Scripts EEM utilisés pour dépanner les volets de tunnel provoqués par des index de paramètres de sécurité non valides

Contenu

Introduction

Ce document décrit l'un des problèmes IPsec les plus courants, à savoir que les associations de sécurité (SA) peuvent devenir désynchronisées entre les périphériques homologues. Par conséquent, un périphérique de chiffrement chiffrera le trafic avec des SA dont le crypteur homologue ne connaît pas la nature.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ces informations dans ce document sont basées sur des tests effectués avec Cisco IOS® version 15.1(4)M4. Les scripts et la configuration doivent également fonctionner avec les versions antérieures du logiciel Cisco IOS, car les deux applets utilisent la version 3.0 de Embedded Event Manager (EEM), qui est prise en charge dans Cisco IOS version 12.4(22)T ou ultérieure. Cependant, cela n'a pas été testé.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Problème

Les paquets sont abandonnés sur l'homologue avec ce message consigné dans le 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
```

Pour plus d'informations sur les index de paramètres de sécurité (SPI) non valides, référez-vous à Erreurs IPSec %RECVD_PKT_INV_SPI et Récupération SPI non valide. Ce document décrit comment dépanner les scénarios dans lesquels l'erreur se produit de façon intermittente, ce qui rend difficile la collecte des données nécessaires au dépannage.

Ce type de problème n'est pas comme un dépannage VPN normal, où vous pouvez obtenir les débogages quand le problème se produit. Afin de dépanner les pannes de tunnel intermittentes causées par des SPI non valides, vous devez d'abord déterminer comment les deux têtes de réseau sont devenues désynchronisées. Comme il est impossible de prédire quand la prochaine panne se produira, les scripts EEM sont la solution.

Solution

Comme il est important de savoir ce qui se passe avant le déclenchement de ce message syslog, continuez à exécuter les débogages conditionnels sur le ou les routeurs et envoyez-les à un serveur syslog afin qu'il n'affecte pas le trafic de production. Si les débogages sont activés dans le script à la place, ils sont générés après le déclenchement du message syslog qui peut ne pas être utile. Voici une liste de débogages que vous pouvez exécuter sur l'expéditeur de ce journal et le destinataire :

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

Le script EEM est conçu pour effectuer deux opérations :

1. Désactivez les débogages sur le récepteur lorsqu'ils sont collectés pendant 18 secondes après la génération du premier message syslog. Le temporisateur de délai doit peut-être être modifié, ce qui dépend du nombre de débogages/journaux générés.
2. En même temps, il désactive les débogages et envoie un déroutement SNMP à l'homologue, qui désactive ensuite les débogages sur le périphérique homologue.

Configuration SNMP

Les configurations SNMP (Simple Network Management Protocol) sont présentées ici :

```
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
```

Script final

Les scripts du destinataire et de l'expéditeur sont affichés ici :

```
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
```

Journaux de script EEM

La liste des messages du journal de script EEM est affichée ici :

```
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
```

Vérification

Afin de vérifier que le problème a été résolu, entrez la commande **show debug**.

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


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

Informations connexes

- Support et documentation techniques - Cisco Systems