Script EEM utilizzati per risolvere i problemi di flap del tunnel causati da indici di parametri di sicurezza non validi

Sommario

Introduzione

Questo documento descrive uno dei problemi IPsec più comuni, ovvero che le associazioni di sicurezza (SA) possono non essere più sincronizzate tra i dispositivi peer. Di conseguenza, un dispositivo di crittografia crittograferà il traffico con le associazioni di protezione di cui il peer non è a conoscenza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sui test eseguiti con Cisco IOS® versione 15.1(4)M4. Gli script e la configurazione devono essere compatibili anche con le versioni precedenti del software Cisco IOS, in quanto entrambe le applet utilizzano Embedded Event Manager (EEM) versione 3.0, supportata in Cisco IOS versione 12.4(22)T o successive. Tuttavia, questo non è stato testato.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

I pacchetti vengono scartati sul peer con questo messaggio registrato nel 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
```

Per informazioni dettagliate sugli SPI (Security Parameter Indexes) non validi, fare riferimento agli errori IPSec %RECVD_PKT_INV_SPI e al recupero SPI non valido. In questo documento viene descritto come risolvere i problemi relativi a scenari in cui l'errore si verifica in modo intermittente, rendendo difficile la raccolta dei dati necessari per la risoluzione dei problemi.

Questo tipo di problema non è come la normale risoluzione dei problemi VPN, in cui è possibile ottenere i debug quando si verifica il problema. Per risolvere i problemi di flap del tunnel intermittenti causati da SPI non validi, è necessario prima determinare in che modo i due headend non sono stati sincronizzati. Poiché è impossibile prevedere quando si verificherà il prossimo guasto, gli script EEM rappresentano la soluzione.

Soluzione

Poiché è importante sapere cosa succede prima che venga attivato questo messaggio syslog, continuare a eseguire i debug condizionali sui router e inviarli a un server syslog in modo che non influisca sul traffico di produzione. Se invece nello script sono abilitati i debug, vengono generati dopo l'attivazione del messaggio syslog che potrebbe non essere utile. Di seguito è riportato un elenco di debug che è possibile eseguire sul mittente di questo registro e sul destinatario:

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

Lo script EEM è progettato per eseguire due operazioni:

1. Spegnere i debug sul ricevitore quando vengono raccolti per 18 secondi dopo la generazione del primo messaggio syslog. Potrebbe essere necessario modificare il timer di ritardo, che dipende dalla quantità di debug/log generati.
2. Allo stesso tempo disattiva i debug, fa in modo che invii una trap SNMP al peer, che quindi disattiva i debug sul dispositivo peer.

Configurazione SNMP

Di seguito sono illustrate le configurazioni del protocollo SNMP (Simple Network Management Protocol):

```
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 finale

Di seguito sono riportati gli script per il destinatario e il mittente:

```
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
```

Log script EEM

Di seguito è riportato un elenco di messaggi di log di script EEM:

```
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
```

Verifica

Per verificare che il problema sia stato risolto, immettere il comando **show debug**.

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


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

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems