Traitement de la grande session de flot simple (écoulement d'éléphant) par les services de puissance de feu

Contenu

Introduction

Le résultat d'aucun site Web de test de vitesse de bande passante, ou la sortie d'aucun outil de mesure de bande passante (par exemple, *iperf*) peut ne pas montrer l'évaluation annoncée de débit des appliances de puissance de feu de Cisco. De même, le transfert d'un fichier très grand sur aucun protocole de transport n'explique pas l'évaluation annoncée de débit d'une appliance de puissance de feu. Il se produit parce que le service de puissance de feu n'emploie pas un écoulement de réseau simple pour déterminer son débit maximal. Ce document décrit pourquoi un à courant simple ne peut pas consommer le débit évalué entier d'une appliance de puissance de feu de Cisco.

Contribué par Nazmul Rajib, et Lipkey adoptif, ingénieurs TAC Cisco.

Le traitement du trafic par reniflent

La technologie sous-jacente de détection du service de puissance de feu est reniflent. L'implémentation Snort sur l'appliance de puissance de feu de Cisco est un procédé simple de thread pour le traitement du trafic. Une appliance est évaluée pour une évaluation spécifique basée sur tout le débit de tous les écoulements allant par l'appliance. On s'attend à ce que les appliances soient déployées sur un réseau d'entreprise, habituellement près de la périphérie et des travaux de cadre avec des milliers de connexions.

La puissance de feu entretient des utilisations que l'Équilibrage de charge du trafic à un certain nombre de différent reniflent le processus avec un reniflent le processus exécuté sur chaque CPU sur l'appliance. Dans le meilleur des cas, le système équilibrent la charge le trafic même à travers

le tout les reniflent des processus. Reniflez les besoins de pouvoir fournir l'analyse contextuelle appropriée pour l'inspection NGFW, IPS, et d'AMPÈRE. Pour assurer Snort est le plus efficace, tout le trafic d'un à courant simple est chargement équilibré à un reniflent l'exemple. Si tout le trafic d'un à courant simple n'était pas équilibré à un simple reniflent l'exemple, le système pourrait être éludé en séparant le trafic de telle manière qu'une règle de renifler puisse être moins pour s'assortir ou les parties d'un fichier ne sont pas contiguës pour l'inspection d'AMPÈRE. Par conséquent, l'algorithme d'Équilibrage de charge est basé sur les informations de connexion qui peuvent seulement identifier une connexion donnée.

algorithme 2-Tuple dans l'ASA avec des services de puissance de feu et le NGIPS virtuel

Sur l'ASA avec la puissance de feu entretenez la plate-forme et NGIPS virtuel, le trafic est chargement balaned pour renifler utilisant un algorithme 2-tuple. Les datapoints pour cet algorithme sont :

- Source ip
- IP de destination

l'algorithme 3-Tuple dans la version de logiciel 5.3 ou diminuent sur la puissance de feu et les appliances FTD

Sur toutes les versions antérieures (5.3 ou diminuent), le trafic est chargement balaned pour renifler utilisant un algorithme 3-tuple. Les datapoints pour cet algorithme sont :

- Source ip
- IP de destination
- IP Protocol

N'importe quel trafic avec la même source, la destination, et l'IP Protocol sont chargement équilibré au même exemple Snort.

algorithme 5-Tuple dans la version de logiciel 5.4, 6.0, et plus grand sur la puissance de feu et les appliances FTD

Sur la version 5.4, 6.0 ou plus grand, le trafic est chargement balaned pour ronfler utilisant un algorithme 5-tuple. Les datapoints qui sont pris en considération sont affichés ci-dessous :

- Source ip
- Port de source
- IP de destination
- Destination port
- IP Protocol

Le but d'ajouter des ports à l'algorithme est d'équilibrer le trafic plus également quand il y a des paires spécifiques de source et de destination qui expliquent de grandes parties du trafic. En ajoutant les ports, les ports éphémères d'ordre élevé de source devraient être différents par écoulement, et devraient ajouter l'entropie supplémentaire équilibrant plus également le trafic à différent reniflent des exemples.

Débit total

Tout le débit d'une appliance est mesuré a basé sur le débit total de tous les exemples de renifler fonctionnant à leur plus pleine capacité. Les pratiques industriellement compatibles pour le débit de mesure sont pour de plusieurs connexions HTTP utilisant de diverses tailles d'objet. Par exemple, la méthodologie de test NSS NGFW mesure le débit total du périphérique utilisant les objets 44k, 21k, 10k, 4.4k, et 1.7k. Ceux-ci se traduisent à une plage des tailles moyennes des paquets de autour des octets 1k à 128 octets en raison des autres paquets impliqués dans la connexion HTTP.

Vous pouvez estimer que le taux d'utilisation des ressources d'une personne reniflent l'exemple en prenant le débit évalué de l'appliance et en divisant cela par le nombre d'exemples Snort qui s'exécutent. Par exemple, si une appliance est évaluée à 10Gbps l'IPS avec une taille moyenne des paquets des octets 1k, et cette appliance a 20 exemples Snort, le débit maximal approximatif pour un exemple simple serait 500 Mbits/s par reniflent. Les différents types de trafic, des protocoles réseau, des tailles des paquets avec des différences dans la stratégie de sécurité globale peuvent tout affecter le débit observé du périphérique.

Résultat de test d'un outil de tiers

Quand vous testez avec n'importe quel site Web de test de vitesse, ou n'importe quel outil de mesure de bande passante, comme, *iperf*, un grand écoulement simple de TCP de flot est généré. Ce type de grand écoulement de TCP s'appelle un **écoulement d'éléphant**. Un écoulement d'éléphant est une session simple, la connexion réseau relativement longue qui consomme une grande ou disproportionnée quantité de bande passante. Ce type d'écoulement est assigné à un reniflent l'exemple, donc le résultat de test affiche le débit de simple reniflent l'exemple, pas l'évaluation de débit total de l'appliance.

Corrections

Contournement intelligent d'application (IAB)

La version de logiciel 6.0 introduit une nouvelle caractéristique appelée le **contournement d'Intelligent Application** (IAB). Quand une appliance de puissance de feu atteint un seuil prédéfini de performances, la caractéristique IAB recherche les écoulements qui répondent à des critères spécifiques pour sauter intelligemment qui allège la pression sur les engines de détection.

> **Conseil** : Plus d'informations sur configurer l'IAB peuvent être trouvées ici.

Identifiez et faites confiance aux grands écoulements

De grands écoulements sont souvent liés au bas trafic de valeur d'inspection d'utilisation élevée par exemple, aux sauvegardes, à la réplication de base de données, etc. Plusieurs de ces applications ne peuvent être bénéficiées de l'inspection. Pour éviter des questions avec de grands écoulements, vous pouvez identifier les grands écoulements et créer des règles de confiance de contrôle d'accès pour elles. Ces règles peuvent identifier seulement de grands écoulements, permettent à ces écoulements pour passer non examiné, et ne pas être limité par le célibataire reniflez le comportement d'exemple.

> Remarque: Pour identifier de grands écoulements pour des règles de confiance, entrez en

contact avec s'il vous plaît la puissance de feu TAC de Cisco.

Documents connexes

- Contrôle d'accès utilisant le contournement intelligent d'application