Détecter le flux d'éléphant sur les périphériques Firepower

Table des matières

Introduction

Ce document décrit comment effectuer la détection de flux d'éléphant dans un environnement Cisco Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Netflow

Composants utilisés

Les informations de ce document sont basées sur un FMC qui exécute la version 7.1 ou ultérieure du logiciel. The information in this document was created from the devices in a specific lab environment. Tous les dispositifs utilisés dans ce document ont démarré par une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La détection des flux d'éléphant dans Cisco Firepower est essentielle pour identifier et gérer les

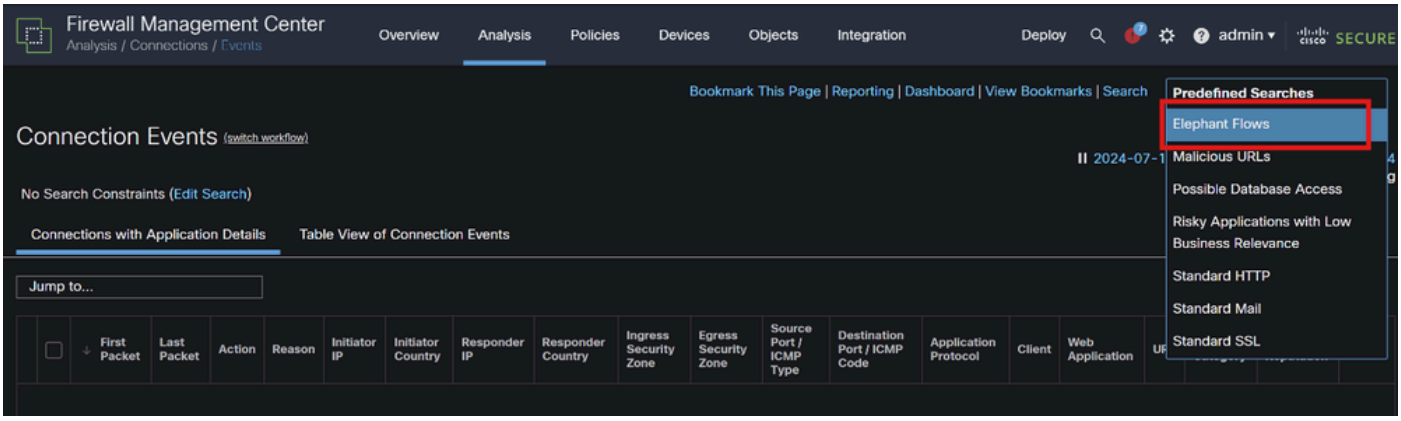
flux volumineux à longue durée de vie qui peuvent consommer des ressources réseau importantes et affecter les performances. Les flux éléphants peuvent se produire dans des applications gourmandes en données telles que la diffusion vidéo en continu, les transferts de fichiers volumineux et la réplication de bases de données. Vous pouvez l'identifier à l'aide des méthodes suivantes :

Méthodes

1. Utilisation de FMC

La détection de flux d'éléphant a été introduite dans la version 7.1. La version 7.2 permet une personnalisation plus facile et la possibilité de contourner ou même de réguler les flux d'éléphants. Le contournement intelligent des applications (IAB) est déconseillé à partir de la version 7.2.0 pour les périphériques Snort 3.

La détection du flux d'éléphant peut être effectuée sous Analysis > Connections > Events > Predefined Searches > Elephant Flows.



Événements de connexion

Ce document fournit un processus pas à pas pour configurer Elephant Flow on Access Control Policy

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html#task_sxp_h2d_jsb

2. Utilisation de CLI

a. La saturation du CPU de l'instance Snort peut également indiquer que le réseau traite le flux Elephant qui peut être identifié à l'aide de la commande suivante :

show asp inspect-dp snort

Voici un exemple pour le résultat de la commande.

> show asp inspect-dp snort

ID ID ID informations d'état d'instance SNORT Inspect

Utilisation du processeur Nombre de segments/paquets État tot (usr | sys)

— ----- ---------- ---------- ---------- ----------

0 16450 8 % (7 %| 0 %) 2,2 K 0 PRÊT

1 16453 9 % (8 %| 0 %) 2,2 K 0 PRÊT

2 16451 6 % (5 %| 1 %) 2,3 K 0 PRÊT

3 16454 5 % (5 %| 0 %) 2,2 K 1 PRÊT

4 16456 6 % (6 %| 0 %) 2,3 K 0 PRÊT

5 16457 6 % (6 %| 0 %) 2,3 K 0 PRÊT

6 16458 6 % (5 %| 0 %) 2,2 K 1 PRÊT

7 16459 4 % (4 %| 0 %) 2,3 K 0 PRÊT

8 16452 9 % (8 %| 1 %) 2,2 K 0 PRÊT

9 16455 100 % (100 %| 0 %) 2,2 K 5 READY <<< Utilisation élevée du CPU 10 16460 7 % (6 %| 0 %) 2,2 K 0 PRÊT

— ----- ---------- ---------- ---------- ----------

Résumé 15 % (14 %| 0 %) 24,6 K 7

b. En outre, la sortie de la commande "top" du mode racine peut également aider à vérifier si une instance de Snort devient élevée.

c. Exportez les détails de la connexion à l'aide de cette commande pour vérifier le trafic supérieur passant par le pare-feu.

show asp inspect-dp snort

show conn detail | redirect disk0:/con-detail.txt

Le fichier se trouve sous "/mnt/disk0" en mode Linux. Copiez le même fichier dans **/ngfw/var/common** pour le télécharger à partir de FMC.

expert cp

/mnt/disk0/<nom de fichier> /ngfw/var/common/

Voici un exemple de résultat détaillé de la connexion.

UDP interne : 10.x.x.x/137 interne : 10.x.x.43/137, indicateurs - N1, 0 inactifs, temps de fonctionnement 6D2h, délai d'attente 2m0s, octets 123131166926 <<< 123 Go et temps de fonctionnement semble être de 6 jours 2 heures

ID de clé de recherche de connexion : 2255619827

UDP interne : 10.x.x.255/137 interne : 10.x.x.42/137, indicateurs - N1, 0 inactifs, temps de fonctionnement 7D5h, délai d'attente 2m0s, octets 116338988274

ID de clé de recherche de connexion : 1522768243

UDP interne : 10.x.x.255/137 interne : 10.x.x.39/137, indicateurs - N1, 0 inactifs, temps de fonctionnement 8D1h, délai d'attente 2m0s, octets 60930791876

ID de clé de recherche de connexion : 1208773687

UDP interne : 10.x.x.255/137 interne : 10.x.x0.34/137, indicateurs - N1, 0 inactifs, temps de fonctionnement 9D5h, délai d'attente 2m0s, octets 59310023420

ID de clé de recherche de connexion : 597774515

3. Utilisation de Netflow

Les flux éléphants sont des flux de trafic à volume élevé qui peuvent affecter les performances du réseau. La détection de ces flux implique la surveillance du trafic réseau afin d'identifier les modèles indiquant des flux importants et persistants. Cisco Firepower fournit des outils et des fonctionnalités pour détecter et analyser le trafic réseau, y compris les flux éléphants. L'outil NetFlow permet de collecter les informations de trafic IP pour la surveillance.

Ce document fournit un processus pas à pas pour configurer la stratégie NetFlow sur FMC

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221612-htz-01-2024-configure-netflow-in-fmc.html

Utilisez un collecteur et un analyseur NetFlow (par exemple, Cisco StealthWatch, SolarWinds ou tout autre outil d'analyse NetFlow) pour analyser les données collectées. Une fois que les flux d'éléphants sont identifiés, vous pouvez prendre des mesures pour atténuer leur impact :

- Traffic Shaping and QoS : implémentez des politiques de qualité de service (QoS) pour hiérarchiser le trafic et limiter la bande passante des flux éléphants.

- Access Control Policies : créez des politiques de contrôle d'accès pour gérer et limiter les flux d'éléphants.

- Segmentation : utilisez la segmentation du réseau pour isoler les flux de gros volumes et minimiser leur impact sur le reste du réseau.

- Load Balancing : mettez en oeuvre l'équilibrage de charge pour répartir le trafic de manière plus homogène sur les ressources réseau.

4. Suivi et ajustement continus

Surveillez régulièrement votre trafic réseau pour détecter de nouveaux flux et ajustez vos politiques et configurations en fonction des besoins.

Grâce à ce processus, vous pouvez détecter et gérer efficacement les flux de données dans votre déploiement Cisco Firepower, garantissant ainsi de meilleures performances réseau et une meilleure utilisation des ressources.

Informations connexes

Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.2

Configuration de NetFlow dans FMC

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.