Gestion y Monitoreo de Redes
Instalacion y Configuracion de NetFlow

Notas:
------
* Comandos que empiezan con un "$" implica que deberia ejecutar el comando
  como un usuario general - no como root.
* Comandos que empiezan con un "#" implica que deberia trabajar como el usuario root.
* Comandos con lineas mas especificas (como "GW-RTR>" o "mysql>") implica que esta
  ejecutando el comando en un equipo remoto o dentro otro programa.
* Si una linea termina con un "\" esto indica que el comando sigue en la proxima
  linea y Ud. deberia tratar el comando si como fuera en una sola linea.

Ejercicios

Flujo de este practica.

* Si hay tiempo/routers - configurar los routers para exportar flujos a los pcs
  en cada grupo.
* Si no hay tiempo/routers - configurar los pcs con el software to coleccion para
  very los flujos en el router de su grupo.
* Opcional: agregar el plug-in Port Tracker al software NfSsen

Ejercicios Parte I

En este curso tenemos todo los flujos de cada router de cada grupo redireccionado
desde la maquina noc.ws.nsrc.org a cada pc en cada grupo - asi, no vamos a configurar
su router porque ya esta configurado. Ver el ejemplo al final de este documento para
saber como configurar un router cisco exportor flujos.

0. HAZ UNA CONECCION SSH A SU PC

1. CONFIGURAR SU PC PARA COLECCIONAR LOS FLUJOS Y VERLOS POR EL WEB

   Verifica que los flujos (flows) estan llegando a su pc:

        # sudo bash
        # apt-get install tcpdump
        # tcpdump -i eth0 -v port 900N

   Donde "N" es el numero de su grupo (1, 2, 3, 4, 5, o 6).

   Despues que un corto plazo deberia ver algo como esto (ejemplo por grupo 2):

        root@pc4:~# tcpdump -i eth0 -v port 9002
        tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
        01:06:49.481983 IP (tos 0x0, ttl 63, id 242, offset 0, flags [none], proto UDP
(17), length 388)
        10.10.0.2.62089 > 10.10.2.4.9002: UDP, length 360

   Instalar NFdump desde fuente.

Primero instalamos los paquetes de apoyo por el software NFdump. Instalamos NFdump desde fuente para permitir instalar el plug-in Port Tracker mas adelante.

Si algunos de este paquetes ya estan instalado no se preocupa el sistema apt-get arregal todo :-)

```
# apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
  libmailtools-perl bison flex php5
```

La instalacion va a demorar algunos minutos en terminar.

Si recibes el mensaje que empieza con:

> "If your MRTG configuration file is readable by users other than the user MRTG runs as ('root' by default) it can present a security risk, as this file contains SNMP community names.
>
> ..."
>
> Selecciona "<Yes>" para seguir

Bajar el fuente por el paquete NFdump. Ponemos el software en un directorio done podemos trabajar.

```
# cd /usr/local/src
# wget http://noc.ws.nsrc.org/downloads/nfdump.tar.gz
```

Si necesitas el fuente de NFdump en el futuro se lo encuentro en http://sourceforge.net/projects/nfdump/

```
# tar xvzf nfdump.tar.gz
# cd nfdump-1.6.3p1
# ./configure --enable-nfprofile
# make
# make install
```

Ya esta instalado NFdump.

Ahora, bajamos el fuente de NfSen

```
# cd /usr/local/src
# wget http://noc.ws.nsrc.org/downloads/nfsen.tar.gz
```

Si necesitas el fuente de NfSen en el futuro se lo encuentro en http://sourceforge.net/projects/nfsen/

```
# tar xvzf nfsen.tar.gz
# cd nfsen-1.3.5/etc
# cp nfsen-dist.conf nfsen.conf
# vi nfsen.conf
```

Ahora busca y cambia varias lineas dentro el archivo nfsen.conf.

Cambia el variable $BASEDIR:

```
$BASEDIR="/var/nfsen";
```

Ajuste el directorio donde estan los herramientas de NFdump:

```
# nfdump tools path
$PREFIX = '/usr/local/bin';
```

Cambia los usuarios para que Apache (servidor http) tiene acceso a los archivos:

```
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data'
```

Ajusta el tamano del buffer para que veamos graficos mas rapido. Y, enlace el proceso de nfsen al 127.0.0.1:

```
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = "2000 -b 127.0.0.1";
```

Encuentra la definicion de fuentes ($sources) y cambiarla a:

```
%sources=(
'rtrX'=>{'port'=>'900X','col'=>'#0000ff','type'=>'netflow'},
);
```

Donde "X" es el numero de su grupo. Si hay entradas puede hacer comentario o borrarlas. Por ejemplo:

```
%sources = (
'rtrX'          => {'port'=>'900X','col'=>'#0000ff','type'=>'netflow'},
#'upstream1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
#'peer1'        => { 'port' => '9996', 'IP' => '172.16.17.18' },
#'peer2'        => { 'port' => '9996', 'IP' => '172.16.17.19' },
);
```

Ahora graba y salga del archivo.

Crear un usuario netflow:

```
# useradd -d /var/netflow -G www-data -m -s /bin/false netflow
```

Inicializa NfSen. Cada vez que cambias etc/nfsen.conf tiene que hacer este paso de nuevo:

```
# cd /usr/local/src/nfsen-1.3.5
# perl install.pl etc/nfsen.conf
```

Si le pregunta por el directorio de Perl solo apreta para aceptar la seleccion.
Si le pregunta si quieres configurar los fuentes nuevos responde "Y".

Arranca NfSen

```
# /var/nfsen/bin/nfsen start
```

Asegura que nfsen arranca cada vez que su maquina inicializa:

Edita el archivo /etc/rc.local

```
# vi /etc/rc.local
```

Agrega una linea _antes_ el fin del archivo para que se vea asi:

```
/var/nfsen/bin/nfsen start
exit 0
```

Salga y graba el archivo.

Antes de ver el interfaz web tiene que reinicializar el servidor web Apache:

```
# service apache2 restart
```

Ahora puedes ver los resultados de NfSen aqui:

```
http://pcN.ws.nsrc.org/nfsen/nfsen.php
```

Esto es la configuracion basica de NfSen. Con tiempo quedara con informacion sobre los flujos del datos a traves su router de su grupo que pueden ser muy utiles.

Ejercicios Opcionales

1. EXTENDER LA CONFIGURACION DE NETFLOW

Sola muestra - no vamos a hacer esto en este curso.

Si hay mas routers que estan apuntando sus flujos a su maquina usando otros puertos de UDP puede tener multiples flujos representados en los diagramas de NfSen.

```
# cd /usr/local/src/nfsen-1.3.5
# vi etc/nfsen.conf
```

Por cada flujo llegando a un puerto diferente agrega una linea en la seccion de $sources.

Solo muestra

```
%sources = (
'rtr' => {'port' => '9000', 'col' => 'e4e4e4' },
'rtr2' => { 'port' => '9001', 'col' => '#0000ff' },
'rtr3' => { 'port' => '9002','col' => '#00cc00' },
'rtr4' => { 'port' => '9003','col' => '#000000' },
'rtr5' => { 'port' => '9004','col' => '#ff0000' },
'rtr6' => { 'port' => '9005','col' => '#ffff00' },
```

```
    );
```

Nota el cambio de colores por cada entrada ('#0000ff', '#00cc00', etc.).

Graba y salga del archivo nfsen.conf

Recuerda que cambiaste la configuracion de NfSen, asi tiene que hacer lo siguiente:

```
    # /var/nfsen/bin/nfsen stop
    # perl install.pl etc/nfsen.conf
    # /var/nfsen/bin/nfsen reconfig
```

Si le pregunta por el directorio de Perl solo apreta para aceptar la seleccion.
Si le pregunta si quieres configurar los fuentes nuevos responde "Y".

Ahora arrance nfsen:

```
    # /var/nfsen/bin/nfsen start
```

Ahora revisa los graficos al:

```
    http://pcN.ws.nsrc.org/nfsen/nfsen.php
```

Se lo demora algunos minutos para empezar salir los graficos nuevos.

2. INSTALAR EL PLUGIN PORT TRACKER

[OJO! Con las maquinas virtuales es muy probable que no hay bastante espacio de disco duro para que funciona la instalacion de Port Tracker. La instalacion requiere que haya 8GB libre en el disco. Usa "df -h" para ver cuanto espacio hay.]

Para empezar.

```
    # cd /usr/local/src/nfsen-1.3.5/contrib/PortTracker/
```

Edita el archivo do_compile y cambia la linea:

```
    NFDUMP="/path/to/nfdump-1.6.1p0"
```

para que dice:

```
    NFDUMP="/usr/local/src/nfdump-1.6.3p1"
```

y sigue con la instalacion.

```
    # ./do_compile
    # cp nftrack /usr/local/bin/.
    # cd /usr/local/src/nfdump-1.6.3p1/extra
    # cp PortTracker.pm /var/nfsen/plugins/
    # cd /usr/local/src/nfsen-1.3.5/contrib/PortTracker/
```

```
     # cp PortTracker.php /var/www/nfsen/plugins/.
     # mkdir -p /data/netflow/porttracker
```

Especifica a Port Tracker donde va a grabar los datos. Edita el archivo /var/nfsen/plugins/PortTracker.pm

```
     # vi /var/nfsen/plugins/PortTracker.pm
```

Encuentra la linea que dice:

```
     my $PORTSDBDIR = "/data/port-db";
```

y cambia la linea a:

```
     my $PORTSDBDIR = "/data/netflow/porttracker";
```

Graba y salga del archivo.

Ahora edita el archivo /usr/local/src/nfsen-1.3.5/etc/nfsen.conf:

```
     # /usr/local/src/nfsen-1.3.5
     # vi etc/nfsen.conf
```

Y busca la seccion:

```
     @plugins = (
         # profile    # module
         # [ '*',     'demoplugin' ],
     );
```

Y la cambia a:

```
     @plugins = (
         # profile    # module
         # [ '*',     'demoplugin' ],
         [ 'live',   'PortTracker'],
     );
```

Ahora vamos a reconfigurar nfsen para usar el plugin:

```
     # /var/nfsen/bin/nfsen stop
     # perl install.pl etc/nfsen.conf
```

Apreta <ENTER> cuando le pregunta por la ubicacion de Perl.

Arranca nfsen de nuevo:

```
     # /var/nfsen/bin/nfsen start
```

Cambia los permisos y duenos de archivos por Port Tracker:

```
     # chown netflow:www-data /data/netflow/porttracker/
```

Inicializa el base de datos de Port Tracker. Esto pude demorar porque

Port Tracker va a crear 8GB de archivos.

```
# chmod 775 /data/netflow/porttracker/
# sudo -u www-data nftrack -I -d /data/netflow/porttracker
```

(This can take a LONG time! - 8 GB worth of files will be created)

Ponemos los permisos en los archivos para que el servidor web puede leer los datos:

```
# chown -R netflow:www-data /data/netflow/porttracker
# chmod -R 775 /data/netflow/porttracker
```

Recargar nfsen:

```
# /var/nfsen/bin/nfsen reload
```

Verifica que funciono:

```
# grep -i 'porttracker.*success' /var/log/syslog
Nov 27 02:46:13 noc nfsen[17312]: Loading plugin 'PortTracker': Success
Nov 27 02:46:13 noc nfsen[17312]: Initializing plugin 'PortTracker': Success
```

Espera algunos minutes y puede ver los resultados en el interfaz Web:

```
http://pcN.ws.nsrc.org/nfsen/nfsen.php
```

Selecciona el menu "Plugins" para ver como funciona Port Tracker.

CONFIGURAR SU ROUTER PARA EXPORTAR LOS FLUJOS

Esto es un ejemplo de configuracion por el router del grupo 1, or rtr1.ws.nsrc.org. En el ejemplo el router manda los flujos (flows) al PC 10.10.1.1, or pc1.ws.nsrc.org. Puede adapter este ejemplo a su router y situacion.

Haz un log in en el router 1 de grupo 1, 10.10.1.254. Vamos a suponer que esta configurado ssh por este router:

```
# ssh cisco@10.10.1.254
rtr1.ws.nsrc.org> enable
```

Tipea la contrasena de "enable" por el router, y luego:

```
rtr1.ws.nsrc.org# configure terminal
rtr1.ws.nsrc.org(config)# interface FastEthernet 0/0
rtr1.ws.nsrc.org(config)# ip route-cache flow
rtr1.ws.nsrc.org(config)# exit
```

Repite por FastEthernet 0/1 (y todo los interfaces que existen)

```
rtr1.ws.nsrc.org# configure terminal
rtr1.ws.nsrc.org(config)# interface FastEthernet 0/1
```

```
     rtr1.ws.nsrc.org(config)# ip route-cache flow
     rtr1.ws.nsrc.org(config)# exit
```

Especifica a donde van los flujos y a que puerto:

```
     rtr1.ws.nsrc.org#conf t
     rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.1.1 9001
     rtr1.ws.nsrc.org(config)# ip flow-export version 5
     rtr1.ws.nsrc.org(config)# ip flow-cache timeout active 5
```

Para que los valores de ifIndex se mantiene despues que una reinicializacion del router:

```
     rtr1.ws.nsrc.org(config)# snmp-server ifindex persist
```

Ahora configuramos los top-talkers:

```
     rtr1.ws.nsrc.org(config)#ip flow-top-talkers
     rtr1.ws.nsrc.org(config-flow-top-talkers)#top 20
     rtr1.ws.nsrc.org(config-flow-top-talkers)#sort-by bytes
     rtr1.ws.nsrc.org(config-flow-top-talkers)#end
```

Ahora verificamos que hemos hecho:

```
     rtr1.ws.nsrc.org# show ip flow export
     rtr1.ws.nsrc.org# show ip cache flow
```

Vea los clientes usando mas datos/paquetes en su router:

```
     rtr1.ws.nsrc.org# show ip flow top-talkers
```

Si todo se vea bien escribir la configuracion en memoria a memoria permanente:

```
     rtr1.ws.nsrc.org#wr mem
```

Puede salir del router:

```
     rtr1.ws.nsrc.org#exit
```

En la maquina donde los flows estan llegando puede verificar que esta funcionando (como root):

```
     # tcpdump -v udp port 9001
```

Despues que algunos segundos deberia ver algo como:

```
     tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
     06:38:25.726825 IP (tos 0x0, ttl 63, id 242, offset 0, flags [none], proto UDP
(17), length 244)
        10.10.0.1.60715 > pc1.ws.nsrc.org.9001: UDP, length 216
     06:38:52.709868 IP (tos 0x0, ttl 63, id 242, offset 0, flags [none], proto UDP
(17), length 532)
       10.10.0.1.60715 > pc1.ws.nsrc.org.9001: UDP, length 504
```

REFERENCIA

Configuracion de su Router

Estamos mandando los flujos de NetFlow desde su router al servidor NOC. Despues, usando un programa llamado "udp-breeder" estamos re-enviando los flujos desde el NOC a cada PC detras de cada router. NetFlow tiene como maximo permitido mandar flujos a dos (2) dispositivos disinto - asi, usando udp-breeder podemos mandar los flujos a todo sus PCs.

Para configurar un router mandar flujos abajo hay un ejemplo:

```
$ ssh cisco@rtrN

        # en
        # conf t
        (config) # interface FastEthernet 0/0
        (config-if) # ip flow ingress
        (config-if) # ip flow egress
        (config-if) # ip route-cache flow
        (config-f) exit
        (config) # ip flow-export version 5
        (config) # ip flow-export destination 10.10.0.250 999N
        (config) # ip flow-cache timeout active 5
        (config) # ip flow-top-talkers
        (config-flow-top-talkers) # top 20
        (config-flow-top-talkers) # sort-by bytes
        (config-flow-top-talkers) # exit
        (config) # exit
        # wr mem
```