

% Monitorización de Netflow con NfSen

%

% Gestión de Redes

Introducción

Metas

- * Aprender a exportar flujos desde un enrutador Cisco
- * Aprender a instalar la familia de herramientas NfSen
- * Instalar el plugin PortTracker

Notas

- * Los comandos precedidos por "\$" implican que debe ejecutar el comando como usuario genérico - no como root
- * Los comandos precedidos por "#" implican que debería estar trabajando como usuario root.
- * Los comandos con inicios de línea más específicos como "RTR-GW>" o "mysql>" indican que debe ejecutar los comandos en un equipo remoto, o dentro de otro programa

Exportar flujos desde un enrutador Cisco

A lo largo de este ejercicio le indicaremos que exporte flujos desde uno de sus enrutadores a dos PCs del taller. Debería trabajar en grupo. O sea, para el grupo 1, los usuarios de pc1, pc2, pc3, pc4 deberían trabajar juntos y elegir una máquina a donde llegarán los flujos.

Además, exportará flujos hacia una segunda máquina en el grupo contiguo. Es decir, por ejemplo, si el grupo 1 ha elegido a pc5 para recibir los flujos, entonces la segunda máquina que elegirá para exportar desde el grupo 1 será pc5. Además, si elige pc1 para recibir flujos de rtr1, entonces esta máquina recibirá, también, flujos desde rtr2.

Estos ejercicios funcionarán sobre el siguiente ejemplo:

Grupo 1, Router 1

rtr1 ==> pc1 en puerto 9001
rtr1 ==> pc5 en puerto 9002

Grupo 2, Router 2

rtr2 ==> pc5 on port 9001
rtr2 ==> pc1 on port 9002

Puede elegir la combinación que desee entre grupos.

He aquí la lista de grupos que han de trabajar juntos:

- * grupo 1 y 2
- * grupo 3 y 4
- * grupo 5 y 6
- * grupo 7 y 8

Si hay un grupo 9, por favor pregunten el instructor.

~~~~~

\$ ssh cisco@rtr1.ws.nsrc.org  
rtr1.ws.nsrc.org> enable

~~~~~

o, si SSH no se ha configurado todavía:

```
~~~~~
$ telnet 10.10.1.54
Username: cisco
Password:
Router1>enable
Password:
~~~~~
```

Recuerde - Este es un EJEMPLO basado en la siguiente situación:

```
rtr1 ==> pc1 on port 9001
rtr1 ==> pc5 on port 9002
```

Los grupos 2, 3, 4, 5, 6, 7, 8 y 9 harán algo diferente.

Lo siguiente configura la interfaz FastEthernet0/0 para enviar flujos.

```
~~~~~
rtr1.ws.nsrc.org# configure terminal
rtr1.ws.nsrc.org(config)# interface FastEthernet 0/0
rtr1.ws.nsrc.org(config-if)# ip flow ingress
rtr1.ws.nsrc.org(config-if)# ip flow egress
rtr1.ws.nsrc.org(config-if)# exit
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.1.1 9001
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.2.5 9002
rtr1.ws.nsrc.org(config)# ip flow-export version 5
rtr1.ws.nsrc.org(config)# ip flow-cache timeout active 5
~~~~~
```

Esto particiona los flujos de larga duración en fragmentos de 5 minutos. Puede elegir cualquier número de minutos entre 1 y 60. Si lo deja en el valor por defecto de 30 minutos, sus reportes de tráfico tendrán picos.

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

Esto hace que los índices SNMP de interfaces nunca cambien al reiniciar el enrutador.

Ahora configure cómo quiere que los top-talkers funcionen:

```
~~~~~
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 verificaremos lo que hemos hecho:

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

Vea los "top talkers" para las diferentes interfaces

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

Si todo parece estar bien, guarde su configuración:

```
~~~~~
```

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

Puede salir del enrutador:

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

Compruebe que los flujos llegan a la PC elegida para recibir en su grupo:

```
$ sudo tcpdump -v udp port 9001
```

Espere unos segundos y debería ver algo como sigue:

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:01:19.027039 IP (tos 0x0, ttl 255, id 1407, offset 0, flags [none], proto UDP (17), length
    rtr1.ws.nsrc.org.64190 > pcl.ws.nsrc.org.9001: UDP, length 552
```

Verifique que los flujos están llegando desde el enrutador del grupo contiguo a la PC elegida en su grupo para recibir flujos (puede que tenga que esperar a que el grupo vecino termine de configurar la exportación)

```
$ sudo tcpdump -v udp port 9002
```

Configure el colector

Actualice, inicie y automatice el software NfSen

NfSen es un interfaz web a la suite de herramientas de netflow nfdump. En sus máquinas virtuales, tanto nfdump como NfSen han sido instalados, en su mayor parte, pero aún es necesario configurarlos.

Para ver los detalles de la instalación de estas herramientas refiérase a la guía de instalación enlazada desde la wiki de este taller.

Actualice NfSen para los dispositivos que están enviándole flujos:

```
cd /usr/local/src/nfsen-1.3.6p1/etc
sudo cp nfsen-dist.conf nfsen.conf
sudo editor nfsen.conf
```

Encuentre la definición de fuentes (sources) y cámbiela para que coincida con la lista de enrutadores que le están enviando flujos. Sustituya rtrA por el nombre de su enrutador y rtrB por el nombre del enrutador vecino que le envía flujos.

```
%sources=(
'rtrA' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
'rtrB' => {'port'=>'9002','col'=>'#00ff00','type'=>'netflow'},
);
```

Grabe y salga.

Iniciar NfSen.

Toda vez que realice cambios en la configuración nfsen.conf, deberá rehacer este paso:

Asegúrese de estar en el lugar correcto:

```
~~~~~  
$ cd /usr/local/src/nfsen-1.3.6p1  
~~~~~
```

Complete la instalación de NfSen:

```
~~~~~  
$ sudo perl install.pl etc/nfsen.conf  
~~~~~
```

Cuando se le pregunte por el camino de Perl, oprima ENTER

Inicie NfSen:

```
~~~~~  
sudo /var/nfsen/bin/nfsen start  
~~~~~
```

Instalar el script de iniciar NfSen

Para que nfsen se pueda arrancar y detener automáticamente cuando se inicia o apaga su sistema, agregue el siguiente enlace en su directorio init.d apuntando al script de inicio de nfsen:

```
~~~~~  
$ sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen  
$ update-rc.d nfsen defaults 20  
~~~~~
```

Visualice los flujos en la interfaz web:

Puede encontrar la página de NfSen aquí:

```
~~~~~  
http://pcX.ws.nsrc.org/nfsen/nfsen.php  
~~~~~
```

Listo! Siga con el segundo ejercicio

Apéndice

En algunas distribuciones de Linux recientes (Fedora Core 16, Ubuntu 12.04, etc) puede que vea un error como el siguiente al iniciar NfSen 1.6.6:

```
Subroutine Lookup::pack_sockaddr_in6 redefined at  
/usr/share/perl/5.14/Exporter.pm line 67.  
at /var/nfsen/libexec/Lookup.pm line 43
```

nfsen se iniciará y funcionará correctamente, así que puede ignorar este error por ahora (o resolver el problema y contribuir al proyecto NfSen!)