Arquitectura de opFlow

El presente documento describe las diferentes arquitecturas en las que se puede trabajar con opFlow para la colección de datos dentro de las redes corporativas. Para poder comprender de manera mas detallada como funciona opFlow debemos conocer la parte técnica la cual describimos a continuación.

Flujos de red

Un flujo de red puede definirse de muchas maneras. Cisco estándar NetFlow versión 5 define un flujo como una secuencia unidireccional de paquetes que todos comparten los siguientes 7 valores:

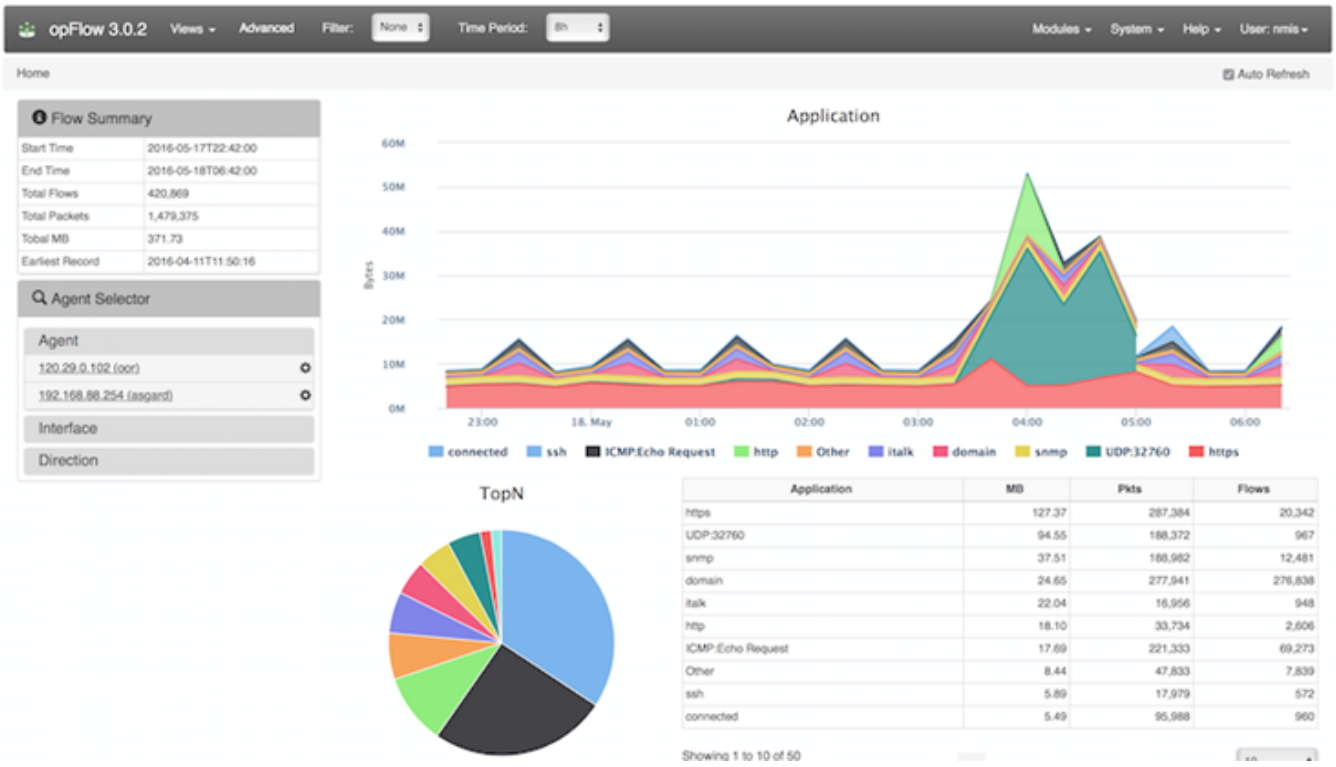
- Interfaz de entrada (SNMP ifIndex)
- Dirección IP origen
- Dirección IP de destino
- Protocolo IP
- Puerto de origen para UDP o TCP, 0 para otros protocolos
- Puerto de destino para UDP o TCP, tipo y código para ICMP, o 0 para otros protocolos
- Tipo de servicio IP

Esta definición de flujos también se utiliza para IPv6, y una definición similar se utiliza para los flujos MPLS y Ethernet. Una salida típica de una herramienta de línea de comandos de NetFlow (nfdump en este caso) al imprimir los flujos almacenados puede verse de la siguiente manera:

```
Date flow start          Duration Proto   Src IP Addr:Port      Dst IP Addr:Port     Packets    Bytes Flows
2010-09-01 00:00:00.459     0.000 UDP     127.0.0.1:24920    ->  192.168.0.1:22126       1       46     1
2010-09-01 00:00:00.363     0.000 UDP     192.168.0.1:22126  ->  127.0.0.1:24920       1       80     1
```

Descripción de opFlow

opFlow reduce el tiempo de inactividad e identifica rápidamente la causa raíz del rendimiento deficiente de la red utilizando flujos. Integrando perfectamente con NMIS, opFlow recopila información de NetFlow para permitir a las organizaciones determinar cuánto de la red está siendo utilizada, por quién y de qué manera.



Compatible con varios proveedores y protocolos, incluyendo NetFlow, NetFlow-Lite, NSEL, Juniper J-Flow, sFlow e IPFIX, opFlow ayudará a analizar la congestión, monitoreando el uso de datos altos e identificando el comportamiento sospechoso.

Ventajas de opFlow

- Provee información que permite a organizaciones determinar qué tanto de la red se está utilizando, por quién y en qué forma;
- Rápida identificación de causas de cuellos de botella;
- Rápida identificación de patrones de tráfico inusuales;
- Provee información clave para planificación y afinamiento de la red;
- Ayuda a reducir los tiempos de caída a través de la identificación del impacto de los cambios, entendiendo el flujo de aplicaciones de negocio en la red.

Como activar el envió de flujos

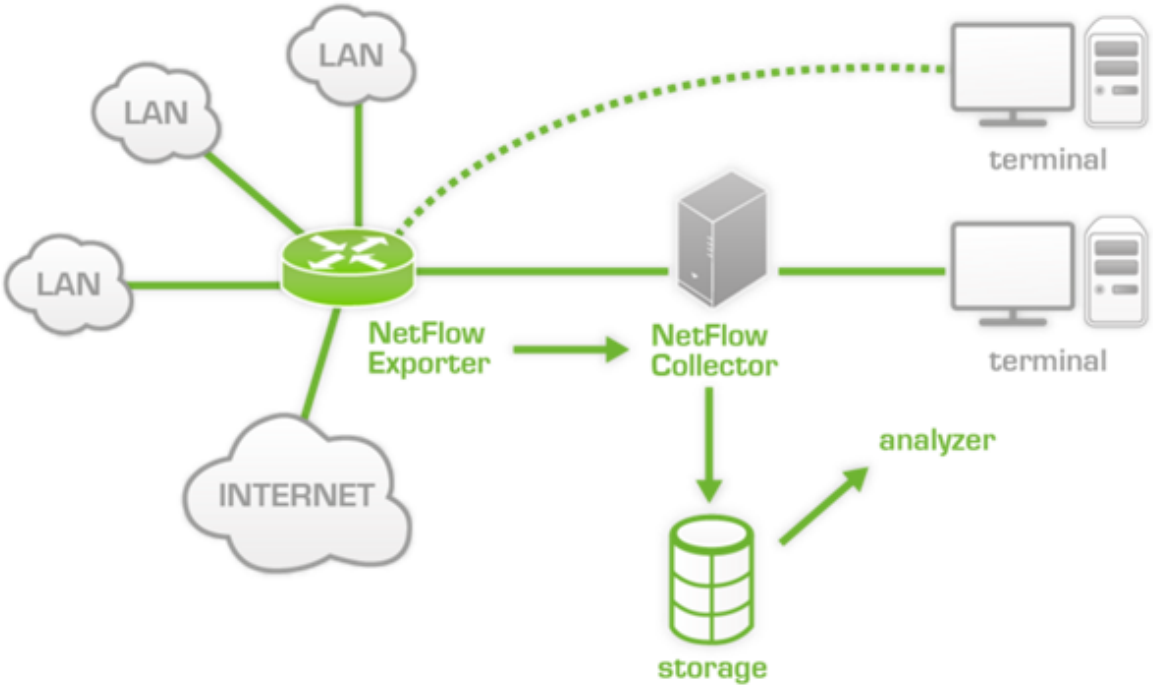
La configuración básica que se debe de aplicar a los router para el envio de los flujos hacia el servidor opFlow es la siguiente considerando que para la versión 3 de opFlow, el puerto de escucha predeterminado es el puerto 9995 más o menos estándar. La siguiente es una configuración básica de Cisco Router para decirle al enrutador que envíe datos Netflow a la opFlow.

```
! this command is optional, this will flow data about in-progress flows, very handy for large file transfers.
ip flow-cache timeout active 1
! version can be 5 or 9 with 9 add IPV4 template
ip flow-export version 5
ip flow-export destination <opflow_server> 12345
!
interface FastEthernet0/0
 !only if you want output traffic
 ip flow ingress
 !only if you want input traffic
 ip flow egress
```

Arquitecturas para la implementación de opFlow

Monitoreo sobre demanda

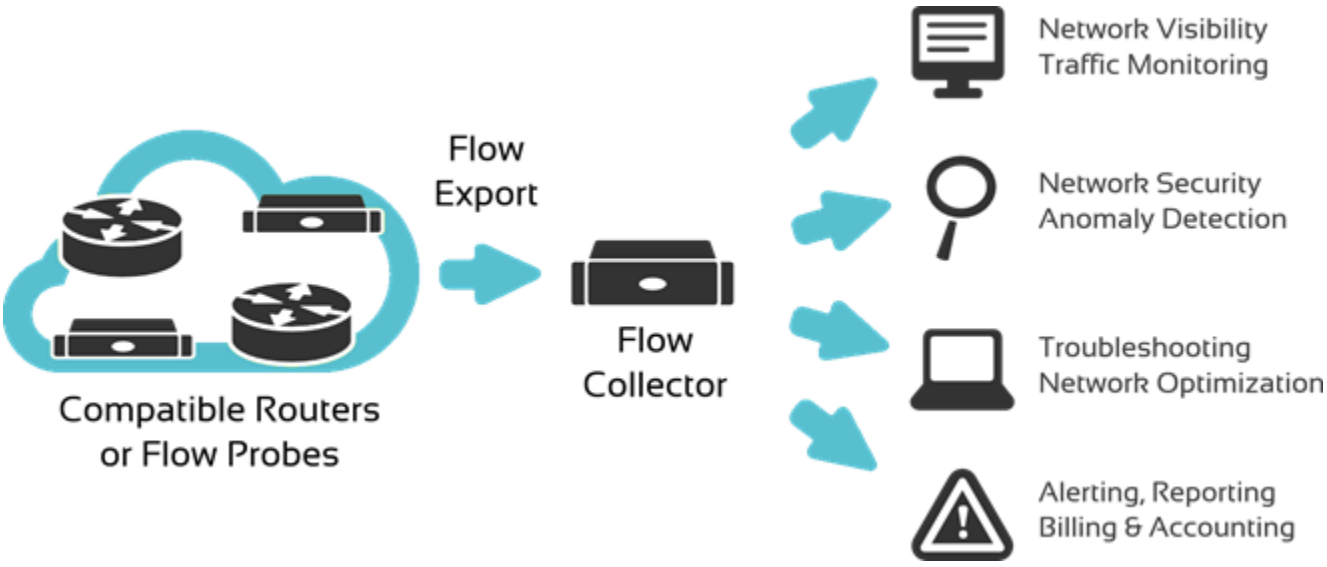
Actualmente se puede trabajar con opFlow escuchando flujos directamente en los servidores de producción si solo se requiere que la consulta sea sobre demanda esto es que se escucharan flujos de manera temporal, opFlow consume recursos del sistema los cuales si existe demasiada información puede afectar los servicios que vivan en dicha maquina. La instalación actualmente esta hecha en los servidores esclavos por lo cual la configuración se deberá realizar en los mismos.



En donde el colector de Netflow será el servidor en cuestión que tenga conectividad con el router que envía los flujos de manera esporádica.

Monitoreo continuo

De ser necesario un monitoreo de flujos continuos para las diversas partes de la red lo ideal será dedicar un servidor independiente en donde solo se instale NMIS y opFlow, de esta manera se puede realizar la escucha de los flujos sin afectar el desempeño de las maquinas virtuales. Esta arquitectura es utilizada por clientes a nivel mundial ya que es recomendación de Opmantek.



Configuración del puerto

Comprobación de los paquetes que llegan al servidor. Ejecutar tcpdump nos dirá si los paquetes están llegando al servidor en absoluto:

```
# change/verify the interface (eth0) and port (if you have changed from the default config)
# this is for a default opFlow 2/flowd
sudo tcpdump -vni eth0 proto \\udp and port 12345
# this is for a default opFlow 3/nfdump
sudo tcpdump -vni eth0 proto \\udp and port 9995
```