Monitorización de red con NetFlow y sFlow

Monitorización de red con NetFlow y sFlow

Introducción al análisis de red en tiempo real

Pandora FMS utiliza una herramienta para analizar la red en tiempo real: NetFlow® y sFlow®. Utiliza el principio de "*escuchar*" por Ethernet de manera continua y analizar el tráfico para generar estadísticas.

Para interceptar el tráfico de la red y poder analizarlo, hace falta tener acceso físico a esa red, ya que el punto de captura de la red debe ser el más apropiado. Para capturar dichos datos se debe redirigir el tráfico de un puerto del *switch* a otro puerto mediante un "port-mirror". No todos los dispositivos de red permiten hacerlo (sólo los de gama media/alta). También se puede hacer un *port-mirror* en algunos *firewalls* comerciales. Es la forma más sencilla de interceptar el tráfico y no requiere hardware adicional. Al enviar todo el tráfico hacia un puerto, ese puerto se conecta directamente al analizador de red (sonda).

Estos *switchs* y/o *firewall* de gama alta permiten realizar la monitorización de manera más sencilla. Esto se debe a que estos dispositivos envían la información estadística del flujo de red directamente al recolector de Pandora FMS sin necesidad de usar una sonda independiente. Se debe consultar las características del hardware para saber si puede habilitar NetFlow y/o sFlow y enviar los flujos a un colector independiente (en este caso, el colector de Pandora FMS).

Monitorización de red con NetFlow

Pandora FMS es capaz de monitorizar el tráfico IP haciendo uso del protocolo NetFlow.

NetFlow® es un protocolo de red, desarrollado por Cisco Systems® y actualmente está soportado para varias plataformas además de Cisco IOS® y NXOS®, como por ejemplo en dispositivos de fabricantes como Juniper®, Enterasys Switches®, y en sistemas operativos como Linux®, FreeBSD®, NetBSD® y OpenBSD®.

Protocolo NetFlow

Los dispositivos con NetFlow habilitado, cuando activan esta característica, generan "registros de netflow" que consisten en pequeños fragmentos de información que envían a un dispositivo central (un servidor o un colector NetFlow), el cual recibe información de los dispositivos (sondas NetFlow) para almacenarla y procesarla.

Esa información se transmite mediante el protocolo NetFlow, basado en UDP o SCTP. Cada registro de NetFlow es un pequeño paquete que contiene una cantidad mínima de información, pero en

ningún caso contiene los datos en bruto del tráfico. Es decir, no envía el *payload* del tráfico que circula por el colector, únicamente los datos estadísticos.

La definición tradicional de Cisco es utilizar una clave de 7 elementos:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto UDP o TCP de origen.
- Puerto UDP o TCP de destino.
- Protocolo IP.
- Interfaz (SNMP ifIndex)
- Tipo de servicio IP

Con el tiempo, otros fabricantes han diseñado sistemas equivalentes para sus dispositivos de red, con diferentes nombres pero propósito similar:

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

Colector NetFlow

Se trata de un dispositivo (PC o servidor) ubicado en la red para recoger toda la información de NetFlow que es enviada desde los *routers* y *switches*.

NetFlow genera y recoge esta información, pero se necesita un software que permita almacenar y analizar dicho tráfico. Con Pandora FMS se utiliza un servidor especial para este propósito, que Pandora FMS iniciará y detendrá cuando se arranque Pandora. Este servidor se llama nfcapd y es necesario instalarlo para poder usar monitorización NetFlow.

Sonda NetFlow

Las sondas (por ejemplo en Raspberry) son generalmente *routers* con NetFlow habilitado, configurado, y enviando información al colector NetFlow (que en este caso será el servidor de Pandora FMS con el demonio nfcapd habilitado).

Requisitos e instalación

Pandora FMS utiliza una herramienta OpenSource llamada nfcapd (perteneciente al paquete nfdump) para procesar todo el tráfico NetFlow. Este *daemon* lo inicia de forma automática el

servidor de Pandora FMS. Este sistema almacena los datos en ficheros binarios, en una ubicación determinada. Debe instalar nfcapd en su sistema antes de poder trabajar con NetFlow en Pandora FMS.

El *daemon* nfcapd por defecto escucha en el puerto 9995/UDP, por lo que tendrá que tenerlo en cuenta si tiene cortafuegos y así abrir este puerto, y a la hora de configurar sus sondas NetFlow.

Instalación de nfcapd

La instalación de nfcapd debe hacerse manualmente, pues Pandora FMS no lo instalará. Para más información, vaya a la página oficinal del proyecto nfcapd.

Pandora FMS por defecto usa el directorio `/var/spool/pandora/data_in/netflow` para procesar la información, de manera que cuando arranque nfcapd utilizará este directorio. Evite modificar esta vía de ubicación, a menos que sea estrictamente necesario y tenga pleno conocimiento de ello.

Es necesario que instale la version 1.6.8p1 de nfdump para
poder usarla con Pandora FMS

Si quiere comprobar que nfcapd esté correctamente instalado, ejecute el siguiente comando para iniciar el proceso en primer plano:

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

Si todo va bien, debería obtener una salida similar a esta:

```
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
```

Tenga en cuenta que es necesario que Pandora FMS, y en concreto el servidor WEB que ejecuta la consola, tenga acceso a esos ficheros de datos. En este ejemplo están en:

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

Instalación de sondas

Si no dispone de un *router* con NetFlow, pero su tráfico pasa por un sistema GNU/Linux, puede instalar un software que actúe de sonda y envíe información de tráfico NetFlow al *colector*.

Instalando fprobe

fprobe captura el tráfico y lo reenvía a un servidor NetFlow. Con él puede generar tráfico NetFlow, de todo el tráfico de red que pasa por sus interfaces.

Para descargar el paquete RPM basta con ejecutar el siguiente comando, y posteriormente instalarlo:

```
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
```

Por ejemplo, ejecutando el siguiente comando se enviará todo el tráfico del interfaz `eth0` al colector NetFlow escuchando en el puerto 9995 de la dirección IP `192.168.70.185`:

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

Una vez generado tráfico, podrá ver estadísticas del mismo en el colector NetFlow con el comando:

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

Instalando pmacct

Experimental.

Entre muchas características de la sonda pmacct están la capacidad de trabajar con NetFlow v1/v5/v7/v8/v9 y sFlow v2/v4/v5 sobre IPv4 e IPv6.

El código fuente está alojado en:

https://github.com/pmacct/pmacct

Rocky Linux 8

Instale las dependencias con derechos de administrador:

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

Descargue el código fuente de pmacct (puede utilizar curl en vez de wget) y compile:

```
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
```

Inicie pmacct como sonda NetFlow en modo *daemon*:

- Cree una configuración para pmacct.

Por ejemplo, se enviará todo el tráfico del interfaz `eth0` al colector NetFlow escuchando en el puerto `9995` de la dirección 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
```

- Inicie pmacctd:

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

Como operar con NetFlow en Pandora FMS

Pandora FMS trabaja con NetFlow como un sistema auxiliar, es decir, no almacena la información de NetFlow en la base de datos. Pandora FMS muestra esta información como informes solicitados bajo demanda.

Pandora FMS opera con NetFlow usando conjuntos de reglas para visualizar un tráfico determinado. Estas reglas pueden ser algo tan sencillo como “Todo el tráfico de la red 192.168.70.0/24” o algo más complejo usando expresiones pcap.

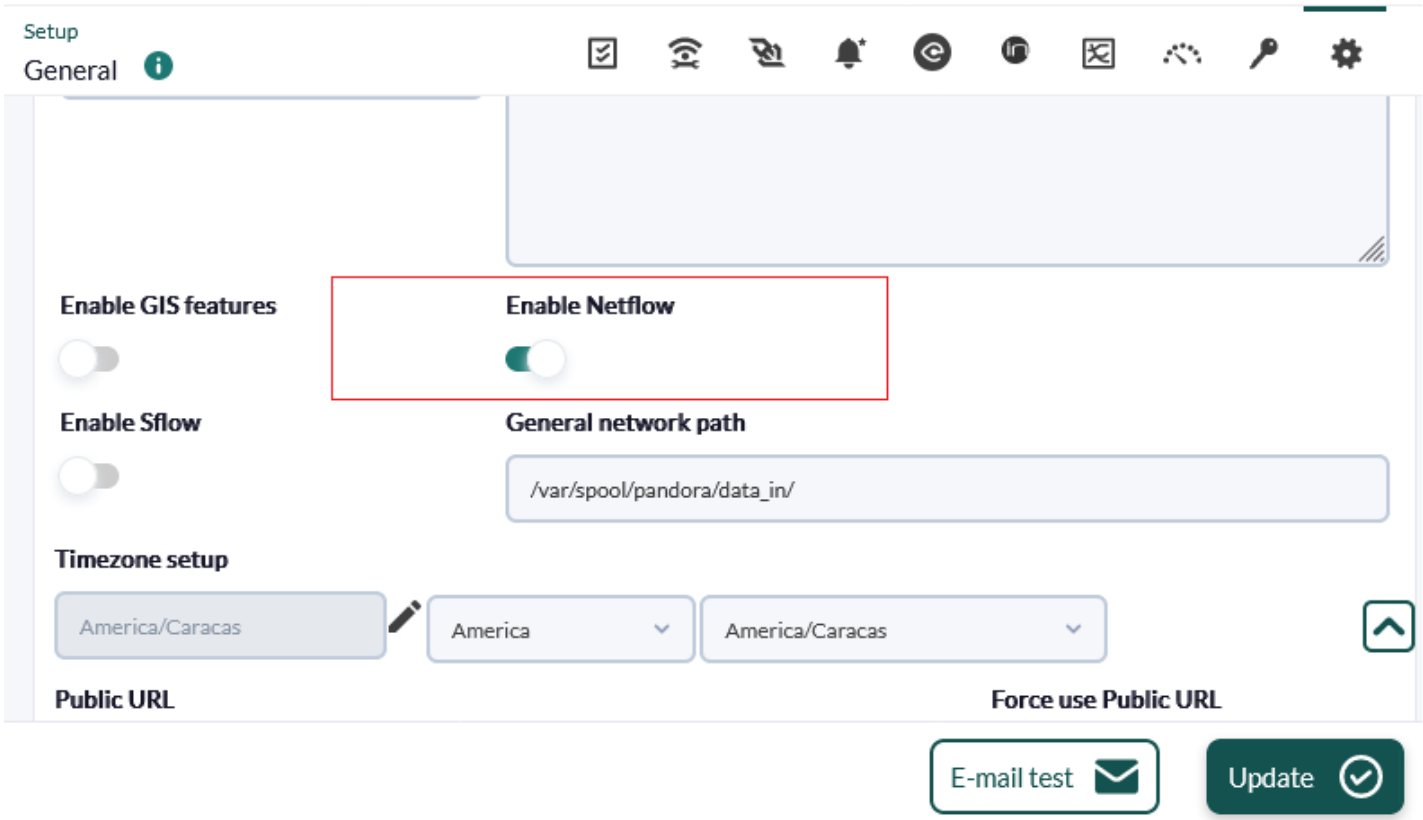
Una vez definidos los filtros, se definen los informes que determinan cómo visualizar los datos (gráficas, listas…) y el intervalo de tiempo. Al definir filtros e informes se deja definida esa información, de forma similar a como se opera con los informes de Pandora FMS, para utilizarla bajo demanda cuando se necesite. Los informes NetFlow aparecerán también como “tipo de informe” en la sección de Informes personalizados de Pandora FMS, para poderlos incorporar a los informes normales de Pandora FMS.

Por otro lado, se dispone de una consola de vista “*en tiempo real*” para analizar el tráfico, componiendo directamente las reglas. Es útil para investigar problemas, ver gráficas puntuales que no corresponden a un filtro determinado, etcétera.

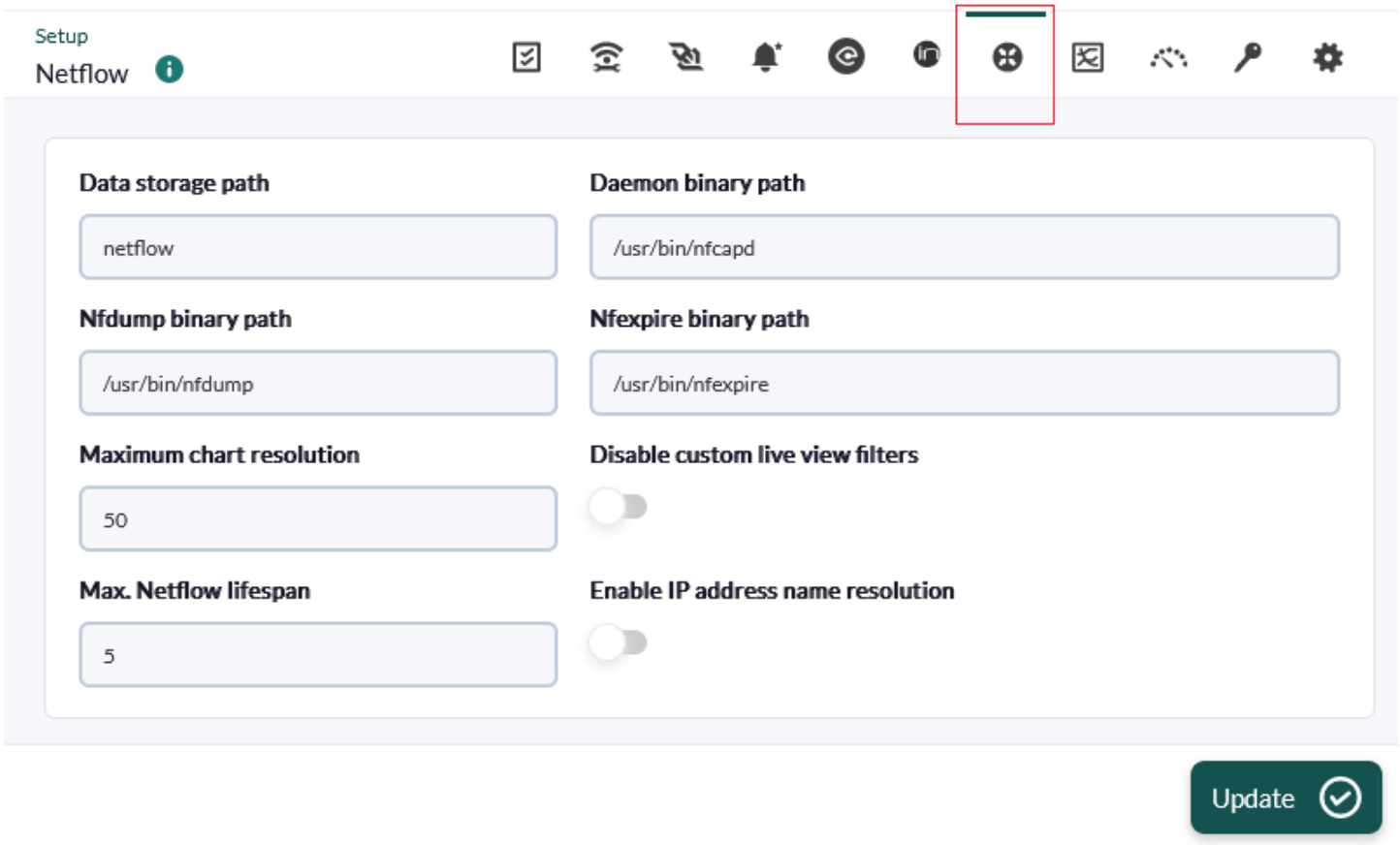
Configuración

La velocidad de acceso del dispositivo de almacenamiento en el que residen los datos de NetFlow es normalmente el factor limitante del rendimiento.

En primer lugar, se debe habilitar NetFlow para que sea accesible desde los menús Operación y Administración. En el apartado de Configuración (menú Administración) hay una opción para habilitar o deshabilitar el NetFlow de manera global.



Una vez activado, aparecerá una nueva opción de configuración de NetFlow en la sección de configuración.



Se debe configurar correctamente este apartado para que el demonio nfcapd pueda iniciarse sin

problemas junto con el servidor de Pandora FMS:

- Data storage path: Directorio donde se almacenarán los ficheros de datos de NetFlow. Se deberá colocar solamente el nombre del directorio, por defecto `netflow` (véase General Setup).
- Daemon binary path: Ruta al binario de nfcapd.
- Nfdump binary path: Ruta al binario de nfdump.
- Nfexpire binary path: Ruta al binario de nfexpire.
- Maximum chart resolution: Número máximo de puntos que mostrará una gráfica de área de NetFlow. Cuanto más alta la resolución, peor el rendimiento. Se recomiendan valores entre 50 y 100.
- Disable custom live view filters: Deshabilita la definición de filtros personalizados desde la vista de NetFlow (los filtros que ya están creados permite seguirlos usando).
- Max. NetFlow lifespan: Indica el máximo tiempo en días de datos NetFlow que se almacenarán.
- Enable IP address name resolution: Permite la resolución de direcciones IP para tratar de obtener los *hostnames* de los dispositivos NetFlow.
- NetFlow interval: Permite ajustar el intervalo de tiempo del daemon NetFlow a 10, 30 ó 60 minutos. Después de realizar un cambio y aplicarlo en el selector de tiempo, es necesario reiniciar el servidor para que este cambio surta efecto.

Una vez configurado NetFlow en la consola, habrá que reiniciar el servidor de Pandora FMS para que éste inicie el servidor nfcapd. Este debe estar correctamente instalado antes de intentar arrancarlo. Compruebe los registros o *logs* del servidor ante cualquier duda.

Si decide almacenar los datos de NetFlow en un dispositivo distinto al servidor PFMS (véase procedimiento de instalación de nfcapd y la configuración distribuida) deberá copiar el fichero binario `/usr/bin/nfexpire` a dicho dispositivo y agregar la siguiente entrada en el fichero `/etc/crontab`:

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

Donde `x_days` es el número máximo de días de antigüedad, de los datos NetFlow, a retener en dicho dispositivo (*en este caso particular la configuración de la* Consola PFMS, *para ese campo, no surtirá efecto*).

Filtros

El menú para la creación y edición de filtros se encuentra en Management → Resources → Netflow filters. En esa vista se encuentra un listado de los filtros ya creados que pueden ser modificados y/o borrados.

También se puede crear un filtro directamente desde la vista de Netflow live view, guardando el filtro activo como uno nuevo. Los filtros NetFlow pueden ser básicos o avanzados. *La diferencia está en que los primeros tienen unos campos fijos de filtrado* (IP origen, IP destino, Puerto origen, Puerto destino) *y los avanzados se definen mediante una expresión* pcap (estándar en expresiones de filtrado para tráfico de red) y utilizan herramientas de todo tipo.

Activar monitorización de NetFlow

Versión 770 o posterior.

En la creación del filtro se puede activar la monitorización del mismo al activar el *token* Enable NetFlow monitoring.

- Esto permite crear un agente que monitorice el volumen del tráfico de este filtro.
- Crea un módulo que mide si el tráfico de cualquier dirección IP de este filtro sobrepasa un cierto umbral.
- Se creará un módulo de tipo texto con la tasa de tráfico de cada dirección IP dentro de este filtro cada cinco minutos (las 10 direcciones IP con más tráfico).

Los parámetros son los siguientes:

- Maximum traffic value of the filter: Especifica la tasa máxima (en bytes por segundo) del tráfico del filtro. Posteriormente se utiliza para calcular el porcentaje del tráfico máximo por dirección IP.
- WARNING threshold for the maximum % of traffic for an IP: Si cualquier dirección IP dentro del filtro sobrepasa el porcentaje establecido, se generará el estado ADVERTENCIA.
- CRITICAL threshold for the maximum % of traffic for an IP: Si cualquier dirección IP dentro del filtro sobrepasa el porcentaje establecido, se generará el estado CRÍTICO.

Informes

Los informes de NetFlow están integrados con los informes de Pandora FMS.

Para crear un elemento de informe, elija uno de los elementos de informe de NetFlow disponibles.

Las siguientes opciones de configuración están disponibles:

- Type: Los tipos de elemento se explicarán a continuación.
- Filter: Filtro de NetFlow a usar.
- Period: Longitud del intervalo de datos a mostrar.
- Resolution: Algunos informes requieren que se recojan muestras cada cierto periodo. Este parámetro sirve para definir el número de muestras. La resolución puede ser baja (6 muestras), media (12 muestras), alta (24 muestras) o ultra alta (30 muestras). Hay dos valores especiales (*hourly* y *daily)* para que no se recoja un valor fijo de muestras sino una cada cierto periodo de horas o días.
- Max. values: Número máximo de elementos para agregados. Por ejemplo, si una gráfica de tráfico HTTP está agregada por dirección IP de origen y Max. values se configura a 5, sólo se mostrarán cinco direcciones IP.

Hay tres tipos de elementos de informe de NetFlow:

- NetFlow area chart: Una gráfica de área, agregada o sin agregar.
- NetFlow data chart: Una representación en texto de la gráfica de área.
- NetFlow summary chart: Resumen de tráfico para el periodo dado. Hay tres elementos: una tabla con información global, un gráfico de tarta con las direcciones IP o puertos más relevantes y una tabla con la misma información del gráfico de tarta desglosada.

Vista en tiempo real

Esta vista se utiliza para consultar el histórico de datos capturados en base a diferentes filtros de búsqueda. Se pueden usar filtros y diferentes formas de visualización de información. Se debe definir la manera de agrupar la información mostrada, así como la manera de obtener dicha información para poder empezar a visualizar datos.

Los filtros se pueden visualizar en tiempo real desde Operation → Monitoring → Network → NetFlow Live View. Esta herramienta permite visualizar los cambios que se realizan en un filtro y guardarlo una vez se obtenga el resultado deseado. También es posible cargar y modificar filtros ya existentes.

La manera de obtener la información puede ser mediante: dirección IP de origen, dirección IP de destino, Puerto de origen o Puerto de destino. Si se escoge, por ejemplo, mostrar la información dirección IP de destino se mostrará la información ordenada por las direcciones IP con más tráfico hacia el destino de mayor a menor. Lo mismo sería para saber el consumo de su red por protocolo, escogiendo por puerto de destino.

Las maneras de visualización posibles son las siguientes:

- Area graph (Gráficas de área de tipo *stacked*): Muestran a lo largo del tiempo (desde la fecha de origen a la fecha de destino), la evolución de los datos. Se debe escoger el nivel de precisión de la gráfica en el token “Resolución”.
- Circular mesh (Gráfico circular): Muestra un gráfico interactivo circular que representa los pares de conexiones entre IP y volumen de tráfico.
- Data table (Tabla de datos): Muestra una tabla de datos con cada IP y un número de filas que depende de la resolución elegida.
- Detailed host trafic (Tráfico detallado de anfitrión): Muestra un mapa de porciones que representa el tráfico por IP.
- Summary (Resumen): Muestra una tabla resumen, una tarta y una tabla con los datos de todo el periodo.
- Top-N connections (Primera N conexiones): Una tabla que muestra el TOP-N de conexiones entre pares de IP Origen - IP Destino, basándose en el tráfico entre dichas direcciones IP (la suma de los porcentajes de los N elementos de la tabla no necesariamente será cien porque pueden haber otras parejas de conexiones src/dst).

Mapas de tráfico de red

Permite crear mapas de red dinámicos, basados en el tráfico entre nodos. Muestra la relación (conexiones) entre diferentes direcciones, mostrando las N conexiones más importantes (por tamaño de los datos transferidos entre ellas).

Configuración distribuida

Es posible ubicar el nodo de Pandora FMS que recoge datos de NetFlow en un *host* independiente

de la Consola. En entornos con muchos datos NetFlow es más que recomendable ubicarlo en un servidor con discos rápidos y una CPU rápida de dos núcleos o más. Para que la Consola de Pandora FMS pueda extraer datos de NetFlow será necesario modificar la configuración por defecto del sistema, siguiendo los pasos descritos a continuación:

- Configurar la autenticación automática SSH entre el usuario propietario del demonio web y el usuario con capacidad de ejecutar nfdump en el nodo colector.

Para su configuración debemos seguir los siguientes pasos:

Habilitar *login* para el usuario apache. Para ello hay que modificar en el fichero `/etc/passwd` la linea del usuario apache con esta configuración:

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

Crear el directorio `.ssh` dentro del directorio `/var/www` y darle los permisos correctos:

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

Crear claves SSH desde el usuario apache y copiarlas al servidor donde esté alojado el tráfico NetFlow.

```
# 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>
```

Una vez compartida se debe comprobar que es posible acceder al servidor mediante el usuario apache sin indicar contraseña:

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

- Crear un script en la consola de Pandora FMS que reemplace a `/usr/bin/nfdump` por uno similar al siguiente:

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

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

Dar permisos de ejecución al *script*:

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

Probar a ejecutar el *script*, de esta forma:

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

Debería devolver algo similar a:

```
nfdump: Version: 1.6.13
```

Monitorización de red con sFlow

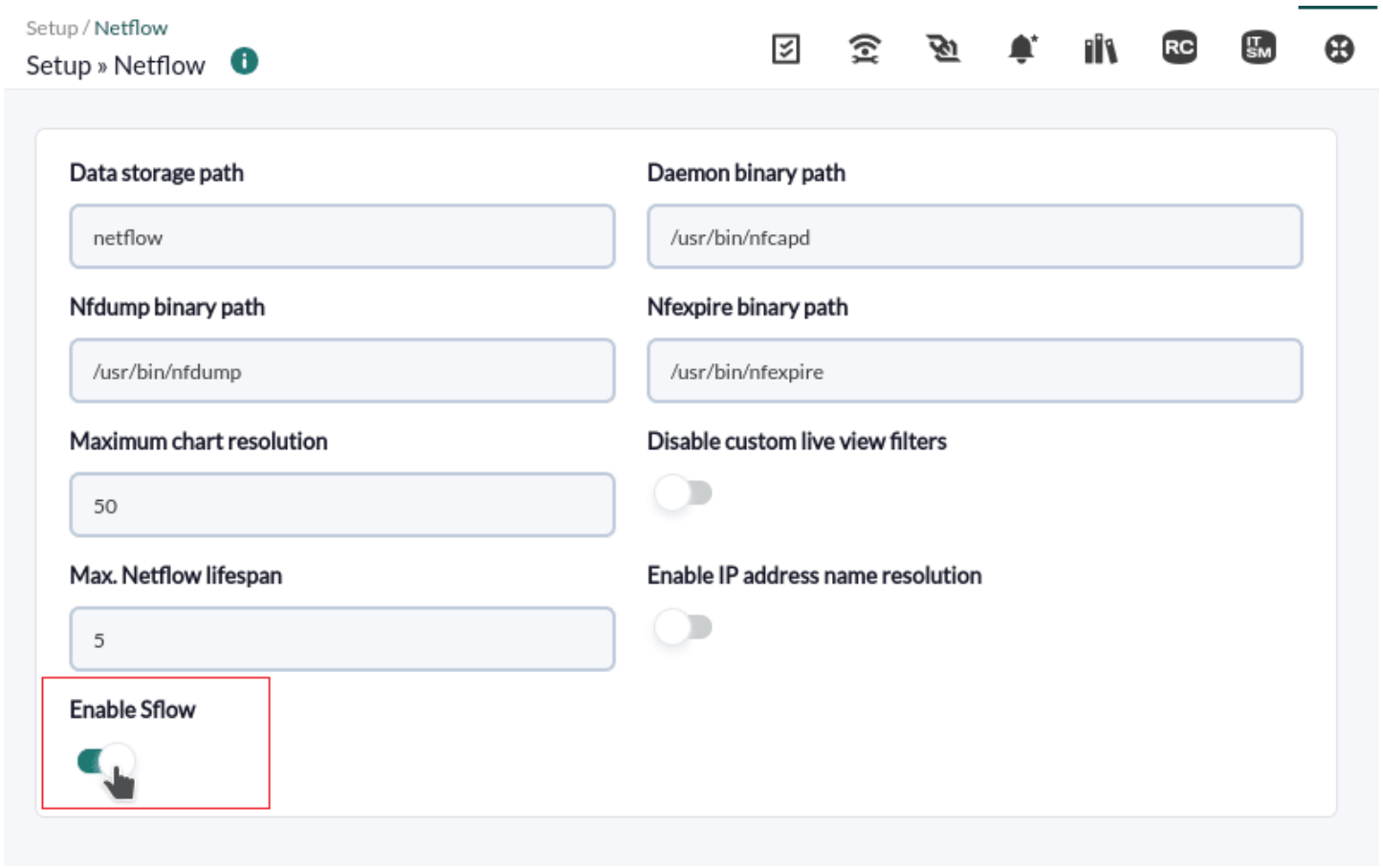
A partir de la versión 770 de Pandora FMS se incluye el soporte para sFlow, un protocolo de red el cual es un estándar industrial en la fabricación de hardware para tráfico de red de datos.

El funcionamiento de sFlow en PFMS es similar al instaurado con NetFlow. En el caso de que ambos protocolos estén activos, los datos serán agrupados; en todo caso siempre serán visualizados accediendo al menú Operation en la barra lateral izquierda, y luego haciendo clic en Network.

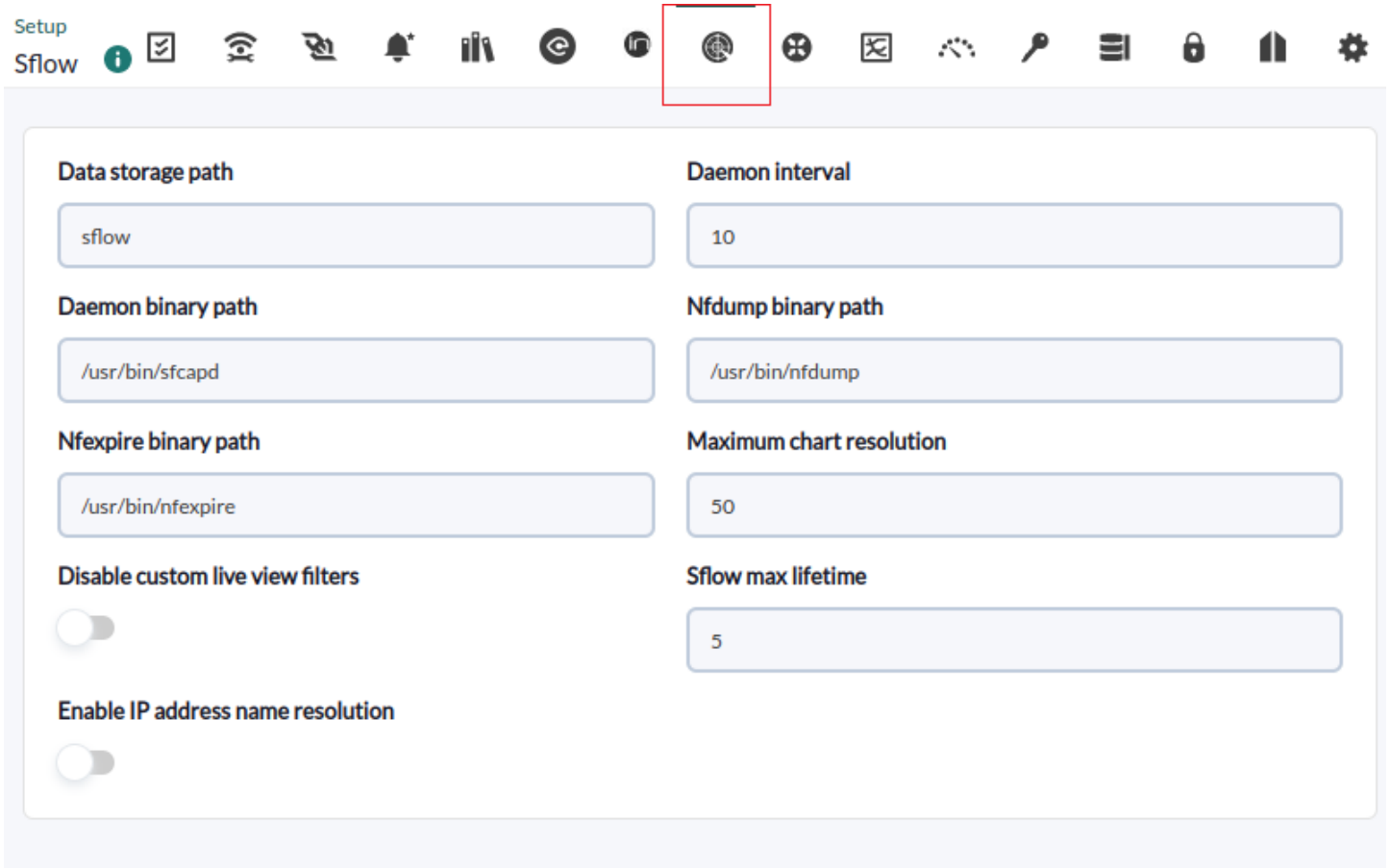
Configuración de sFlow

Versión 775 o posterior.

Debe habilitar sFlow para que sea accesible desde los menús Operation y Management. En el apartado de configuración de NetFlow existe una opción para habilitar o deshabilitar sFlow de manera global.



Una nueva pestaña será habilitada específicamente para sFlow:



- Data storage path: Directorio donde se almacenarán los ficheros de datos de sFlow (véase General

Setup).

- Daemon binary path: Ruta al binario de nfcapd.
- Nfdump binary path: Ruta al binario de nfdump.
- Nfexpire binary path: Ruta al binario de nfexpire.
- Maximum chart resolution: Número máximo de puntos que mostrará una gráfica de área de sFlow. Cuanto más alta la resolución, peor el rendimiento. Se recomiendan valores entre 50 y 100.
- Disable custom live view filters: Deshabilita la definición de filtros personalizados desde la vista de sFlow (los filtros que ya están creados permite seguirlos usando).
- sFlow max lifetime: Indica el máximo tiempo en días de datos sFlow que se almacenarán.
- Enable IP address name resolution: Permite la resolución de direcciones IP para tratar de obtener los *hostnames* de los dispositivos sFlow.

Volver al índice de documentación de Pandora FMS.