Netflow мониторинг с помощью NfSen

Contents

1 Введение

1.1 Цели

- Научиться экспортировать потоки с роутера Cisco

1.2 Замечания

- Команды, предваряемые “$” означают, что они должны быть выполнены с правами обычного пользователя – а не администратора.
- Команды, предваряемые “#” означают, что вы должны иметь права администратора.
- Команды с более специфичными подсказками (например “rtrX>” или “mysql>”) означают что вы выполняете их либо на удаленном оборудовании, либо в какой-то другой программе.

2 Экспорт потоков с роутера Cisco

Вы настроите ваш роутер экспортировать потоки на все машины вашей группы

2.1 Группа 1, Роутер 1

```
rtr1 ==> pc1 на порт 9001
rtr1 ==> pc2 на порт 9001
rtr1 ==> pc3 на порт 9001
rtr1 ==> pc4 на порт 9001
```

2.2 Группа 2, Роутер 2

```
rtr2 ==> pc5 на порт 9001
rtr2 ==> pc6 на порт 9001
rtr2 ==> pc7 на порт 9001
rtr2 ==> pc8 на порт 9001
```

и т.д.

3 Настройка роутера

```
$ ssh cisco@rtrX.ws.nsrc.org
rtrX> enable
```

или, если ssh на роутере еще не настроен:

```
$ telnet 10.10.1.254
Username: cisco
Password:
Router1>enable
Password:
```

Нижеследующее сконфигурирует интерфейс FastEthernet 0/0 для экспорта потоков. Замените 10.10.X.A до 10.10.X.D на IP адреса машин вашей группы.

```
rtrX# configure terminal
rtrX(config)# flow exporter EXPORTER-1
rtrX(config-flow-exporter)# description Export to pcA
rtrX(config-flow-exporter)# destination 10.10.X.A
rtrX(config-flow-exporter)# transport udp 9001
rtrX(config-flow-exporter)# template data timeout 300
... repeat for EXPORTER-2 and pcB
... repeat for EXPORTER-3 and pcC
... repeat for EXPORTER-4 and pcD
rtrX(config-flow-exporter)# flow monitor FLOW-MONITOR-V4
```

```
rtrX(config-flow-monitor)# exporter EXPORTER-1
rtrX(config-flow-monitor)# exporter EXPORTER-2
rtrX(config-flow-monitor)# exporter EXPORTER-3
rtrX(config-flow-monitor)# exporter EXPORTER-4
rtrX(config-flow-monitor)# record netflow ipv4 original-input
rtrX(config-flow-monitor)# cache timeout active 300
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 input
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 output
rtrX(config-if)# exit
```

Поскольку вы не указали версию протокола NetFlow, по умолчанию будет использован NetFlow версии 9.

Команда “cache timeout active 300” разбивает долгоживущие потоки на 5-минутные фрагменты. Если вы оставите значение по умолчанию (30 минут), отчеты о трафику будут иметь пики.

> Замечание: для мониторинга потоков IPv6 вам пришлось бы создать новый монитор потоков для IPv6 и подсоединить его к интерфейсу и к существующим экспортерам потоков.
>
> ```
> flow monitor FLOW-MONITOR-V6
>  exporter EXPORTER-1
>  exporter EXPORTER-2
>  exporter EXPORTER-3
>  exporter EXPORTER-4
>  record netflow ipv6 original-input
>  cache timeout active 300
> interface FastEthernet 0/0
>  ipv6 flow monitor FLOW-MONITOR-V6 input
>  ipv6 flow monitor FLOW-MONITOR-V6 output
> ```

Также введите следующую команду:

```
rtrX(config)# snmp-server ifindex persist
```

Это включит неизменяемость значений ifIndex между перезагрузками роутера, а также в случае добавления либо удаления интерфейсных модулей на устройстве.

Теперь мы проверим, что все в порядке.

Вначале выйдите из режима кнофигурации:

```
rtrX(config)# exit
```

```
rtrX# show flow exporter EXPORTER-1
rtrX# show flow exporter EXPORTER-2
etc...
rtrX# show flow monitor FLOW-MONITOR-V4
```

Можно просмотреть индивидуальные активные потоки на роутере:

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache
```

У нас будут тысячи индивидуальных потоков, поэтому это не очень полезная возможность. Нажмите ‘q’ для выхода из постраничного вывода (если необходимо).

Вместо этого, сгруппируйте потоки так, что вы можете посмотреть список наиболее активных пользователей (по источникам и назначениям). Для этого используется вот такая длинная команда:

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source address
      ipv4 destination address sort counter bytes top 20
```

Если все выглядит нормально, сохраните конфигурацию в постоянной памяти:

```
rtrX#wr mem
```

Теперь вы можете выйти из роутера:

```
rtrX#exit
```

Убедитесь в том, что tcpdump установлен:

```
$ sudo apt-get install tcpdump
```

Теперь убедитесь, что потоки приходят с роутера на вашу машину:

```
$ sudo tcpdump -i eth0 -nn -Tcnfp port 9001
```

Подождите несколько секунд и вы должны увидеть что-то в этом роде:

```
06:12:00.953450 IP s2.ws.nsrc.org.54538 > noc.ws.nsrc.org.9009: NetFlow v5, 9222.333 uptime, 1359871921.013
  started 8867.952, last 8867.952
    10.10.0.241/0:0:53 > 10.10.0.250/0:0:49005 >> 0.0.0.0
    udp tos 0, 1 (136 octets)
  started 8867.952, last 3211591.733
    10.10.0.241/10:0:0 > 0.0.0.0/10:0:4352 >> 0.0.0.0
    ip tos 0, 62 (8867952 octets)
[...]
```

Это пакеты UDP, содержащие индивидуальные записи потоков.

(Обратите внимание, что реальный вывод может быть неправильным, так как tcpdump не декодирует пакеты NetFlow правильно)

На этом лабораторная работа закончена.

Перейдите к следующей работе, exercise2-install-nfdump-nfsen.