IPsec アンチリプレイウィンドウの拡張と無効化

Cisco IP セキュリティ（IPsec）認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます。それらの番号に基づいて、デクリプタが検知したパケットを追跡します。現在、デフォルトのウィンドウ サイズは、64 パケットです。一般的にはこの数字（ウィンドウ サイズ）で十分ですが、このウィンドウ サイズを拡張する必要がある場合もあります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

IPsec アンチ リプレイ ウィンドウの拡張と無効化の前提条件

- この機能を設定する前に、クリプトマップまたは暗号プロファイルを作成しておく必要があります。
- IPsec アンチリプレイウィンドウの拡張とディセーブル化機能を設定するには、次の概念を理解しておく必要があります。IPsec アンチ リプレイ ウィンドウ （2 ページ）

IPsecアンチリプレイウィンドウの拡張と無効化に関する情報

IPsec アンチ リプレイ ウィンドウ

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます（セキュリティ アソシエーション（SA）アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです）。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値Xはデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64パケット ウィンドウ サイズでは不十分な場合があります。たとえば、Cisco Quality of Service（QoS）によってハイプライオリティパケットにプライオリティが与えられている場合、一部のロープライオリティパケットは、それらがデクリプタに64パケットのリプレイウィンドウを超えて到着すると、廃棄されてしまう可能性があります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

IPsecアンチリプレイウィンドウの拡張と無効化機能の設定方法

IPsec アンチ リプレイ ウィンドウの拡張と無効化のグローバル設定

IPsec アンチ リプレイ ウィンドウ：拡張と無効化をグローバルに設定する（その結果、作成されるすべての SA が影響を受けます）には、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec security-association replay window-size** [*N*] 例： `Router (config)# crypto ipsec security-association replay window-size 256`	SA リプレイ ウィンドウのサイズをグローバルに設定します。 （注） このコマンドまたは **crypto ipsec security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 4	**crypto ipsec security-association replay disable** 例： `Router (config)# crypto ipsec security-association replay disable`	検査をグローバルにイネーブルにします。 （注） このコマンドまたは **crypto ipsec security-association replay window-size** コマンドを設定します。この2つのコマンドは、同時に使用できません。

クリプトマップ上における IPsec アンチリプレイウィンドウの拡張と無効化の設定

暗号マップ上でIPsecアンチリプレイ ウィンドウの拡張と無効化を、特定の暗号マップまたはプロファイルを使用して作成された SA に影響を与えるように設定するには、次の手順を実行します。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] 例： `Router (config)# crypto map ETHO 17 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始し、動的に作成されるクリプトマップの設定のためのテンプレートを提供する暗号プロファイルを作成します。
ステップ 4	**set security-association replay window-size** [*N*] 例： `Router (crypto-map)# set security-association replay window-size 128`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルによって指定されたポリシーを使用して作成される SA を制御します。 （注） このコマンドまたは **set security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 5	**set security-association replay disable** 例： `Router (crypto-map)# set security-association replay disable`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルに対するリプレイ検査をディセーブルにします。 （注） このコマンドまたは **set security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

トラブルシューティングのヒント

• 受信されるパケットの数に対して十分高い数字がリプレイ ウィンドウ サイズに設定されていない場合、次のようなシステム メッセージが受信されます。

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

受信されたメッセージが、アンチ リプレイ ウィンドウの範囲を超えていると判断されると、上記メッセージが生成されます。

IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定例

アンチ リプレイ ウィンドウのグローバル拡張と無効化：例

次の例は、アンチ リプレイ ウィンドウ サイズがグローバルに 1024 に設定されていることを示しています。

```
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
```

暗号マップまたは暗号プロファイルのアンチ リプレイ ウィンドウの拡張および無効化：例

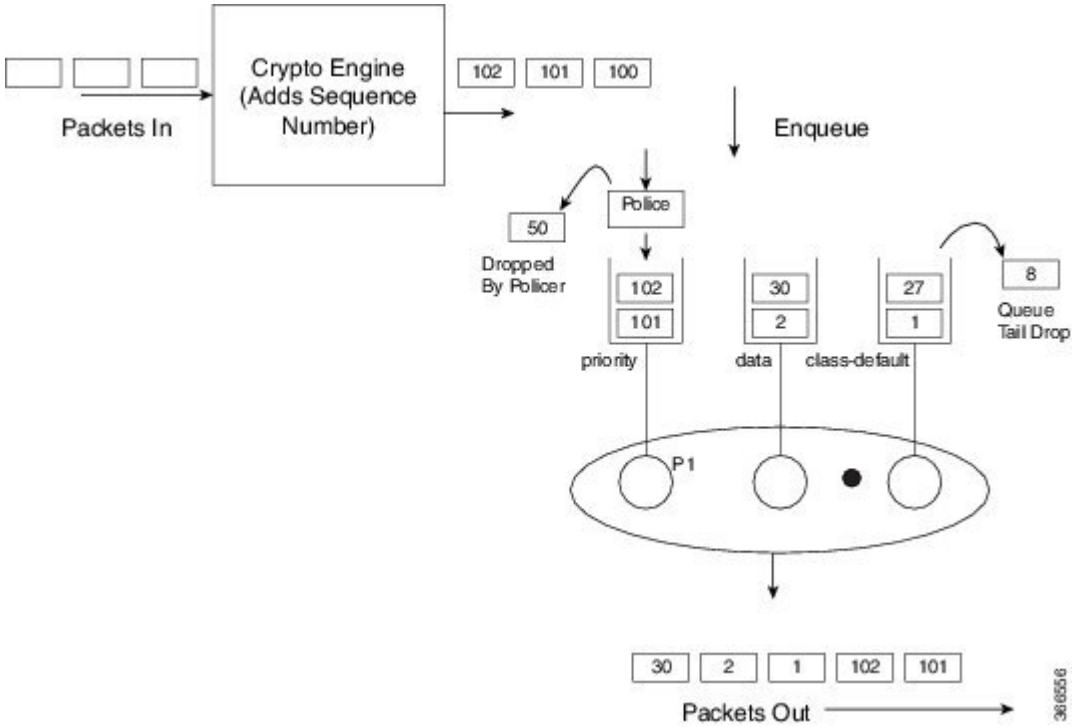
次の例では、アンチ リプレイ検査が、172.17.150.2 への IPsec 接続に関してディセーブルにされているが、172.17.150.3 および 172.17.150.4 への IPsec 接続に関してはイネーブル（および、デフォルトのウィンドウ サイズが 64）にされていることを示しています。

```
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
```

QoS のための IPsec アンチリプレイのメカニズム

QoS メカニズム（暗号化デバイスの出力インターフェイスまたはパス内の他のネットワーク要素上）、ロードバランシング メカニズム、またはルーティング/パス選択メカニズム（異なるパスを介して異なるフローを送信する）が使用される IP ネットワークでは、パケットの順序が変更されるのは通常のことです。

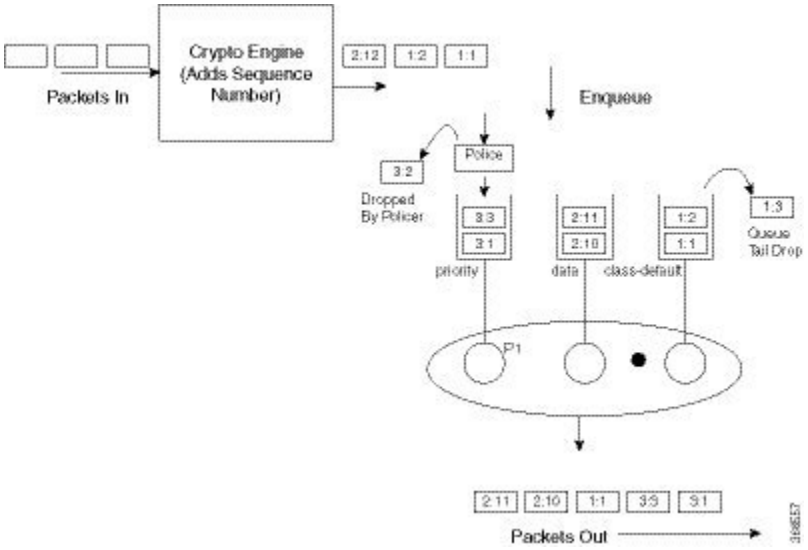


上の図は、QoS がパケットの順序を変更するときに、アンチリプレイ保護システムがどのように問題を引き起こすのかを示しています。暗号化エンジンはシーケンス番号を追加します。これらの番号が追加されると、パケットは、そのパケット内のアプリケーションに応じて出力キューに入れられます。図の例では、シーケンス番号 101 および 102 のパケットがプライオリティキューに入れられるときに、パケットがすでに帯域幅キュー（data および class-default）に

存在しています。プライオリティパケットが最初にスケジュールされます。復号デバイスがシーケンス番号 101 のパケットを受信すると、スライディングウィンドウの履歴は 101 に移動します。これは、スライディングウィンドウがシーケンス番号 30 ～ 101 の履歴を作成することを意味します。シーケンス番号 102 を持つ次のパケットが受信されると、スライディングウィンドウの履歴が 39 ～ 102 に変更されます。この時点で、プライオリティキューにパケットがないため、他のキューのいずれかからパケット（たとえば、シーケンス番号 1 のパケット）が取得されます。復号デバイスがシーケンス番号1のパケットを受信するのはこれが初めてですが、スライディングウィンドウで履歴が維持されているため、パケットはドロップされます。

暗号化の前に QoS スケジューリングを移動すると、アンチリプレイの問題が解決される可能性がありますが、QoS機能が役に立たなくなります。さらに、スケジューリングは、出力インターフェイス（またはそのインターフェイスのシェイパー）の輻輳によって駆動される必要があります。アンチリプレイウィンドウのサイズを大きくすると、この機能を処理するデバイスのメモリに大きな負荷がかかります。

そのため、セキュリティアソシエーションごとに複数のシーケンス番号スペースを維持するソリューションが導入されました。特定のキュー内のすべてのパケットが同じシーケンス番号スペースからシーケンス番号を受け取るように、番号スペースが出力キューイングスキームに合わせて調整されます。シーケンス番号スペース内のすべてのパケットが同じキューを通過するため、出力 QoS によってそれらのパケットの順序が変更される可能性がなくなります。番号スペース内の順序変更がネットワークの他の場所で発生する可能性は依然としてあります（ただし、可能性は低い）。パケットがシーケンス番号どおりにキューに入れられずにテールドロップされた（順不同で入れられたのではない）場合でも、シーケンス番号は受信側で受信されます。そのため、シーケンス番号スペースごとの履歴ウィンドウは維持されますが、その履歴はかなり短くなります。



この図は、シーケンス番号がセレクタとシーケンス番号の2つの部分で設定されていることを示しています。受信側は、セレクタを使用して、使用する正しい履歴を選択し、シーケンス番号は通常どおりに動作します。

（注） 複数のシーケンス番号スペース（マルチ SNS）が有効になっている場合、IPsec アンチリプレイ機能は Group Encrypted Transport VPN（GETVPN）をサポートしません。

IPsec アンチリプレイパケット損失の回避

IPsec アンチリプレイパケット損失の回避の機能により、QoS が IPsec で設定されている場合に、不要な IPsec アンチリプレイパケットのドロップが回避されます。ただし、IPSec アンチリプレイが有効な状態で QoS が使用されている場合、特定の状況下で一部のパケットのドロップが発生する可能性があります。暗号インターフェイスがピアルータに接続されているときにクラスマップが追加または削除されると、マルチ SNS が有効になっている場合、1 ～ 2 秒間、アンチリプレイドロップが発生します。トラフィックは数秒後に回復し、その後はドロップが見られません。

アンチリプレイドロップは、次の状況で発生する可能性があります。

- パケットの転送中に、クラスが QoS ポリシーマップから削除されます。このクラスに属するパケットが使い果たされ、着信パケットが、class-default キューに入っているすべてのパケットの後にキューイングされます。これにより、シーケンス番号スペースが壊れ、アンチリプレイドロップが発生する可能性があります。キューが空になり、システムはすぐに回復して通常の動作を再開します。
- ESP ベースのハイアベイラビリティが設定され、オーバーサブスクライブされたトラフィックがすべてのシーケンス番号スペースを介して送信されるときに、アンチリプレイドロップが発生します。送信側でオーバーサブスクライブされたトラフィックがある場合、トラフィックは QoS ポリシーに基づいてシェーピングされます。その結果、受信側ルータが、シーケンス番号の順序が正しくないパケットを受信します。これらのドロップは一時的であり、すぐに回復します。
- セキュリティ アソシエーション（SA）のキー再生成中に、ルータが、新旧両方のインバウンド セキュリティ パラメータ インデックス（SPI）を短期間保持します。古い SA は短期間で削除されます。古い SA が削除された後、ルータが古い SPI を持つパケットを受信すると（QoS ポリシーが存在する場合に発生する可能性があります）、無効 SPI エラーによりパケットがドロップされます。

QoS のための IPsec アンチリプレイの設定

次に、IPsec SA ごとに複数のシーケンス番号スペースを有効にするコマンドを示します。

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

注意 この機能を設定する前に、既存のすべてのセッションをクリアする必要があります。そうしないと、既存のセッションからのトラフィックがドロップされます。

注意 この機能は、IPsec 接続の両方のトンネルルータで設定する必要があります。この機能が一方のルータでしか有効になっていない場合、もう一方のルータはパケットをドロップします。

コマンドの表示

show platform hardware qfp active feature ipsec datapath crypto-sa

このコマンドにより、QFP の IPsec SA におけるシーケンス番号スペースとシーケンス番号の間のマッピングが表示されます。

```
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

このコマンドは、Cisco QuantumFlow Processor（Cisco QFP）の IPsec SA を表示します。

```
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

このコマンドは、指定されたフロー ID の fman-fp プロセスの IPsec SA を表示します。

```
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

このコマンドは、指定されたピアの IPsec SA ID を取得し、IOS レイヤから QFP レイヤまでのすべてのレイヤの SA を表示します。

```
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:
```

その他の参考資料

次の項では、IPsec アンチ リプレイ ウィンドウの拡張無効化の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Security Command Reference』
IP セキュリティおよび暗号化	IPsec を使用した VPN のセキュリティの設定

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec アンチ リプレイ ウィンドウの拡張と無効化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPsec* アンチ リプレイ ウィンドウの機能情報：拡張と無効化

機能名	リリース	機能情報
IPsec アンチ リプレイ ウィンドウの拡張と無効化	Cisco IOS XE Release 2.1 IPsec アンチリプレイウィンドウの拡張と無効化 （1 ページ）	次のコマンドが導入または変更されました。**crypto ipsec security-association replay disable**、**ipsec security-association replay window-size**、**security-association replay disable**、**security-association replay window-size**
IPsec アンチリプレイは、CSR プラットフォームで QoS が有効になっている場合に機能します。	Cisco IOS XE リリース 16.6.1	この機能により、Cisco Cloud Services Router 1000V シリーズで QoS が有効になっている場合、IPSec アンチリプレイメカニズムのサポートが有効になります。 次のコマンドが導入または変更されました。**show platform hardware qfp active feature ipsec**、**show platform software ipsec fp active flow**、**show crypto ipsec sa**。
IPsec アンチリプレイは、ISR 4300/4200 プラットフォームで QoS が有効になっている場合に機能します。	Cisco IOS XE リリース 16.7.1	この機能により、ISR 44xx を除く ISR プラットフォームで QoS が有効になっている場合、IPsec アンチリプレイメカニズムが確実に機能します。
アンチリプレイ QoS/IPsec パケット損失の回避	Cisco IOS XE リリース 16.8.1	この機能により、IPSec アンチリプレイが有効な状態で QoS が使用されている場合に、IPsec アンチリプレイパケットのドロップが回避されます。 このサポートは、Octeon ベースの ASR プラットフォームにのみ追加されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。