Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Problème](#)
[Solution](#)
[Configuration SNMP](#)
[Script final](#)
[Logs de script EEM](#)
[Vérification](#)
[Informations connexes](#)

Introduction

Ce document décrit une des questions d'IPsec les plus communes, qui est que les associations de sécurité (SAS) peuvent devenir hors du sync entre les périphériques de pair. En conséquence, un périphérique chiffrant chiffrera le trafic avec SAS que l'unité de chiffrement de pair ne connaît pas.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ces informations dans ce document sont basées sur des tests terminés avec la release 15.1(4)M4 de Cisco IOS®. Les scripts et la configuration devraient fonctionner avec des versions de logiciel plus tôt de Cisco IOS aussi bien, puisque l'utilisation de les deux applet a inclus la version 3.0 du gestionnaire d'événement (EEM) qui est prise en charge dans la Cisco IOS version 12.4(22)T ou ultérieures. Cependant, ceci n'a pas été testé.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Problème

Des paquets sont lâchés sur le pair avec ce message connecté au Syslog :

Pour des informations détaillées sur les index non valides de paramètre de Sécurité (SPI), référez-vous aux erreurs d'IPSec %RECVD_PKT_INV_SPI et à la reprise non valide SPI. Ce document décrit comment dépanner les scénarios dans lesquels l'erreur se produit par intermittence, qui le rend dur pour collecter les données nécessaires pour dépanner.

Ce type de problème n'est pas comme le dépannage VPN normal, où vous pouvez obtenir met au point quand le problème se pose. Afin de dépanner les instabilités intermittentes de tunnel provoquées par des SPI non valides, vous devez d'abord déterminer comment les deux headends sont sortis du sync. Puisqu'il est impossible à prévoir quand la prochaine panne se produira, les scripts EEM sont la solution.

Solution

Puisqu'il est important de savoir ce qui se produit avant que ce message de Syslog soit déclenché, continuez à exécuter le conditionnel met au point sur les routeurs et les envoie à un serveur de Syslog de sorte qu'il n'affecte pas le trafic de production. Si met au point sont activés dans le script à la place, ils sont générés après que le message de Syslog soit déclenché qui peut ne pas être utile. Voici une liste de met au point que vous pourriez vouloir s'exécuter sur l'expéditeur de ce log et le récepteur :

Le script EEM est conçu pour faire deux choses :

1. Arrêtez met au point sur le récepteur quand ils sont collectés pour 18 secondes après que le premier message de Syslog est généré. Le temporisateur de délai pourrait dont devoir être modifié, dépend de la quantité met au point/logs générés.
2. En même temps il désactive le met au point, fait envoyer un déroutement SNMP au pair, qui désactive alors met au point sur le périphérique de pair.

Configuration SNMP

Les configurations de Protocole SNMP (Simple Network Management Protocol) sont affichées ici :

Script final

Des scripts pour le récepteur et l'expéditeur sont affichés ici :

Logs de script EEM

Une liste de messages de log de script EEM est affichée ici :

Vérification

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

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

Informations connexes

- Support et documentation techniques - Cisco Systems