Inspection du trafic agrégé par lien par Sourcefire FirePOWER et appliances virtuelles

Contenu

Introduction

L'agrégation de liaisons a été normalisée par IEEE sur 802.3ad 802.3ax. Les réalisations communes de l'agrégation de liaisons sont EtherChannel, Control Protocol d'agrégation de liaisons (LACP), Protocole PAgP (Port Aggregation Protocol), etc. Cet article décrit comment le lien de traitement d'appareils de Sourcefire a agrégé le trafic.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur des modèles de périphérique de Sourcefire FirePOWER, périphérique virtuel modèle, le Control Protocol d'agrégation de liaisons (LACP), l'EtherChannel, et le Protocole PAgP (Port Aggregation Protocol).

Support d'agrégation de liaisons

Une appliance de Sourcefire peut fonctionner avec toutes les réalisations standard d'agrégation de liaisons, parce qu'un protocole d'agrégation de liaisons n'ajoute aucune informations supplémentaires au paquet elle-même. Il n'y a aucun problème connu entre l'implémentation des appliances de Sourcefire et aucun protocole d'agrégation de liaisons.

Choses à considérer

Les points suivants doivent être considérés quand vous déployez une appliance de Sourcefire

dans le déploiement agrégé par lien :

1. Si une appliance de Sourcefire est en mode passif et tous les liens d'EtherChannel sont surveillés par la même engine de détection, alors la configuration d'agrégation de liaisons n'importe pas.
2. Si une engine simple de détection surveillera seulement certains des liens ou le périphérique est déployé comme périphérique intégré, alors l'il est recommandé que l'agrégation de liaisons est configuré pour utiliser des adresses de source et de MAC de destination. Ceci évitera les problèmes de performances liés au routage asynchrone.
3. Snort est capable de traiter le trafic agrégé par lien sans le problème. Cependant, Snort ne pourra pas décoder les paquets de contrôle d'agrégation de liaisons envoyés entre les Commutateurs.
4. Des méthodes d'Équilibrage de charge dans l'EtherChannel sont basées sur chaque circulation et pas sur chaque trame ou paquet, ainsi les écoulements sont ce qui obtient le chargement équilibré. La configuration du « IP de source ip et de destination » dans l'EtherChannel peut affecter l'Équilibrage de charge à travers Sourcefire reniflent des exemples. C'est seulement si hachant des résultats exécutés dans plus d'ensemble limité d'IPS pour choisir de. L'utilisation du « MAC et MAC de destination de source » peut aider avec la répartition de charge.

Problème connu

Le problème connu suivant sur le LACP est signalé sur toutes les versions avant et inclure 5.3.1.1 :

Dans certains cas, l'application change en votre stratégie de contrôle d'accès, stratégie d'intrusion, stratégie de détection de réseau, ou configuration de périphérique, ou installer une mise à jour de règle d'intrusion ou la mise à jour de la base de données de vulnérabilité (VDB) fait éprouver le système une interruption dans le trafic qui utilise le Control Protocol d'agrégation de liaisons (LACP) dans le mode rapide. Comme contournement, configurez les liens LACP en mode lent. (112070)

Document connexe

- Notes de mise à jour en 5.3.1.1 de version de système de FireSIGHT