Scripts EEM usados para solucionar problemas de flaps de túnel causados por índices de parâmetro de segurança inválidos

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Problema](#)
[Solução](#)
[Configuração SNMP](#)
[Script final](#)
[Logs de script EEM](#)
[Verificação](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve um dos problemas mais comuns do IPsec, que é que as associações de segurança (SAs) podem ficar fora de sincronia entre os dispositivos correspondentes. Como resultado, um dispositivo de criptografia criptografará o tráfego com SAs que o criptografador de peer não conhece.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Essas informações neste documento são baseadas em testes concluídos com o Cisco IOS® versão 15.1(4)M4. Os scripts e a configuração também devem funcionar com versões anteriores do software Cisco IOS, já que ambos os miniaplicativos usam o Embedded Event Manager (EEM) versão 3.0 que é compatível com o Cisco IOS versão 12.4(22)T ou posterior. No entanto, isso não foi testado.

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Problema

Os pacotes são descartados no peer com esta mensagem registrada no 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
```

Para obter informações detalhadas sobre Índices de Parâmetros de Segurança (SPIs) inválidos, consulte Erros de IPSec %RECVD_PKT_INV_SPI e Recuperação de SPI Inválida. Este documento descreve como solucionar problemas em cenários em que o erro ocorre intermitentemente, o que dificulta a coleta dos dados necessários para a solução de problemas.

Esse tipo de problema não é como a solução de problemas de VPN normal, na qual você pode obter as depurações quando o problema ocorrer. Para solucionar problemas de flaps intermitentes de túnel causados por SPIs inválidos, primeiro é necessário determinar como os dois headends ficaram dessincronizados. Como é impossível prever quando a próxima interrupção ocorrerá, os scripts de EEM são a solução.

Solução

Como é importante saber o que acontece antes que essa mensagem de syslog seja disparada, continue a executar as depurações condicionais no(s) roteador(es) e envie-as para um Servidor syslog para que não afete o tráfego de produção. Se, em vez disso, as depurações estiverem ativadas no script, elas serão geradas depois que a mensagem syslog for disparada, o que pode não ser útil. Aqui está uma lista de depurações que você pode querer executar no remetente deste log e no receptor:

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

O script EEM foi projetado para fazer duas coisas:

1. Desative as depurações no receptor quando elas forem coletadas por 18 segundos após a geração da primeira mensagem do syslog. O temporizador de atraso pode precisar ser modificado, o que depende da quantidade de depurações/logs gerados.
2. Ao mesmo tempo, desabilita as depurações, faça com que ele envie uma interceptação SNMP ao peer, que desabilita as depurações no dispositivo peer.

Configuração SNMP

As configurações do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) são mostradas aqui:

```
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

Os scripts do receptor e do remetente são mostrados aqui:

```
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
```

Logs de script EEM

Uma lista de mensagens de log de script do EEM é mostrada aqui:

```
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
```

Verificação

Para verificar se o problema foi resolvido, digite o comando **show debug**.

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


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

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems