IPsec Anti-Replay 검사 실패 문제 해결

목차

소개

이 문서에서는 IPsec(Internet Protocol Security) 재전송 방지 검사 실패와 관련된 문제에 대해 설명하고 가능한 해결책을 제공합니다.

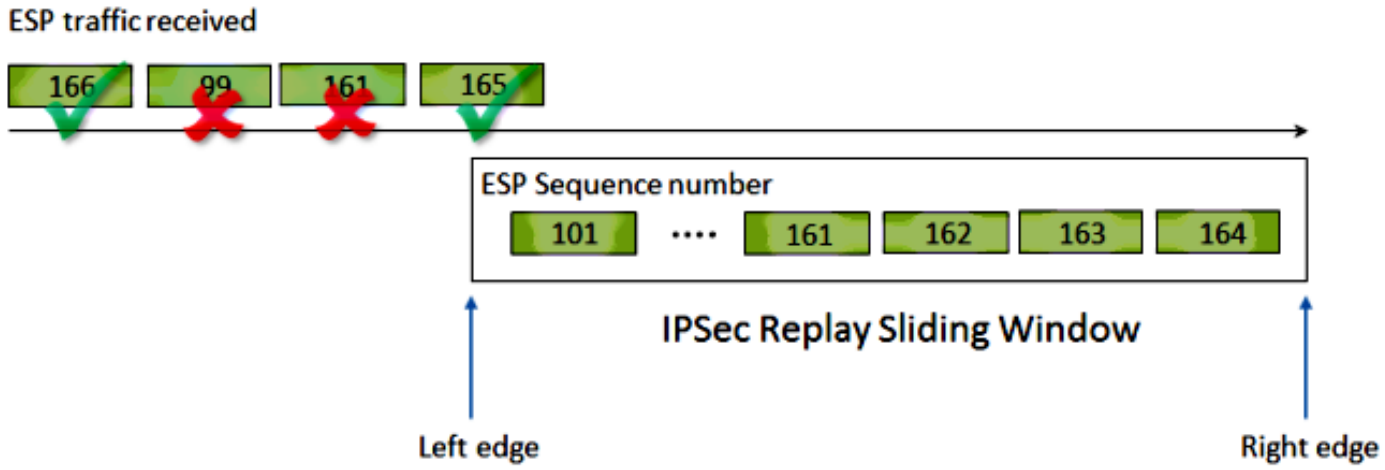
배경 정보

재생 공격 개요

리플레이 공격은 유효한 데이터 전송이 악의적 또는 부정하게 기록되고 나중에 반복되는 네트워크 공격의 한 형태입니다. 합법적인 통신을 녹음하고 이를 반복하는 사람이 올바른 사용자를 가장하여 합법적인 연결에 부정적인 영향을 주거나 방해하기 위해 보안을 파괴하려는 시도입니다.

IPsec Replay Check 보호

IPsec에서 암호화된 각 패킷에 단조롭게 증가하는 시퀀스 번호를 할당하여 공격자에 대한 재전송 방지 보호를 제공합니다. 수신 IPsec 끝점은 이러한 번호를 사용할 때 이미 처리된 패킷과 허용 가능한 시퀀스 번호의 슬라이딩 윈도우를 추적합니다. Cisco IOS® 구현의 기본 재전송 방지 창 크기는 이 이미지에 표시된 대로 64개 패킷입니다.



IPsec 터널 엔드포인트에 재전송 방지 보호가 활성화된 경우 수신 IPsec 트래픽은 다음과 같이 처리됩니다.

- 시퀀스 번호가 기간 내에 있고 이전에 수신되지 않은 경우, 패킷의 무결성이 검사됩니다. 패킷이 무결성 확인 검사를 통과하면 수락되고 라우터가 이 시퀀스 번호가 수신되었음을 표시합니다. 예를 들어, ESP(Encapsulating Security Payload) 시퀀스 번호가 162인 패킷입니다.
- 시퀀스 번호가 기간 내에 있지만 이전에 수신된 경우에는 패킷이 삭제됩니다. 이 중복 패킷은 폐기되고 삭제 내용은 재생 카운터에 기록됩니다.
- 시퀀스 번호가 창에서 가장 높은 시퀀스 번호보다 크면 패킷의 무결성이 검사됩니다. 패킷이 무결성 확인 검사를 통과하면 슬라이딩 창이 오른쪽으로 이동합니다. 예를 들어, 시퀀스 번호가 189인 유효한 패킷이 수신되면 창의 새 오른쪽 가장자리는 189로 설정되고 왼쪽 가장자리는 125(189 - 64 [window size])입니다.
- 시퀀스 번호가 왼쪽 가장자리보다 작으면 패킷이 삭제되고 재생 카운터 내에 기록됩니다. 이 패킷은 out-of-order 패킷으로 간주됩니다.

재생 확인 실패가 발생하고 패킷이 삭제되는 경우 라우터는 다음과 유사한 Syslog 메시지를 생성합니다.

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

참고: 재생 감지는 IPsec SA(Security Association)가 두 피어 사이에만 존재한다는 가정 하에 수행됩니다. GETVPN(Group Encrypted Transport VPN)은 여러 피어 간에 단일 IPsec SA를 사용합니다. 따라서 GETVPN은 Time Based Anti-Replay Failure라는 완전히 다른 재전송 방지 검사 메커니즘을 사용합니다. 이 문서에서는 포인트-투-포인트 IPsec 터널에 대한 카운터 기반 재전송 방지만 다룹니다.

참고: 재전송 방지 보호는 IPsec 프로토콜에서 제공하는 중요한 보안 서비스입니다. IPsec 재전송 방지 기능이 비활성화되어 있으면 보안상 문제가 있으므로 신중히 수행해야 합니다.

IPsec 재생 삭제를 일으킬 수 있는 문제

전술한 바와 같이, 재생 검사의 목적은 패킷의 악의적인 반복을 방지하는 것이다. 그러나 재생 검사가 실패한 경우 악의적인 이유로 인해 실패하지 않을 수 있는 몇 가지 경우가 있습니다.

  - 이 오류는 터널 엔드포인트 간의 네트워크 경로에서 순서가 재지정된 충분한 패킷에서 발생할 수 있습니다. 이는 피어 간에 여러 네트워크 경로가 있는 경우 발생할 수 있습니다.

  - 이 오류는 Cisco IOS 내부의 패킷 처리 경로가 동일하지 않기 때문에 발생할 수 있습니다. 예를 들어, 암호 해독 전에 IP 리어셈블리가 필요한 프래그먼트된 IPsec 패킷은 처리 시간까지 재생 윈도우 밖에 놓이도록 충분히 지연될 수 있습니다.
  - 전송 IPsec 엔드포인트 또는 네트워크 경로 내에서 활성화된 QoS(Quality of Service)로 인해 오류가 발생할 수 있습니다. Cisco IOS 구현에서는 IPsec 암호화가 이그레스 방향의 QoS 전에 발생합니다. LLQ(Low Latency Queueing)와 같은 특정 QoS 기능으로 인해 IPsec 패킷 전달이 순서를 벗어나고 재생 확인 실패로 인해 수신 엔드포인트에 의해 삭제될 수 있습니다.

  - 네트워크 컨피그레이션/운영 문제는 네트워크를 통과하는 패킷을 복제할 수 있습니다.

- 공격자(man-in-the-middle)는 잠재적으로 ESP 트래픽을 지연, 삭제 및 복제할 수 있습니다.

IPsec 재생 삭제 문제 해결

IPsec 재생 삭제 트러블슈팅의 핵심은 재생으로 인해 어떤 패킷이 삭제되었는지 식별하고, 패킷 캡처를 사용하여 이러한 패킷이 실제로 재생된 패킷인지 또는 재생 창 외부에 있는 수신 라우터에 도착한 패킷인지 확인하는 것입니다. 삭제된 패킷을 스니퍼 추적에서 캡처한 패킷과 정확히 일치시키기 위해 첫 번째 단계는 삭제된 패킷이 속한 피어 및 IPsec 흐름과 패킷의 ESP 시퀀스 번호를 식별하는 것입니다.

Cisco IOS XE Datapath 패킷 추적 기능 사용

Cisco IOS® XE를 실행하는 라우터 플랫폼에서는 재전송 방지 문제를 해결하기 위해 삭제 발생 시 피어 및 IPsec SPI(Security Parameter Index) 정보가 Syslog 메시지에 인쇄됩니다. 그러나 여전히 놓치는 핵심 정보 중 하나는 ESP 시퀀스 번호입니다. ESP 시퀀스 번호는 지정된 IPsec 흐름 내에서 IPsec 패킷을 고유하게 식별하는 데 사용됩니다. 시퀀스 번호가 없으면 패킷 캡처에서 어떤 패킷이 삭제되는지 정확하게 식별하기가 어려워집니다.

Cisco IOS XE 데이터 경로 패킷 추적 기능은 다음과 같은 Syslog 메시지와 함께 재생 삭제를 확인할 때 이 상황에서 사용할 수 있습니다.

```
%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
```

삭제된 패킷의 ESP 시퀀스 번호를 식별하기 위해 패킷 추적 기능을 사용하여 다음 단계를 완료합니다.

1. 피어 디바이스의 트래픽을 매칭하려면 플랫폼 조건부 디버그 필터를 설정합니다.

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

1. 패킷 헤더 정보를 복사하려면 copy 옵션을 사용하여 패킷 추적을 활성화합니다.

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

1. 재생 오류가 발견되면 패킷 추적 버퍼를 사용하여 재생으로 인해 삭제된 패킷을 식별하고 복사된 패킷에서 ESP 시퀀스 번호를 찾을 수 있습니다.

```
<#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
```

이전 출력에서는 패킷 번호 6과 7이 삭제되었으므로 이제 자세히 검토할 수 있습니다.

```
<#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
```

ESP 시퀀스 번호의 오프셋은 이전 출력에서 굵게 강조된 것처럼 IP 헤더에서 시작하는 24바이트(또는 IP 패킷의 페이로드 데이터의 4바이트)입니다. 이 특정 예에서 삭제된 패킷의 ESP 시퀀스 번호는 0x6입니다.

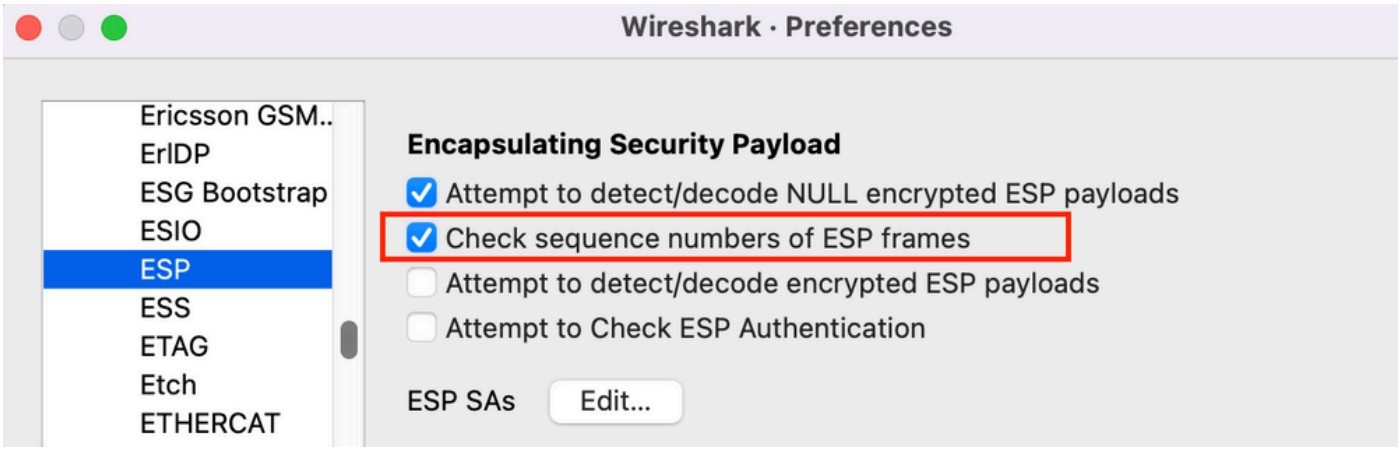
패킷 캡처 수집

재생 확인 실패로 인해 삭제된 패킷에 대한 패킷 정보를 식별하는 것 외에 문제의 IPsec 흐름에 대

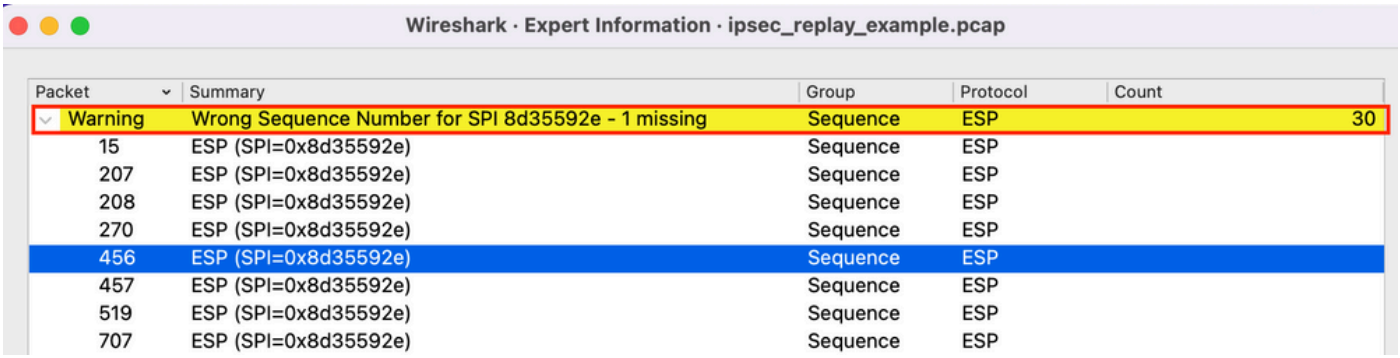
한 패킷 캡처를 동시에 수집해야 합니다. 이는 동일한 IPsec 흐름 내에서 ESP 시퀀스 번호 패턴을 검사하여 재생 삭제 이유를 확인하는 데 도움이 됩니다. Cisco IOS XE 라우터에서 EPC(Embedded Packet Capture)를 사용하는 방법에 대한 자세한 내용은 Embedded Packet Capture for Cisco IOS and Cisco IOS XE Configuration Example을 참조하십시오.

Wireshark 시퀀스 번호 분석 사용

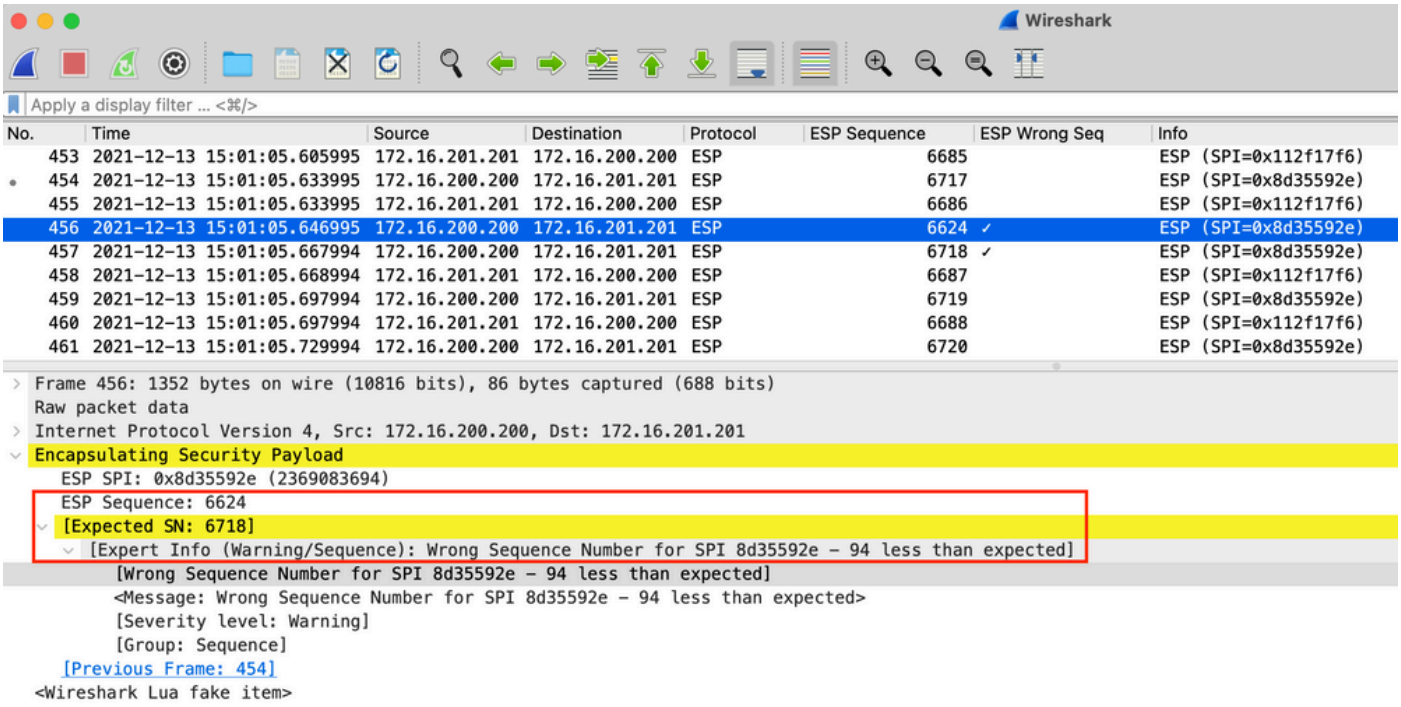
WAN 인터페이스의 암호화된(ESP) 패킷에 대한 패킷 캡처가 수집되면 Wireshark를 사용하여 임의의 시퀀스 번호 이상 징후에 대한 ESP 시퀀스 번호 분석을 수행할 수 있습니다. 먼저 이미지에 표시된 대로 Preferences(환경 설정) > Protocols(프로토콜) > ESP에서 Sequence Number Check(시퀀스 번호 확인)가 활성화되어 있는지 확인합니다.



다음으로 Analyze(분석) > Expert information(전문가 정보)에서 ESP Sequence Number(ESP 시퀀스 번호) 문제를 다음과 같이 확인합니다.



다음과 같이 추가 세부 정보를 보려면 잘못된 시퀀스 번호의 패킷을 클릭합니다.



솔루션

피어가 식별되고 재생 삭제에 대한 패킷 캡처가 수집되면 재생 실패를 설명할 수 있는 세 가지 시나리오가 있습니다.

1. 지연된 유효한 패킷입니다.
   패킷 캡처는 패킷이 실제로 유효한지, 네트워크 레이턴시 또는 전송 경로 문제로 인해 문제가 미미하거나 보다 심층적인 트러블슈팅이 필요한지 확인하는 데 도움이 됩니다. 예를 들어, 캡처는 순서 없이 도착하는 시퀀스 번호 X의 패킷을 보여주며, 재생 윈도우 크기는 현재 64로 설정되어 있습니다. 시퀀스 번호가 (X + 64)인 유효한 패킷이 패킷 X보다 먼저 도착하면 창이 오른쪽으로 이동한 다음 패킷 X가 재생 실패로 인해 삭제됩니다.

   이러한 시나리오에서는 재생 윈도우의 크기를 늘리거나 재생 검사를 비활성화하여 그러한 지연이 허용되는 것으로 간주되고 합법적인 패킷이 폐기되지 않도록 할 수 있습니다. 기본적으로 재생 윈도우 크기는 상당히 작습니다(윈도우 크기 64). 크기를 늘린다고 공격 위험이 크게 높아지는 것은 아니다. IPsec Anti-Replay Window를 구성하는 방법에 대한 자세한 내용은 IPsec Anti-Replay Window를 구성하는 방법: 문서 확장 및 비활성화를 참조하십시오.

> 팁: VTI(Virtual Tunnel Interface)에서 사용되는 IPSec 프로파일에서 재생 창이 비활성화되거나 변경되는 경우 보호 프로파일을 제거하고 다시 적용하거나 터널 인터페이스를 재설정해야 변경 사항이 적용됩니다. IPsec 프로필은 터널 인터페이스가 시작될 때 터널 프로필 맵을 만드는 데 사용되는 템플릿이므로 이는 예상된 동작입니다. 인터페이스가 이미 실행 중인 경우, 인터페이스를 재설정할 때까지 프로파일을 변경해도 터널에 영향을 주지 않습니다.

> 참고: 초기 ASR(Aggregation Services Router) 1000 모델(예: ASR1000, ESP5, ESP10,

> ESP20, ESP40 및 ASR1001)은 CLI에서 해당 컨피그레이션을 허용했지만 창 크기 1024를 지원하지 않았습니다. 따라서 show crypto ipsec sa 명령 출력에 보고된 창 크기가 올바르지 않을 수 있습니다. 하드웨어 재전송 방지 창 크기를 확인하려면 show crypto ipsec sa peer ip-address platform 명령을 사용합니다. 기본 창 크기는 모든 플랫폼에서 64패킷입니다. 자세한 내용은 Cisco 버그 ID CSCso45946을 참조하십시오. 최신 Cisco IOS XE 라우팅 플랫폼(예: ESP100 및 ESP200이 포함된 ASR1K, ASR1001-X 및 ASR1002-X, ISR(Integrated Service Router) 4000 Series 라우터, Catalyst8000 Series 라우터)은 15.2(2)S 버전 이상에서 1024 패킷의 윈도우 크기를 지원합니다.

2. 이는 전송 엔드포인트의 QoS 컨피그레이션 때문입니다.
   이러한 상황을 완화하기 위해서는 면밀한 검토와 일부 QoS를 조정해야 합니다. 이 항목과 잠재적인 솔루션에 대한 자세한 설명은 V3PN(Voice and Video Enabled IPSec VPN) 문서의 재전송 방지 고려 사항을 참조하십시오.

3. 이전에 수신한 중복 패킷입니다.
   이 경우 동일한 IPsec 흐름 내에서 동일한 ESP 시퀀스 번호를 가진 둘 이상의 패킷이 패킷 캡처에서 관찰될 수 있습니다. 이 경우 IPsec 재생 보호는 네트워크에서 재생 공격을 방지하기 위한 의도대로 작동하며 Syslog는 정보 제공에 불과하므로 패킷이 삭제될 것으로 예상됩니다. 이 상태가 지속되면 잠재적 보안 위협으로 조사해야 합니다.

> 참고: IPsec 변형 집합에서 인증 알고리즘을 사용하도록 설정한 경우에만 재생 검사 오류가 표시됩니다. 이 오류 메시지를 억제하는 또 다른 방법은 인증을 비활성화하고 암호화만 수행하는 것입니다. 그러나 비활성화된 인증의 보안 문제로 인해 이러한 방법은 권장되지 않습니다.

추가 정보

Cisco IOS Classic으로 레거시 라우터의 재생 오류 트러블슈팅

Cisco IOS를 사용하는 레거시 ISR G2 Series 라우터의 IPsec 재생 삭제는 Cisco IOS XE를 사용하는 라우터와 다릅니다.

<#root>

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

connection id=529, sequence number=13

메시지 출력은 피어 IP 주소 또는 SPI 정보를 제공하지 않습니다. 이 플랫폼에서 문제를 해결하려면 오류 메시지에 "conn-id"를 사용하십시오. 재생은 SA별 검사(피어별이 아님)이므로 오류 메시지에서 "conn-id"를 식별하고 show crypto ipsec sa 출력에서 이를 찾습니다. Syslog 메시지는 패킷 캡처에서 삭제된 패킷을 고유하게 식별하는 데 도움이 되는 ESP 시퀀스 번호도 제공합니다.

참고: 다른 버전의 코드에서 "conn-id"는 인바운드 SA의 conn id 또는 flow_id입니다.

이 그림은 다음과 같습니다.

<#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>
```

이 출력에서 알 수 있듯이, 재생 삭제는 인바운드 ESP SA SPI가 0xE7EDE943인 10.2.0.200 피어 주소에서 가져옵니다. 삭제된 패킷의 ESP 시퀀스 번호는 13이라는 것도 로그 메시지 자체에서 확인할 수 있습니다. 패킷 캡처에서 삭제된 패킷을 고유하게 식별하기 위해 피어 주소, SPI 번호 및 ESP 시퀀스 번호의 조합을 사용할 수 있습니다.

참고: Cisco IOS Syslog 메시지는 분당 1회로 드롭되는 데이터 플레인 패킷에 대해 속도가 제한됩니다. 삭제된 정확한 패킷 수의 정확한 카운트를 얻으려면 앞에서 설명한 것처럼 show crypto ipsec sa detail 명령을 사용합니다.

이전 Cisco IOS XE Software와 연동

이전 Cisco IOS XE 릴리스를 실행하는 라우터에서 Syslog에 보고된 "REPLAY_ERROR"는 재생된 패킷이 삭제되는 피어 정보와 함께 실제 IPsec 흐름을 인쇄하지 못할 수 있습니다.

```
%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
```

올바른 IPsec 피어 및 흐름 정보를 식별하려면 QFP(Quantum Flow Processor)에서 IPsec 흐름 정보를 검색하려면 Syslog 메시지에 인쇄된 DP(Data Plane) Handle을 이 명령의 입력 매개 변수 SA Handle로 사용합니다.

<#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>
```

EEM(Embedded Event Manager) 스크립트를 사용하여 데이터 수집을 자동화할 수도 있습니다.

```
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"
```

이 예에서는 수집된 출력이 부트플래시로 리디렉션됩니다. 이 출력을 보려면 more bootflash:replay-error.txt 명령을 사용합니다.

관련 정보

- 음성 및 비디오 지원 IPSec VPN(V3PN) 솔루션 참조 네트워크 설계
- IPsec Anti-Replay Window 구성 방법: 확장 및 비활성화.
- 기술 지원 및 문서 − Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.