



# Surveillance du réseau avec NetFlow et sFlow



From:

<https://pandorafms.com/manual/!775/>

Permanent link:

[https://pandorafms.com/manual/!775/fr/documentation/pandorafms/monitoring/18\\_netflow](https://pandorafms.com/manual/!775/fr/documentation/pandorafms/monitoring/18_netflow)

2024/03/18 21:03



# Surveillance du réseau avec NetFlow et sFlow

## Introduction à l'analyse de réseau en temps réel

Pandora FMS utilise un outil pour analyser le réseau en temps réel : NetFlow. Il utilise le principe d'“écoute” sur Ethernet en continu et analyse le trafic pour générer des statistiques. L'idée est “ d'intercepter ” le trafic réseau pour l'envoyer à une sonde qui l'analyse et envoie ces résultats à Pandora FMS.

Pour intercepter le trafic du réseau et pouvoir l'analyser, il est nécessaire d'avoir un accès physique à ce réseau ou au moins de comprendre sa topologie, car le point de capture du réseau doit être le plus approprié. Ce n'est pas la même chose, par exemple, de capturer le trafic réseau d'un *router* ou d'un AP local, que tout le trafic du réseau de serveurs juste avant d'atteindre le *router* de sortie.

Pour capturer ces données, le trafic doit être redirigé d'un port du commutateur vers un autre port à l'aide d'un port-mirror. Tous les périphériques réseau ne le permettent pas (uniquement les périphériques de milieu et de haut de gamme). Vous pouvez également mettre en miroir les ports de 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, ce port est connecté directement à l'analyseur de réseau (sonde NetFlow).

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

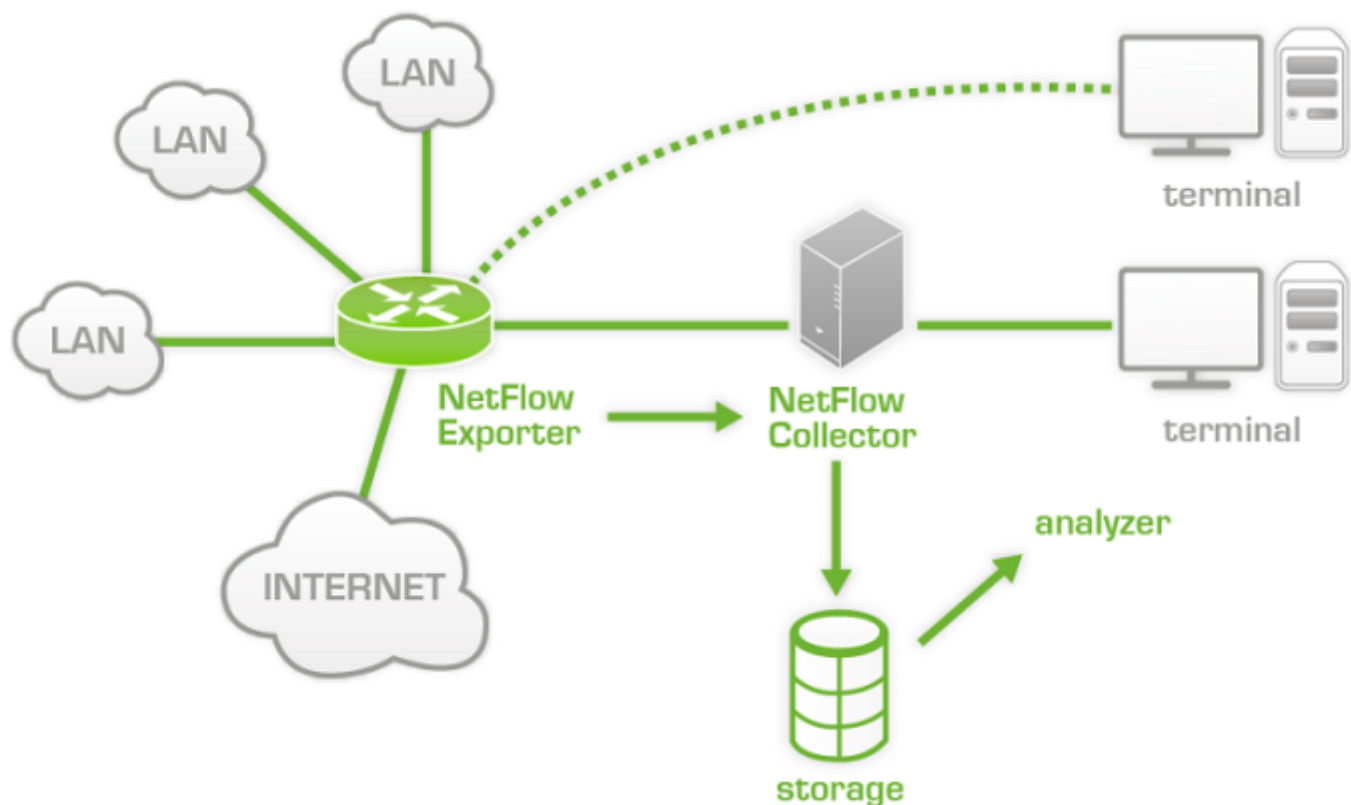
## Surveillance du réseau avec Netflow

### Introduction à Netflow

Depuis la version 5.0, Pandora FMS est capable de surveiller le trafic IP en utilisant le protocole NetFlow. Il permet d'afficher des modèles et des données générales sur le trafic qui sont très utiles.

NetFlow® est un protocole réseau, développé par Cisco Systems® pour collecter des informations sur le trafic IP. Il est devenu un standard de l'industrie pour la surveillance du trafic réseau et est actuellement pris en charge pour diverses plates-formes en plus de Cisco IOS et NXOS, comme les périphériques de fabricants tels que Juniper®, Enterasys Switches®, et les systèmes d'exploitation

tels que Linux®, FreeBSD®, NetBSD®, et OpenBSD®.



Il y a quelque temps, nous avons écrit un article sur notre blog parlant de Netflow, jetez un coup d'oeil pour en savoir plus sur ce protocole : <https://pandorafms.com/blog/fr/quest-ce-que-netflow/>

## Protocole Netflow

Les périphériques avec Netflow activé, lorsqu'ils activent cette fonction, génèrent des “journaux de netflow” composés de petits morceaux d'informations qu'ils envoient à un dispositif central (un serveur ou un collecteur Netflow), qui est celui qui reçoit les informations des périphériques (sondes Netflow) pour les stocker et les traiter.

Ces informations sont transmises via le protocole Netflow, basé sur UDP ou SCTP. Chaque enregistrement Netflow est un petit paquet contenant une quantité minimale d'informations, mais en aucun cas il ne contient les données brutes de trafic. En d'autres termes, il n'envoie pas la charge utile du trafic transitant par le collecteur, seulement des données statistiques.

Il y a plusieurs différences entre les versions d'implémentation du Netflow original, donc certaines incorporent plus de données, mais en gros, le Netflow de base envoie au moins les informations suivantes. Bien que Netflow ait été décrit de nombreuses façons, la définition Cisco traditionnelle consiste à utiliser une clé à 7 éléments, où le flux est défini comme une séquence unidirectionnelle de paquets qui partagent les 7 valeurs suivantes :

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

Au fil du temps, d'autres fabricants ont conçu des systèmes équivalents pour leurs appareils de réseau, avec des noms différents mais dans un but similaire :

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

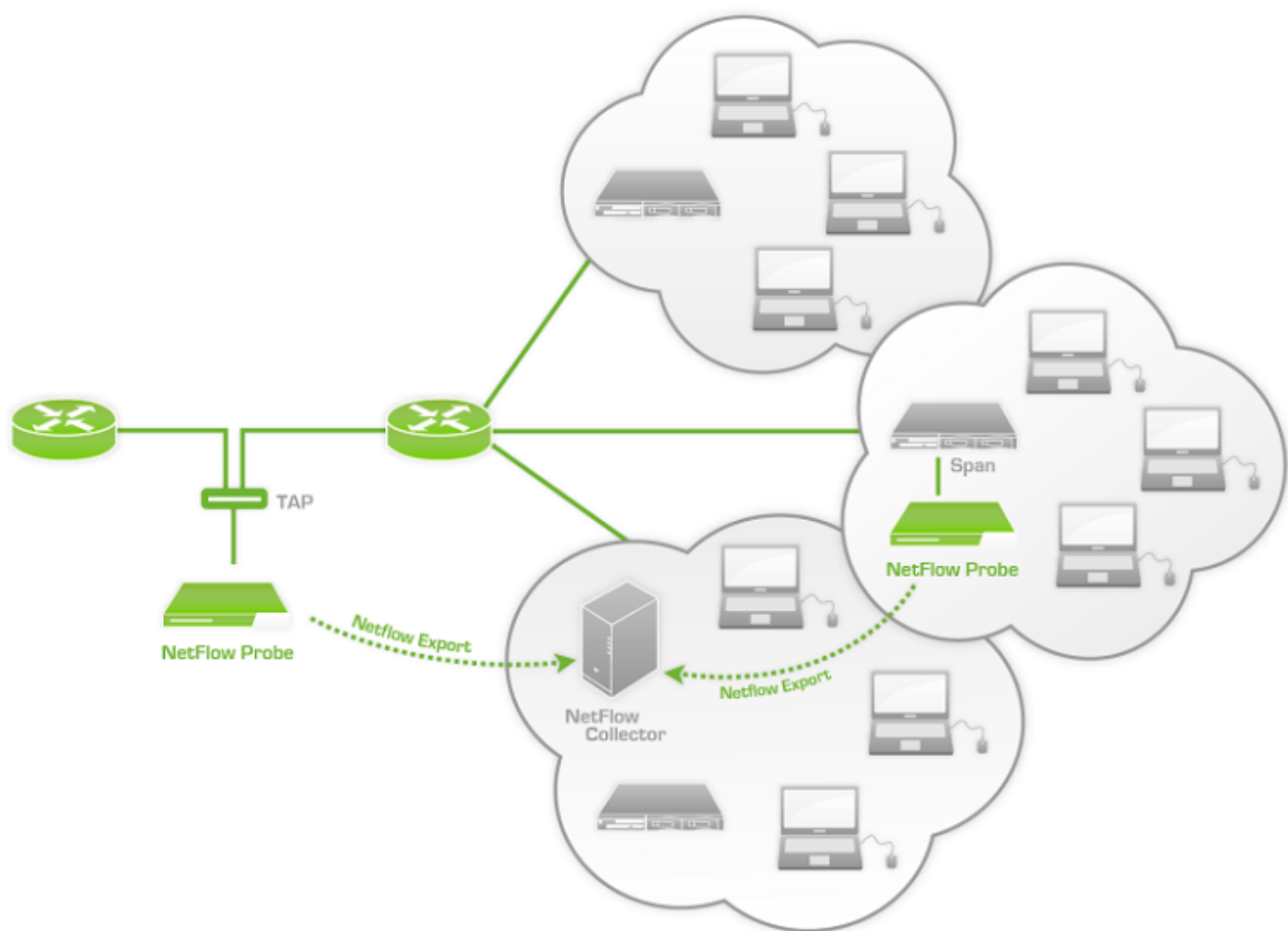
### **Collecteur Netflow**

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 surveillance Netflow.

### **Sonde Netflow**

Les sondes 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 démon nfcapd activé).



Dans notre blog, nous publions un article technique détaillé sur la construction d'une sonde Netflow avec une framboise de 60 Euro :

<https://pandorafms.com/blog/netflow-probe-using-raspberry/>

## 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. Ne le modifiez pas si vous ne savez pas exactement ce que vous faites.

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

Si vous voulez vérifier que `nfcapd` est correctement installé, vous pouvez essayer d'exécuter la commande suivante pour démarrer 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 paquet rpm, exécutez simplement la commande suivante, puis installez-le :

```
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
```

Qui devrait afficher des informations similaires à celles qui suivent :

```
Aggregated flows 1286
Top 10 flows ordered by packets:
Date flow start      Duration Proto      Src IP Addr:Port      Dst IP
Addr:Port  Packets  Bytes Flows
2011-12-22 20:41:35.697  901.035 TCP      192.168.60.181:50935 ->
192.168.50.2:22      2105  167388  4
2011-12-22 20:41:35.702  900.874 TCP      192.168.50.2:22      ->
192.168.60.181:50935  1275  202984  4
2011-12-22 20:48:15.057  1.347 TCP      157.88.36.34:80     ->
192.168.50.15:40044  496  737160  1
2011-12-22 20:48:14.742  1.790 TCP      91.121.124.139:80   ->
192.168.50.15:60101  409  607356  1
2011-12-22 20:46:02.791  76.616 TCP      192.168.50.15:80    ->
192.168.60.181:40500  370  477945  1
2011-12-22 20:48:15.015  1.389 TCP      192.168.50.15:40044 ->
157.88.36.34:80      363  22496  1
2011-12-22 20:46:02.791  76.616 TCP      192.168.60.181:40500 ->
192.168.50.15:80      303  24309  1
2011-12-22 20:48:14.689  1.843 TCP      192.168.50.15:60101 ->
91.121.124.139:80    255  13083  1
2011-12-22 20:48:14.665  1.249 TCP      178.32.239.141:80  ->
192.168.50.15:38476  227  335812  1
2011-12-22 20:48:21.350  0.713 TCP      137.205.124.72:80  ->
192.168.50.15:47551  224  330191  1
```

Top 10 flows ordered by bytes:

```
Date flow start      Duration Proto      Src IP Addr:Port      Dst IP
```



Addr:Port	Packets	Bytes	Flows		
2011-12-22 20:48:15.057	1.347	TCP	157.88.36.34:80	->	
192.168.50.15:40044	496	737160	1		
2011-12-22 20:48:14.742	1.790	TCP	91.121.124.139:80	->	
192.168.50.15:60101	409	607356	1		
2011-12-22 20:46:02.791	76.616	TCP	192.168.50.15:80	->	
192.168.60.181:40500	370	477945	1		
2011-12-22 20:48:14.665	1.249	TCP	178.32.239.141:80	->	
192.168.50.15:38476	227	335812	1		
2011-12-22 20:48:21.350	0.713	TCP	137.205.124.72:80	->	
192.168.50.15:47551	224	330191	1		
2011-12-22 20:48:15.313	1.603	TCP	89.102.0.150:80	->	
192.168.50.15:52019	212	313432	1		
2011-12-22 20:48:14.996	1.433	TCP	212.219.56.138:80	->	
192.168.50.15:36940	191	281104	1		
2011-12-22 20:51:12.325	46.928	TCP	192.168.50.15:80	->	
192.168.60.181:40512	201	245118	1		
2011-12-22 20:52:05.935	34.781	TCP	192.168.50.15:80	->	
192.168.60.181:40524	167	211608	1		
2011-12-22 20:41:35.702	900.874	TCP	192.168.50.2:22	->	
192.168.60.181:50935	1275	202984	4		

Summary: total flows: 1458, total bytes: 5.9 M, total packets: 15421, avg bps: 49574, avg pps: 15, avg bpp: 399

Time window: 2011-12-22 20:40:46 - 2011-12-22 20:57:21

Total flows processed: 1458, Records skipped: 0, Bytes read: 75864

Sys: 0.006s flows/second: 208345.2 Wall: 0.006s flows/second: 221177.2

Si ce système fonctionne, la prochaine chose à faire est de configurer Pandora FMS pour utiliser cette configuration.

### 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

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 nous le voulons.

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, nous 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.

Pour les versions 769 et antérieures :

Configuration » General ?

General settings

Language code	Español ▼
Remote configuration directory ⓘ	/var/spool/pandora/data_in
Phantomjs bin directory ⓘ	/usr/bin
Automatic login (hash) password	.....
Time source	System ▼
Automatically check for updates	<input checked="" type="checkbox"/>
Enforce https	<input checked="" type="checkbox"/>
Use SSL certificate	<input type="checkbox"/>
Attachment directory ⓘ	/var/www/html/pandora_console/attachment
IP list with API access	*
API password ⓘ	.....
Enable GIS features	<input checked="" type="checkbox"/>
<b>Enable Netflow</b>	<input checked="" type="checkbox"/>
Enable Network Traffic Analyzer	<input type="checkbox"/>

Pour la version 770 et les versions ultérieures :

Setup  
General i

**Enable GIS features**

**Enable Sflow**

**Timezone setup**  
America/Caracas ✎ America ▼ America/Caracas ▼

**Public URL** Force use Public URL

**Enable Netflow**

**General network path**  
/var/spool/pandora/data\_in/

E-mail test ✉ Update ✓

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

Pour les versions 769 et antérieures :

Configuration » Netflow

Data storage path ⓘ	<input type="text" value="/var/spool/pandora/data_in/netflow"/>
Daemon interval ⓘ	<input type="text" value="3600"/>
Daemon binary path	<input type="text" value="/usr/bin/nfcapd"/>
Nfdump binary path	<input type="text" value="/usr/bin/nfdump"/>
Nfexpire binary path	<input type="text" value="/usr/bin/nfexpire"/>
Maximum chart resolution ⓘ	<input type="text" value="50"/>
Disable custom live view filters ⓘ	<input type="checkbox"/>
Max. Netflow lifespan ⓘ	<input type="text" value="2"/>
Enable IP address name resolution ⓘ	<input type="checkbox"/>

Pour la version 770 et les versions ultérieures :

Setup  
Netflow

**Data storage path**  
netflow

**Daemon binary path**  
/usr/bin/nfcapd

**Nfdump binary path**  
/usr/bin/nfdump

**Nfexpire binary path**  
/usr/bin/nfexpire

**Maximum chart resolution**  
50

**Disable custom live view filters**

**Max. Netflow lifespan**  
5

**Enable IP address name resolution**

Update

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.
  - Pour les versions 769 et antérieures : Entrer le chemin d'accès complet.
  - Pour les versions 770 et ultérieures : Seulement le nom du répertoire, 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 : (*Version 769 ou antérieure*) L'intervalle de temps en secondes après lequel les fichiers de données sont tournés. Une valeur de 3600 est recommandée. Un intervalle plus grand signifie des fichiers potentiellement plus grands, ce qui signifie moins de surcharge d'E/S, mais ralentit également la recherche de données pour un intervalle spécifique.

*Version 770 ou supérieure :*

Si vous devez modifier la valeur par défaut de l'intervalle du démon (Daemon interval), procédez comme suit :

- Par le biais d'une session de ligne de commande ou de [l'interface DB](#), modifiez la valeur, en secondes, du jeton `netflow_interval`, par exemple pour la remplacer par 300 secondes : `UPDATE tconfig SET value = '300' where token = 'netflow_interval';`
- [Arrêtez le serveur PFMS](#).
- Ouvrez une fenêtre de terminal et supprimez les données générées avec l'intervalle ci-dessus avec `rm -i /var/spool/pandora/data_in/netflow`.
- Démarrez le serveur PFMS.

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.

Version 769 et antérieures : Le serveur NetFlow n'apparaîtra pas en tant que serveur dans la vue des serveurs de Pandora FMS, car il ne s'agit pas d'un serveur de Pandora FMS. À partir de la version 770, il apparaît dans la liste.

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` :

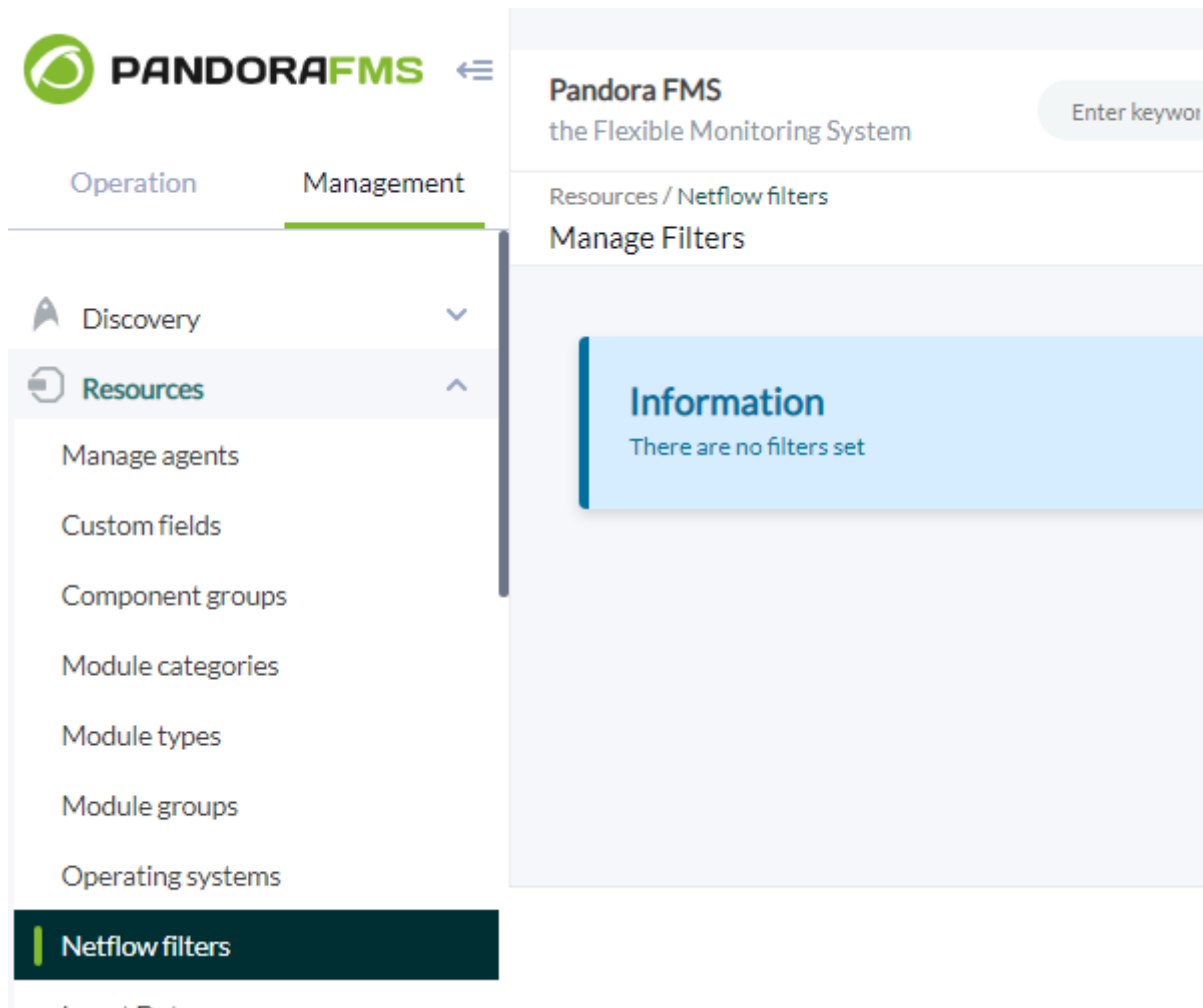
```
0 * * * * root yes 2>/dev/null | /usr/bin/nfexpire -e  
"/var/spool/pandora/data_in/netflow" -t X_days d
```

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*).

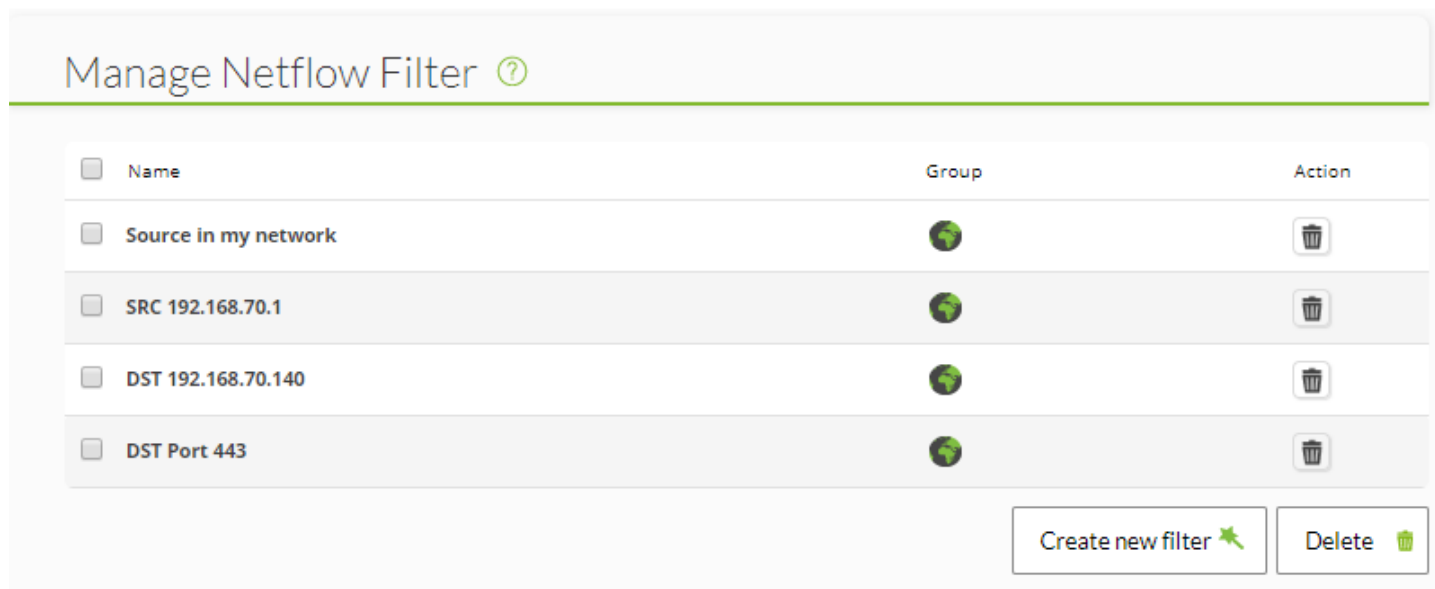
## Filtres

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.

## Création du filtre

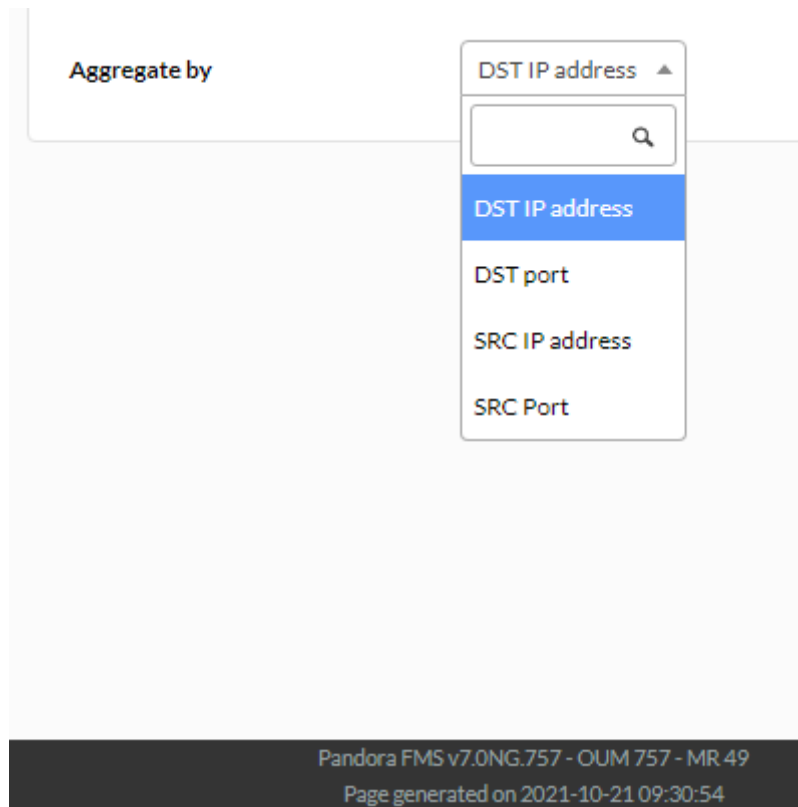
Ce serait une vue d'édition de base d'un filtre Netflow :

The screenshot shows the 'Netflow Filter' configuration window. The title bar contains 'Netflow Filter' with a help icon and a plus icon. The main form area contains the following fields:

- Name:** SRC 192.168.70.1
- Group:** All (dropdown menu)
- Filter:** Normal (selected radio button), Advanced (unselected radio button)
- DST IP:** (empty text input field)
- SRC IP:** 192.168.70.1
- DST port:** (empty text input field)
- SRC Port:** (empty text input field)
- Aggregate by:** SRC IP address (dropdown menu)

At the bottom right of the form is an 'Update' button with a refresh icon.

- Name : Il est conseillé que le nom du filtre soit descriptif.
- Group : Un utilisateur peut seulement créer un filtre ou modifier un filtre d'un groupe auquel il a accès.
- Filter : Il existe deux types de filtres, les filtres de base et les filtres avancés. Le filtre avancé vous permet d'entrer des expressions avancées dans le même format que nfdump. Le filtre de base vous permet de filtrer le trafic par IP source SRC IP address, IP destination DST IP address, Port source SRC Port et Port destination DST port. Les listes valides sont des listes d'adresses IP (si elles sont laissées vides, toutes les adresses IP seront affichées), ainsi que des listes de ports (de même, si elles sont laissées vides, tous les ports seront affichés), séparées par des virgules.
- Aggregate by : Le trafic sera regroupé selon l'un de ces critères :
  - DST IP address : affiche le trafic pour chaque IP d'origine différente.
  - DST port : affiche le trafic pour chaque IP de destination différente.
  - SRC IP address : Agrupa el tráfico para cada puerto de origen diferente.
  - SRC Port : le trafic pour chaque port d'origine différente est affiché.



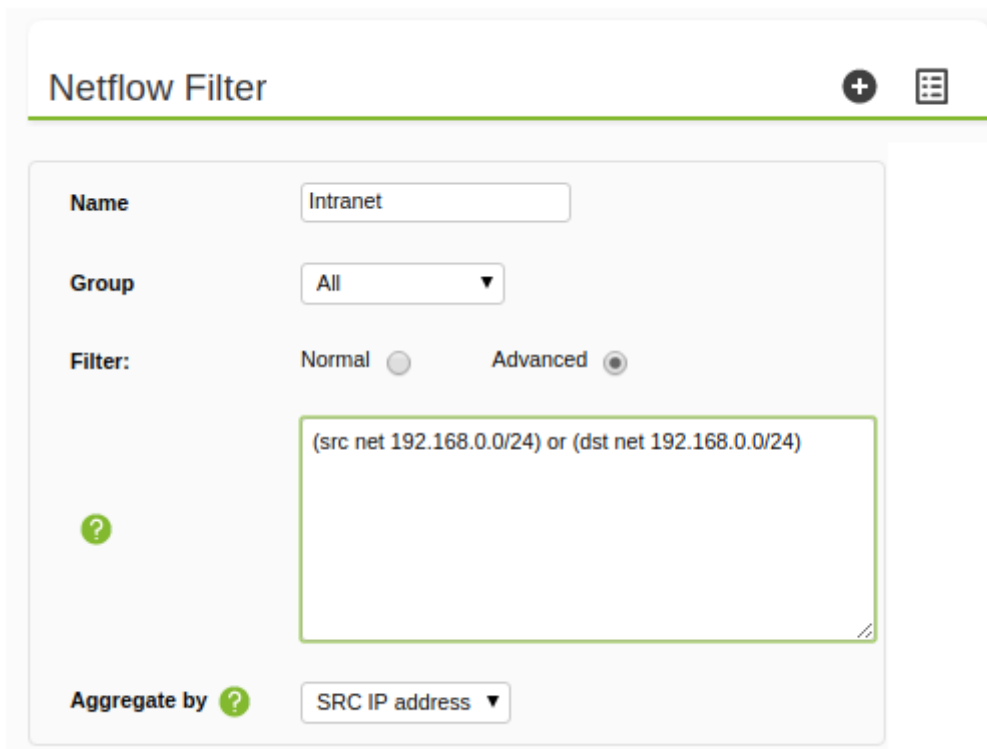
## Exemples

Par exemple, ce serait un filtre de base pour le trafic Web :

The image shows a screenshot of the 'Netflow Filter' configuration form in Pandora FMS. The form has a title 'Netflow Filter' and a plus sign icon. The form contains the following fields:

- Name:** DST 443,80
- Group:** All
- Filter:** Normal (selected), Advanced
- DST IP:** (empty)
- SRC IP:** (empty)
- DST port:** 443,80
- SRC Port:** (empty)
- Aggregate by:** DST port

Ou par exemple un filtre avancé pour le trafic vers et depuis un intranet :



**Netflow Filter**

Name: Intranet

Group: All

Filter: Normal  Advanced

(src net 192.168.0.0/24) or (dst net 192.168.0.0/24)

Aggregate by: SRC IP address

Plus d'exemples de filtres avancés :

- Capture du trafic entrant ou sortant depuis 192.168.0.1 :

```
hôte 192.168.0.1
```

- Capturer le trafic entrant au 192.168.0.1 :

```
dst host 192.168.0.1
```

- Capturer le trafic sortant du 192.168.0.0.0/24 :

```
src net 192.168.0.0.0/24
```

\* Capturer le trafic HTTP et HTTPS (habituellement ports 80 et 443) :

```
(port 80) or (port 443)
```

- Capturer tout le trafic à l'exception du DNS (53) :

```
port not 53
```

- Capturer le trafic vers 192.168.0.1 du protocole SSH (habituellement port 22) :

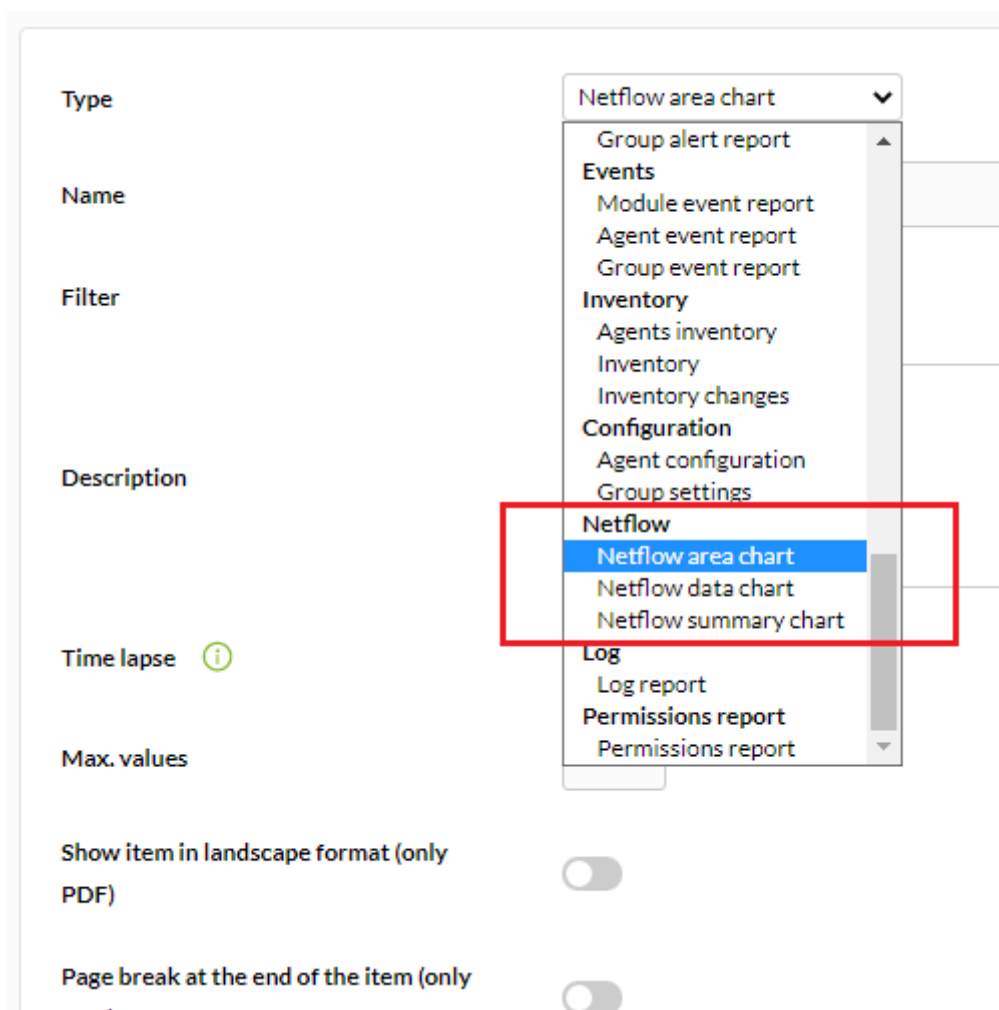
```
(port 22) and (host dst 192.168.0.1)
```

## Rapports

Les rapports Netflow sont intégrés aux rapports Pandora FMS (voir [Informes](#) pour plus

d'informations).

Pour créer un élément d'état, sélectionnez l'un des éléments d'état Netflow disponibles.



The image shows a configuration window for creating a status item. On the left, there are fields for 'Type', 'Name', 'Filter', 'Description', 'Time lapse' (with an information icon), 'Max. values', and two toggle switches for 'Show item in landscape format (only PDF)' and 'Page break at the end of the item (only ---)'. On the right, a dropdown menu is open, displaying a list of status item types. The 'Netflow' section is highlighted with a red box, and 'Netflow area chart' is selected and highlighted in blue. Other categories in the list include 'Group alert report', 'Events', 'Inventory', 'Configuration', 'Log', and 'Permissions report'.

Field	Value
Type	Netflow area chart
Name	
Filter	
Description	
Time lapse	
Max. values	
Show item in landscape format (only PDF)	<input type="checkbox"/>
Page break at the end of the item (only ---)	<input type="checkbox"/>

- Group alert report
- Events
  - Module event report
  - Agent event report
  - Group event report
- Inventory
  - Agents inventory
  - Inventory
  - Inventory changes
- Configuration
  - Agent configuration
  - Group settings
- Netflow**
  - Netflow area chart**
  - Netflow data chart
  - Netflow summary chart
- Log
  - Log report
- Permissions report
  - Permissions report

Et l'installer. Les options de configuration suivantes sont disponibles :

The screenshot shows a configuration form for a 'Netflow area chart'. The fields are as follows:

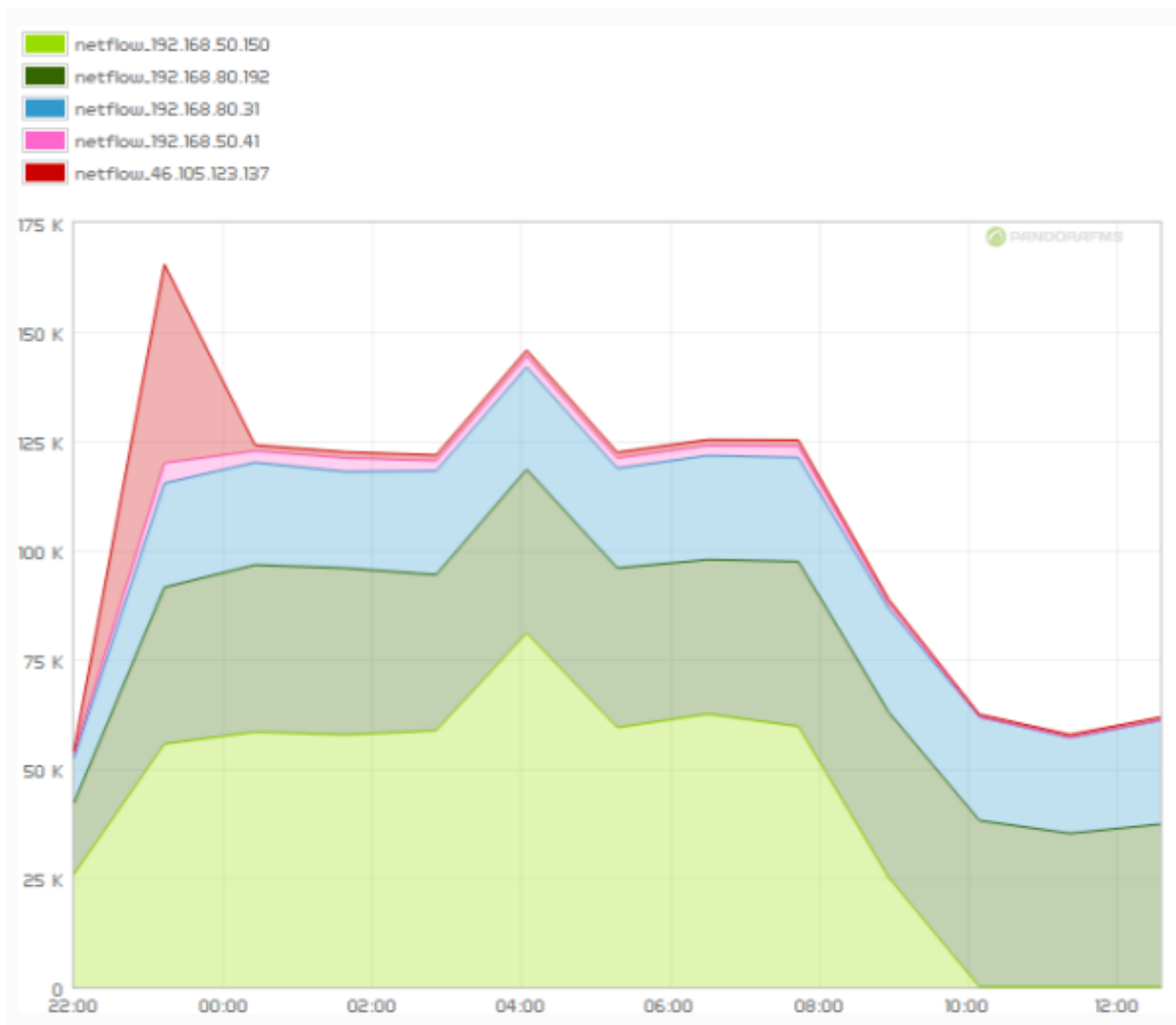
- Type:** Netflow area chart (dropdown menu)
- Name:** (empty text input field)
- Filter:** DST 192.168.70.140 (dropdown menu)
- Description:** (empty text area)
- Time lapse:** 1 day (dropdown menu)
- Max. values:** 0 (text input field)
- Show item in landscape format (only PDF):** (disabled toggle switch)
- Page break at the end of the item (only PDF):** (disabled toggle switch)

At the bottom right of the form is a 'Create item' button with a green star icon. Below the form, a footer bar contains the text: 'Pandora FMS v7.0NG.757 - OUM 757 - MR 49' and 'Page generated on 2021-10-21 10:15:32'.

- Type : Les types d'éléments seront expliqués ci-dessous.
- Filter : Filtre Netflow à utiliser.
- Description : Description de l'élément.
- Period : Longueur de la plage de données à afficher.
- Resolution : Certains rapports exigent que des échantillons soient prélevés à chaque certaine période. Ce paramètre permet de définir le nombre d'échantillons. La résolution peut être basse (6 échantillons), moyenne (12 échantillons), haute (24 échantillons) ou ultra haute (30 échantillons). Il y a deux valeurs spéciales (*horaire et journalier* de sorte qu'une valeur fixe d'échantillons n'est pas collectée mais une à chaque période déterminée).
- 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 les valeurs Max. sont définies sur 5, seules 5 adresses IP seront affichées.

Il existe trois types d'éléments de reporting Netflow :

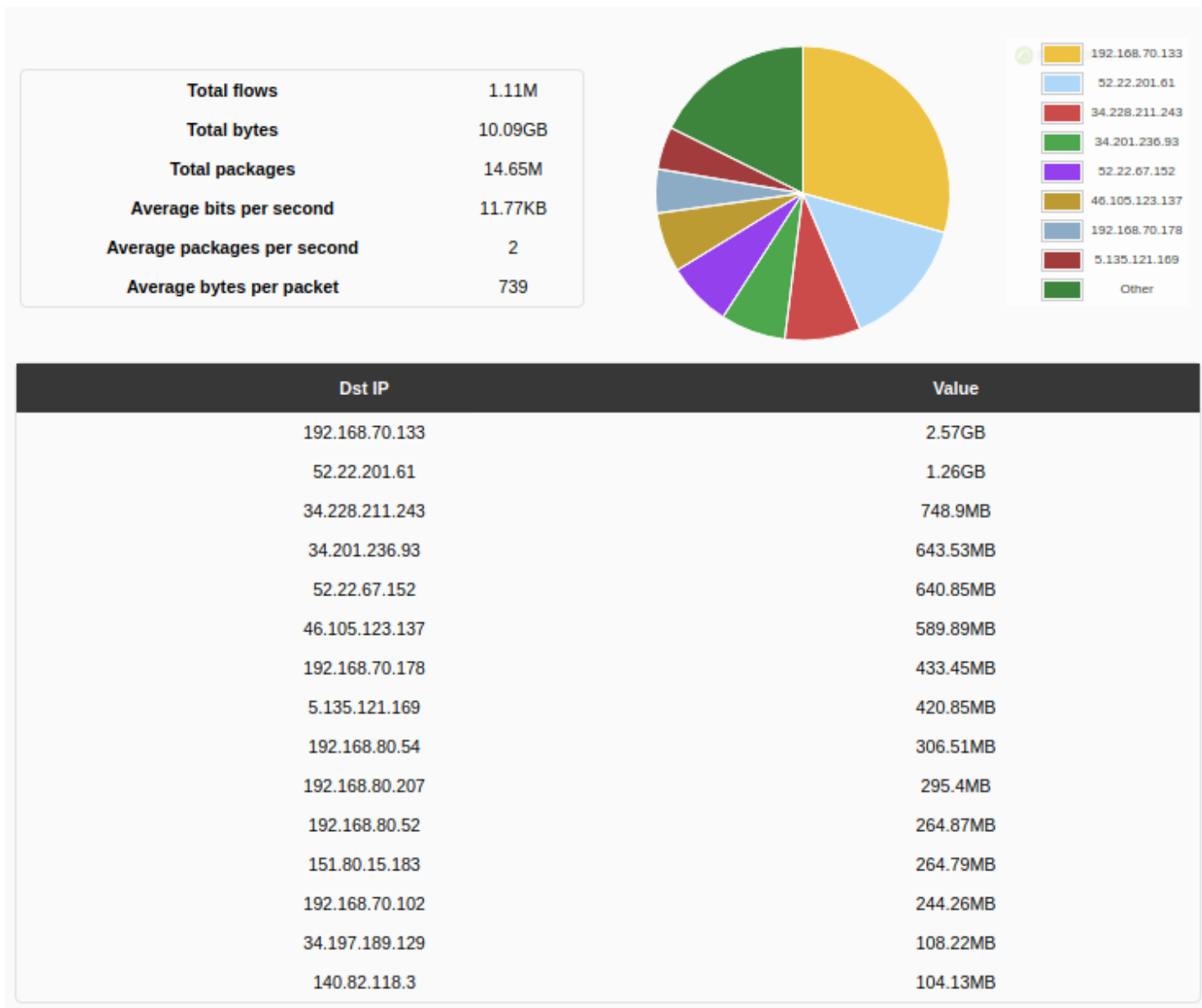
- Netflow area chart : Un graphique de zone, agrégé ou non agrégé.



- Netflow data chart : Représentation textuelle du graphique de zone.

Timestamp	192.168.50.150	192.168.80.192	192.168.80.31	192.168.50.41	46.105.123.137	192.168.80.207
22:00	107.48MB	68.4MB	42.4MB	4.18MB	2.63MB	16.42KB
23:12	231.93MB	149.59MB	99.37MB	19.2MB	189.5MB	51.13KB
00:25	243.36MB	159.52MB	97.77MB	10.92MB	5.64MB	295.38MB
01:38	240.64MB	159.17MB	92.06MB	12.88MB	5.75MB	47.24KB
02:51	244.72MB	148.73MB	99.16MB	9.51MB	5.48MB	56.48KB
04:04	337.9MB	156.11MB	97.5MB	10.62MB	5.71MB	49.42KB
05:17	247.55MB	152.34MB	95.19MB	9.57MB	5.55MB	53.33KB
06:29	260.56MB	147.26MB	99.37MB	9.63MB	5.5MB	3.19MB
07:42	248.66MB	157.46MB	99.18MB	10.95MB	5.77MB	47.74KB
08:55	104.08MB	157.98MB	98.99MB	4.65MB	4.01MB	39.14KB
10:08	53.57KB	158.83MB	98.69MB	284.7KB	2.4MB	47.97KB
11:21	59.4KB	146.61MB	91.24MB	275.65KB	2.65MB	132.61KB
12:34	65.48KB	155.42MB	98.85MB	283.54KB	2.89MB	68.19KB

- Netflow summary chart : récapitulatif du trafic pour la période donnée. Il y a trois éléments : un tableau avec des informations globales, un camembert avec les adresses IP ou ports les plus pertinents et un tableau avec les mêmes informations que le camembert ventilé.



## Visualisation en temps réel

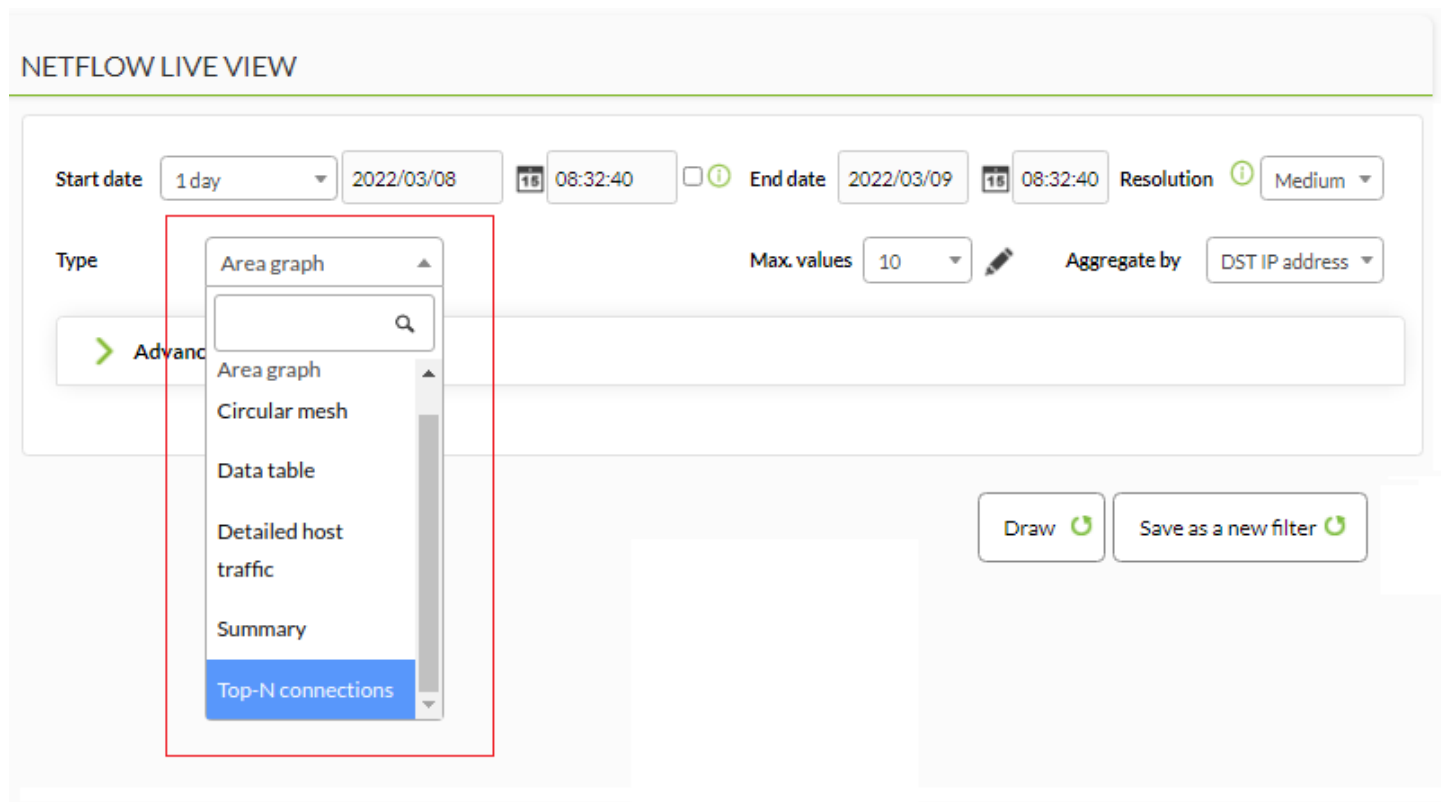
Cette vue permet de consulter l'historique des données capturées à partir de différents filtres de recherche. Vous pouvez utiliser des filtres et différentes façons d'afficher les informations. Il est nécessaire de définir la manière de regrouper les informations affichées, ainsi que la manière d'obtenir ces informations afin de commencer à visualiser les données.

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



The screenshot displays the Pandora FMS Enterprise web interface. At the top left is the Pandora FMS logo. The main navigation menu on the left includes: Monitoring, Topology maps, Reporting, Events, Workspace, Tools, Discovery, Resources, Profiles, Configuration, Alerts, Events, Servers, Setup, Admin tools, Links, Update manager, and Module library. A sub-menu for 'Views' is open, listing: Inventory, Network, Log viewer, SNMP, Cluster view, AWS View, SAP view, and VMware view. The 'Network' option is selected, showing a secondary sub-menu with: Netflow explorer, Netflow Live View, and Network usage map. The 'Netflow Live View' option is highlighted. At the top right, there are date and time filters: Start date (1 years 1 days, 2020/11/07, 14:14:09) and End date. A 'Max. values' dropdown is also visible. The footer contains the text: Pandora FMS v7.0NG.758 - OUM 758 - MR 50, Page generated on 2021-11-08 14:15:41.

Allez dans [Rapports](#) et [Filtres](#) pour apprendre à configurer les options de vue en temps réel.

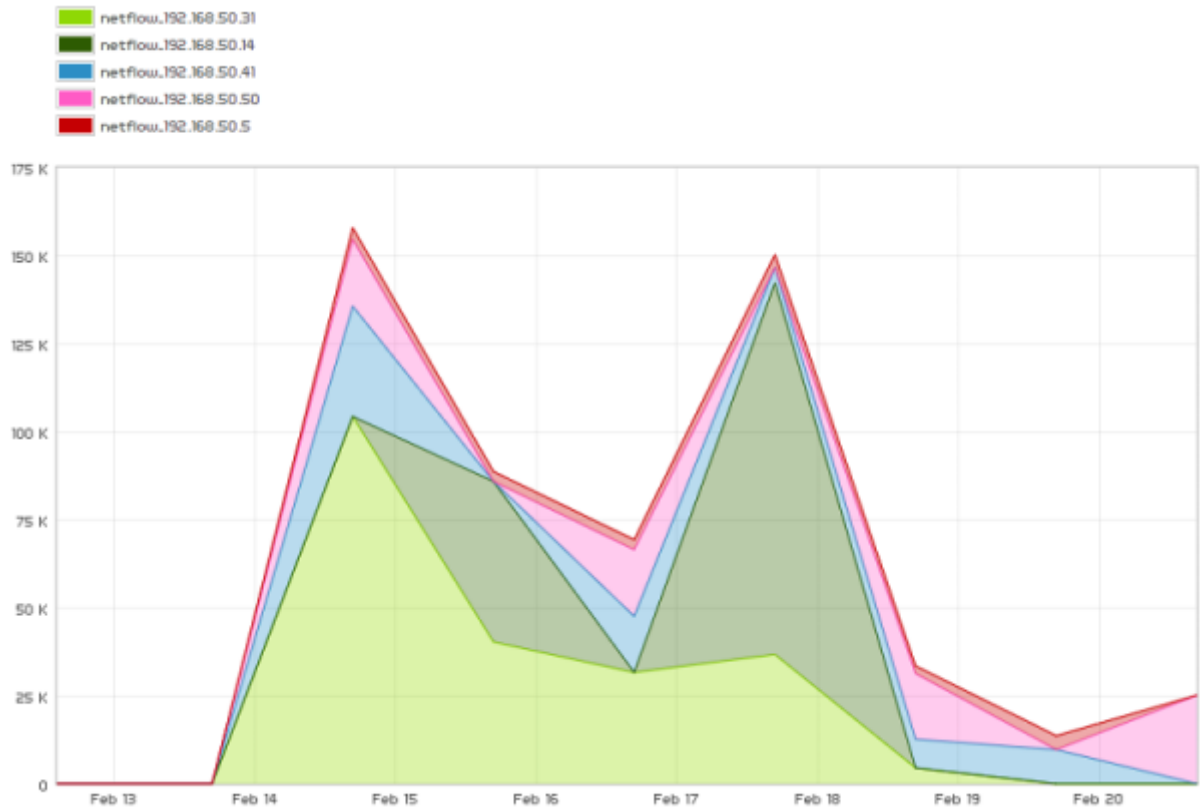


The screenshot displays the 'NETFLOW LIVE VIEW' interface. At the top, there are controls for 'Start date' (1 day, 2022/03/08, 08:32:40) and 'End date' (2022/03/09, 08:32:40), along with a 'Resolution' dropdown set to 'Medium'. Below this, the 'Type' dropdown is open, showing options: 'Area graph', 'Circular mesh', 'Data table', 'Detailed host traffic', 'Summary', and 'Top-N connections'. The 'Top-N connections' option is highlighted in blue. To the right of the dropdown, there are 'Max. values' (10) and 'Aggregate by' (DST IP address) controls. At the bottom right, there are 'Draw' and 'Save as a new filter' buttons.

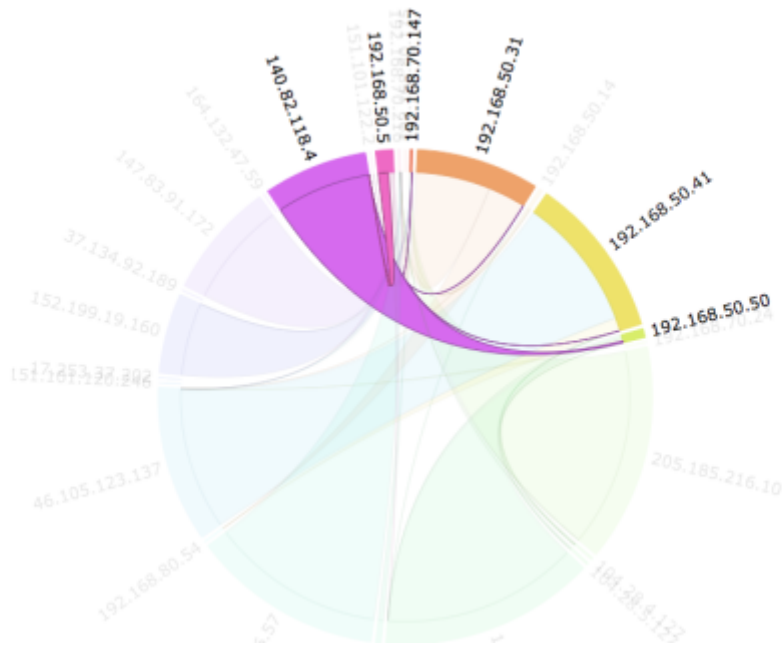
La façon d'obtenir l'information peut être par : IP source, IP destination, Port source ou Port destination. Si vous choisissez, par exemple, d'afficher les informations IP de destination, les informations ordonnées par les IP ayant le plus de trafic vers la destination de la plus haute à la plus basse seront affichées. Il en va de même pour connaître la consommation de votre réseau par protocole, choisir par port de destination.

Les possibilités de visualisation sont les suivantes :

- Area graph (type *stacked*) : Il montre dans le temps (de la date d'origine à la date de destination), l'évolution des données. Vous devez choisir le niveau de précision du graphique dans le jeton " Résolution ".



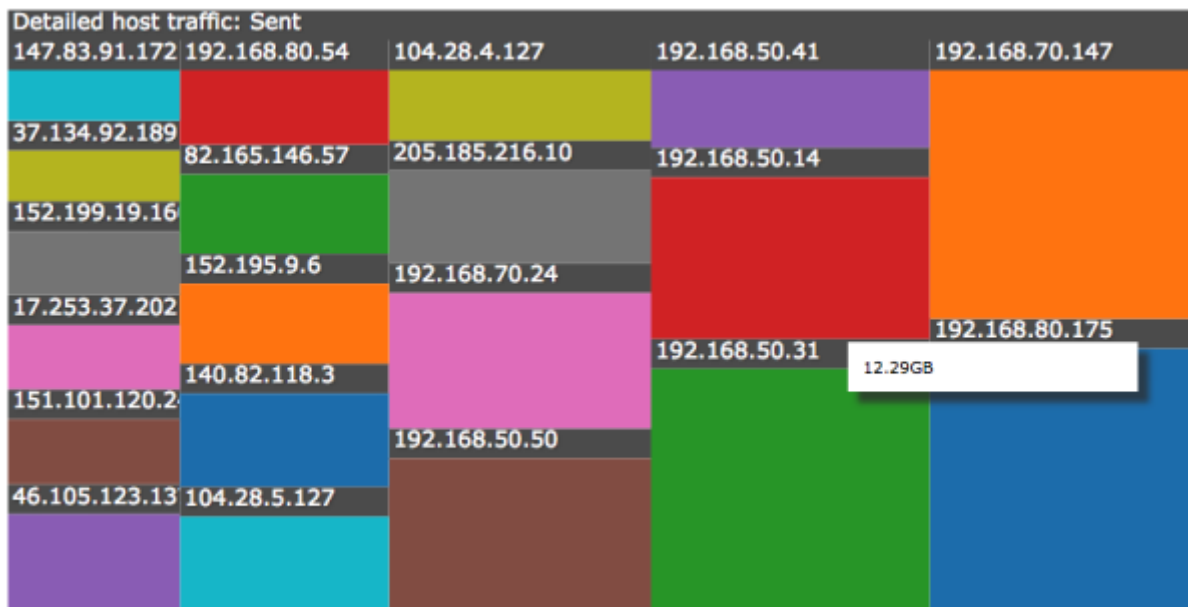
- Circular mesh (Graphique circulaire) : Affiche un graphique circulaire interactif représentant les paires de connexions entre l'IP et le volume de trafic.



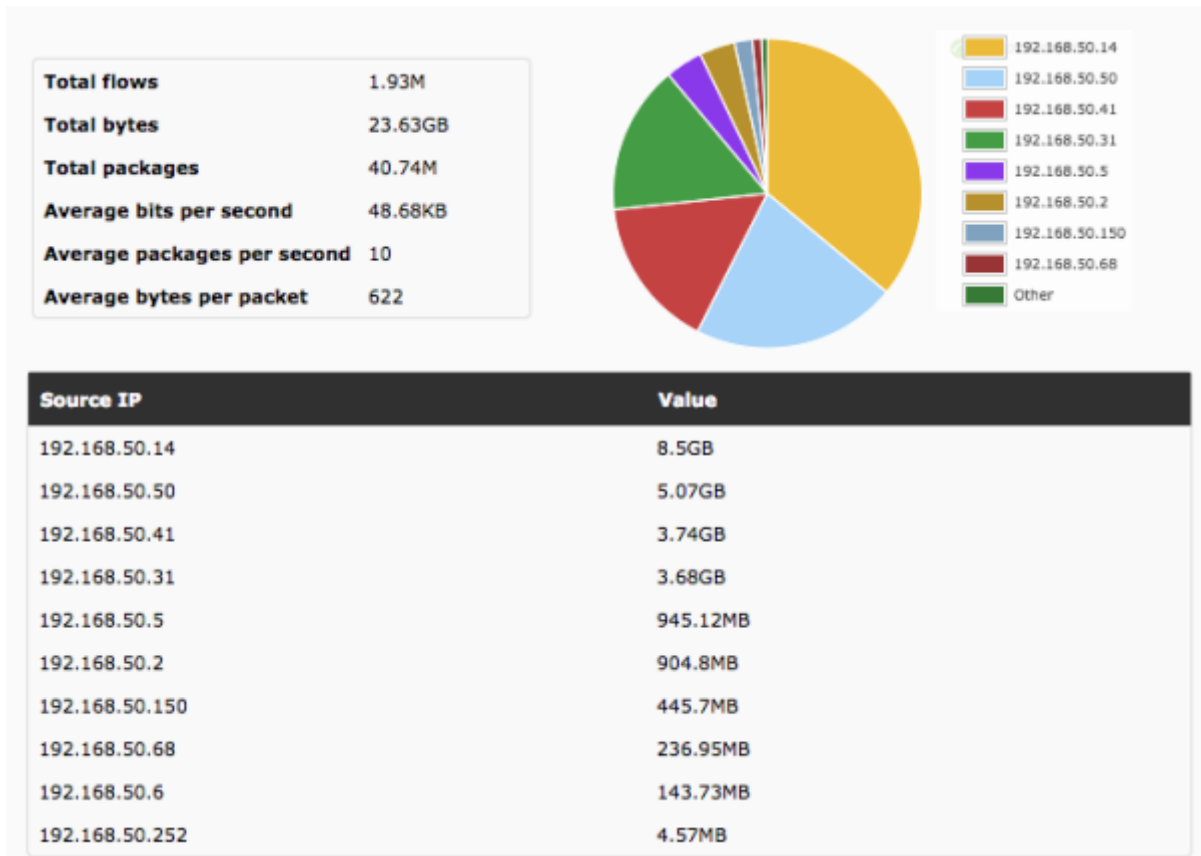
- Data table (Tableau de données) : Affiche un tableau de données avec chaque IP et un nombre de lignes en fonction de la résolution choisie.

Timestamp	192.168.50.14	192.168.50.50	192.168.50.41	192.168.50.31	192.168.50.5	192.168.50.2	192.168.50.150	192.168.50.68	192.168.50.6	192.168.50.252
Jan 25 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Jan 30 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 04 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 09 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 14 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 19 17h	8.5GB	5.07GB	3.74GB	3.68GB	945.09MB	904.52MB	443.13MB	236.24MB	137.35MB	4.57MB
Feb 24 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 01 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 06 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 11 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 16 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 21 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 26 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B

- Detailed host traffic (Détailé) : Il affiche une carte des portions représentant le trafic par IP.



- Summary (Résumé) : Affiche un tableau récapitulatif, un gâteau et un tableau avec les données de la période entière.



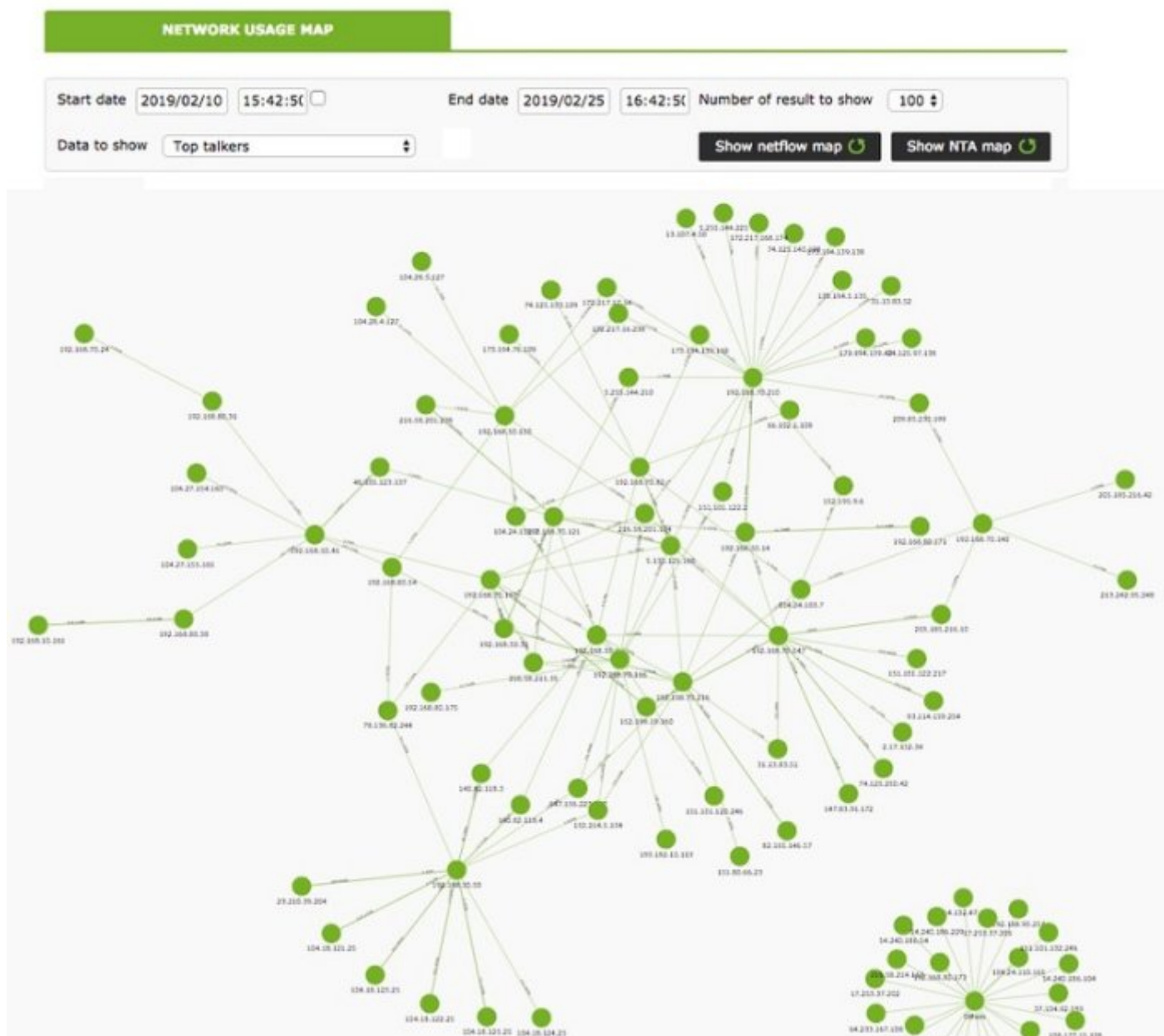
- Top-N connections (Premières N connexions) : Une table qui montre le TOP-N de connexions entre paires d'IP d'origine - IP destination, basé sur le trafic entre lesdites adresses IP ( la somme des pourcentages des N éléments de la table ne sera pas cent parce qu'il y a beaucoup d'autres paires de connexions src/dst qui ne se trouvent pas sur la table).

<b>Total flows</b>	232.81K
<b>Total bytes</b>	102.52MB
<b>Total packages</b>	107.86M
<b>Average bits per second</b>	92.25KB
<b>Average packages per second</b>	11.85K
<b>Average bytes per packet</b>	0

Source IP	Destination IP	Bytes	% Traffic	Avg. Throughput
59.220.158.122:9221	10.12.233.210:53	7.4MB	7.22 %	6.66 Kbps
172.30.20.102:9010	62.12.190.10:993	7.38MB	7.20 %	6.64 Kbps
247.104.20.202:40	10.12.190.10:123	7.31MB	7.13 %	6.58 Kbps
112.10.20.10:40	172.30.190.10:80	7.3MB	7.12 %	6.57 Kbps
192.168.20.10:40	202.12.190.10:443	7.28MB	7.10 %	6.55 Kbps
10.10.20.122:12001	84.12.190.210:8080	7.24MB	7.07 %	6.52 Kbps
10.154.20.12:9010	77.12.190.94:3306	7.2MB	7.02 %	6.48 Kbps
192.168.20.202:40	42.12.190.10:6682	6.9MB	6.73 %	6.21 Kbps
112.10.100.10:40	192.168.120.10:21	6.89MB	6.72 %	6.2 Kbps
172.30.20.102:40	222.12.190.10:22	6.89MB	6.72 %	6.2 Kbps

## Cartes de trafic réseau

Il s'agit d'une nouvelle fonctionnalité introduite dans OUM 733 qui sera améliorée à l'avenir. Il crée des cartes réseau dynamiques, basées sur le trafic entre les nœuds. Il montre la relation (les connexions) entre les différentes directions, montrant les N connexions les plus importantes (par 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 au suivant.

```
#!/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

Version 770 ou ultérieure.

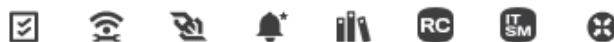
À partir de la version 770 de Pandora FMS, la prise en charge de **sFlow**, un protocole réseau qui est une norme industrielle dans la fabrication de matériel pour le trafic des réseaux de données, est incluse.

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.



<b>Data storage path</b> <input type="text" value="netflow"/>	<b>Daemon binary path</b> <input type="text" value="/usr/bin/nfcapd"/>
<b>Nfdump binary path</b> <input type="text" value="/usr/bin/nfdump"/>	<b>Nfexpire binary path</b> <input type="text" value="/usr/bin/nfexpire"/>
<b>Maximum chart resolution</b> <input type="text" value="50"/>	<b>Disable custom live view filters</b> <input type="checkbox"/>
<b>Max. Netflow lifespan</b> <input type="text" value="5"/>	<b>Enable IP address name resolution</b> <input type="checkbox"/>
<b>Enable Sflow</b> <input checked="" type="checkbox"/>	

Un nouvel onglet sera activé spécifiquement pour sFlow :

Setup  
Sflow               

<b>Data storage path</b> <input type="text" value="sflow"/>	<b>Daemon interval</b> <input type="text" value="10"/>
<b>Daemon binary path</b> <input type="text" value="/usr/bin/sfcapd"/>	<b>Nfdump binary path</b> <input type="text" value="/usr/bin/nfdump"/>
<b>Nfexpire binary path</b> <input type="text" value="/usr/bin/nfexpire"/>	<b>Maximum chart resolution</b> <input type="text" value="50"/>
<b>Disable custom live view filters</b> <input type="checkbox"/>	<b>Sflow max lifetime</b> <input type="text" value="5"/>
<b>Enable IP address name resolution</b> <input type="checkbox"/>	

- 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](#)