Verify IPsec %RECVD_PKT_INV_SPI Errors and Invalid SPI Recovery Feature Information

Contents

Introduction

This document describes the IPsec issue when Security Associations (SAs) become out of sync between the peer devices.

Problem

One of the most common IPsec issues is that SAs can become out of sync between the peer devices. As a result, the encryption endpoint encrypts traffic with an SA that it's peer does not know about. These packets are dropped by the peer and this message appears in the syslog:

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0xB761863E(3076621886), srcaddr=10.1.1.1
```

> **Note**: On the Cisco IOS® XE routing platforms, for example, the Cisco Aggregation Services Routers (ASR) and Cisco Catalyst 8000 series routers, this particular drop is registered under both the global Quantum Flow Processor (QFP) drop counter as well as in the IPsec feature drop counter, as shown in the next examples.

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
  IpsecDenyDrop                           0              0
  IpsecIkeIndicate                        0              0
  IpsecInput                              0              0     <======
  IpsecInvalidSa                          0              0
  IpsecOutput                             0              0
  IpsecTailDrop                           0              0
  IpsecTedIndicate                        0              0
```

```
Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
        4  IN_US_V4_PKT_SA_NOT_FOUND_SPI                          64574    <======
        7  IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI                        0
       12  IN_US_V6_PKT_SA_NOT_FOUND_SPI                              0
```

It is important to note that this particular message is rate-limited in Cisco IOS® at a rate of one per minute for the obvious security reasons. If this message for a particular flow (SRC, DST, or SPI) only appears once in the syslog, then it is likely a transient condition that is present at the same time as the IPsec rekey, where one peer can start to use the new SA while the peer device is not quite ready to use the same SA. This is normally not a problem, as it is only temporary and would only affect a few packets.

However, if the same message persists for the same flow and SPI number, then it is indicative the IPsec SAs have gone out of sync between the peers. For example:

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643), srcaddr=10.1.1.1
Sep  2 13:37:48.039: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643), srcaddr=10.1.1.1
```

This is an indication that traffic is black-holed and cannot recover until the SAs expire on the sending device or until the Dead Peer Detection (DPD) is activated.

Solution

This section provides information that you can use in order to resolve the issue that is described in the previous section.

Invalid SPI Recovery

In order to resolve this issue, Cisco recommends that you enable the invalid SPI recovery feature. For example, enter the **crypto isakmp invalid-spi-recovery** command. Here are some important notes that describe the use of this command:

- First, invalid SPI recovery only serves as a recovery mechanism when the SAs are out of sync. It helps recover from this condition, but it does not address the root issue that caused the SAs to become out of sync in the first place. In order to better understand the root cause, you must enable ISAKMP and IPsec debugs on both of the tunnel end points. If the problem occurs often, then obtain the debugs and attempt to address the root cause (and not just mask the problem).

- There is a common misconception about the purpose and functionality of the **crypto isakmp invalid-spi-recovery** command. Even without this command, Cisco IOS already performs a type of invalid SPI recovery functionality when it sends a DELETE notification to the sending peer for the SA that is received if it already has an IKE SA with that peer. Again, this occurs regardless of whether the **crypto isakmp invalid-spi-recovery** command is activated.

- The **crypto isakmp invalid-spi-recovery** command attempts to address the condition where a router receives IPsec traffic with invalid SPI, and it does not have an IKE SA with that peer. In this case, it tries to establish a new IKE session with the peer and sends a DELETE notification over the newly created IKE SA. However, this command does not function for all crypto-configurations. The only configurations that this command works for are static crypto-maps where the peer is explicitly defined and static peers that are derived from instantiated crypto-maps, such as VTI. Here is a summary of the commonly used crypto-configurations and whether invalid SPI recovery works with that configuration:

Crypto-configuration	Invalid SPI Recovery
Static crypto-map	Yes
Dynamic crypto-map	No
P2P GRE with Tunnel Protection	Yes
mGRE Tunnel Protection that uses w/ static NHRP mapping	Yes
mGRE Tunnel Protection that uses w/ dynamic NHRP mapping	No
sVTI	Yes
EzVPN client	N/A

Troubleshoot Intermittent Invalid SPI Error Messages

Many times the invalid SPI error message occurs intermittently. This makes it difficult to troubleshoot, as it becomes very hard to collect the relevant debugs. Embedded Event Manager (EEM) scripts can be very useful in this case.

> **Note**: For more details, refer to the EEM Scripts used to Troubleshoot Tunnel Flaps Caused by Invalid Security Parameter Indexes Cisco document.

Known Bugs

This list shows bugs that can either cause IPsec SAs to go out of sync or are related to Invalid SPI recovery:

- Cisco bug ID CSCvn31824 Cisco IOS XE ISAKMP deletes new SPI if rx new SPI packet before installation is done
- Cisco bug ID CSCvd40554 IKEv2: Cisco IOS cannot parse INV_SPI notification with SPI size 0 - sends INVALID_SYNTAX
- Cisco bug ID CSCvp16730 Incoming ESP packets with SPI value that starts with 0xFF are dropped due to Invalid SPI error