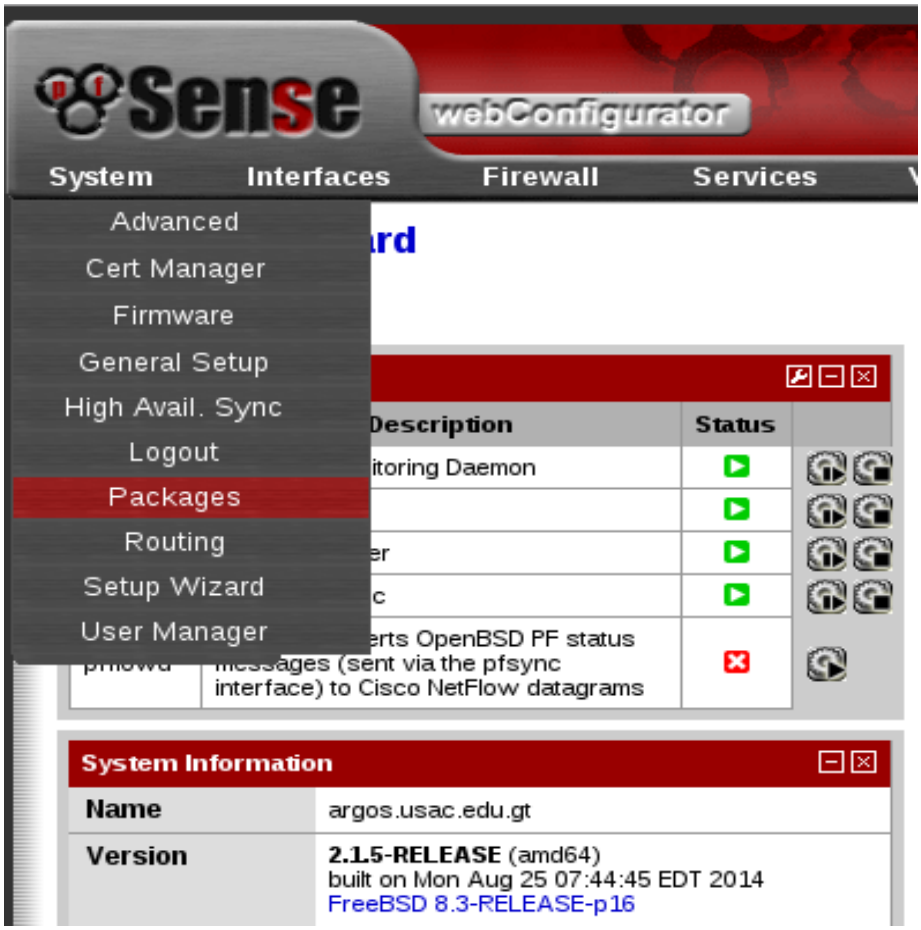
Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

Instalación de netflow en pfsense para enviar flujos a nfsen server

Antes que nada, agradezco el entrenamiento recibido de parte de la NSRC (Carlos Armas, Antonio Lobo y José Domínguez) en Manta, así como a la WAL2014 por haberme considerado para subvención de la matrícula.

Este manual está basado en las prácticas del workshop de Gestión de Redes (http://www.eslared.org.ve/walc2014/index.php/tracks/track-3) con las modificaciones del caso, ya que NO usaré un router CISCO sino PfSense como generador de flujos dado que es mi máquina central en la red. La mayor parte de los ejercicios originales se queda casi en su totalidad invariable, solamente se ajusta a mis necesidades.

Instalando NetFlow en PfSense



Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

Seleccionamos e instalamos el package `pfflowd` y en los paquetes instalados queda como se muestra a continuación:

Luego se procede a montar un servidor distinto con ubuntu 12.04.
Se instala la siguiente paquetería:

```
$ sudo apt-get install build-essential
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
libmailtools-perl php5 bison flex autoconf
```

Se crea un usuario llamado `jaimec`, aunque pudo llamarse de cualquier manera. Este sirve para compilar la paquetería que no viene como paquete de ubuntu.

Descargar `nfdump` del sitio oficial http://sourceforge.net/projects/nfdump/:

```
$ whoami
$ jaimec
$ pwd
$ /home/jaimec
$ wget  http://downloads.sourceforge.net/project/nfdump/stable/nfdump-
1.6.12/nfdump-1.6.12.tar.gz

$ tar xzvf nfdump-1.6.12.tar.gz
$ cd nfdump-1.6.12
```

Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

```
$ ./configure --help # optional, shows the build settings available
$ ./configure --enable-nfprofile --enable-nftrack
$ make
$ sudo make install (notar que esto se hace como root)
```

En pfsense lo configura de esta manera:

De esta forma pfsense comenzará a enviar flujos de netflow versión 9 desde la ip 10.0.0.1 que es la máquina donde está pfsense hacia 10.0.0.82 que es la máquina donde tengo nfdump.

Probando nfcapd y nfdump

```
$ mkdir /tmp/nfcap-test
$ nfcapd -E -p 9001 -l /tmp/nfcap-test
```

… despues de un tiempo, una serie de flujos deben ser descargados en la pantalla.

Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

Detenga la herramienta con CTRL + C y luego revise el contenido en `/tmp/nfcap-test`
`$ ls -l /tmp/nfcap-test`

Debería ver uno o mas archivos llamados nfcapd. <AÑO> <MES> <DIA> <HR> <min>

Procesar el/los archivo(s) con nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.2013wwxxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.2013wwxxyyzz -s srcip/bytes
```

Se debe obtener alguna información como la siguiente:

```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets
Bytes Flows
2014-11-17 20:45:35.639    57.361 UDP         10.4.0.119:61922 ->          10.0.0.5:53           3
177     1
2014-11-17 20:45:35.639    57.361 UDP           10.0.0.5:53    ->        10.4.0.119:61922         0
0     1
2014-11-17 20:45:35.639   196.608     0          0.0.0.0:119   ->       224.17.10.4:2560          0
0     1
2014-11-17 20:45:35.639    57.361 UDP           10.0.0.5:53    ->        10.4.0.119:61922         3
177     1
2014-11-17 20:45:35.639   131.072     0          0.0.0.0:119    ->       224.17.10.4:2560      8.0 M
34339.9 T     1
2014-11-17 20:45:35.639    57.361 UDP           10.0.0.5:53    ->        10.4.0.119:24046         0
0     1
```

Instalación y comfiguración de NFSen

Descargar y compilar. El parche es para arreglar un problema reportado en:
http://sourceforge.net/p/nfsen/bugs/31/

```
$ cd /home/jaimec
$ wget  http://downloads.sourceforge.net/project/nfsen/stable/nfsen-1.3.6p1/nfsen-1.3.6p1.tar.gz

$ tar xvzf nfsen-1.3.6p1.tar.gz
$ cd nfsen-1.3.6p1
$ wget https://dl.dropboxusercontent.com/u/20707729/ParcheNFSen/nfsen-socket6.patch

/* Este parche es importante aplicarlo y no se consigue en internet sino solamente con el personal de la NSRC, al menos yo no lo encontré publicado. Por ello se deja esa dirección de dropbox de forma pública */

$ patch -p0 < nfsen-socket6.patch
$ cd etc
```

Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

```
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
```
Ajuste la variable `$ BASEDIR`

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

Ajuste los usuarios como corresponde, para que Apache pueda acceder a los archivos:

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

Ajuste el tamanño del bufer a algo pequenño, y observara datos rapidamente. No se recomienda hacer esto en un sistema de producción.

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

Encuentre la definición de fuentes `(%sources),` y cambiela a:

```
%sources = (
    'pfsense'    => { 'port' => '9001', 'col' => '#0000ff', 'type' => 'netflow' },
);
```

Crear el usuario netflow en el sistema

```
$ sudo useradd -d /var/nfsen -G www-data -m -s /bin/false netflow
```

Instalar NFSen e iniciarlo

```
$ cd
$ cd nfsen-1.3.6p1
```

Ahora se instala con el siguiente comando:

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

Cuando se solicite la ruta de perl, presiones ENTER.

Instalar el script de inicio

Con el fin de que nfsen se inicie y se detenga automaticamente cuando se inicie el sistema, se tiene que agregar un enlace al diretorio init.d apuntando al script de inicio nfsen:

Jaime Cabrera Letona
Universidad de San Carlos de Guatemala
jaimeco at usac.edu.gt
Noviembre 2014

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

Iniciar Nfsen

```
$ sudo service nfsen start
```

Compruebe que el proceso nfcapd se ha inciado:

```
$ ps auxwww | grep nfcapd
```

Ver los flujos a traves de la web:
Puede encontrar la pagina nfsen aqui:

```
http://servidor.dominio/nfsen/nfsen.php
```

Es posible que aparezca un mensaje como:
`Frontend - Backend version missmatch!`
Esto desaparecera si vuelve a cargar la pagina, no es un problema.

Hasta pronto