Risoluzione dei problemi di riesecuzione anti-IPSec di SD-WAN cEdge

Sommario

Introduzione

Questo documento descrive il comportamento anti-replay di IPSec in SD-WAN IPsec per router Edge e come risolvere i problemi relativi all'anti-replay.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- IPsec (Internet Protocol Security)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C800V versione 17.06.01
- ASR 1001-X versione 17.06.03a
- vManage versione 20.7.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'autenticazione IPsec fornisce una protezione anti-replay incorporata contro pacchetti IPsec vecchi o duplicati con il numero di sequenza nell'intestazione ESP selezionata sul destinatario. La perdita dei pacchetti anti-replay è uno dei problemi più comuni del piano dati con IPsec a causa di pacchetti consegnati fuori dall'ordine all'esterno della finestra anti-replay. Un approccio generale per la risoluzione dei problemi relativi alle perdite anti-replay di IPsec è disponibile in Errori di controllo anti-replay di IPsec, e la tecnica generale si applica anche a SD-WAN. Tuttavia, esistono alcune differenze di implementazione tra IPsec tradizionale e IPsec utilizzato nella soluzione Cisco SD-WAN. In questo articolo vengono illustrate queste differenze e l'approccio delle piattaforme cEdge con Cisco IOS ®XE.

Considerazioni sul rilevamento della riproduzione SD-WAN

Chiave di gruppo e chiave di parità

A differenza dell'IPsec tradizionale, in cui le SA IPsec vengono negoziate tra due peer con l'utilizzo del protocollo IKE, l'SD-WAN utilizza un concetto di chiave di gruppo. In questo modello, un dispositivo edge SD-WAN genera periodicamente un'associazione di protezione in entrata del piano dati per TLOC e invia queste associazioni di protezione al controller vSmart, che a sua volta propaga l'associazione di protezione agli altri dispositivi edge della rete SD-WAN. Per una descrizione più dettagliata delle operazioni del piano dati SD-WAN, vedere Panoramica sulla sicurezza del piano dati SD-WAN.

> **Nota**: da Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2, le chiavi pairwise IPsec sono supportate. Vedere Cenni preliminari sulle chiavi di coppia IPSec. Con le chiavi Pairwise, la protezione anti-replay di IPsec funziona esattamente come la protezione IPsec tradizionale. Questo articolo si concentra principalmente sul controllo della ripetizione con l'uso del modello di chiave di gruppo.

SPI codificato

Nell'intestazione ESP IPsec, il valore SPI (Security Parameter Index) è un valore a 32 bit utilizzato dal destinatario per identificare l'associazione di protezione (SA) con cui viene decriptato un pacchetto in entrata. Con SD-WAN, questo SPI in entrata può essere identificato con **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)
```

Nota: anche se l'SPI in entrata è lo stesso per tutti i tunnel, il ricevitore ha un'associazione di sicurezza diversa e l'oggetto della finestra di riproduzione corrispondente associato all'associazione di sicurezza per ciascun dispositivo peer edge, in quanto l'associazione di sicurezza è identificata dall'origine, dall'indirizzo IP di destinazione, dall'origine, dalle porte di destinazione a 4 tuple e dal numero SPI. Quindi essenzialmente, ogni peer ha il proprio oggetto finestra anti-replay.

Notare che il valore SPI del pacchetto inviato dal dispositivo peer è diverso dall'output precedente. Di seguito viene riportato un esempio dell'output di analisi dei pacchetti con l'opzione di copia dei pacchetti abilitata:

```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

L'indice SPI effettivo nell'intestazione ESP è **0x04000123.** Il motivo è che i primi bit dell'SPI per SD-WAN sono codificati con informazioni aggiuntive, e solo i bit inferiori del campo SPI sono allocati per l'SPI effettivo.

IPsec tradizionale:

```
 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)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Dove:

- **CTR** (primi 4 bit, bit 0-3) - Bit di controllo, utilizzato per indicare il tipo specifico di pacchetti di controllo. Ad esempio, il bit di controllo 0x8000000 viene utilizzato per BFD.
- **MSNS** (successivi 3 bit, 4-6) - Indice di spazio per numeri di sequenza multipli. Questa opzione viene usata per individuare il contatore di sequenza corretto nella matrice dei contatori di sequenza per controllare la riproduzione del pacchetto specificato. Per SD-WAN, il protocollo a 3 bit di MSNS consente di mappare 8 diverse classi di traffico nello spazio dei numeri di sequenza. Ciò implica che il valore SPI effettivo che può essere utilizzato per la selezione SA è il minore ordine a 25 bit dal valore completo a 32 bit del campo.

Spazio per numeri di sequenza multipli per QoS

Ècomune osservare errori di ripetizione IPsec in un ambiente in cui i pacchetti vengono

consegnati in modo non corretto a causa di QoS, ad esempio LLQ, poiché QoS viene sempre eseguito dopo la crittografia e l'incapsulamento IPsec. La soluzione Spazio dei numeri di sequenza risolve questo problema con l'uso di più spazi dei numeri di sequenza mappati a diverse classi di traffico QoS per una determinata associazione di sicurezza. Lo spazio del numero di sequenza diverso viene indicizzato in base ai bit MSNS codificati nel campo SPI del pacchetto ESP come illustrato. Per una descrizione più dettagliata, vedere Meccanismo anti-replay IPsec per QoS.

Come accennato in precedenza, l'implementazione del numero di sequenza multiplo implica che il valore SPI effettivo che può essere utilizzato per la selezione SA è il basso ordine ridotto di 25 bit. Un'altra considerazione pratica da tenere in considerazione quando le dimensioni della finestra di ripetizione vengono configurate con questa implementazione è che le dimensioni della finestra di ripetizione configurate si riferiscono alla finestra di ripetizione aggregata, quindi le dimensioni effettive della finestra di ripetizione per ogni spazio dei numeri di sequenza sono pari a 1/8 dell'aggregazione.

Esempio di configurazione:

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

> **Nota**: le dimensioni effettive della finestra di ripetizione per ogni spazio dei numeri di sequenza sono 1024/8 = 128.

> **Nota**: dal Cisco IOS ®XE. 17.2.1, le dimensioni della finestra di ripetizione aggregata sono state aumentate a 8192 in modo che ogni spazio del numero di sequenza possa avere una finestra di ripetizione massima di 8192/8 = 1024 pacchetti.

Su un dispositivo cEdge, l'ultimo numero di sequenza ricevuto per ciascuno spazio dei numeri di sequenza può essere ottenuto dall'output **show crypto ipsec sa peer x.x.x.x piattaforma** IPsec dataplane:

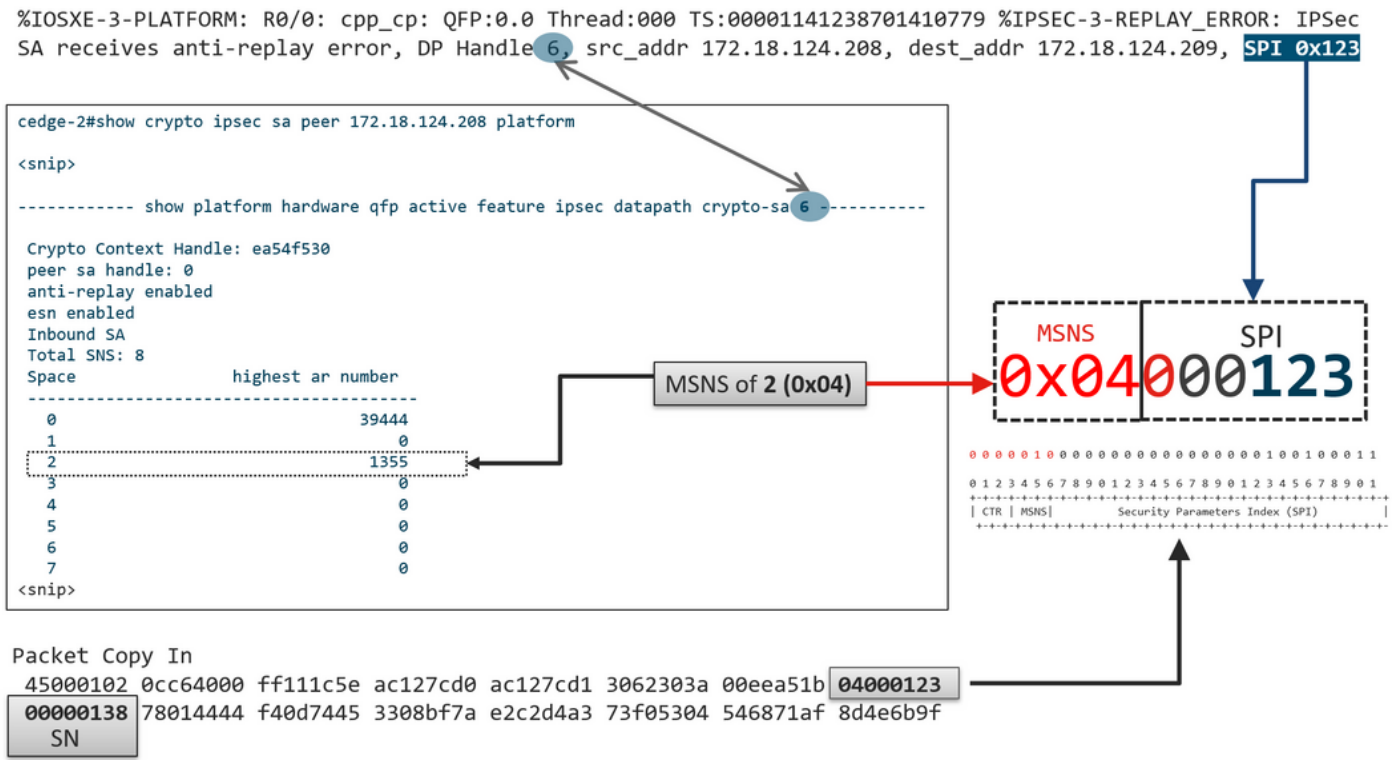
```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<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>
```

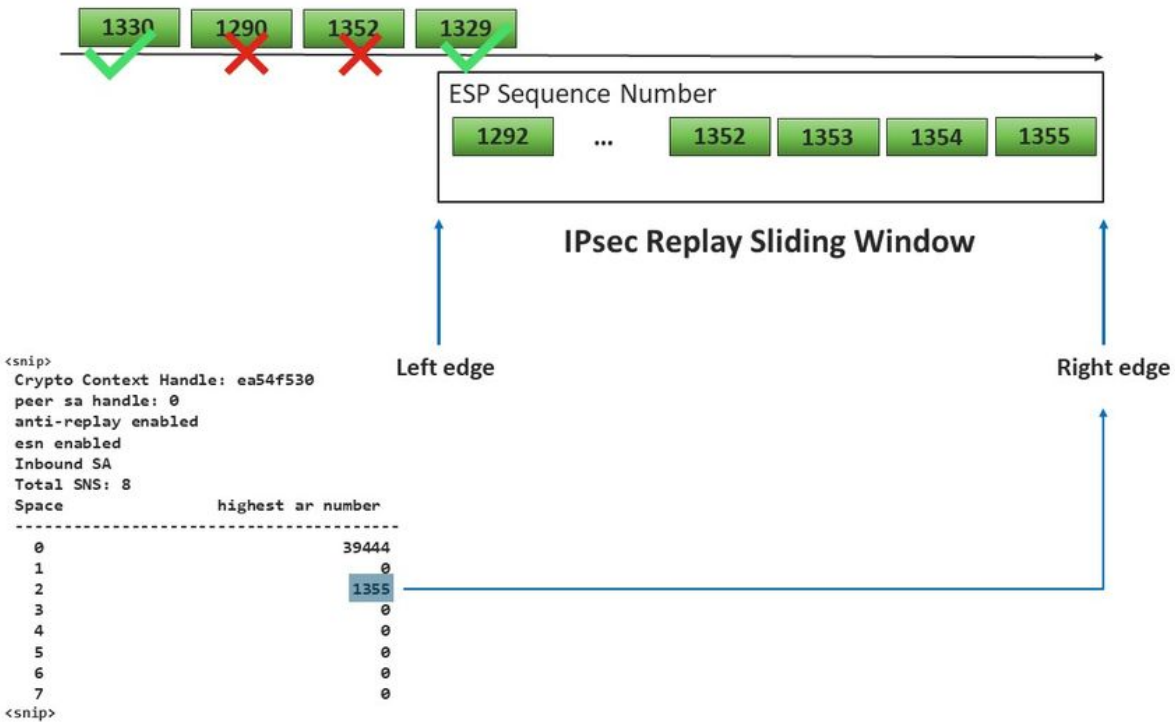
Nell'esempio, la finestra anti-replay più alta (il bordo destro della finestra scorrevole anti-replay) per MSNS di 0 **(0x00)** è **39444**, e per MSNS di **2 (0x04)** è **1335**, e questi contatori vengono usati per controllare se il numero di sequenza è all'interno della finestra di replay per i pacchetti nello stesso spazio di numeri di sequenza.

> **Nota**: esistono differenze di implementazione tra la piattaforma ASR1k e le altre piattaforme di routing Cisco IOS ®XE (ISR4k, ISR1k, CSR1kv). Di conseguenza, vi sono alcune discrepanze nei termini dei comandi show e del loro output per queste piattaforme.

Èpossibile raggruppare gli errori Anti-Replay e gli output show per trovare l'SPI e l'indice del numero di sequenza, come mostrato nell'immagine.



Con le informazioni precedenti ottenuto il bordo destro (finestra superiore) e la finestra scorrevole appare come mostrato nell'immagine.



Comandi per rendere effettiva la finestra di ripetizione configurata

A differenza del normale IPsec (non SD-WAN), il comando rekey non ha effetto sulla finestra anti-replay.

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

Questi comandi attivano la finestra di ripetizione configurata per rendere effettiva:

> **Avvertenza**: accertarsi di aver compreso l'impatto potenziale di qualsiasi comando, poiché influisce sulle connessioni di controllo e sul piano dati.

```
clear sdwan control connection
```

o

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

o

```
Interface Tunnelx
shutdown/ no shutdown
```

Risoluzione dei problemi relativi agli errori di replay drop

Risoluzione dei problemi relativi alla raccolta dei dati

In caso di caduta della funzione anti-replay di IPSec, è importante comprendere le condizioni e i potenziali trigger del problema. Raccogliere almeno l'insieme di informazioni per fornire il contesto:

- Informazioni sul dispositivo sia per il mittente che per il destinatario in caso di perdita del pacchetto di riproduzione. Include tipo di dispositivo, confronto tra cEdge e vEdge, versione del software e configurazione.
- Cronologia dei problemi. Da quanto tempo è in atto l'installazione? Quando è iniziato il problema? Qualsiasi modifica recente apportata alla rete o alle condizioni del traffico.
- Qualunque schema alla ripetizione cala, per esempio., è sporadico o costante? Ora del problema e/o evento significativo, ad esempio, si verifica solo durante le ore di produzione di picco del traffico elevato, o solo durante la reimpostazione delle chiavi e così via?

Con le informazioni raccolte in precedenza, procedere con il flusso di lavoro di risoluzione dei problemi.

Risoluzione dei problemi del flusso di lavoro

L'approccio generale per la risoluzione dei problemi di ripetizione IPsec è simile a quello utilizzato per gli IPsec tradizionali, tenendo conto dello spazio di sequenza SA per peer e dello spazio dei numeri di sequenza multipli, come spiegato. Quindi procedere come segue:

Passaggio 1. Identificare innanzitutto il peer per la perdita di replay dal syslog e la velocità di rilascio. Per le statistiche di rilascio, raccogliete sempre più istantanee con timestamp dell'output in modo che la frequenza di rilascio possa essere quantificata:

```
*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
```

> **Nota**: non è raro notare occasionali perdite di replay dovute al riordino della consegna dei pacchetti nella rete, ma le perdite di replay persistenti influiscono sul servizio e possono essere analizzate.

Passaggio 2a. Per una velocità di traffico relativamente bassa, prendere una traccia del pacchetto con la condizione impostata come indirizzo ipv4 del peer con l'opzione **copy packet** ed esaminare i numeri di sequenza per il pacchetto scartato sul bordo destro della finestra di ripetizione corrente e i numeri di sequenza nei pacchetti adiacenti per verificare se sono effettivamente duplicati o al di fuori della finestra di ripetizione.

Passaggio 2b. Per una velocità di traffico elevata senza trigger prevedibili, configurare un'acquisizione EPC con buffer circolare ed EEM per interrompere l'acquisizione quando vengono

rilevati errori di riproduzione. Poiché EEM non è attualmente supportato su vManage a partire dalla versione 19.3, ciò implica che cEdge dovrebbe essere in modalità CLI quando viene eseguita questa attività di risoluzione dei problemi.

Passaggio 3. Raccogliere la piattaforma **show crypto ipsec sa peer x.x.x.x** sul ricevitore idealmente nello stesso momento in cui viene raccolta l'acquisizione o la traccia dei pacchetti. Questo comando include le informazioni della finestra di riproduzione del piano dati in tempo reale per l'associazione di sicurezza in entrata e in uscita.

Passaggio 4. Se il pacchetto non viene consegnato correttamente, è possibile effettuare delle clip simultanee sia dal mittente che dal destinatario per verificare se il problema è causato dalla sorgente o dal livello di consegna della rete sottostante.

Passaggio 5. Se i pacchetti vengono scartati, anche se non sono duplicati né esterni alla finestra di riproduzione, in genere ciò indica un problema software sul ricevitore.

Esempio di risoluzione dei problemi per ASR1001-x

Descrizione del problema:

HW: ASR1001-X
SW: 17.06.03a

Più errori Anti-replay ricevuti per la sessione peer 10.62.33.91, quindi la sessione BFD continua a fluttuare e il traffico tra questi due siti è influenzato.

```
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
```

Passaggio 1. Verificare che la finestra Anti Replay configurata sia 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"
```

Nota: in questo esempio, le dimensioni effettive della finestra di ripetizione per ogni spazio

dei numeri di sequenza devono essere 8192/8= 1024.

Passaggio 2. Verificare le dimensioni effettive della finestra di riproduzione per il peer 10.62.33.91 per confrontare e confermare il valore configurato.

```
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
```

OSPF (Open Shortest Path First) **Dimensione finestra: 64** visualizzato nell'output non corrisponde alla finestra di riproduzione configurata **8192 (8192/8=1024)**, il che significa che anche se è stato configurato il comando non ha avuto effetto.

> **Nota**: la finestra di riproduzione effettiva viene visualizzata solo sulle piattaforme ASR. Per verificare che le dimensioni effettive della finestra di anti-replay siano uguali a quelle configurate, applicare uno dei comandi della sezione per rendere effettiva la finestra di anti-replay configurata.

Passaggio 3. Configurare e abilitare contemporaneamente l'acquisizione di analisi e monitoraggio dei pacchetti (facoltativo) per il traffico in entrata dall'origine della sessione: 10.62.33.91, destinazione: 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
```

Passaggio 4. Raccogli riepilogo traccia pacchetti:

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

Passaggio 5. Espandere alcuni pacchetti ignorati (IpsecInput) acquisiti.

(IpsecInput) Perdite di pacchetti:

```
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 utilizza ESP incapsulato UDP:

- l'intestazione UDP è 304f303b 00770000,
- Il successivo è SPI (**04000106**)
- Pertanto **00b6e00d** è il numero di sicurezza (SN).
- L'indice MSNS è **2** (**x04**00106) a causa di SPI a 32 bit (**0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1).

Passaggio 6. Verifica l'indice 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: 0x00000000010dc0
index: 1, win_top: 0000000000000000
  index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

La finestra anti-replay più alta (il bordo destro della finestra scorrevole anti-replay) per MSNS di 2 (0x04) è **0b65f00.**

Passaggio 7. Espandere alcuni pacchetti inoltrati (FWD) acquisiti.

Pacchetti inoltrati:

```
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
```

Pacchetto: 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
```

Passaggio 8. Raccogliere e ottenere le informazioni sul numero di sequenza da più pacchetti inoltrati (FWD) prima, dopo e dopo le cadute.

```
FWD:
839 PKT: 00b6e003 FWD
838 PKT: 00b6e001 FWD
837 PKT: 00b6e000 FWD
815 PKT: 00b6e044 FWD
814 PKT: 00b6dfe8 FWD
813 PKT: 00b6e00d FWD

DROP:
816 PKT: 00b6dfed DROP
817 PKT: 00b6dfec DROP
818 PKT: 00b6dfeb DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

Passaggio 9. Convertire in Decimale il numero di serie e riordinarli in calcolo semplice:

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

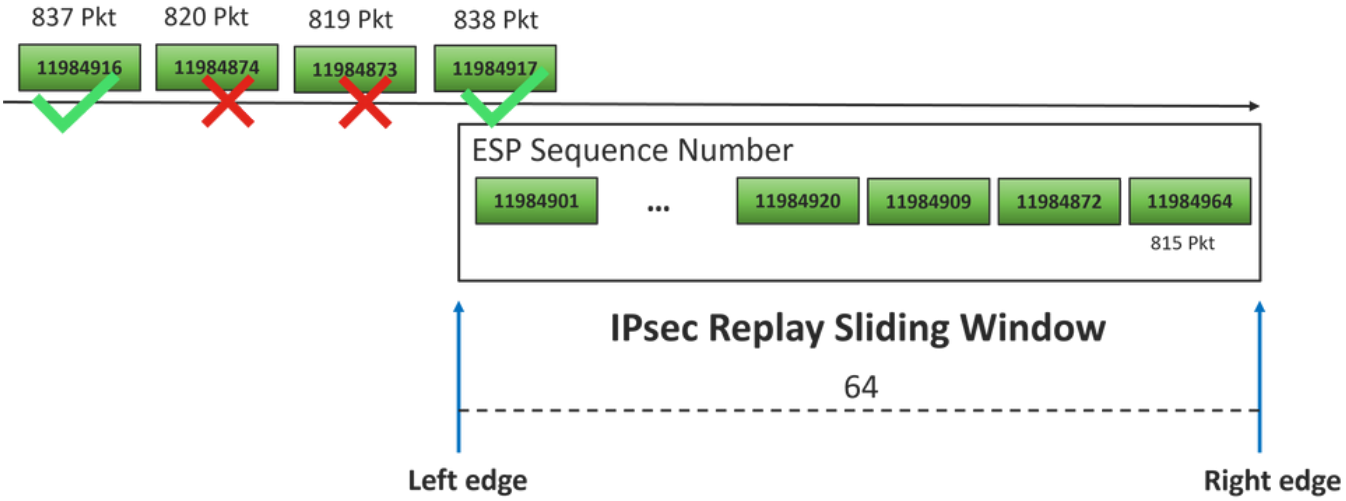
> Nota: se il numero di sequenza è maggiore del numero di sequenza più alto nella finestra, l'integrità del pacchetto viene verificata. Se il pacchetto supera il controllo di integrità, la finestra scorrevole viene spostata verso destra.

Passaggio 10. Convertire in Decimale il numero di serie e riordinarli in calcolo semplice:

```
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
```

Per questo esempio, è possibile visualizzare la finestra scorrevole con la **dimensione della finestra 64** e il **bordo destro11984964** come mostrato nell'immagine.



Il numero di sequenza ricevuto per i pacchetti drop è molto più avanti del bordo destro della finestra di ripetizione per quello spazio di sequenza.

Soluzione

Poiché le dimensioni della finestra sono ancora nel valore precedente 64, come illustrato nel passaggio 2, è necessario applicare uno dei comandi della sezione Comandi per rendere effettiva la finestra di ripetizione configurata affinché le dimensioni della finestra 1024 abbiano effetto.

Strumento aggiuntivo di acquisizione Wireshark

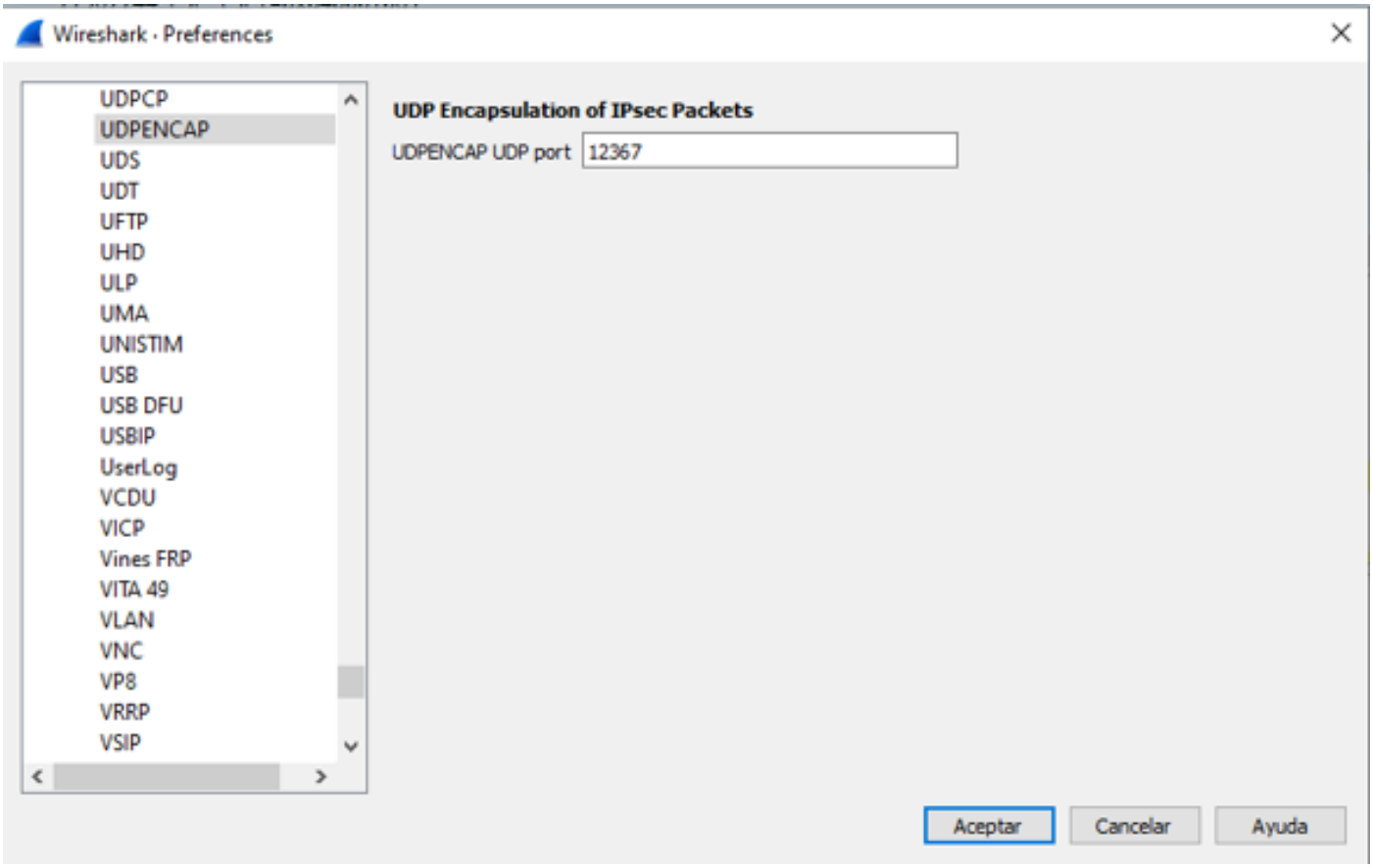
Un altro strumento utile per correlare l'ESP SPI e il numero di sequenza è il software Wireshark.

> **Nota**: è importante raccogliere l'acquisizione del pacchetto quando si verifica il problema e se è possibile raccogliere contemporaneamente la traccia fia, come descritto in precedenza

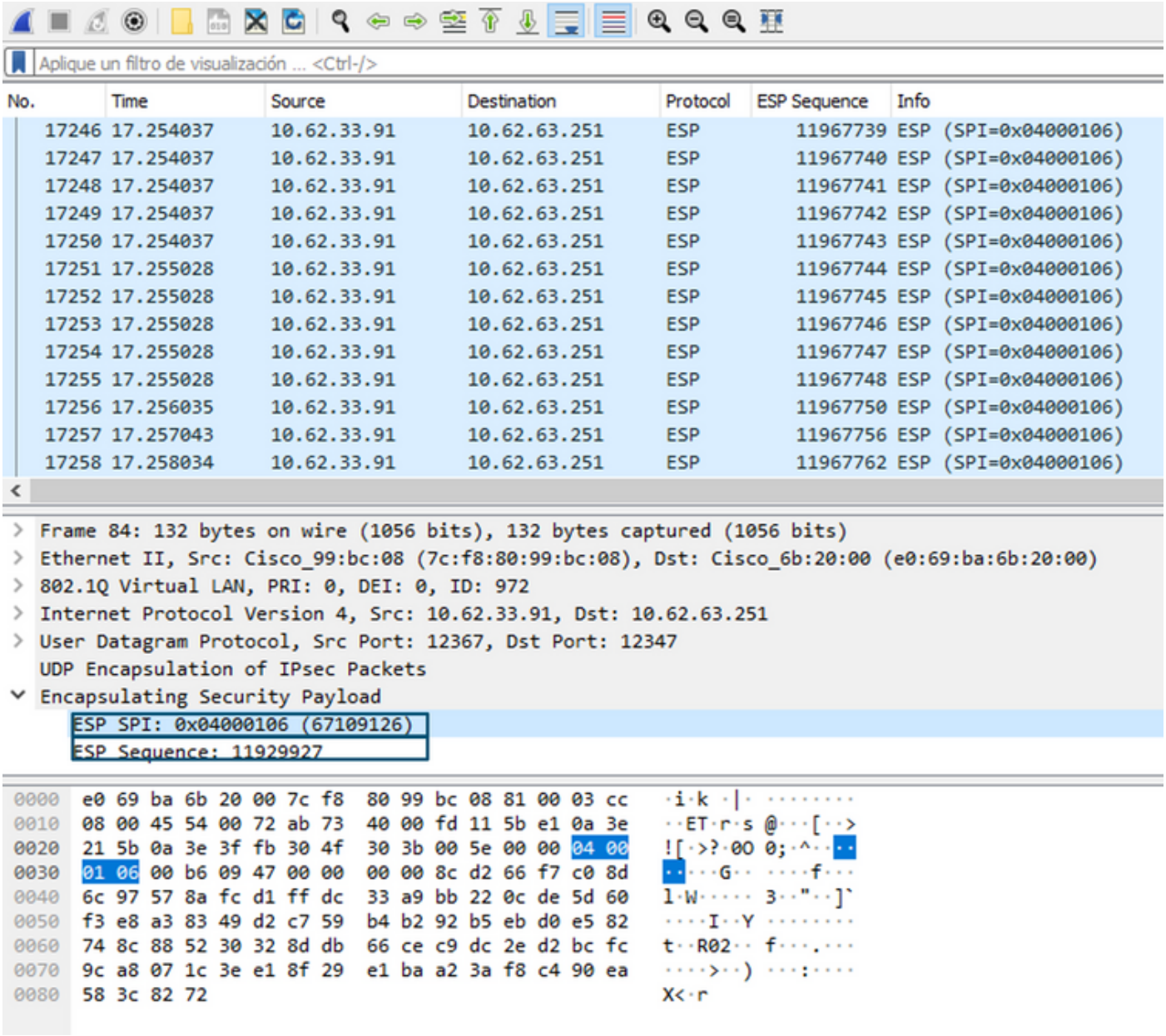
Configurare l'acquisizione dei pacchetti per la direzione in entrata ed esportarla nel file pcap.

```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Quando si apre la cattura di pcap in Wireshark, per poter vedere lo SPI ESP e il numero di sequenza, espandere un pacchetto, fare clic con il pulsante destro del mouse e selezionare **le preferenze di protocollo**, cercare **UDPENCAP** e modificare la porta predefinita in SD-WAN (porta di origine), come mostrato nella figura.



Dopo aver inserito UDPENCAP con la porta corretta, le informazioni ESP vengono visualizzate come mostrato nell'immagine.



Informazioni correlate

- [Errori di controllo anti-replay IPSec - Articolo di TechZone]
- [Espansione e disattivazione della finestra Anti-Replay di IPSec]
- [Supporto tecnico e download Cisco]

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).