Controleer IPsec %RECVD_PKT_INV_SPI-fouten en ongeldige informatie over SPI-herstel

Inhoud

Inleiding

Dit document beschrijft de kwestie IPsec wanneer Security Associations (SA's) niet meer synchroon lopen tussen de peer-apparaten.

Probleem

Een van de meest voorkomende problemen met IPsec is dat SA's niet meer kunnen synchroniseren tussen de peer-apparaten. Dientengevolge, versleutelt een versleuteld apparaat verkeer met SA's waarvan zijn peer niet op de hoogte is. Deze pakketten worden door de peer laten vallen en dit bericht verschijnt in 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
```

> **Opmerking:** Met NAT-T werden **RECVD_PKT_INV_SPI-**berichten niet correct gemeld tot Cisco bug-id CSC59183 was hersteld. (IPsec rapporteert geen **RECVD_PKT_INV_SPI-**berichten met NAT-T.)

> **Opmerking:** Op het Cisco Aggregation Services Routers (ASR) platform zijn de **%CRYPTO-4-RECVD_PKT_INV_SPI-**berichten niet geïmplementeerd tot Cisco IOS® XE release 2.3.2 (12.2(33)XNC2). Let ook met het ASR-platform op dat deze bepaalde val wordt geregistreerd onder zowel de wereldwijde QFP-drop-teller (Quantum Flow Processor) als in de IPsec-functie drop-teller, zoals in de volgende voorbeelden wordt getoond.

```
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
```

Het is belangrijk om op te merken dat dit bepaalde bericht in Cisco IOS aan een tarief van één per minuut om de duidelijke veiligheidsredenen is beperkt. Als dit bericht voor een bepaalde stroom (SRC, DST, of SPI) slechts eenmaal in het logboek verschijnt, dan kan het slechts een voorbijgaande voorwaarde zijn die op hetzelfde ogenblik als de sleutel van IPsec aanwezig is waar één peer kan beginnen om nieuwe SA te gebruiken terwijl het peer apparaat niet vrij klaar is om zelfde SA te gebruiken. Normaal gesproken is dit geen probleem, omdat het slechts van tijdelijke aard is en slechts een paar pakketten zou treffen. Er zijn echter insecten geweest waar dit een probleem kan zijn.

> **Tip**: Raadpleeg bijvoorbeeld Cisco bug-id CSCsl68327 (pakketverlies tijdens sleutel), Cisco bug-id CSCtr14840 (ASR: pakketdalingen tijdens fase 2 (opnieuw instellen onder bepaalde voorwaarden) of Cisco-fout-id CSC30063 (ASR gebruikt nieuwe SPI voordat QM is voltooid).

Als alternatief is er een probleem als meer dan één instantie van hetzelfde bericht wordt waargenomen om hetzelfde SPI voor dezelfde stroom te melden, zoals deze berichten:

```
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
```

Dit is een indicatie dat verkeer zwart-holed is en niet kan herstellen tot de SA's verlopen op het apparaat dat verstuurt of tot de Dead Peer Detection (DPD) is geactiveerd.

Oplossing

Dit gedeelte bevat informatie die u kunt gebruiken om het probleem op te lossen dat in het vorige gedeelte wordt beschreven.

Ongeldig SPI-herstel

Om dit probleem op te lossen, raadt Cisco u aan de ongeldige SPI-herstelfunctie in te schakelen. Voer bijvoorbeeld de opdracht **crypto isakmp Invalid-spi-recovery in**. Hier zijn enkele belangrijke opmerkingen die het gebruik van deze opdracht beschrijven:

- Ten eerste, ongeldig SPI-herstel fungeert alleen als een herstelmechanisme wanneer de SA's niet synchroon zijn. Het helpt herstellen van deze conditie, maar het lost niet de wortelkwestie op die de SAs om uit synchronisatie in de eerste plaats veroorzaakte. Om de basisoorzaak beter te begrijpen, moet u de debuggen van ISAKMP en IPsec op beide tunneleindpunten inschakelen. Als het probleem vaak voorkomt, dan verkrijg debugs en probeer om de worteloorzaak (en niet alleen maskeren het probleem) aan te pakken.

- Er is een algemene misvatting over het doel en de functionaliteit van de **crypto isakmp ongeldige-spi-recovery** opdracht. Zelfs zonder deze opdracht voert Cisco IOS al een type

ongeldige SPI-herstelfunctionaliteit uit wanneer er een Delete-melding wordt verzonden naar de verzendende peer voor de SA die wordt ontvangen als er al een IKE SA met die peer is. Opnieuw, komt dit ongeacht voor of de **crypto isakmp ongeldig-spi-recovery** opdracht wordt geactiveerd.

- De opdracht **crypto isakmp Invalid-spi-recovery** probeert de voorwaarde aan te pakken waar een router IPsec-verkeer ontvangt met ongeldige SPI, en het heeft geen IKE SA met die peer. In dit geval, probeert het om een nieuwe IKE-sessie met de peer op te zetten en verstuurt een Delete-melding via de nieuw gemaakte IKE SA. Deze opdracht werkt echter niet voor alle cryptoconfiguraties. De enige configuraties waarvoor dit commando werkt zijn statische crypto-kaarten waar de peer expliciet is gedefinieerd en statische peers die zijn afgeleid van geconcretiseerde crypto-kaarten, zoals VTI. Hier is een samenvatting van de algemeen gebruikte crypto-configuraties en of de ongeldige terugwinning van SPI met die configuratie werkt:

Crypto-configuratie	Ongeldig SPI herstel?
Statische cryptokaart	Ja
Dynamische crypto-kaart	Nee
P2P GRE met tunnelbescherming	Ja
mGRE Tunnelbescherming die gebruik maakt van statische NHRP-mapping	Ja
mGRE Tunnelbescherming die gebruik maakt van w/dynamic NHRP mapping	Nee
sVTI	Ja
EzVPN-client	N.v.t.

Intermitterende ongeldige SPI-foutmeldingen oplossen

Vaak komt de ongeldige SPI-foutmelding met tussenpozen voor. Dit maakt het moeilijk om problemen op te lossen, aangezien het zeer moeilijk wordt om relevante debugs te verzamelen. Embedded Event Manager (EEM) scripts kunnen in dit geval erg nuttig zijn.

> **Opmerking:** Raadpleeg voor meer informatie de EEM-scripts die worden gebruikt om tunnelflaps op te lossen die worden veroorzaakt door ongeldige Cisco-documenten van Security Parameter Indexes.

Bekende insecten

Deze lijst toont insecten die of IPsec SAs kunnen veroorzaken om uit synchronisatie te gaan of verwant aan Ongeldig SPI herstel:

- Cisco bug-id CSCvn31824 Cisco IOS-XE ISAKMP verwijdert nieuwe SPI als rx nieuw SPI-pakket voordat de installatie is voltooid
- Cisco bug-id CSC40554 IKEv2: Cisco IOS kan INV_SPI-melding niet parseren met SPI-grootte 0 - verstuurt ONGELDIGE_SYNTAX
- Cisco bug-id CSCvp16730 inkomende ESP-pakketten met SPI-waarde die begint met 0xFF worden verwijderd vanwege ongeldige SPI-fout

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.