Install nfdump/nfsen on Slackware

Concepts you should know:

A device is setup to constantly send out netflow information, it is not polled.

A receiver listens for the netflow information 'streams' from devices and processes them.

How to install

A) Install/configure Apache 1) enable php

B) Configure the Cisco router to send netflow

1) Login to the Cisco router:

```
# telnet <YOUR ROUTER IP>
gw>enable
```

2) Configure the desired interface:

```
nm-gw# configure terminal
nm-gw(config)# interface S0/0
nm-gw(config)# ip route-cache flow
nm-gw(config)# exit
```

3) Repeat for all interfaces you want.

```
nm-gw# configure terminal
nm-gw(config)# interface F0/1
nm-gw(config)# ip route-cache flow
nm-gw(config)# exit
```

4) Set the flow destination and break long flows into 5 minute segments:

```
nm-gw# ip flow-export destination <YOUR NFSEN BOX IP> 9996
nm-gw# ip flow-export version 5
nm-gw# ip flow-cache timeout active 5
```

5) Make the changes permanent:

```
nm-gw# snmp-server ifindex persist
nm-gw# ^Z
nm-gw# write mem
```

6) Verify that it works:

```
nm-gw# show ip flow export
nm-gw# show ip cache flow
```

C) Install NFDUMP

1) Install nfdump. MAKE SURE "–enable-nfprofile" is set during .configure.

```
   At the time of this writing, there is a nfdump SBo pending approval. It
has nfprofile enabled.
```

D) Install NFSEN

1) Install RRDTool via SBo

2) Install MailTools (Perl) via SBo

3) Install Socket6 via CPAN

```
   perl -MCPAN -e 'install Socket6'
```

4) tar -svf nfsen-1.3.6p1.tar.gz

5) cd nfsen-1.3.6p1

6) Add nfsen dirs

```
   mkdir /data
   mkdir /data/nfsen
```

7) cp ./etc/nfsen-dist.conf /etc

8) Edit /etc/nfsen-dist.conf

```
   FROM: $HTMLDIR    = "/var/www/nfsen/";
   TO:   $HTMLDIR    = "/var/www/htdocs/nfsen/";
   FROM: $USER    = "netflow";
   TO: $USER    = "apache";
   FROM: $WWWUSER  = "www";
   TO: $WWWUSER  = "apache";
   FROM: $WWWGROUP = "www";
   TO: $WWWGROUP = "apache";
   FROM: $PREFIX  = '/usr/local/bin';
   TO: $PREFIX = '/usr/bin/';
   FROM: 'upstream1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' =>
'netflow' },
   and
   FROM: 'peer1'        => { 'port' => '9996', 'IP' => '172.16.17.18' },
   TO: 'sitename' => { 'port' => '9995', 'col' => '#0000ff', 'type' =>
'netflow' },
```

```
   and/or
   TO: 'sitename' => { 'port' => '9996', 'IP' => '172.16.17.18' },
   If you use the 'port only' version, each device will have to come in on
it's own port.
   If you use the 'IP' version, all devices can come in on the same port.
   You can send all the flows in on one port and use filters to separate
them.
```

7) cd /data/nfsen/bin/nfsen start

If installed correctly, you should be able to open your web browser and see stuff

```
   http://<YOU NFESENBOX>/nfsen/nfsen.php
```

Sources

howtos, software, nfsen, nfdump, network monitoring, needs attention, author arfon