Contenu

Introduction

Un système de FireSIGHT génère des événements quand il détecte un nouvel hôte sur votre segment surveillé de réseau. Il peut détecter un système d'exploitation ou un service inexactement, ou avec moins de confiance. Si un événement est marqué comme *inconnu*, il signifie que le trafic est analysé, mais les systèmes d'exploitation n'apparient pas les empreintes digital connues l'unes des. Ce document fournit une liste de contrôle et des recommandations de réduire des événements *inconnus*.

Conditions préalables

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

- Système de FireSIGHT, appliances de puissance de feu, et appliances virtuelles NGIPS
- Version de logiciel 5.2 ou plus tard

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.

Listes de contrôle de dépannage

Si votre système de FireSIGHT génère les événements qui sont dans l'état en suspens ou dans inconnu, vous pouvez suivre les étapes ci-dessous pour commencer dépanner cette question :

> Remarque: Les hôtes *non identifiés* ne sont pas identiques que des *hôtes inconnus*. Les hôtes *non identifiés* sont des hôtes au sujet dont un système n'a pas encore recueilli assez d'informations pour identifier leurs systèmes d'exploitation.

Dépannez la liste de contrôle	Recommandations
1. Quelle version VDB est installée au centre de Gestion de FireSIGHT ?	La dernière version VDB a plus d'informations d'empreinte digital. toujours recommandé pour avoir la dernière version installée au ce de Gestion de FireSIGHT.
2. Quelle est la limite d'hôte de votre permis de FireSIGHT ? Combien d'hôtes ont été détectés par FireSIGHT ?	Si la limite d'hôte dépasse, un système de FireSIGHT taille les don les plus anciennes pendant que les nouvelles données entrent. Vo pouvez configurer la stratégie de système pour relâcher de nouvea hôtes quand la limite d'hôte a atteint.
3. Combien de sauts loin que les hôtes se trouvent du périphérique géré de FireSIGHT ?	Plus le compte de saut entre les hôtes et un périphérique géré est élevé, plus loin l'hôte est du périphérique, et la probabilité accrue a le trafic a été modifiée et ne permettra pas l'identification précise.
4. Y a-t-il des périphériques intégrés entre les hôtes et le périphérique géré ?	La présence de tout périphérique intégré ; comme le Pare-feu, le périphérique NAT, l'équilibreur de charge et le serveur proxy peuve modifier le TCP ou les informations d'origine d'en-tête IP qui peuve également être les causes de la mauvaise ou non identifiée collect d'informations des hôtes.
5. Les périphériques gérés surveillent-ils le trafic dans un réseau asynchrone de routage ?	Si un trafic asynchrone de routage de moniteurs système de FireSIGHT, il peut ne pas pouvoir voir la session complète.
6. Y a-t-il des ports non standard utilisés pour des services ? Y a-t-il des décodeurs faits sur commande configurés pour adresser les ports non standard ?	Un décodeur fait sur commande incorrectement configuré peut être conflit avec les décodeurs par défaut.

Les informations supplémentaires

Si toutes les recommandations ci-dessus sont suivies, mais il restent inconnu, en attendant ou les hôtes non identifiés trouvés, alors nous devrons analyser le data&colon suivant ;

1. Le trafic de la réunion plénière

Le trafic de la réunion plénière des hôtes qui sont identifiés inexactement, ou marqués en tant qu'inconnu ou en suspens.

2. Dépannage des fichiers

Le dépannage classe du centre et du périphérique géré de Gestion de FireSIGHT. La carte du réseau ou la topologie affichant l'emplacement du périphérique géré serait utile.

3. Capture de paquet (PCAP)

Les paquets reçus par le périphérique géré peuvent être différents que les paquets lancés sur les hôtes. Il se produit si n'importe quelle en-tête modifiant le périphérique intégré existe entre les hôtes et le périphérique géré. Par conséquent, il vaut mieux de capturer PCAP des deux extrémités - des hôtes et des périphériques gérés, qui laisse comparer les en-têtes des deux PCAPs. N'importe quelle non-concordance entre les paquets peut entraîner l'identification erronée des services ou des hôtes.