériel. La taille de fenêtre par défaut est 64 paquets sur toutes les Plateformes. Le pour en savoir plus, se rapportent à l'ID de bogue Cisco CSCso45946. De plus nouveaux modèles ASR1K (tels que l'ASR1K avec ESP100 et ESP200, l'ASR1001-X et l'ASR1002-X, et également l'ISR-4400) prennent en charge une taille de fenêtre de 1024 paquets dans les versions 15.2(2)S et ultérieures.

2. **C'est un paquet qui tombe en dehors de la fenêtre de l'anti-relecture du récepteur :** Au cas où le point final de réception d'IPSec relâcherait les paquets rejoués (pendant qu'on le suppose à), les captures simultanées de renifleur du côté WAN de l'expéditeur et le récepteur aident à dépister si ceci est provoqué par par la mauvaise conduite de l'expéditeur, ou par des paquets rejoués dans le transit network.

3. **Il est dû à la configuration QoS sur l'extrémité de l'expéditeur :** Cette situation exige l'examen soigneux et certain un QoS accordant afin d'atténuer la condition. Pour une description plus en profondeur de ce thème et d'une solution potentielle, référez-vous aux considérations d'anti-relecture dans une Voix et un article d'IPSec activé par vidéo VPN (V3PN).

Note: Des pannes de contrôle de rediffusion sont seulement vues quand un algorithme d'authentification est activé dans le jeu de transformations d'IPSec. Une autre manière de supprimer ce message d'erreur est de désactiver l'authentification et d'exécuter le cryptage seulement ; cependant, c'est fortement dû découragé aux implications en matière de

sécurité de l'authentification handicapée.

Informations connexes

- Voix et conception de réseaux de référence de solution d'IPSec activée par vidéo VPN (V3PN)
- Comment configurer la fenêtre d'anti-relecture d'IPsec : Développer et désactiver.
- Support et documentation techniques - Cisco Systems