Solucionar Falhas de Verificação de Antirrepetição de IPsec

Contents

[Introdução](#)
[Informações de Apoio](#)
[Uma visão geral dos ataques de repetição](#)
[Proteção de Verificação de Repetição IPsec](#)
[Problemas que podem causar quedas de repetição de IPsec](#)
[Solucionar Problemas de Quedas de Repetição de IPsec](#)
[Usar o recurso de rastreamento de pacote de caminho de dados do Cisco IOS XE](#)
[Coletar capturas de pacotes](#)
[Usar Análise do Número de Sequência do Wireshark](#)
[Solução](#)
[Informações adicionais](#)
[Identificar e Solucionar Problemas de Repetição em Roteadores Legados com o Cisco IOS Classic](#)
[Trabalhar com software Cisco IOS XE anterior](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve um problema relacionado a falhas de verificação antirreprodução do Internet Protocol Security (IPsec) e fornece soluções possíveis.

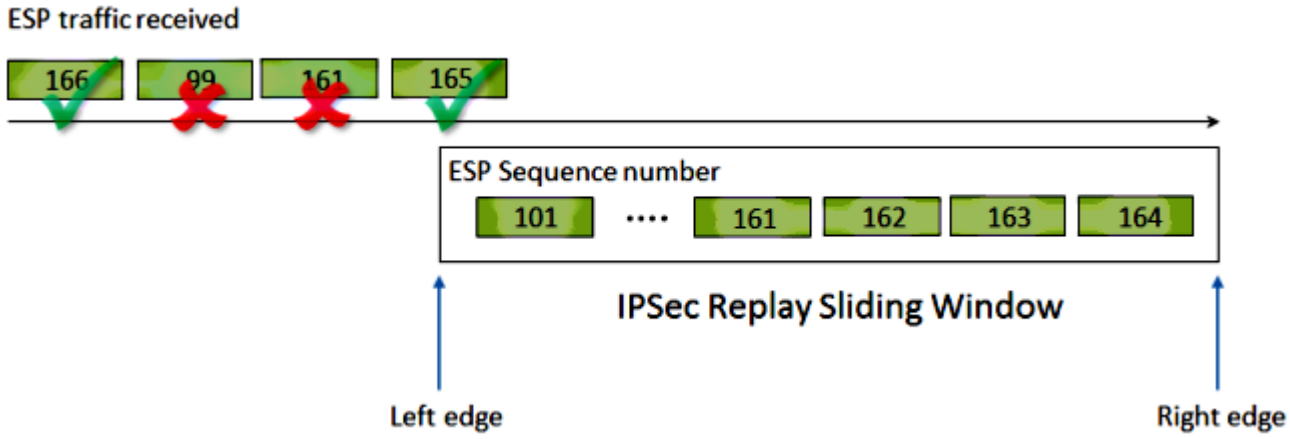
Informações de Apoio

Uma visão geral dos ataques de repetição

Um ataque de repetição é uma forma de ataque à rede em que a transmissão de dados válida é gravada de forma maliciosa ou fraudulenta e depois repetida. É uma tentativa de subverter a segurança por alguém que registra comunicações legítimas e as repete para se passar por um usuário válido e interromper ou causar um impacto negativo em conexões legítimas.

Proteção de Verificação de Repetição IPsec

Um número de sequência que aumenta de forma monótona é atribuído a cada pacote criptografado pelo IPsec para fornecer proteção antirreprodução contra um invasor. O ponto final de IPsec receptor rastreia quais pacotes já foram processados quando ele usa esses números e uma janela móvel de números de sequência aceitáveis. O tamanho padrão da janela de antireprodução na implementação do Cisco IOS® é de 64 pacotes, como mostrado nesta imagem:



Quando um ponto final de túnel IPsec tem proteção antirreprodução habilitada, o tráfego IPsec de entrada é processado da seguinte maneira:

- Se o número de sequência cair dentro da janela e não tiver sido recebido anteriormente, a integridade do pacote será verificada. Se o pacote passar na verificação de integridade, ele será aceito e o roteador marcará que esse número de sequência foi recebido. Por exemplo, um pacote com o número de sequência ESP (Encapsulating Security Payload) 162.
- Se o número de sequência cair dentro da janela, mas tiver sido recebido anteriormente, o pacote será descartado. Esse pacote duplicado é descartado e a queda é registrada no contador de repetição.

- Se o número de sequência for maior que o número de sequência mais alto na janela, a integridade do pacote será verificada. Se o pacote passar na verificação de integridade, a janela deslizante será movida para a direita. Por exemplo, se um pacote válido com um número de sequência de 189 for recebido, a nova borda direita da janela será definida como 189 e a borda esquerda será 125 (189 - 64 [tamanho da janela]).

- Se o número de sequência for menor que a borda esquerda, o pacote será descartado e registrado no contador de repetição. Este é considerado um pacote fora de ordem.

Nos casos em que ocorre uma falha de verificação de repetição e o pacote é descartado, o roteador gera uma mensagem de Syslog semelhante a esta:

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

Observação: a detecção de repetição é baseada na suposição de que a Associação de Segurança (SA) do IPsec existe entre apenas dois pares. O Group Encrypted Transport VPN (GETVPN) usa um único SA IPsec entre vários pares. Como resultado, o GETVPN utiliza um mecanismo de verificação antirrepetição totalmente diferente chamado Falha antirrepetição baseada em tempo. Este documento abrange somente antirreprodução baseada em contador para túneis IPsec ponto a ponto.

Observação: a proteção antirreprodução é um serviço de segurança importante que o protocolo IPsec oferece. O antirreplay do IPsec desabilitado tem implicações de segurança e deve ser feito com critério.

Problemas que podem causar quedas de repetição de IPsec

Conforme descrito anteriormente, a finalidade das verificações de repetição é proteger contra repetições mal-intencionadas de pacotes. No entanto, há alguns cenários em que uma verificação de repetição com falha pode não ser devido a um motivo mal-intencionado:

    - O erro pode resultar de um pacote suficiente que é reorganizado no caminho de rede entre os pontos finais do túnel. Isso provavelmente pode ocorrer se houver vários caminhos de rede entre os pares.

    - O erro pode ser causado por caminhos de processamento de pacotes desiguais dentro do Cisco IOS. Por exemplo, os pacotes IPsec fragmentados que exigem remontagem de IP antes da descriptografia podem ser atrasados o suficiente, pois ficam fora da janela de repetição no momento em que são processados.
    - O erro pode ser causado pela Qualidade de Serviço (QoS) habilitada no ponto de extremidade IPsec de envio ou no caminho da rede. Com a implementação do Cisco IOS, a criptografia IPsec ocorre antes da QoS na direção de saída. Certos recursos de QoS, como o enfileiramento de baixa latência (LLQ), podem fazer com que a entrega de pacotes IPsec fique fora de serviço e seja descartada pelo endpoint receptor devido a uma falha de verificação de repetição.

    - Um problema operacional/de configuração de rede pode duplicar pacotes enquanto transitam pela rede.

- Um invasor (man-in-the-middle) poderia atrasar, descartar e duplicar o tráfego ESP.

Solucionar Problemas de Quedas de Repetição de IPsec

A chave para solucionar problemas de quedas de repetição de IPsec é identificar quais pacotes são descartados devido à repetição e usar capturas de pacotes para determinar se esses pacotes são realmente pacotes repetidos ou pacotes que chegaram ao roteador receptor fora da janela de repetição. Para corresponder corretamente os pacotes descartados ao que é capturado no farejador de rastreamento, a primeira etapa é identificar o peer e o fluxo de IPsec ao qual os pacotes descartados pertencem e o número de sequência ESP do pacote.

Usar o recurso de rastreamento de pacote de caminho de dados do Cisco IOS XE

Em plataformas de roteador que executam o Cisco IOS® XE, as informações sobre o peer, bem como o Índice de Parâmetros de Segurança (SPI - Security Parameter Index) IPsec, são impressas na mensagem Syslog quando ocorre uma queda, para ajudar a solucionar problemas de antirreprodução. No entanto, uma informação-chave que ainda falta é o número de sequência ESP. O número de sequência ESP é usado para identificar exclusivamente um pacote IPsec em um determinado fluxo IPsec. Sem o número de sequência, torna-se difícil identificar exatamente qual pacote é descartado em uma captura de pacote.

O recurso de rastreamento de pacote de caminho de dados do Cisco IOS XE pode ser usado nesta situação quando a queda de repetição é observada, com esta mensagem de 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
```

Para ajudar a identificar o número de sequência ESP para o pacote descartado, conclua estes passos com o

recurso de rastreamento de pacote:

1. Configure o filtro de depuração condicional da plataforma para corresponder o tráfego do dispositivo par:

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

1. Habilite o rastreamento de pacote com a opção **copy** para copiar as informações de cabeçalho do pacote:

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

1. Quando erros de repetição forem detectados, use o buffer de rastreamento de pacote para identificar o pacote descartado devido à repetição, e o número de sequência ESP pode ser encontrado no pacote copiado:

<#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
```

A saída anterior mostra que os números de pacote 6 e 7 foram descartados, para que possam ser examinados em detalhes agora:

```
<#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
```

O número de sequência ESP tem um deslocamento de 24 bytes que começa a partir do cabeçalho IP (ou 4 bytes dos dados de payload do pacote IP), como enfatizado em negrito na saída anterior. Neste exemplo específico, o número de sequência ESP para o pacote descartado é 0x6.

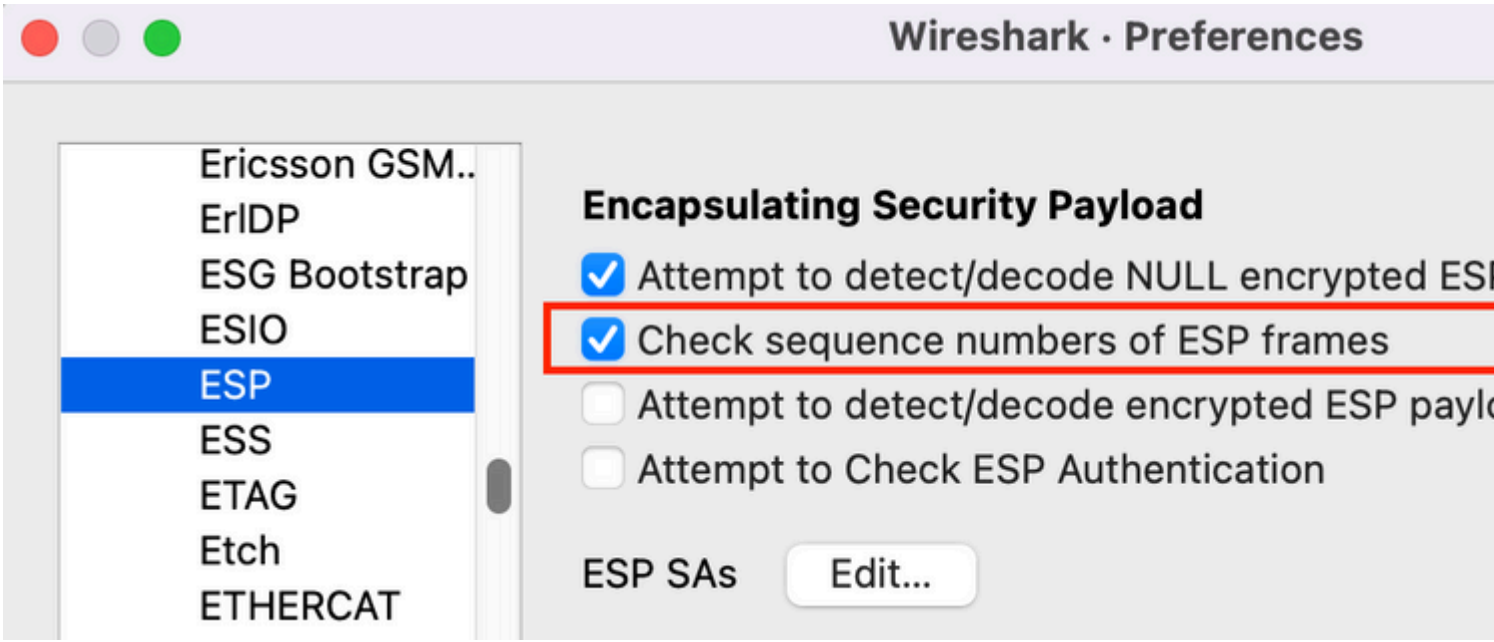
Coletar capturas de pacotes

Além da identificação das informações de pacote para o pacote descartado devido à falha de verificação de repetição, uma captura de pacote para o fluxo IPsec em questão precisa ser coletada simultaneamente. Isso

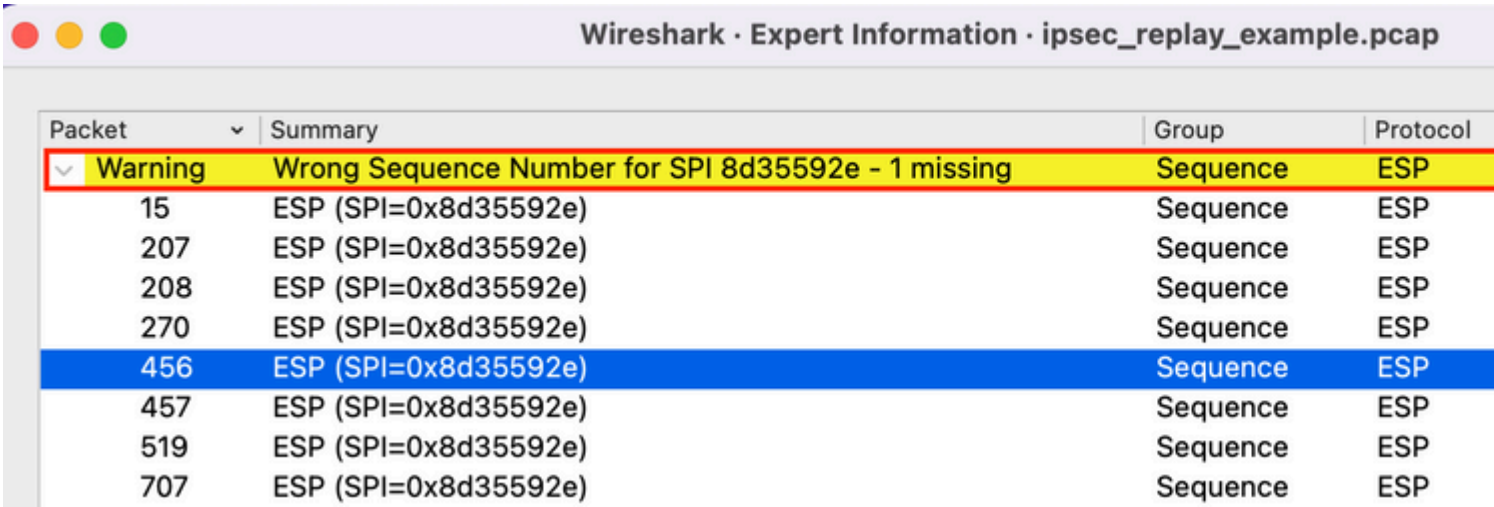
ajuda no exame do padrão de número de sequência ESP dentro do mesmo fluxo de IPsec para ajudar a determinar o motivo da queda de repetição. Para obter detalhes sobre como usar o Embedded Packet Capture (EPC) em roteadores Cisco IOS XE, consulte Exemplo de Configuração do Embedded Packet Capture para Cisco IOS e Cisco IOS XE.

Usar Análise do Número de Sequência do Wireshark

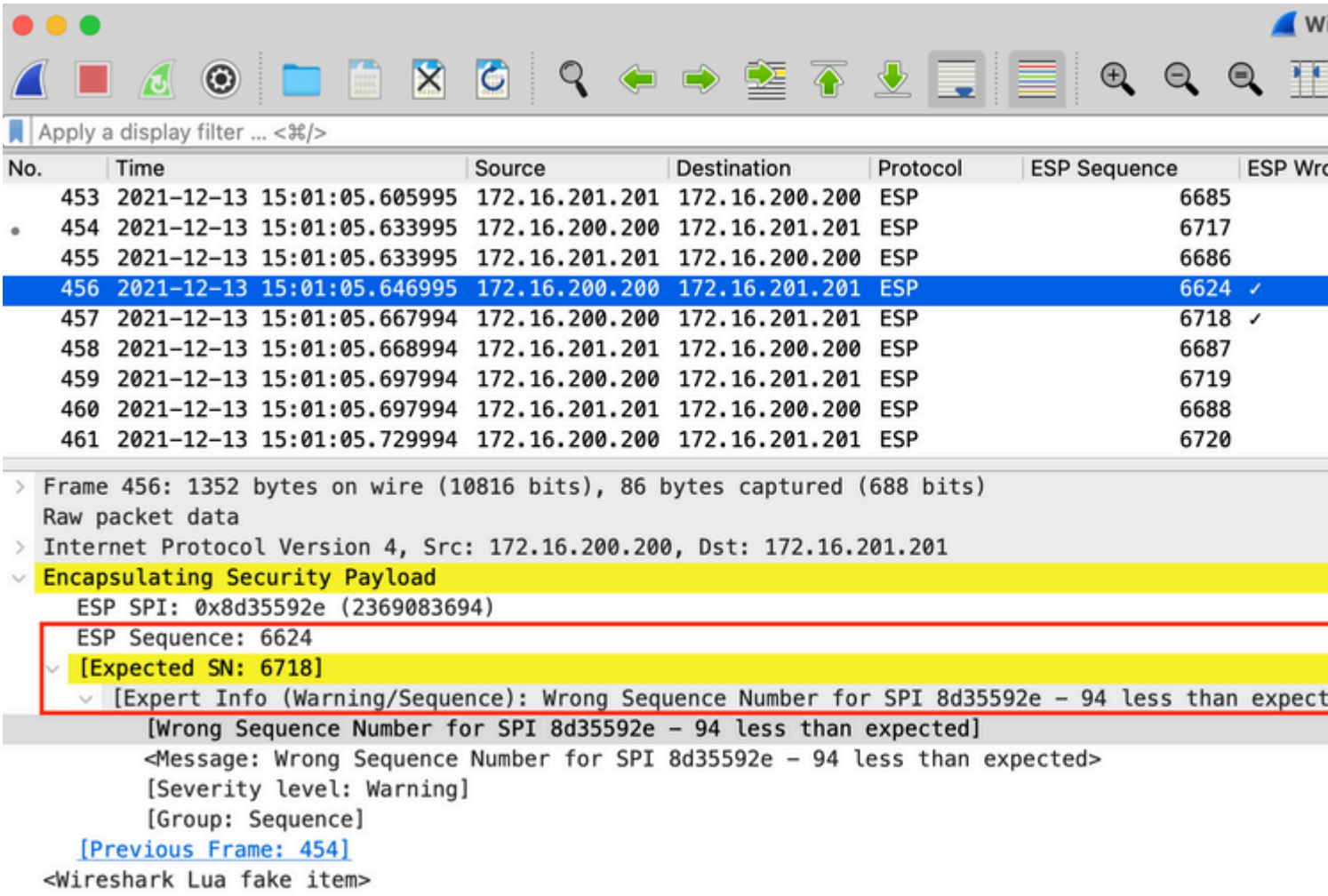
Depois que a captura de pacotes para os pacotes criptografados (ESP) na interface WAN tiver sido coletada, o Wireshark pode ser usado para executar a análise do número de sequência ESP para qualquer anomalia de número de sequência. Primeiro, certifique-se de que a verificação do número de sequência esteja ativada em **Preferências > Protocolos > ESP** conforme mostrado na imagem:



Em seguida, verifique se há algum problema de ESP Sequence Number sob **Analyze > Expert**, da seguinte maneira:



Clique em qualquer um dos pacotes com o número de sequência incorreto para obter detalhes adicionais da seguinte maneira:



Solução

Depois que o peer é identificado e a captura de pacotes é coletada para as quedas de repetição, três cenários possíveis podem explicar as falhas de repetição:

1. É um pacote válido que foi atrasado:
   As capturas de pacotes ajudam a confirmar se o pacote é realmente válido e se o problema é insignificante (devido à latência da rede ou a problemas no caminho de transmissão) ou exige uma solução de problemas mais detalhada. Por exemplo, a captura mostra um pacote com um número sequencial de X que chega fora de ordem e o tamanho da janela de repetição está definido atualmente como 64. Se um pacote válido com número de sequência (X + 64) chegar antes do pacote X, a janela será deslocada para a direita e o pacote X será descartado devido a uma falha de repetição.

   Nesses cenários, é possível aumentar o tamanho da janela de repetição ou desativar a verificação de repetição para garantir que tais atrasos sejam considerados aceitáveis e que os pacotes legítimos não sejam descartados. Por padrão, o tamanho da janela de repetição é relativamente pequeno (tamanho de janela de 64). Se você aumentar o tamanho, não aumentará muito o risco de um ataque. Para obter informações sobre como configurar uma janela IPsec Anti-Replay, consulte o documento Como configurar a janela IPsec Anti-Replay: Expandindo e desativando.

> **Dica:** se a janela de repetição for desativada ou alterada no perfil IPSec usado em uma Virtual Tunnel Interface (VTI), as alterações não entrarão em vigor até que o perfil de proteção seja removido e reaplicado ou a interface de túnel seja redefinida. Esse é o comportamento esperado

---

porque os perfis IPsec são um modelo usado para criar um mapa de perfil de túnel quando a interface de túnel é ativada. Se a interface já estiver ativa, as alterações no perfil não afetarão o túnel até que a interface seja redefinida.

Observação: os modelos anteriores do Aggregation Services Router (ASR) 1000 (como o ASR1000 com ESP5, ESP10, ESP20 e ESP40, juntamente com o ASR1001) não suportavam um tamanho de janela de 1024, mesmo que o CLI permitisse essa configuração. Como resultado, o tamanho da janela relatado na saída do comando **show crypto ipsec sa** pode não estar correto. Utilize o comando **show crypto ipsec sa peer ip-address platform** para verificar o tamanho da janela de antirreprodução do hardware. O tamanho padrão da janela é de 64 pacotes em todas as plataformas. Para obter mais informações, consulte o bug da Cisco ID CSCso45946. As plataformas de roteamento posteriores do Cisco IOS XE (como o ASR1K com ESP100 e ESP200, o ASR1001-X e ASR1002-X, roteadores da série Integrated Service Router (ISR) 4000 e roteadores da série Catalyst8000) suportam um tamanho de janela de 1024 pacotes nas versões 15.2(2)S e posteriores.

2. Isso se deve à configuração de QoS no endpoint de envio:
   Essa situação requer um exame cuidadoso e o ajuste de alguns QoS para mitigar a condição. Para obter uma descrição mais detalhada deste tópico e de uma possível solução, consulte o artigo Considerações sobre antirreprodução em uma VPN IPSec habilitada para voz e vídeo (V3PN).

3. É um pacote duplicado que foi recebido anteriormente:
   Se esse for o caso, dois ou mais pacotes com o mesmo número de sequência ESP dentro do mesmo fluxo IPsec podem ser observados na captura de pacotes. Nesse caso, espera-se que o pacote seja descartado, pois a proteção de repetição do IPsec funciona como planejado para evitar ataques de repetição na rede, e o Syslog é apenas informativo. Se essa condição persistir, ela deverá ser investigada como uma possível ameaça à segurança.

Observação: as falhas de verificação de repetição só são vistas quando um algoritmo de autenticação está habilitado no conjunto de transformação IPsec. Outra maneira de suprimir essa mensagem de erro é desabilitar a autenticação e executar somente a criptografia; no entanto, isso é altamente desaconselhado devido às implicações de segurança da autenticação desabilitada.

Informações adicionais

Identificar e Solucionar Problemas de Repetição em Roteadores Legados com o Cisco IOS Classic

Os descartes de repetição de IPsec nos roteadores ISR G2 Series legados que usam o Cisco IOS são diferentes dos roteadores que usam o Cisco IOS XE, como mostrado aqui:

<#root>

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

connection id=529, sequence number=13

Observe que a saída da mensagem não fornece o endereço IP do peer nem informações SPI. Para solucionar problemas nessa plataforma, use o "conn-id" na mensagem de erro. Identifique o "conn-id" na mensagem de erro e procure-o na saída do comando **show crypto ipsec sa**, já que a repetição é uma verificação por SA (em oposição a uma verificação por peer). A mensagem Syslog também fornece o número de sequência ESP, que pode ajudar a identificar exclusivamente o pacote descartado na captura de pacotes.

> **Observação**: com versões diferentes de código, o "conn-id" é o **conn id** ou o **flow_id** para a SA de entrada.

Isso é ilustrado aqui:

<#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>
```

Como pode ser visto nessa saída, a queda de repetição é do endereço de peer 10.2.0.200 com um ESP SA SPI de entrada de 0xE7EDE943. Também pode ser observado na própria mensagem de registro que o número de sequência ESP para o pacote descartado é 13. A combinação de endereço de peer, número SPI e número de sequência ESP pode ser usada para identificar exclusivamente o pacote descartado na captura de pacotes.

> **Observação**: a mensagem do Syslog do Cisco IOS tem taxa limitada para o pacote de dataplane que cai para um por minuto. Para obter uma contagem precisa do número exato de pacotes descartados, use o comando **show crypto ipsec sa detail** como mostrado anteriormente.

Trabalhar com software Cisco IOS XE anterior

Nos roteadores que executam as versões anteriores do Cisco IOS XE, o "REPLAY_ERROR" relatado no Syslog pode não imprimir o fluxo IPsec real com as informações de peer em que o pacote repetido é descartado, como mostrado aqui:

```
%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
```

Para identificar as informações corretas de peer e fluxo do IPsec, use o Identificador de Plano de Dados (DP - Data Plane) impresso na mensagem Syslog como o parâmetro de entrada SA Handle neste comando, para recuperar as informações de fluxo do IPsec no Processador de Fluxo Quântico (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>
```

Um script do Embedded Event Manager (EEM) também pode ser usado para automatizar a coleta de dados:

```
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"
```

Neste exemplo, a saída coletada é redirecionada para o **flash de inicialização.** Para ver essa saída, use o

comando **more bootflash:replay-error.txt**.

Informações Relacionadas

- Projeto de Rede de Referência da Solução VPN IPSec (V3PN) Habilitada para Voz e Vídeo
- How to Configure IPsec Anti-Replay Window: Expanding and Disabling (Como configurar a janela de antirreprodução IPsec: expandindo e desabilitando).
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.