EEM Scripts used to Troubleshoot Tunnel Flaps Caused by Invalid Security Parameter Indexes

TAC **Document ID: 116005**

Contributed by Anu M Chacko, Cisco TAC Engineer.
Mar 20, 2013

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Problem
Solution
SNMP Configuration
Final Script
EEM Script Logs
Verification
Related Information

Introduction

This document describes one of the most common IPsec issues, which is that Security Associations (SAs) can become out of sync between the peer devices. As a result, an encrypting device will encrypt traffic with SAs that the peer encryptor does not know about.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This information in this document is based on tests completed with Cisco IOS® Release 15.1(4)M4. The scripts and configuration should work with earlier Cisco IOS software versions as well, since both applets use Embedded Event Manager (EEM) version 3.0 which is supported in Cisco IOS Release 12.4(22)T or later. However, this has not been tested.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem

Packets are dropped on the peer with this message logged to the syslog:

```
*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
```

For detailed information on invalid Security Parameter Indexes (SPIs), refer to IPSec %RECVD_PKT_INV_SPI Errors and Invalid SPI Recovery. This document describes how to troubleshoot scenarios in which the error occurs intermittently, which makes it hard to collect the necessary data to troubleshoot.

This type of problem is not like normal VPN troubleshooting, where you can obtain the debugs when the problem occurs. In order to troubleshoot intermittent tunnel flaps caused by invalid SPIs, you must first determine how the two headends got out of sync. Since it is impossible to predict when the next outage will occur, EEM scripts are the solution.

Solution

Since it is important to know what happens before this syslog message is triggered, continue to run the conditional debugs on the router(s) and send them to a syslog server so that it does not affect the production traffic. If debugs are enabled in the script instead, they are generated after the syslog message is triggered which may not be useful. Here is a list of debugs that you might want to run on the sender of this log and the receiver:

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

The EEM script is designed to do two things:

1. Turn off the debugs on the receiver when they are collected for 18 seconds after the first syslog message is generated. The delay timer might need to be modified, which is dependent upon the amount of debugs/logs generated.
2. At the same time it disables the debugs, have it send an SNMP trap to the peer, which then disables the debugs on the peer device.

SNMP Configuration

The Simple Network Management Protocol (SNMP) configurations are shown here:

```
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
```

Final Script

Scripts for the receiver and sender are shown here:

```
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 "undebug 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 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
    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 "undebug all"
 action 4.0 syslog msg "DONE ON SPOKE"
!
end
```

EEM Script Logs

A list of EEM script log messages is shown here:

```
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
```

Verification

In order to verify the problem has been resolved, enter the **show debug** command.

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


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

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 20, 2013 Document ID: 116005