Risoluzione dei problemi relativi agli errori di verifica della protezione da riesecuzione IPSec

Sommario

Introduzione

In questo documento viene descritto un problema relativo agli errori dei controlli anti-replay di Internet Protocol Security (IPsec) e vengono fornite possibili soluzioni.

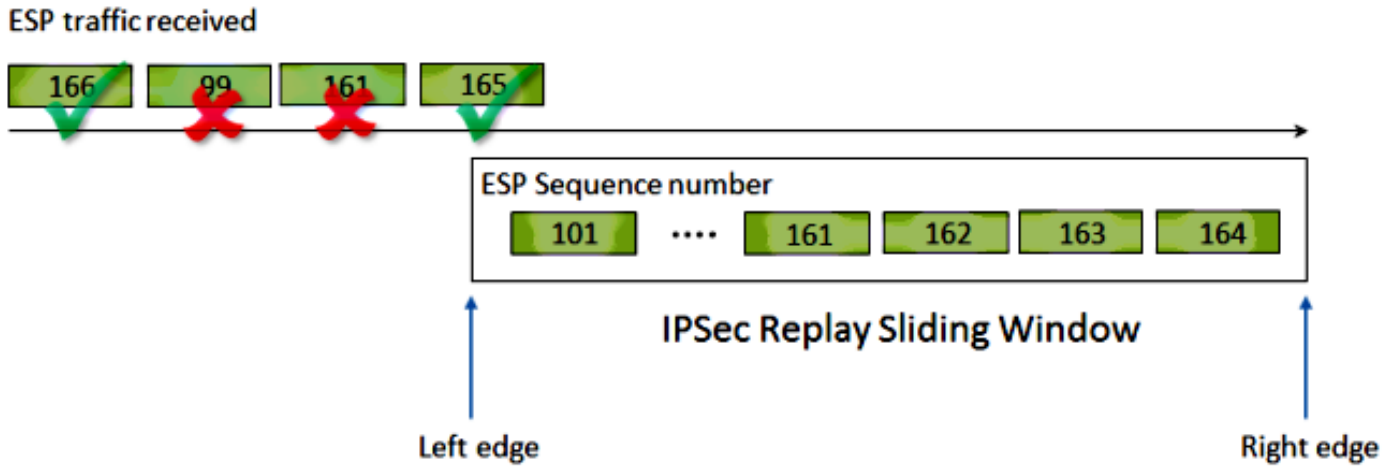
Premesse

Panoramica degli attacchi di tipo replay

Un attacco di tipo replay è una forma di attacco di rete in cui una trasmissione di dati valida viene registrata in modo dannoso o fraudolento e successivamente ripetuta. È un tentativo di sovvertire la sicurezza da parte di qualcuno che registra comunicazioni legittime e le ripete per impersonare un utente valido e interrompere o causare un impatto negativo sulle connessioni legittime.

Protezione controllo riproduzione IPsec

IPsec assegna a ciascun pacchetto crittografato un numero di sequenza che aumenta in modo monotono per fornire una protezione anti-replay contro un attacco. L'endpoint IPSec ricevente tiene traccia dei pacchetti già elaborati quando utilizza questi numeri e di una finestra scorrevole con numeri di sequenza accettabili. Le dimensioni predefinite della finestra anti-replay nell'implementazione di Cisco IOS® sono di 64 pacchetti, come mostrato nell'immagine:



Quando per un endpoint del tunnel IPsec è abilitata la protezione anti-replay, il traffico IPsec in ingresso viene elaborato come segue:

- Se il numero di sequenza rientra nella finestra e non è stato ricevuto in precedenza, l'integrità del pacchetto viene verificata. Se il pacchetto supera il controllo di integrità, viene accettato e il router contrassegna che è stato ricevuto questo numero di sequenza. Ad esempio, un pacchetto con numero di sequenza 162 Encapsulating Security Payload (ESP).
- Se il numero di sequenza rientra nella finestra ma è stato ricevuto in precedenza, il pacchetto viene scartato. Il pacchetto duplicato viene scartato e la perdita viene registrata nel contatore di riproduzione.

- Se il numero di sequenza è maggiore del numero di sequenza più alto nella finestra, l'integrità del pacchetto viene verificata. Se il pacchetto supera il controllo di integrità, la finestra scorrevole viene spostata verso destra. Ad esempio, se si riceve un pacchetto valido con numero di sequenza 189, il nuovo bordo destro della finestra viene impostato su 189 e il bordo sinistro su 125 (189 - 64 [dimensioni finestra]).

- Se il numero di sequenza è inferiore al bordo sinistro, il pacchetto viene scartato e registrato nel contatore di riproduzione. Si tratta di un pacchetto non ordinato.

Nei casi in cui si verifica un errore nel controllo della riproduzione e il pacchetto viene scartato, il router genera un messaggio Syslog simile al seguente:

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

Nota: il rilevamento della riproduzione si basa sul presupposto che l'associazione di sicurezza (SA, Security Association) IPSec esista solo tra due peer. GETVPN (Group Encrypted Transport VPN) utilizza una singola associazione di sicurezza IPsec tra più peer. Di conseguenza, GETVPN utilizza un meccanismo di controllo anti-replay completamente diverso chiamato Time Based Anti-Replay Failure. Questo documento copre solo la funzione anti-replay basata su contatori per i tunnel IPsec point-to-point.

Nota: la protezione anti-replay è un servizio di sicurezza importante offerto dal protocollo IPsec. La funzionalità anti-replay di IPsec disabilitata ha implicazioni sulla sicurezza e deve essere eseguita con discrezione.

Problemi che possono causare interruzioni di riproduzione IPSec

Come descritto in precedenza, lo scopo dei controlli di ripetizione è quello di proteggere il sistema da ripetizioni involontarie dei pacchetti. In alcuni casi, tuttavia, un errore nel controllo della ripetizione potrebbe non essere dovuto a un motivo dannoso:

- L'errore potrebbe essere causato da un pacchetto sufficiente che viene riordinato nel percorso di rete tra gli endpoint del tunnel. Ciò può verificarsi se tra i peer sono presenti più percorsi di rete.
- L'errore potrebbe essere causato da percorsi di elaborazione dei pacchetti non uguali all'interno di Cisco IOS. Ad esempio, i pacchetti IPsec frammentati che richiedono il riassemblaggio dell'IP prima della decrittografia potrebbero subire un ritardo tale da fuoriuscire dalla finestra di riproduzione al momento dell'elaborazione.
- L'errore potrebbe essere causato da QoS (Quality of Service) abilitato sull'endpoint IPSec di invio o nel percorso di rete. Con l'implementazione di Cisco IOS, la crittografia IPsec viene eseguita prima della modalità QoS nella direzione di uscita. Alcune funzionalità QoS, ad esempio LLQ (Low Latency Queueing), potrebbero causare un problema di consegna del pacchetto IPsec e essere ignorate dall'endpoint ricevente a causa di un errore del controllo di ripetizione.
- Un problema operativo o di configurazione di rete può duplicare i pacchetti durante il transito sulla rete.
- Un utente malintenzionato (man-in-the-middle) potrebbe potenzialmente ritardare, eliminare e duplicare il traffico ESP.

Risoluzione dei problemi relativi alle interruzioni di riproduzione IPSec

Per risolvere i problemi di perdita dei pacchetti di ripetizione IPsec, è necessario identificare i pacchetti ignorati a causa della ripetizione e usare le acquisizioni dei pacchetti per stabilire se si tratta di pacchetti riprodotti o di pacchetti arrivati sul router ricevente al di fuori della finestra di ripetizione. Per far corrispondere correttamente i pacchetti ignorati a quello acquisito nella traccia dello sniffer, il primo passaggio consiste nell'identificare il peer e il flusso IPsec a cui appartengono i pacchetti ignorati e il numero di sequenza ESP del pacchetto.

Usa funzionalità di traccia pacchetti datapath Cisco IOS XE

Sulle piattaforme router che eseguono Cisco IOS® XE, le informazioni sul peer e l'indice dei parametri di sicurezza IPsec (SPI) vengono stampate nel messaggio Syslog quando si verifica

una perdita, al fine di facilitare la risoluzione dei problemi anti-replay. Tuttavia, un'informazione fondamentale che ancora manca è il numero di sequenza ESP. Il numero di sequenza ESP viene usato per identificare in modo univoco un pacchetto IPsec all'interno di un determinato flusso IPsec. Senza il numero di sequenza, diventa difficile identificare esattamente quale pacchetto viene scartato durante l'acquisizione.

La funzione packet-trace del percorso dei dati Cisco IOS XE può essere utilizzata in questa situazione quando viene osservata la perdita della riproduzione, con questo messaggio 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
```

Per identificare facilmente il numero di sequenza ESP del pacchetto scartato, attenersi alla seguente procedura con la funzione di traccia dei pacchetti:

1. Configurare il filtro di debug condizionale della piattaforma in modo che corrisponda al traffico proveniente dal dispositivo peer:

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

1. Abilitare la traccia dei pacchetti con l'opzione copy per copiare le informazioni dell'intestazione del pacchetto:

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

1. Quando vengono rilevati errori di ripetizione, utilizzare il buffer di traccia del pacchetto per identificare il pacchetto scartato a causa della ripetizione e il numero di sequenza ESP può essere trovato nel pacchetto copiato:

<#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
```

L'output precedente mostra che i numeri di pacchetto 6 e 7 vengono scartati, quindi possono essere esaminati in dettaglio ora:

<#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
```

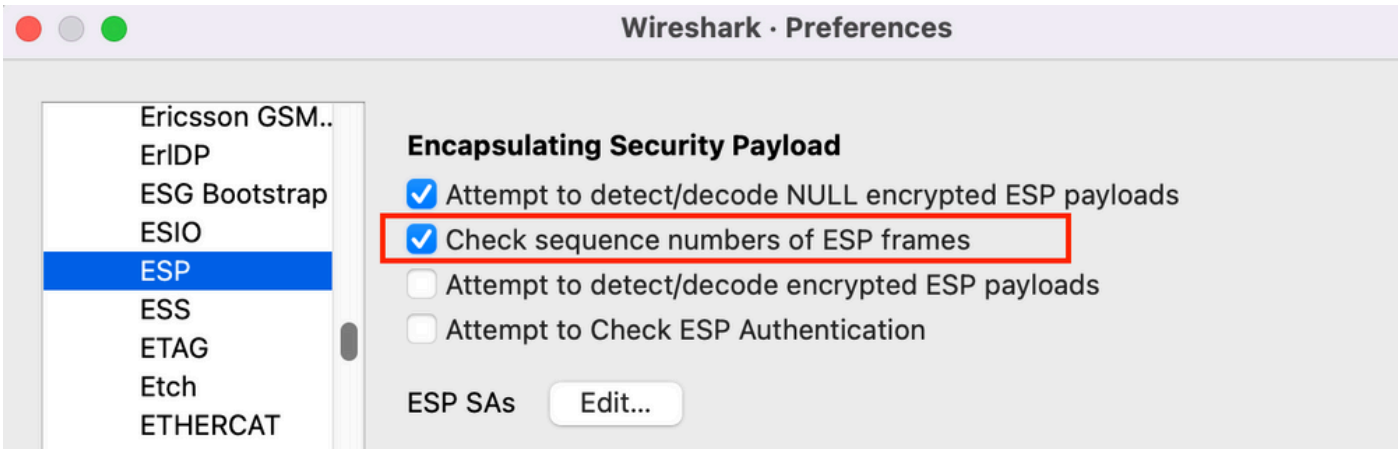
Il numero di sequenza ESP ha una posizione relativa di 24 byte che inizia dall'intestazione IP (o 4 byte dei dati di payload del pacchetto IP), come evidenziato in grassetto nell'output precedente. In questo particolare esempio, il numero di sequenza ESP per il pacchetto scartato è 0x6.

Raccogli acquisizioni pacchetti

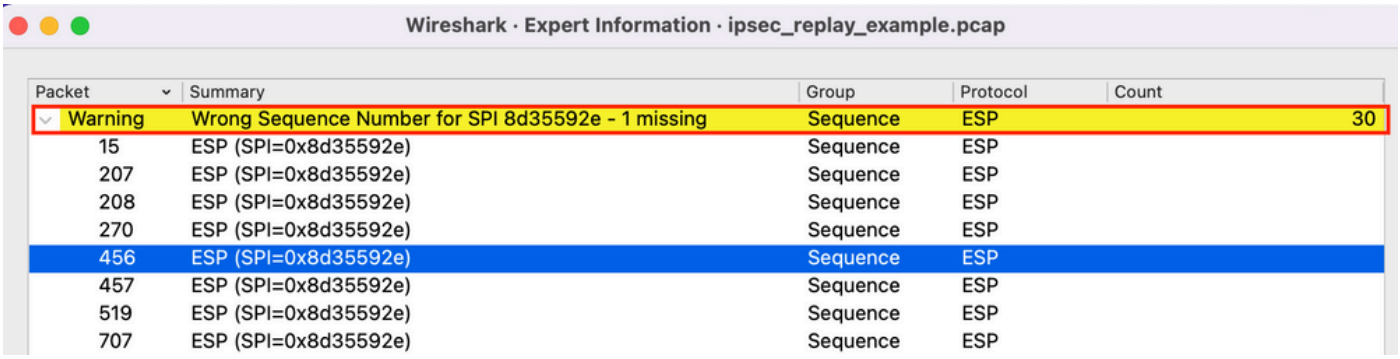
Oltre all'identificazione delle informazioni del pacchetto scartato a causa di un errore del replay check, è necessario raccogliere contemporaneamente un pacchetto di acquisizione per il flusso IPsec in questione. Ciò aiuta nell'esame del modello di numero di sequenza ESP all'interno dello stesso flusso IPSec a determinare la causa della perdita di ripetizione. Per i dettagli su come utilizzare Embedded Packet Capture (EPC) sui router Cisco IOS XE, vedere Esempio di configurazione di Embedded Packet Capture per Cisco IOS e Cisco IOS XE.

Utilizzo dell'analisi dei numeri di sequenza di Wireshark

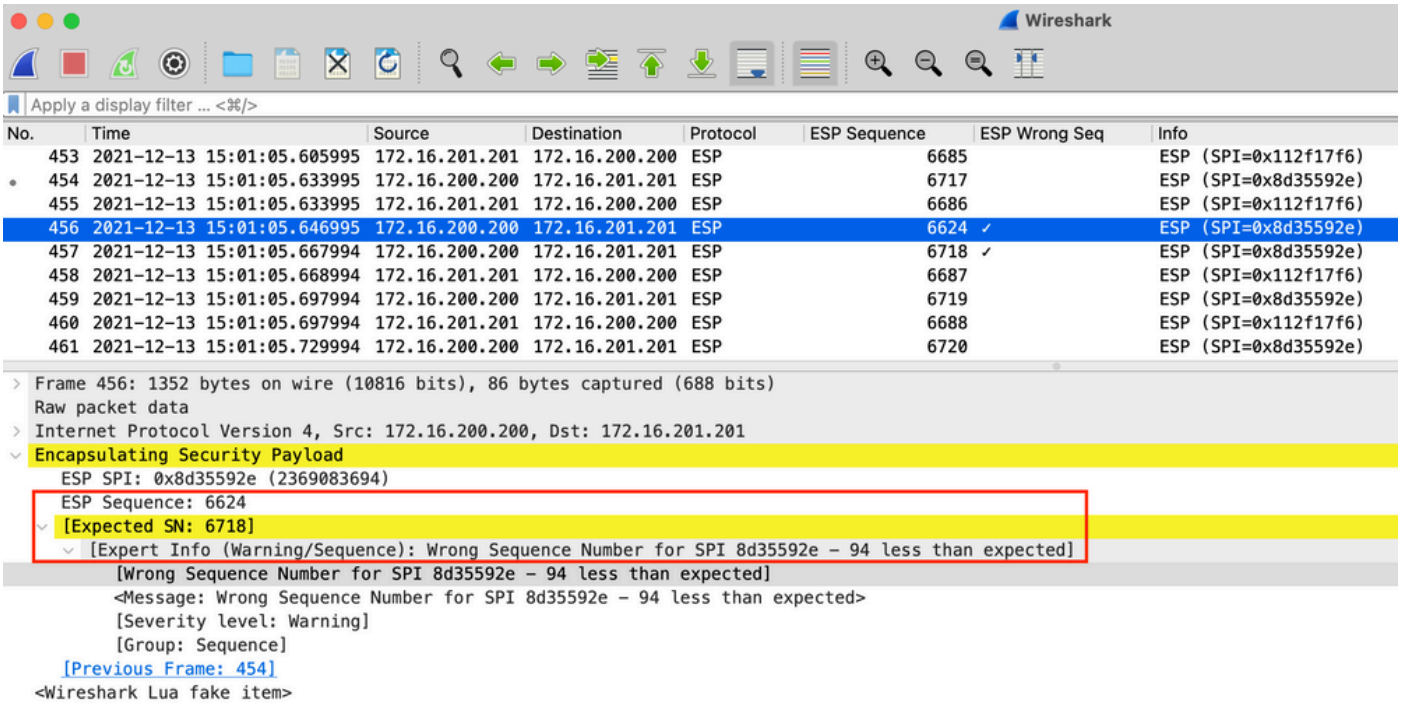
Una volta raccolta l'acquisizione dei pacchetti crittografati (ESP) sull'interfaccia WAN, Wireshark può essere usato per eseguire l'analisi del numero di sequenza ESP e rilevare eventuali anomalie. Per prima cosa, accertarsi che il controllo del numero di sequenza sia abilitato in Preferenze > Protocolli > ESP, come mostrato nell'immagine:



Controllare quindi eventuali problemi di numeri di sequenza ESP in Analisi > Informazioni esperto come indicato di seguito:



Fare clic su uno dei pacchetti con il numero di sequenza errato per ottenere ulteriori dettagli, come indicato di seguito:



Soluzione

Dopo l'identificazione del peer e la raccolta dell'acquisizione dei pacchetti per le perdite di replay, tre possibili scenari possono spiegare gli errori di replay:

1. È un pacchetto valido che è stato ritardato:
   Le acquisizioni dei pacchetti permettono di verificare se il pacchetto è effettivamente valido e se il problema è insignificante (a causa di problemi di latenza della rete o del percorso di trasmissione) o richiede una risoluzione più approfondita dei problemi. Ad esempio, l'acquisizione mostra un pacchetto con un numero di sequenza di X che arriva fuori ordine e le dimensioni della finestra di riproduzione sono attualmente impostate su 64. Se un pacchetto valido con numero di sequenza (X + 64) arriva prima del pacchetto X, la finestra viene spostata a destra e il pacchetto X viene scartato a causa di un errore di riproduzione.

   In questi scenari, è possibile aumentare le dimensioni della finestra di ripetizione o disabilitare il controllo della ripetizione per assicurarsi che tali ritardi vengano considerati

accettabili e che i pacchetti legittimi non vengano scartati. Per impostazione predefinita, le dimensioni della finestra di riproduzione sono piuttosto ridotte (dimensione finestra 64). Se si aumentano le dimensioni, il rischio di attacco non aumenta in modo significativo. Per informazioni su come configurare una finestra Anti-Replay di IPSec, consultare il documento How to Configure IPsec Anti-Replay Window: Expanding and Disabling (Come configurare la finestra Anti-Replay di IPSec: espansione e disattivazione).

Suggerimento: se la finestra di riproduzione viene disabilitata o modificata nel profilo IPSec utilizzato su un'interfaccia VTI (Virtual Tunnel Interface), le modifiche non avranno effetto finché il profilo di protezione non verrà rimosso e riapplicato o l'interfaccia del tunnel non verrà reimpostata. Questo è il comportamento previsto perché i profili IPsec sono un modello utilizzato per creare una mappa dei profili del tunnel quando viene visualizzata l'interfaccia del tunnel. Se l'interfaccia è già attiva, le modifiche al profilo non influiscono sul tunnel finché l'interfaccia non viene reimpostata.

Nota: i primi modelli di Aggregation Services Router (ASR) 1000 (come ASR1000 con ESP5, ESP10, ESP20 ed ESP40, insieme ad ASR1001) non supportavano una finestra di 1024 anche se la CLI consentiva tale configurazione. Di conseguenza, le dimensioni della finestra indicate nell'output del comando show crypto ipsec sa potrebbero non essere corrette. Usare il comando show crypto ipsec sa peer ip-address platform per verificare le dimensioni della finestra hardware anti-replay. La dimensione predefinita della finestra è di 64 pacchetti su tutte le piattaforme. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCso45946. Le piattaforme di routing Cisco IOS XE più recenti (ad esempio ASR1K con ESP100 ed ESP200, ASR1001-X e ASR1002-X, i router ISR (Integrated Service Router) serie 4000 e i router Catalyst serie 8000) supportano una finestra di 1024 pacchetti nelle versioni 15.2(2)S e successive.

---

2. È dovuta alla configurazione QoS sull'endpoint di invio:
   Questa situazione richiede un esame attento e il tuning di alcune funzionalità QoS per attenuare la condizione. Per una descrizione più dettagliata di questo argomento e di una soluzione potenziale, fare riferimento all'articolo Considerazioni sull'anti-replay in un articolo sulla VPN IPSec (V3PN) abilitata per voce e video.

3. È un pacchetto duplicato ricevuto in precedenza:
   In questo caso, è possibile osservare due o più pacchetti con lo stesso numero di sequenza ESP nello stesso flusso IPsec durante l'acquisizione del pacchetto. In questo caso, si prevede la perdita di pacchetti perché la protezione IPsec replay funziona in modo da prevenire attacchi di tipo replay nella rete e il syslog è puramente informativo. Se questa condizione persiste, è necessario indagare su di essa come una potenziale minaccia per la sicurezza.

Nota: gli errori dei controlli di ripetizione vengono visualizzati solo quando nel set di trasformazioni IPSec è abilitato un algoritmo di autenticazione. Un altro modo per eliminare questo messaggio di errore è disabilitare l'autenticazione ed eseguire solo la crittografia; tuttavia, ciò è fortemente sconsigliato a causa delle implicazioni di sicurezza dell'autenticazione disabilitata.

Ulteriori informazioni

Risoluzione dei problemi di riproduzione sui router legacy con Cisco IOS Classic

I replay IPsec scarti sui router ISR serie G2 legacy che usano Cisco IOS sono diversi dai router che usano Cisco IOS XE, come mostrato di seguito:

```
<#root>

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

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

Notare che l'output del messaggio non fornisce l'indirizzo IP del peer o le informazioni SPI. Per risolvere i problemi relativi a questa piattaforma, utilizzare il comando "conn-id" nel messaggio di errore. Identificare il "conn-id" nel messaggio di errore e cercarlo nell'output del comando show crypto ipsec sa, in quanto la riproduzione è un controllo per SA (in contrapposizione a un controllo per peer). Il messaggio Syslog fornisce anche il numero di sequenza ESP, che può aiutare a identificare in modo univoco il pacchetto scartato nell'acquisizione del pacchetto.

Nota: nelle diverse versioni del codice, il "conn-id" è l'id conn o il flow_id per l'associazione di sicurezza in ingresso.

Di seguito viene illustrato quanto segue:

```
<#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>
```

Come si può vedere da questo output, il rilascio della ripetizione proviene dall'indirizzo peer 10.2.0.200 con un SPI SA ESP in entrata di 0xE7EDE943. Si può anche notare dal messaggio di log stesso che il numero di sequenza ESP per il pacchetto scartato è 13. La combinazione di indirizzo peer, numero SPI e numero di sequenza ESP può essere utilizzata per identificare in

modo univoco il pacchetto scartato nell'acquisizione del pacchetto.

Nota: il messaggio Cisco IOS Syslog ha una velocità limitata per il pacchetto del dataplane che scende a uno al minuto. Per ottenere un conteggio accurato del numero esatto di pacchetti scartati, usare il comando show crypto ipsec sa detail, come mostrato in precedenza.

Uso del software Cisco IOS XE precedente

Sui router che eseguono le versioni precedenti di Cisco IOS XE, il comando "REPLAY_ERROR" segnalato nel syslog potrebbe non stampare il flusso IPsec effettivo con le informazioni del peer in cui il pacchetto riprodotto viene scartato, come mostrato di seguito:

```
%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
```

Per identificare le informazioni corrette sul peer IPsec e sul flusso, usare l'handle del piano dati (DP) stampato nel messaggio Syslog come parametro di input SA Handle in questo comando, per recuperare le informazioni sul flusso IPsec sul QFP (Quantum Flow Processor):

<#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>
```

Per automatizzare la raccolta dei dati, è inoltre possibile utilizzare uno script EEM (Embedded Event Manager):

```
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"
```

Nell'esempio, l'output raccolto viene reindirizzato al dispositivo bootflash. Per visualizzare questo output, usare il comando more bootflash:replay-error.txt.

Informazioni correlate

- Progettazione di rete di riferimento per la soluzione IPSec VPN (V3PN) abilitata per voce e video
- Come configurare la finestra Anti-Replay di IPSec: Espansione e disattivazione.
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).