Содержание

1. First, add the new data receiver to nfsen configuration:

```
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. Second, activate configuration changes:

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

3. Enable receiving UDP to port 9999 in iptables:

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

4. Activate sending the full netflow on DPI:

```
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 is not the best tool to study the full netflow. However, it allows to build simple reports (check the page Netflow Processing: for example, top by IP).

Full netflow sends the original port number by default. Therefore the report by protocols does not work. In order to activate coding of the protocol's information in a port number you have to activate configuration parameter netflow_full_port_swap=1