Содержание

Построение отчетов по IP

1. Добавить новый приемник данных в конфигурацию nfsen

```
vi /usr/local/nfsen/etc/nfsen.conf

%sources = (
'protocols' => { 'port' => '9997', 'col' => '#00ff00', 'type' => 'netflow'
},
'directions' => { 'port' => '9998', 'col' => '#ffff00', 'type' => 'netflow'
},
'full' => { 'port' => '9999', 'col' => '#114422', 'type' => 'netflow' }
);
```

2. активировать изменения в конфигурации

```
/usr/local/nfsen/bin/nfsen reconfig
```

3. разрешить прием udp на порт 9999 в iptables

```
vi /etc/sysconfig/iptables
-A INPUT -m state --state NEW -m udp -p udp --dport 9999 -j ACCEPT
service iptables restart
```

4. Активировать на dpi отправку полного netflow на созданный коллектор (в дополнении к коллекторам протоколов и направлений)

```
vi /etc/dpi/fastdpi.conf
netflow=11
netflow_full_collector=127.0.0.1:9999
netflow_passive_timeout=20
netflow_active_timeout=60
service fastdpi restart
```

nfsen не лучший инструмент для исследования полного netflow но позволяет строить простые отчеты (раздел на страничке Netflow Processing, например, top по ip)

В полном netflow по умолчанию передается оригинальный номер порта, поэтому отчет по протоколам не работает. Чтобы активировать кодирование в номере порта информации о протоколе нужно активировать настройку netflow_full_port_swap=1