IPSecアンチリプレイチェック障害のトラブルシューティング

内容

はじめに

このドキュメントでは、Internet Protocol Security(IPSec)アンチリプレイチェックの障害に関連する問題について説明し、考えられる解決策を示します。

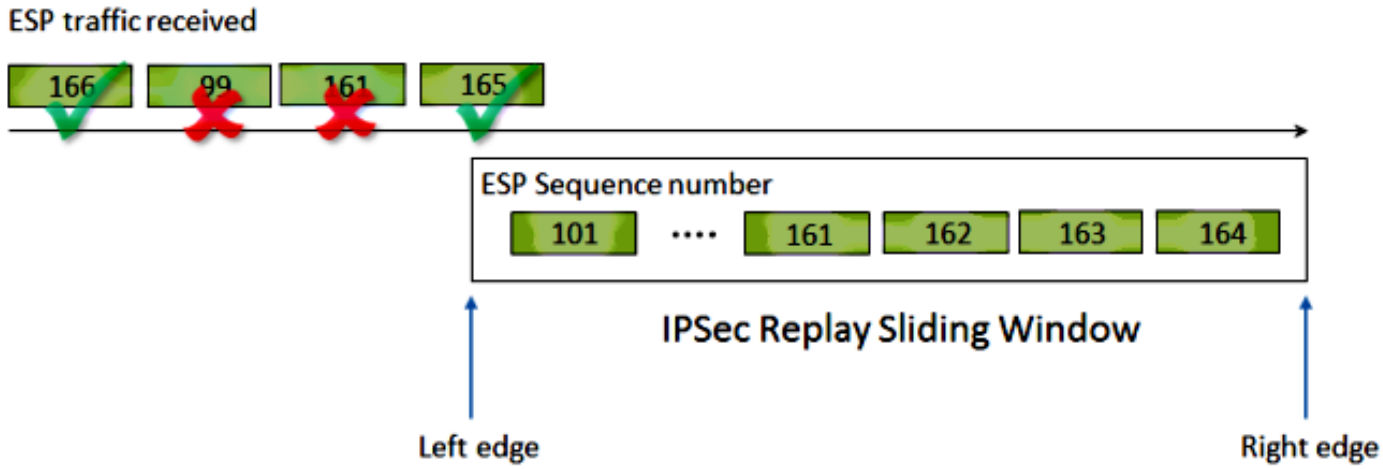
背景説明

リプレイアタックの概要

リプレイアタックは、有効なデータ伝送が悪意をもって、または不正に記録され、後で繰り返されるネットワーク攻撃の一種です。これは、有効なユーザになりすまして正当な接続を中断または悪影響を及ぼすために、正当な通信を記録し、それを繰り返す人物によるセキュリティの弱体化を試みます。

IPsecリプレイチェック保護

IPsecにより暗号化されたパケット毎に単調増加するシーケンス番号を割り当て、攻撃者に対するアンチリプレイ保護を提供する。受信側のIPsecエンドポイントは、これらの番号と受け入れ可能なシーケンス番号のスライディングウィンドウを使用して、すでに処理したパケットを追跡します。Cisco IOS®実装のデフォルトのアンチリプレイウィンドウサイズは、次の図に示すように64パケットです。



IPsecトンネルエンドポイントでアンチリプレイ保護が有効になっている場合、着信IPsecトラフィックは次のように処理されます。

- シーケンス番号がウィンドウ内にあり、以前に受信されていない場合、パケットの整合性がチェックされます。パケットが整合性検証チェックに合格すると、そのパケットは受け入れられ、ルータはこのシーケンス番号が受信されたことを示すマークを付けます。たとえば、Encapsulating Security Payload(ESP)シーケンス番号が162のパケットです。
- シーケンス番号がウィンドウ内にあるものの、以前に受信された場合、パケットはドロップされます。この重複パケットは廃棄され、ドロップはリプレイカウンタに記録されます。

- シーケンス番号がウィンドウ内の最も大きいシーケンス番号よりも大きい場合、パケットの整合性がチェックされます。パケットが整合性検証チェックに合格すると、スライディングウィンドウが右側に移動します。たとえば、シーケンス番号が189の有効なパケットを受信した場合、ウィンドウの新しい右エッジは189に設定され、左エッジは125 (189 - 64 [ウィンドウサイズ]) になります。

- シーケンス番号が左端より小さい場合、パケットはドロップされ、リプレイカウンタに記録されます。これは不正なパケットと見なされます。

リプレイチェックが失敗し、パケットがドロップされた場合、ルータは次のようなSyslogメッセージを生成します。

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

注：リプレイ検出は、IPSecセキュリティアソシエーション(SA)が2つのピア間にのみ存在するという前提に基づいています。Group Encrypted Transport VPN(GETVPN)は、多数のピア間で単一のIPsec SAを使用します。その結果、GETVPNでは、時間ベースのアンチリプレイ障害と呼ばれるまったく異なるアンチリプレイチェックメカニズムが使用されます。このドキュメントでは、ポイントツーポイントIPSecトンネルのカウンタベースのアンチリプレイのみを取り上げます。

注：アンチリプレイ保護は、IPsecプロトコルが提供する重要なセキュリティサービスです。IPSecアンチリプレイを無効にすると、セキュリティ上の問題が発生するため、慎重に行う必要があります。

IPSecリプレイドロップを引き起こす可能性のある問題

すでに説明したように、リプレイ チェックの目的は、悪意によるパケットの繰り返しを防止することです。ただし、次のように、リプレイ チェックが悪意以外の理由で失敗となるシナリオがあります。

- このエラーは、トンネルのエンドポイント間のネットワークパスで十分なパケットが並べ替えられることによって発生する可能性があります。これは、ピア間に複数のネットワークパスがある場合に発生する可能性があります。
- Cisco IOS 内でパケット処理パスが不均等になることによってエラーが発生する場合。たとえば、フラグメント化されたIPsecパケットで、復号化の前にIPの再構成が必要なものは、処理されるまでにリプレイウィンドウの範囲外に入るため、十分に遅延する可能性があります。
- このエラーは、送信側のIPsecエンドポイントまたはネットワークパス内で有効になっているQuality of Service(QoS)が原因で発生する可能性があります。Cisco IOS実装では、出力方向のQoSの前にIPsec暗号化が行われます。Low Latency Queueing（LLQ；低遅延キューイング）などの特定のQoS機能により、IPSecパケット配信が順不同になり、リプレイチェックの失敗が原因で受信側エンドポイントによってドロップされる可能性があります。
- ネットワークの設定や動作に問題があると、パケットがネットワークを通過する際にパケットが重複する可能性があります。

- 攻撃者(man-in-the-middle)は、ESPトラフィックを遅延、ドロップ、および複製する可能性があります。

IPSec リプレイ ドロップのトラブルシューティング

IPSecリプレイドロップのトラブルシューティングで重要となるのは、どのパケットがリプレイによってドロップしたかを特定し、パケットキャプチャを使用して、これらのパケットが実際にリプレイされたパケットであるか、またはリプレイウィンドウ外の受信側ルータに到着したパケットであるかを判別することです。ドロップされたパケットをスニファトレースでキャプチャされた内容と正しく照合するには、最初のステップとして、ピア、ドロップされたパケットが属するIPsecフロー、およびパケットのESPシーケンス番号を特定します。

Cisco IOS XEデータパスパケットトレース機能の使用

Cisco IOS® XEを実行するルータプラットフォームでは、ドロップが発生するとアンチリプレイ問題のトラブルシューティングに役立てるため、ピアに関する情報とIPsec Security Parameter Index(SPI)がSyslogメッセージに出力されます。ただし、まだ失われる重要な情報は、ESPシーケンス番号です。ESP シーケンス番号は、特定の IPSec フローの中の IPSec パケットを一意に

識別するのに使用されます。このシーケンス番号がないと、どのパケットがドロップされたかをパケット キャプチャで識別することが難しくなります。

Cisco IOS XEデータパスのパケットトレース機能は、リプレイドロップが発生した場合に次のsyslogメッセージを表示して使用できます。

```
%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
```

ドロップされたパケットの ESP シーケンス番号を特定するには、パケット トレース機能で次の手順を実行します。

1. ピアデバイスからのトラフィックを照合するために、プラットフォームの条件付きデバッグフィルタを設定します。

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

1. パケット ヘッダー情報をコピーするため、次のように、copy オプションを付加した状態でパケット トレースを有効にします。

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

1. リプレイ エラーが検出されたら、パケット トレース バッファを使用して、リプレイを原因としてドロップされたパケットを識別します。ESP シーケンス番号は、コピーされたパケットの中に表示されます。

<#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
```

上記の出力から、パケット番号 6 と 7 がドロップされていることがわかります。これで、次の詳細な調査が可能になります。

<#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
```

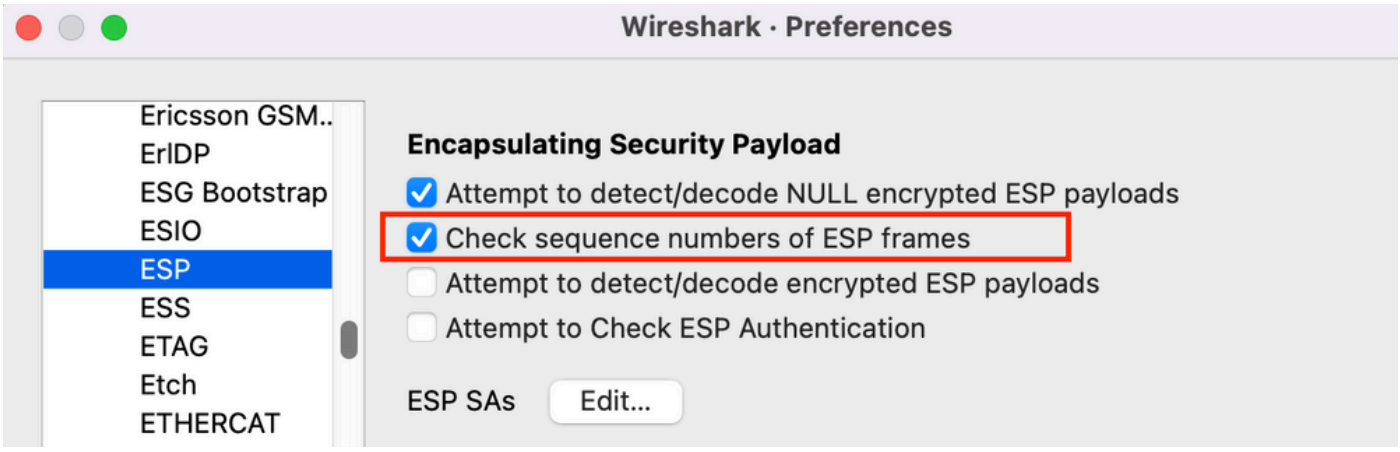
上記の出力で太字で強調されているように、ESPシーケンス番号には、IPヘッダー（またはIPパケットのペイロードデータの4バイト）から始まる24バイトのオフセットがあります。この例では、ドロップされたパケットの ESP シーケンス番号は 0x6 です。

パケットキャプチャの収集

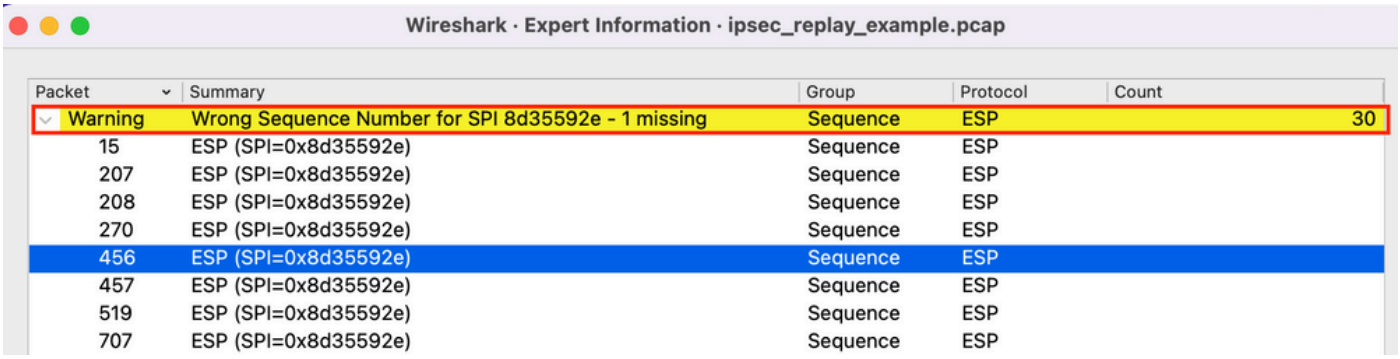
リプレイチェックの失敗によってドロップされたパケットのパケット情報の識別に加えて、対象のIPsecフローのパケットキャプチャを同時に収集する必要があります。これは、同じIPSecフロー内のESPシーケンス番号パターンを調べて、リプレイドロップの理由を特定するのに役立ちます。Cisco IOS XEルータでEmbedded Packet Capture(EPC)を使用する方法の詳細については、「Cisco IOSおよびCisco IOS XEの組み込みパケットキャプチャの設定例」を参照してください。

Wiresharkシーケンス番号分析の使用

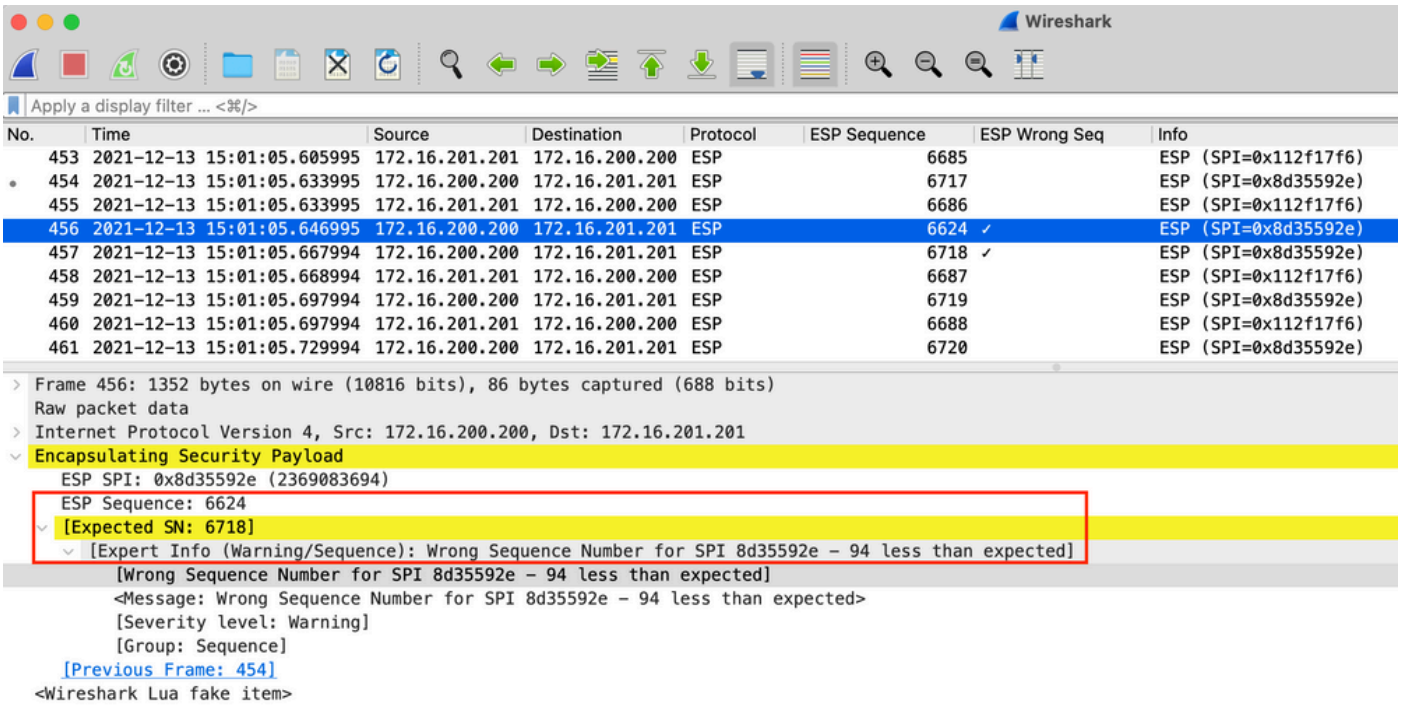
WANインターフェイス上の暗号化(ESP)パケットのパケットキャプチャが収集されると、Wiresharkを使用して、シーケンス番号の異常に対するESPシーケンス番号分析を実行できます。最初に、図に示すように、Preferences > Protocols > ESPでSequence Number Checkが有効になっていることを確認します。



次に、Analyze > Expertの順に選択して、ESPシーケンス番号の問題を確認します。



誤ったシーケンス番号のパケットをクリックすると、次のような詳細情報が表示されます。



解決方法

ピアが特定され、リプレイドロップのパケットキャプチャが収集された後、次の3つのシナリオでリプレイエラーが発生する可能性があります。

1. 遅延した有効なパケットである場合：
   パケット キャプチャは、パケットが実際に有効であるか、また、問題は（ネットワーク遅延または伝送パスの問題による）軽微なものであるか詳細なトラブルシューティングが必要であるか、確認するのに役立ちます。たとえば、このキャプチャでは、シーケンス番号がXのパケットが順不同で到着し、リプレイウィンドウサイズが64に設定されているとします。シーケンス番号(X + 64)を持つ有効なパケットがパケットXの前に到着すると、ウィンドウが右に移動し、パケットXはリプレイ障害のためにドロップされます。

   このようなシナリオでは、リプレイウィンドウのサイズを増やすか、リプレイチェックを無効にして、このような遅延を許容できるものと見なし、正当なパケットが廃棄されないようにすることができます。デフォルトでは、リプレイウィンドウのサイズはかなり小さくなります（ウィンドウサイズは64）。サイズを大きくしても、攻撃のリスクが大幅に高まるこ

とはありません。IPSecアンチリプレイウィンドウの設定方法については、『IPSecアンチリプレイウィンドウの設定方法：拡張と無効化』を参照してください。

ヒント：仮想トンネルインターフェイス(VTI)で使用されているIPSecプロファイルでリプレイウィンドウが無効または変更されている場合、保護プロファイルが削除されて再適用されるか、トンネルインターフェイスがリセットされるまで、変更は有効になりません。IPsecプロファイルは、トンネルインターフェイスの起動時にトンネルプロファイルマップを作成するために使用されるテンプレートであるため、これは正常な動作です。インターフェイスがすでにアップしている場合、プロファイルに対する変更は、インターフェイスがリセットされるまでトンネルに影響しません。

注：初期のアグリゲーションサービスルータ(ASR)1000モデル（ASR1001に加えてESP5、ESP10、ESP20、およびESP40を搭載）では、CLIで1024のウィンドウサイズが許可されていましたが、サポートされていませんでした。その結果、show crypto ipsec saコマンドの出力で報告されるウィンドウサイズが正しくないことがあります。ハードウェアのアンチリプレイウィンドウのサイズを確認するには、show crypto ipsec sa peer ip-address platformコマンドを使用します。デフォルトのウィンドウ サイズは、すべてのプラットフォームで 64 パケットとなっています。詳細は、Cisco Bug ID CSCso45946 を参照してください。新しいCisco IOS XEルーティングプラットフォーム(ESP100およびESP200を搭載したASR1K、ASR1001-XおよびASR1002-X、Integrated Service Router(ISR)4000シリーズルータ、Catalyst8000シリーズルータなど)は、バージョン15.2(2)S以降で1024パケットのウィンドウサイズをサポートします。

---

2. これは、送信側エンドポイントのQoS設定が原因です。
この状況では、この状態を緩和するために、注意深く調査し、いくつかのQoSを調整する必要があります。このトピックの詳細と、考えられる解決策については、記事『音声ビデオ対応 IPSec VPN（V3PN）でのアンチリプレイの考慮事項』を参照してください。

3. 以前に受信した重複パケットである場合：
この場合、同じIPSecフロー内で同じESPシーケンス番号を持つ2つ以上のパケットがパケットキャプチャで観察される可能性があります。この場合、IPsecリプレイ保護がネットワークでのリプレイ攻撃を防止するように意図したとおりに機能するため、パケットのドロップが予想されます。Syslogは単なる情報です。この状態が続く場合は、潜在的なセキュリティの脅威として調査する必要があります。

注：リプレイチェックの失敗が発生するのは、IPSecトランスフォームセットで認証アルゴリズムが有効になっている場合だけです。このエラーメッセージを抑制するもう1つの方法は、認証を無効にして暗号化のみを実行することです。ただし、認証を無効にするとセキュリティが低下するため、この方法はお勧めできません。

追加情報

Cisco IOS Classicを使用するレガシールータでのリプレイエラーのトラブルシューティング

Cisco IOSを使用するレガシーISR G2シリーズルータでのIPsecリプレイドロップは、次に示すようにCisco IOS XEを使用するルータとは異なります。

```
<#root>

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

connection id=529, sequence number=13
```

メッセージ出力は、ピアのIPアドレスまたはSPI情報を提供しないことに注意してください。このプラットフォームでトラブルシューティングを行うには、エラーメッセージで「conn-id」を使用します。リプレイは（ピアごとではなく）SAごとにチェックされるため、エラーメッセージで「conn-id」を特定し、show crypto ipsec saの出力でそれを探します。SyslogメッセージはESPシーケンス番号も提供します。これは、パケットキャプチャでドロップされたパケットを一意に識別するのに役立ちます。

注：コードのバージョンによって、「conn-id」は着信SAのconn idまたはflow_idになります。

これを以下に示します。

```
<#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>
```

この出力からわかるように、リプレイドロップはピアアドレス10.2.0.200から発生しており、そのインバウンドESP SA SPIは0xE7EDE943です。また、ログメッセージ自体から、ドロップされたパケットのESPシーケンス番号が13であることもわかります。ピアアドレス、SPI番号、およびESPシーケンス番号の組み合わせを使用して、パケットキャプチャでドロップされたパケットを一意に識別できます。

注:Cisco IOS Syslogメッセージは、1分あたり1つにドロップされるデータプレーンパケットに対してレート制限されています。ドロップされたパケットの厳密なカウントを正確に取得するには、前に示したように show crypto ipsec sa detail コマンドを使用します。

以前のCisco IOS XEソフトウェアとの連携

以前のCisco IOS XEリリースを実行するルータでは、次に示すように、Syslogに報告される「REPLAY_ERROR」によって、リプレイされたパケットがドロップされたピア情報を含む実際のIPsecフローが出力されない場合があります。

```
%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
```

正しいIPsecピアとフローの情報を特定するには、Syslogメッセージに出力されたデータプレーン(DP)ハンドルをこのコマンドの入力パラメータSA Handleとして使用し、Quantum Flow Processor(QFP)でIPsecフロー情報を取得します。

```
<#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>
```

Embedded Event Manager(EEM)スクリプトを使用して、データ収集を自動化することもできます。

```
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"
```

この例では、収集された出力はブートフラッシュにリダイレクトされます。この出力を表示するには、more bootflash:replay-error.txtコマンドを使用します。

関連情報

- 音声ビデオ対応 IPSec VPN（V3PN）ソリューション参照ネットワーク設計
- IPSecアンチリプレイウィンドウの設定方法：拡張と無効化」を参照してください。
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。