FireSIGHT peut identifier un hôte de manière incorrecte ou marquer un événement comme étant en attente ou inconnu

Table des matières

Introduction

Un système FireSIGHT génère des événements lorsqu'il détecte un nouvel hôte sur votre segment de réseau surveillé.Il peut détecter un système d'exploitation ou un service de manière incorrecte ou avec moins de confiance. Si un événement est marqué comme *Inconnu*, cela signifie que le trafic est analysé, mais les systèmes d'exploitation ne correspondent à aucune des empreintes connues. Ce document fournit une liste de contrôle et des recommandations pour réduire les événements *inconnus*.

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Système FireSIGHT, appliances FirePOWER et appliances virtuelles NGIPS
- Version de logiciel 5.0 ou ultérieure

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.

Listes de contrôle de dépannage

Si votre système FireSIGHT génère des événements en attente ou dans un état inconnu, vous

pouvez suivre les étapes ci-dessous pour commencer à résoudre ce problème :

> **Note**: *Les* hôtes *non identifiés* ne sont pas identiques aux hôtes *inconnus*. *Les* hôtes *non identifiés* sont des hôtes sur lesquels un système n'a pas encore recueilli suffisamment d'informations pour identifier leurs systèmes d'exploitation.

Liste de vérification	Recommandations
1. Quelle version de VDB est installée sur FireSIGHT Management Center ?	La dernière version de VDB contient plus d'informations sur les empreintes digitales. Il est toujours recommandé d'installer la dernière version sur FireSIGHT Management Center.
2. Quelle est la limite d'hôte de votre licence FireSIGHT ? Combien d'hôtes ont été détectés par FireSIGHT ?	Si la limite d'hôtes est dépassée, un système FireSIGHT élague les données les plus anciennes au fur et à mesure de leur arrivée. Vous pouvez configurer la stratégie système pour supprimer de nouveaux hôtes lorsque la limite d'hôtes est atteinte.
3. Combien de sauts séparent les hôtes du périphérique géré FireSIGHT ?	Plus le nombre de sauts entre les hôtes et un périphérique géré est élevé, plus l'hôte est éloigné du périphérique, ce qui augmente la probabilité que le trafic ait été modifié et ne permette pas une identification précise.
4. Existe-t-il des périphériques en ligne entre les hôtes et le périphérique géré ?	la présence de tout dispositif en ligne; tels que le pare-feu, le périphérique NAT, l'équilibreur de charge et le serveur proxy peuvent modifier les informations d'en-tête TCP ou IP d'origine qui peuvent également être les causes d'une collecte d'informations mal identifiées ou non identifiées à partir des hôtes.
5. Les périphériques gérés surveillent-ils le trafic dans un réseau de routage asynchrone ?	Si un système FireSIGHT surveille le trafic de routage asynchrone, il peut ne pas être en mesure de voir la session complète.
6. Des ports non standard sont-ils utilisés pour des services ? Existe-t-il des décodeurs personnalisés configurés pour gérer les ports non standard ?	Un décodeur personnalisé mal configuré peut entrer en conflit avec les décodeurs par défaut.

Données supplémentaires

Si toutes les recommandations ci-dessus sont suivies, mais qu'il existe toujours des hôtes inconnus, en attente ou non identifiés, nous devrons alors analyser les données suivantes :

1. Trafic de session complète

Trafic de session complet en provenance des hôtes qui sont identifiés de manière incorrecte ou marqués comme inconnus ou en attente.

2. Fichiers de dépannage

Dépannage des fichiers à partir de FireSIGHT Management Center et du périphérique géré. La carte réseau ou la topologie indiquant l'emplacement du périphérique géré serait utile.

3. Capture de paquets (PCAP)

Les paquets reçus par le périphérique géré peuvent être différents des paquets provenant des hôtes. Il se produit si un périphérique en ligne modifiant l'en-tête existe entre les hôtes et le périphérique géré. Par conséquent, il est préférable de capturer le PCAP des deux extrémités (hôtes et périphériques gérés), ce qui permet de comparer les en-têtes des deux PCAP. Toute non-correspondance entre les paquets peut entraîner une mauvaise identification des services ou des hôtes.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.