EEM-Skripte zur Fehlerbehebung bei Tunnelzugriffen, die durch ungültige Sicherheitsparameterindizes verursacht werden

Inhalt

Einführung

Dieses Dokument beschreibt eines der häufigsten IPsec-Probleme, nämlich dass Sicherheitszuordnungen (SAs) nicht synchronisiert zwischen den Peer-Geräten werden können. Das Ergebnis ist, dass ein Verschlüsselungsgerät Datenverkehr mit SAs verschlüsselt, von denen der Peer-Verschlüsseler nichts weiß.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Diese Informationen in diesem Dokument basieren auf Tests, die mit Cisco IOS® Version 15.1(4)M4 abgeschlossen wurden. Die Skripts und die Konfiguration sollten auch mit früheren Cisco IOS-Softwareversionen funktionieren, da beide Applets den Embedded Event Manager (EEM) Version 3.0 verwenden, der von Cisco IOS Release 12.4(22)T oder höher unterstützt wird. Dies wurde jedoch nicht getestet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Problem

Pakete werden auf dem Peer verworfen, wobei diese Meldung im Syslog protokolliert wird:

```
*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
```

Detaillierte Informationen zu ungültigen Security Parameter Indexes (SPIs) finden Sie unter IPSec %RECVD_PKT_INV_SPI Errors und Invalid SPI Recovery. In diesem Dokument wird beschrieben, wie Sie in Szenarien, in denen der Fehler periodisch auftritt, eine Fehlerbehebung durchführen. Dadurch wird es schwierig, die zur Fehlerbehebung erforderlichen Daten zu erfassen.

Diese Art von Problem ist nicht vergleichbar mit der normalen VPN-Fehlerbehebung, bei der Sie die Fehlerbehebung abrufen können, wenn das Problem auftritt. Um zeitweise auftretende Tunnelklappen, die durch ungültige SPIs verursacht wurden, zu beheben, müssen Sie zunächst ermitteln, wie die beiden Headends nicht synchronisiert wurden. Da es nicht möglich ist, vorherzusagen, wann der nächste Ausfall eintritt, sind EEM-Skripte die Lösung.

Lösung

Da es wichtig ist, zu wissen, was vor der Auslösung dieser Syslog-Meldung geschieht, führen Sie die bedingten Debugging-Vorgänge auf den Routern aus, und senden Sie sie an einen Syslog-Server, damit sich dies nicht auf den Produktionsdatenverkehr auswirkt. Wenn stattdessen Debugger im Skript aktiviert sind, werden sie generiert, nachdem die Syslog-Meldung ausgelöst wurde, was möglicherweise nicht sinnvoll ist. Im Folgenden finden Sie eine Liste von Debuggen, die Sie möglicherweise auf dem Absender dieses Protokolls und dem Empfänger ausführen möchten:

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

Das EEM-Skript ist für zwei Aufgaben konzipiert:

1. Schalten Sie die Debugger auf dem Receiver aus, wenn sie 18 Sekunden lang gesammelt werden, nachdem die erste Syslog-Meldung generiert wurde. Möglicherweise muss der Verzögerungszeitgeber geändert werden. Dies hängt von der Menge der generierten Debug-/Protokolldateien ab.
2. Gleichzeitig wird das Debuggen deaktiviert. Lassen Sie es einen SNMP-Trap an den Peer senden, der dann die Debug auf dem Peer-Gerät deaktiviert.

SNMP-Konfiguration

Die SNMP-Konfigurationen (Simple Network Management Protocol) werden hier angezeigt:

```
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
```

Letztes Skript

Skripte für Empfänger und Absender werden hier angezeigt:

```
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-Skriptprotokolle

Eine Liste der EEM-Skript-Protokollmeldungen wird hier angezeigt:

```
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
```

Überprüfung

Um zu überprüfen, ob das Problem behoben wurde, geben Sie den Befehl **show debug ein**.

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


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

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems