IPsec Anti-Replay Window Expanding and Disabling

Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPsec Anti-Replay Window Expanding and Disabling

- Before configuring this feature, you should have already created a crypto map or crypto profile.

- To configure the IPsec Anti-Replay Window: Expanding and Disabling feature, you should understand the following concept: IPsec Anti-Replay Window, on page 2

Information About IPsec Anti-Replay Window Expanding and Disabling

IPsec Anti-Replay Window

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded when they arrive outside of the 64 packet replay window at the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

How to Configure IPsec Anti-Replay Window Expanding and Disabling

Configuring IPsec Anti-Replay Window Expanding and Disabling Globally

To configure IPsec Anti-Replay Window: Expanding and Disabling globally (so that it affects all SAs that are created), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size** [*N*]
4. **crypto ipsec security-association replay disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec security-association replay window-size** [*N*] **Example:** `Router (config)# crypto ipsec security-association replay window-size 256`	Sets the size of the SA replay window globally. **Note** Configure this command or the **crypto ipsec security-association replay disable** command. The two commands are not used at the same time.
Step 4	**crypto ipsec security-association replay disable** **Example:** `Router (config)# crypto ipsec security-association replay disable`	Disables checking globally. **Note** Configure this command or the **crypto ipsec security-association replay window-size** command. The two commands are not used at the same time.

Configuring IPsec Anti-Replay Window Expanding and Disabling on a Crypto Map

To configure IPsec Anti-Replay Window: Expanding and Disabling on a crypto map so that it affects those SAs that have been created using a specific crypto map or profile, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
4. **set security-association replay window-size** [*N*]
5. **set security-association replay disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] **Example:** `Router (config)# crypto map ETHO 17 ipsec-isakmp`	Enters crypto map configuration mode and creates a crypto profile that provides a template for configuration of dynamically created crypto maps.
Step 4	**set security-association replay window-size** [*N*] **Example:** `Router (crypto-map)# set security-association replay window-size 128`	Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or cyrpto profile. **Note** Configure this command or the **set security-association replay disable** command. The two commands are not used at the same time.
Step 5	**set security-association replay disable** **Example:** `Router (crypto-map)# set security-association replay disable`	Disables replay checking for a particular crypto map, dynamic crypto map, or crypto profile. **Note** Configure this command or the **set security-association replay window-size** command. The two commands are not used at the same time.

Troubleshooting Tips

- If your replay window size has not been set to a number that is high enough for the number of packets received, you will receive a system message such as the following:

```
*Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection
id=1
```

The above message is generated when a received packet is judged to be outside the anti-replay window.

Configuration Examples for IPsec Anti-ReplayWindow Expanding and Disabling

Global Expanding and Disabling of an Anti-Replay Window Example

The following example shows that the anti-replay window size has been set globally to 1024:

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252  serial restart-delay 0  crypto map mymap !
ip classless
ip route 0.0.0.0 0.0.0.0 192.165.200.1
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101 remark
 Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

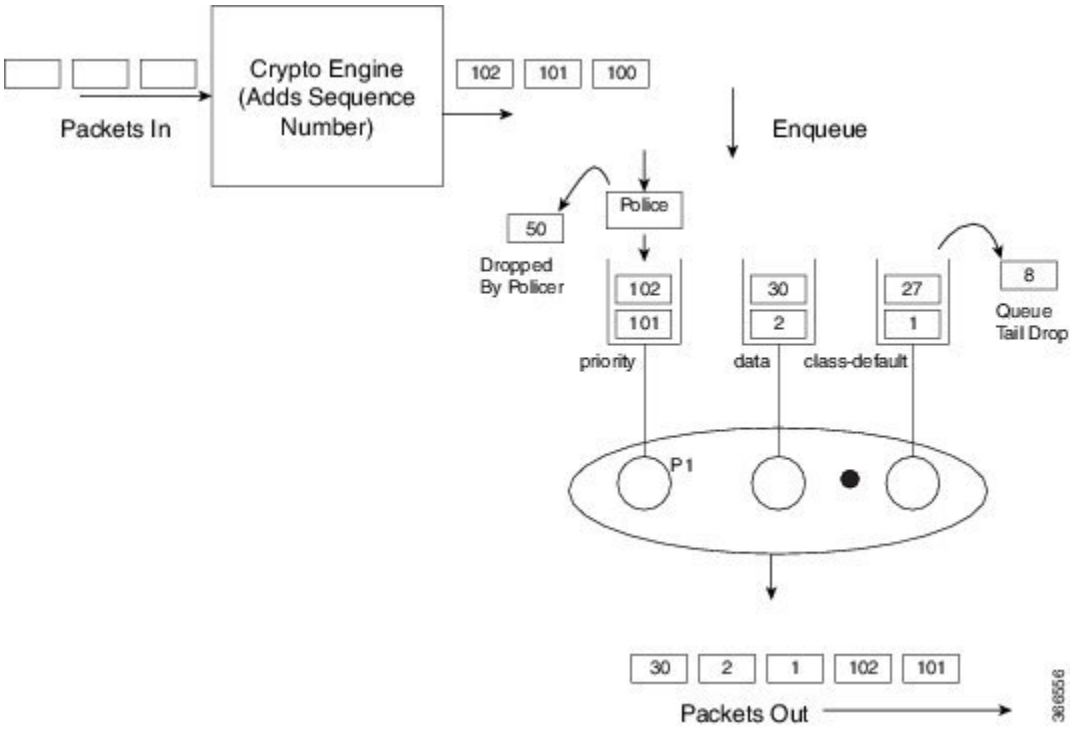
Expanding and Disabling of an Anti-Replay Window for Crypto Maps or Crypto Profiles Example

The following example shows that anti-replay checking is disabled for IPsec connections to 172.17.150.2 but enabled (and the default window size is 64) for IPsec connections to 172.17.150.3 and 172.17.150.4:

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1 enable password ww !
ip subnet-zero
!
cns event-service server
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set 180cisco
 esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170 crypto
 map ETH0 18 ipsec-isakmp  set peer 192.168.1.3 set transform-set 180cisco match address
180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set 190cisco match
address 190 !
interface FastEthernet0
 ip address 172.17.150.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no mop enabled
 crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !
access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip 172.16.160.0
 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
logi
end
```

IPsec Anti Replay Mechanism for QoS

It is normal for packets to be reordered in IP networks, where QoS mechanisms (on the egress interface of the encrypting device or on other network elements in the path), loadbalancing mechanisms or routing / path selection mechanisms (that send different flows over different paths) are used.

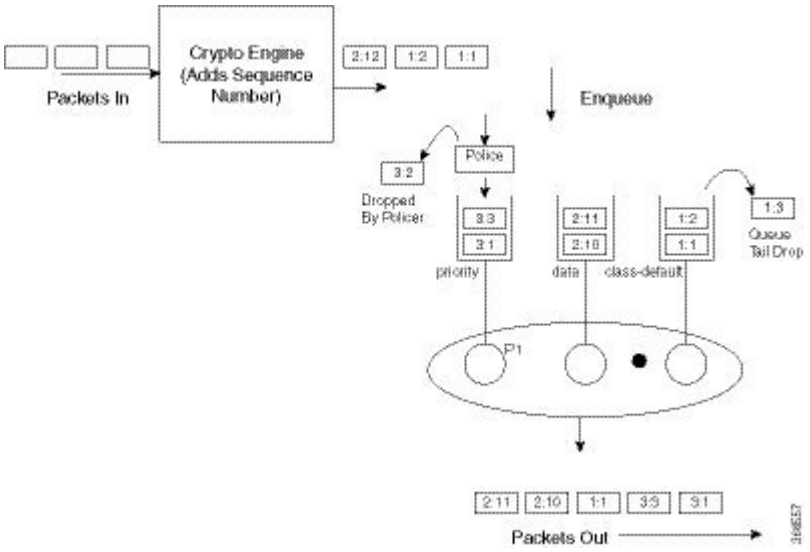


The above diagram shows how anti-replay protection system causes problems when QoS reorders packets. The encryption engine adds sequence numbers. After these numbers are added, packets are enqueued in egress queues depending on the application within that packet. In the example in the diagram, packets are already present in the bandwidth queues (data and class-default), when packets with the sequence numbers 101 and 102 are enqueued in the priority queue. The priority packets will be scheduled first. When the decrypting device receives the packet with the sequence number 101, the history in the sliding window is moved to 101, implying that the sliding window creates a history of sequence numbers 30-101. When the next packet which has the sequence number 102 is received, the history in the sliding window is changed to 39-102. Now, that there are no more packets in the priority queue, packets from one of the other queue is taken – for example, packet with the sequence number 1. Although this is the first time the decrypting device is receiving a packet with sequence number 1, the packet is dropped because of the history maintained in the sliding window.

Moving QoS scheduling before the encryption may solve the anti-replay issue but would render the QoS functionality useless. In addition, scheduling needs to be driven by the congestion of the egress interface (or a shaper on that interface). Increasing the size of the anti-replay window places a huge load load on the memory of the devices that handles this functionality.

Hence, the solution of maintaining multiple sequence number spaces per security association was introduced. The number spaces would be aligned with the egress queuing scheme such that all packets in a given queue would receive a sequence number from the same sequence number space. Since all packets within a sequence number space would go through the same queue, the possibility of egress QoS causing reordering within those packets is eliminated. It is still possible (but unlikely) that reordering within a number space could happen

elsewhere in the network. If packets are tail dropped rather than enqueued out of sequence (not out of order), sequence numbers will still be received on the receiving side. Hence, we still maintain a history window per sequence number space but that history is considerably shorter.



The image shows that the sequence number consists of two parts, namely the selector and the sequence number. The receiving side would use the selector to choose the correct history to use and the sequence number would operate as always.

Note IPSec Anti-Replay feature does not support Group Encrypted Transport VPN (GETVPN) when multiple sequence number space (multi-SNS) is enabled.

IPsec Anti-Replay Packet Loss Avoidance

The IPsec Anti-Replay Packet Loss Avoidance feature avoids unnecessary IPSec Anti-Replay packet drops when QoS is configured with IPSec. However, some packet drops can happen under certain circumstances when QoS is used together with IPSec Anti-Replay enabled. Anti-Replay drops are seen for a second or two with multi-SNS enabled when a class-map is added or removed while crypto interface is attached on the peer router. The traffic recovers after a couple of seconds and no drops are seen after that.

The Anti-Replay drops can occur in the following situations:

- When a packet is in transit, a class is deleted from the QoS policymap. The packets that belong to this class are exhausted and the incoming packets are queued behind all the packets in the class-default queue. This can cause disruption in the sequence number space causing Anti-Replay drops. The queue becomes empty and the system recovers soon enough to resume normal behavior.
- When an ESP-based High Availability is configured and the over-subscribed traffic is sent through all the sequence number spaces Anti-Replay drops occur. With over-subscribed traffic on the sender side, traffic is shaped based on QoS policy. As a result, the receiving router gets packets with out of order sequence numbers. These drops are momentary and are recovered soon.
- During rekeying of security associations (SA), a router keeps both the old and new inbound Security Parameter Index (SPI) for a short period of time. Old SA is deleted after a short period. After the old SA

is deleted, if router receives any packet with old SPI (which can happen when there is a QoS policy), it drops the packet with invalid SPI error.

Configuring IPsec Anti-Replay for QoS

Given below is the command to enable multiple sequence number space per IPSec SA:

```
Device(config)#crypto ipsec security-association multi-sn
```

Caution All existing sessions need to be cleared before configuring this feature. Else, traffic from the existing sessions will be dropped.

Caution This feature needs to be configured on both the tunnel routers in an IPSec connection. If this featues is only enabled on one router, the other router will drop packets.

Show Commands

show platform hardware qfp active feature ipsec datapath crypto-sa

This command displays the mapping between the sequence number spaces and the sequence numbers in an IPsec SA in QFP:

```
Device# show platform hardware qfp active feature ipsec datapath crypto-sa 4
Crypto Context Handle: e8b06b60
peer sa handle: 0
anti-replay enabled
esn disabled
Outbound SA
Total SNS: 16
Space                current seq number
----------------------------------------
   0                                   0
   1                                   0
   2                                   0
   3                                   0
   4                                   0
   5                                   0
   6                                   0
   7                                   0
   8                                   0
   9                                   0
  10                                   0
  11                                 100
  12                                   0
  13                                   0
  14                                   0
  15                                   0
```

show platform hardware qfp active feature ipsec sa

This command displays the IPsec SA in Cisco QuantumFlow Processor (Cisco QFP):

```
Device# show platform hardware qfp active feature ipsec sa 6
QFP ipsec sa Information

         QFP sa  id: 6
          pal sa id: 170
         QFP spd id: 1
          QFP sp id: 2
            QFP spi: 0xa4a5244(172642884)
        crypto ctx: 0x00000000e8b14a20
              flags: 0x4640068 (Details below)
                   : src:IKE  valid:Yes  soft-life-expired:No  hard-life-expired:No
                   : replay-check:No  proto:ESP  mode:Receive-only  direction:Egress
                  : qos_preclassify:No  qos_group:No
                   : frag_type:AFTER_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: 0x59e=1438
            mtu_adj: 0x588=1416
          sar_delta: 0
         sar_window: 0x0
         sibling_sa: 0x0
             sp_ptr: 0xe8abc000
            sbs_ptr: 0xe8a73878
     local endpoint: 33.0.0.3
    remote endpoint: 33.0.0.4
   cgid.cid.fid.rid: 1.1.1.11141121
               ivrf: 0
               fvrf: 0
    trans udp sport: 0
    trans udp dport: 0
    first intf name: Tunnel0
nat fixup src port: 0
    nat fixup  ip: 0.0.0.0
```

show platform software ipsec fp active flow

This command displays the IPsec SA in the fman-fp process for a given flow ID:

```
Device# show platform software ipsec fp active flow identifier 169
Flow id: 169
                mode: tunnel
           direction: inbound
            protocol: esp
                 SPI: 0xbcd8840
      local IP addr: 33.0.0.3
     remote IP addr: 33.0.0.4
   crypto device id: 0
      crypto map id: 1
             SPD id: 1
          QFP SPD id: 1
    ACE line number: 1
      QFP SA handle: 5
IOS XE interface id: 11
     interface name: Tunnel0
   Crypto SA ctx id: 0x00000000e8b148c0
              cipher: AES-128
                auth: SHA256
initial seq.number: 0
      timeout, mins: 0
               flags: exp time;exp traffic;
Time limits
```

```
    soft limit(sec): 3401
    hard limit(sec): 3568
Traffic limits

     soft limit(kb): 3962880
     hard limit(kb): 4608000
     inline_tagging: DISABLED
anti-replay window: 64
SPI Selector:

   remote addr low: 0.0.0.0
  remote addr high: 0.0.0.0
    local addr low: 33.0.0.3
   local addr high: 33.0.0.3
Classifier: range

   src IP addr low: 33.0.0.3
  src IP addr high: 33.0.0.3
   dst IP addr low: 33.0.0.4
  dst IP addr high: 33.0.0.4
      src port low: 0
     src port high: 65535
      dst port low: 0
     dst port high: 65535
      protocol low: 47
     protocol high: 47
------------- Statistics

            octets(delta): 0
      total octets(delta): 4718576880
           packets(delta): 0
   dropped packets(delta): 0
      replay drops(delta): 0
      auth packets(delta): 0
        auth fails(delta): 0
encrypted packets(delta): 0
     encrypt fails(delta): 0
---------- End statistics

       object state: active
--------------- AOM

         cpp aom id: 894
         cgm aom id: 0
          n2 aom id: 891
          if aom id: 0
```

show crypto ipsec sa <ip> peer

This command retrieves the IPSec SA ID for the given peer and displays the SA in all the layers, which is from the IOS layer to the QFP layer.

```
Device# polaris-csr#show crypto ipsec sa peer 33.0.0.4 platform

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 33.0.0.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (33.0.0.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (33.0.0.4/255.255.255.255/47/0)
   current_peer 33.0.0.4 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 190, #pkts encrypt: 190, #pkts digest: 190
```

```
    #pkts decaps: 190, #pkts decrypt: 190, #pkts verify: 190
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 33.0.0.3, remote crypto endpt.: 33.0.0.4
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
     current outbound spi: 0xA4A5244(172642884)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xBCD8840(198019136)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 2169, flow_id: CSR:169, sibling_flags FFFFFFFF80004048, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607985/3255)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA4A5244(172642884)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 2170, flow_id: CSR:170, sibling_flags FFFFFFFF80004048, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607989/3255)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Additional References

The following sections provide references related to IPsec Anti-Replay Window: Expanding and Disabling.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Security Command Reference
IP security and encryption	Configuring Security for VPNs with IPsec

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for IPsec Anti-Replay Window Expanding and Disabling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IPsec Anti-Replay Window: Expanding and Disabling

Feature Name	Releases	Feature Information
IPsec Anti-Replay Window: Expanding and Disabling	Cisco IOS XE Release 2.1	Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets. The following commands were introduced or modified: **crypto ipsec security-association replay disable**, **ipsec security-association replay window-size**, **security-association replay disable**, **security-association replay window-size**.
IPSec anti-replay should work when QoS is enabled in CSR platforms.	Cisco IOS XE Release 16.6.1	This feature enables support for IPSec anti-replay mechanism when QoS is enabled in Cisco Cloud Services Router 1000V Series. The following commands were introduced or modified: **show platform hardware qfp active feature ipsec**, **show platform software ipsec fp active flow**, **show crypto ipsec sa**.
IPSec anti-replay should work when QoS is enabled in ISR 4300/4200 platforms.	Cisco IOS XE Release 16.7.1	This feature ensures that IPSec anti-replay mechanism works when QoS is enabled in ISR platforms except ISR 44xx.
Anti-replay QoS/IPSec packet loss avoidance	Cisco IOS XE Release 16.8.1	This feature avoids IPSec anti-replay packet drops when QoS is used with IPSec anti-replay enabled. This support is added on Octeon-based ASR platforms only.