

# EEM-scripts die gebruikt worden om tunneltoewijzingen te probleemoplossing te bieden die gebruikt worden door ongeldige security parameter-indexen

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Probleem](#)

[Oplossing](#)

[SNMP-configuratie](#)

[Eindscripts](#)

[Vastlegging EEM-scripts](#)

[Verificatie](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document beschrijft een van de meest voorkomende IPsec-problemen, namelijk dat Security Associations (SA's) mogelijk niet sync tussen de peer-apparaten kunnen worden. Als resultaat hiervan zal een encryptie-apparaat verkeer met SAs versleutelen waarvan de peer-encryptor niet weet.

## [Voorwaarden](#)

### [Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

### [Gebruikte componenten](#)

Deze informatie in dit document is gebaseerd op tests die met Cisco IOS® release 15.1(4)M4 zijn voltooid. De scripts en configuratie zouden ook met eerdere Cisco IOS-softwareversies moeten werken, omdat beide applets Embedded Event Manager (EEM) versie 3.0 gebruiken die wordt ondersteund in Cisco IOS release 12.4(22)T of hoger. Dit is echter niet getest.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## Probleem

De pakketten worden op de peer gedropt terwijl dit bericht aan de syslog is geregistreerd:

```
*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
  has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
  srcaddr=11.1.1.3, input interface=Ethernet0/0
```

Raadpleeg voor gedetailleerde informatie over ongeldige veiligheidsparameter-indexen (SPI's) [fouten en ongeldig SPI-herstel bij IPsec %RECVD\\_PKT\\_INV\\_SPI](#). Dit document beschrijft hoe u scenario's voor een probleemoplossing kunt bedenken waarin de fout met tussenpozen optreedt. Dit maakt het moeilijk om de benodigde gegevens te verzamelen voor het oplossen van problemen.

Dit type probleem is niet zoals de normale probleemoplossing in VPN, waar u de problemen kunt oplossen wanneer het probleem zich voordoet. Om de intermitterende tunnelflaps van de oplossing door ongeldige SPI's te kunnen oplossen, moet u eerst bepalen hoe de twee head-ends uit sync zijn geraakt. Omdat het onmogelijk is om te voorspellen wanneer de volgende eindjes zullen voorkomen, zijn EEM scripts de oplossing.

## Oplossing

Aangezien het belangrijk is te weten wat er gebeurt voordat dit syslog-bericht wordt geactiveerd, kunt u de voorwaardelijke signalen op de router(en) blijven uitvoeren en ze naar een syslog-server sturen zodat ze het productieverkeer niet beïnvloeden. Als debugs in het script ingeschakeld zijn, worden ze gegenereerd nadat het syslogbericht is geactiveerd en mogelijk is dit niet handig. Hier is een lijst van ontdekkingen die je op de zender van dit logbestand en de ontvanger kunt uitvoeren:

```
debug crypto condition peer ipv4 <peer IP address> debug crypto isakmp debug crypto ipsec debug
crypto engine
```

Het EEM-script is ontworpen om twee dingen te doen:

1. Schakel de stoppen op de ontvanger uit als ze 18 seconden worden verzameld nadat het eerste syslog bericht is gegenereerd. De vertragingstimer moet mogelijk worden gewijzigd, wat afhankelijk is van de hoeveelheid uitwerpselen/logboeken die worden gegenereerd.
2. Op hetzelfde moment schakelt het de debugs uit, laat het een SNMP-val naar de peer sturen, die dan de debugs op het peer-apparaat blokkeert.

## SNMP-configuratie

De formaties Simple Network Management Protocol (SNMP) worden hier weergegeven:

Receiver:

=====

```
snmp-server enable traps event-manager
snmp-server host 11.1.1.3 public event-manager
snmp-server manager
```

Sender:

=====

```
snmp-server enable traps event-manager
snmp-server host 213.163.222.7 public event-manager
snmp-server manager
```

## Eindscripts

De geschriften voor de ontvanger en de afzender worden hier getoond:

Receiver:

=====

```
!--- To test if this output gets logged to the file called "hub" sh ip int bri | tee /append
disk0:hub.txt conf t ! event manager applet command_hub event syslog pattern "CRYPTO-4-
RECVD_PKT_INV_SPI.*srcaddr=11.1.1.3" action 1 cli command "enable" action 2 syslog msg
"command_hub is running ..." priority informational action 3 cli command "show crypto sockets |
append disk0:hub.txt" action 4 cli command "show crypto isa sa | append disk0:hub.txt" action 5
cli command "show crypto ipsec sa detail | append disk0:hub.txt" action 6 cli command "show
dmvpn detail | append disk0:hub.txt" action 7 wait 18 action 8 cli command "undebg all" action
8.1 snmp-trap intdata1 2323232 strdata "" action 9 syslog priority informational msg "DONE ON
HUB" ! end
```

Sender:

=====

```
conf t
!
event manager applet spoke_app
  event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.1.2.3.1.9.
    oid-val "2323232" op eq src-ip-address 213.163.222.7 maxrun 35
  action 1.0 syslog msg "Received trap from Hub..."
  action 2.0 cli command "enable"
  action 3.0 cli command "undebg all"
  action 4.0 syslog msg "DONE ON SPOKE"
!
```

## Vastlegging EEM-scripts

Hieronder vindt u een lijst van EEM-scripts met logberichten:

Receiver:

=====

```
*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
  has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
  srcaddr=11.1.1.3, input interface=Ethernet0/0
*Mar 12 18:22:10.727: %HA_EM-6-LOG: command_hub: command_hub is running ...
hub#
*Mar 12 18:22:30.026: %HA_EM-6-LOG: command_hub: DONE ON HUB
```

```
Sender:
=====
```

```
spoke#
*Mar 12 18:22:30.542: %HA_EM-6-LOG: spoke_app: Received trap from Hub...
*Mar 12 18:22:30.889: %HA_EM-6-LOG: spoke_app: DONE ON SPOKE
```

## Verificatie

Om het probleem te verifiëren is opgelost, voer de **show debug** opdracht in.

```
Receiver:
=====
hub# show debug
```

```
Sender:
=====
spoke# show debug
```

## Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)