Secure Network Analytics Virtual Appliance Configuration de l'interface réseau Limites

Table des matières

Problème

Un scénario de déploiement était en cours d'évaluation pour Secure Network Analytics (SNA) avec stockage non-données où le collecteur de flux a plusieurs interfaces réseau attribuées via la plate-forme de virtualisation.

Voici les questions précises qui ont été soulevées :

- Indique si le collecteur de flux virtuel peut fonctionner avec deux cartes réseau : une pour la communication interne SNA et une autre pour la réception NetFlow
- Indique si l'appliance Virtual Manager peut être configurée avec plusieurs cartes réseau pour obtenir des flux de menaces lorsque le segment de communication interne ne peut pas accéder à Internet

Environnement

- Secure Network Analytics (StealthWatch) version 7.6.0
- Versions des appliances virtuelles de tous les composants SNA (Manager, Flow Collector)
- Architecture réseau avec segments de communication interne et de réception NetFlow séparés

Résolution

Le collecteur de flux Cisco Secure Network Analytics (SNA) peut être déployé avec deux interfaces de carte réseau. Ce comportement a été validé dans un environnement de travaux pratiques :

1. Deux interfaces : accès de gestion et réception NetFlow

- Le collecteur de flux peut être configuré avec une interface pour l'accès à la gestion et une seconde interface dédiée à la réception de NetFlow.
- Cependant, l'accès à la gestion reste accessible via l'une ou l'autre interface (gestion ou NetFlow). Il n’existe actuellement aucune option permettant de limiter une interface strictement à son objectif.

2. Deux interfaces : réception NetFlow et réception de flux de menaces

- Les mises à jour des flux de menaces sont récupérées via un accès Internet à partir du collecteur de flux.
- Si l'interface de gestion IP n'a pas d'accès direct à Internet, l'option proxy disponible sur le collecteur de flux peut être configurée pour répondre à cette exigence, tandis que la seconde interface continue de recevoir NetFlow.

Remarque importante sur la portée
Les deux scénarios ont été vérifiés dans le cadre d’une configuration de TP et ne sont pas documentés dans le guide de conception SNA. Ils doivent donc être considérés comme un comportement observé plutôt qu'une recommandation de conception publiée officiellement. Les clients planifiant un tel déploiement sont encouragés à le valider dans leur propre environnement de test.

Motif

Ce comportement a été conçu dans l'architecture de l'appliance Secure Network Analytics Flow Collector. L'appliance prend en charge l'attribution d'une carte réseau supplémentaire et la télémétrie (NetFlow) peut être reçue sur cette interface secondaire tandis que l'interface principale est utilisée pour la gestion. Cependant, le logiciel de l'appliance exécute ses services de gestion (interface utilisateur d'administration de l'appliance, SSH et communication SNA inter-appliance) liés à toutes les interfaces configurées et adressées, et il n'expose aucune liaison de service par interface ou option de contrôle d'accès. Par conséquent, l’accès à la gestion reste accessible depuis l’une ou l’autre des cartes réseau et ne peut pas être limité à l’interface désignée à cet effet.

De même, la récupération des flux de menaces n'est pas liée à une carte réseau spécifique. Le processus de mise à jour initie simplement une connexion sortante basée sur la table de routage de l'appliance, de sorte que toute interface avec un chemin valide vers les services Internet envoie la requête. Lorsque l'interface de gestion n'a pas d'accessibilité directe à Internet, l'option de configuration de proxy dans Appliance Admin relaie la requête sortante via un serveur proxy approuvé, permettant ainsi au flux de menaces de se mettre à jour sans modifier les rôles d'interface.

Étant donné que les déploiements de collecteurs de flux multi-cartes réseau et la séparation des rôles d'interface ne sont pas abordés dans le Guide de conception Secure Network Analytics, ce comportement n'est pas documenté et n'est pas pris en charge. Les résultats sont uniquement basés sur la validation en laboratoire.

Autres informations utiles

- Guide d'installation de l'appliance Secure Network Analytics Virtual Edition

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.