Supervision réseau avec NetFlow et sFlow

Supervision réseau avec NetFlow et sFlow

Introduction à l'analyse de réseau en temps réel

Pandora FMS utilise un outil d'analyse du réseau en temps réel : NetFlow® et sFlow®. Il utilise le principe de « l'écoute » en continu sur Ethernet et analyse le trafic pour générer des statistiques.

Pour intercepter le trafic réseau et l'analyser, il est nécessaire d'avoir un accès physique à ce réseau, le point de capture du réseau devant être le plus approprié. Pour capturer ces données, le trafic doit être redirigé d'un port du commutateur vers un autre port via un port mirror. Tous les appareils réseau ne le permettent pas (uniquement les appareils de milieu et de haut de gamme). Le port-mirroring est également possible sur certains pare-feu commerciaux. C'est le moyen le plus simple d'intercepter le trafic et il ne nécessite aucun matériel supplémentaire. En envoyant tout le trafic vers un seul port, celui-ci est directement connecté à l'analyseur de réseau (sonde).

Ces commutateurs et/ou pare-feu haut de gamme facilitent la supervision. En effet, ces dispositifs envoient les informations statistiques du flux réseau directement au collecteur Pandora FMS sans qu'il soit nécessaire d'utiliser une sonde indépendante. Vous devez consulter les caractéristiques du matériel pour savoir si vous pouvez activer NetFlow et/ou sFlow et envoyer les flux à un collecteur indépendant (dans ce cas, le collecteur Pandora FMS).

Supervision réseau avec NetFlow

Pandora FMS est capable de superviser le trafic IP à l'aide du protocole NetFlow.

NetFlow® est un protocole de réseau développé par Cisco Systems® et actuellement pris en charge sur plusieurs plateformes en plus de Cisco IOS® et NXOS®, par exemple sur des appareils de fabricants tels que Juniper®, Enterasys Switches®, et sur des systèmes d'exploitation tels que Linux®, FreeBSD®, NetBSD® et OpenBSD®.

Protocole NetFlow

Lorsqu'ils activent cette fonction, les appareils dotés de la fonction NetFlow génèrent des « enregistrements de flux nets » qui consistent en de petits éléments d'information qu'ils envoient à un appareil central (un serveur ou collecteur NetFlow), qui reçoit les informations des appareils (sondes NetFlow) en vue de leur stockage et de leur traitement.

Ces informations sont transmises via le protocole NetFlow, basé sur UDP ou SCTP. Chaque enregistrement NetFlow est un petit paquet qui contient une quantité minimale d'informations, mais qui ne contient en aucun cas les données brutes du trafic. En d'autres termes, il n'envoie pas

la charge utile du trafic passant par le collecteur, mais uniquement les données statistiques.

La définition traditionnelle de Cisco consiste à utiliser une clé à 7 éléments :

- Adresse IP source.
- Adresse IP de destination.
- Port UDP ou TCP source.
- Port UDP ou TCP de destination.
- Protocole IP.
- Interface (SNMP ifIndex)
- Type de service IP

Au fil du temps, d'autres fabricants ont conçu des systèmes équivalents pour leurs dispositifs de réseau, avec des noms différents mais des objectifs similaires :

- Jflow ou cflowd de Juniper Networks®.
- NetStream de 3Com/H3C|HP®.
- NetStream de Huawei®.
- Cflowd d'Alcatel Lucent®.
- Rflow d'Ericsson®.
- AppFlow®.
- sFlow®.

Collecteur NetFlow

Il s'agit d'un dispositif (PC ou serveur) situé sur le réseau pour collecter toutes les informations NetFlow envoyées par les routeurs et commutateurs.

NetFlow génère et collecte ces informations, mais un logiciel est nécessaire pour stocker et analyser ce trafic. Avec Pandora FMS, nous utiliserons un serveur spécial à cet effet, que Pandora FMS démarrera et arrêtera au démarrage de Pandora. Ce serveur est appelé nfcapd et il est nécessaire de l'installer pour pouvoir utiliser la supervision NetFlow.

Sonde NetFlow

Les sondes (par exemple dans Raspberry) sont généralement des routeurs avec NetFlow activé, configuré et envoyant des informations au collecteur NetFlow (qui dans ce cas sera le serveur Pandora FMS avec le daemon nfcapd activé).

Exigences et installation

Pandora FMS utilise un outil OpenSource appelé nfcapd (appartenant au paquet nfdump) pour traiter tout le trafic NetFlow. Ce *daemon* est automatiquement levé par le serveur Pandora FMS. Ce système stocke les données dans des fichiers binaires, dans un certain emplacement. Vous

devez installer nfcapd dans votre système avant de pouvoir travailler avec NetFlow dans Pandora FMS.

Le *daemon* par défaut nfcapd écoute au port 9995/UDP, vous devrez donc en tenir compte si vous avez des pare-feu pour ouvrir ce port et lors de la configuration de vos sondes NetFlow.

Installation de nfcapd

L'installation de nfcapd doit se faire manuellement, car Pandora FMS ne l'installera pas. Pour plus d'informations, rendez-vous sur la page officielle du projet nfcapd.

Pandora FMS utilise par défaut le répertoire `/var/spool/pandora/data_in/netflow` pour traiter l'information, donc quand il démarre nfcapd il utilise ce répertoire. Évitez de modifier ce chemin d'accès, à moins que cela ne soit strictement nécessaire et que vous en soyez pleinement conscient.

Vous devez installer version 1.6.8p1 de nfdump pour
l'utiliser avec Pandora FMS.

Si vous souhaitez vérifier que nfcapd est correctement installé, exécutez la commande suivante pour lancer le processus au premier plan :

```
nfcapd -l /var/spool/pandora/data_in/netflow
```

Si tout se passe bien, vous devriez avoir une issue similaire à celle-ci :

```
Add extension: 2 byte input/output interface index
Add extension: 4 byte input/output interface index
Add extension: 2 byte src/dst AS number
Add extension: 4 byte src/dst AS number
Add extension: 4 byte output bytes
Add extension: 8 byte output bytes
Add extension: NSEL Common block
Add extension: NSEL xlate ports
Add extension: NSEL xlate IPv4 addr
Add extension: NSEL xlate IPv6 addr
Add extension: NSEL ACL ingress/egress acl ID
Add extension: NSEL username
Add extension: NSEL max username
Add extension: NEL Common block
Bound to IPv4 host/IP: any, Port: 9995
Startup.
Init IPFIX: Max number of IPFIX tags: 62
```

Gardez à l'esprit qu'il est nécessaire que Pandora FMS, et en particulier le serveur WEB qui exécute la console, ait accès à ces fichiers de données. Dans cet exemple ils sont dans :

```
/var/spool/pandora/data_in/netflow
```

Installation des sondes

Si vous n'avez pas de routeur NetFlow, mais que votre trafic passe par un système Linux, vous pouvez installer un logiciel qui agit comme une sonde et envoie les informations trafic NetFlow au collecteur.

Installation de fprobe

fprobe capture le trafic et le transmet à un serveur NetFlow. Avec lui, vous pouvez générer du trafic NetFlow, à partir de tout le trafic réseau qui passe par vos interfaces.

Pour télécharger le paquetage RPM, il suffit d'exécuter la commande suivante, puis de l'installer :

```
wget http://repo.iotti.biz/CentOS/7/x86_64/fprobe-1.1-2.el7.lux.x86_64.rpm
yum install fprobe-1.1-2.el7.lux.x86_64.rpm
```

Par exemple, l'exécution de la commande suivante enverra tout le trafic d'interface *eth0* au collecteur NetFlow qui écoute sur le port *9995* de l'IP `192.168.70.185` :

```
/usr/sbin/fprobe -i eth0 192.168.70.185:9995
```

Une fois le trafic généré, vous pourrez en voir les statistiques dans le collecteur NetFlow avec la commande :

```
nfdump -R /var/spool/pandora/data_in/netflow
```

Installation de pmacct

Expérimental.

Parmi les nombreuses caractéristiques de la sonde pmacct sont la capacité de travailler avec NetFlow v1/v5/v7/v8/v9 et sFlow v2/v4/v5 à propos de IPv4 et IPv6.

Le code source est hébergé à l'adresse suivante :

https://github.com/pmacct/pmacct

Rocky Linux 8

Installez les dépendances avec des droits d'administrateur :

```
dnf config-manager --set-enabled powertools
dnf groupinstall 'Development Tools'
dnf install libpcap libpcap-devel
```

Télécharger le code source de pmacct (vous pouvez utiliser curl au lieu de wget) et le compiler :

```
cd /tmp
wget -O pmacct-1.7.7.tar.gz
"https://github.com/pmacct/pmacct/releases/download/v1.7.7/pmacct-1.7.7.tar.gz"
tar xvzf pmacct-1.7.7.tar.gz
cd pmacct-1.7.7
./autogen.sh
./configure
make && make install
```

Démarrer pmacct comme une sonde NetFlow en mode *daemon* :

- Créez une configuration pour pmacct.

Par exemple, enverra tout le trafic d'interface `eth0` au collecteur NetFlow qui écoute sur le port `9995` de l'IP `192.168.70.185` :

```
cat> pmacctd_probe.conf <<EOF
daemonize: true
pcap_interface: eth0
aggregate: src_host, dst_host, src_port, dst_port, proto, tos
plugins: nfprobe
nfprobe_receiver: 192.168.70.185:9995
nfprobe_version: 9
EOF
```

- Démarrer pmacctd :

```
pmacctd -f pmacctd_probe.conf
```

Comment utiliser NetFlow sur Pandora FMS

Pandora FMS fonctionne avec NetFlow comme système auxiliaire, c'est-à-dire qu'il ne stocke pas les informations NetFlow dans la base de données. Pandora FMS affiche ces informations sous forme de rapports demandés sur demande.

Pandora FMS fonctionne avec NetFlow en utilisant des « filtres », des ensembles de règles pour visualiser un certain trafic. Ces règles peuvent être aussi simples que « All network traffic 192.168.70.0/24 » ou plus complexes en utilisant des expressions pcap.

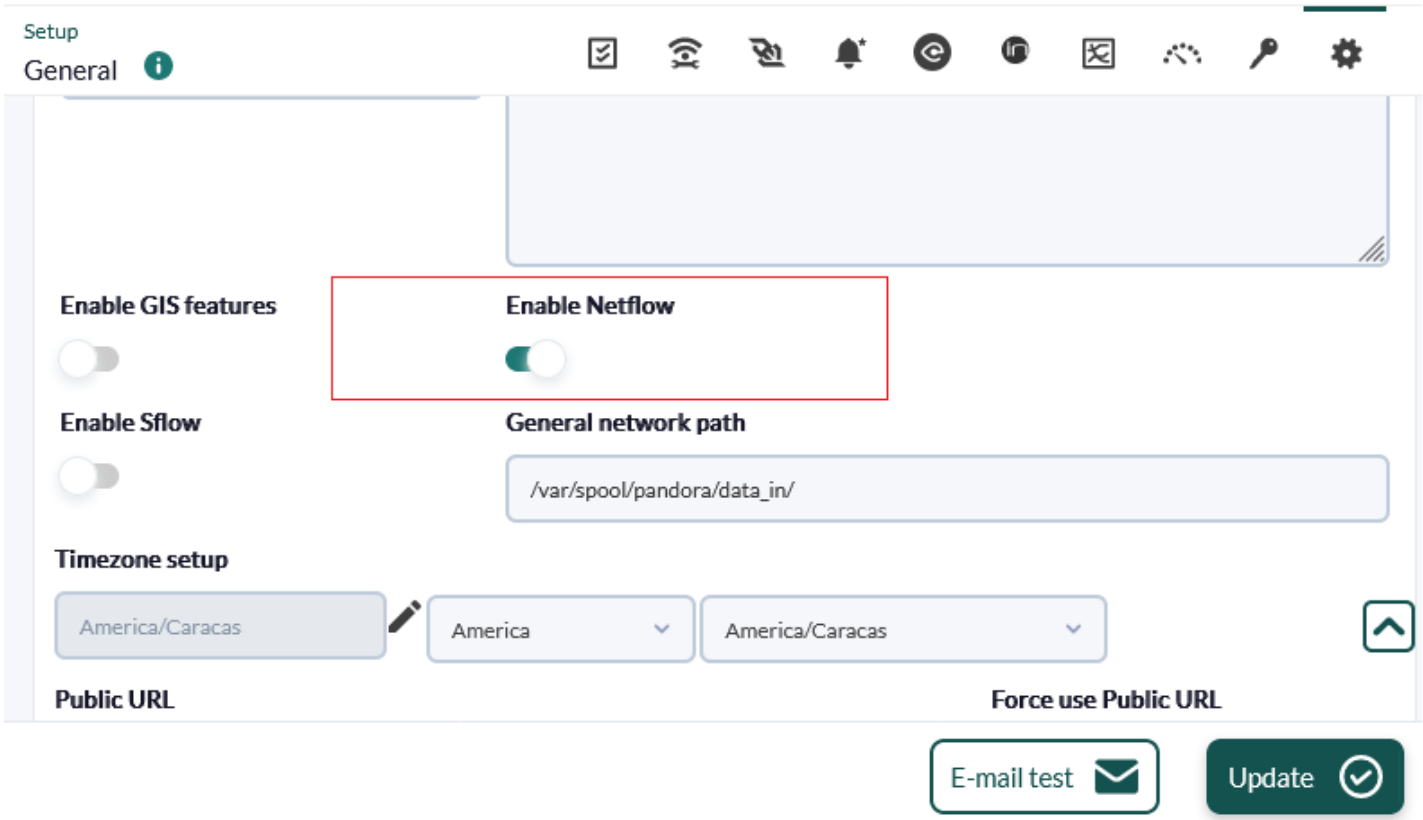
Une fois les filtres définis, nous définirons les rapports, qui déterminent comment nous allons voir les données (graphiques, listes...) et dans quel intervalle de temps. Lors de la définition des filtres et des rapports, nous laissons cette information définie, de la même manière qu'elle fonctionne avec les rapports Pandora FMS, pour l'utiliser - à la demande - quand vous le voulez. Les rapports NetFlow apparaîtront également comme « type de rapport » dans la section Rapports personnalisés de Pandora FMS, pour pouvoir les incorporer aux rapports « normaux » de Pandora FMS.

D'autre part, disposons d'une console de visualisation « temps réel » pour analyser le trafic, en composant directement les règles. Il est utile d'étudier les problèmes, voir les graphiques ponctuels qui ne correspondent pas à un filtre spécifique, etc.

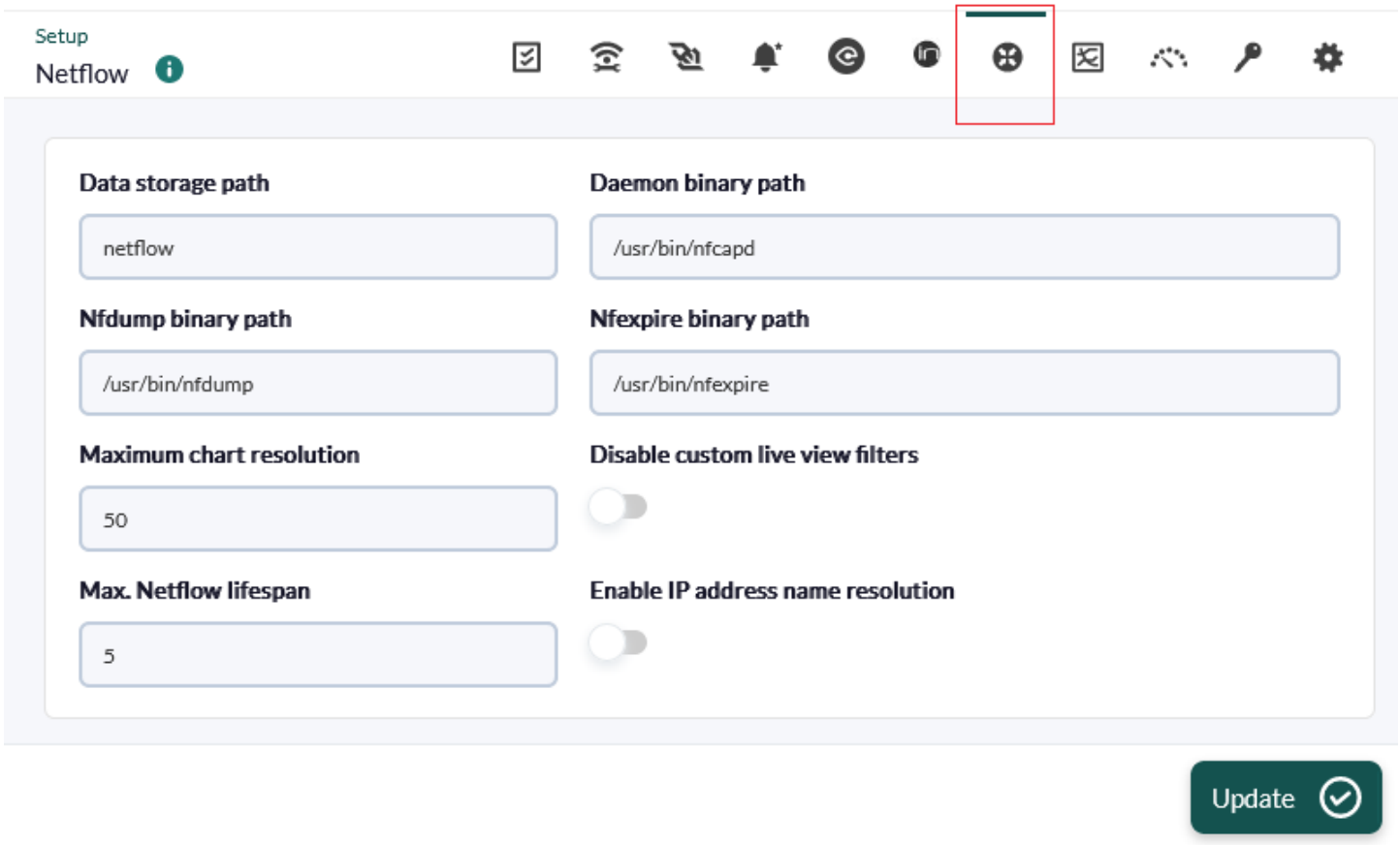
Configuration

La vitesse d'accès du disque sur lequel résident les données NetFlow est normalement le facteur limitant de la performance.

Tout d'abord, NetFlow doit être activé pour être accessible à partir des menus Operation et Administration. Dans la section Configuration (menu d'administration) il y a une option pour activer ou désactiver NetFlow globalement.



Une fois activée, une nouvelle option de configuration NetFlow apparaîtra dans la section configuration.



Cette section doit être configurée correctement pour que le démon nfcapd puisse démarrer sans

problème avec le serveur Pandora FMS :

- Data storage path : Répertoire dans lequel les fichiers de données NetFlow seront stockés. Seul le nom du répertoire doit être saisi, par défaut `netflow` (voir General Setup).
- Daemon binary path : Chemin vers le binaire nfcapd.
- Nfdump binary path : Chemin vers le binaire nfdump.
- Nfexpire binary path : Chemin vers le binaire nfexpire.
- Maximum chart resolution : Nombre maximale de points qu'un graphique de zone NetFlow affichera. Plus la résolution est élevée, plus les performances sont pauvres. Des valeurs comprises entre 50 et 100 sont recommandées.
- Disable custom live view filters : Il désactive la définition des filtres personnalisés dans la vue NetFlow (cela n'autoriserait que l'utilisation des filtres déjà créés).
- Max. NetFlow lifespan : Il indique la durée maximale en jours des données NetFlow à stocker.
- Enable IP address name resolution : Il permet la résolution des adresses IP afin d'essayer d'obtenir les noms d'hôtes des périphériques NetFlow.
- Daemon interval : Il permet de définir l'intervalle de temps du démon NetFlow sur 10, 30 ou 60 minutes. Une fois la modification effectuée et appliquée dans le sélecteur de temps, le serveur doit être redémarré pour que la modification soit prise en compte.

Une fois NetFlow configuré dans la console, il sera nécessaire de redémarrer le serveur Pandora FMS pour qu'il démarre le serveur nfcapd. Ceci doit être correctement installé avant d'essayer de le démarrer. Vérifiez les journaux du serveur pour tout doute.

Si vous décidez de stocker les données NetFlow sur un périphérique autre que le serveur PFMS (voir la procédure d'installation de nfcapd et la configuration distribuée), vous devez copier le fichier binaire `/usr/bin/nfexpire` sur ce périphérique et ajouter l'entrée suivante dans `/etc/crontab` :

```
0 * * * * root yes 2>/dev/null | /usr/bin/nfexpire -e
"/var/spool/pandora/data_in/netflow" -t X_days d
```

Où `x_days` est le nombre maximale de jours d'ancienneté des données NetFlow à conserver sur ce dispositif (*dans ce cas particulier, la configuration de la console PFMS n'aura aucun effet pour ce champ*).

Filtres

Le menu de création et d'édition des filtres se trouve sous Resources → NetFlow filters. Dans cette vue, nous trouvons une liste de filtres déjà créés qui peuvent être modifiés et supprimés.

Vous pouvez également créer un filtre directement à partir de la vue NetFlow live view, en enregistrant le filtre actif comme un nouveau filtre. Les filtres NetFlow peuvent être « de base » ou « avancés ». La différence est que les premiers ont des champs de filtrage fixes (IP source, IP destination, IP source, Port source, Port destination) *et les plus avancés sont définis par une expression* pcap (standard dans les expressions de filtrage du trafic réseau) et utilisent toutes

sortes d'outils.

Activer la supervision NetFlow

Version 770 ou ultérieure.

Lors de la création du filtre, la supervision du filtre peut être activée en activant l'option *token* Enable NetFlow monitoring.

- Cela permet de créer un agent qui supervise le volume de trafic de ce filtre.
- Crée un module qui mesure si le trafic provenant d'une adresse IP de ce filtre dépasse un certain seuil.
- Un module de texte sera créé avec le taux de trafic de chaque adresse IP au sein de ce filtre toutes les cinq minutes (les 10 adresses IP les plus fréquentées).

Les paramètres sont les suivants :

- Maximum traffic value of the filter : Il spécifie le taux maximum (en octets par seconde) du trafic du filtre. Il est ensuite utilisé pour calculer le pourcentage du trafic maximal par adresse IP.
- WARNING threshold for the maximum % of traffic for an IP : Si une adresse IP du filtre dépasse le pourcentage fixé, un état d'AVERTISSEMENT est généré.
- CRITICAL threshold for the maximum % of traffic for an IP : Si une adresse IP du filtre dépasse le pourcentage fixé, un état CRITIQUE est généré.

Rapports

Les rapports NetFlow sont intégrés aux rapports de Pandora FMS.

Pour créer un élément de rapport, choisissez l'un des éléments de rapport NetFlow disponibles.

Les options de configuration suivantes sont disponibles :

- Type : Les types d'éléments sont expliqués ci-dessous.
- Filter : Filtre NetFlow à utiliser.
- Period : Longueur de l'intervalle de données à afficher.
- Resolution : Certains rapports exigent que des échantillons soient collectés à intervalles réguliers. Ce paramètre permet de définir le nombre d'échantillons. La résolution peut être faible (6 échantillons), moyenne (12 échantillons), élevée (24 échantillons) ou très élevée (30 échantillons). Il existe deux valeurs spéciales (*hourly* et *daily*) qui permettent de ne pas collecter une valeur fixe d'échantillons, mais un échantillon toutes les heures ou tous les jours.
- Max. values : Nombre maximal d'éléments pour les agrégats. Par exemple, si un graphique de trafic HTTP est agrégé par adresse IP source et que Max. values est fixé à 5, seules cinq adresses IP seront affichées.

Il existe trois types d'éléments de rapport NetFlow:

- NetFlow area chart : Un diagramme de zone, agrégé ou non agrégé.

- NetFlow data chart : Représentation textuelle du graphique de zone.
- NetFlow summary chart : Synthèse du trafic pour la période donnée. Il y a trois éléments : un tableau avec des informations agrégées, un diagramme circulaire avec les adresses IP ou les ports les plus pertinents, et un tableau avec les mêmes informations que le diagramme circulaire ventilées.

Visualisation en temps réel

Cette vue permet de consulter l'historique des données capturées en fonction de différents filtres de recherche. Des filtres et différents modes d'affichage des informations peuvent être utilisés. La manière de regrouper les informations affichées doit être définie, ainsi que la manière d'obtenir ces informations afin de pouvoir commencer à visualiser les données.

Les filtres peuvent être visualisés en temps réel à partir de Operation → Monitoring → Network → NetFlow Live View. Cet outil permet de visualiser les modifications apportées à un filtre et de le sauvegarder une fois le résultat souhaité obtenu. Il est également possible de charger et de modifier des filtres existants.

Les informations peuvent être obtenues par l'intermédiaire de l'adresse IP source, de l'adresse IP de destination, du port source ou du port de destination. Si vous choisissez, par exemple, d'afficher les informations sur l'adresse IP de destination, les informations seront affichées triées par les adresses IP ayant le plus de trafic vers la destination, de la plus élevée à la plus basse. Il en va de même pour connaître la consommation de votre réseau par protocole, en choisissant par port de destination.

Les possibilités de visualisation sont les suivantes :

- Area graph (Graphes de surface de type *stacked*) : Montrer dans le temps (de la date source à la date cible), l'évolution des données. Le niveau de précision du graphique doit être choisi dans le jeton “Résolution”.
- Circular mesh (Graphique circulaire) : Il affiche un graphique circulaire interactif représentant les paires de connexions IP et le volume de trafic.
- Data table (Tableau de données) : Il affiche un tableau de données avec chaque IP et un nombre de lignes dépendant de la résolution choisie.
- Detailed host trafic (Trafic détaillé de l'hôte) : Il affiche une carte de portions représentant le trafic par IP.
- Summary (Résumé) : Il affiche un tableau récapitulatif, un camembert et un tableau avec les données de toute la période.
- Top-N connections (Connexions Top-N) : Un tableau montrant les TOP-N connections entre les paires Source IP - Destination IP, basé sur le trafic entre ces adresses IP (la somme des pourcentages des N éléments du tableau ne sera pas nécessairement égale à cent car il peut y avoir d'autres paires de connexions src/dst).

Cartes de trafic réseau

Il permet de créer des cartes de réseau dynamiques, basées sur le trafic entre les nœuds. Il affiche les relations (connexions) entre différentes adresses, en montrant les N connexions les plus

importantes (en fonction de la taille des données transférées entre elles).

Configuration distribuée

Il est possible de localiser le nœud Pandora FMS qui collecte les données NetFlow dans un hôte indépendant de la console. Dans les environnements avec beaucoup de données NetFlow, il est plus que recommandé de le placer sur un serveur avec des disques rapides et un CPU rapide d'au moins deux cœurs. Pour que la console Pandora FMS puisse extraire les données NetFlow, il sera nécessaire de modifier la configuration par défaut du système, en suivant les étapes décrites ci-dessous :

- Configurez l'authentification automatique SSH entre le propriétaire utilisateur du démon web et l'utilisateur ayant la capacité d'exécuter nfdump dans le nœud collecteur.

Pour sa configuration, nous devons suivre les étapes suivantes :

Activer la connexion pour l'utilisateur apache. Pour ce faire, vous devez modifier dans le fichier `/etc/passwd` la ligne de l'utilisateur apache avec cette configuration :

```
apache:x:48:48:Apache:/var/www:/bin/bash
```

Créez le répertoire `.ssh` dans le répertoire `/var/www` et donnez-lui les bonnes permissions :

```
# mkdir /var/www/.ssh
# chown apache:apache /var/www/.ssh
```

Créez des clés ssh à partir de l'utilisateur apache et copiez-les sur le serveur où le trafic NetFlow est hébergé.

```
# su apache
bash-4.2$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/var/www/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /var/www/.ssh/id_rsa.
Your public key has been saved in /var/www/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:vYvl5V00E4faa14zN08ARzGUQ9IfAQJnMzkaqLAGRHI apache@<server>
The key's randomart image is:
+---[RSA 2048]----+
|+oE     ...*o=B+.|
|.o .   . .oo+o++ |
|  . o .   o o o+o|
|   o .   o   =  +|
|  .     S . . oo.|
```

```
|            .   +o|
|           o . o+=|
|          + + + +*|
|         . o . o .|
+----[SHA256]-----+
bash-4.2$ ssh-copy-id root@<netflow_server>
```

Une fois partagé, il faut vérifier qu'il est possible d'accéder au serveur via l'utilisateur apache sans spécifier de mot de passe :

```
bash-4.2$ ssh usuario@<netflow_server>
```

- Créez un script dans la console FMS de Pandora qui remplace`/usr/bin/nfdump` par un script similaire ausuivant.

```
#!/bin/bash
NFDUMP_PARAMS=$(sed 's/(\(.*\))/\"\(\1\)\"/' <<<"$@");

ssh usuario@<netflow_server> "/usr/bin/nfdump $NFDUMP_PARAMS"
```

Donner les permissions d'exécution au script :

```
chmod 755 /usr/bin/nfdump
```

Essayez d'exécuter le *script*, de cette façon :

```
/usr/bin/nfdump -V
```

Il devrait renvoyer quelque chose de similaire à :

```
nfdump: Version: 1.6.13
```

Supervision réseau avec sFlow

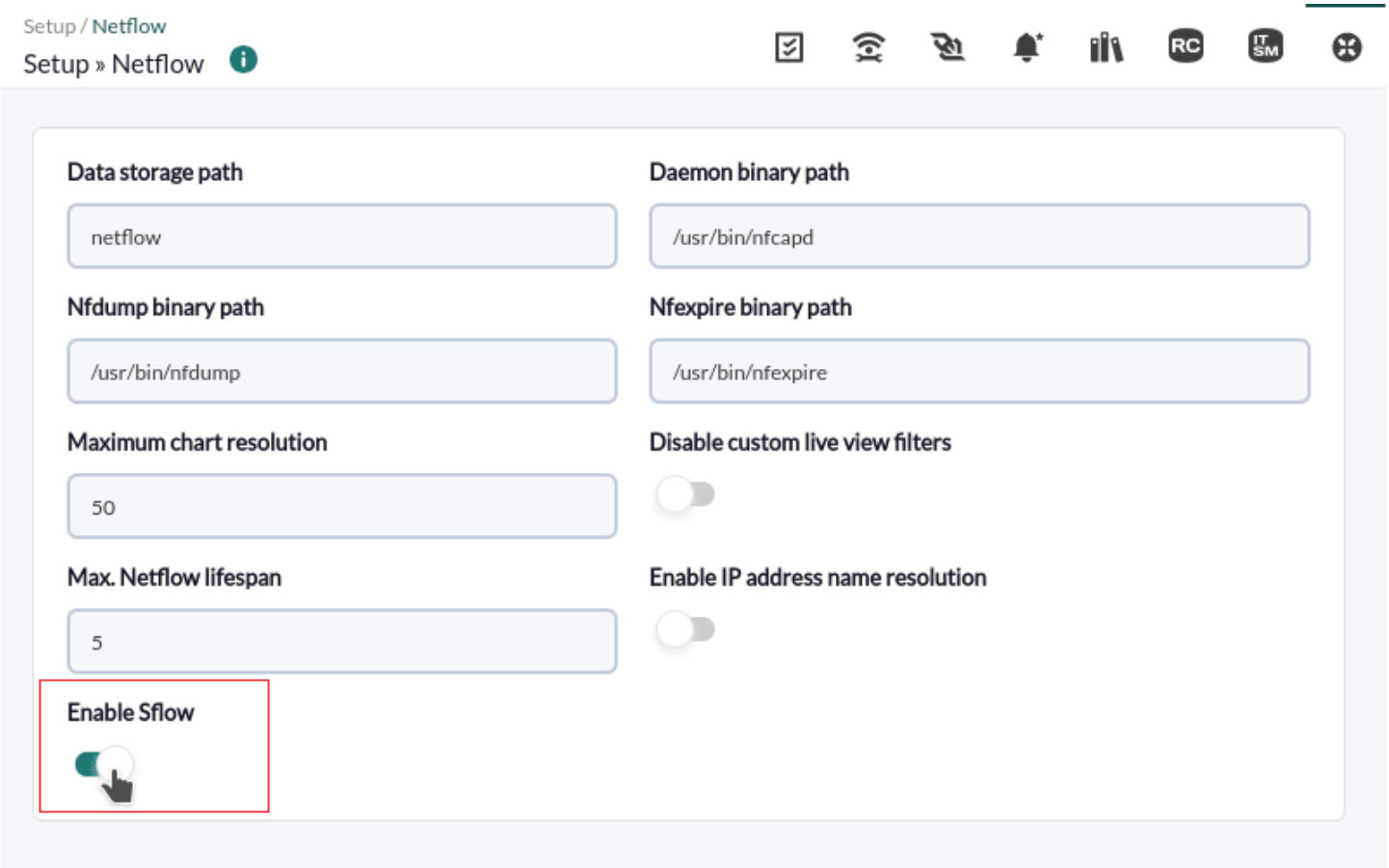
À partir de la version 770 de Pandora FMS, la prise en charge de sFlow, un protocole réseau qui est une norme industrielle dans la fabrication de matériel pour le trafic des réseaux de données, est incluse.

Le fonctionnement de sFlow dans le PFMS est similaire à celui de NetFlow. Si les deux protocoles sont actifs, les données seront regroupées ; dans tous les cas, elles seront toujours affichées en accédant au menu Operation dans la barre latérale gauche, puis en cliquant sur Network.

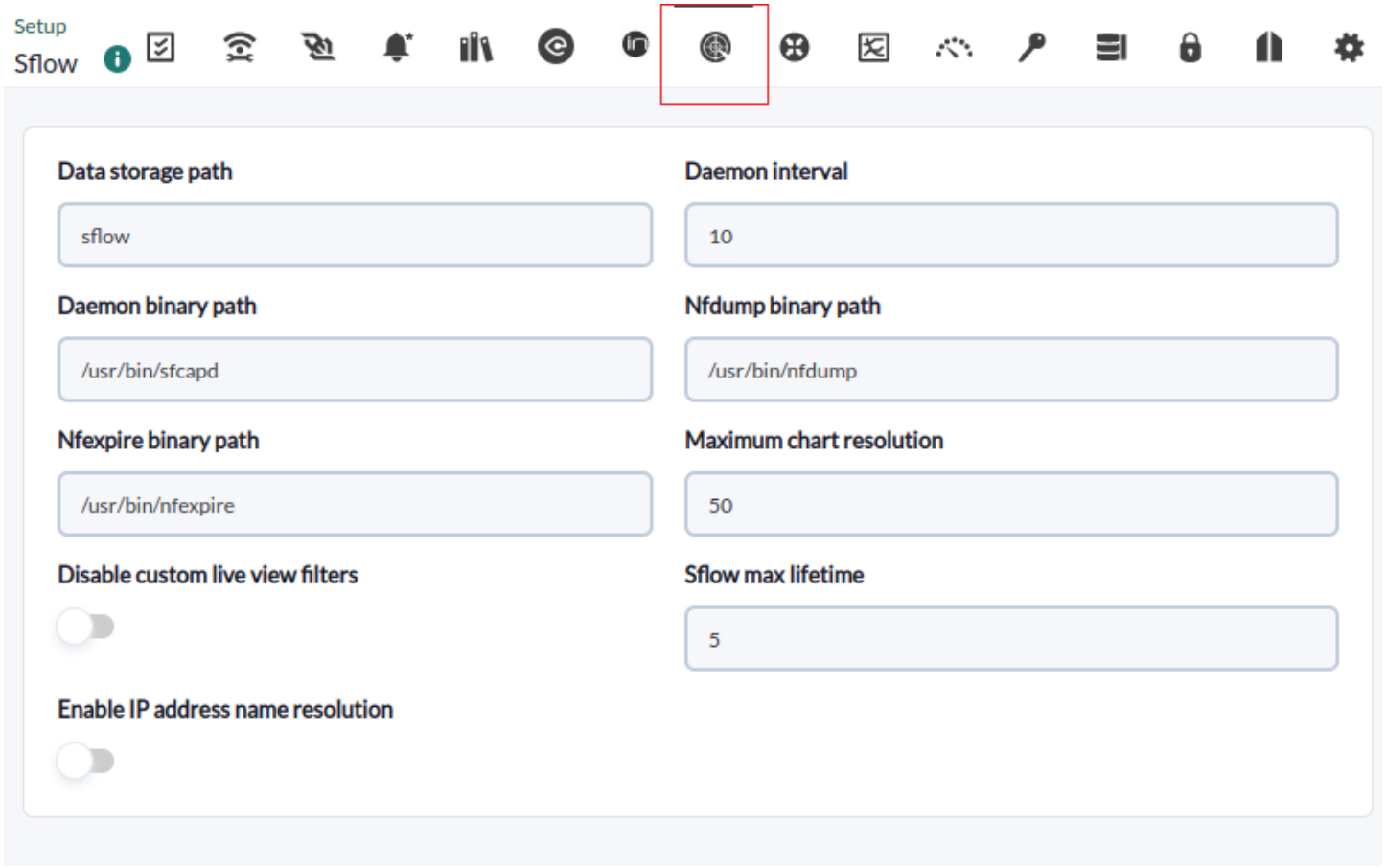
Configuration de sFlow

Version 775 ou supérieure.

Activez sFlow pour qu'il soit accessible à partir des menus Operation et Management. Dans NetFlow configuration, une option permet d'activer ou de désactiver sFlow globalement.



Un nouvel onglet sera activé spécifiquement pour sFlow :



- Data storage path : Répertoire où les fichiers de données sFlow seront stockés (voir General Setup).
- Daemon binary path : Chemin d'accès au binaire de nfcapd.
- Nfdump binary path : Chemin d'accès au binaire de nfdump.
- Nfexpire binary path : Chemin d'accès au binaire de nfexpire.
- Maximum chart resolution : Nombre maximal de points affichés dans un graphique de zone sFlow. Plus la résolution est élevée, moins les performances sont bonnes. Les valeurs recommandées se situent entre 50 et 100.
- Disable custom live view filters : Il désactive la définition de filtres personnalisés dans la vue sFlow (les filtres déjà créés peuvent toujours être utilisés).
- sFlow max lifetime : Il indique la durée maximale en jours de stockage des données sFlow.
- Enable IP address name resolution : Il active la résolution d'adresse IP pour tenter d'obtenir les noms d'hôte des dispositifs sFlow.

Retour à l'index de documentation du Pandora FMS