Überprüfen von IPsec %RECVD_PKT_INV_SPI-Fehlern und ungültigen Informationen zu SPI-Wiederherstellungsfunktionen

Inhalt

Einleitung

In diesem Dokument wird das IPsec-Problem beschrieben, wenn Sicherheitszuordnungen (SAs) zwischen den Peer-Geräten nicht mehr synchronisiert sind.

Problem

Eines der häufigsten IPsec-Probleme ist, dass SAs zwischen den Peer-Geräten nicht mehr synchronisiert sind. Daher verschlüsselt ein verschlüsseltes Gerät Datenverkehr mit SAs, über die sein Peer nichts weiß. Diese Pakete werden vom Peer verworfen, und die folgende Meldung wird im Syslog angezeigt:

```
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
```

> **Anmerkung:** Bei NAT-T wurden **RECVD_PKT_INV_SPI-**Meldungen nicht korrekt gemeldet, bis Cisco Bug-ID CSCsq59183 behoben wurde. (IPsec meldet keine **RECVD_PKT_INV_SPI-**Nachrichten mit NAT-T.)

> **Anmerkung:** Auf der Cisco Aggregation Services Router (ASR)-Plattform wurden die Nachrichten **%CRYPTO-4-RECVD_PKT_INV_SPI** erst ab Cisco IOS® XE Version 2.3.2 (12.2(33)XNC2) implementiert. Beachten Sie bei der ASR-Plattform außerdem, dass dieser spezielle Tropfen sowohl unter dem globalen Quantum Flow Processor (QFP)-Tropfenzähler als auch im IPsec-Feature-Tropfenzähler registriert wird, wie in den folgenden Beispielen gezeigt.

```
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
```

Es ist wichtig zu beachten, dass diese spezielle Nachricht in Cisco IOS aus Sicherheitsgründen mit einer Rate von einer pro Minute begrenzt ist. Wenn diese Meldung für einen bestimmten Datenfluss (SRC, DST oder SPI) nur einmal im Protokoll erscheint, kann es sich nur um eine vorübergehende Bedingung handeln, die gleichzeitig mit dem IPsec-Schlüssel vorliegt, bei dem ein Peer mit der Verwendung der neuen SA beginnen kann, während das Peer-Gerät nicht ganz bereit ist, dieselbe SA zu verwenden. Dies ist normalerweise kein Problem, da es nur vorübergehend ist und sich nur auf einige wenige Pakete auswirken würde. Es gibt jedoch Fehler, bei denen dies ein Problem sein kann.

> **Tipp:** Beispiele finden Sie unter Cisco Bug-ID CSCsl68327 (Paketverlust während rekey), Cisco Bug-ID CSCtr14840 (ASR: Paket wird unter bestimmten Bedingungen während Phase 2 rekey verworfen) oder Cisco Bug-ID CSCty30063 (ASR verwendet neue SPI, bevor QM abgeschlossen ist).

Alternativ besteht ein Problem, wenn mehrere Instanzen derselben Nachricht dieselbe SPI für denselben Fluss melden, z. B.:

```
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
```

Dies ist ein Hinweis darauf, dass der Datenverkehr durch einen Black-Holing unterbrochen wird und sich erst wieder erholen kann, wenn die SAs auf dem sendenden Gerät ablaufen oder die Dead Peer Detection (DPD) aktiviert ist.

Lösung

Dieser Abschnitt enthält Informationen, die Sie zur Behebung des im vorherigen Abschnitt beschriebenen Problems verwenden können.

Ungültige SPI-Wiederherstellung

Um dieses Problem zu beheben, empfiehlt Cisco die Aktivierung der ungültigen SPI-Wiederherstellungsfunktion. Geben Sie beispielsweise den Befehl **crypto isakmp invalid-spi-recovery** ein. Im Folgenden finden Sie einige wichtige Hinweise zur Verwendung dieses Befehls:

- Erstens dient eine ungültige SPI-Wiederherstellung nur dann als Wiederherstellungsmechanismus, wenn die SAs nicht synchronisiert sind. Es hilft bei der Wiederherstellung nach diesem Zustand, behandelt jedoch nicht das Problem, das die SAs veranlasst hat, überhaupt nicht mehr synchronisiert zu sein. Um die Ursache besser zu verstehen, müssen Sie ISAKMP- und IPsec-Debugging-Dienste an beiden Tunnelendpunkten

aktivieren. Wenn das Problem häufig auftritt, holen Sie die Fehlerbehebungsschritte ein, und versuchen Sie, die Ursache anzugehen (und nicht nur das Problem zu maskieren).

- Es gibt eine weit verbreitete Fehleinschätzung des Zwecks und der Funktionalität des Befehls **crypto isakmp invalid-spi-recovery**. Selbst ohne diesen Befehl führt Cisco IOS bereits eine Art ungültiger SPI-Wiederherstellungsfunktionalität aus, wenn es eine DELETE-Benachrichtigung an den sendenden Peer für die SA sendet, die empfangen wird, wenn bereits eine IKE SA mit diesem Peer vorhanden ist. Auch dies geschieht unabhängig davon, ob der Befehl **crypto isakmp invalid-spi-recovery** aktiviert ist.

- Der Befehl **crypto isakmp invalid-spi-recovery** versucht, die Bedingung zu beheben, in der ein Router IPsec-Datenverkehr mit einem ungültigen SPI empfängt, und weist keine IKE-SA mit diesem Peer auf. In diesem Fall versucht er, eine neue IKE-Sitzung mit dem Peer herzustellen, und sendet eine DELETE-Benachrichtigung über die neu erstellte IKE SA. Dieser Befehl funktioniert jedoch nicht für alle Krypto-Konfigurationen. Die einzigen Konfigurationen, für die dieser Befehl funktioniert, sind statische Crypto-Maps, bei denen der Peer explizit definiert ist, und statische Peers, die von instanziierten Crypto-Maps, z. B. VTI, abgeleitet sind. Nachfolgend finden Sie eine Zusammenfassung der häufig verwendeten Krypto-Konfigurationen und der Frage, ob eine ungültige SPI-Wiederherstellung mit dieser Konfiguration funktioniert:

Verschlüsselungskonfiguration	Ungültige SPI-Wiederherstellung?
Statische Crypto-Map	Ja
Dynamische Crypto-Map	Nein
P2P GRE mit Tunnelschutz	Ja
mGRE-Tunnelschutz mit statischer NHRP-Zuordnung	Ja
mGRE-Tunnelschutz mit dynamischer NHRP-Zuordnung	Nein
sVTI	Ja
EzVPN-Client	–

Fehlerbehebung: Ungültige SPI-Fehlermeldungen mit Unterbrechungen

Häufig tritt die ungültige SPI-Fehlermeldung unregelmäßig auf. Dies erschwert die Fehlerbehebung, da es sehr schwierig wird, die relevanten Debugs zu sammeln. Embedded Event Manager (EEM)-Skripts können in diesem Fall sehr nützlich sein.

> **Anmerkung:** Weitere Informationen finden Sie im Cisco Dokument EEM Scripts used to Troubleshoot Tunnel Flaps Caused by Invalid Security Parameter Indexes.

Bekannte Bugs

Diese Liste zeigt Fehler, die dazu führen können, dass IPsec-SAs nicht mehr synchronisiert sind oder die mit der ungültigen SPI-Wiederherstellung in Zusammenhang stehen:

- Cisco Bug-ID CSCvn31824 Cisco IOS-XE ISAKMP löscht neuen SPI, wenn rx neues SPI-Paket vor Abschluss der Installation vorhanden ist
- Cisco Bug-ID CSCvd4054 IKEv2: Cisco IOS kann INV_SPI-Benachrichtigung mit SPI-Größe 0 nicht analysieren - sendet INVALID_SYNTAX

- Cisco Bug-ID CSCvp16730 Eingehende ESP-Pakete mit SPI-Wert, die mit 0xFF beginnen, werden aufgrund eines ungültigen SPI-Fehlers verworfen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.