

# Grande session de flot simple de processus (écoulement d'éléphant) par des services de FirePOWER

## Contenu

[Introduction](#)

[Informations générales](#)

[Le trafic de processus par reniflent](#)

[algorithme 2-Tuple dans l'ASA avec des services de FirePOWER et le NGIPS virtuel](#)

[l'algorithme 3-Tuple dans la version de logiciel 5.3 ou diminuent sur FirePOWER et des appliances FTD](#)

[algorithme 5-Tuple dans la version de logiciel 5.4, 6.0, et plus grand sur FirePOWER et des appliances FTD](#)

[Débit total](#)

[Résultat de test d'outil de tiers](#)

[Corrections](#)

[Contournement intelligent d'application \(IAB\)](#)

[Identifiez et faites confiance aux grands écoulements](#)

[Informations connexes](#)

## Introduction

Ce document décrit pourquoi un à courant simple ne peut pas consommer le débit évalué entier d'une appliance de Cisco FirePOWER.

## [Informations générales](#)

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) ne pourrait pas montrer l'évaluation annoncée de débit des appliances de Cisco FirePOWER. 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 FirePOWER. Il se produit parce que le service de FirePOWER n'emploie pas un écoulement de réseau simple afin de déterminer son débit maximal.

## Le trafic de processus par reniflent

La technologie sous-jacente de détection du service de FirePOWER est reniflent. L'implémentation Snort sur l'appliance de Cisco FirePOWER est un processus simple de thread afin de traiter le trafic. Une appliance est évaluée pour une évaluation spécifique basée sur tout le débit de tous les écoulements qui passe 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.

L'Équilibrage de charge d'utilisation de services de FirePOWER du trafic à un certain nombre de différent reniflent le processus avec un reniflent le processus qui fonctionne 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 le Pare-feu de la deuxième génération (NGFW), le Système de prévention d'intrusion (IPS) et l'inspection avancée de protection de malware (AMP). Afin d'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 et le trafic renversé de telle manière qu'une règle de renifler pourrait être moins pour s'assortir ou les parties d'un fichier ne soient pas contiguës pour l'inspection d'AMP. 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 FirePOWER et le NGIPS virtuel**

Sur l'appliance de sécurité adaptable (ASA) avec la plate-forme de service de FirePOWER et le système de prévention des intrusions de nouvelle génération (NGIPS) virtuels, le trafic est chargement équilibré afin de renifler avec l'utilisation d'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 FirePOWER et des appliances FTD**

Sur toutes les versions antérieures (5.3 ou diminuent), le trafic est le chargement équilibré pour renifler qui utilise 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 FirePOWER et des appliances FTD**

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

- 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. Par

l'ajout des ports, les ports éphémères d'ordre élevé de source doivent être différents par écoulement, et doivent ajouter l'entropie supplémentaire plus également qui équilibre 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 qui fonctionne à leur plus pleine capacité. Les pratiques industriellement compatibles afin de mesurer le débit sont pour de plusieurs connexions HTTP avec de diverses tailles d'objet. Par exemple, la méthodologie de test NSS NGFW mesure le débit total du périphérique avec les objets 44k, 21k, 10k, 4.4k, et 1.7k. Ceux-ci se traduisent à une plage des tailles moyennes des paquets de autour de 1k et des octets 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. Prenez le débit évalué de l'appliance et divisez cela par le nombre d'exemples Snort qui fonctionnent. 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'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 l'IAB. Quand une appliance de FirePOWER atteint un seuil prédéfini de performances, la caractéristique IAB recherche les écoulements qui répondent à des critères spécifiques afin de sauter intelligemment qui allège la pression sur les engines de détection.

**Conseil** : Plus d'informations sur la configuration de 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 pas être bénéficiées de l'inspection. Afin d'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.

**Note:** Afin d'identifier de grands écoulements pour des règles de confiance, contactez Cisco FirePOWER TAC.

## [Informations connexes](#)

- [Contrôle d'accès utilisant le contournement intelligent d'application](#)
- [Support et documentation techniques - Cisco Systems](#)