Initial NetFlow Configuration

On this page:

Setting NetFlow Collection Port

When you start the NetFlow Analyzer for the first time, you need to set NetFlow collection port before you can see traffic.

NetFlow collection port is a port on NetVizura server listening for NetFlow traffic exported by network devices. You need to set exporting port number on all your network devices to match NetFlow collection port. Default port number is 2055.

To set the NetFlow collection port:

1. Go to **Settings > NetFlow Settings > Configuration** tab
2. Type a new value in **Collection port** field
3. Click **Save**.

Checking the System

Now is a good time to check if the system is working properly.

To do so, follow these steps:

1. Check if the Collection port is set properly
   To see the Collection port number, go to **Settings > NetFlow Settings > Configuration** tab, and you will find the Service socket port field. Collection port number must match with the port number your network devices are exporting the netflow data to.

2. Make sure NetFlow data is collected
   Go to **TopN > System** tab. Packets tab shows if netflow UDP packets are received and Flows chart shows how many flows have been exported to NetVizura server

3. Check the system for warnings or errors.
   Click on the **Show log** arrow (in the bottom right corner). Any warnings or errors will be displayed as well as the instruction to resolve them.

4. Finally, check if the network traffic is available
   Go to **TopN > All Exporters** tab. Network traffic should be shown on the graphs, this is a verification that the network traffic data has been collected by the NetFlow Collector and that the data has been processed by NetFlow Aggregator.

Note that it may take up to 10 minutes to see traffic from a new exporter. This is the time needed for the application to create the finest sample of traffic since one sample lasts 5 minutes and two samples are needed to draw a line on the chart.

To learn more about system settings in general, go to chapter Configuring NetFlow System.

All other settings you do not need to set right away. However, you should get back to them once you get to know NetFlow Analyzer a little better and fine-tune the behaviour of your system.

Setting End User Traffic (Optionally)

In addition to general network traffic (Exporters, Traffic Patterns and Subnets Sets), you can view traffic made by organization end users (domain usernames).

To setup this traffic:

1. Check if the Collection port is set properly
   To see the Collection port number, go to **Settings > NetFlow Settings > Configuration** tab, and you will find the Service socket port field. End users collection port number must match with the port number your Syslog agent is exporting the logon syslog messages to.

2. Update existing or add new End User mapping rule

   If you use Snare as your Syslog agent, then you can use one of the provided mapping rules. In this case, just update **Source IP** field, verify if rule is matching users and change status to Active. To do so, go to **Settings > NetFlow Settings > End Users**.

If rule for your Syslog agent is not provided with NetVizura by default, you should create your own rule in order to successfully map users (link username with an IP address at specific time). Read more about how to setup custom End User mapping rule in the the article Configuring End Users.

3. Finally, check if the network traffic is available
   Go to **TopN > End Users** tab. Network traffic should be shown on the graphs, this is a verification that the network traffic data has been collected by the NetFlow Collector and that the data has been processed by NetFlow Aggregator.

Note that it may take up to 10 minutes to see traffic for a new user. This is the time needed for the application to create the finest sample of traffic since the sample lasts 5 minutes and two samples are needed to draw a line on the chart.

Specifying too broad subnet in the **Source IP** field might result in performance penalty. For best results consider changing Source IP to more specific value or concrete IP address.