



NetVizura 4.3 User Guide

1. What's New
2. Installation and Setup
2.1 System Requirements
2.2 Downloading
2.3 Installing
2.3.1 Linux DEB (Debian) Installation
2.3.2 Linux DEB (Ubuntu) Installation
2.3.3 Linux RPM (CentOS) Installation
2.3.4 Linux ISO (CentOS) Installation
2.4 Configuring Network Devices for NetFlow Export
2.4.1 Choosing Server Location
2.4.2 Configuring NetFlow Export (Ingress vs. Egress)
2.4.3 Choosing Exporters
2.4.4 Configuring Cisco Devices
2.4.5 Exporting Without NetFlow Capable Device (Mirroring to Daemon Server)
2.4.6 Exporting to Multiple Servers
2.5 Licensing
2.5.1 Upgrading License
2.5.2 Updating License
2.5.3 Estimating Number of Flows (NetFlow Analyzer License)
2.6 Updating NetVizura
2.6.1 Linux DEB (Debian & Ubuntu) Update
2.6.2 Linux RPM (CentOS) Update
2.7 Installing and Configuring Syslog Agent for End User Traffic
3. Getting Started
3.1 Initial Configuration
3.1.1 Initial General Configuration
3.1.2 Initial NetFlow Configuration
3.1.3 Initial EventLog Configuration
3.2 Navigation
3.2.1 General Navigation
3.2.2 NetFlow Navigation
3.2.3 EventLog Navigation
3.2.4 MIB Navigation
4. Using NetVizura
4.1 Basic NetFlow Usage
4.1.1 Using Charts and Tables
4.1.2 Traffic Distributions (Top Talkers)
4.1.2.1 Distribution by Interfaces
4.1.2.2 Distribution by Hosts
4.1.2.3 Distribution by Conversations
4.1.2.4 Distribution by Services
4.1.2.5 Distribution by Protocols
4.1.2.6 Distribution by QoS
4.1.2.7 Distribution by AS
4.1.3 Exporters and Interfaces Traffic
4.1.3.1 All Exporters Traffic
4.1.3.2 Exporter Traffic
4.1.3.3 Interface Traffic
4.1.3.4 Working with Exporters and Interfaces
4.1.4 Basic Traffic Patterns
4.1.4.1 Understanding Traffic Patterns
4.1.4.2 Viewing Traffic Patterns
4.1.4.3 Subnet Traffic in Traffic Patterns
4.1.4.4 Exporter Traffic vs Traffic Pattern
4.1.4.5 Basic Traffic Pattern Examples
4.1.5 Subnet Sets
4.1.5.1 Traffic Pattern in Subnet Sets
4.1.5.2 Viewing Subnet Set Traffic
4.1.5.3 Subnet Traffic in Subnet Sets
4.1.5.4 Subnet Set vs Subnet Traffic
4.1.6 Managing NetFlow Favorites
4.1.7 Reading NetFlow Details
4.1.8 Generating Reports
4.2 Advanced NetFlow Usage
4.2.1 Advanced Traffic Pattern Examples
4.2.2 Inspecting Raw Data (Flow Records)
4.2.3 Viewing End User Traffic
4.2.3.1 All Users Traffic
4.2.3.2 Domain Users Traffic
4.2.3.3 End User Traffic by Hosts
4.2.3.4 End User Traffic by Conversations
4.2.3.5 End User Traffic by Services
4.2.3.6 End User Traffic by Protocols
4.2.3.7 End User Traffic by QoS
4.2.3.8 End User Traffic by AS
4.2.4 Using NetFlow Alarms

4.2.5	Understanding NetFlow System Traffic
4.2.6	Using Activity Log
4.3	EventLog Usage
4.3.1	Viewing Syslog Messages
4.3.2	Inspecting Syslogs
4.3.3	Viewing SNMP Traps
4.3.4	Understanding Eventlog System Traffic
4.3.5	Using EventLog Alarms
4.3.6	Syslog How to...
4.4	MIB Usage
4.4.1	Searching OIDs
4.4.2	Setting a Current Device
4.4.3	Making SNMP Request
4.4.4	Managing MIB Favorites
4.4.5	Reading MIB Details
5.	Configuration
5.1	General Configuration
5.1.1	Managing Users
5.1.2	Configuring SNMP Policies
5.1.3	Configuring Devices
5.1.4	Managing License
5.1.5	Configuring E-Mail
5.1.6	Configuring Display Names
5.1.7	Configuring Time Window
5.2	NetFlow Configuration
5.2.1	Configuring Traffic Patterns
5.2.1.1	Defining the Traffic of Interest
5.2.1.2	Setting IP Address Ranges
5.2.1.3	Fine-tuning a Traffic Pattern
5.2.1.4	Manual Deduplication
5.2.2	Configuring Subnets
5.2.3	Configuring Subnet Sets
5.2.4	Configuring End Users
5.2.5	Configuring TopN Rules
5.2.6	Configuring NetFlow Alarms
5.2.7	Configuring Aggregator Filters
5.2.8	Configuring NetFlow Sampling
5.2.9	Configuring NetFlow System
5.2.9.1	NetFlow Service Options
5.2.9.2	NetFlow Database Maintenance
5.2.9.3	Archiving Raw Data
5.2.9.4	Importing/Exporting Configuration
5.2.9.5	Automatic Deduplication
5.3	EventLog Configuration
5.3.1	Syslog and SNMP Trap Filtering
5.3.2	Configuring EventLog Alarms
5.3.3	Configuring Eventlog System
5.4	MIB Configuration
5.4.1	Configuring MIB Modules
5.4.2	Configuring MIB Options
6.	Troubleshooting
6.1	General Troubleshooting
6.1.1	NetVizura is slow
6.1.2	Web interface not running
6.1.3	How to recover from Exception caught: 500 The call failed on the server
6.1.4	How to recover from RPC failure error
6.1.5	How to restart the application
6.1.6	How to submit a request
6.2	NetFlow Troubleshooting
6.2.1	No NetFlow traffic captured
6.2.2	End User traffic impact on NetVizura performance
6.3	EventLog Troubleshooting
6.3.1	I do not receive any Syslog messages
6.3.2	I set the Syslog socket port to 514 but I am still not receiving syslog messages (Linux)
6.4	MIB Troubleshooting
6.4.1	SNMP request lasts too long
6.4.2	SNMP request fails on a device
6.4.3	I can not add a MIB to Modules
6.4.4	I can not find an OID in the MIB tree
6.4.5	I can not set the OID value on a device
7.	FAQ
7.1	License FAQ
7.2	NetFlow FAQ

What's New

What's new in NetVizura version 4.3:

NETFLOW ANALYZER

1. End User traffic added
2. IP addresses are now shown as hostnames
3. IP addresses now include Whois description
4. AS are now shown as names instead of AS numbers
5. Admin can now remove exporters
6. User with Read privileges can now schedule reports, too
7. Traffic illustration images improved
8. Traffic table layout improved
9. Menu Panel (left sidebar) is now resizable
10. System performance optimized
11. Minor bugs fixed

MIB BROWSER

1. Modules bulk import added
2. Menu Panel (left sidebar) is now resizable

GENERAL

1. Latest online guide published [NetVizura Guide Homepage](#)

Installation and Setup

The following instructions are intended for users with administrator privileges (application and server) and a basic familiarity with netflow export and device configuration.

In this chapter we will guide you through the installation and basic setup related actions:

- [System Requirements](#)
- [Downloading](#)
- [Installing](#)
- [Configuring Network Devices for NetFlow Export](#)
- [Licensing](#)
- [Updating NetVizura](#)
- [Installing and Configuring Syslog Agent for End User Traffic](#)

System Requirements

System requirements depend primarily on the number of IP flows that will be received and processed by the system. The bigger the network traffic volume, the higher the number of IP flows. This reflects strongly on IP flow processing speed and Raw Data file size. The former rises the CPU speed requirement and the latter rises the amount of HDD space needed to store Raw Data.

In addition to this, HDD space requirement rises with the number of Traffic Patterns and subnets you create and with the amount of Raw Data files you decide to store on your system. The number of Traffic Patterns you create also affects the IP flow processing speed.

Hardware Requirements

NetFlow Analyzer

Package (max fps)	CPU	RAM	HDD Space
Free (5 fps)	Singe core 1.6GHz processor	2GB	5 GB
Express (50 fps)	Singe core 1.6GHz processor	4GB	10 GB
SME (500 fps)	Singe core 1.6GHz processor	4GB	100 GB
Enterprise (5,000 fps)	Modern dual core processor, each core at least 1.6GHz	16GB	100 GB - SAS or SSD in RAID 0 or similar setup with striping
Large Enterprise (10,000 fps)	Modern quad core processor, each core at least 1.6GHz	16GB	200 GB - SAS or SSD in RAID 0 or similar setup with striping

Note: The recommended server requirements assume default configuration for NetVizura NetFlow Analyzer. Significantly increasing the number of flows processed (above 10.000 fps on average), and monitoring nodes can increase CPU and memory requirements. Significantly increasing the number of flows and flow archive storing time will increase flow archive size and require more HDD space and/or additional external storage.

Assumptions: 10.000 fps, 1.000 counters, 30 days of Raw Data and 365 days of database history stored.

- NetVizura comes with built-in database which will be installed on the NetVizura server. You can use a different server for your database to achieve better performance but note that NetVizura only supports PostgreSQL version 9.2 or higher.
- NetFlow Analyzer Raw Data files are stored on the NetVizura server. You can store them in some other storage, but keep in mind that it can have a considerable impact on the performance due to large files being transferred across your network between the NetVizura server and Raw data files storage.

EventLog Analyzer

logs/s	CPU	RAM	HDD Space
100	Singe core 1.6 GHz	8GB	2 GB/day - SAS or SSD in RAID 0 or similar set-up with striping
5,000	Quad Core 2.00 GHz	8GB	100 GB/day- SAS or SSD in RAID 0 or similar setup with striping
10,000	Quad Core 2.00 GHz	8GB	365 GB/day - SAS or SSD in RAID 0 or similar setup with striping
20,000	Quad Core 2.00 GHz	8GB	725 GB/day - SAS or SSD in RAID 0 or similar setup with striping

On this page:

- Hardware Requirements
 - NetFlow Analyzer
 - EventLog Analyzer
- Software Requirements
- Supported OS
- Supported Browsers

NetFlow Analyzer is highly flexible and you can configure it to minimize system requirements cost. To get more details on configuration, see [NetFlow Settings > Configuration](#).

To learn more on how calculation is made or how to make your own custom HDD space estimation, see [NV NetFlow HDD calculator.xlsx](#).

Note: The recommended server requirements assume default configuration. Significantly increasing the number of Syslogs and SNMP traps processed (above 20000 per second on average) and adding alarms can increase CPU and memory requirements. Significantly increasing the number of logs will increase EventLog database size and require more HDD space.

Software Requirements

	Packaged with NetFlow Analyzer	Notes
Oracle Java 7	No	<ul style="list-style-type: none"> Downloaded from Oracle site Oracle Java 8 can be used, but is not thoroughly tested
Apache Tomcat 6	No	<ul style="list-style-type: none"> Installed from default Linux repositories Should be installed only after Oracle Java is installed Other versions of Tomcat are not tested
PostgreSQL 9.2+	No	<ul style="list-style-type: none"> Detailed installation described in installation guide PostgreSQL 8.4 and later versions are all tested, but 9.2 is recommended minimum

Supported OS

	Versions and Distributions	Notes
Linux	Debian Wheezy 7 (64 bit),	Installed with DEB package
Linux	Ubuntu Precise 12.04 (64-bit)	Installed with DEB package
Linux	Ubuntu Trusty 14.04 (64-bit)	Installed with DEB package
Linux	CentOS 6 (64 bit)	Installed with RPM package






Supported Browsers

	Versions	Notes
Chrome	35.0+	
Firefox	26.0+	
Internet Explorer	10.0+	

Downloading

Use the following steps to download the required files for NetVizura installation:

1. Navigate to **Downloads** page where latest software version are offered
2. Choose the desired software version from the cards below and click **Download**
3. Provide your registration information and click **Submit**
4. Read the given instructions and click on **Download link**
5. The installer file will be downloaded to your computer

<p>Linux RPM (Cent OS)</p> <p>version 4.2.1 (Free Trial)</p>  <p>CentOS</p> <p>47 MB</p> <p>Download</p>	<p>Linux DEB (Debian)</p> <p>version 4.2.1 (Free Trial)</p>  <p>debian</p> <p>47 MB</p> <p>Download</p>	<p>ISO image (CentOS)</p> <p>version 4.2.1 (Free Trial)</p>  <p>ISO</p> <p>765 MB</p> <p>Download</p>	<p>Windows OS</p> <p>version 4.2.1 (Free Trial)</p>  <p>765 MB</p> <p>Contact Us</p>
<p> Still not sure? Try Out Online now! Before downloading Free Trial version, please read the terms of our End User License Agreement (EULA).</p>			

Free Trial licence with evaluation period of 30 days from the day of installation includes the following functional restrictions:

- NetFlow module allows you to process up to three exporters, and up to 10.000 flows per minute
- For EventLog module allows you to process up to three exporters
- MIB module has no restrictions

- To upgrade your Free Trial or Commercial license, read more at [Upgrading License](#).
- If you want to transfer your configuration from old software version to new one, see more at [Importing/Exporting Configuration](#).

Installing

NetVizura can be installed on Linux (CentOS and Debian) distributions. The following sections describe installation procedures for each stated operating system:

- [Linux DEB \(Debian\) Installation](#)
- [Linux DEB \(Ubuntu\) Installation](#)
- [Linux RPM \(CentOS\) Installation](#)
- [Linux ISO \(CentOS\) Installation](#)

Linux DEB (Debian) Installation

Before installing NetVizura make sure to set the time on your server correctly. Time change after the installation will invalidate the license!

Before installing NetVizura you will have to install: Oracle Java 1.7, Tomcat 7 and PostgreSQL 9.3 or higher, in that order. The installation process has been tested on Debian 7.

On this page:

- NetVizura Installation Steps
- Post Install Steps
 - Tomcat Memory Allocation
 - Tweaking PostgreSQL
 - PostgreSQL "safe" tweaks
 - PostgreSQL "unsafe" tweaks

NetVizura Installation Steps

To install NetVizura follow these steps:

Step 1: sudo package installation: execute `apt-get install sudo`

Step 2: Oracle Java 1.7 package installation:

Default Java implementation is OpenJDK. You need to install Oracle Java package. Java packages should be installed before the Tomcat7 packages, if not Tomcat will use OpenJDK

1. To add the WebUpd8 Oracle Java PPA repository to the Software Sources in Debian, use the following commands:

```
echo "deb http://ppa.launchpad.net/webupd8team/java/ubuntu precise
main" | tee /etc/apt/sources.list.d/webupd8team-java.list
echo "deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu
precise main" | tee -a
/etc/apt/sources.list.d/webupd8team-java.list
apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
EEA14886
```

2. execute command `apt-get update`
 - a. ignore the error about "public key is not available"
3. execute command `apt-get install oracle-java7-installer` and answer affirmatively to "Proceed without verification" and all other installation questions
4. execute command `ln -s /usr/lib/jvm/java-7-oracle /usr/lib/jvm/default-java` to set Oracle's Java as a default Java on the system
5. check if java is properly installed with command `java -version`

If you are behind a firewall / router that blocks some of the redirects required to download the Oracle Java archive, you can download the JDK tar.gz archive manually and place it under `/var/cache/oracle-jdk7-installer` - then, installing the "oracle-java7-installer" package will use the local archive instead of trying it to download it itself.

Step 3: Tomcat 7 package installation:

1. execute command `apt-get install tomcat7`
2. start Tomcat: `service tomcat7 start`
3. verify that Tomcat is running properly with the command `service tomcat7 status`

Step 4: PostgreSQL package installation

1. Create a file `pgdg.list` in `/etc/apt/sources.list.d/` with some text editor: `nano /etc/apt/sources.list.d/pgdg.list` and add the following line:
`deb http://apt.postgresql.org/pub/repos/apt/ wheezy-pgdg main`
2. execute command: `wget --quiet -O - http://apt.postgresql.org/pub/repos/apt/ACCC4CF8.asc | sudo apt-key add -`
3. execute command `apt-get update`
4. execute command `apt-get install postgresql postgresql-client`
5. verify that PostgreSQL is running properly with the command `service postgresql status`

Step 5: NetVizura packages installation

After this steps, install the NetVizura packages downloaded from the website with the command: `dpkg -i downloaded_file_name.deb`

To access the application, type <http://myip:8080/netvizura> in your browser. The default user account with administrator privileges is: username: **admin**, password: **admin01**

Post Install Steps

Tomcat Memory Allocation

After installation tweaking of configuration files is required in order to utilize the installed RAM to the fullest extent. The main consumers of RAM are operating system, PostgreSQL database and Tomcat. General rule for distributing memory is to split it in ratio 2:1 between PostgreSQL and Tomcat with 1 GB or more reserved for operating system. For instance:

Installed RAM	PostgreSQL	Tomcat	OS
4 GB	2 GB	1 GB	1 GB
16 GB	10 GB	5 GB	1 GB

During installation NetVizura automatically allocates memory for Tomcat process. The amount allocated to Tomcat process is calculated according to the formula:

$(RAM_{total} - 1GB) / 3$ but no less than 1GB.

For instance:

Total RAM	Tomcat
3 GB	1 GB
4 GB	1 GB
16 GB	5 GB

However, if you need to tweak Tomcat RAM allocation differently (the example for 2048MB):

1. Edit file `/etc/default/tomcat7`
2. Locate `JAVA_OPTS` environment variable that defines memory and uncomment it if it is commented. This line looks something like the following:
`JAVA_OPTS="{JAVA_OPTS} -Xmx1024m -Xms1024m +UseConcMarkSweepGC"`
3. Modify the `-Xmx` parameter to allocate additional memory to Tomcat. Additionally, set parameter `-Xms` to the same amount. This should look something like:
`JAVA_OPTS="-Djava.awt.headless=true -Xmx2048M -Xms2048M -XX:+UseConcMarkSweepGC"`
4. Save the file and restart Tomcat: `service tomcat7 restart`

Tweaking PostgreSQL

Tweaking PostgreSQL for best performance is a topic on which many books were written, but the following are some common sense suggestions. In general there are two groups of PostgreSQL tweaks that are helpful for NetVizura performance - "safe" and "unsafe" tweaks. "Safe" tweaks are those which can be applied in all cases. "Unsafe" tweaks trade reliability for performance. For the curious ones recommended reads (among countless others) are [PostgreSQL Optimization Guide](#), [PostgreSQL Tuning Guide](#), [this article](#) and [this book](#).

In order to apply following tweaks edit file `/etc/postgresql/Pg_VERSION_NUMBER/main/postgresql.conf`. You will need to restart the PostgreSQL service after done editing with command: `service postgresql restart`. Almost all of the following parameters are commented with carron character (`#`). Although these tweaks are considered "safe" do take notice of the default values. Usually you can comment out the parameter that has been changed and PostgreSQL will revert to the default value.

PostgreSQL "safe" tweaks

In the following example it is assumed that 4 GB of RAM is allocated for PostgreSQL.

parameter	recommended value	comment
max_connections	30	NetVizura rarely uses more than 10 connections simultaneously, but it is good to have some reserve
shared_buffers	1024MB	the recommended amount is RAM/4
effective_cache_size	2048MB	the recommended amount is RAM/2, possibly even RAM * 3/4
checkpoint_segments	32	for write intensive apps (as NetVizura) it should be at least 16, with 32 as safe maximum
checkpoint_completion_target	0.9	
default_statistics_target	100	
work_mem	8MB - 12MB	The formula used is max_connections*work_mem <= RAM/8, but using a bit more is still "safe"

PostgreSQL "unsafe" tweaks

These optimizations are considered "unsafe" since they *could* in very rare cases lead to data loss and/or corruption. If your VM is properly backed up we would consider the following optimizations safe. The following bring huge performance boosts to DB write process.

parameter	recommended value	comment
maintenance_work_mem	32MB	speeds up DB self clean process, not really important
wal_buffers	16MB	
full_page_writes	off	
fsync	off	don't wait for HDD to finish previous <i>write</i> operation. This brings the most benefit, but is considered potentially the most unsafe of all. If there is OS or HDD failure in exact instant when PSQL issues write command to HDD, that data will be lost and the DB itself could be corrupted. On the other hand, DB can issue several magnitude more write commands in the same time period and consider all these done, thus improving write performance immensely.
synchronous_commit	off	similarly to "fsync" but less unsafe and with less benefit
checkpoint_segments	64	how much is cached in temp files before it is issued to <i>proper</i> DB files. Issuing big chunks of data for write rarely is usually better for performance than issuing small chunks often

Linux DEB (Ubuntu) Installation

Before installing NetVizura make sure to set the time on your server correctly. Time change after the installation will invalidate the license!

Before installing NetVizura you will have to install: Oracle Java 1.7, Tomcat 7 and PostgreSQL 9.3 or higher, in that order. The installation process has been tested on Ubuntu 14.

On this page:

- NetVizura Installation Steps
- Post Install Steps
 - Tomcat Memory Allocation
 - Tweaking PostgreSQL
 - PostgreSQL "safe" tweaks
 - PostgreSQL "unsafe" tweaks

NetVizura Installation Steps

To install NetVizura follow these steps:

Step 1: sudo package installation: execute `apt-get install sudo`

Step 2: Oracle Java 1.7 package installation:

Default Java implementation is OpenJDK. You need to install Oracle Java package. Java packages should be installed before the Tomcat7 packages, if not Tomcat will use OpenJDK

1. in file `/etc/apt/sources.list`, add the following lines:

```
deb http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main
deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu
trusty main
```

2. execute command `apt-get update`

1. a. ignore the error about "public key is not available"

If you receive something like:

```
W: GPG error: http://ppa.launchpad.net trusty InRelease: The following
signatures couldn't be verified because the public key is not available:
NO_PUBKEY C2518248EEA14886
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/main/source/Sources Hash Sum mismatch

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/universe/source/Sources Hash Sum mismatch

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/main/binary-amd64/Packages Hash Sum mismatch

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/universe/binary-amd64/Packages Hash Sum mismatch

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/main/binary-i386/Packages Hash Sum mismatch

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/trusty-security/universe/binary-i386/Packages Hash Sum mismatch

E: Some index files failed to download. They have been ignored, or old
ones used instead.
```

enter the following commands:

```
rm /var/lib/apt/lists/* -vf
apt-get update
```

3. execute command `apt-get install oracle-java7-installer` and answer affirmatively to "Proceed without verification" and all other installation questions

4. execute command `ln -s /usr/lib/jvm/java-7-oracle /usr/lib/jvm/default-j`

ava to set Oracle's Java as a default Java on the system

5. check if java is properly installed with command `java -version`

Step 3: Tomcat 7 package installation:

1. execute command `apt-get install tomcat7`
2. start Tomcat: `service tomcat7 start`
3. verify that Tomcat is running properly with the command `service tomcat7 status`

Step 4: PostgreSQL package installation

1. Create a file `pgdg.list` in `/etc/apt/sources.list.d/` with some text editor:

`nano /etc/apt/sources.list.d/pgdg.list` and add the following line:

```
deb http://apt.postgresql.org/pub/repos/apt/ trusty-pgdg main
```

2. execute command: `wget --quiet -O - http://apt.postgresql.org/pub/repos/apt/ACCC4CF8.asc | sudo apt-key add -`
3. execute command `apt-get update`
4. execute command `apt-get install postgresql postgresql-client`
5. verify that PostgreSQL is running properly with the command `service postgresql status`

Step 5: NetVizura packages installation

After this steps, install the NetVizura packages downloaded from the website with the command: `dpkg -i downloaded_file_name.deb`

To access the application, type <http://myip:8080/netvizura> in your browser. The default user account with administrator privileges is: username: admin, password: admin01

Post Install Steps

Tomcat Memory Allocation

After installation tweaking of configuration files is required in order to utilize the installed RAM to the fullest extent. The main consumers of RAM are operating system, PostgreSQL database and Tomcat. General rule for distributing memory is to split it in ratio 2:1 between PostgreSQL and Tomcat with 1 GB or more reserved for operating system. For instance:

Installed RAM	PostgreSQL	Tomcat	OS
4 GB	2 GB	1 GB	1 GB
16 GB	10 GB	5 GB	1 GB

During installation NetVizura automatically allocates memory for Tomcat process. The amount allocated to Tomcat process is calculated according to the formula:

$(RAM_{total} - 1GB) / 3$ but no less than 1GB.

For instance:

Total RAM	Tomcat
3 GB	1 GB
4 GB	1 GB
16 GB	5 GB

However, if you need to tweak Tomcat RAM allocation differently (the example for 2048MB):

1. Edit file `/etc/default/tomcat7`
2. Locate `JAVA_OPTS` environment variable that defines memory and uncomment it if it is commented. This line looks something like the following:
`JAVA_OPTS="{JAVA_OPTS} -Xmx1024m -Xms1024m +UseConcMarkSweepGC"`
3. Modify the `-Xmx` parameter to allocate additional memory to Tomcat. Additionally, set parameter `-Xms` to the same amount. This should look something like:
`JAVA_OPTS="-Djava.awt.headless=true -Xmx2048M -Xms2048M -XX:+UseConcMarkSweepGC"`
1. Save the file and restart Tomcat: `service tomcat7 restart`

Tweaking PostgreSQL

Tweaking PostgreSQL for best performance is a topic on which many books were written, but the following are some common sense suggestions. In general there are two groups of PostgreSQL tweaks that are helpful for NetVizura performance - "safe" and "unsafe" tweaks. "Safe" tweaks are those which can be applied in all cases. "Unsafe" tweaks trade reliability for performance. For the curious ones recommended reads (among countless others) are [PostgreSQL Optimization Guide](#), [PostgreSQL Tuning Guide](#), this article and this book.

In order to apply following tweaks edit file `/etc/postgresql/Pg_VERSION_NUMBER/main/postgresql.conf`. You will need to restart the PostgreSQL service after done editing with command: `service postgresql restart`. Almost all of the following parameters are commented with carron character (#). Although these tweaks are considered "safe" do take notice of the default values. Usually you can comment out the parameter that has been changed and PostgreSQL will revert to the default value.

PostgreSQL "safe" tweaks

In the following example it is assumed that 4 GB of RAM is allocated for PostgreSQL.

parameter	recommended value	comment
<code>max_connections</code>	30	NetVizura rarely uses more than 10 connections simultaneously, but it is good to have some reserve
<code>shared_buffers</code>	1024MB	the recommended amount is $RAM/4$
<code>effective_cache_size</code>	2048MB	the recommended amount is $RAM/2$, possibly even $RAM * 3/4$
<code>checkpoint_segments</code>	32	for write intensive apps (as NetVizura) it should be at least 16, with 32 as safe maximum
<code>checkpoint_completion_target</code>	0.9	
<code>default_statistics_target</code>	100	
<code>work_mem</code>	8MB - 12MB	The formula used is $max_connections * work_mem \leq RAM/8$, but using a bit more is still "safe"

PostgreSQL "unsafe" tweaks

These optimizations are considered "unsafe" since they *could* in very rare cases lead to data loss and/or corruption. If your VM is properly backed up we would consider the following optimizations safe. The following bring huge performance boosts to DB write process.

parameter	recommended value	comment
<code>maitenance_work_mem</code>	32MB	speeds up DB self clean process, not really important
<code>wal_buffers</code>	16MB	
<code>full_page_writes</code>	off	

<code>fsync</code>	off	don't wait for HDD to finish previous <i>write</i> operation. This brings the most benefit, but is considered potentially the most unsafe of all. If there is OS or HDD failure in exact instant when PSQL issues write command to HDD, that data will be lost and the DB itself could be corrupted. On the other hand, DB can issue several magnitude more write commands in the same time period and consider all these done, thus improving write performance immensely.
<code>synchronous_commit</code>	off	similarly to "fsync" but less unsafe and with less benefit
<code>checkpoint_segments</code>	64	how much is cached in temp files before it is issued to <i>proper</i> DB files. Issuing big chunks of data for write rarely is usually better for performance than issuing small chunks often

Linux RPM (CentOS) Installation

Before installing NetVizura make sure to set the time on your server correctly. Time change after the installation will invalidate the license!

Before installing NetVizura you will have to install: Oracle Java 1.7, Apache Tomcat 6 and PostgreSQL 9.3 or higher, in that order. The installation process has been tested on CentOS 6.6.

On this page:

- NetVizura Installation Steps
- Post Install Steps
 - Tomcat Memory Allocation
 - Tweaking PostgreSQL
 - PostgreSQL L "safe" tweaks
 - PostgreSQL L "unsafe" tweaks

NetVizura Installation Steps

To install NetVizura follow these steps:

Step 1: sudo command installation: `yum install sudo`

Step 2: Oracle Java 1.7 package installation:

Default Java implementation is OpenJDK. You need to install Oracle Java package. Java packages should be installed before the Tomcat6 packages, if not Tomcat will use OpenJDK.

1. download .rpm JDK package from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
2. install the downloaded package: `rpm -Uvh file_name.rpm`
3. execute the following commands (adjust the filepath to the JDK installation path if needed)
 - a. `alternatives --install /usr/bin/java java /usr/java/jdk1.7.0_21/jre/bin/java 20000`
 - b. `alternatives --install /usr/bin/javaws javaws /usr/java/jdk1.7.0_21/jre/bin/javaws 20000`
 - c. `alternatives --install /usr/bin/javac javac /usr/java/jdk1.7.0_21/bin/javac 20000`
 - d. `alternatives --install /usr/bin/jar jar /usr/java/jdk1.7.0_21/bin/jar 20000`
4. check if Java is properly installed with command `java -version`

Step 3: Apache Tomcat 6 package installation:

1. execute command `yum install tomcat6`
2. in folder `/usr/sbin` edit file `tomcat6`: change the line "`set_javacmd`" to "`JAVACMD=/usr/java/latest/bin/java`"
3. save changes and start tomcat: `service tomcat6 start`
4. verify that Tomcat is running properly with the command `service tomcat6 status`
5. add Tomcat service to system startup: `chkconfig tomcat6 on`

Step 4: PostgreSQL package installation:

1. edit file `/etc/yum/repos.d/CentOS-Base.repo`
 - a. in section [base] add line "`exclude=postgresql*`"
 - b. in section [updates] add line "`exclude=postgresql*`"
2. go to <http://yum.postgresql.org/> and choose appropriate PostgreSQL package in regard to your CentOS version and architecture.
CentOS 6, 64 bit example: http://yum.postgresql.org/9.3/redhat/rhel-6-x86_64/pgdg-centos93-9.3-6.noarch.rpm
3. in the folder where the file is downloaded execute command `rpm -ivh pgdg-centos93-9.3-6.noarch.rpm`
4. execute command `yum install postgresql93-server`
5. execute command `service postgresql-9.3 initdb`
6. execute command `service postgresql-9.3 start`
7. verify that PostgreSQL is running properly with the command `service postgresql-9.3 status`
8. add PostgreSQL service to system startup: `chkconfig postgresql-9.3 on`

Step 5: Installing NetVizura packages

After this steps, install the NetVizura packages downloaded from the website with the command `yum localinstall downloaded_file_name.rpm`

To access the application, type <http://myip:8080/netvizura> in your browser. The default user account with administrator privileges is: username: **admin**, password: **admin01**

Post Install Steps

Tomcat Memory Allocation

After installation tweaking of configuration files is required in order to utilize the installed RAM to the fullest extent. The main consumers of RAM are operating system, PostgreSQL database and Tomcat. General rule for distributing memory is to split it in ratio 2:1 between PostgreSQL and Tomcat with 1 GB or more reserved for operating system.

For instance:

Installed RAM	PostgreSQL	Tomcat	OS
4 GB	2 GB	1 GB	1 GB
16 GB	10 GB	5 GB	1 GB

During installation NetVizura automatically allocates memory for Tomcat process. The amount allocated to Tomcat process is calculated according to the formula:

$(RAM_{total} - 1GB) / 3$ but no less than 1GB.

For instance:

Total RAM	Tomcat
3 GB	1 GB
4 GB	1 GB
16 GB	5 GB

However, if you need to tweak Tomcat RAM allocation differently (the example for 2048MB):

1. Edit file `/etc/tomcat6/tomcat6.conf`
2. Locate `JAVA_OPTS` environment variable that defines memory This line looks something like the following:
`JAVA_OPTS="{JAVA_OPTS} -Xmx1024m -Xms1024m"`
3. Modify the `-Xmx` and `-Xms` to the same amount. This should look something like:
`JAVA_OPTS="{JAVA_OPTS} -Xmx2048M -Xms2048M"`
4. Save the file and restart Tomcat: `service tomcat6 restart`

Tweaking PostgreSQL

Tweaking PostgreSQL for best performance is a topic on which many books were written, but the following are some common sense suggestions. In general there are two groups of PostgreSQL tweaks that are helpful for NetVizura performance - "safe" and "unsafe" tweaks. "Safe" tweaks are those which can be applied in all cases. "Unsafe" tweaks trade reliability for performance. For the curious ones recommended reads (among countless others) are [PostgreSQL Optimization Guide](#), [PostgreSQL Tuning Guide](#), [this article](#) and [this book](#).

In order to apply following tweaks edit file `/var/lib/pgsql/Pg_VERSION_NUMBER/data/postgresql.conf`. You will need to restart the PostgreSQL service after done editing with command: `service postgresql restart`. Almost all of the following parameters are commented with carron character (`#`). Although these tweaks are considered "safe" do take notice of the default values. Usually you can comment out the parameter that has been changed and PostgreSQL will revert to the default value.

PostgreSQL "safe" tweaks

In the following example it is assumed that 4 GB of RAM is allocated for PostgreSQL.

parameter	recommended value	comment
max_connections	30	NetVizura rarely uses more than 10 connections simultaneously, but it is good to have some reserve
shared_buffers	1024MB	the recommended amount is RAM / 4
effective_cache_size	2048MB	the recommended amount is RAM / 2, possibly even RAM * 3 / 4
checkpoint_segments	32	for write intensive apps (as NetVizura) it should be at least 16, with 32 as safe maximum
checkpoint_completion_target	0.9	
default_statistics_target	100	
work_mem	8MB - 12MB	The formula used is max_connections*work_mem <= RAM / 8, but using a bit more is still "safe"

PostgreSQL "unsafe" tweaks

These optimizations are considered "unsafe" since they *could* in very rare cases lead to data loss and/or corruption. If your VM is properly backed up we would consider the following optimizations safe. The following bring huge performance boosts to DB write process.

parameter	recommended value	comment
maintenance_work_mem	32MB	speeds up DB self clean process, not really important
wal_buffers	16MB	
full_page_writes	off	
fsync	off	don't wait for HDD to finish previous <i>write</i> operation. This brings the most benefit, but is considered potentially the most unsafe of all. If there is OS or HDD failure in exact instant when PSQL issues write command to HDD, that data will be lost and the DB itself could be corrupted. On the other hand, DB can issue several magnitude more write commands in the same time period and consider all these done, thus improving write performance immensely.
synchronous_commit	off	similarly to "fsync" but less unsafe and with less benefit
checkpoint_segments	64	how much is cached in temp files before it is issued to <i>proper</i> DB files. Issuing big chunks of data for write rarely is usually better for performance than issuing small chunks often

Linux ISO (CentOS) Installation

The following guide shows how to install CentOS-6.5 with NetVizura.

netvizura-x.y.z-linux.iso is a modified installation of CentOS-6.5-x86_64-Minimal.ISO Linux operating system. The ISO provides fast and easy way to install NetVizura and operating system on your virtual or hardware machine.

CentOS.6.5-NetVizura.iso includes following software packages:

- CentOS-6.5-x86_64-Minimal.ISO: <http://wiki.centos.org/Manuals/ReleaseNotes/CentOSMinimalCD6.5>;
- various dependency packages: sudo, Java-jdk-7u51-linux-x64, Tomcat6, postgresql93-server;
- NetVizura RPM installation package.

If you are installing on VM by using hypervisor:

- Some hypervisors can bypass boot scripts using its own OS installation rules from selected templates.
- When you create VM for **netvizura-x.y.z-linux.iso**, do not use any hypervisor templates which refer to some OS.
- Select **Other** from selection menu, attach **netvizura-x.y.z-linux.iso** on virtual CD controller and boot ISO straight from virtual CD.
- If Welcome screen (shown in the first step below) appears during boot, then the installation is properly launched.

On this page:

- NetVizura Installation Steps
- Post Install Steps

NetVizura Installation Steps

Step-by-step guide:

1. Select Auto-Installer

First screen shows the following options:

```
Welcome to NetVizura(CentOS-6.5_x86.64) Installer!  
  
NetVizura Auto-Installer  
Check installation media  
Boot from local drive  
Memory test
```

Press [Tab] to edit options



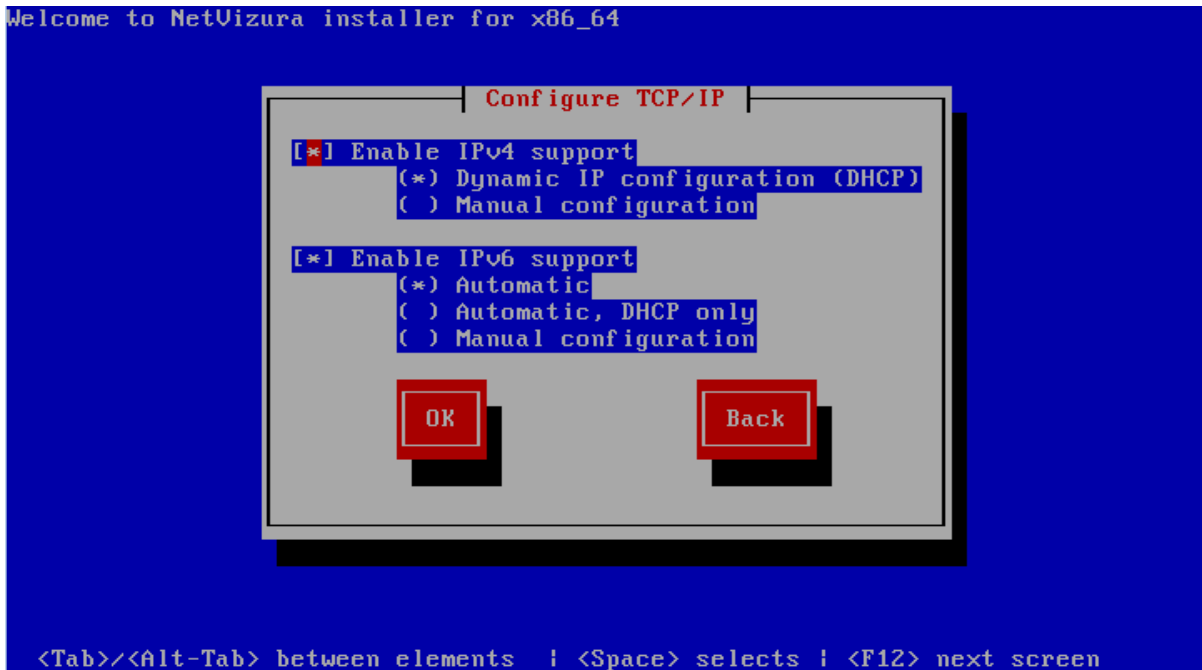
- Use Tab, arrows or Page Up/Down to move between options
- Use Space to confirm the selection

On this screen choose "**NetVizura Auto-installer**" option and press **Enter**.

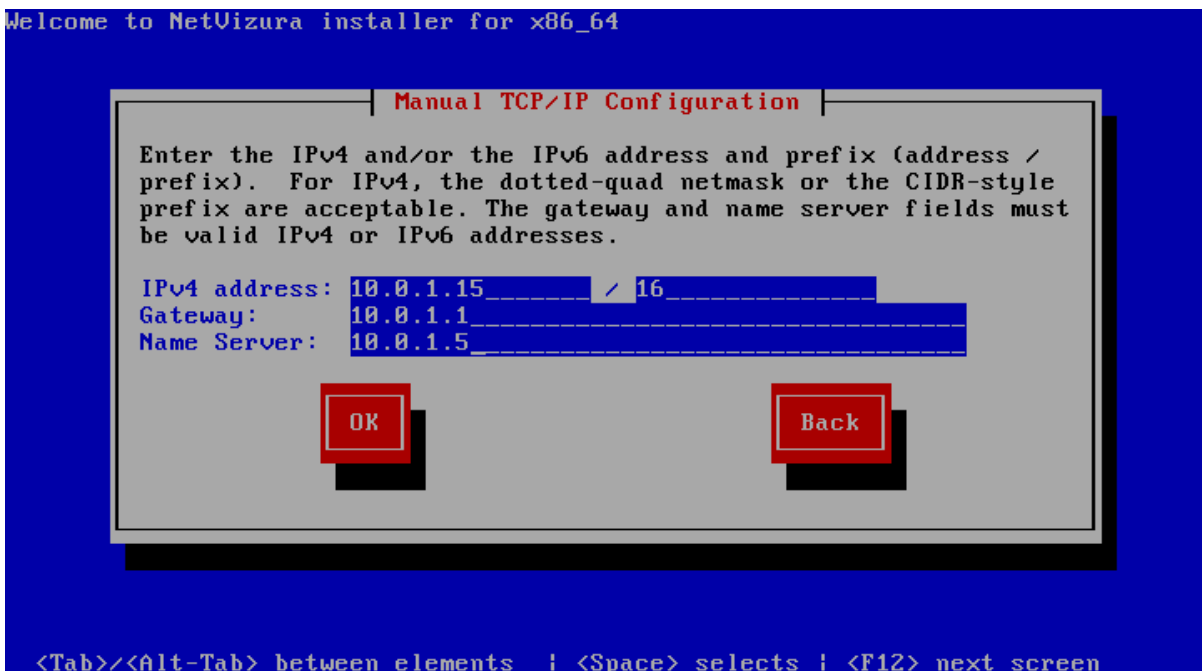
This will lead you to complete installation of NetVizura software with all necessary software dependency packages.

2. Configure network

On the following "Configure TCP/IP" screen you can set up the network subsystem.



- Select IP version support option (either **Enable IPv4 support** or **Enable IPv6 support**)
- Select suboption:
 - **Dynamic IP configuration (DHCP)**: Choose this option if you have DHCP server in your network and wait for NetworkManager to configure your network interface.
 - **Manual configuration**: Choose this option for manual network configuration

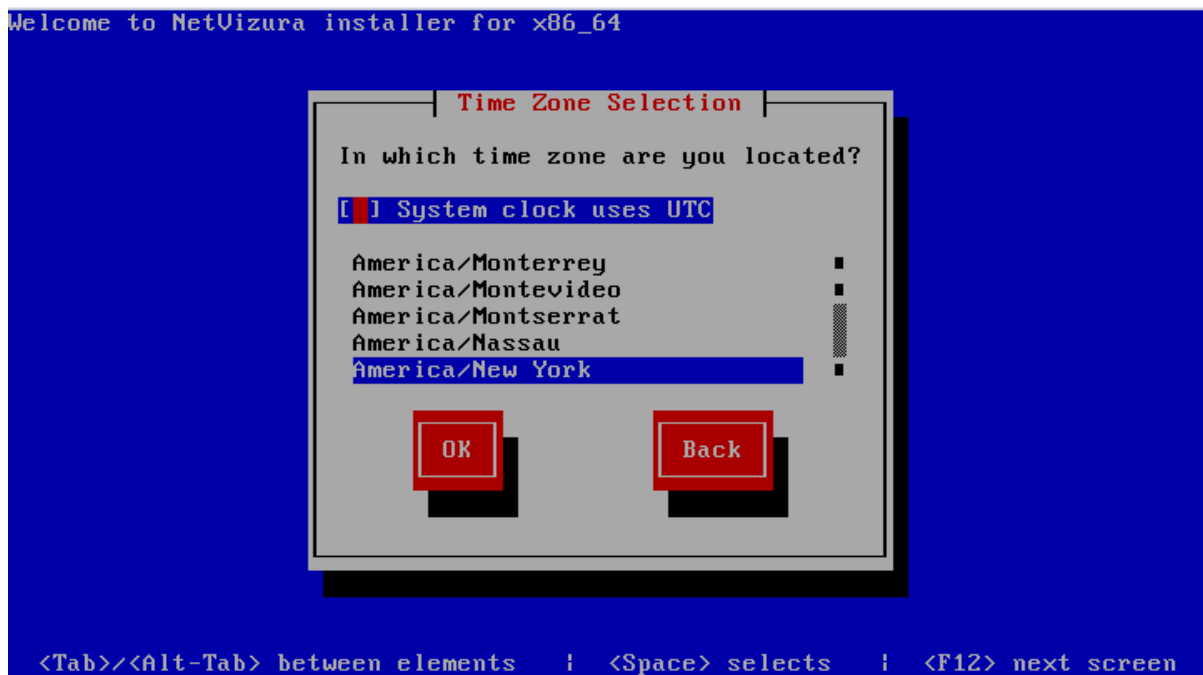


3. Choose your zone

Be sure to set time correctly:

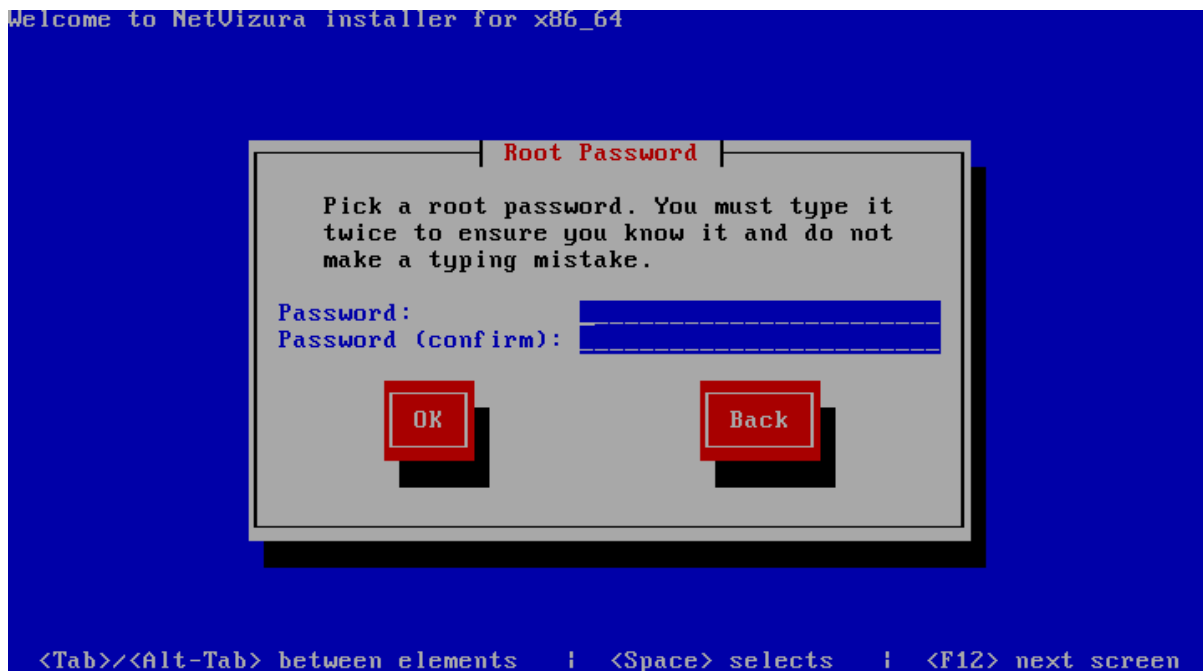
It is very important to set the correct UTC time in your BIOS setup because traffic analysis, charts and logs depend on it.

Also, set the time before installation. Time change after the installation will invalidate the license!

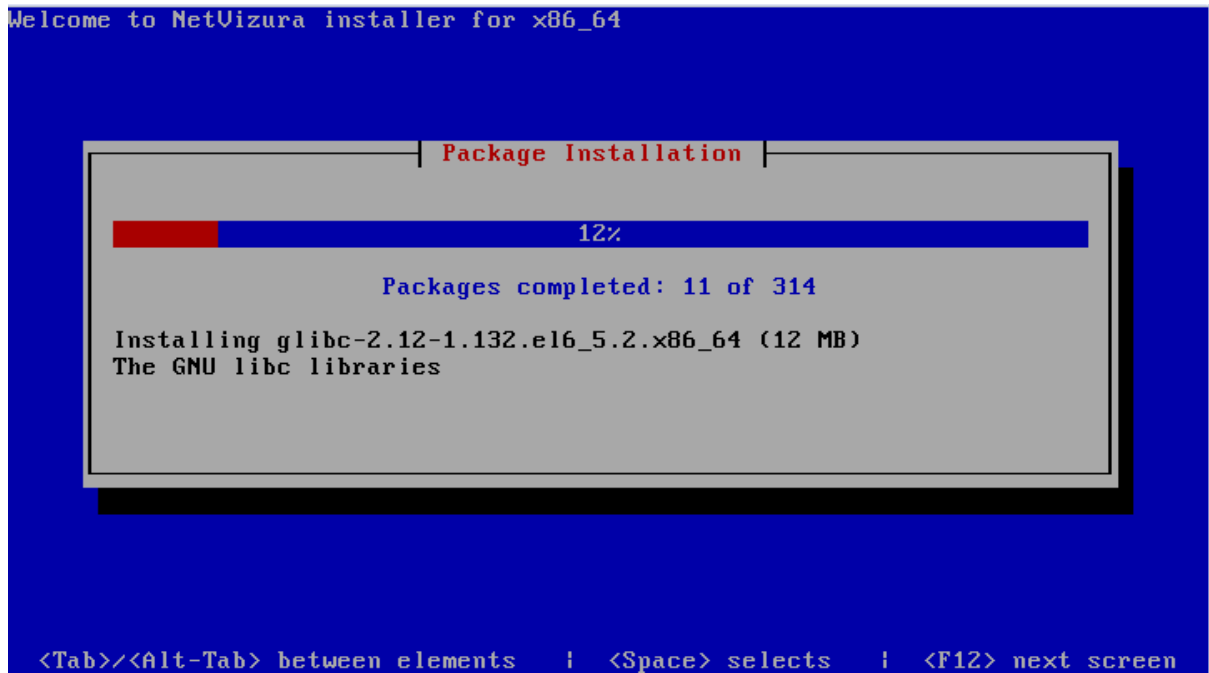


4. Choose Root Password

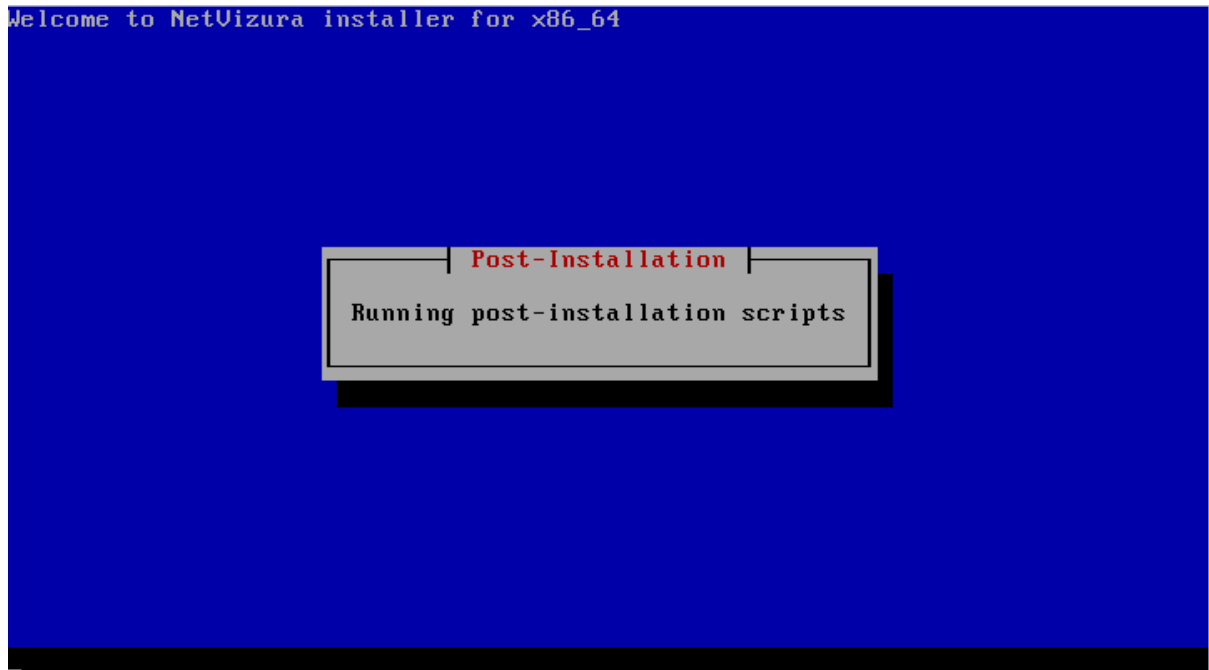
- Insert your root password
- Confirm your password and press Enter.



5. Wait for package installer to complete the installation.



6. Post installation scripts will automatically install NetVizura RPM package.

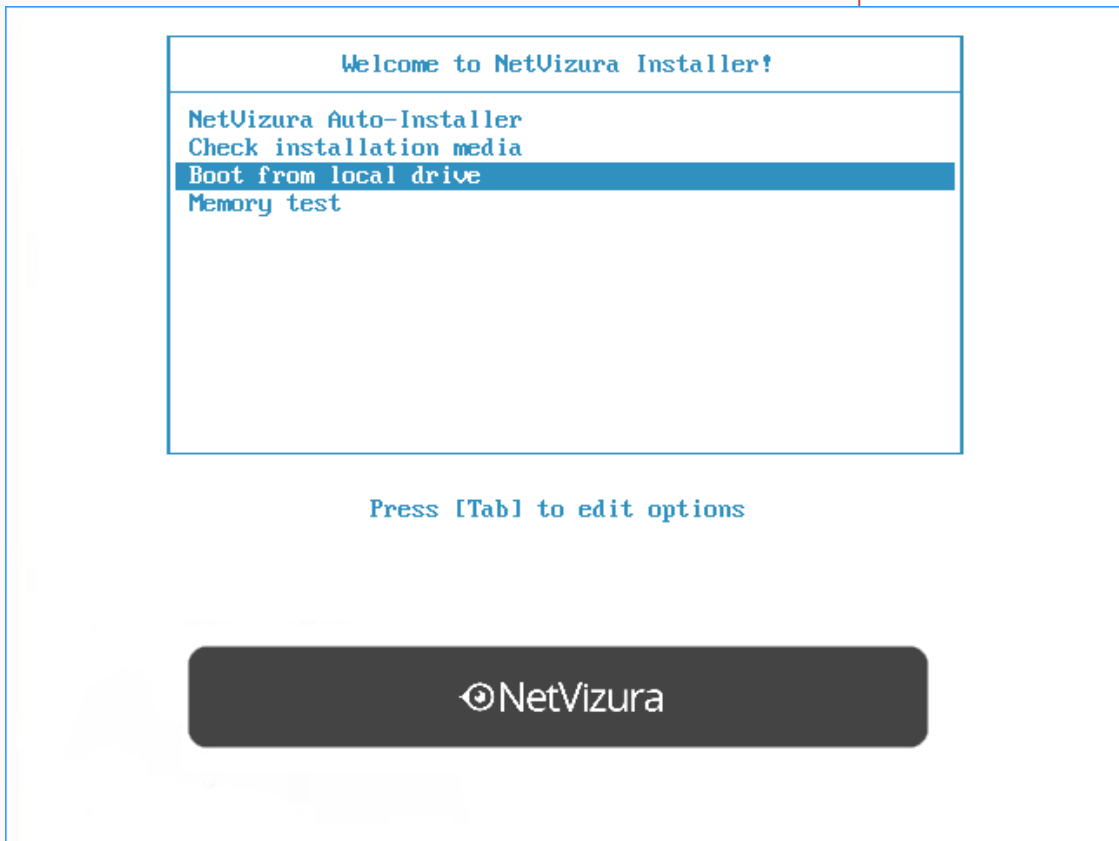


7. Automatic booting into CentOS.6.5 with NetVizura software



If you are installing on VM by using hypervisor:

Some hypervisors like xencenter will not run automatic booting. You will be prompted again in welcome screen and asked to choose an option. Now, you should choose option "Boot from local drive":



8. After boot the following screen will appear


```
CentOS release 6.5 (Final)
Kernel 2.6.32-431.el6.x86_64 on an x86_64

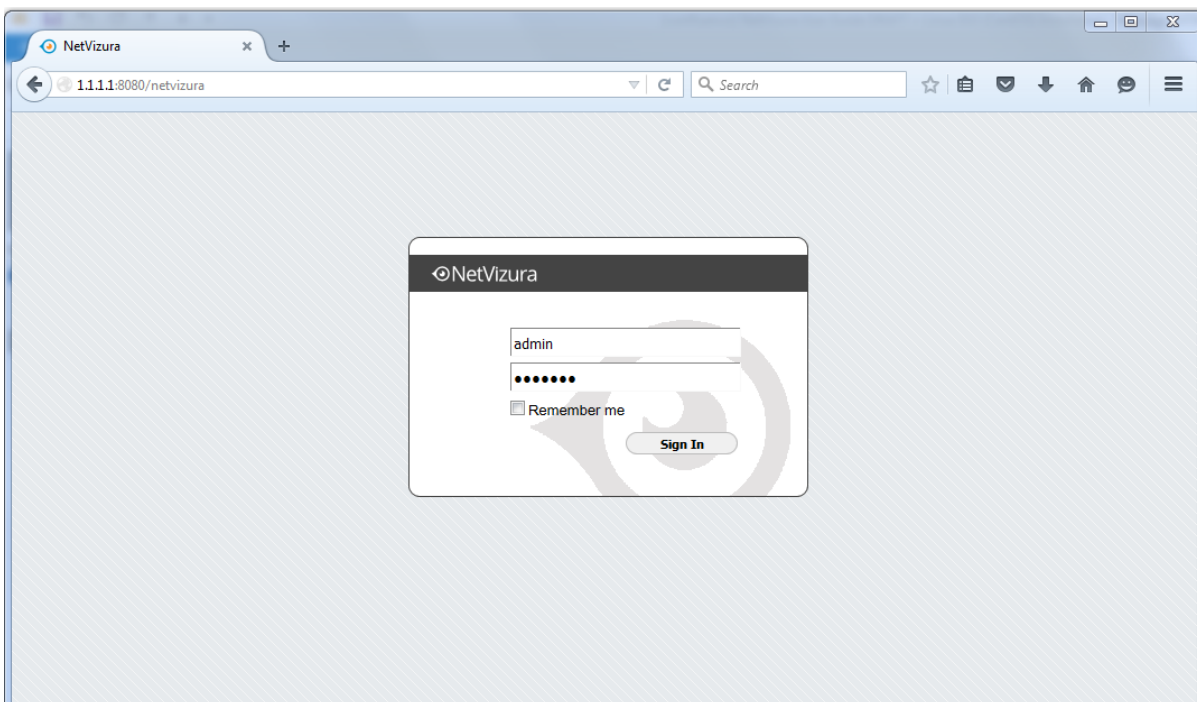
The web interface can be found at http://<this-host>:8080/NetVizura
localhost login: _
```

9. Access your web interface

Now you can log in to NetVizura web interface. For example, if you have chosen as the IP of your server 1.1.1.1 point your browser to <http://1.1.1.1:8080/netvizura> like in the screenshot below:

Default credentials:

- Username: **admin**
- Password: **admin01**



Post Install Steps

See Post install steps in article [Linux RPM \(CentOS\) Installation](#).

Configuring Network Devices for NetFlow Export

In terms of NetFlow export, there are two basic types of network devices:

- **Exporters** - network devices capable of netflow statistics export (for instance routers or L3 switches).
- **Server** - the computer that collects netflow statistics from exporters. This is also the computer on which NetVizura NetFlow Analyzer is installed.

The following issues should be addressed regarding network devices configuration:

- [Choosing Server Location](#)
- [Configuring NetFlow Export \(Ingress vs. Egress\)](#)
- [Choosing Exporters](#)
- [Configuring Cisco Devices](#)
- [Exporting Without NetFlow Capable Device \(Mirroring to Daemon Server\)](#)
- [Exporting to Multiple Servers](#)

Choosing Server Location

NetFlow Server location in the network depends on the network topology. The amount of netflow data exported from network devices is in direct correlation to the amount of traffic passing through that device (exporter). Studies show that the netflow traffic is 0.5% to 2% of total traffic, therefore NetFlow Server should not be “too far” from the exporter.

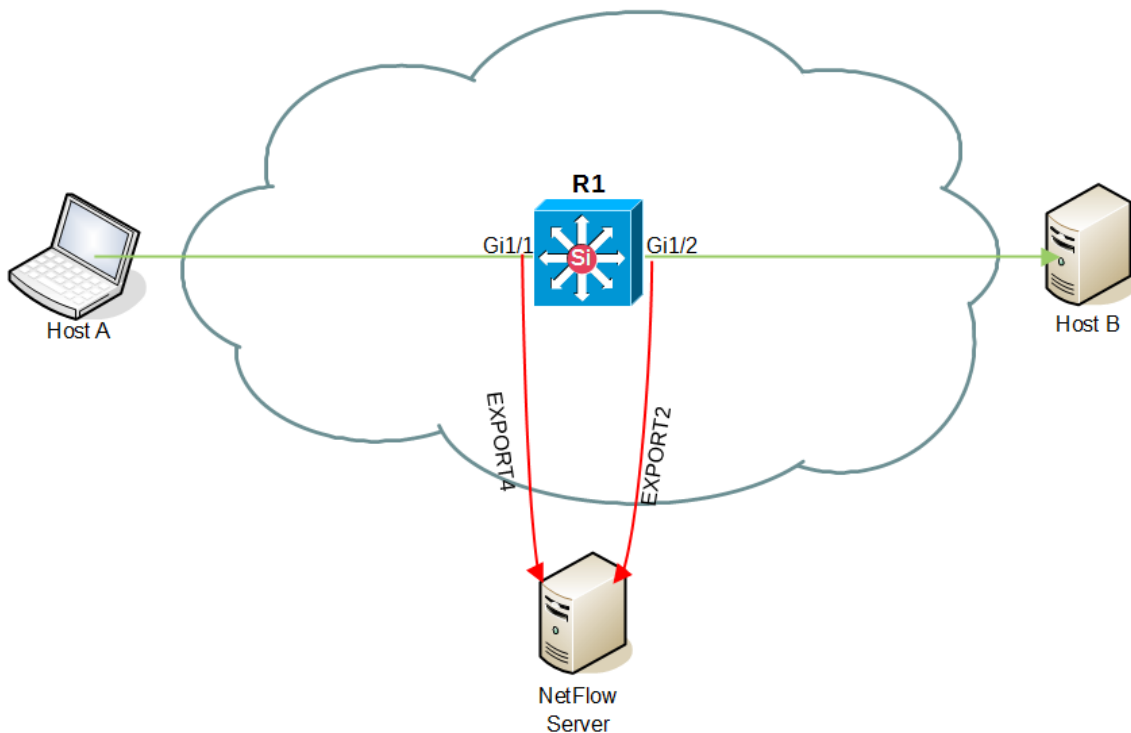
More important parameters are the availability and security of the NetFlow Server. NetFlow Server is usually connected to the central network node or close to it, because the most of the traffic passes through this node. In the case of an exporter or link fail, it is important to have NetFlow Server still available so you can analyze the traffic.

For security reasons, it is recommended that you set a separate VLAN for the NetFlow Server and raise a firewall on the server for its protection.

Configuring NetFlow Export (Ingress vs. Egress)

The following explains in which situations is better to use incoming (in/Ingress) or outgoing (out/Egress) flow on the interface for collecting NetFlow traffic.

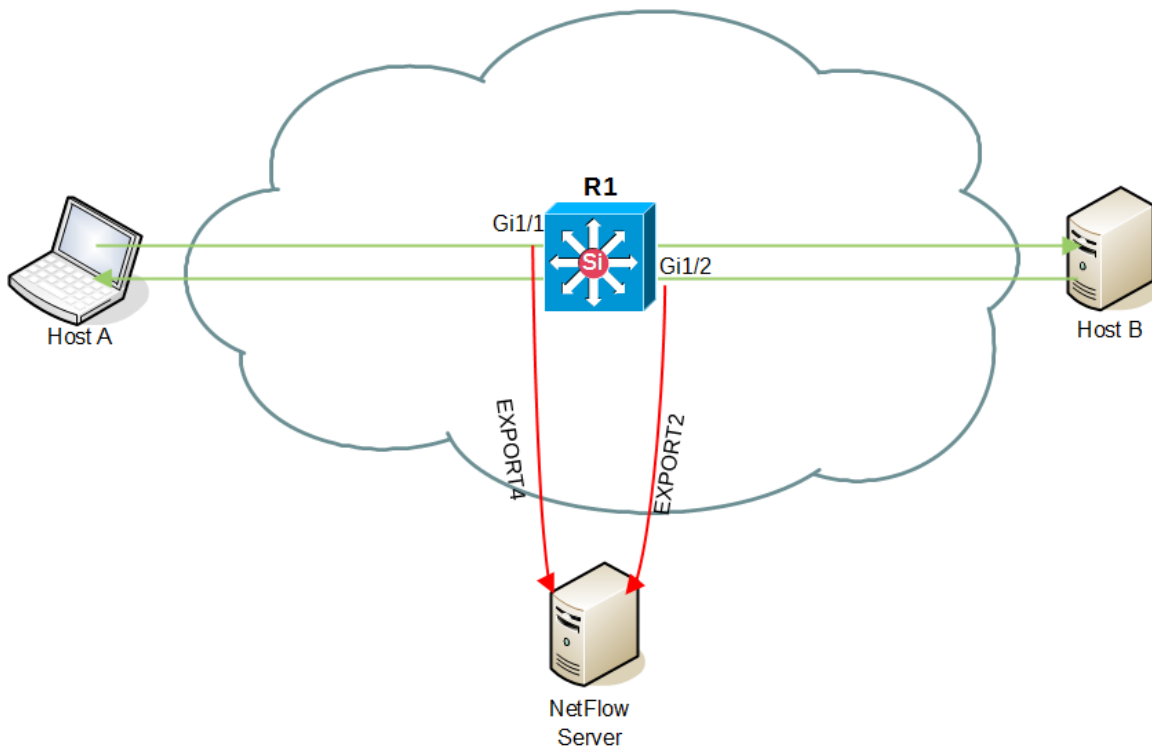
Incorrect NetFlow Export



On the figure above you can see that interfaces Gi1/1 and Gi1/2 are set to collect NetFlow traffic, Gi1/1 in *IN* direction and Gi1/2 in *OUT* direction. This example shows that a flow traveling from Host A to Host B will be collected and exported twice to NetFlow server, while a flow traveling from Host B to Host A will not be matched and exported. The result is a false NetFlow traffic: double amount of flows for A to B direction, and zero flows for B to A direction.

It is very important that all interfaces on a single device are configured to collect flow in only one direction, *IN* or *OUT*.

Correct NetFlow Export



Here, both interface Gi1/1 and interface Gi1/2 are set to collect the NetFlow traffic in *IN* direction. This time, a flow traveling from Host A to Host B will be collected only once, and a flow traveling from Host B to Host A will be collected as well. Now, NetFlow traffic will be correct and none of the charts in TopN > Exporters will have duplicated data.

Ingress or Egress?

When considering to configure Ingress or Egress flow on an exporter device, you must be aware that it depends on software version and supervisor module (if existing). For this information, please check release notes of your device vendor.

Ingress export enabled on all the interfaces of a device will in general deliver all necessary information. It is specially recommended in the following situations:

1. NetFlow v9 supports Ingress and Egress, but NetFlow v5 only supports Ingress flows. If your device is only supported by NetFlow v5, your flows should necessarily be Ingress.
2. In addition, Ingress export provides monitoring of Blocked traffic (traffic sent to Interface Out 0).

Egress should be considered in these situations:

1. Some routers (e.g. Cisco WAAS, Riverbed, etc.) have option to compress flows, so the Out traffic will be significantly larger than In traffic. Egress export provides more precise information on traffic transferred in the network.
2. When multicast flows are sent, Ingress exported flows have a destination interface 0 because the router doesn't know interface Out before processing. Egress exported flows deliver the destination interfaces, and in addition if the flow is headed for multiple interfaces it will be exported as multiple flows.

Continue reading on to [Choosing Exporters](#).

Choosing Exporters

If you have a large network with many routers and switches, exporting NetFlow from all these devices might significantly impact the complexity of export configuration, NetFlow Analyzer performance, as well as license needed.

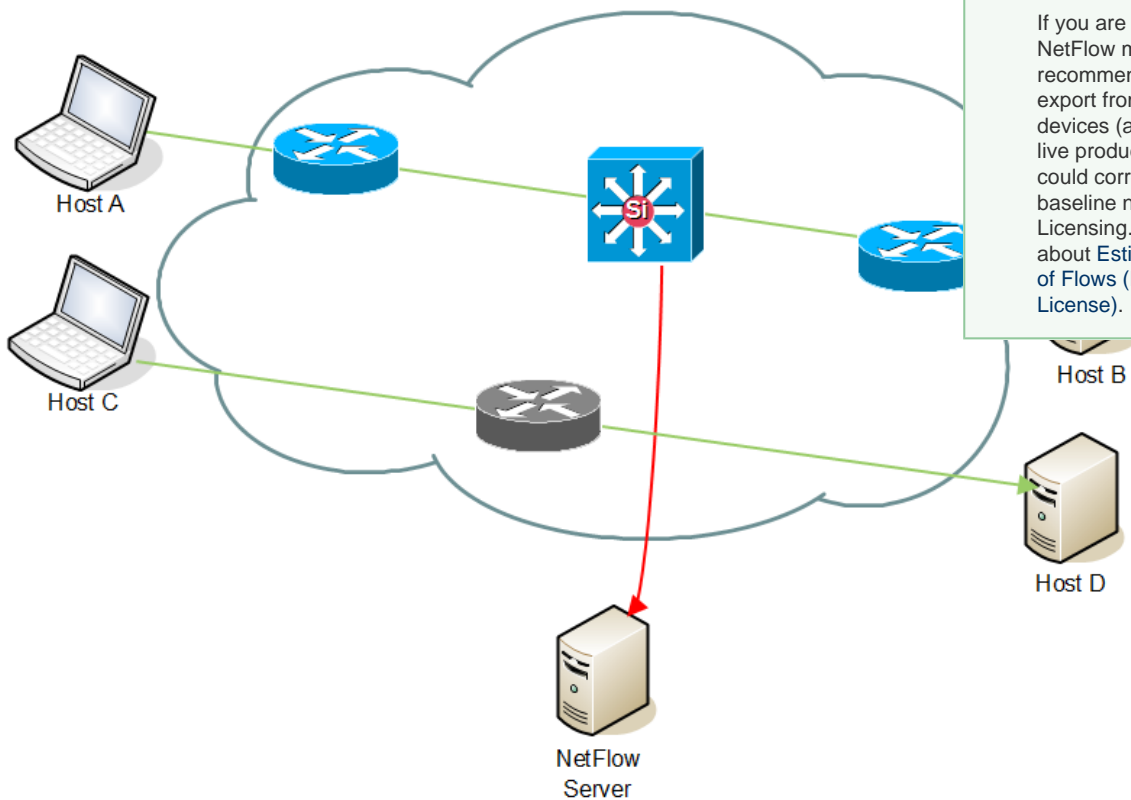
This article will help you decide which devices exactly to choose as necessary for your netflow export and overcome these challenges.

Choosing Traffic to Export

The basic principle is to export only the traffic that is of your interest. For this reason, it is necessary for you first to understand well your network topology and flow routing.

For example, you can export netflow only from devices in data center and regional units, and not from branch locations. Or, if you want to make Traffic Pattern that captures all internal company's traffic where part of the traffic passes via central router and part passes directly between other routers, then you should export from all these routers.

Incomplete Traffic Export



This is a situation when netflow traffic is not exported for one part of the network. The traffic that passes through the central router (Host A to Host B) will be captured, while traffic that does not pass via central router (Host C to Host D) will not.

Complete Traffic Export

On this page:

- Choosing Traffic to Export
 - Incomplete Traffic Export
 - Complete Traffic Export
- Deciding Whether to Use Automatic Deduplication
 - Automatic Deduplication Disabled
 - Automatic Deduplication Enabled
 - Automatic Deduplication Not Possible

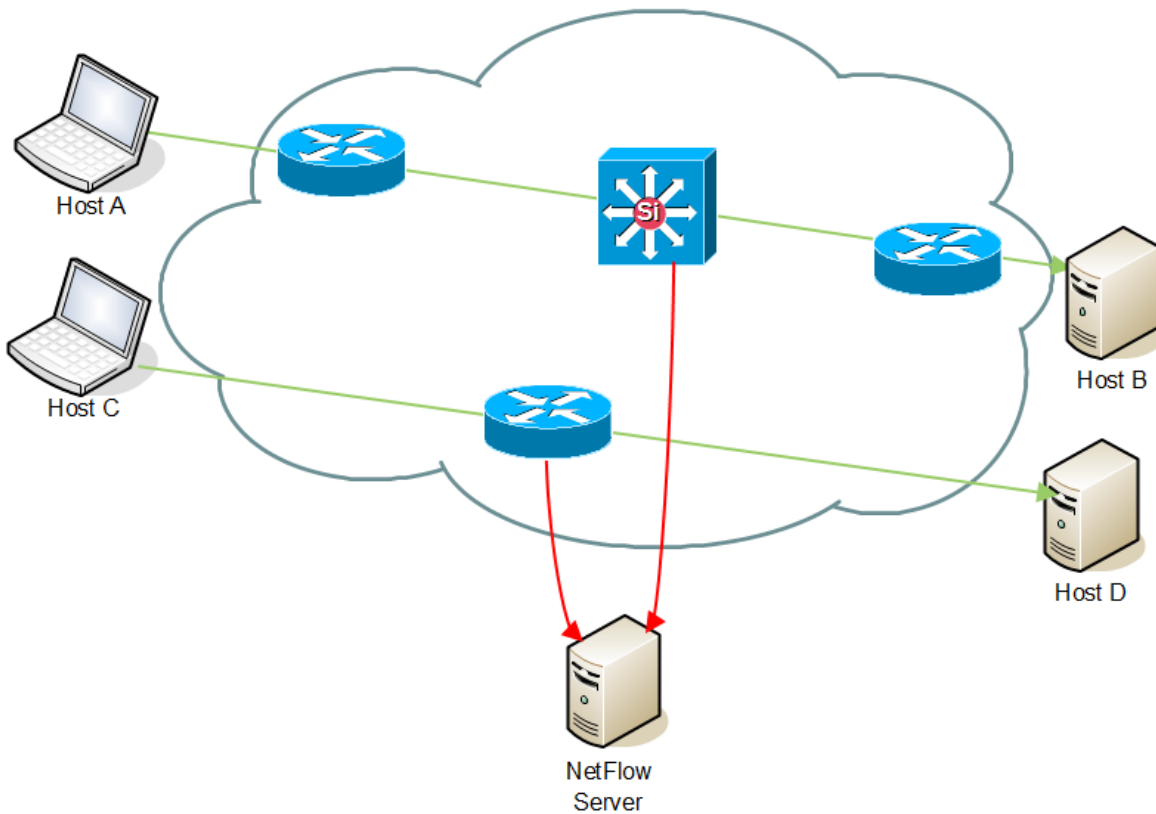


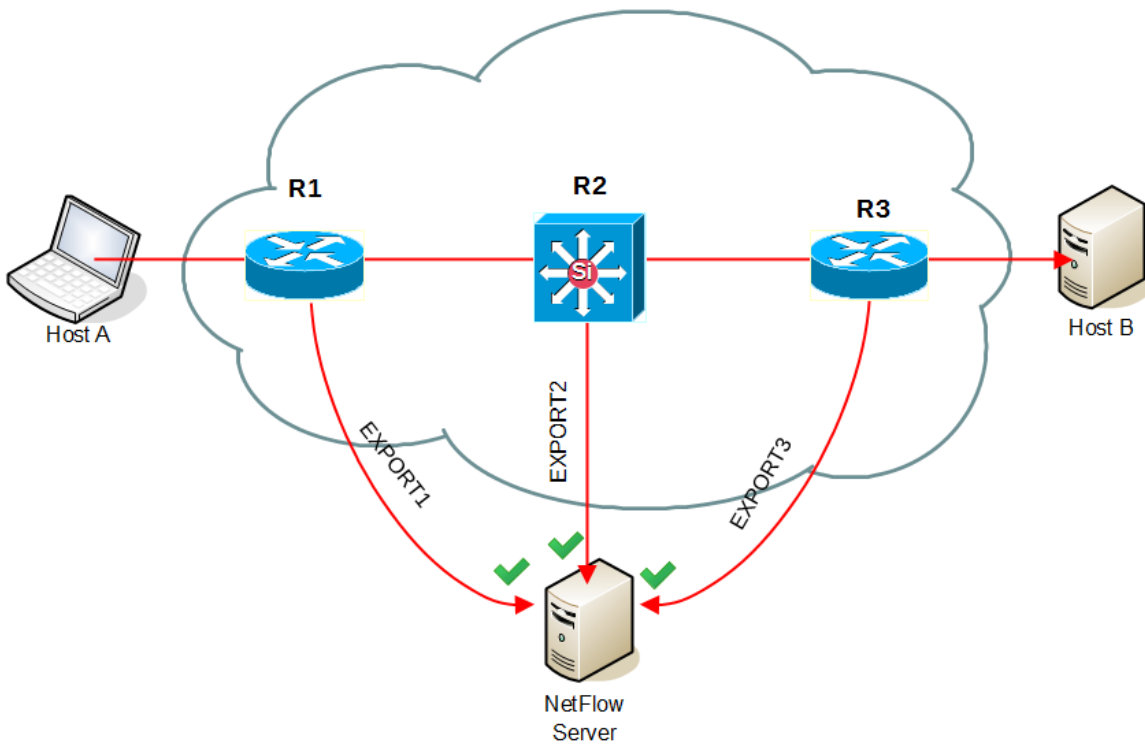
Figure above shows an example of communication when we want to monitor communication that is not passing through the central router. It is necessary to configure the netflow export on network devices on which that communication is passing through.

Deciding Whether to Use Automatic Deduplication

Since Exporters charts present data as they are actually exported by devices, none of the Exporter traffic will have duplicated data.

However, when you create Traffic Patterns and Subnet Sets they may include data exported by multiple exporters and as a consequence netflow data will be duplicated. This naturally depends on which devices are configured as exporters, as well as traffic routing and network topology.

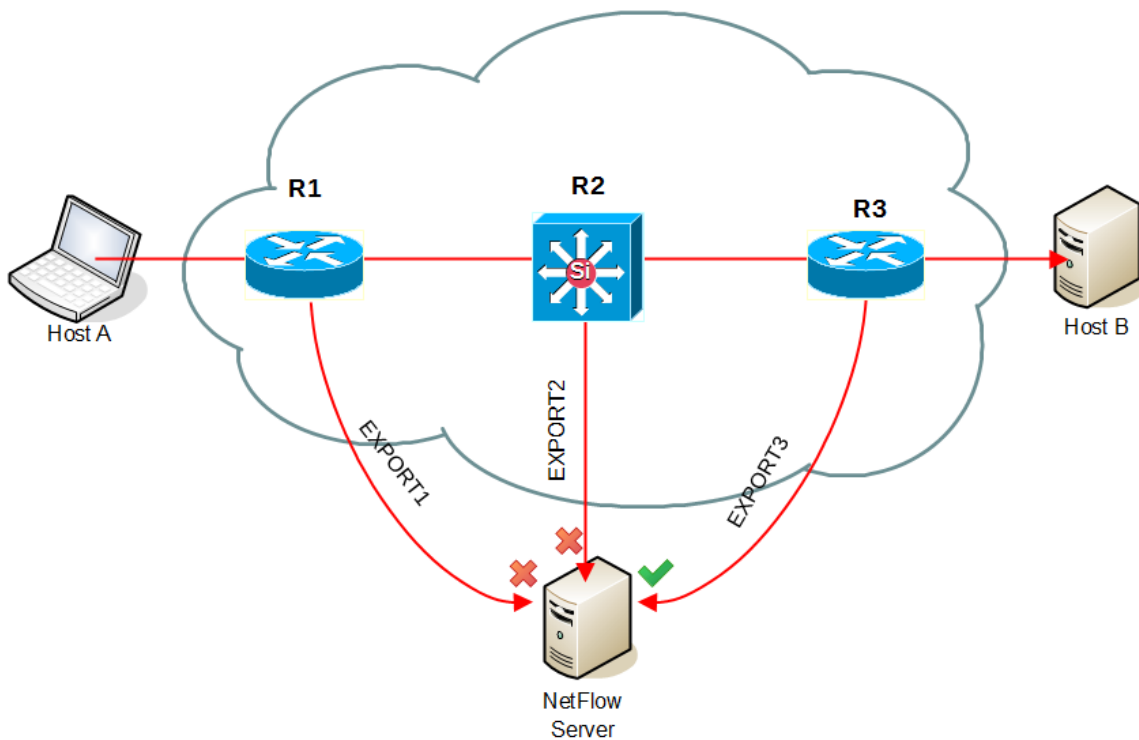
Automatic Deduplication Disabled



When automatic deduplication is disabled, a flow traveling from Host A to B and passes via multiple exporters, NetFlow Server will receive same flow from R1, R2 and R3 so flow will be processed three times.

Automatic deduplication is enabled by default. To disable it, go to **NetFlow Settings > Configuration > Automatic Deduplication** and select **Disable**.

Automatic Deduplication Enabled



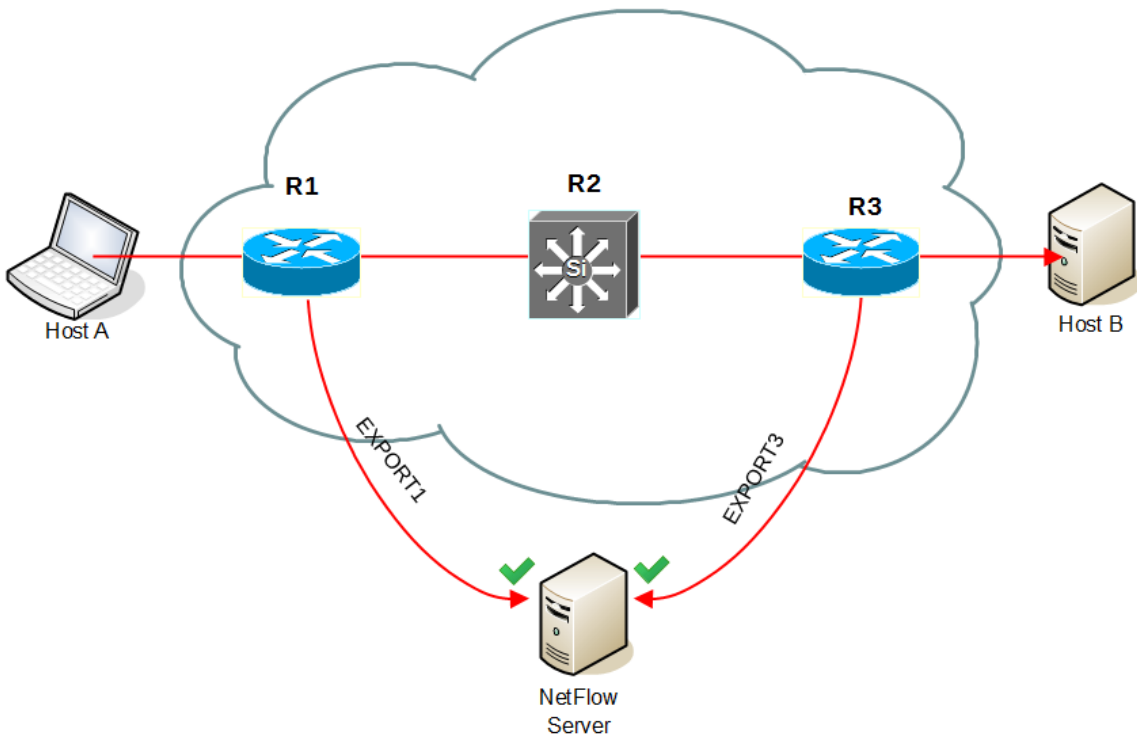
Automatic deduplication solves this problem based on the next hop - when an exporter exports a flow, and this flow includes IP address of another exporter as next hop information, then the flow will be skipped by the Traffic Pattern/Subnet Set counter.

For example, when three consecutive routers in the flow route are exporting flows then NetVizura will have enough information to skip flows from R1 and R2 (since R2 and R3 exporters are mentioned as next hop) and include only flow from R3 in the Traffic Pattern.

In order to achieve automatic flow deduplication in Traffic Patterns and Subnet Sets, it is required that ALL devices in flow continuity are configured as exporters.

Automatic Deduplication Not Possible

However, sometimes not possible to achieve automatic deduplications. For example, if device is not NetFlow export capable, when part of the network is managed by third party (ISP) or if exporting from too much devices is not desired.



In the figure above, we see that even though automatic deduplication is enabled, flow will be duplicated by two exporters (R1 and R3) that are not in the flow continuity (R3 will not be mentioned as next hop in R1 flow export).

In case it is not possible to enable automatic deduplication by exporting all devices in flow continuity, deduplication could also be achieved manually. Read more at [Manual Deduplication](#).

Configuring Cisco Devices

It is recommended that only users with experience in configuring Cisco devices follow these steps.

This section offers a brief guide for setting up NetFlow on a Cisco router or switch. For more detailed information, refer to the [Cisco website](#).

Device	Supported
Cisco 800, 1700, 2600	Yes
Cisco 1800, 2800, 3800	Yes
Cisco 4500	Yes
Cisco 6500	Yes
Cisco 7200, 7300, 7500	Yes
Cisco 7600	Yes
Cisco 10000, 12000, CRS-1	Yes
Cisco 2900, 3500, 3660, 3750	Yes

Software Platform Configuration


The following is an example of a basic router configuration for NetFlow. NetFlow basic functionality is very easy to configure. NetFlow is configured on a per interface basis. When NetFlow is configured on the interface, IP packet flow information will be captured into the NetFlow cache. Also, the NetFlow data can be configured to export the NetFlow data to the NetFlow Server.

1. Configuring the interface to capture flows into the NetFlow cache. CEF followed by NetFlow flow capture is configured on the interface

```
Router(config)# ip cef
Router(config)# interface ethernet 1/0
Router(config-if)# ip flow ingress
```

Or

```
Router(config-if)# ip route-cache flow
```

 Either `ip flow ingress` or `ip route-cache flow` command can be used depending on the Cisco IOS Software version. IP flow ingress is available in Cisco IOS Software Release 12.2(15)T or above.

2. For exporting the NetFlow cache to the NetFlow Server. A version or a format of the NetFlow export packet is chosen and then the destination IP address of the server (in this example 172.22.23.7). The 2055 is the UDP port the NetFlow Server will use to receive the UDP export from the Cisco device. 2055 is a default value, you can change this as described in chapter Configuring the service settings on page 141 (Collection port).

```
Router(config)# ip flow-export version 9
Router(config)# ip flow-export destination 172.22.23.7 2055
```

 More Information on NetFlow Configuration is available at [Cisco website](#).

Cisco Catalyst 6500 Series Switch Platform NetFlow Configuration

The following is an example of NetFlow on a Cisco Catalyst 6500 Series Switch. The Cisco Catalyst 6500 Series Switch has two aspects of NetFlow configuration, configuration of hardware based NetFlow and software NetFlow. Almost all flows on the Cisco Catalyst 6500 Series Switch are hardware switched and the MLS commands are used to characterize NetFlow in hardware. The MSFC (software based NetFlow) will characterize software based flows for packets that are punted up to the MSFC.

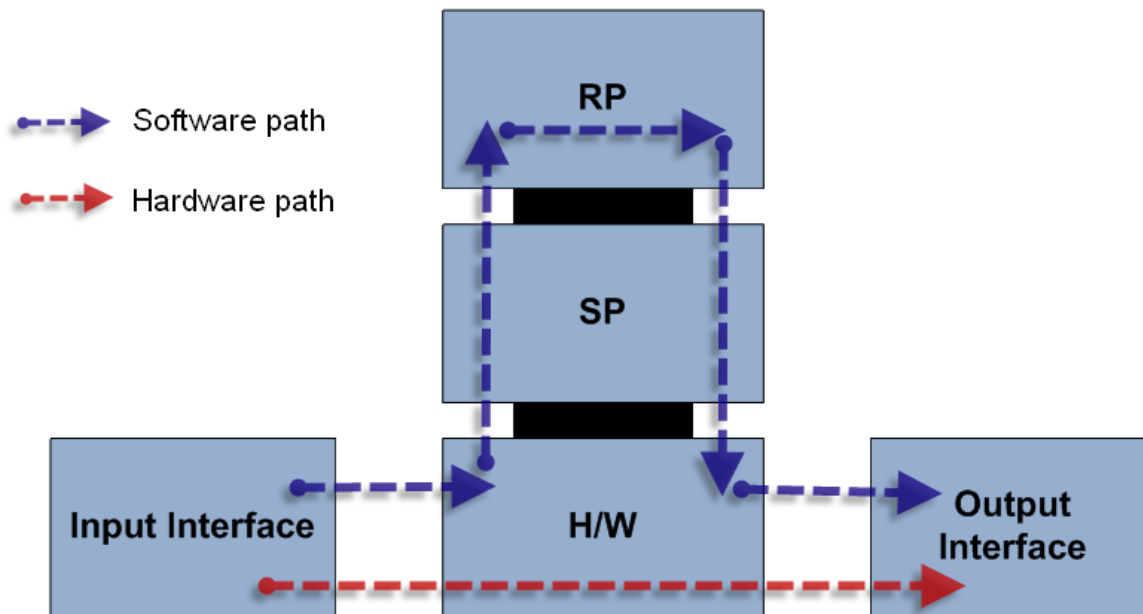


Figure above shows the concept of two paths for NetFlow packets, the hardware (red) and software (blue) paths and the configuration for each path. Normally on Cisco Catalyst 6500 Series Switch both hardware and software based NetFlow is configured.

The hardware switched flows use the MLS commands to configure NetFlow. Remember that for the hardware based flows NetFlow is enabled on all interfaces when configured.

```

mls aging normal 32 (Set aging of inactive flows to 32
seconds)
mls flow ip interface-full (Optionally configure a flow
mask)
mls nde sender version 5 (Specify the version for export
from the PFC)
mls nde interface (send interface information with the
export, command available by default with
Supervisor720/Supervisor 32)

```

The following is the configuration for NetFlow on the MSFC for software based flows. This configuration is equivalent to what is shown in Cisco Catalyst 6500 Series Switch Platform NetFlow Configuration. The user configures NetFlow per interface to activate the flow characterization and also configures an export destination for the hardware and software switched flows.

```

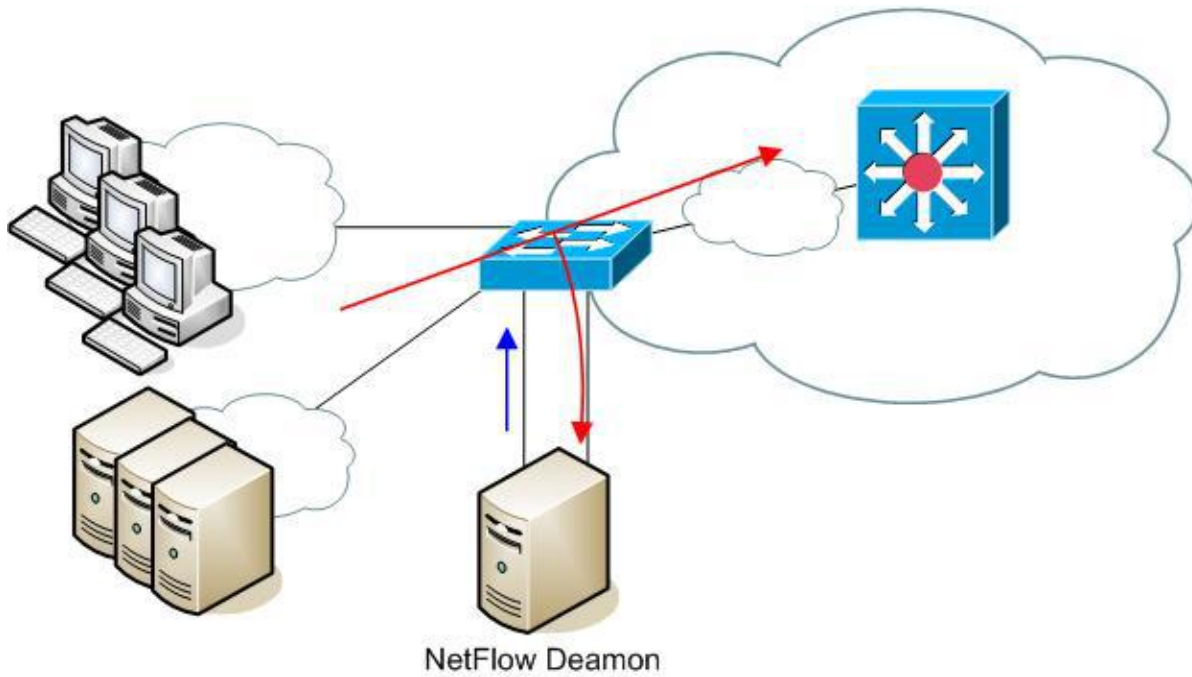
interface POS9/14
  ip address 42.50.31.1 255.255.255.252
  ip route-cache flow (also ip flow ingress can be
used)
  ip flow-export version 5 (The export version is
setup for the software flows exported from the MSFC)
  ip flow-export destination 10.1.1.209 2055 (The
destination for hardware and software flows is
specified)

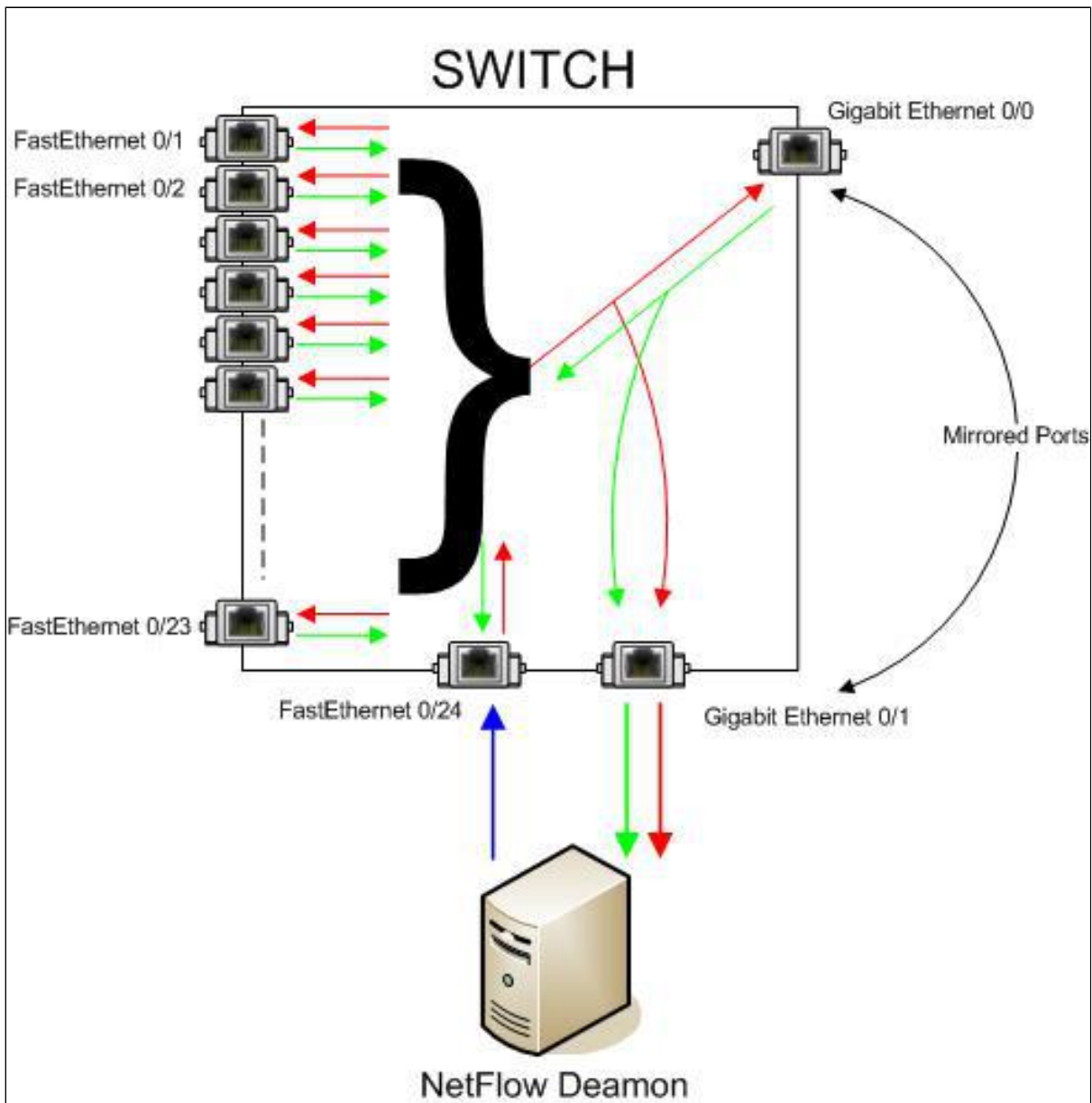
```

More Information on the Cisco Catalyst 6500 Series Switch NetFlow Configuration can be viewed at [Cisco website](#).

Exporting Without NetFlow Capable Device (Mirroring to Daemon Server)

In the situation when network device is not supporting NetFlow protocol, the concept of Traffic Patterns allows you to redirect traffic to the server with a netflow probe. The netflow probe analyzes traffic and generates netflow traffic. We will call the server on which this probe is started the NetFlow Daemon Server. Figure below shows an example of this situation:

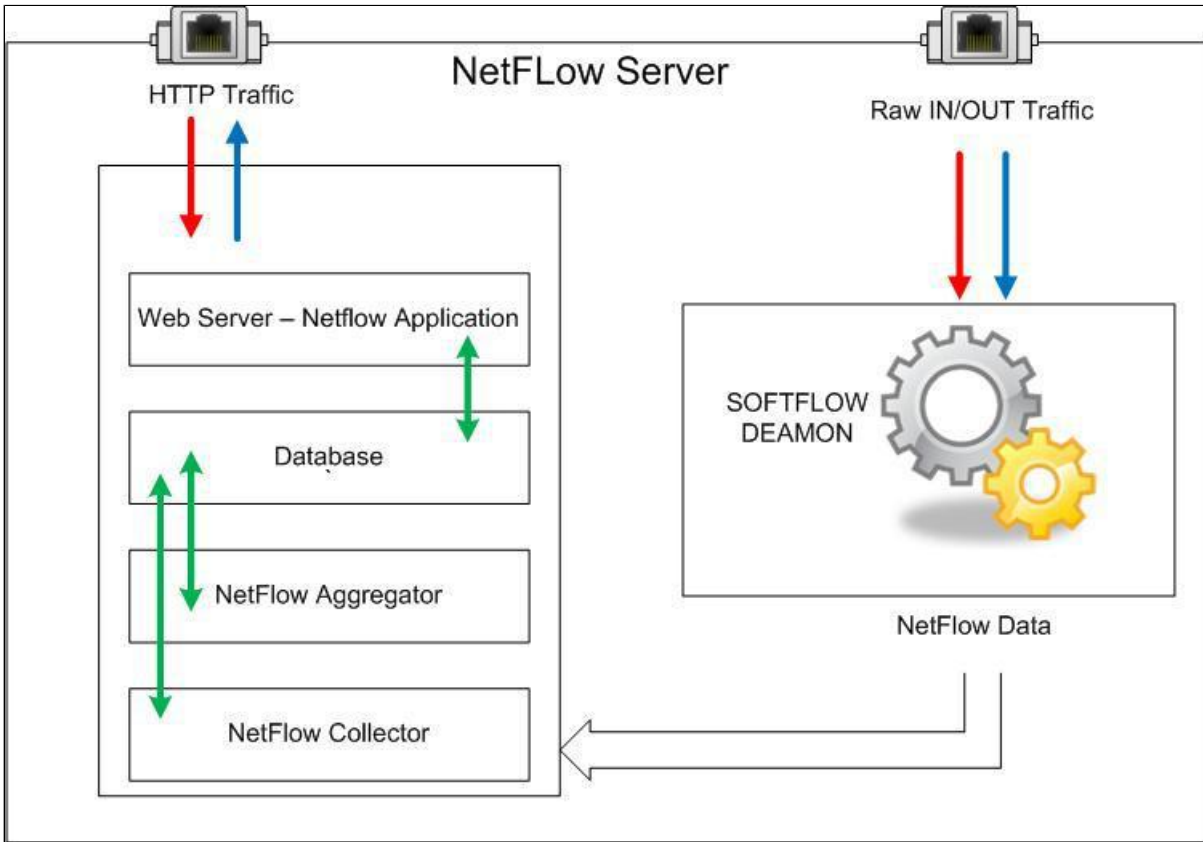
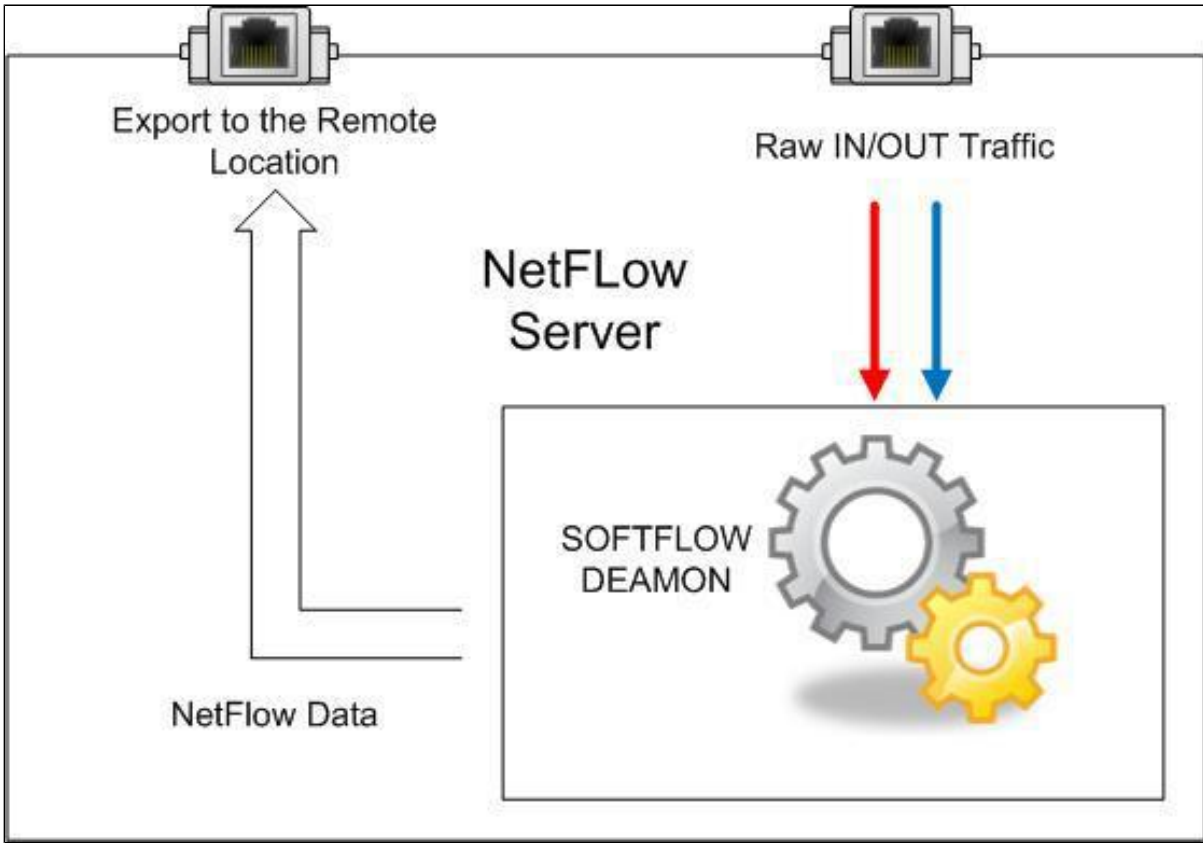




Figures above show the redirection of traffic (port mirroring) to the server on which the NetFlow Daemon Server is started. When the port mirroring is started on a switch, interface to whom all traffic is directed to becomes useless for normal device communication. It only passes all of its traffic (In and Out) from port mirroring interface.

The problem is: How to export netflow traffic if the interface on which the NetFlow Daemon Server is connected to is unusable for normal communication?

One solution is to add additional network card to the server and connect to the switch. This configuration enables netflow exporting even from the L2 switches. The drawback is the additional port utilization on the switch and the need for an additional server. One port on the switch is used for receiving mirrored In/Out traffic and another one for exporting netflow traffic. The blue arrow in the figure above shows netflow export from the additional network card on the server.



Now, it is possible to start the netflow probe on the NetFlow Daemon Server. One of these applications is the SoftFlowd that has the possibility of exporting netflow traffic locally (127.0.0.1) to the UDP port on the same server or to a UDP port on a remote server.

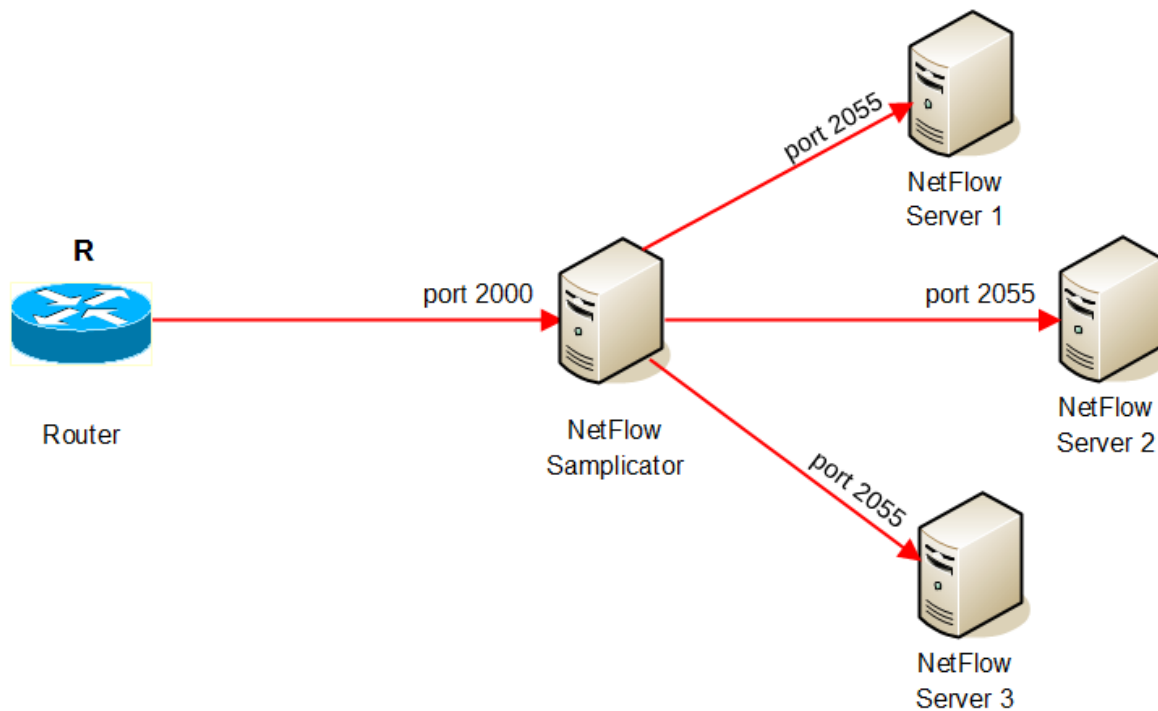
Above figures show examples of local netflow export and remote netflow export.

Exporting to Multiple Servers

Often it is necessary to export netflow traffic on more than one server (production, development, test...). Having in mind that Cisco, Juniper and other devices can often export netflow data only on two devices, there is a need for tools for multiplication of netflow traffic.

One of these tools is Samplicator. It is a software package for Linux that listens to UDP datagrams at defined port and sends copies to set of other IP addresses we define.

Samplicator works according to the figure below:



Samplicator receives traffic from some exporter via port 2000, then copies and sends copies to multiple NetFlow Servers via port 2055.

How to do it:

1. Download latest Samplicator version [here](#)
2. Unpack: `tar -zxf samplicator-x.y.z.tar.gz`
3. Go to directory: `cd samplicator-x.y.z`
4. As a root run configure script: `./configure`
5. Make command to make binary files: `make`
6. Then install application with command: `make install`
7. Softver will run with command: `samplicate`

Optional commands to use:

Option	Description
<code>-p <port></code>	UDP port to accept flows on (default %d)
<code>-s <adresa></code>	Interface address to accept flows on (default any)
<code>-d</code>	Debug level

-b	Set socket buffer size (default %lu)
-n	Do not compute UDP checksum (leave at 0)
-S	Maintain (spoof) source address.
-x <delay>	Transmission delay in microseconds.
-c	Defining location of configuration file from which configuration is read.
-f	Fork. This option setss samplicate to work as background process.

This example describes netflow package duplication as on the figure above:

```
samplicate -S -f -p 2000 10.1.37.20/2055  
10.1.15.211/2055 10.1.7.18/2055
```

Licensing

NetVizura modules (NetFlow, EventLog and MIB) are activated with a license key which is bound to NetVizura server via Installation key.

Different modules have different license models:

NetFlow Analyzer license depends on the number of flows you are exporting to NetVizura server, regardless of the number of exporters (routers and switches) and their interfaces involved. You can collect data from as many devices as you need and the total number of flows will reflect your network traffic volume.

With this approach you have a possibility for a wider usage of NetFlow software across your network and choose the license that best fits your network traffic volume.

EventLog Analyzer license has no limitations on number of exporters or syslog and SNMP traps received.

MIB Browser license has no limitations of usage.

The following sections provide instruction for licensing NetVizura:

- [Upgrading License](#)
- [Updating License](#)
- [Estimating Number of Flows \(NetFlow Analyzer License\)](#)

Upgrading License

To upgrade your current licence (converting Free Trail to Commercial license, or lower Commercial to higher Commercial license) you need to purchase appropriate Commercial license. For help with finding an optimal license for you, complete this [Get Quote](#) form on our web site or get in touch with us at sales@netvizura.com.

After this, you should provide us with the Installation Code for your NetVizura server so we can issue you a license key.

To send us the Installation Code:

1. Log in as admin
2. Go to **Settings > Control Panel > License**
3. Click **Send** to send us an automatically filled out e-mail with your Installation Code

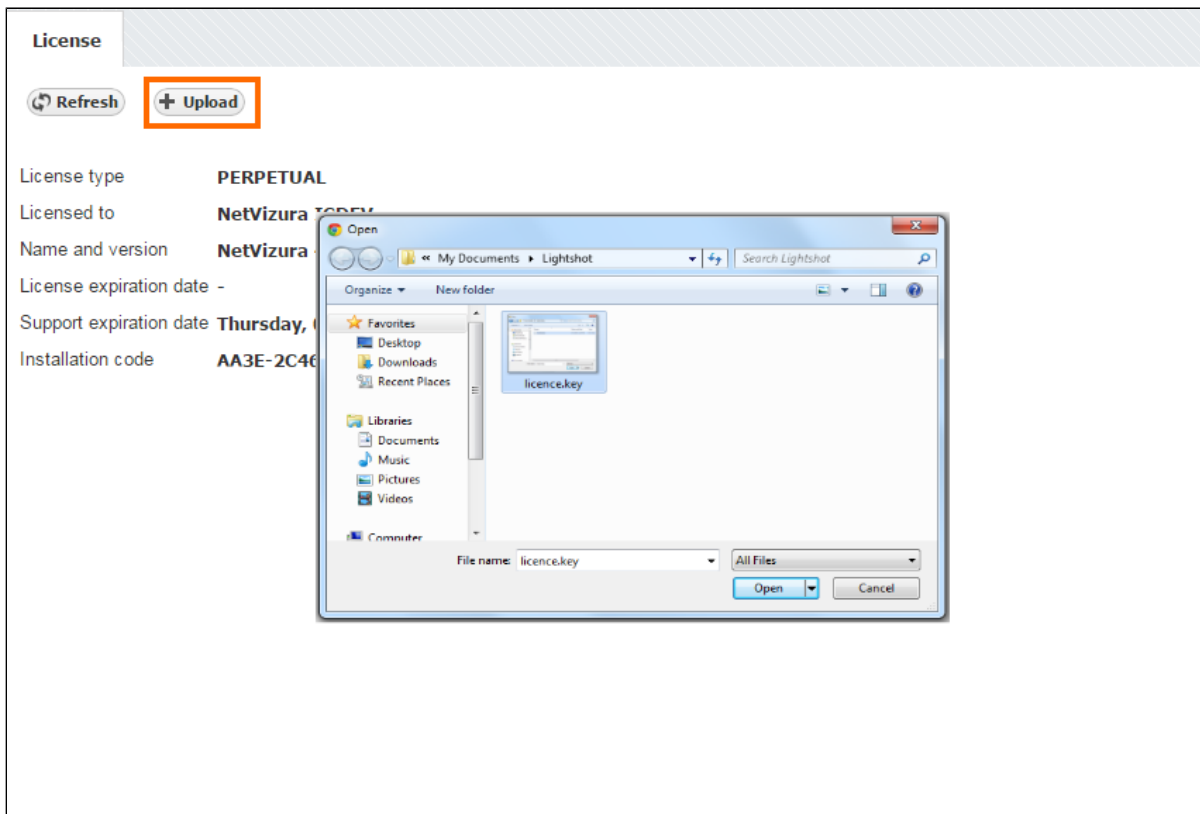
If you are upgrading NetFlow Analyzer to a higher Commercial license, first you need to estimate how many flows you need. For more instruction go to [Estimating Number of Flows \(NetFlow Analyzer License\)](#)

License	
License type	PERPETUAL
Licensed to	NetVizura ICDEV
Name and version	NetVizura 4.1
License expiration date	-
Support expiration date	Thursday, 01 Oct 2015
Installation code	AA3E-2C46-525E-C647-8449-5F76-BC75-76D Send

After we receive the Installation Code, we will send you your license key in one working day. Note that you can apply the license key to your existing installation keeping your configuration and data.

To apply your License key:

1. Go to **Settings > Control Panel > License**
2. Click **Upload** license key
3. Find the path to the new License key
4. Click **Open**



After the new license key is loaded a popup window will appear prompting you to reset NetVizura (log-out and log-in again). When you log-in again, verify that the new license has been applied by checking **About** or by going to **Settings > Control Panel > License**.

Should you experience any difficulties with application of your licence key, do not hesitate to email us at support@netvizura.com.

Updating License

NetVizura provides two types of Commercial licenses: Perpetual and Subscription license. Perpetual license includes unlimited usage and first year maintenance and support, whereas Subscription license includes one year usage, maintenance and support.

In any case, after your current maintenance and support expires you need to purchase a new license key that allows software update and support tickets. For help with payment requests, get in touch with us at sales@netvizura.com.

For the new license key, you should provide us with your Installation Code.

To send us the Installation Code:

1. Log in as admin
2. Go to **Settings > Control Panel > License**
3. Click **Send** to send us an automatically filled out e-mail with your Installation Code

The screenshot shows the 'License' section of the NetVizura settings. On the left is a navigation menu with 'Settings', 'Modules', 'Control Panel', and 'Miscellaneous'. The 'License' section on the right contains a 'Refresh' button and an 'Upload' button. Below these are the following details:

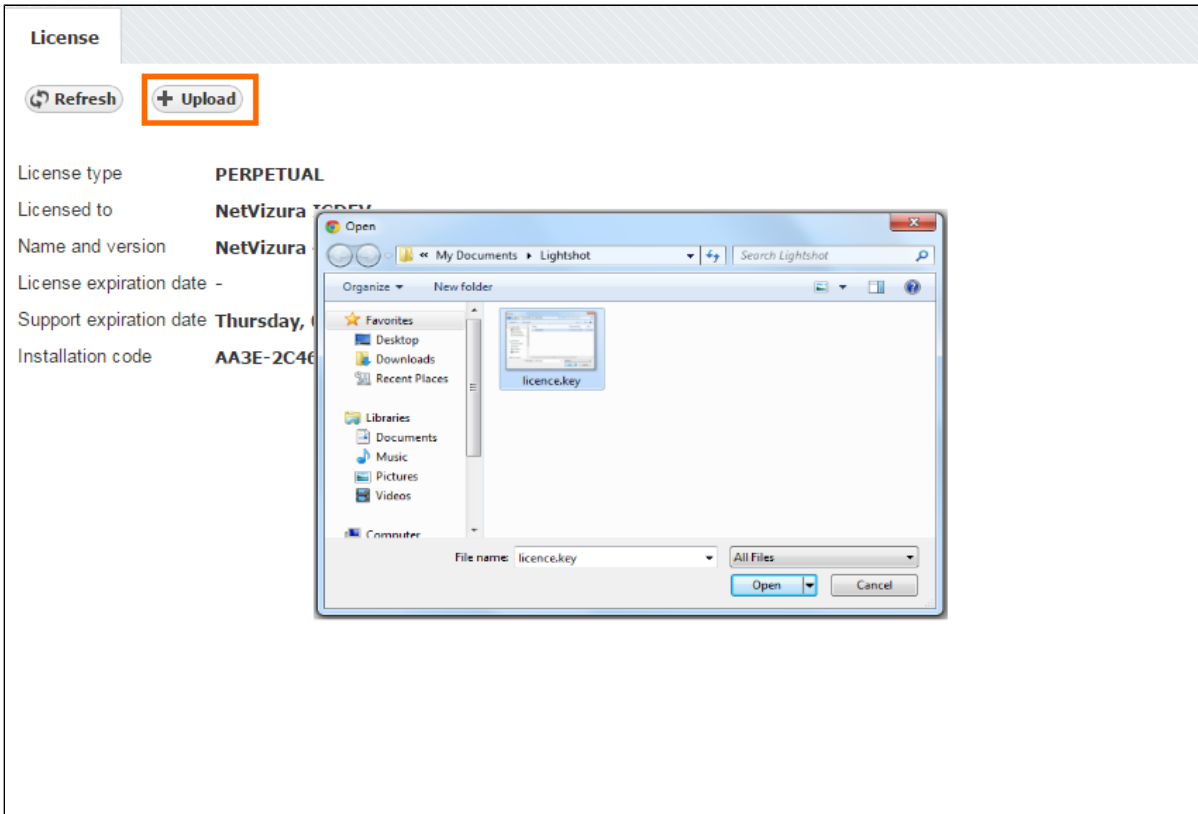
License type	PERPETUAL
Licensed to	NetVizura ICDEV
Name and version	NetVizura 4.1
License expiration date	-
Support expiration date	Thursday, 01 Oct 2015
Installation code	AA3E-2C46-525E-C647-8449-5F76-BC75-76D

A 'Send' button is located to the right of the installation code, highlighted with a red box.

After we receive the Installation Code, we will send you your license key in one working day. Note that you can apply the license key to your existing installation keeping your configuration and data.

To apply your License key:

1. Go to **Settings > Control Panel > License**
2. Click **Upload** license key
3. Find the path to the new License key
4. Click **Open**



After the new license key is loaded a popup window will appear prompting you to reset NetVizura (log-out and log-in again). When you log-in again, verify that the new license has been applied by checking **About** or by going to **Settings > Control Panel > License**.

Should you experience any difficulties with application of your licence key, do not hesitate to email us at support@netvizura.com.

Estimating Number of Flows (NetFlow Analyzer License)

The best way to estimate number of flows needed for your NetFlow Analyzer Commercial license is based on your past data.

To do this:

1. Log in as admin
2. Go to **Top N > System**
3. Click **Flows** tab
4. Choose the **Last Month** in the Time Window



In the Number of flows graph you will notice peaks in traffic. These peaks will tell when you had the highest rate of flows exported by your devices. Max Total stored value in the table will give you the maximum number of flows per second exported by your network devices (highest peak) for the set Time Window (preferably Last month).

Unlicensed flows (red on the graph) mean that your network devices are exporting more flows than your license allows. These flows will not be processed and, therefore, information provided by them will not be included when creating and displaying traffic statistics. In this case, you should upgrade your license.

We recommend you to include export from all desired devices (as it should be on live production), so that you could correctly estimate fps baseline needed for Licensing.


Updating NetVizura

- Linux DEB (Debian & Ubuntu) Update
- Linux RPM (CentOS) Update

Linux DEB (Debian & Ubuntu) Update

1. If you want to update versions 4.0.0, 4.0.5 or 4.1.0 to 4.3.0, we kindly urge you to first successively update to version 4.2.1 and then to version 4.3.0.
2. Application will not work if update is made after support period has expired. Make sure that your support has not expired before you start updating.
3. It is not possible to update NetVizura on free trial. If you want to extend trial period for one additional month, please request a new trial license.


Step-by-step guide

1. Check free space on disk with `df -h` command. If there is less than 8GB of free space on disk, delete some files to make at least 8GB available space on disk (easiest way is to delete old raw data files in archive which is usually located in `/var/lib/netvizura/flow/archive`)
2. Download the update package (assumed filename is `netvizura-x.y.z-linux.deb`) to NetVizura server's `/tmp` directory
 `x.y.z` is NetVizura version number.
3. Execute `cd /tmp`
4. Execute `dpkg -i netvizura-x.y.z-linux.deb`
5. Refresh your browser (Ctrl + F5)
6. Check if the update is successful on NetVizura's license page: http://<netvizura_ip>:8080/netvizura/#settings/license

Linux RPM (CentOS) Update

1. If you want to update versions 4.0.0, 4.0.5 or 4.1.0 to 4.3.0, we kindly urge you to first successively update to version 4.2.1 and then to version 4.3.0.
2. Application will not work if update is made after support period has expired. Make sure that your support has not expired before you start updating.
3. It is not possible to update NetVizura on free trial. If you want to extend trial period for one additional month, please request a new trial license.

Step-by-step guide

1. Check free space on disk with `df -h` command. If there is less than 8GB of free space on disk, delete some files to make at least 8GB available space on disk (easiest way is to delete old raw data files in archive which is usually located in `/var/lib/netvizura/flow/archive`)
2. Download the update package (assumed filename is `netvizura-x.y.z-linux-rpm.tgz`) to NetVizura server's `/tmp` directory
 `x.y.z` is NetVizura version number.
3. Execute `cd /tmp`
4. Execute `tar -xzf netvizura-x.y.z-linux-rpm.tgz`
5. Execute `./update.sh`
6. Refresh your browser (Ctrl + F5)
7. Check if the update is successful on NetVizura's license page: http://<netvizura_ip>:8080/netvizura/#settings:license

If downloaded from Internet Explorer, the filename would be `netvizura-linux-x.y.z-rpm.gz`.

Installing and Configuring Syslog Agent for End User Traffic

End User Traffic functionality requires separate Syslog agent to be installed on working stations or domain controller.

NetVizura, by default, includes built-in support for Snare OpenSource agent. Installation and configuration of Snare agent is described in the following steps.

If you have another Syslog agent then you can create a separate rule for that agent: [Configuring End Users](#).

1. Step - Downloading Snare OpenSource

Download Snare OpenSource Syslog agent from the official website, www.intersectalliance.com.

2. Step - Installing Snare agent on Windows

Install Snare OpenSource agent on domain controller and/or Windows working station by following these instructions.

- Run Snare OpenSource installer with administrative privileges
- Accept License Agreement and press **next**
- Leave defaults for EventLog configuration and press **next**
- Select **Use System account** and press **next**
- Choose to **enable** Web access for Snare Remote Control Interface and be sure that you enter password to protect configuration interface and press **next**.
- From now on just click **next** til the end of installation.

3. Step - Configuring Snare

If you have followed previous steps carefully, you will be able to access Remote Control Interface using your browser of choice.

To access Remote Control Interface paste <http://localhost:6161/> into your address bar in your browser and press **Enter**.

In order to fully configure Snare OpenSource agent to work correctly with NetVizura follow these steps.

1. Network configuration

Click on **Network Configuration** on the left side of the Control Interface. Locate *Destination Snare Server address* field and put IP address of your NetVizura server here. Open NetVizura application, and navigate to **Settings > NetFlow Settings > Configuration** and search for *End users collection port* value. By default collection port should be set to 33515. Locate *Destination Port* field in Snare Remote Control Interface and paste the port value from NetVizura Settings configuration. To finish network configuration check *Enable Syslog Header* checkbox. Click **Change Configuration** to save changes.

2. Objectives Configuration

Click on **Objectives Configuration** on the left side of the Control Interface. Make sure that objective named **Logon_Logoff** exists in the list. Other objectives are not needed for NetVizura to work properly and therefore can be deleted from the list.

3. Apply new configuration

In order for new configuration settings to be applied you should restart Snare service by executing following commands inside Windows command prompt.

Make sure to run Command Prompt with Administrative privileges

First stop Snare service by running:

```
net stop snare
```

After that, start Snare again by running:

```
net start snare
```

By now, you should have your Snare agent successfully installed and configured to work with NetVizura.

Follow step 4 to make sure that NetVizura is actually receiving Syslog messages from Snare agent.

4. Step - Checking installation and configuration

If you have EventLog module activated, you can easily check if you are receiving Syslog messages by going to **EventLog > Syslog** tab.

Otherwise, login to your NetVizura server over SSH, and first check if NetVizura is listening for Syslog messages on specified port.

In order to perform this check run the following command inside your shell.

```
netstat -lnup | grep 33515
```

33515 is a default port. If you have configured collection port to have another value, put that value in the previous command instead of 33515.

If collection is working fine you should see something similar to the following after running this command.

```
udp    0      0  :::33515          :::*
31414/jsvc.exec
```

Next, check if Snare agent is sending syslog to Netvizura collector by running tcpdump.

```
tcpdump port 33515
```

Once again, default port value is used. In case some other value is configured through Settings, replace that value into provided command.

After running tcpdump command, you should see packets incoming to your server from workstations or domain controller.

If tcpdump is not installed on your server do the following:

Debian/Ubuntu

```
sudo apt-get update
sudo apt-get install tcpdump
```

CentOS

```
sudo yum update
sudo yum install tcpdump
```

Getting Started

This chapter covers where is what in NetVizura and initial configuration steps of NetVizura:

- Initial Configuration
 - Initial General Configuration
 - Initial NetFlow Configuration
 - Initial EventLog Configuration
- Navigation
 - General Navigation
 - NetFlow Navigation
 - EventLog Navigation
 - MIB Navigation

Initial Configuration

You must log in as administrator to be able to configure NetVizurar. Default username and password are **admin/admin01**.

Initial configuration consists of the following steps:

- [Initial General Configuration](#)
- [Initial NetFlow Configuration](#)
- [Initial EventLog Configuration](#)

Initial General Configuration

Changing Default Administrator Password

Changing the default administrator credentials is necessary to secure your system from unauthorized access.

To change default administrator account:

1. Login as existing administrator (admin/admin01)
2. Click on the Settings icon (gear)
3. Click on Control Panel > Users
4. Select administrator account and click **Edit**
5. Change the password
6. Add email and other user information
7. Click **Save**.

You can also add more admin accounts and delete the default one. To see more details about managing your account, see [My Account](#). To learn more about managing users, go to [Managing Users](#).

On this page:

- Changing Default Administrator Password
- Creating Users
- Configuring SNMP Policies
- Enabling Email Notifications


Tip

Adding email to an admin account will ensure that the admin gets critical system messages such as license messages, low disk space etc.

Creating Users

To enable multiple users to access NetVizura, you need to create user accounts.

To add a new user:

1. Click **+Add**
2. Insert user's **Login and Contact Information** into appropriate fields.
 -  First name, Last name, Username and Password are mandatory fields.
3. Choose the **Permissions** from the drop-down lists
4. Click **Save**.

For more details on managing users, go to [Managing Users](#) page.

Adding email to an account will allow the user to be added as a recipient of email alarms in NetVizura modules.

Configuring SNMP Policies

After configuring your devices and installing NetVizura you should:

1. Add policies (SNMP configuration) for accessing your devices.

This allows getting useful information from your devices like its name and its interface names. For more information on policies and how to add them, go to article [Configuring SNMP Policies](#).
2. Add policies to your network devices and check if policies are working.

For more information on devices and policy testing, go to article [Configuring Devices](#).

Enabling Email Notifications

Set NetVizura email account to get notifications like system alarms, license info and module alarms.

This will allow you to get notifications like system alarms, license info and module alarms. For more information, go to article [Configuring E-Mail](#).

Initial NetFlow Configuration

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.

i 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.

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](#).

On this page:

- [Setting NetFlow Collection Port](#)
- [Checking the System](#)
- [Setting End User Traffic \(Optionally\)](#)


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.

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.

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.

Initial EventLog Configuration

After configuring your devices and installing NetVizura EventLog you should verify that:

1. Devices are exporting syslog and trap messages to the same port that NetVizura EventLog is listening to.
2. Messages are passing the network firewall and reaching the NetVizura Server
3. NetVizura Server Ports to which syslog and trap messages are sent is open

The screenshot shows the NetVizura EventLog configuration interface. On the left is a sidebar with 'Settings' (selected), 'Modules' (containing 'MIB Settings' and 'EventLog Settings'), and 'Users'. The main area has three tabs: 'Syslog filtering', 'SNMP Trap filtering', and 'Configuration'. Under the 'Configuration' tab, the 'Service options' section contains three settings: 'Syslog socket port' (33514), 'Trap socket port' (33162), and 'Maximal severity level shown' (3 - Error).

By default, syslog messages are exported from the devices to port 514, while NetVizura listens on the port 33514. You need to (1) redirect syslog messages to the 33514, or (2) export syslog messages to 33514, or (3) change NetVizura EventLog configuration. Same applies to trap socket port.

On Linux systems ports lower than 1024 can not be used by application, unless the root privileges are given to NetVizura EventLog.

To change NetVizura EventLog configuration go to **Settings > EventLog Settings > Configuration** and under **Service options** change the **Socket port** values.

Navigation

This chapter covers navigation in NetVizura its modules. In order to get familiar with what is where in NetVizura, be sure to check the following:

- [General Navigation](#)
- [NetFlow Navigation](#)
- [EventLog Navigation](#)
- [MIB Navigation](#)

General Navigation

This chapter explains the basic navigation in NetVizura to allow you to more quickly learn where is what in NetVizura.

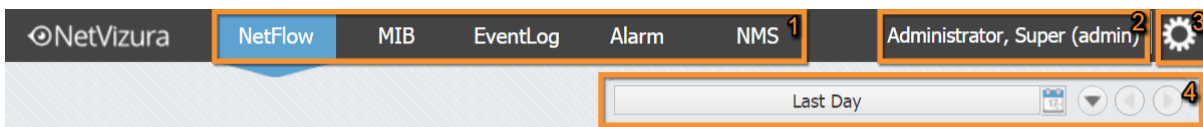
NetVizura interface can be roughly separated in two:

- Top navigation bar
- Main Panel.

Top level Navigation bar is always displayed independent to the Main Panel data. Main Panel shows module specific data in view mode or Settings Panel in settings mode.

Top Navigation Bar

All pages within NetVizura show a navigation bar spanning across the top of the screen.



The Top navigation bar consists of the following options from left to right:

1. **Module Menu** - shows available modules and active module (highlighted in blue).
2. **User Menu** - shows current user and allows access to Log-out and My Account options.
3. **Settings Menu** - link to Settings, website Homepage and About information.
4. **Time Window Menu** - sets time window for which data will be displayed in a module.

Module Menu

Module Menu shows all modules available to the logged in user. You can set which modules will be seen by each user in Settings > Control Panel > Users. (Read more in [Managing Users](#)).

To choose a module simply click on the module name. Active module will be highlighted in blue.

User Menu

User Menu shows currently logged in user (username and user type) and allows access to options Log Out and My Account. To Log-out or get to My Account simply hover over User Menu and choose the desired option.

Use My Account to manage your account information and change your password.

To manage your NetVizura account:

1. Go to User Menu (in the upper right corner, besides Settings)
2. Select **My Account**
3. Click **Edit**
4. Update your password or contact information
5. Click **Save**

Name Surname (Username)

Login Information:

Old password:

New password:

Repeat password:

Contact Information:

E-mail:

Address:

Phone:

Mobile:

Note that guest users (user type guest) can not change My Account settings since it is a shared account. For more information on user types, go to [Managing Users](#) page.

On this page:

- Top Navigation Bar
- Module Menu
- Settings Menu
 - Settings Navigation
 - About information
- Time Window Menu

Settings Menu allows you to go to Settings mode, website Homepage and view About information.

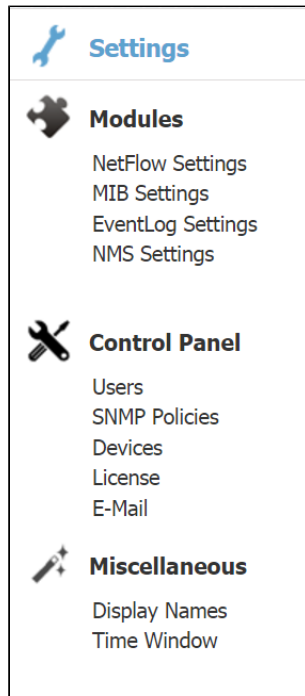
Settings Navigation

To access Settings hover over the Settings Menu (gear icon) and click Settings option.

Settings is divided in two panels: Settings Options Panel to the left and Main Settings Panel in the centre of the screen. Settings Panel will show specific settings depending on the settings option selected.

Settings Options Panel shows the following group of options:

1. **Modules** - settings for each module
2. **Control Panel** - user, SNMP policies, license and Email settings
3. **Miscellaneous** - Time Window and date preferences and Display options



To configure NetVizura or its modules:

1. Choose what you want to configure by selecting it Settings Options Panel
2. Specify what exactly you want to configure by selecting a tab from Tab Panel

Note that display options depend on the user type and permissions: Control Panel is only visible to NetVizura administrators (user type admin), module setting is only visible if the user has permission to see the module, editing module data is only possible if user has write privileges for the module etc.

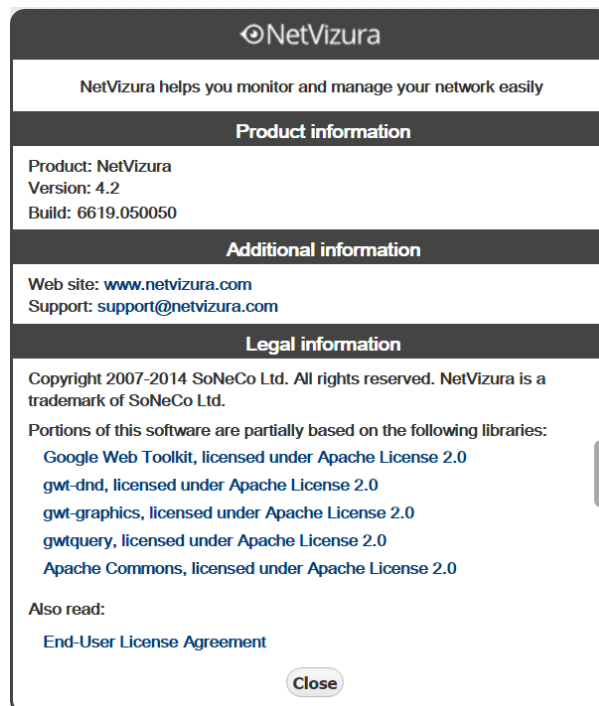
For more information on user types, go to [Managing Users](#) page.

About information

To access About hover over the Settings Menu (gear icon) and click About option.

About shows:

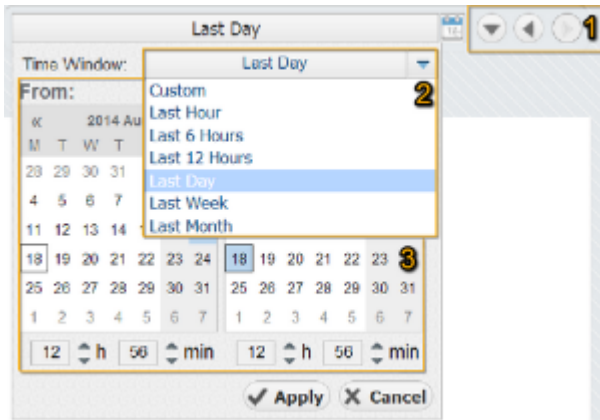
- NetVizura product information:
 - product name
 - product version
- Additional information:
 - website link
 - support email
- Legal information:
 - copyright information
 - list of used libraries
 - EULA



Time Window Menu

Time Window is used to select a time interval for which data will be displayed. For example, if Time Window is set to Last Day then the active module will show only data and events that occurred during last day.

You can set default Time Window and date format preference. To learn how, go to [Configuring Time Window](#).



Time Window options:

1. **Shortcuts** – history, previous and next Time Window value
2. **Standard List** – predefined time interval list: Last Hour, Last 6 Hours, Last 12 Hours, Last Day, Last Week, Last Month
3. **Custom Fields** – any time interval (dates, hours or minutes) picker

Time Window is independent from the views and modules i.e. no matter where you navigate and what statistics you select to view, Time Window value will remain the same and will be applied to the data shown (if applicable).

NetFlow Navigation

This chapter explains what is where in NetVizura NetFlow Analyzer module.

To access NetFlow Analyzer module, click NetFlow on the Module Menu in the Top navigation bar.


When NetFlow module is selected the Flow main screen will show, as shown on the picture below. Note that data displayed will be according to Time Window value: if Time Window is set to Last Day, charts and tables will show netflow traffic that occurred in the last 24h.

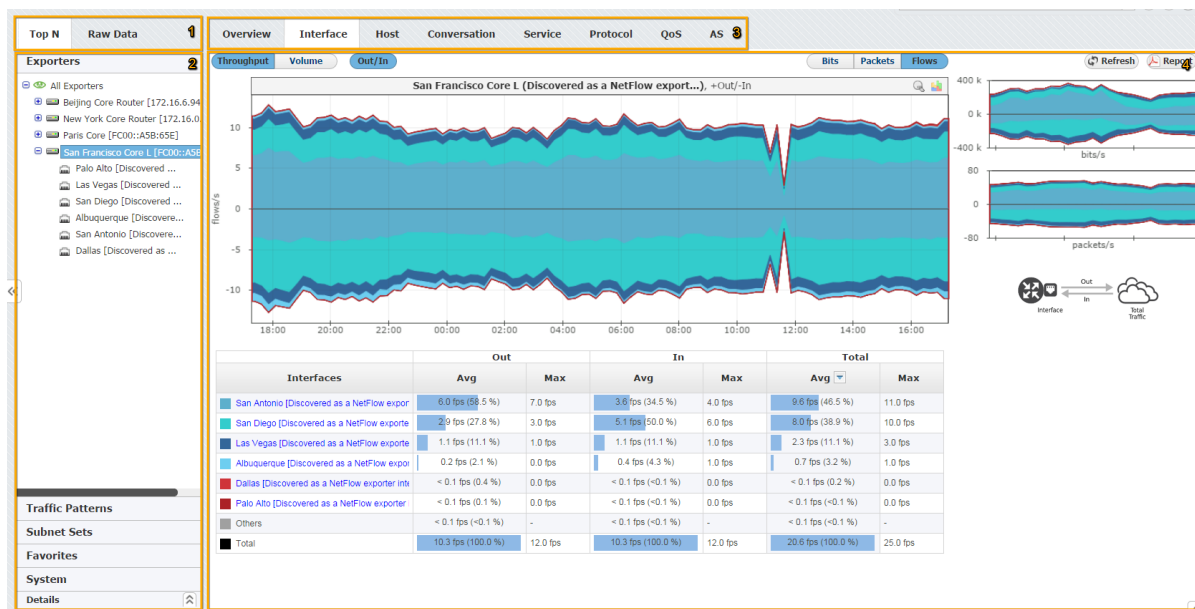
On this page:

- NetFlow Analyzer User Interface
- Navigating TopN
- Navigating Raw Data

NetFlow Analyzer User Interface

First let us define main parts of the NetFlow Analyzer user interface:

1. **Mode Panel** – choose between the TopN and Raw Data mode
 Only users with NetFlow write module permission can see Raw Data mode
2. **Menu Panel** – shows options available in the selected mode
3. **Tab Panel** - shows additional options depending on selected mode and menu option (and selected node)
4. **Main Panel** – shows network traffic charts and tables for the set Time Window



To make navigation easier for you, several indicators (blue or white highlights) show where you are and what you are doing – which mode, option, graph, etc. you are currently using or setting. On the figure above you can see that the selected Mode is TopN, selected Menu option is Exporter (San Francisco is the active node), and that selected Tab options is Interface - this results in Main Panel showing the TopN interfaces for exporter San Francisco.

Navigating TopN

To access TopN choose TopN in the Menu mode.

Main parts of the NetFlow TopN interface are:

1. Time Window - sets the time window for TopN traffic
2. Menu Panel shows:
 - a. Exporters and Interfaces Node tree
 - b. Traffic Patterns and subnets Node tree
 - c. Traffic Patterns and Subnet Sets Node tree
 - d. Favorite nodes
 - e. System traffic types
 - f. Details for selected node in the Node Tree.
3. Selected node - active node for which the traffic is displayed in the Main Panel
4. Traffic distribution (Tab Panel) – traffic distribution by subnets (Traffic Pattern view only), interfaces (Exporter view only), hosts, conversations, services, protocols, QoS and AS
5. Chart and table (Main Panel) – traffic values for the selected node by selected distribution

during time set in Time Window

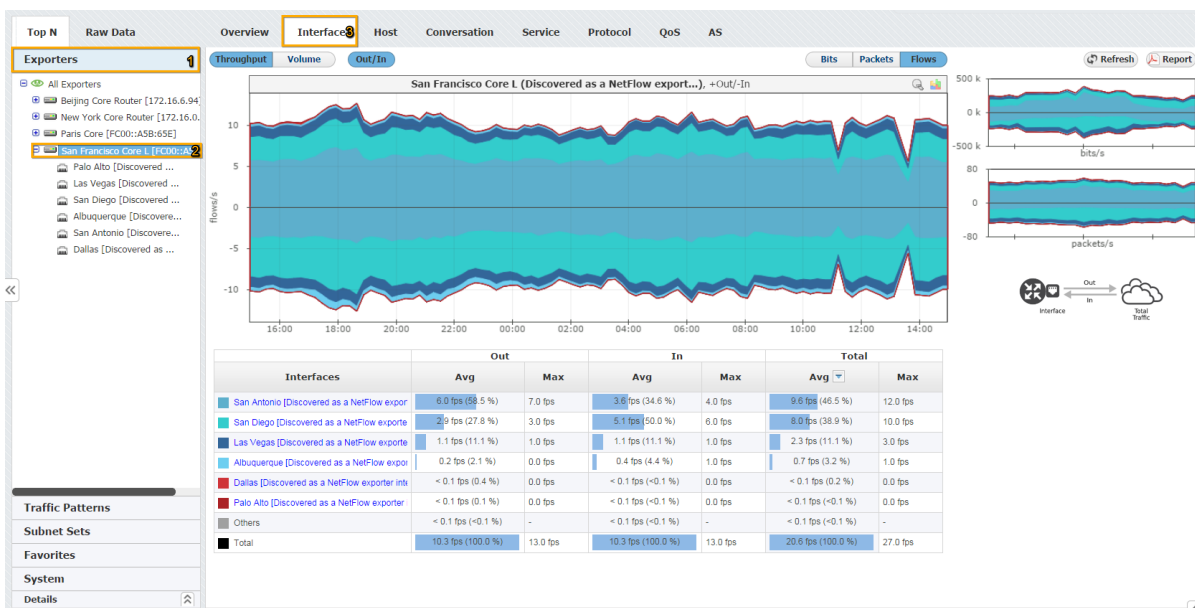
- Side Panel – two small charts showing (bits, packets or flow traffic), PDF reports and refresh options



In Figure above you can see TopN host (4) for Traffic Pattern All Traffic (3) during last 6 hours (1). You can also see that the top host is 172.16.1.41.

To navigate to a desired TopN traffic:

- Set Time Window
- Select TopN in the Mode Panel
- Select an option from the Menu Panel (Exporters, Traffic Patterns, Subnet Sets or Favorites)
- Select the desired node (Exporter, Interface, Traffic Pattern, Subnet Set or Subnet) from the Node Tree
- Select the desired traffic distribution (Overview, Interface, Subnet, Host, Conversation, Service, Protocol, QoS or AS) from the Tab Panel



Navigating Raw Data

By selecting the Raw Data menu option, you will be able to inspect raw data files in the Main panel.


You can also notice the Raw Data Tree right under the Raw Data menu option. Raw Data Tree groups raw data files in folders according to day/hour/minute. Note that Raw Data Tree will show raw data files for the specified time period set in Time Window.

There are 3 ways of inspecting raw data files:

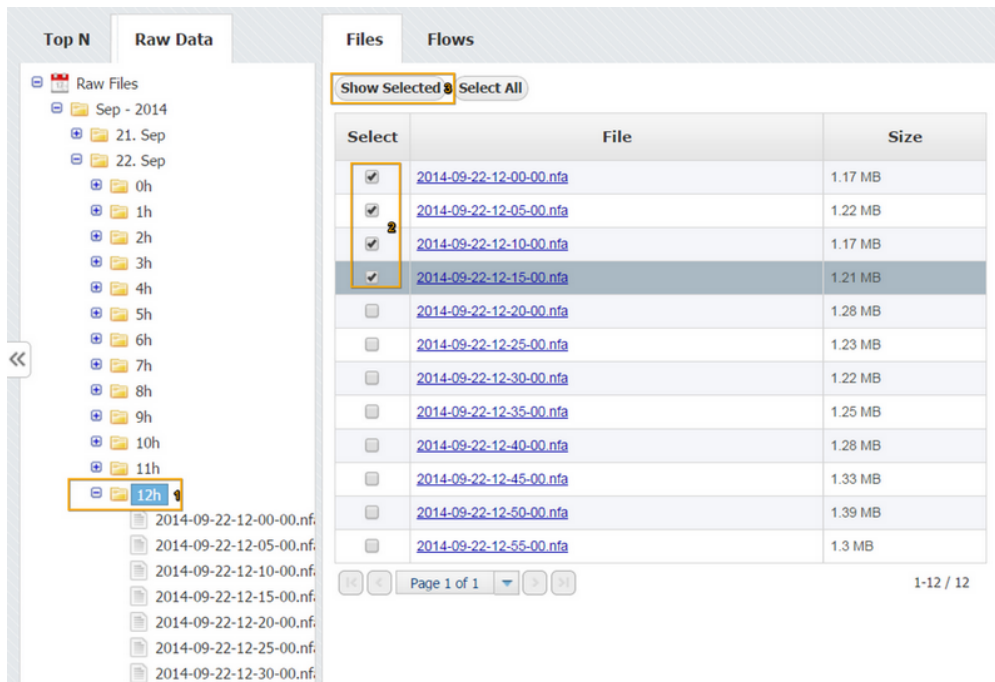
1. Select check boxes next to files you want to inspect and click Show Selected
2. Select a single file in the Raw Data Tree and click Show Selected
3. Click on a single file to inspect it

To navigate and view Raw Data from specific files:

1. Select a date/time folder from the Node Tree
2. Select desired Raw Data files from File Table

 Raw Data includes vast quantity of information about each single flow. Unpacking many files would require significant processing power and memory space, and therefore it is suggested to select and view only a few files at a time.

3. Click **Show Selected**



The screenshot shows the 'Raw Data' section of a software interface. On the left, a 'Raw Files' tree view shows a hierarchy of folders for 'Sep - 2014', '21. Sep', and '22. Sep', with sub-folders for hours from 0h to 12h. The '12h' folder is selected. Below the tree, a list of raw data files is shown, including '2014-09-22-12-00-00.nf' through '2014-09-22-12-30-00.nf'. On the right, a 'Files' table is displayed with columns for 'Select', 'File', and 'Size'. The table contains 12 rows of data, with the first four rows selected (checked boxes). The 'Show Selected' button is highlighted. The table footer shows 'Page 1 of 1' and '1-12 / 12'.

Select	File	Size
<input checked="" type="checkbox"/>	2014-09-22-12-00-00.nfa	1.17 MB
<input checked="" type="checkbox"/>	2014-09-22-12-05-00.nfa	1.22 MB
<input checked="" type="checkbox"/>	2014-09-22-12-10-00.nfa	1.17 MB
<input checked="" type="checkbox"/>	2014-09-22-12-15-00.nfa	1.21 MB
<input type="checkbox"/>	2014-09-22-12-20-00.nfa	1.28 MB
<input type="checkbox"/>	2014-09-22-12-25-00.nfa	1.23 MB
<input type="checkbox"/>	2014-09-22-12-30-00.nfa	1.22 MB
<input type="checkbox"/>	2014-09-22-12-35-00.nfa	1.25 MB
<input type="checkbox"/>	2014-09-22-12-40-00.nfa	1.28 MB
<input type="checkbox"/>	2014-09-22-12-45-00.nfa	1.33 MB
<input type="checkbox"/>	2014-09-22-12-50-00.nfa	1.39 MB
<input type="checkbox"/>	2014-09-22-12-55-00.nfa	1.3 MB

By clicking on the Show selected, Raw Data Table will open showing the information from selected raw data files.

Files		Flows		Filtering		Grouping		Sorting						
Request	Names	Details	X	Clear	Src IP	Src Port	Dst IP	Dst Port	Protocol	TOS	TCP Flags	Flows	Packets	Bytes
11-08-2014 10:20:50.00	30-08-2014 03:24:02.298	10:10:57.296 sec	10:101.168.156	50725	172.16.177.238	80	0	0	A	1	1	1	8	340
11-08-2014 10:20:52.00	30-08-2014 03:23:39.298	10:10:57.296 sec	10:247.179.156	80	172.16.1.41	7088	0	0	A	1	1	1	1	1,404
11-08-2014 10:20:52.00	30-08-2014 03:23:39.298	10:10:57.296 sec	10:247.179.156	80	172.16.1.41	7088	0	0	AP	1	1	1	1	971
11-08-2014 10:21:33.00	30-08-2014 03:24:29.298	10:10:57.296 sec	10:29.228.156	50895	172.16.68.101	27154	0	0	A	1	1	1	1	40
11-08-2014 10:20:43.00	30-08-2014 03:24:29.298	10:10:57.296 sec	10:4.237.100	55905	172.16.27.71	30038	0	0	A	1	1	1	8	13,170
11-08-2014 10:20:53.00	30-08-2014 03:24:25.298	10:10:57.296 sec	10:4.237.100	55905	172.16.27.71	30038	0	0	AP	1	1	2	2	2,928
11-08-2014 10:21:06.00	30-08-2014 03:24:29.298	10:10:57.296 sec	10:123.248.156	29511	172.16.170.49	26798	0	0	AS	1	1	1	1	40
11-08-2014 10:20:51.00	30-08-2014 03:23:38.298	10:10:57.296 sec	10:44.1.157	80	172.16.1.41	20812	0	0	A	1	1	1	1	52
11-08-2014 10:21:06.00	30-08-2014 03:23:53.298	10:10:57.296 sec	10:44.1.157	80	172.16.1.41	23010	0	0	A	1	1	1	1	52
11-08-2014 10:20:51.00	30-08-2014 03:23:38.298	10:10:57.296 sec	10:161.2.157	1084	172.16.20.86	54189	0	0	AP	1	1	1	1	108
11-08-2014 10:20:44.00	30-08-2014 03:23:31.298	10:10:57.296 sec	10:6.10.157	45402	192.168.13.48	52214	17	0	none	1	1	1	1	470
11-08-2014 10:20:53.00	30-08-2014 03:23:59.298	10:10:58.296 sec	10:28.29.157	3297	172.16.108.1	25	0	0	A	1	1	2	2	80
11-08-2014 10:21:06.00	30-08-2014 03:24:13.298	10:10:57.296 sec	10:28.29.157	3297	172.16.108.1	25	0	0	AP	1	1	1	1	78
11-08-2014 10:21:18.00	30-08-2014 03:24:06.298	10:10:57.296 sec	10:164.38.157	51413	172.16.18.20	2270	0	0	A	1	1	1	1	1,404
11-08-2014 10:21:35.00	30-08-2014 03:24:22.298	10:10:57.296 sec	FC00_A7D:439D	80	FC00_A83:268C	49067	0	0	A	1	1	1	1	1,404
11-08-2014 10:21:35.00	30-08-2014 03:24:22.298	10:10:57.296 sec	10:125.77.157	80	192.168.38.140	49067	0	0	A	1	1	1	1	845
11-08-2014 10:21:09.00	30-08-2014 03:23:59.298	10:10:57.296 sec	10:49.80.157	57890	172.16.198.10	8080	0	0	A	1	1	1	1	40
11-08-2014 10:21:07.00	30-08-2014 03:23:54.298	10:10:57.296 sec	10:49.80.157	57905	172.16.198.10	8080	0	0	AP	1	1	1	1	1,081
11-08-2014 10:21:40.00	30-08-2014 03:24:27.298	10:10:57.296 sec	10:154.87.157	80	172.16.1.41	27618	0	0	AP	1	1	1	1	1,343
11-08-2014 10:21:14.00	30-08-2014 03:24:01.298	10:10:57.296 sec	10:162.125.157	80	172.16.1.41	23922	0	0	A	1	1	1	1	1,404
11-08-2014 10:21:40.00	30-08-2014 03:24:27.298	10:10:57.296 sec	10:162.125.157	80	172.16.1.41	27615	0	0	A	1	1	1	1	52
11-08-2014 10:21:34.00	30-08-2014 03:24:21.298	10:10:57.296 sec	10:162.125.157	80	172.16.1.45	44113	0	0	AS	1	1	1	1	60
11-08-2014 10:21:22.00	30-08-2014 03:24:09.298	10:10:57.296 sec	10:95.129.157	80	172.16.8.10	32975	0	0	A	1	1	1	1	52
11-08-2014 10:20:49.00	30-08-2014 03:23:36.298	10:10:57.296 sec	10:95.129.157	80	172.16.1.41	20535	0	0	A	1	1	1	1	52
11-08-2014 10:20:49.00	30-08-2014 03:23:38.298	10:10:57.296 sec	10:85.129.157	80	172.16.8.104	2970	0	0	AP	1	1	1	1	1,008

For easier navigation according to your interest you can further filter, group and sort Raw Data Table records by certain fields.

EventLog Navigation

EventLog User interface

When EventLog module is selected main screen will show the following parts:

1. **Mode Panel** - choose between the Syslog and SNMP Trap mode.
2. **Main Panel** - displays results of SNMP request and MIB search operations.

For the purpose of this chapter, we will focus on the navigation in the Syslog mode.

Navigating in Syslog mode

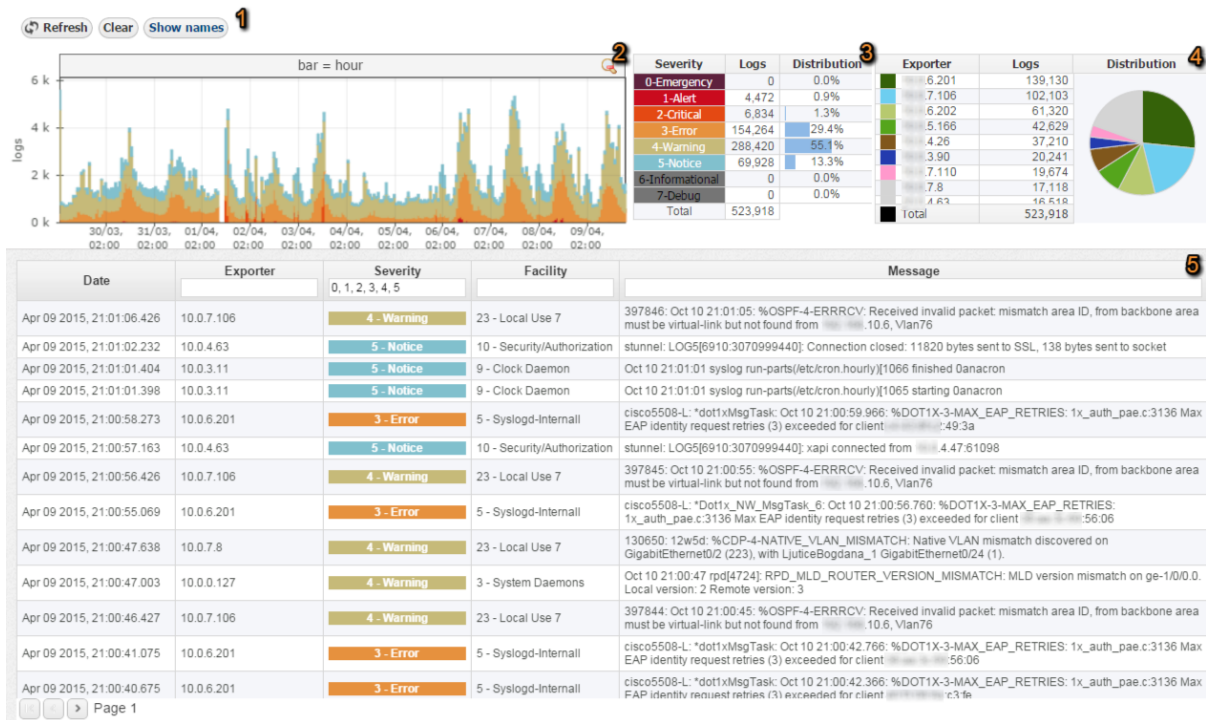
To view syslog go to EventLog module and click Syslog tab. Here you can see syslog messages sent from different exporters for a chosen Time Window.

1. Show Options
2. EventLog Chart
3. Severity Table
4. Exporter Table
5. EventLog Table

On this page:

- Show Options
- Syslog Chart
- Severity Table
- Exporter Table
- Syslog Table

Table and charts will show logs that have (1) the same severity as set in Severity Table (2) for the time set in Time Window. For these logs Exporter table will show distribution by exporters and Severity Table will show distribution by log's severity.



For example, on the screenshot to the left, you can see that logs that occurred during the selected Time Window and severity 0 to 5 are shown. You can also see that there was 523,918 such logs (Severity Table) of which most numerous were Warnings (55%) and Errors (29%).

You can also see the distribution of these logs by exporters in the Exporter table: exporter x.x.6.201 generated the most logs (139,130).

Show Options

Show Options:

1. Refresh Data – manually refresh data on charts and tables
2. Clear filters – clear all filters
3. Show Exporter Names – show names of exporters (routers) instead of their IP address

Syslog Chart

EventLog Chart shows distribution of syslog messages (logs) by severity:

1. Logs per bar (y-axis)
2. Time axis (x-axis)
3. Bar width
4. Zoom out

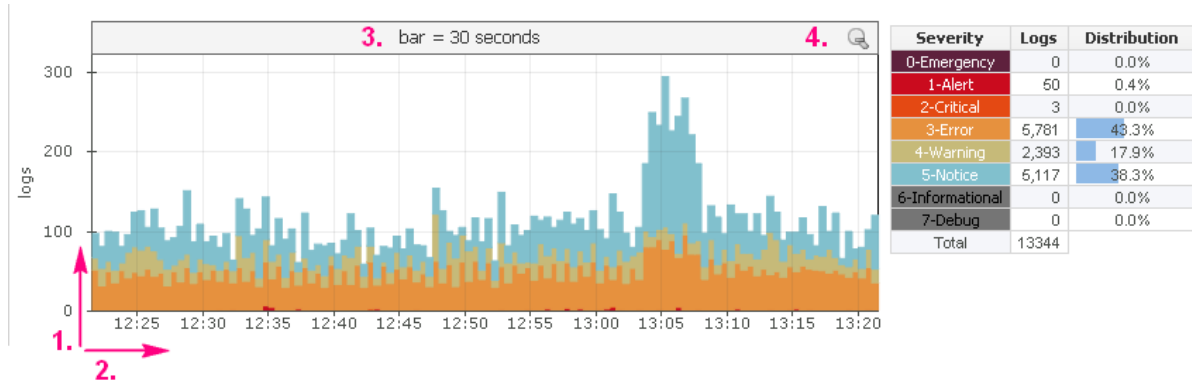


Chart shows number of logs in certain time chunks (1 minute, 1 day, 1 hour). Width of the chart bars and number of bars depends on the Time Window selected. See table below:

Time Window	Bar Width	Number of Bars
Last hour	30 seconds	120
Last 6 hours	5 minutes	72
Last 12 hours	5 minutes	144
Last day	15 minutes	96
Last week	1 hour	168
Last month	6 hours	120

Chart has two axis: numerical y-axis and time x-axis. Numerical axis shows the number of logs per bar. Time shown on the x-axis of the chart is the same time as set in the Time Window. Next to the Syslog Chart is the Severity Table in which you can select if syslog messages of the certain severity will be displayed on the chart or not. Colors on the chart correspond with the colors of the syslog Severity in the Severity Table.

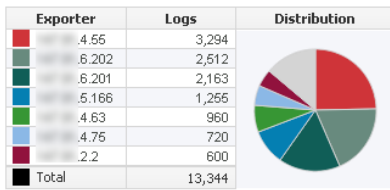
On the EventLog Chart above you can see that one bar on the chart represents logs during 30 seconds (bar = 30 seconds).

Severity Table

Severity Table shows log distribution by severity, for the logs of selected severity that occurred in the selected Time Window. On screenshot to the right currently selected severity levels are 0, 1, 2 and 3. This means that Syslog chart and tables will show only logs with this severity levels. By clicking on the corresponding severity in the Severity Table you can switch on/off logs of that severity. Switched off severity is shown with a gray background and logs with that severity are not shown on the carts and graphs.

Severity	Logs	Distribution
0-Emergency	0	0.0%
1-Alert	959	1.3%
2-Critical	39	0.1%
3-Error	71,679	98.6%
4-Warning	0	0.0%
5-Notice	0	0.0%
6-Informational	0	0.0%
7-Debug	0	0.0%
Total	72,677	

Exporter Table



Exporter Table shows log distribution by exporter, for the logs of selected severity that occurred in the selected Time Window. Top 7 exporters have a color assigned, while other exporters are grey and under Others on the pie chart. To see other exporters, scroll down the exporter list. Clicking on an exporter will show only logs for that exporter on the charts and table. By clicking on it again, you can switch back to seeing logs for all exporters.

Syslog Table

EventLog Table shows messages with selected severity (in Severity Table) that were received during time set in the Time Window. For each message Date, Exporter, Severity, Facility and Message content is displayed. Severity levels are shown with the corresponding color, as in the chart and Severity Table. 9/19 Figure 7: Exporter Table Figure 6: Severity Table Syslog Table can be filtered by Exporter, Severity, Facility and Message content. Note that the filters can be activated by selecting items in the Severity and Exporter Tables, as described above. To clear all filters, click the Clear button above the Syslog chart. To show exporter DNS names, click the Show Names button above the Syslog chart.

Date	Exporter	Severity	Facility	Message
Jul 29 2013, 18:16:19.288	7.106, 4.75	0,1,2,3,4,5		
Jul 29 2013, 18:16:17.464	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Connection closed: 11468 bytes sent to SSL, 138 bytes sent to socket
Jul 29 2013, 18:16:14.244	7.106	4 - Warning	23 - Local Use 7	1379813: Jul 29 18:16:16: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 10.6.10.6, Vlan76
Jul 29 2013, 18:16:14.246	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Post check: verification level is low, skipping check
Jul 29 2013, 18:16:07.465	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: xapi connected from 4.82.60074
Jul 29 2013, 18:16:07.465	7.106	4 - Warning	23 - Local Use 7	1379812: Jul 29 18:16:06: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 10.6.10.6, Vlan76
Jul 29 2013, 18:15:57.465	7.106	4 - Warning	23 - Local Use 7	1379811: Jul 29 18:15:56: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 10.6.10.6, Vlan76
Jul 29 2013, 18:15:47.472	7.106	4 - Warning	23 - Local Use 7	1379810: Jul 29 18:15:46: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 10.6.10.6, Vlan76
Jul 29 2013, 18:15:44.231	4.75	3 - Error	10 - Security/Authorization	stunnel: LOG3[7582:3072637840]: SSL_read: Connection reset by peer (104)
Jul 29 2013, 18:15:44.231	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Connection reset: 11426 bytes sent to SSL, 138 bytes sent to socket
Jul 29 2013, 18:15:44.181	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Post check: verification level is low, skipping check

Page 1

MIB Navigation

When MIB module is selected the MIB main screen will show the following parts:

1. **Mode Panel** - choose between the MIB and Device mode.
2. **Menu Panel** - shows options available in the selected mode
3. **Tab Panel** - tab contains the information on the OID requested and the device the SNMP Query was sent to. For each SNMP request a new tab will open.
4. **Main Panel** - displays results of SNMP request and MIB search operations.

On this page:

- Navigating in MIB Mode
- Navigating in Device Mode

The screenshot shows the MIB Browser interface with the MIB tree on the left, a table of interface entries in the center, and details for the selected ifTable node at the bottom.

index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus
.1	1	GigabitEthernet0/1	ethernetCsmacd(6)	1500	1000000000	00:11:5c:82:96:00	up(1)	up(1)
.2	2	GigabitEthernet0/2	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:02	up(1)	down(2)
.3	3	GigabitEthernet0/3	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:03	up(1)	down(2)
.4	4	GigabitEthernet0/4	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:04	up(1)	down(2)
.5	5	GigabitEthernet0/5	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:05	up(1)	down(2)
.6	6	GigabitEthernet0/6	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:06	up(1)	down(2)
.7	7	GigabitEthernet0/7	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:07	up(1)	down(2)
.8	8	GigabitEthernet0/8	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:08	up(1)	down(2)
.9	9	GigabitEthernet0/9	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:09	up(1)	down(2)
.10	10	GigabitEthernet0/10	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:0a	up(1)	down(2)
.11	11	GigabitEthernet0/11	ethernetCsmacd(6)	1500	100000000	00:11:5c:82:96:0b	up(1)	down(2)
.12	12	GigabitEthernet0/12	ethernetCsmacd(6)	1500	1000000000	00:11:5c:82:96:0c	up(1)	up(1)
.13	13	Null0	other(1)	1500	4294967295		up(1)	up(1)
.14	14	Vlan1	propVirtual(53)	1500	1000000000	00:11:5c:82:96:00	up(1)	up(1)
.15	15	Loopback0	softwareLoopback(24)	1514	4294967295		up(1)	up(1)

Details for ifTable:

- Type: Object
- Name: ifTable
- OID: .1.3.6.1.2.1.2.2
- Status: mandatory
- Access: not-accessible
- Value Type: SEQUENCE OF ifEntry
- Description: A list of interface entries. The

On the screenshot above, you can see that MIB ifTable is selected in the MIB tree and that after SNMP request the Main Panel shows the ifTable with OID values for the currently selected device (cisco3550-xxx). In the Details it is visible that the ifTable OID is .1.3.6.1.2.1.2.2.

Navigating in MIB Mode

MIB Browser is selected by default and it shows the MIB tree with its options for SNMP request and OID search.

MIB browser options:

1. **MIB Tree** – shows the MIB Tree and corresponding options:
 - a) searching the MIB tree for particular OID
 - b) request a SNMP Query for particular MIB on the Current device
2. **Favorites** – shows all user favorite OIDs (added from the MIB Tree)
3. **Details** – shows OID details (name, description etc.) for the selected node in the MIB tree

Navigating in Device Mode

Device mode is used to set the Current device. Any SNMP request in the MIB tab will be sent to the Current device.

The screenshot shows the MIB Browser interface in MIB mode. The MIB tree is visible on the left, and the details for the selected ifTable node are shown at the bottom.

Details for ifTable:

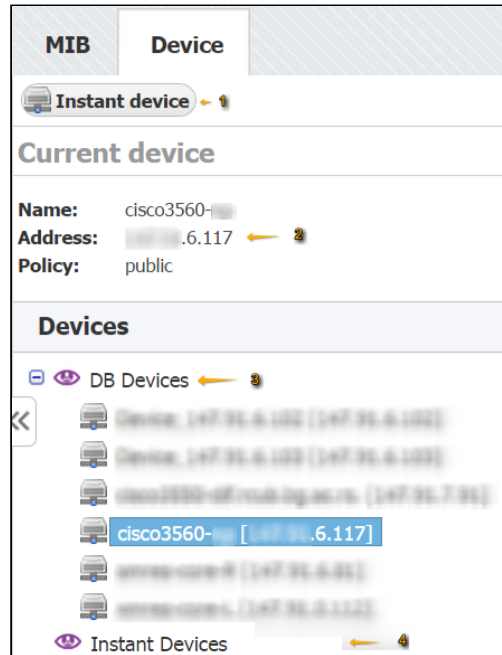
- Type: Object
- Name: ifTable
- OID: .1.3.6.1.2.1.2.2
- Status: mandatory
- Access: not-accessible
- Value Type: SEQUENCE OF ifEntry
- Description: A list of interface entries. The

Device mode is available only if NMS module is included in NetVizura application.

On screenshot to the left you can see that the Current device is cisco-xyz. When you click on the Request in the MIB tab, SNMP Query command will be sent to this device.

Device Tab includes following options and information:

1. Add instant device
2. Current device
3. List of devices in the application database
4. List of instant devices



Devices added in the **Settings > MIB Settings > Devices** will show in the list of devices and will be always available.

Instant devices are user added devices that will not be saved in the database (the list will be cleared after logout). Instant devices are used if you want to quickly check an OID on a device but do not want the device to be stored for later use.

Using NetVizura

This chapter shows how to use NetVizura and its modules:

- Basic NetFlow Usage
 - Using Charts and Tables
 - Traffic Distributions (Top Talkers)
 - Exporters and Interfaces Traffic
 - Basic Traffic Patterns
 - Subnet Sets
 - Managing NetFlow Favorites
 - Reading NetFlow Details
 - Generating Reports
- Advanced NetFlow Usage
 - Advanced Traffic Pattern Examples
 - Inspecting Raw Data (Flow Records)
 - Viewing End User Traffic
 - Using NetFlow Alarms
 - Understanding NetFlow System Traffic
 - Using Activity Log
- EventLog Usage
 - Viewing Syslog Messages
 - Inspecting Syslogs
 - Viewing SNMP Traps
 - Understanding Eventlog System Traffic
 - Using EventLog Alarms
 - Syslog How to...
- MIB Usage
 - Searching OIDs
 - Setting a Current Device
 - Making SNMP Request
 - Managing MIB Favorites
 - Reading MIB Details

Basic NetFlow Usage

In this chapter you will find out what network traffic is available to you and how to make the best use of it. Network traffic is available in NetFlow Analyzer module.

This chapter covers:

- **Traffic Distributions (Top Talkers)** - how network traffic is split by categories (such as hosts, conversations, QoS etc.).
- **Using Charts and Tables** - how to use charts and tables showing network traffic
- **Exporters and Interfaces Traffic** - how to view traffic for exporters and their interfaces
- **Basic Traffic Patterns** - how to start analyzing logical structures of network traffic, independent of the physical infrastructure.
- **Subnet Sets** - how to analyze statistics for group of Subnets (IP ranges) or smaller Subnet Sets.
- **Favorites** - how to manage frequently monitored nodes.
- **Details** - how to view additional information for a selected node.
- **Reports** - how to export traffic to PDF file or schedule a report.

Using Charts and Tables

Traffic is represented in several visual manners in order to provide you quick insight in the traffic structure:

- **Throughput Chart** (area and bar time chart) - time diagram, which represents one or more parameters within the selected time frame allowing you to follow changes in traffic and recognize traffic trends with ease.
- **Volume Chart** (pie chart) - distribution of Top N bandwidth consumers in a pie chart form, allowing you to easily visualize and compare bandwidth consumers with each other.
- **Table** (text table) - in addition, Throughput and Volume charts are followed below by a corresponding top-talker table. Top-talker table shows entities most contributing to the traffic showed on Throughput and Volume charts.

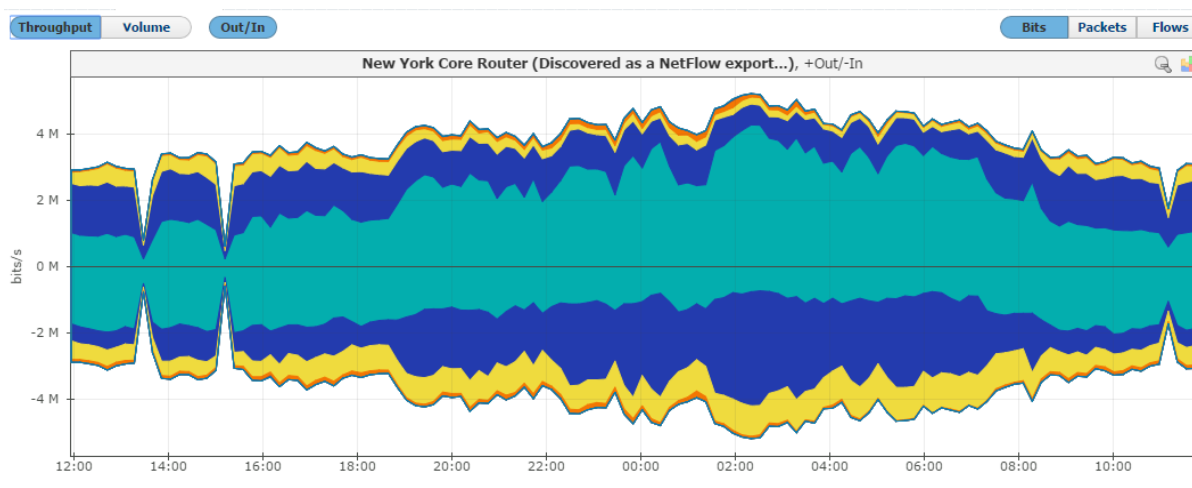
Charts and tables are network element and time specific. In other words, each chart and table shows traffic for a selected node in the Navigation tree for the given Time Window.

On this page:

- Throughput Chart
 - View Options
 - Zooming
- Volume Chart
- Table
 - IP Address Resolution
- Additional Options
 - Set Metrics
 - Side Charts
 - Top Talker Isolation
 - Top Talker Drill-Down
 - Top Talker Highlight

Throughput Chart

Throughput is a time chart enabling you to see large number of parameters in an arbitrary time interval (set by Time Window). This is particularly suitable for viewing changes in the traffic over time, spotting traffic trends and anomalies:



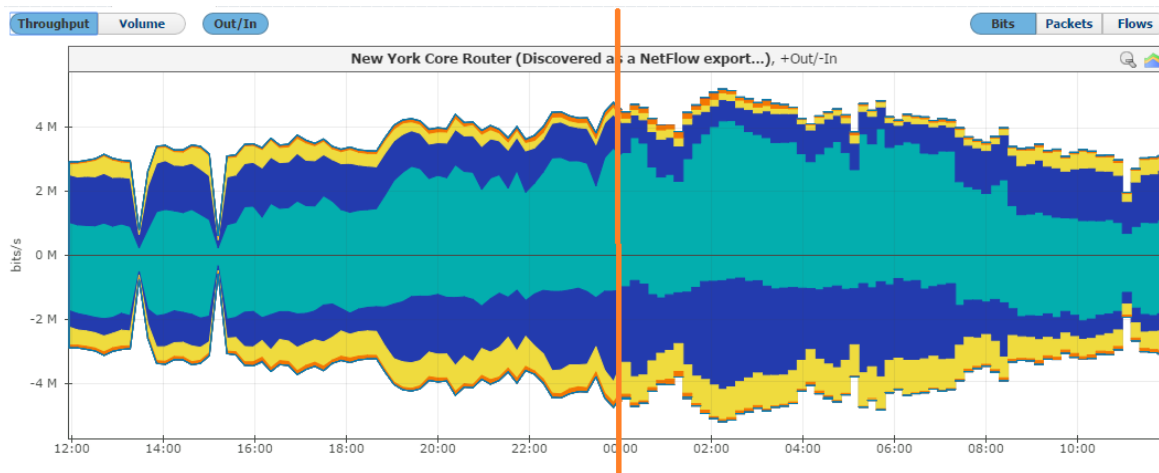
On the graph, positive part of the y-axis shows outbound (Out) traffic, while negative part of the y-axis shows inbound (In) traffic. Out traffic is traffic originated from the internal network to external network, while In traffic is traffic destined to the internal network from external network.

The Top-talker table below will show average and maximum values for In and Out traffic achieved during the given time interval, as well as Total traffic in the selected measurement unit (bps, pps, fps) and as percentage of total traffic for each table entry.

View Options

Throughput chart can be seen as area or bar chart. Area chart enables you to see the flow of traffic more smoothly, while bar chart gives you the ability to view traffic by each sample. Use the area chart for spotting trends and over-viewing the traffic of large time intervals. Use the bar chart when solving problems and when you need more details on the sample level (time interval you are inspecting is relatively small).

To switch between the area and bar chart click the Area chart or Bar chart button. This will give you a chart as shown in screenshot below. Re-selecting the option will give you the original view back.



Zooming

You can zoom in and out of the Throughput chart. This enables you to quickly and more directly select the time window you are interested in (in comparison to the time Time Window).

To zoom in:

1. Move the cursor over the chart (cursor will turn from arrow to hand).
2. Position the mouse to the beginning of the time interval you are interested in.
3. Press and hold the left mouse button.
4. Drag the cursor to the end of the time interval you are interested in
5. Release mouse button

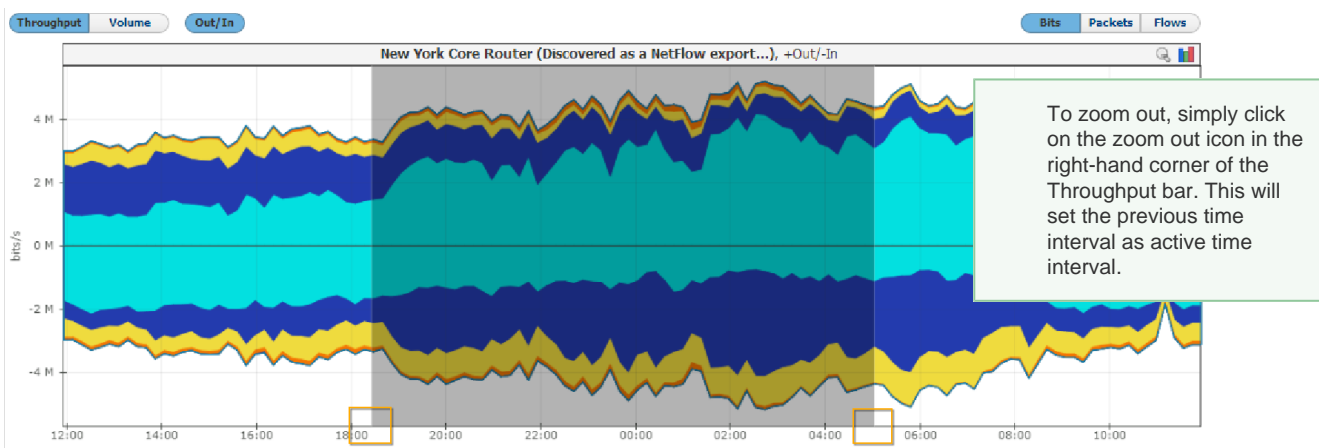


Chart and table are now showing the traffic for the interval you have just set.



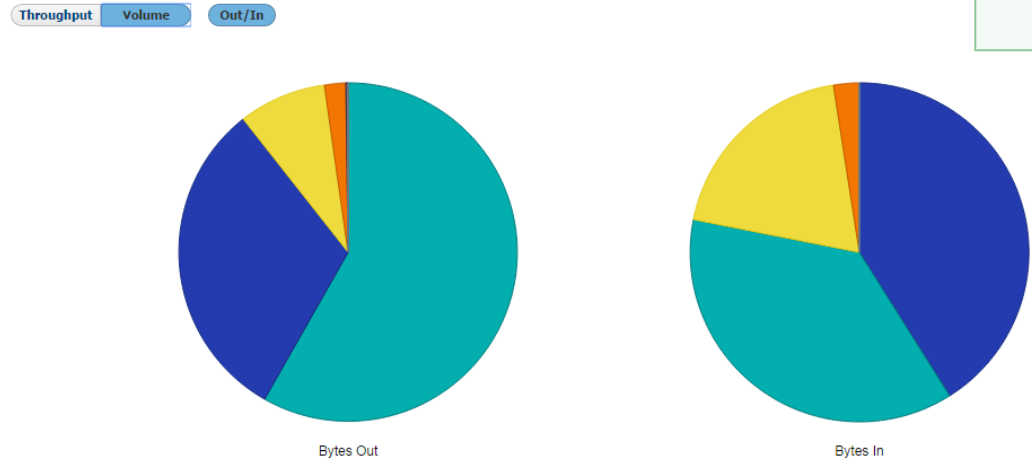
Time Window is in sync with zoom in and out meaning that zooming will set a new Time Window value. The Top-talker table is adjusted to show traffic for the zoom time interval. Zooming in also activates the zoom out icon (beside area or bar chart icon).

Volume Chart

Volume is a pie chart enabling you to easily visualize top-talkers in regard to total traffic and each other, for the given Time Window.

There are two charts, for inbound (In) and outbound (Out) traffic.

To change the number of top-talkers shown in the charts and tables, read more about [Configuring TopN Rules](#).



Top-talker table will show total traffic volume values if Volume chart option is active. It will show values in the selected measurement unit (bytes, packets, flows) and as percentage of the total traffic for each table entry.

Table

Text table shows average, maximum and total values for top-talker contributors. Additional columns, such as In, Out, Src or Dst, will show if applicable.

Hosts	Out (Src)		In (Src)		Total (Src)	
	Avg	Max	Avg	Max	Avg	Max
bud02s24-in-f14.1e100.net	0.0 bps (0.0 %)	0.0 bps	357.4 kbps (11.4 %)	31.9 Mbps	357.4 kbps (10.2 %)	31.9 Mbps
a10_static.akamai technologies.com	0.0 bps (0.0 %)	0.0 bps	289.0 kbps (9.2 %)	67.0 Mbps	289.0 kbps (8.3 %)	67.0 Mbps
bud02s22-in-f14.1e100.net	0.0 bps (0.0 %)	0.0 bps	140.6 kbps (4.5 %)	14.3 Mbps	140.6 kbps (4.0 %)	14.3 Mbps
13.107.4.50	0.0 bps (0.0 %)	0.0 bps	131.9 kbps (4.2 %)	18.5 Mbps	131.9 kbps (3.8 %)	18.5 Mbps
bud02s21-in-f14.1e100.net	0.0 bps (0.0 %)	0.0 bps	130.8 kbps (4.2 %)	19.4 Mbps	130.8 kbps (3.7 %)	19.4 Mbps
87.98.131.77	0.0 bps (0.0 %)	0.0 bps	128.9 kbps (4.1 %)	135.7 kbps	128.9 kbps (3.7 %)	135.7 kbps
rockradio.kbcnet.rs	0.0 bps (0.0 %)	0.0 bps	125.0 kbps (4.0 %)	405.5 kbps	125.0 kbps (3.6 %)	405.5 kbps
www.soneco.rs	0.0 bps (0.0 %)	0.0 bps	124.0 kbps (3.9 %)	504.5 kbps	124.0 kbps (3.5 %)	504.5 kbps
8.254.105.125	0.0 bps (0.0 %)	0.0 bps	89.1 kbps (2.8 %)	17.7 Mbps	89.1 kbps (2.5 %)	17.7 Mbps
5.22.191.81	0.0 bps (0.0 %)	0.0 bps	69.0 kbps (2.2 %)	12.9 Mbps	69.0 kbps (2.0 %)	12.9 Mbps
Others	351.1 kbps (100.0 %)	-	1.6 Mbps (49.6 %)	-	1.9 Mbps (54.7 %)	-
Total	351.1 kbps (100.0 %)	4.7 Mbps	3.1 Mbps (100.0 %)	70.4 Mbps	3.5 Mbps (100.0 %)	71.8 Mbps

Table can be sorted by any column in decreasing or increasing order. Selecting the column again will switch between decreasing, increasing and no ordering. Table also shows if there were any alarms during the selected Time Window for all top-talkers.

"Others" entry in the charts and table (in gray) represents traffic not belonging to top-talkers. Only exception to this is the display of Subnets where "Others" entry represents all values that are matched to a traffic but not matched with any defined subnet for that traffic.

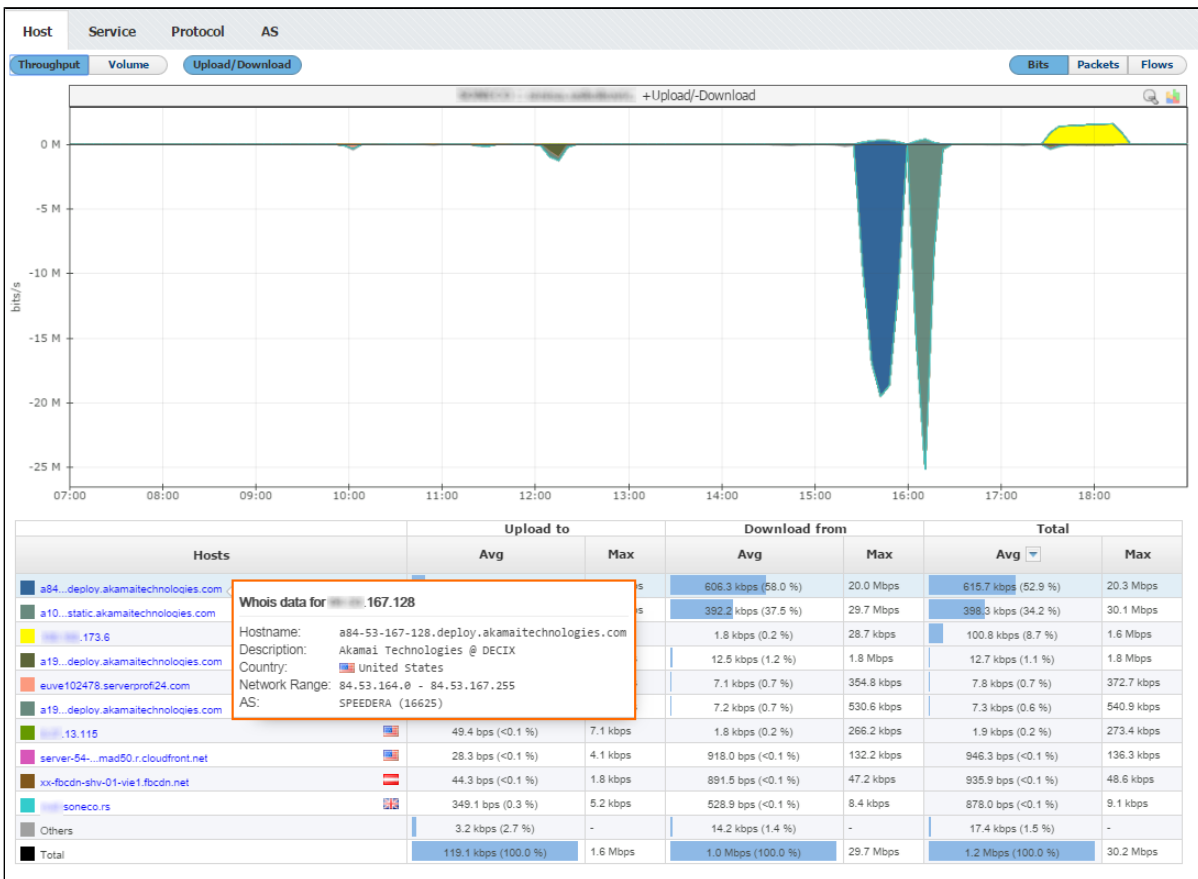
IP Address Resolution

In order to enable IP address resolution, your NetVizura server should have local or remote communication with DNS server (for Hostname) and Internet access (for Whois information).

To completely understand host, conversation and AS traffic it is necessary to have background knowledge about the host IP addresses that participated. However, this may prove time consuming and network admins often don't have time to browse manually for this information online.

For this reason, NetVizura provides IP address resolution (Hostname, Geo-location and Whois information) that significantly saves time, improves readability of the statistics and increases overall contextual awareness.

A typical attack example is when you notice that a great number of flows or small packets have occurred in a short amount of time.



As you can see in the screenshot above, this end user had two bigger downloads at around 16h from two IP Addresses belonging organization Akamai Technologies, located in United States.

Additional Options

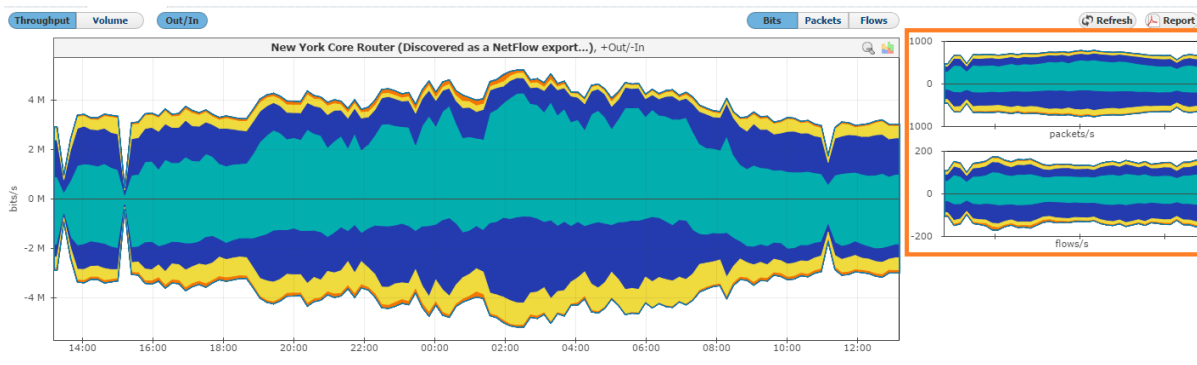
Set Metrics

As a measurement unit for the observed traffic, the charts and table can show:

- **Bits** - bits per second (bits/s, bps)
- **Packets** - packets per second (packet/s, pps) and
- **Flows** - flows per second (flow/s, fps)

Side Charts

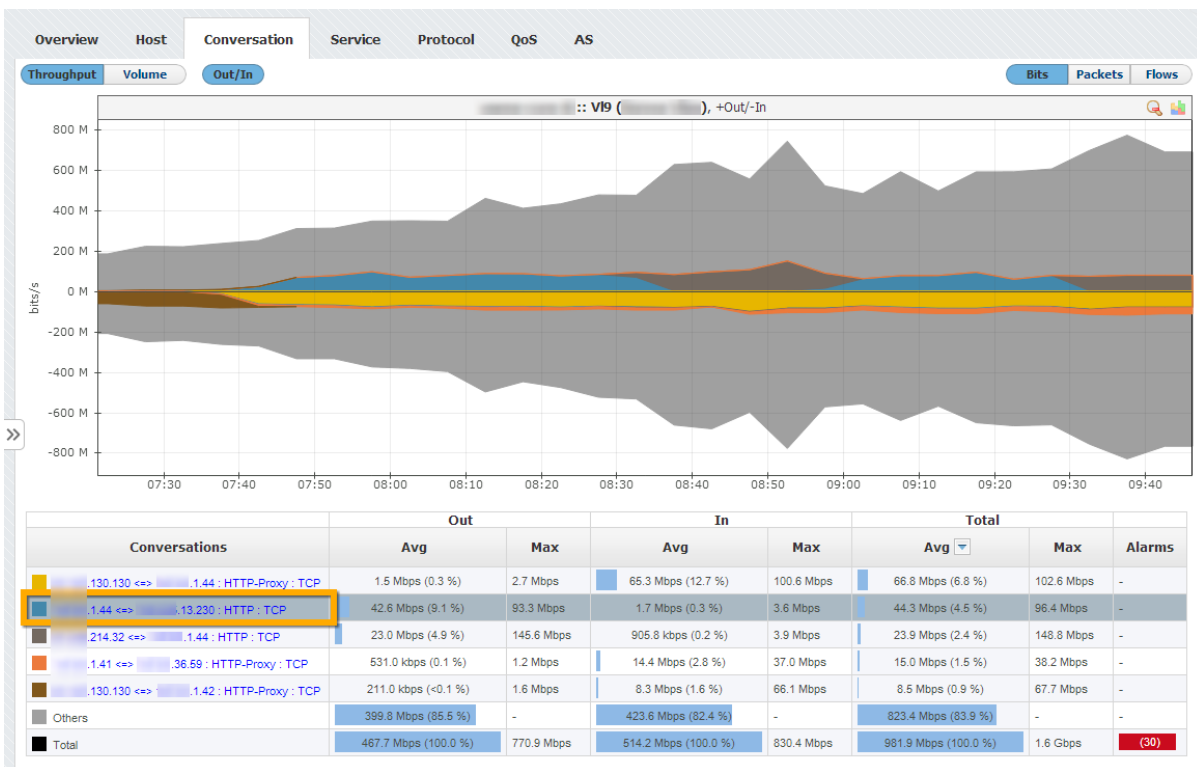
To the right of the main chart with selected measurement, you can see also two other measurements:



This view helps you to quickly compare the number of flows and/or packets with their size in bytes, enabling you to recognize attacks.

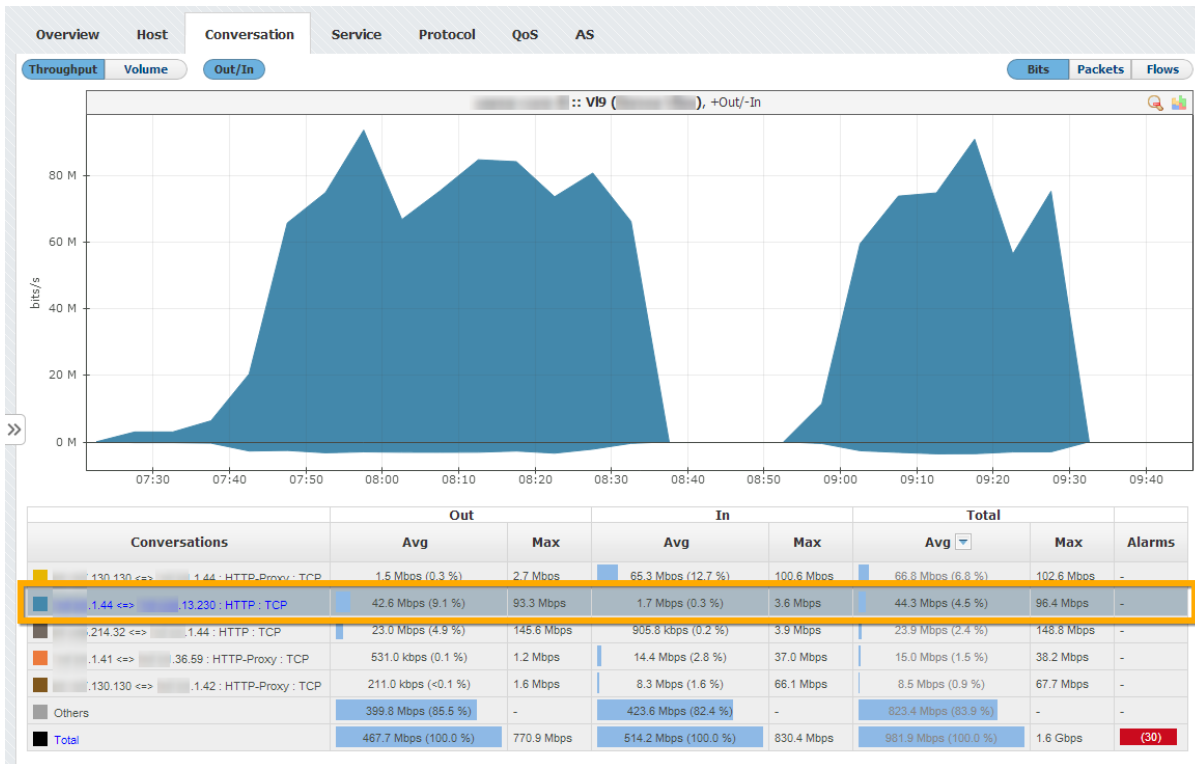
Top Talker Isolation

You can isolate contribution of any top talker by clicking on the top talker name in the table. This will reload the chart to show the contribution of the selected top talker only.



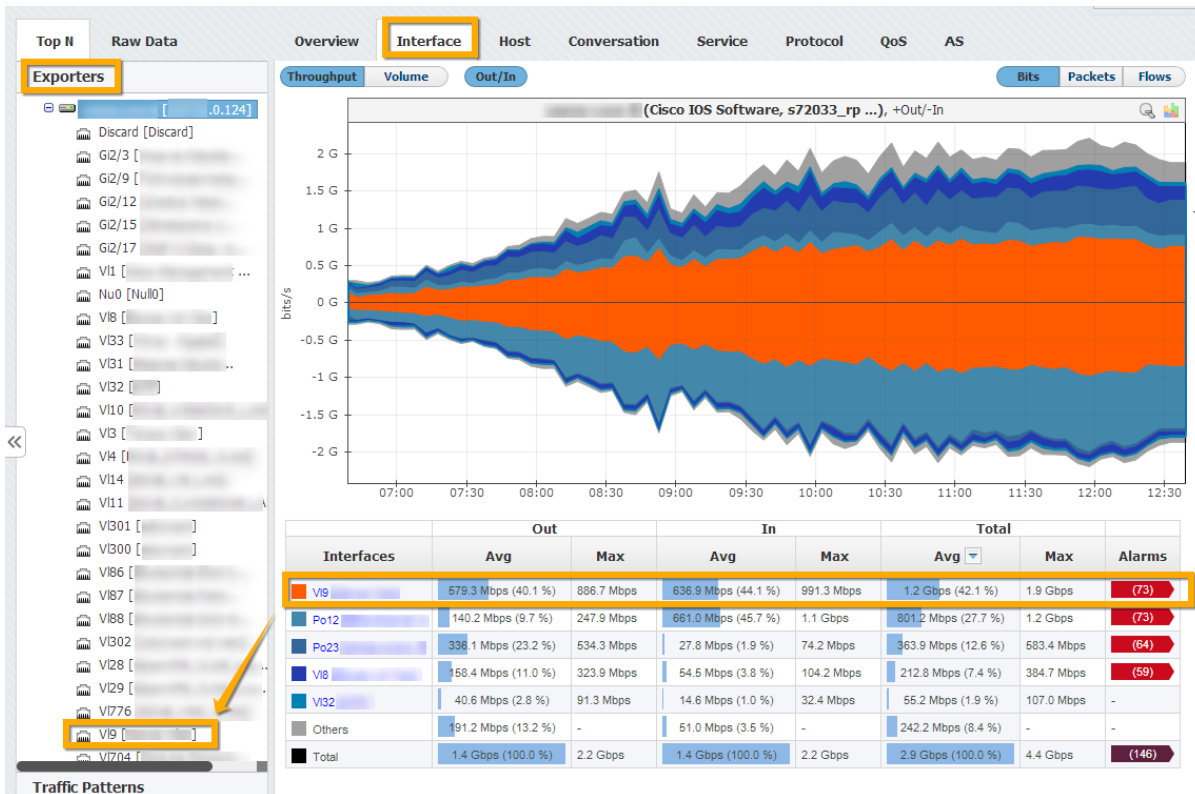
In the example above you can see top conversations. If you click on the second conversation A.B.1.44 => C.D.13.230 : HTTP : TCP, chart will reload to show the selected conversation traffic only (screenshot below).

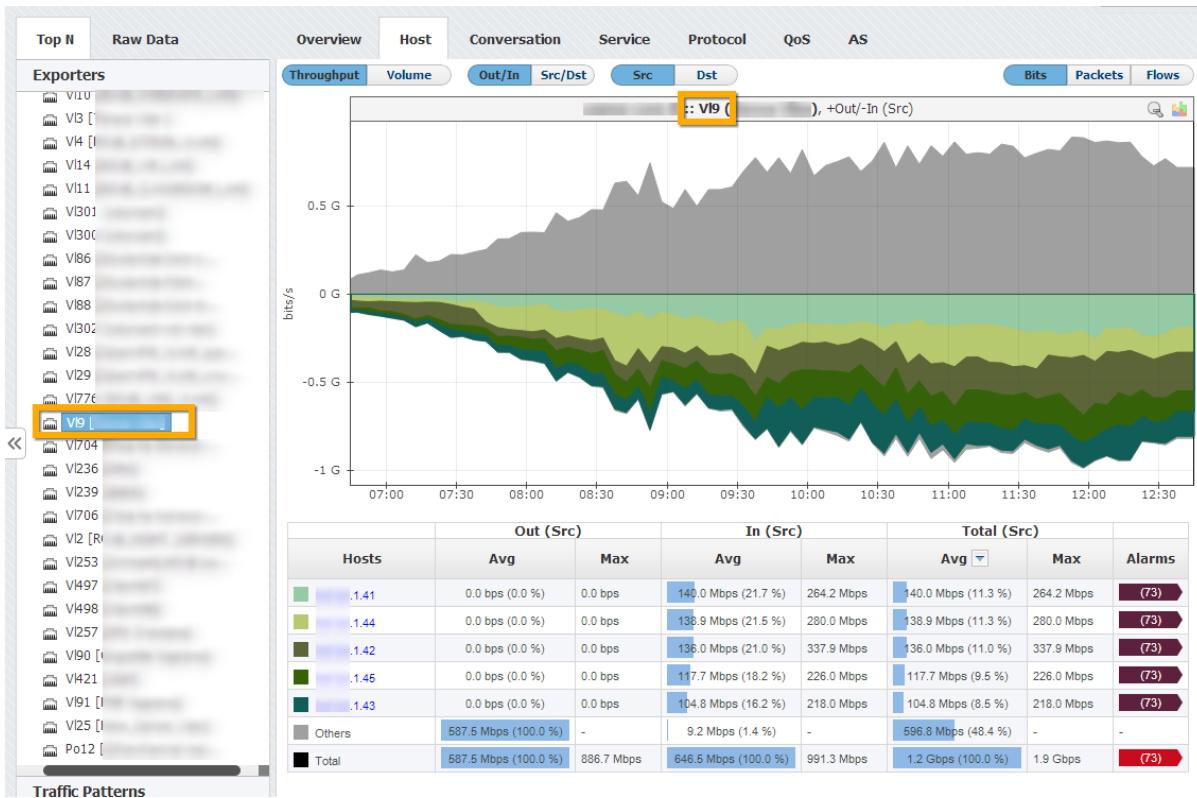
To cancel the top talker isolation, click on the top talker name again.



Top Talker Drill-Down

If a top talker is an exporter, interface, Subnet or Subnet Set, clicking on its name will result in the jump to that top talker in the Node Tree rather than the top talker isolation. The jump occurs because more detailed traffic for that top talker is available by jumping to its node than by simply isolating it on the chart.

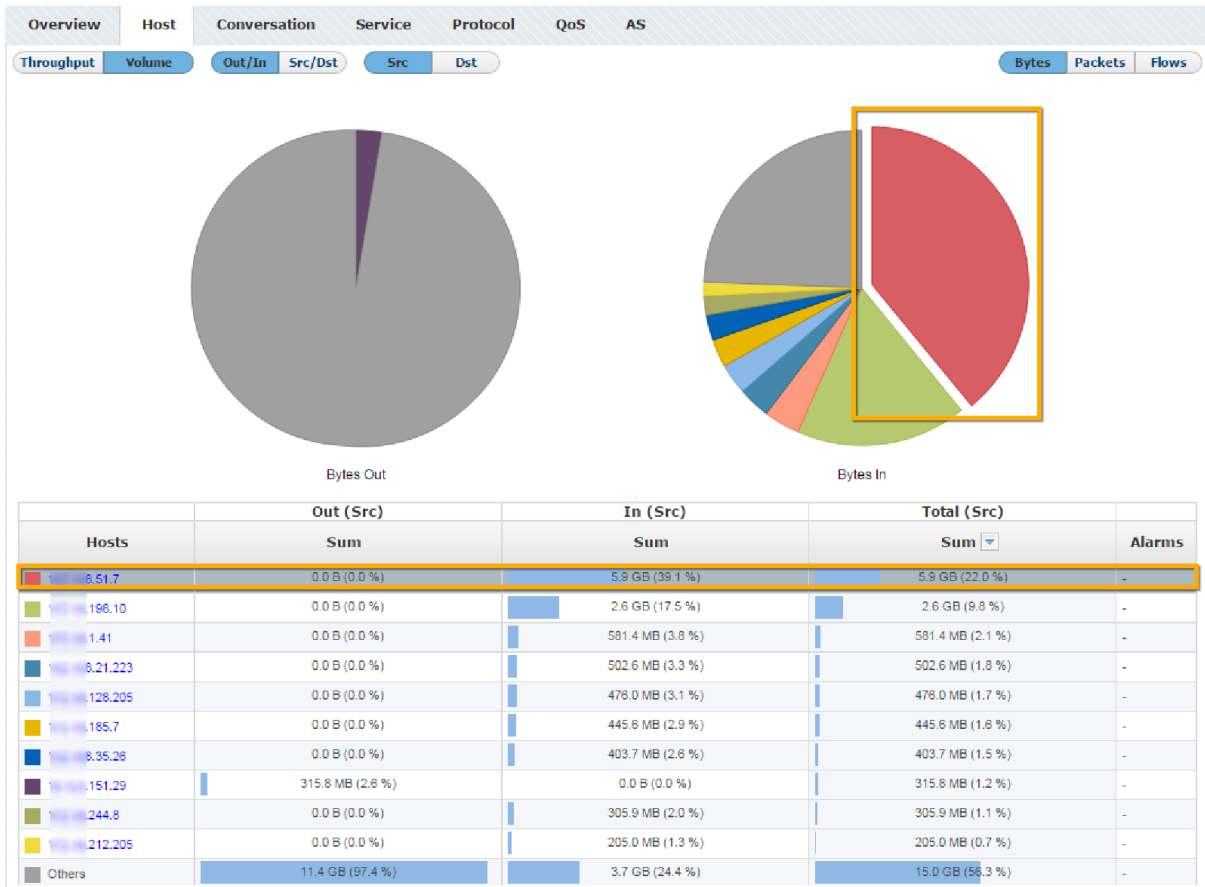




In the example above (first screenshot) you can see top interfaces of an exporter. If you click on the first interface VI9, you will jump to that interface to view its traffic in more details (second screenshot above).

Top Talker Highlight

To highlight a top talker on the chart or table, simply click on it in the chart or on its table cell in the table. Chart field and table row will become highlighted:



This can be very useful if colors on the chart are similar.

Traffic Distributions (Top Talkers)

Traffic can be viewed by several types of nodes: (1) Exporters and their Interfaces, (2) Traffic Patterns and their Subnets, (3) Subnet Sets and their Subnets and (4) End Users. For each of these nodes there are several traffic distributions that will show top talkers:

- [Distribution by Interfaces](#)
- [Distribution by Hosts](#)
- [Distribution by Conversations](#)
- [Distribution by Services](#)
- [Distribution by Protocols](#)
- [Distribution by QoS](#)
- [Distribution by AS](#)

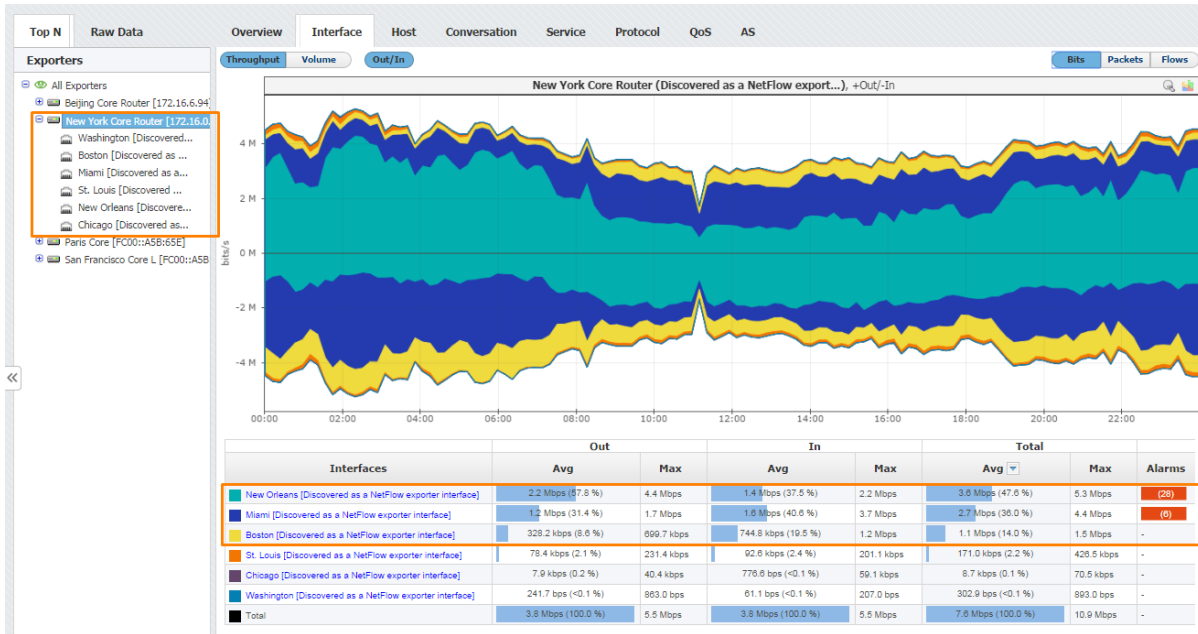
Distribution by Interfaces

Distribution of traffic by interfaces is available for Exporter node only. It shows how network traffic that passed through the selected exporter is distributed to its interfaces and which interfaces are top bandwidth consumers. This is useful if you want to look into how much exporter traffic has passed through specific interface (in total, In and Out directions).

To view exporter traffic distribution by interface:

1. Select an exporter from Navigation Tree in the Menu Panel
2. Select **Interface** tab in Tab Panel

The Menu Panel Navigation Tree presents interfaces belonging to the selected exporter. Main Panel shows throughput or volume chart and table statistics for bits, packets or flows for the selected Time Window. Note that top talkers for bits, packets and flows can differ (e.g. a top talker by flows may not be a top talker by bits).



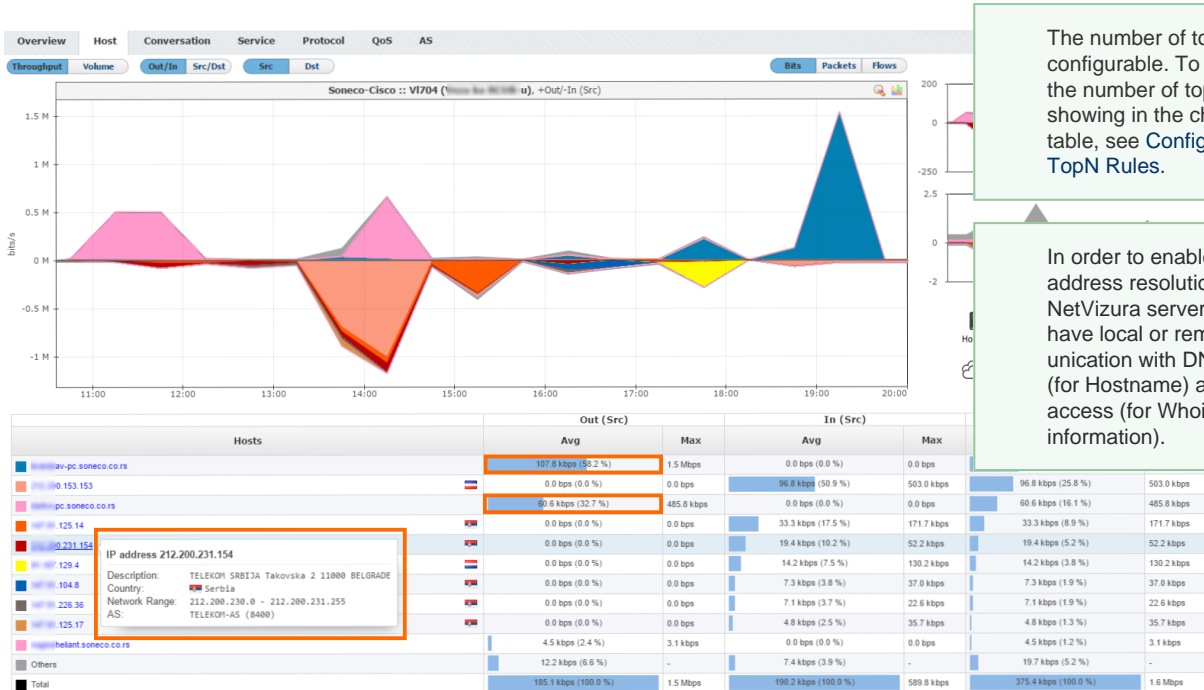
Screenshot above gives an example of exporter traffic distribution by interface for the exporter named New York Core router. From six interfaces of the New York Core router, the top talkers by bits are: New Orleans, Miami and Boston interfaces. You can also see that more than 90% of all traffic passing through the New York Core router passes through these three interfaces.

Distribution by Hosts

Distribution by hosts shows the contribution of top hosts (individual IP addresses) to the specified traffic. It presents the traffic activity for both internal and external IP addresses.

To view traffic distribution by hosts:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node from the Node Tree
3. Choose **Host** from the Tab panel



The number of top hosts is configurable. To change the number of top hosts showing in the chart and table, see [Configuring TopN Rules](#).

In order to enable IP address resolution, your NetVizura server should have local or remote communication with DNS server (for Hostname) and Internet access (for Whois information).

The screenshot above indicates that over 90% of outgoing traffic came from first and third host in the table.

Besides that, if you move your mouse over some host, you can see Whois information that significantly saves time, improves readability of the statistics and increases overall contextual awareness.

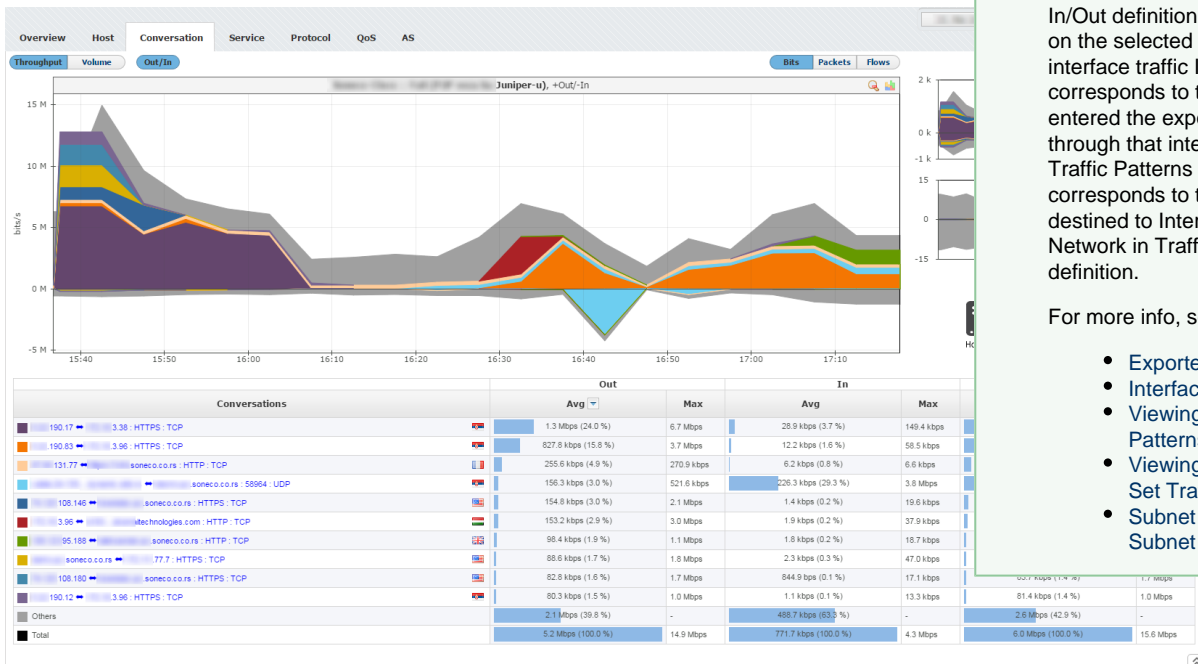
- Host is in its essence an IP address. Host can be employee computer and server. One employee can use multiple IP addresses, but also more employees can use the same IP address.
- You can expect top talkers to be proxy servers within your company network, since they provide the access to the internet.
- Also, since the number of hosts on the company level can be quite big, you can expect a considerable amount of traffic grouped as "others" entry because most of computers in your network will have very small amount of traffic in comparison to proxy servers.

Distribution by Conversations

Distribution by conversation shows who is talking with whom (end to end), i.e. which conversation is consuming most of the bandwidth, information valuable for further network optimization.

To see top conversations:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node (Exporter, Interface, Traffic Pattern, Subnet Set, Subnet or End User) from the Node Tree
3. Choose **Conversation** from the Tab panel

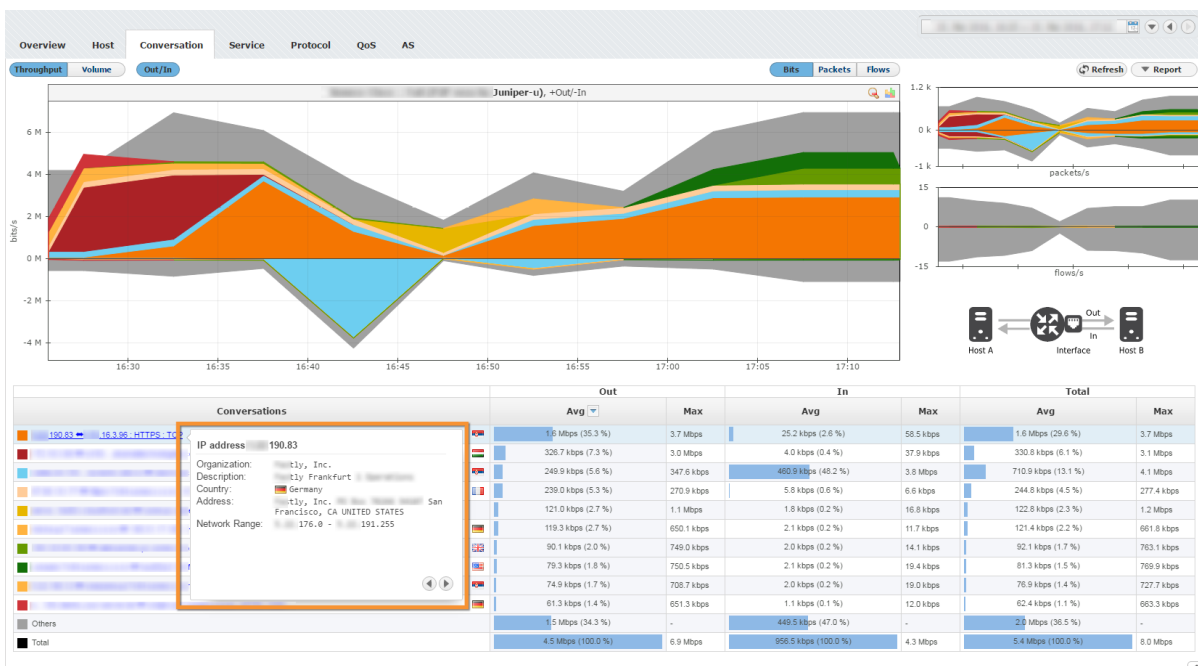


In/Out definition depends on the selected node. For interface traffic In traffic corresponds to traffic that entered through that interface. For Traffic Patterns In traffic corresponds to the traffic destined to Internal Network in Traffic Pattern definition.

For more info, see:

- Exporter Traffic
- Interface Traffic
- Viewing Traffic Patterns
- Viewing Subnet Set Traffic
- Subnet Traffic in Subnet Sets

The screenshot above indicates that top conversation is between X.X.190.17 and X.X.3.38, using HTTPS service and TCP protocol. It is also notable that the conversation consumed Max 6.7 Mbps of Out traffic and 149.4 kbps of In traffic.



For each conversation participant, additional DNS and WHOIS lookup are performed. IP is presented as Hostname, whereas WHOIS description is shown in a tooltip when specific conversation is hovered. Tooltip contains information about organization name and address, network range, additional description and more, depending on data availability. In screenshot above, you can see that the first address relates to organization located in Germany, you can also see network range and name of the organization. By clicking on the arrow keys in the bottom left corner of the tooltip you can switch to info for the other address in this conversation.

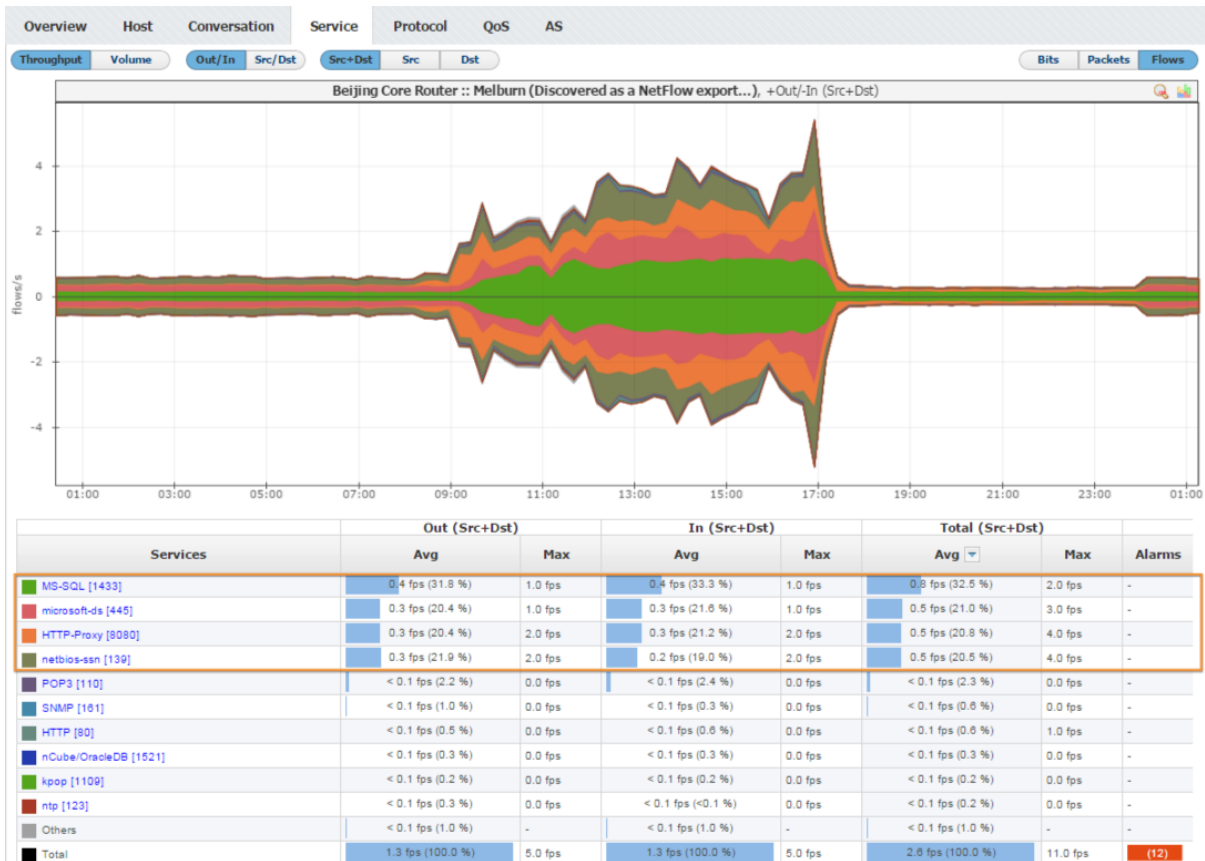
- Conversation consists of two hosts/IP addresses, service and protocol. Traffic between two hosts is treated as one conversation only if same service and protocol are used.
- Lower IP address is placed first, higher is second - the order of IP addresses does not depend on whether host is Source/Destination or in Internal/External Network.
- Service is not the same as port - one service can use more different ports. In this case, traffic between two hosts using any port associated to a same service is treated as one conversation.

Distribution by Services

Distribution by services shows each service contribution to the specified traffic. It presents which services are mostly used, when they were used, and if there is any use of forbidden services (such as BitTorrent).

To view traffic distribution by services:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node from the Node Tree
3. Choose **Service** from the Tab panel



The screenshot above indicates that on Melburn interface belonging to Beijing Core Router top services consumed are MS-SQL, microsoft-ds, HTTP-Proxy and netbios-ssn.

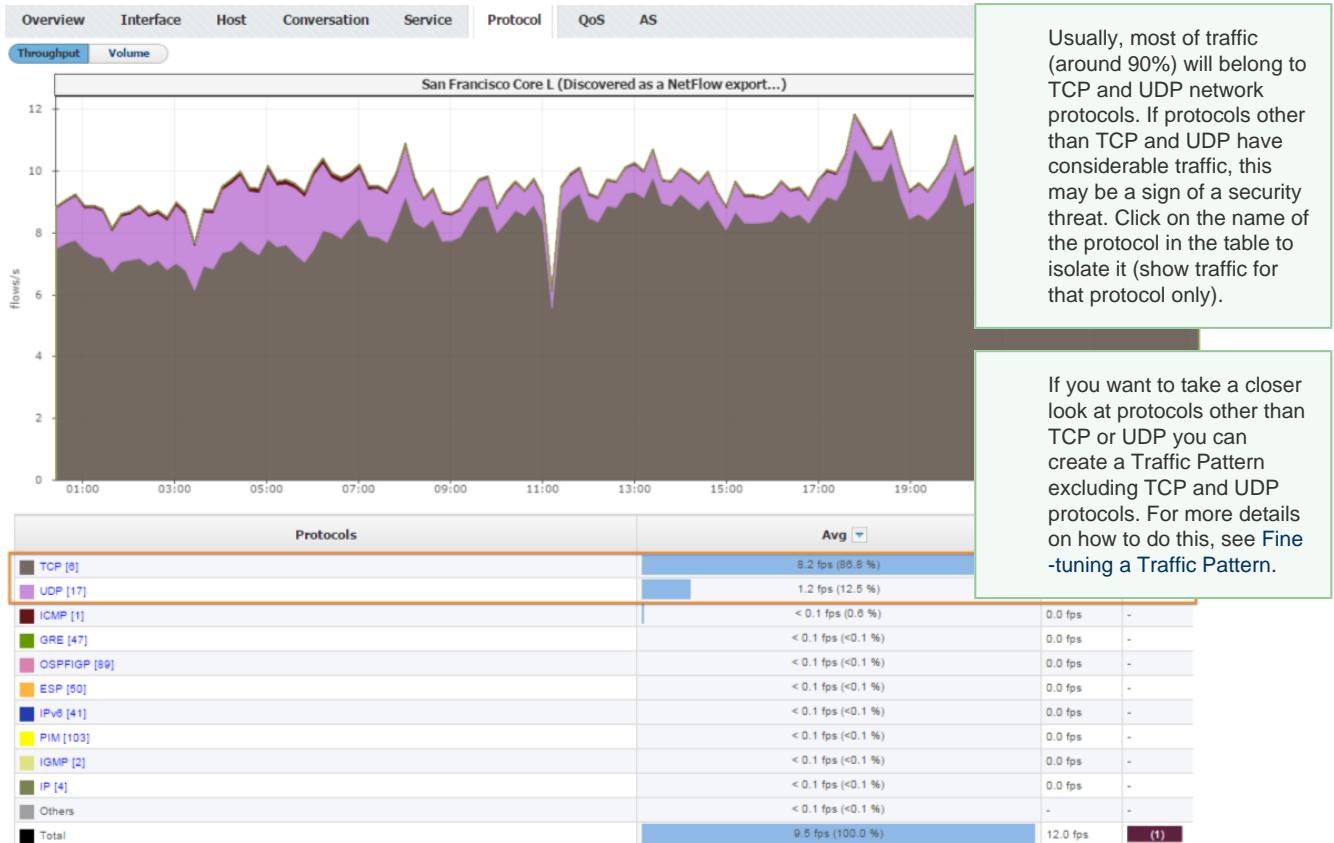
- Services are applications identified by the TCP/UDP ports they use. To display the name of a service instead of its TCP/UDP port number, it is necessary to previously map the TCP/UDP ports with service's names. See more at [Configuring Service](#).
- In some cases, VPN traffic can be forwarded through TCP port 443 thus service's traffic (SSH, HTTP, etc.) will be masked as HTTPS.

Distribution by Protocols

Distribution by protocols shows contribution of each protocol to the specific traffic.

To view traffic distribution by protocol:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node from the Node Tree
3. Choose **Protocol** from the Tab panel



Usually, most of traffic (around 90%) will belong to TCP and UDP network protocols. If protocols other than TCP and UDP have considerable traffic, this may be a sign of a security threat. Click on the name of the protocol in the table to isolate it (show traffic for that protocol only).

If you want to take a closer look at protocols other than TCP or UDP you can create a Traffic Pattern excluding TCP and UDP protocols. For more details on how to do this, see [Fine-tuning a Traffic Pattern](#).

The screenshot above indicates that on the San Francisco exporter TCP and UDP are the main protocols. Other protocols with minor traffic are also presented.

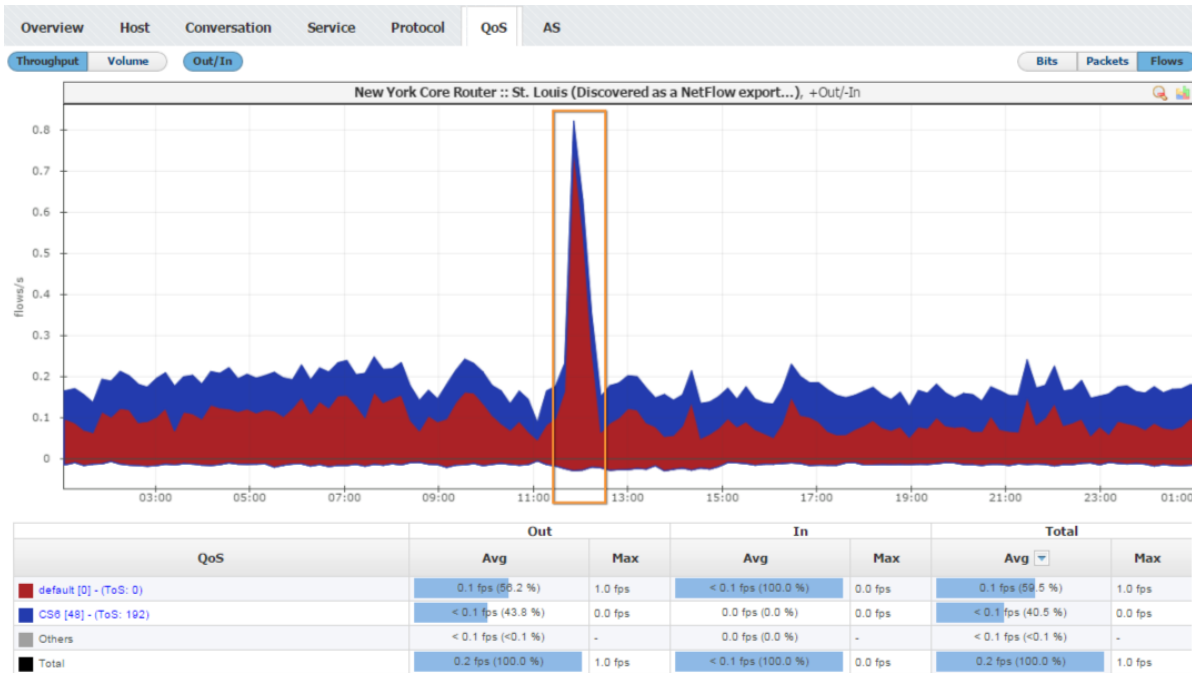
- NetVizura gives the possibility of viewing the traffic which is transferred over IP protocols (such as TCP, UDP, ICMP, etc.). All protocols are monitored and analyzed over a standardized protocol number used in IP packets and received from netflows.
- In order to perform the network traffic analysis in a way that best suits your needs, you might need to define some protocols not included in NetVizura. To learn how to define new protocols, go to [Configuring Protocol](#)

Distribution by QoS

Distribution by QoS shows specific traffic in the terms of service quality. This is interesting in particular to companies that provide a QoS based service or use such services themselves.

To view traffic distribution by QoS:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node from the Node Tree
3. Choose **QoS** from the Tab panel



The screenshot above indicates two main QoS used on the New York's router's St. Louis interface - Default and CS6. It is also noted that at 12h when major increase of Default traffic occurred, CS6 traffic simultaneously experienced a significant drop.

- Quality of Service is used for prioritization of critical applications and/or network users (transferring data across the network is prioritized). You can think of these demands as tolerance a certain application or protocol has towards the amount of data loss (packet dropping), delay, jitter... Eg. providing low-latency voice or streaming media, while providing simple best-effort for web traffic or file transfers.
- QoS was initially implemented via ToS and Precedence (IP Prec) 3-bit field, and now via Differentiated Services Code Point (DSCP) 6-bit field and Explicit Congestion Notification (ECN) 2-bit field. Read more about [Configuring DSCP](#).

Distribution by AS

NetFlow Analyzer can show the traffic between two autonomous systems. This can be done by obtaining the information about Src AS and Dst AS from the netflow data. In order to make this possible, the network device that is exporting netflow data (Exporter) must have a full BGP table. This is because the network communication between autonomous systems is done via BGP network protocol, and, therefore, information about Src and Dst AS are known through BGP.

Distribution by AS shows specific traffic by autonomous systems. It allows comparison of the AS traffic volume, watching trends and level of AS traffic in use (for instance, during which hours is the traffic towards Facebook at its highest), monitoring if employees generate forbidden traffic (Google, Facebook, YouTube, etc.).

To view traffic distribution by AS:

1. Choose a node type (Exporters, Traffic Patterns, Subnet Sets or Favorites) from the accordion in the Menu Panel
2. Select desired node from the Node Tree
3. Choose **AS** from the Tab panel



- Autonomous system (AS) is a network or group of networks a under unique administrative control. Every AS has its autonomous system number (ASN), which is globally unique. This makes an ASN an AS ID.
- To learn more on how to configure Autonomous systems, see [Configuring AS](#).

Exporters and Interfaces Traffic

In order to view Exporters and Interface Traffic, you first need to configure your network devices to send netflow data to NetVizura. After that, exporters and its interfaces will automatically appear in the node tree as they start making traffic. Read more at [Configuring Network Devices for NetFlow Export](#).

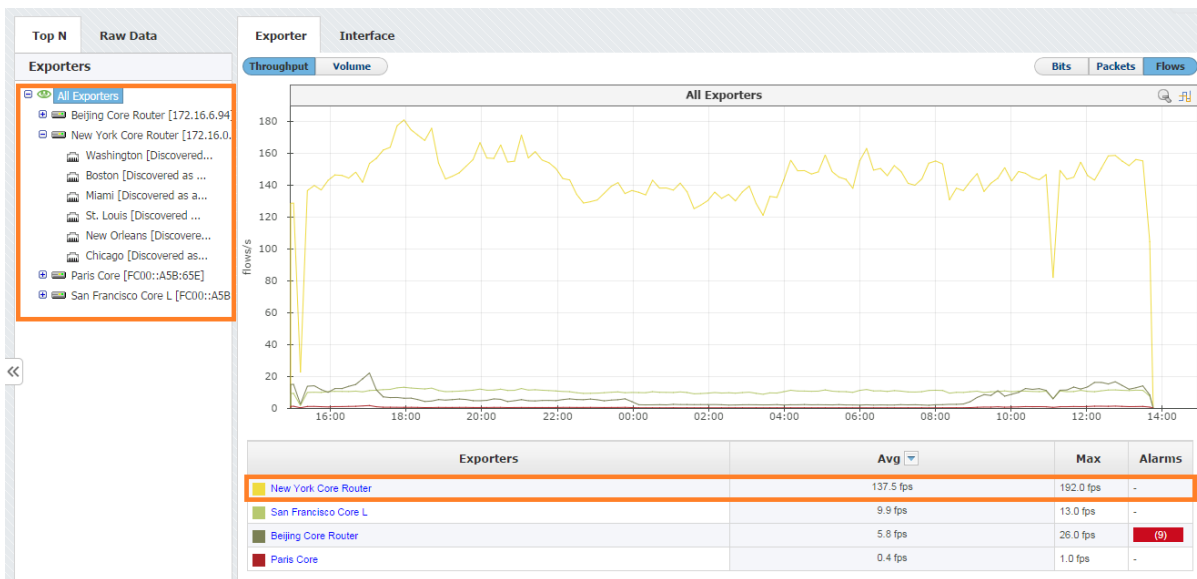
This chapter covers viewing traffic for all exporters, single exporter and single interface; and explains how exporter and interface name discovery works.

- [All Exporters Traffic](#)
- [Exporter Traffic](#)
- [Interface Traffic](#)
- [Working with Exporters and Interfaces](#)

All Exporters Traffic

All Exporters view shows top exporters and interfaces in the whole network.

To select this view, go to **TopN > Exporters** option and select **All Exporters** node.



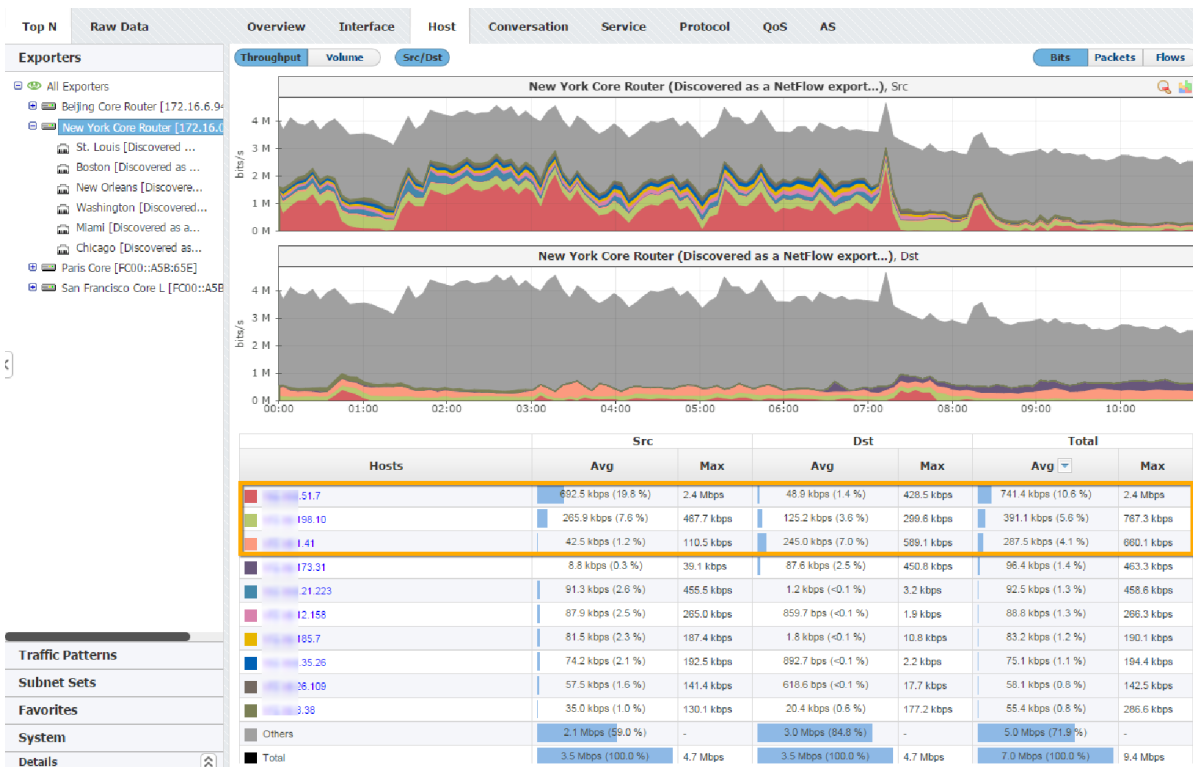
The Navigation Tree in the Menu Panel shows exporters with their belonging interfaces, and Main Panel shows top exporters or interfaces (throughput or volume, in bits, packets or flows). Exporter tab will show which exporters have the most traffic passing through them, while Interface tab will show you which interfaces have the most traffic passing through them in your network.

Figure above shows an example of top exporters traffic. You can see that out of four exporters (Beijing, New York, Paris and San Francisco Core Routers) exporter New York Core router has by far the most traffic in flows passing through it.

Exporter Traffic

Exporter view shows traffic of the specific exporter in your network.

To see traffic for an exporter, go to **TopN > Exporter** option and select the desired exporter node.



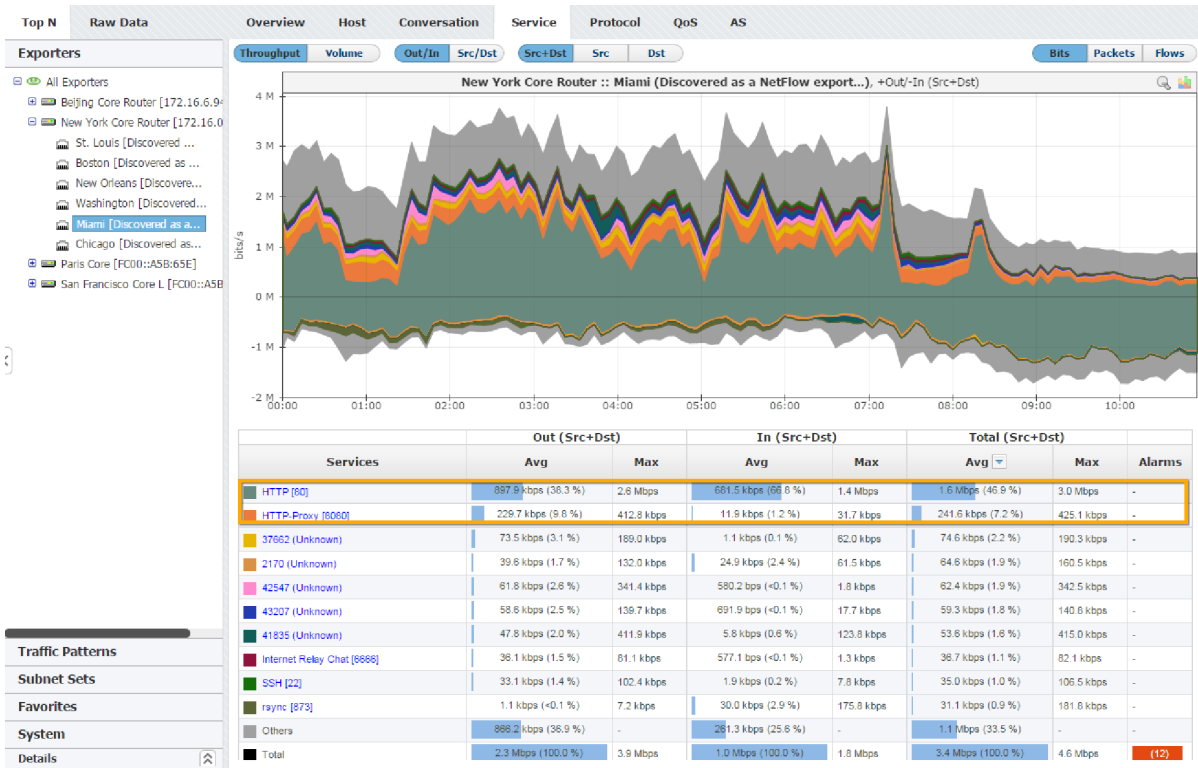
The Navigation Tree in the Menu Panel shows interfaces of the selected exporter, while Main Panel shows traffic for for the selected exporter (throughput or volume, in bits, packets or flows). Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Hosts tab will give you top hosts for the selected exporter).

Figure above shows traffic of the New York Core Router by hosts. You can see that top three hosts that generated traffic via that exporter are X.X.51.7, X.X.198.10 and X.X.1.41, where X.X.51.7 is also the top Source while X.X.1.41 is the top Destination host.

Interface Traffic

Interface view shows traffic of the specific interface in your network.

To see traffic for an interface, go to **TopN > Exporter** option, select the desired exporter and then the desired interface node.



The Navigation Tree in the Menu Panel shows interfaces of the selected exporter, while Main Panel shows traffic for for the selected interface (throughput or volume, in bits, packets or flows). Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Service tab will give you top services for the selected interface).

Figure above shows service traffic for the interface Miami. You can see that HTTP and HTTP Proxy services were mainly used via that interface.

Working with Exporters and Interfaces

Exporters and Interfaces Discovery

In order to complete exporter names discovery, it is required to have basic network administration knowledge and access to network devices.

Also, you need administrator privileges for setting up SNMP policies in NetVizura Control Panel.

On this page:

- Exporters and Interfaces Discovery
- Exporters Removal

First time when NetFlow Analyzer receives and processes netflow packets from a network device, it is automatically added to Exporters tree. Device initially appears as IP address (configured for NetFlow export), and its interfaces appear with dedicated SNMP indexes.

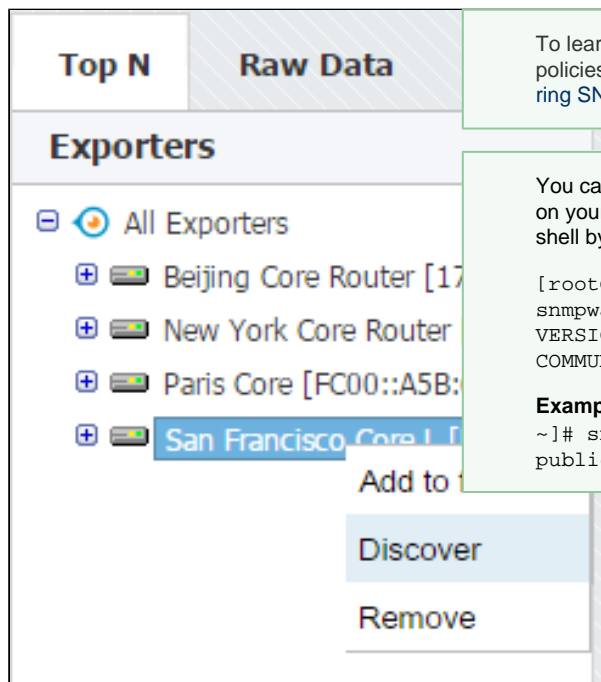
However, to further discover exporter and interface names you will need to set up SNMP policies:

1. Enable and set SNMP on your exporters
2. Make sure that NetVizura can send SNMP requests to the exporters
3. Add SNMP policies to NetVizura (**Settings > Control Panel > SNMP Policies**).

After that, name discovering process is very easy:

1. Go to **Top N > Exporters** tree
2. Right click on exporter or interface node
3. Select **Discover**

Exporter or interface name will be set to sysName, while description (in tooltip) will be set to sysDescr value received via SNMP request.



To learn how to configure SNMP policies in NetVizura, see [Configuring SNMP Policies](#).

You can test SNMP configuration on your devices from NetVizura shell by using command:

```
[root@NetVizura ~]# snmpwalk -v <SNMP VERSION> -c <SNMP COMMUNITY> <IP ADDRESS>
```

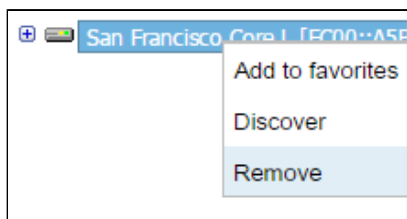
Example: [root@NetVizura ~]# snmpwalk -v 2c -c public 192.168.2.101

After discovery, additional information about the selected exporter or interface is available in the Details panel (Read more in chapter [Reading NetFlow Details](#)).

Exporters Removal

You need to have administrator privileges in order to confirm exporter removal.

During the course of work, you might have old exporters that no longer send NetFlow data but are still available in the tree. For this reason, you might want to clean them up. To remove an exporter:



1. Go to **Top N > Exporters** tree
2. Right click on exporter node
3. Select **Remove**
4. Confirm your administrator password
5. Click **OK**

If exporter continues sending NetFlow to NetVizura from a new interface, it will reappear in the tree so make sure to stop NetFlow export on the exporter before its removal.

Exporter will no longer be shown in the Exporter tree.

Basic Traffic Patterns

In order to view Traffic Patterns, you first need to setup Traffic Patterns of your interest. After that, they will automatically appear in the node tree. Check out [Configuring Traffic Patterns](#).

This chapter introduces the concept of Traffic Patterns, viewing traffic for a single Traffic Pattern, viewing statistics for a single Subnet in Traffic Pattern tree, and explains what are the differences between Exporter Traffic and Traffic Pattern.

- [Understanding Traffic Patterns](#)
- [Viewing Traffic Patterns](#)
- [Subnet Traffic in Traffic Patterns](#)
- [Exporter Traffic vs Traffic Pattern](#)
- [Basic Traffic Pattern Examples](#)

Understanding Traffic Patterns

What is a Traffic Pattern? It is a logical structure you create in order to analyze the network traffic you are interested in. Traffic Patterns are completely independent of the physical infrastructure. This enables you to focus on logical properties of your traffic instead focusing on physical links, network devices and their interfaces.

Traffic Pattern is a part of the totally collected network traffic. It represents the traffic between two networks, namely:

- **Internal Network** - usually represents the whole or part of your internal network (company network) from which the NetFlow data are exported and collected
- **External Network** - can be an arbitrary network – other part of your network (such as a network in another city, database center etc), Internet provider's network, or the whole Internet.

The traffic between the Internal Network and External Network is always bidirectional. This means that the Traffic Pattern will match the traffic going from the Internal Network to External Network, and from the External Network to Internal Network. The statistics are generated for the traffic between Internal and External Networks separately in two opposite directions, referenced from the Internal Network perspective:

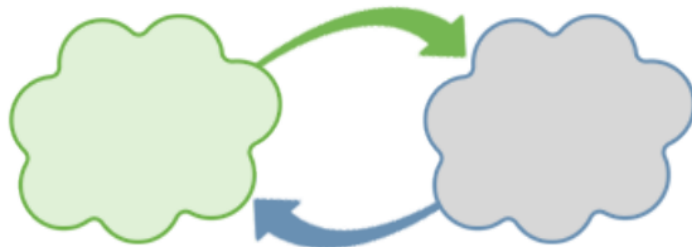
- **Outgoing (Out)** traffic – going out of the Internal network or, in other words, traffic sourced from the Internal Network and destined to the External Network.
- **Incoming (In)** traffic – coming into the Internal network or, in other words, traffic sourced from the External Network and destined to the Internal Network.

There are three types of Traffic depending on the direction of traffic in regards to you Internal network:

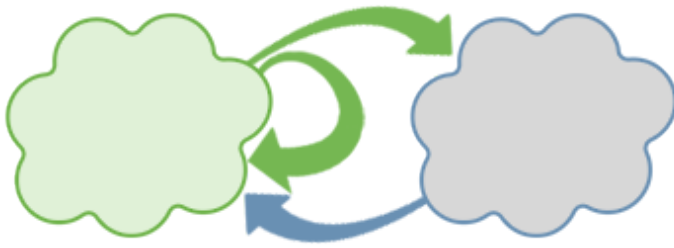
- **Self Traffic** - within one network. In other words, source and destination of the traffic are both within a single network. Naturally, the network in question has to be within your internal network. In this case, your internal network (or its part) is both Internal Network and External Network.. In the case of Self Traffic, outbound traffic volume is the same as the inbound traffic volume.



- **Normal Traffic** - between two different networks (network IP ranges do not overlap). Usually, one of these network is your company' network (or its part) and some external network such as the whole Internet or some specific network like Facebook.



- **Custom Traffic** - a combination of Self-Traffic and Normal Traffic. For example, if you want to track the entire network communication of your PR department. This means tracking (1) to which part of your company network did they communicate with and (2) to which networks outside of your company network did they communicate with. The Internal Network is your PR department and the External Network is all networks except PR department network.

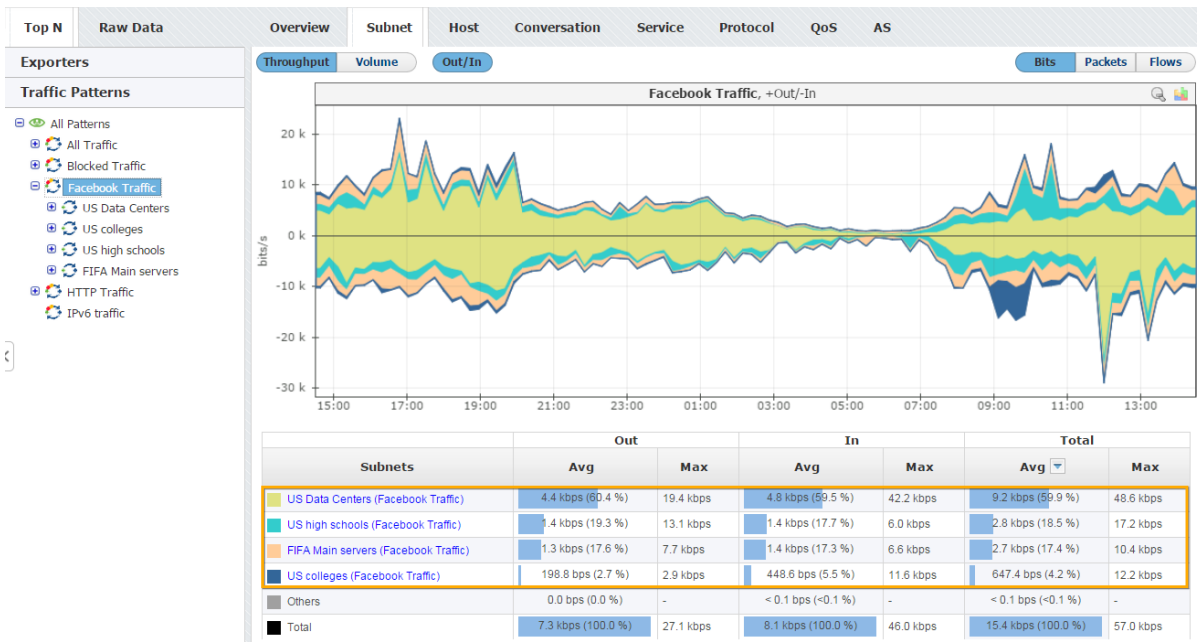


Traffic Pattern's Internal and External networks are defined by IP address ranges and other parameters collected by the NetFlow and similar protocols can be used as filters to further specify Traffic Patterns. Learn more about [Configuring Traffic Patterns](#).

Viewing Traffic Patterns

Traffic Pattern view presents a specific, customly configured traffic.

To show a Traffic Pattern, go to **TopN > Traffic Patterns** option and select the node of your interest.



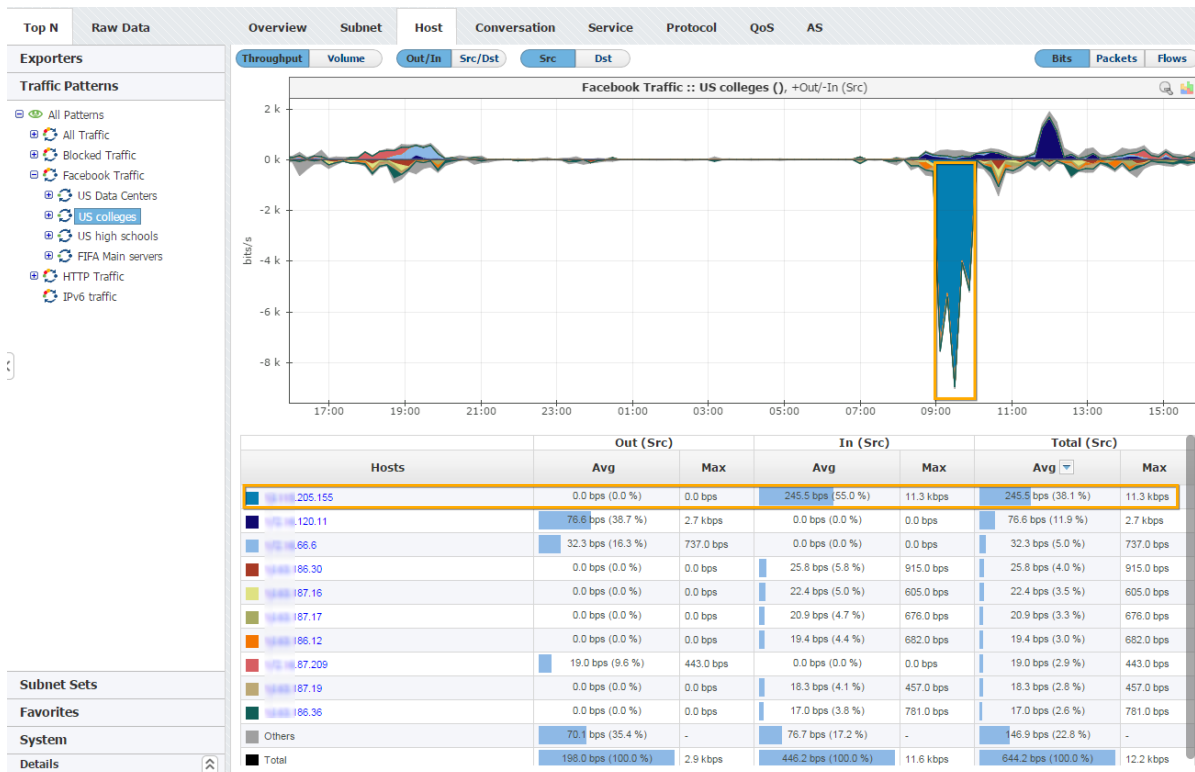
The Navigation Tree in the Menu Panel shows Traffic Patterns and their Subnets, while Main Panel shows traffic data for for the selected Traffic Pattern (throughput or volume, in bits, packets or flows) or its subnet. Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Subnets tab will give you top Subnets for the selected Traffic Pattern).

Figure above shows Facebook Traffic. You can see that US Data Centers subnet takes the most of Facebook Traffic, followed by US high schools and FIFA Main servers, whereas US colleges subnet takes the least.

Subnet Traffic in Traffic Patterns

Subnet view shows traffic for the specific Subnet within the specific Traffic Pattern.

To see traffic for a Subnet, go to **TopN > Traffic Patterns** option, select the desired Traffic Pattern and then the desired Subnet.



The Navigation Tree in the Menu Panel shows Subnets of the selected Traffic Pattern, while Main Panel shows traffic for for the selected Subnet (throughput or volume, in bits, packets or flows). Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Host tab will give you top hosts for the selected Subnet).

Figure above shows distribution of Facebook Traffic for the US colleges by host. You can see that X.X.205.155 host was the major Facebook bandwidth consumer and that the most of the downloads (In traffic) occurred between 9 and 10 AM.

Info

1. Subnet will be listed under a Traffic Pattern only if its IP address range is a subset of the included IP address range in the Traffic Pattern Internal Network.
2. Keep in mind that subnet traffic depends on the parent Traffic Pattern. Same subnet will have different traffic in different Traffic Patterns it belongs to since the traffic matched to each Traffic Pattern is different.

Exporter Traffic vs Traffic Pattern

This article helps in understanding the differences between Exporter Traffic and Traffic Pattern and what are they used for.

	Exporter Traffic	Traffic Pattern
Setup	✔ provided by default	✔ requires custom setup
Based on	✔ physical infrastructure	✔ logical definition
Nodes	✔ exporters and interfaces	✔ Traffic Patterns, Subnet Sets and Subnets
Monitors	✔ traffic on routers, L3 switches and interfaces	✔ specific (custom defined) traffic
Analysis focus	✔ whole traffic on specific physical infrastructure	✔ specific traffic between two networks
Level of expertise	✔ fast setup and easy to understand	✔ complex setup and harder to understand

In general you will use:

- [Exporter Traffic](#) when you are interested in monitoring the bandwidth of an interface or exporter (whole traffic passing through the physical infrastructure)
- [Traffic Patterns](#) to isolate a specific type of traffic (traffic via specific ports, protocols, AS etc.): YouTube Traffic, certain service traffic, blocked traffic etc.
- [Traffic Patterns with Subnet Sets](#) to monitor whole or specific traffic per logical unit: company departments, regional company offices, member organisations, data centre traffic etc.

Basic Traffic Pattern Examples

Traffic Patterns are made to be very flexible and that means a lot of configuration parameters. The main goals of this chapter are to (1) provide you with examples of Traffic Patterns and their usage and (2) to give you an idea on how to create your own Traffic Patterns. In this article only basic Traffic Patterns, that can be created with only IP address ranges and de-duplication filters, will be explained. For advanced examples, see [Advanced Traffic Pattern Examples](#).

General steps to take:

1. Determine the traffic of interest.
2. Determine which Traffic Pattern type to use (it will help you with populating Internal and External Network address ranges).
3. Determine IP address ranges for Internal and External Networks.
4. Determine which filter (if any) you should use to filter traffic further, if needed.

Below are to most common examples of Traffic Patterns.

Internet Traffic Pattern

If you are interested in monitoring Internet traffic, first you need to prepare a specific Traffic Pattern for this purpose. Since this is practically the traffic between your network and external world where External network is negation of Internal Network) you should select Normal type which will automatically populate part of the IP address ranges. Here your company's IP address range is treated as Internal, whereas all other networks as External. In the end, you should use Exporter or Next Hop filtering to remove eventual duplicate flows, if needed.

1. Create Internet Traffic
2. Select Normal (default) as Traffic Pattern type
3. IP Address ranges:
 - a. Internal: Add your company network's IP range(s) and click Include
 - b. External: your company network's range is excluded automatically (Normal Traffic Pattern)
4. Filters:
 - a. Use Exporter or Next Hop filter to de-duplicate flows, if needed.
 - b. To read more on flow de-duplication, see [Resolving Duplicated Export](#).

Data Center Traffic Pattern

Another example of most commonly used Traffic Pattern is Data Center Traffic. This traffic occurs between all your company and your data center, you should include your company's IP address range and exclude your data center's IP range in Internal Network, and include your data center's IP range in External network (here your data center is treated as "Outside" network). Since Internal Network (company network without Data center) and External Networks (Data Center) IP ranges overlap you should use Custom type (turns off automatic IP address range population). Do not forget Exporter or Next Hop filtering to remove duplicate flows, if needed.

1. Create Data Center Traffic
2. Select Custom as Traffic Pattern type
3. IP Address ranges:
 - a. Internal: add your company network's range and click Include
 - b. Internal: add your data center's range and click Exclude
 - c. External: add your data center's range and click Include
4. Filters:
 - a. Use Exporter or Next Hop filter to de-duplicate flows, if needed.
 - b. To read more on flow de-duplication, see [Resolving Duplicated Export](#).

To continue reading about more complex examples, go to article [Advanced Traffic Pattern Examples](#).

Tip

Note that subnet nodes in a Traffic Pattern are shown only if they are included in the Internal Network in the Traffic Pattern definition.

Subnet Sets

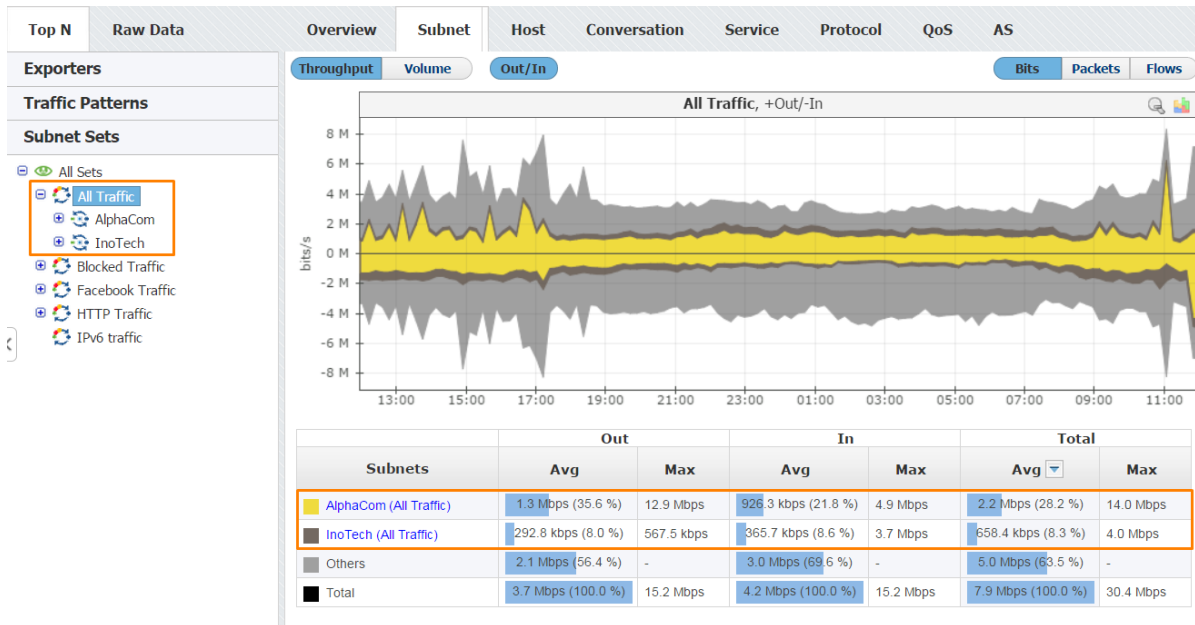
This chapter shows three types of traffic that are available in Subnet Sets Tree - Traffic Patterns, Subnet Sets and Subnets, as well as comparison between Subnet Set and Subnet Traffic.

- [Traffic Pattern in Subnet Sets](#)
- [Viewing Subnet Set Traffic](#)
- [Subnet Traffic in Subnet Sets](#)
- [Subnet Set vs Subnet Traffic](#)

Traffic Pattern in Subnet Sets

Traffic Pattern node in Subnet Sets view, in contrast to normal Traffic Pattern view, shows Subnet Set distribution instead of Subnets.

To show a Traffic Pattern for the specific Subnet Set, go to **TopN > Subnet Sets** option and select the Traffic Pattern node of your interest.



The Navigation Tree in the Menu Panel shows Traffic Patterns and their Subnet Sets, while Main Panel shows traffic data for for the selected Traffic Pattern (throughput or volume, in bits, packets or flows), its Subnet Sets or Subnets of those Subnet Sets. Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Subnets tab will give you top Subnet Sets for the selected Traffic Pattern).

Figure above shows All Traffic. You can see traffic for AlphaCom and InoTech Subnet Sets (an example of two organizations).

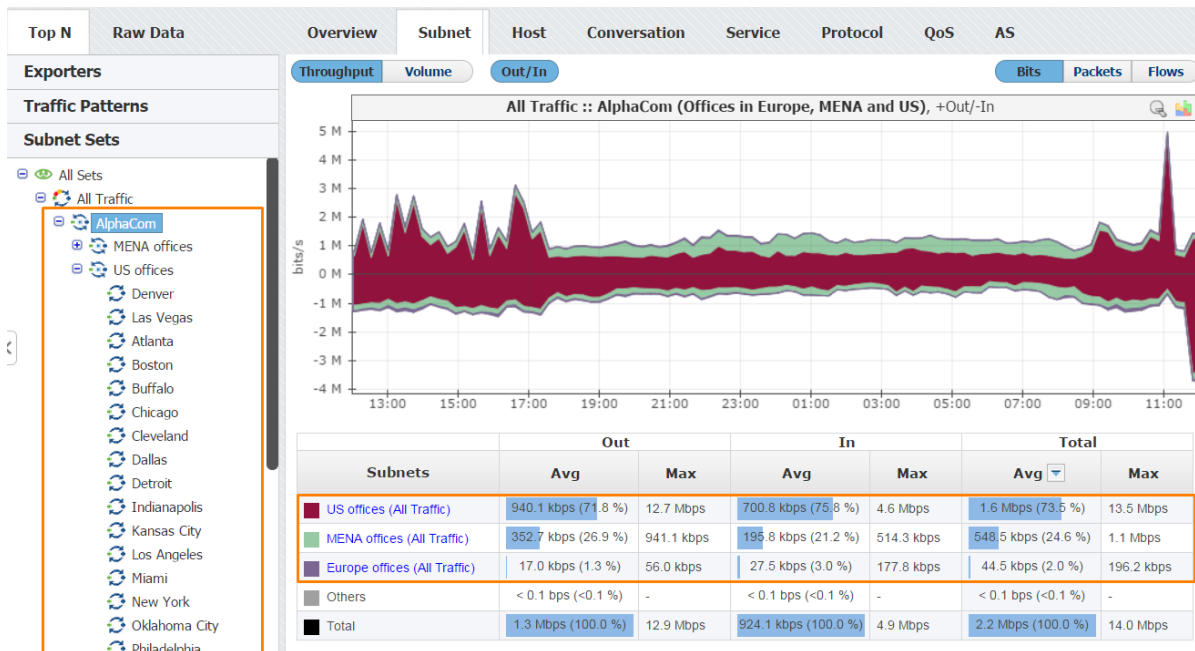
Info

Note that Subnets that do not belong to any Subnet Set will not show as child nodes of their respectful Traffic Pattern in Subnet Set view. Their contribution to traffic will be added to others category, since this view focuses on Subnet Sets instead of subnets.

Viewing Subnet Set Traffic

Subnet Set view shows traffic for the specific Subnet Set in Traffic Pattern.

To show traffic for a Subnet Set, go to **TopN > Subnet Sets** option, select the wanted Traffic Pattern and then the desired Subnet Set.



The Navigation Tree in the Menu Panel shows Subnet Sets (with their belonging Subnet Sets and Subnets), while Main Panel shows traffic data for for the selected Subnet Set (throughput or volume, in bits, packets or flows). Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Subnets tab will give you lower-level top Subnet Sets of the selected Subnet Set).

Figure above shows traffic for the AlphaCom. Traffic distributions shows traffic for the US, MENA and Europe Subnet Sets that were previously defined.

Info

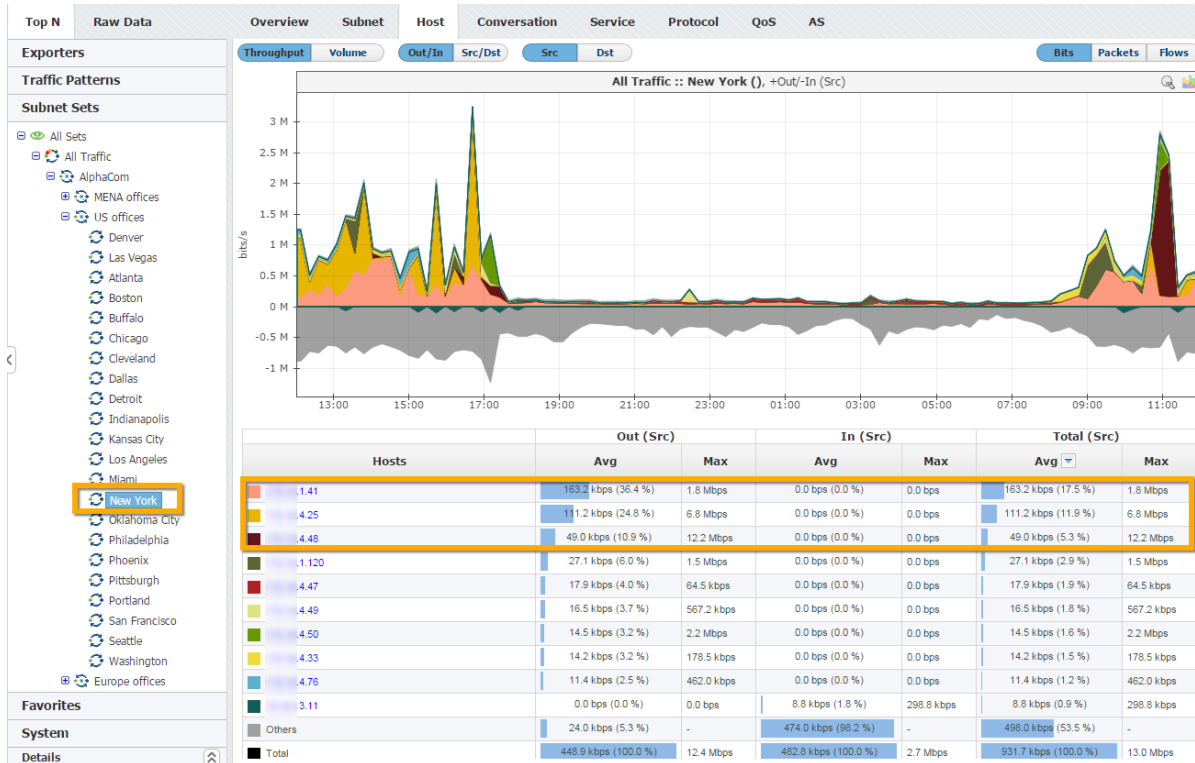
Keep in mind that Subnet Set traffic depends on the parent Traffic Pattern. Same Subnet Sets will have different traffic values in different Traffic Patterns since the traffic matched to each of them is different.

Subnet Traffic in Subnet Sets

Subnet view in Subnet Sets shows traffic for the specific Subnet within the specific Subnet Set (and its Traffic Pattern).

To see traffic for a Subnet, go to **TopN > Subnet Sets** option, select the desired Traffic Pattern, Subnet Set and then the desired Subnet.

The Navigation Tree in the Menu Panel shows selected Subnet (and its belonging parent Subnet Sets and Traffic Pattern), while Main Panel shows traffic for for the selected Subnet (throughput or volume, in bits, packets or flows). Clicking on any tab option will show traffic distribution by that category (e.g. clicking on the Host tab will give you top hosts for the selected Subnet).



Screenshot above shows New York office traffic that belongs to US offices and AlphaCom Subnet Sets and All Traffic Pattern. You can see that X.X.1.41, X.X.4.25 and X.X.4.45 hosts were the major bandwidth consumers of the New York office, i.e. that most of the traffic in the New York US office of AlphaCom involved these three hosts.

Info

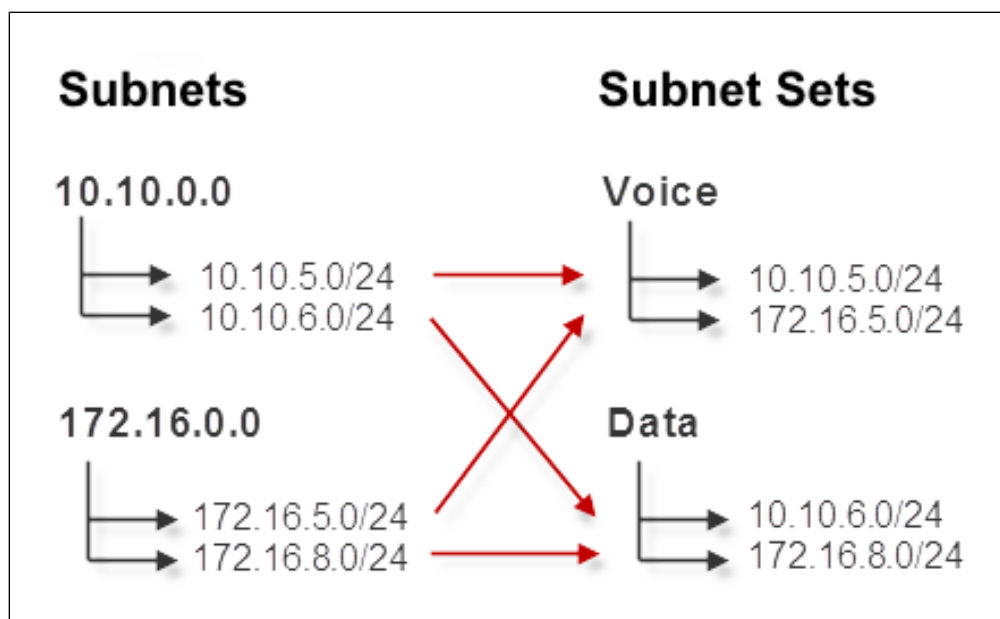
1. Subnet will be listed under a Traffic Pattern only if its IP address range is a subset of the included IP address range in the Traffic Pattern Internal Network.
2. Keep in mind that Subnet traffic depends on the parent Traffic Pattern and Subnet Set. Same Subnet will have different traffic values in different Traffic Patterns and Subnet Sets it belongs to since the traffic matched to each of them is different.

Subnet Set vs Subnet Traffic

This article explains differences between Subnet Set and Subnet traffic and how to best use them.

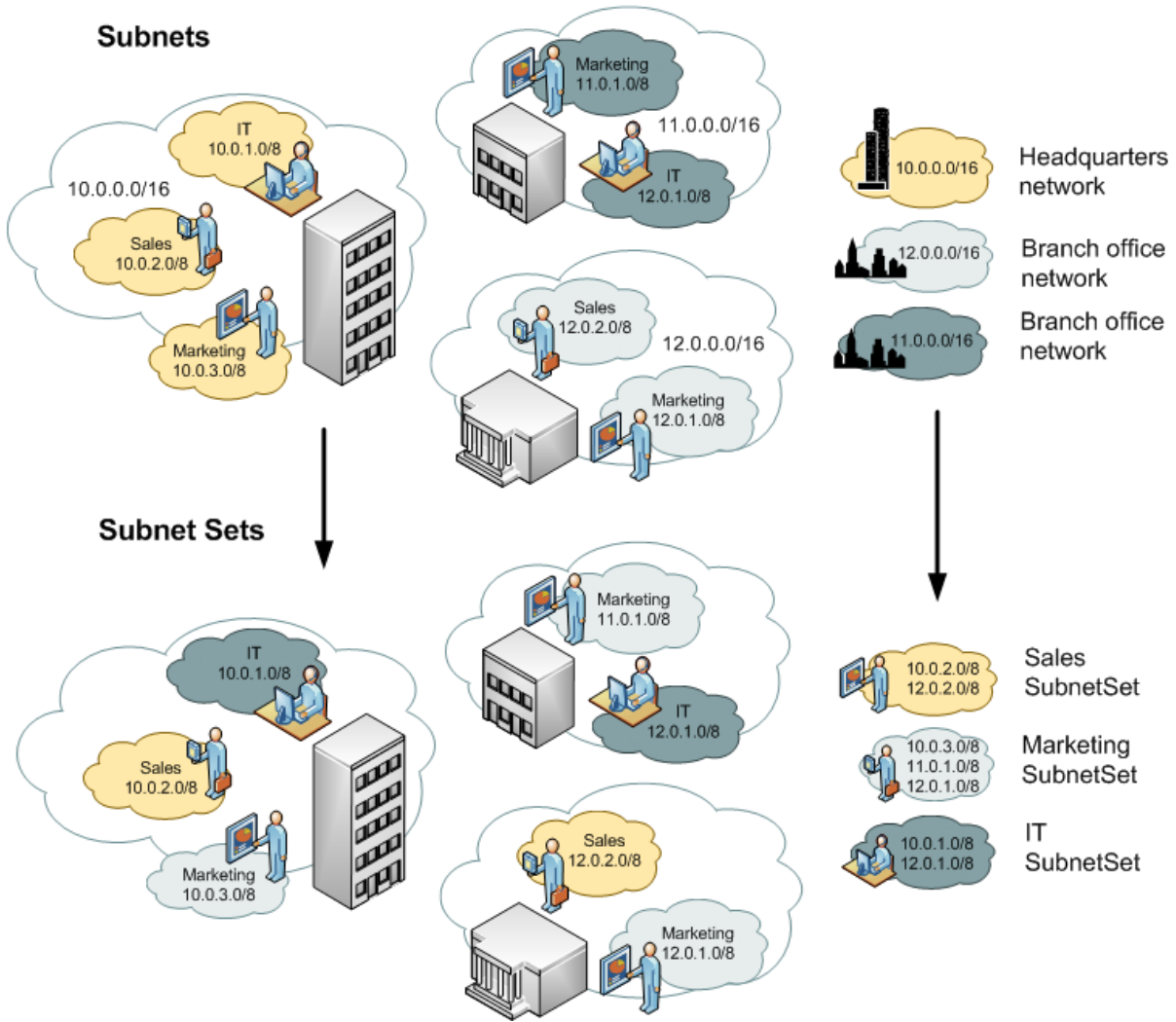
	Subnet Traffic	Subnet Set Traffic
Defined as	✓ IP address range	✓ group of Subnets or other Subnet Sets
Monitors	✓ subnet traffic	✓ organisational unit or logical group traffic
Used for	✓ hierarchical network division based on IP address	✓ combining smaller subnets into logical groups independent to IP address hierarchy
Examples	✓ 10.10.5.0/24, 10.10.6.0/24, 172.16.5.0/24 etc.	✓ Voice traffic, IT department, US offices, etc.

Let us say that you have two networks with different IP address ranges (10.10.0.0 and 172.16.0.0), each with separate data and voice segments. All these segments are separate Subnets. The Traffic Pattern and Subnets view will give you total traffic, traffic on each network, and traffic on each segment. However, Traffic Patterns and Subnets cannot give total voice or total data traffic (made by both networks combined). For that purpose, it is necessarily to create two Subnet Sets, one with both voice Subnets, and the other with both data Subnets. Subnet Set option will show these traffics.



In the other example, IT department might consist of employees working on computers in different Subnets because they are in different buildings, towns or even countries. This usually means you can not cover all of them by a single IP address range. With Subnets Sets, you simply group all individual IT subnets into IT Subnet Set and traffic for the IT department will be available.

Subnets



Managing NetFlow Favorites

Frequently monitored nodes (Exporter, Traffic Pattern, Subnet, etc.), can be added to Favorites for quick access.

This way there is no need to search and navigate every time in order to view desired traffic.

To add a favorite:

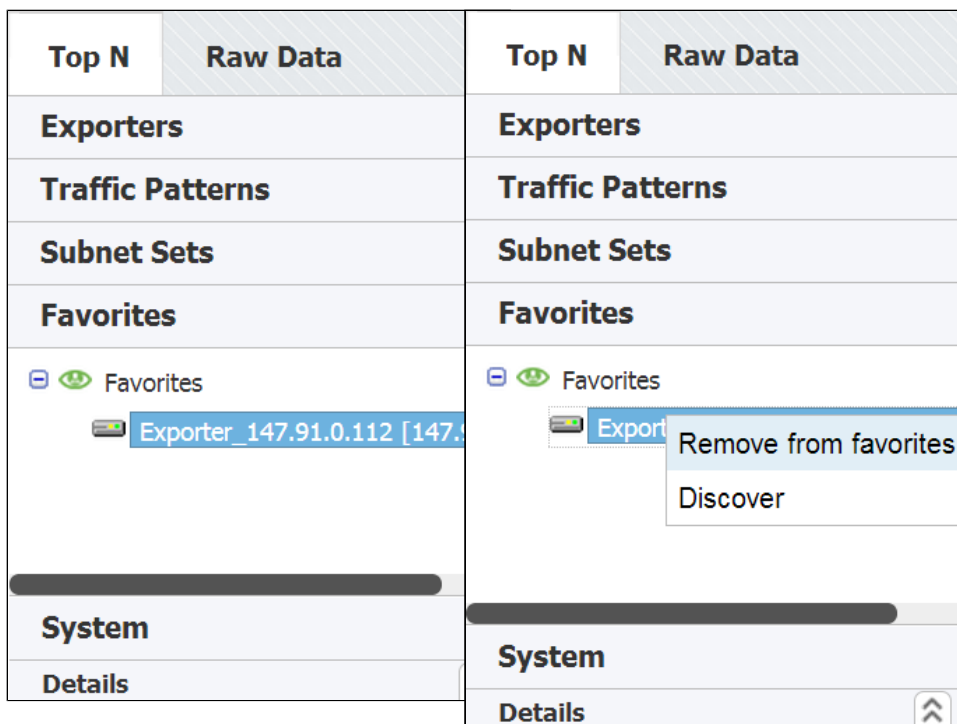
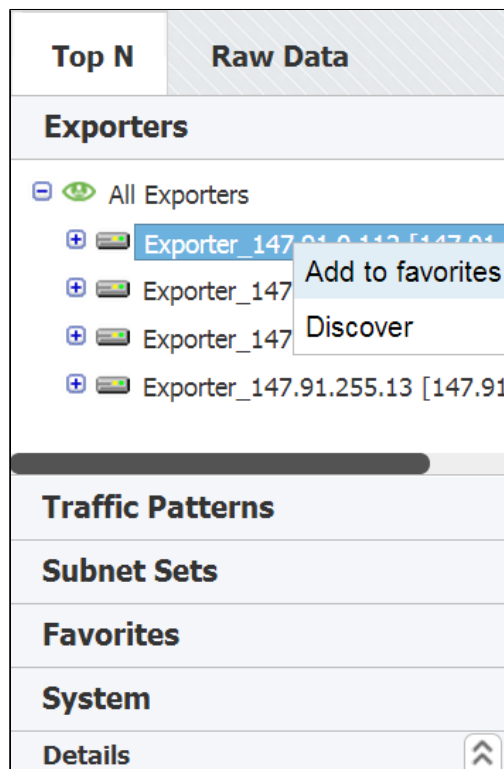
1. Right click on a desired node from Navigation Tree
2. Select **Add to favorites**

To view traffic for added favorite, simply:

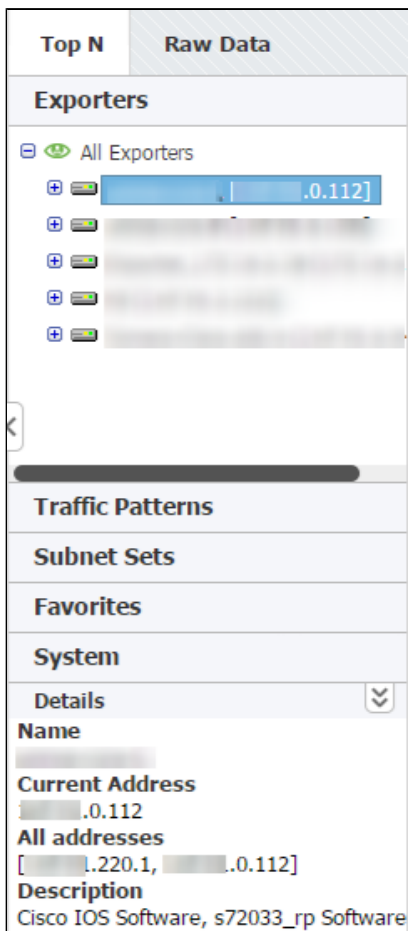
1. Click on the **Favorites** tab
2. Select desired Favorite node from Navigation Tree

And, to remove a favorite:

1. Go to **Favorites** tab
2. Right click on a desired favorite
3. Select **Remove from favorites**



Reading NetFlow Details



The screenshot shows a web interface with two tabs: 'Top N' and 'Raw Data'. The 'Exporters' section is active, displaying a list of exporters under 'All Exporters'. The first exporter is selected, and its details are shown in a sidebar on the right. The details include:

- Name: [Redacted]
- Current Address: [Redacted].0.112
- All addresses: [Redacted].220.1, [Redacted].0.112
- Description: Cisco IOS Software, s72033_rp Software

Details show additional information about the selected node, such as Name, SNMP Index, Address and Description (where applicable).

To view details for a selected node, click **Show details** arrow in the bottom left corner in the Top mode.

Details show current IP address (only for exporters), as well as all used NetFlow export IP addresses.

SNMP policies need to be set in order to have these details. For more on SNMP policies and exporter discovery see chapters [Configuring SNMP Policies](#) and [Working with Exporters and Interfaces](#).

Generating Reports

Exporting Reports

Traffic Statistics can be exported to a PDF file in a form of report that can be printed and presented to third parties.

To generate traffic statistics report, click **Report > Export** in the upper right corner of the Main Panel while in Top N mode.

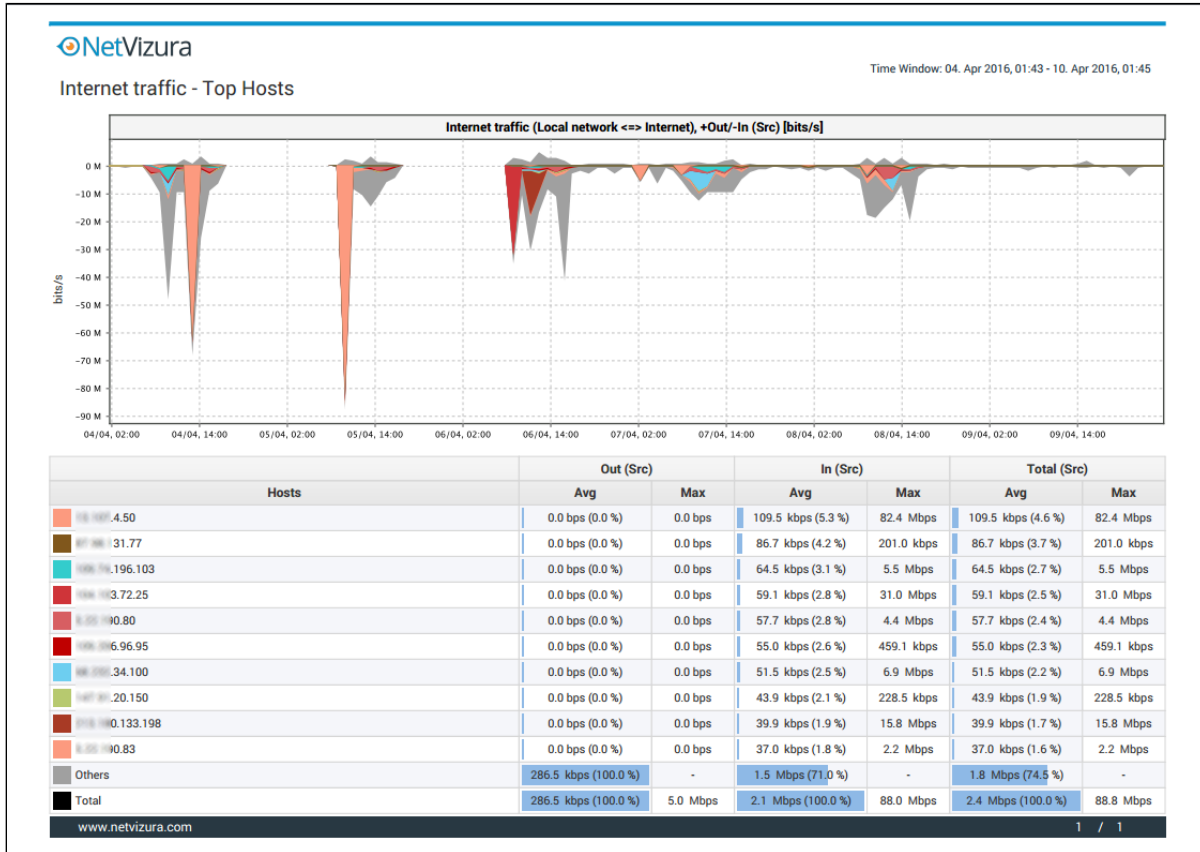


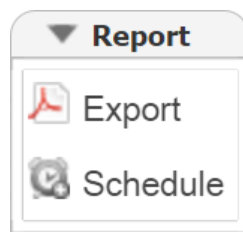
Figure above shows an example of a PDF report generated by NetFlow Analyzer. This report was generated by clicking Report while node Internet Traffic (Traffic Pattern) and tab option Host was selected.

Scheduling Email Reports

Adding Email Reports

Desired PDF report can be scheduled for periodical delivery via email.

To schedule email report, select **Report > Schedule** in the upper right corner of the Main Panel while in TopN mode.





Here you are able to set report's:


1. **Name** - that will be used in the further report management in the Settings
2. **To** - third party recipients which will receive emails (i Recipient does not have to be included as NetVizura user, practically meaning that any email address can be used)
3. **Frequency** - period when email will be delivered (i Email will be delivered on the 1st day of each period. For weekly reports, 1st day of the week depends the server local time configuration).
4. **Message** - text that will show in the body of the email.


Managing Email Reports

Existing reports are further managed in **NetFlow Settings > Reports** where scheduled reports can be edited, removed or cloned.

To edit an existing report:

1. Select pen icon ()
2. You are able to modify the following report's:
 - a. Report Name
 - b. To recipients
 - c. Frequency
 - d. Scope  Only same-level nodes are possible to change for the same report. All other report options, such as Throughput, bits, In/Out etc. are unchangeable)
 - e. Subject of the message
 - f. Message body
3. Click Save

To remove a report, select minus icon ()

To clone a report, select copy icon (), and follow modification steps similar to report editing.

Advanced NetFlow Usage

In this chapter you will learn how to setup NetVizura to show advanced traffic, alarms and how to analyse flow records.

- [Advanced Traffic Pattern Examples](#)
- [Inspecting Raw Data \(Flow Records\)](#)
- [Viewing End User Traffic](#)
- [Using NetFlow Alarms](#)
- [Understanding NetFlow System Traffic](#)
- [Using Activity Log](#)

Advanced Traffic Pattern Examples

This article uses filtering based on netflow parameters. For more information on how to add a specific filter, see chapter [Configuring Traffic Patterns](#) and article [Fine-tuning a Traffic Pattern](#).

On this page:


- [Discarded Traffic Pattern \(Exporter Filtering Example\)](#)
- [Internet HTTP Traffic Pattern \(Service Filtering Example 1\)](#)
- [Email Traffic Pattern \(Service Filtering Example 1\)](#)
- [Facebook Traffic Pattern \(AS Filtering Example\)](#)
- [Unexpected Protocols Traffic Pattern \(Protocol Filtering Example\)](#)

Discarded Traffic Pattern (Exporter Filtering Example)

Discarded Traffic is the traffic that your network devices send to the Null interface. On Cisco routers, traffic is sent to the null interface if you have invalid routing (routing tables are not complete) or the traffic is blocked by access lists. So, this traffic can give you information on (1) routing problems and (2) on blocked traffic, which is potentially an attack or an attempt of unauthorized access to your network.

Let us see how to make a Traffic Pattern for this purpose. You are only interested in the traffic within your network, so you should create a Self-Traffic type. This being said, you should only set the Internal Network IP address range to your company network's whereas your company network's range will be automatically included in the External network IP address range (Self-Traffic). As for using filters, since you are interested in the discarded traffic (null interfaces), you need to use the Exporter filter. Furthermore, as you are interested in discarded traffic on all exporters, you need to include all exporters into the filter while setting the Out interface field to 0 (code for the null value).

1. Select Self-Traffic (Traffic Pattern type)
2. IP Address ranges:
 - a. Internal: include your company network's range
 - b. External: your company network's range is included automatically (Self-Traffic)
3. Filters:
 - a. Click on the Exporter:
 - b. Add Exporter IP address and set Interface Out value to 0, click Include


 It is necessary to repeat this step for each exporters that are sending netflow data to your NetFlow Analyzer.

Internet HTTP Traffic Pattern (Service Filtering Example 1)

In some cases, you might want to take a detailed look at HTTP traffic.

Since this traffic is between an outside network and your internal network, you should use the Normal Traffic Pattern type. You need cover the traffic between your whole internal network and any other network (Internet). This being said, you should set the Internal Network IP address range to your company network's range - the External network IP address range will be populated automatically (Normal Traffic). As for using the filters, since you are dealing with a web service which is recognized by its port(s), you need to use an Service filter and enter its Service number, HTTP (80) in this example.

1. Select Normal (default Traffic Pattern type)
2. IP Address ranges:
 - a. Internal: include your company network's range
 - b. External: your company network's range is excluded automatically
3. Filters:
 - a. Exporter or Next Hop: read more about [Manual Deduplication](#)
 - b. Service:
 - i. Include Source port(s) 80 / Destination port(s) empty (All)
 - ii. Include Source port(s): empty (All) / Destination port(s) 80

 It is necessary to repeat this step for each port that is used for HTTP (eg. 8080, 443, etc.).

Email Traffic Pattern (Service Filtering Example 1)

You can use NetFlow Analyzer for dedicated monitoring of your Email traffic.

You should use the Custom Traffic Pattern type, since IP address ranges overlap. You need to cover the traffic between your whole internal network with mail servers. This being said, you should set the Internal Network IP address range to your company network's range, with exception of your mail server's IP, and set the External network IP address range as your mail server's IP (in this case your email server is treated as "Outside" network). As for using the filters, since you are interested in service which is recognized by its port(s), you need to use an Service filter and add Service number for the service, Email POP3 port (110) in this example.

1. Select Custom (Traffic Pattern type)
2. Address

- a. Internal: include your company network's range, and exclude you mail server's IP
 - b. External: include you mail server's IP
3. Filters:
- a. Exporter or Next Hop: read more about [Manual Deduplication](#)
 - b. Service
 - i. Include Source port(s): 110 / Destination: empty (All)
 - ii. Include Source port(s): empty (All) / Destination: 110

i It is necessary to repeat this step for each port used for email traffic (eg. 25, 995, ...).

Other examples of the filtering based on service are SMTP, SSH, MS-SQL Traffic, etc.

Facebook Traffic Pattern (AS Filtering Example)

You may want to measure the traffic between your network (or its part) and a specific web service such as Facebook.

Since this traffic is between an outside network (Facebook) and your internal network, you should use the Normal Traffic Pattern type. You need to cover traffic between your whole internal network and any other network. This being said, you should set the Internal Network IP address range to your company network's range - the External network IP address range will be populated automatically (Normal Traffic). As for using the filters, since you are interested in a web service which is recognized by its AS, you need to use an AS filter and enter AS number for the service, in this example the ASN is Facebook's ASN (32934).

You can also join all major social network traffics in into one Social Network Traffic Pattern.

1. Select Normal (default Traffic Pattern type)
2. IP Address ranges:
 - a. Internal: include your company network's range
 - b. External: your company network's range is excluded automatically
3. Filters:
 - a. Exporter or Next Hop: read more about [Manual Deduplication](#)
 - b. AS
 - i. Include Source port(s): 32934 / Destination: empty (All)
 - ii. Include Source: empty (All) / Destination: 32934

Other examples of AS filtering are YouTube, Twitter and Skype Traffic Patterns. You can also monitor these services in a same Traffic Pattern.

It is necessary that your exporters have BGP table included, and that they are configured to export AS numbers.

Unexpected Protocols Traffic Pattern (Protocol Filtering Example)

Some traffic important to you might be small in the terms of volume and, therefore, not easily spotted on charts and graphs, if so - create a separate Traffic Pattern for that traffic.

One example of this is when you are interested in traffic made by protocols other than UDP and TCP. Since these two protocols usually take up to 99% of all traffic, it will be hard to spot any other protocol on graphs. Protocols other than TCP and UDP (we will call them unexpected protocols) might indicate a tunneling protocol or a potential attack.

Let us see how to make a Traffic Pattern for this purpose. You need to cover the traffic between your whole internal network and any other network - attacks are usually expected to come from the External Network to Internal Network (your internal network), but keep in mind that your own network security can be compromised and an attack might be launched from your network to some other network (both Internal and External network). You will do that by choosing Custom for the Traffic Pattern type. This being said, you should set the Internal network IP address range to your company's network range and leave the External network IP address range empty, since you want to cover all other networks. As for using the filters, since you are interested in protocols, you need to use the Protocol filter and enter service port numbers for TCP and UDP which are 6 and 17.

1. Select Custom (Traffic Pattern type)
2. IP Address ranges:
 - a. Internal: include your company network's range
3. Filters:
 - a. Exporter or Next Hop: read more about [Manual Deduplication](#)
 - b. Protocol
 - i. Exclude Protocol number(s): 6
 - ii. Exclude Protocol number(s): 17

Other examples of Protocol filtering are dedicated ICMP, IPv6 and GRE Traffic Patterns.

Inspecting Raw Data (Flow Records)

Raw Data files store flow records exported in a 5-minute interval.

Raw Data Tree groups Raw Data files in folders according to day/hour/minute. Selecting a node from the tree allows inspection of specific Raw Data files.

Inspecting Raw Data

To inspect Raw Data:

1. Go To **NetFlow > Raw Data > Files**
2. **Specify time period** in Time Window. The main panel and Raw Data Tree will show gathered files
3. **Select files** you want to inspect from the Main Panel (or alternatively, select a single file from Raw Data Tree)
4. Click **Show Selected**

The screenshot shows the NetFlow interface. On the left, the 'Raw Data' tree is expanded to '15h', showing a list of files for the time period 2014-08-14-15-00-00.n to 2014-08-14-15-40-00.n. The file '2014-08-14-15-00-00.n' is selected. In the main panel, the 'Files' tab is active, displaying a table of selected files. The table has columns for 'Select', 'File', and 'Size'. The selected file is highlighted in blue.

Select	File	Size
<input type="checkbox"/>	2014-08-14-14-45-00.nfa	40.25 MB
<input type="checkbox"/>	2014-08-14-14-50-00.nfa	40.9 MB
<input type="checkbox"/>	2014-08-14-14-55-00.nfa	39.66 MB
<input checked="" type="checkbox"/>	2014-08-14-15-00-00.nfa	37.81 MB
<input type="checkbox"/>	2014-08-14-15-05-00.nfa	37.1 MB
<input type="checkbox"/>	2014-08-14-15-10-00.nfa	35.45 MB
<input type="checkbox"/>	2014-08-14-15-15-00.nfa	35.83 MB
<input type="checkbox"/>	2014-08-14-15-20-00.nfa	34.95 MB
<input type="checkbox"/>	2014-08-14-15-25-00.nfa	35.63 MB
<input type="checkbox"/>	2014-08-14-15-30-00.nfa	34.73 MB
<input type="checkbox"/>	2014-08-14-15-35-00.nfa	36.45 MB
<input type="checkbox"/>	2014-08-14-15-40-00.nfa	35.48 MB

Raw Data table shows flow records from the selected Raw Data file(s). Data can be filtered, grouped and sorted by almost any field (source IP address, Bytes, Protocol etc.).

The screenshot shows the NetFlow interface with a table of flow records. The table has columns for Start Time, End Time, Duration, Src IP, Src Port, Dst Port, Protocol, TOS, TCP Flags, Flows, Packets, Bytes, and Throt. The table is filtered by Src IP (172.16.2.148) and grouped by Dst Port (443). The table is sorted by Bytes. The table contains 20 rows of data.

Start Time	End Time	Duration	Src IP	Src Port	Dst Port	Protocol	TOS	TCP Flags	Flows	Packets	Bytes	Throt	
22-10-2014 09:42:57.840	22-10-2014 09:44:56.500	118.560 sec	172.16.2.163	58986	107.20.249.204	443	6	0	APRS	1	11	2,480	167.3 bps
22-10-2014 09:43:15.12	22-10-2014 09:44:56.504	101.492 sec	172.16.2.163	58988	108.160.166.140	443	6	0	APRS	1	11	2,579	203.3 bps
22-10-2014 09:44:46.380	22-10-2014 09:44:56.580	10.200 sec	172.16.2.19	55084	213.180.204.90	80	6	0	APSF	1	7	729	570.6 bps
22-10-2014 09:44:46.456	22-10-2014 09:44:56.676	10.220 sec	213.180.204.90	80	172.16.2.19	55084	6	0	APSF	1	6	671	525.2 bps
22-10-2014 09:44:56.712	22-10-2014 09:44:56.712	0.0 sec	148.251.76.148	80	172.16.2.144	54116	6	0	AF	1	1	40	-
22-10-2014 09:44:27.232	22-10-2014 09:44:57.596	30.364 sec	172.16.3.67	36177	108.160.166.253	443	6	0	APSF	1	16	2,508	660.8 bps
22-10-2014 09:44:27.492	22-10-2014 09:44:57.568	30.76 sec	108.160.166.253	443	172.16.3.67	36177	6	0	APSF	1	14	6,339	1.7 Kbps
22-10-2014 09:39:58.44	22-10-2014 09:39:58.44	0.0 sec	172.16.0.4	64476	82.117.194.2	53	17	0	A	1	1	61	-
22-10-2014 09:39:58.108	22-10-2014 09:44:28.412	270.304 sec	172.16.2.148	57581	74.125.206.188	5228	6	0	A	1	7	287	8.5 bps
22-10-2014 09:39:58.184	22-10-2014 09:44:28.188	270.4 sec	63.251.34.69	12975	172.16.2.164	1619	6	0	AP	1	78	10,956	324.6 bps
22-10-2014 09:39:58.428	22-10-2014 09:42:31.884	153.556 sec	172.16.0.4	53013	82.117.194.2	53	17	0	A	1	3	192	10.0 bps
22-10-2014 09:39:58.820	22-10-2014 09:44:43.656	284.836 sec	74.125.133.125	5222	172.16.2.108	49712	6	0	AP	1	12	3,693	103.7 bps
22-10-2014 09:39:58.820	22-10-2014 09:44:43.656	284.798 sec	172.16.2.108	49712	74.125.133.125	5222	6	0	AP	1	10	511	14.4 bps
22-10-2014 09:44:53.664	22-10-2014 09:44:56.576	5.912 sec	148.251.76.148	80	172.16.2.144	54152	6	0	APSF	1	8	531	83.0 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.264	16.232 sec	172.16.2.19	54990	193.109.246.48	80	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.180	16.128 sec	172.16.2.19	54991	193.109.246.48	80	6	0	APSF	1	11	1,160	575.4 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.32	15.980 sec	172.16.2.19	54992	193.109.246.48	80	6	0	APSF	1	26	1,745	873.6 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.32	15.980 sec	172.16.2.19	54993	193.109.246.48	80	6	0	APSF	1	26	1,745	873.6 bps
22-10-2014 09:44:40.56	22-10-2014 09:44:56.132	16.76 sec	172.16.2.19	54994	193.109.246.48	80	6	0	APSF	1	26	1,745	873.6 bps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.352	16.232 sec	193.109.246.48	80	172.16.2.19	54990	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.260	16.140 sec	193.109.246.48	80	172.16.2.19	54991	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.104	15.984 sec	193.109.246.48	80	172.16.2.19	54992	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.124	22-10-2014 09:44:56.100	15.976 sec	193.109.246.48	80	172.16.2.19	54993	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.124	22-10-2014 09:44:56.200	16.76 sec	193.109.246.48	80	172.16.2.19	54994	6	0	APSF	1	12	1,203	582.9 bps
22-10-2014 09:44:40.916	22-10-2014 09:44:57.180	16.264 sec	172.16.2.19	55002	108.168.157.176	80	6	0	APSF	1	12	1,203	582.9 bps

In order to enable IP address resolution, your NetVizura server should have local or remote communication with DNS server (for Hostname) and Internet access (for Whois information).

Clicking on **Names** button provides IP address resolution. If you move your mouse cursor over specific IP address you can see Whois information about that host.

Start Time	End Time	Duration	Src IP	Src Port	Dst IP	Dst Port	Protocol
17-03-2016 02:54:57.708	17-03-2016 02:54:57.804	0.96 sec	sheilant.soneco.co.rs	52676	91.127.144	SSH	TCP
17-03-2016 02:54:57.888	17-03-2016 02:54:57.996	0.108 sec	sheilant.soneco.co.rs	55010	37.129.4	SSH	TCP
17-03-2016 02:59:55.796	17-03-2016 02:59:56.44	0.248 sec	6.0.45	55136	5.113.12	HTTP	TCP
17-03-2016 02:59:55.808	17-03-2016 02:59:56.924	1.116 sec	172-230-119.static.isp.telekom.rs				
17-03-2016 02:59:55.904	17-03-2016 02:59:56.540	0.636 sec	172-20-103.static.isp.telekom.rs				
17-03-2016 02:59:55.916	17-03-2016 02:59:56.164	0.248 sec	.113.12				
17-03-2016 02:59:57.224	17-03-2016 02:59:57.520	0.296 sec	sheilant.soneco.co.rs				
17-03-2016 02:54:58.772	17-03-2016 02:54:58.360	0.288 sec	sheilant.soneco.co.rs				
17-03-2016 02:54:58.252	17-03-2016 02:54:58.716	0.464 sec	sheilant.soneco.co.rs				
17-03-2016 02:54:58.424	17-03-2016 02:59:55.568	297.144 sec	ina-7x64.soneco.co.rs	51427	118.234.66	17771	UDP
17-03-2016 02:54:58.516	17-03-2016 02:59:58.464	299.948 sec	18.234.66	17771	ana-7x64.soneco.co.rs	51427	UDP
17-03-2016 02:54:58.544	17-03-2016 02:59:42.56	283.512 sec	pc.soneco.co.rs	63383	n-f188.1e100.net	5228	TCP
17-03-2016 02:54:58.548	17-03-2016 02:59:55.532	296.984 sec	ina-7x64.soneco.co.rs	51427	254.151.86	59168	UDP
17-03-2016 02:54:58.584	17-03-2016 02:59:42.36	283.452 sec	-f188.1e100.net	5228	-pc.soneco.co.rs	63383	TCP
17-03-2016 02:54:58.588	17-03-2016 02:58:59.480	240.892 sec	soneco.rs	IMAP4	16.3.91	49433	TCP
17-03-2016 02:54:58.588	17-03-2016 02:58:59.692	241.104 sec	6.3.91	49433	soneco.rs	IMAP4	TCP
17-03-2016 02:54:58.708	17-03-2016 02:59:27.608	268.900 sec	sheilant.soneco.co.rs	0	6-60-108.static.isp.telekom.rs	2048	ICMP
17-03-2016 02:59:56.796	17-03-2016 02:59:57.520	0.724 sec	-237-189.static.isp.telekom.rs	SSH	sheilant.soneco.co.rs	59168	TCP
17-03-2016 02:59:58.104	17-03-2016 02:59:58.356	0.252 sec	sheilant.soneco.co.rs	46305	6-63-221.static.isp.telekom.rs	SSH	TCP
17-03-2016 02:59:58.216	17-03-2016 02:59:58.284	0.68 sec	sheilant.soneco.co.rs	45745	222.246.173	MS Office antipiracy/DirectAdmin	TCP
17-03-2016 02:54:59.280	17-03-2016 02:54:59.556	0.276 sec	sheilant.soneco.co.rs	58491	222.248.253	SSH	TCP

IP address 178.222.230.119

Description: TELEKOM SRBIJA, ADSL users Takovska 2 11000 BELGRADE SERBIA

Country: Serbia

Network Range: 178.222.0.0 - 178.222.255.255

AS: TELEKOM-AS (8400)

Exporting Raw Data

Raw Data table can be exported as a CSV file in order to present captured netflow records as a report to a third party or for further analysis.

To export Raw Data, click on the the **Export** button in the upper right corner of the Raw Data Table.

Start Time	End Time	Duration	Src IP	Src Port	Dst IP	Dst Port
22-10-2014 09:42:57.940	22-10-2014 09:44:56.500	118.560 sec	163	59896	49.204	443
22-10-2014 09:43:15.12	22-10-2014 09:44:56.504	101.492 sec	163	59898	166.140	443
22-10-2014 09:44:46.360	22-10-2014 09:44:56.580	10.220 sec	19	55084	204.90	80
22-10-2014 09:44:46.456	22-10-2014 09:44:56.676	10.220 sec	204.90	80	19	55084
22-10-2014 09:44:56.712	22-10-2014 09:44:56.712	0.0 sec	76.148	80	144	54116
22-10-2014 09:44:27.232	22-10-2014 09:44:57.596	30.364 sec	67	36177	166.253	443
22-10-2014 09:44:27.492	22-10-2014 09:44:57.568	30.76 sec	166.253	443	67	36177
22-10-2014 09:39:58.44	22-10-2014 09:39:58.44	0.0 sec	4	64478	94.2	53
22-10-2014 09:39:58.108	22-10-2014 09:44:28.412	270.304 sec	148	57581	06.188	5228
22-10-2014 09:39:58.184	22-10-2014 09:44:28.188	270.4 sec	169	12975	164	1619
22-10-2014 09:39:58.428	22-10-2014 09:42:31.984	153.556 sec	4	53013	94.2	53
22-10-2014 09:39:58.820	22-10-2014 09:44:43.656	284.836 sec	33.125	5222	108	49712
22-10-2014 09:39:58.820	22-10-2014 09:44:43.608	284.788 sec	108	49712	33.125	5222
22-10-2014 09:44:53.464	22-10-2014 09:44:58.576	5.112 sec	76.148	80	144	54152
22-10-2014 09:44:40.52	22-10-2014 09:44:56.284	16.232 sec	19	54990	246.48	80
22-10-2014 09:44:40.52	22-10-2014 09:44:56.180	16.128 sec	19	54991	246.48	80
22-10-2014 09:44:40.52	22-10-2014 09:44:56.32	15.980 sec	19	54992	246.48	80

Grouping, filtering and sorting the raw data table will affect the CSV as well. This will also make a CSV file much smaller.

Depending on the amount of data, export can last a couple of minutes

Depending on your browser settings, browser may ask you were to save the file or it will save the file to a default folder (usually **Downloads** folder). Some spreadsheet software may ask you which separator to use when opening the file - select **Comma**.

Viewing End User Traffic

In order to view End User Traffic, you first need to configure NetVizura to collect syslog logon messages and map users to IP addresses. After that, end users will automatically appear in the node tree as they logon to their workstations and start making traffic. To learn more go to [Setting End User Traffic](#).

End User Traffic is visible only to Admin users with Write permission on the NetFlow module.

When you investigate atypical behavior or a threat in the network, information about IP address often does not provide precise identification of the responsible person. Linking an address to a username is very important because it allows administrators to determine exactly who used the IP address at the specific time. This significantly improves situational awareness and reduces incident response/resolution time - help desk agent can quickly call the responsible person to ask if he/she logged on to the device, and cross-check suspicious behavior.

Traffic for one user is presented as the sum of the traffic from all IP addresses he used during a certain time window.

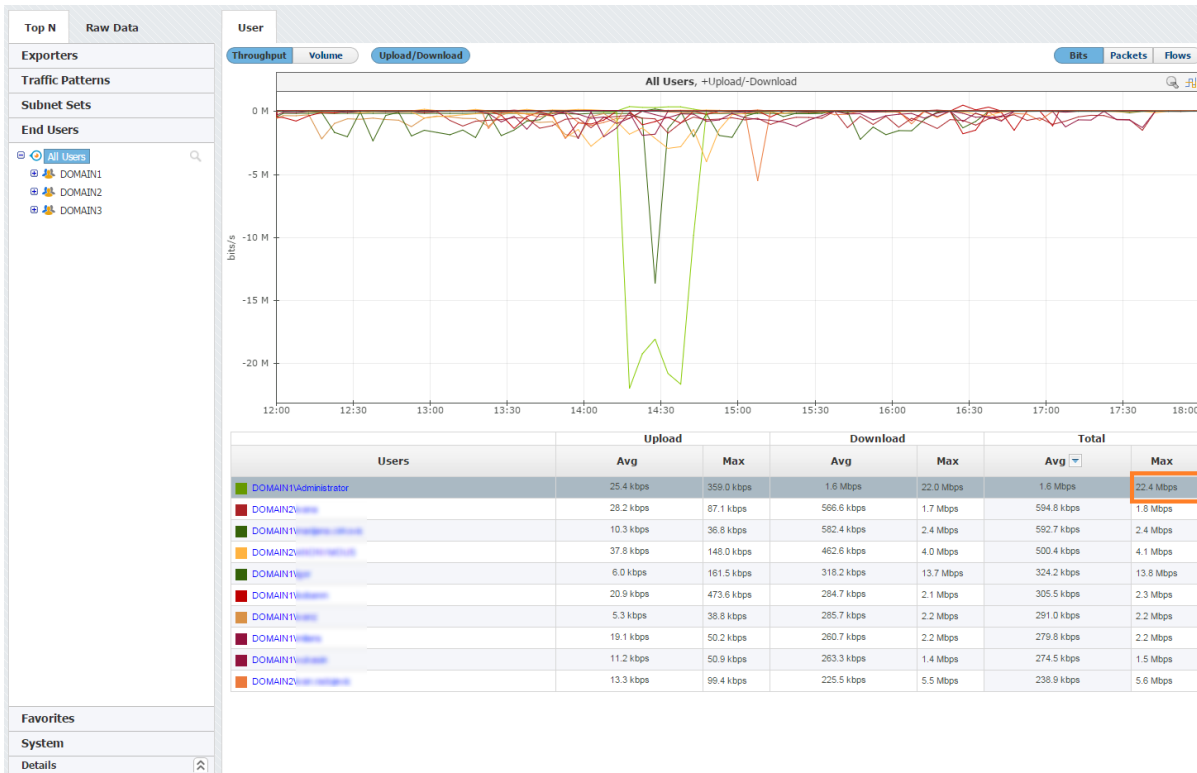
End Users Traffic shows top talkers for:

- [All Users Traffic](#)
- [Domain Users Traffic](#)
- [End User Traffic by Hosts](#)
- [End User Traffic by Conversations](#)
- [End User Traffic by Services](#)
- [End User Traffic by Protocols](#)
- [End User Traffic by QoS](#)
- [End User Traffic by AS](#)

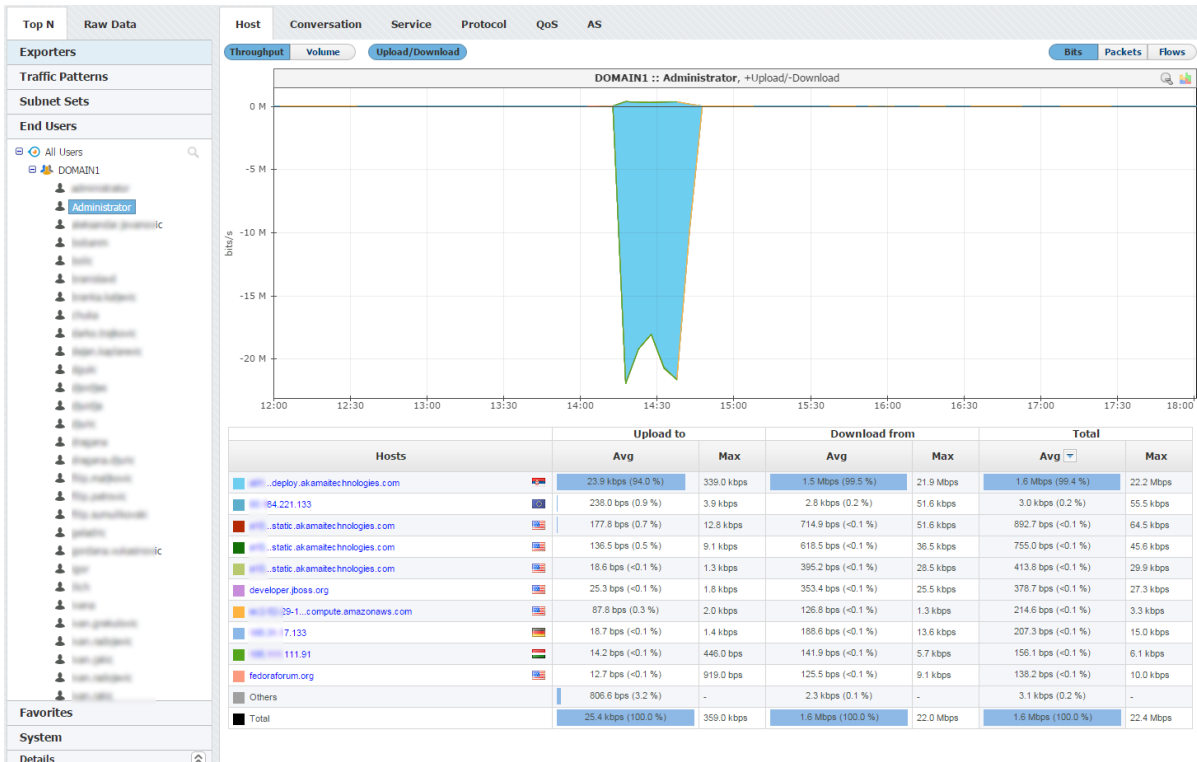
All Users Traffic

All Users View shows end-users with the most traffic in your network (from all domains).

To see this view, go to **Top N > End Users** option and select **All Users** node.



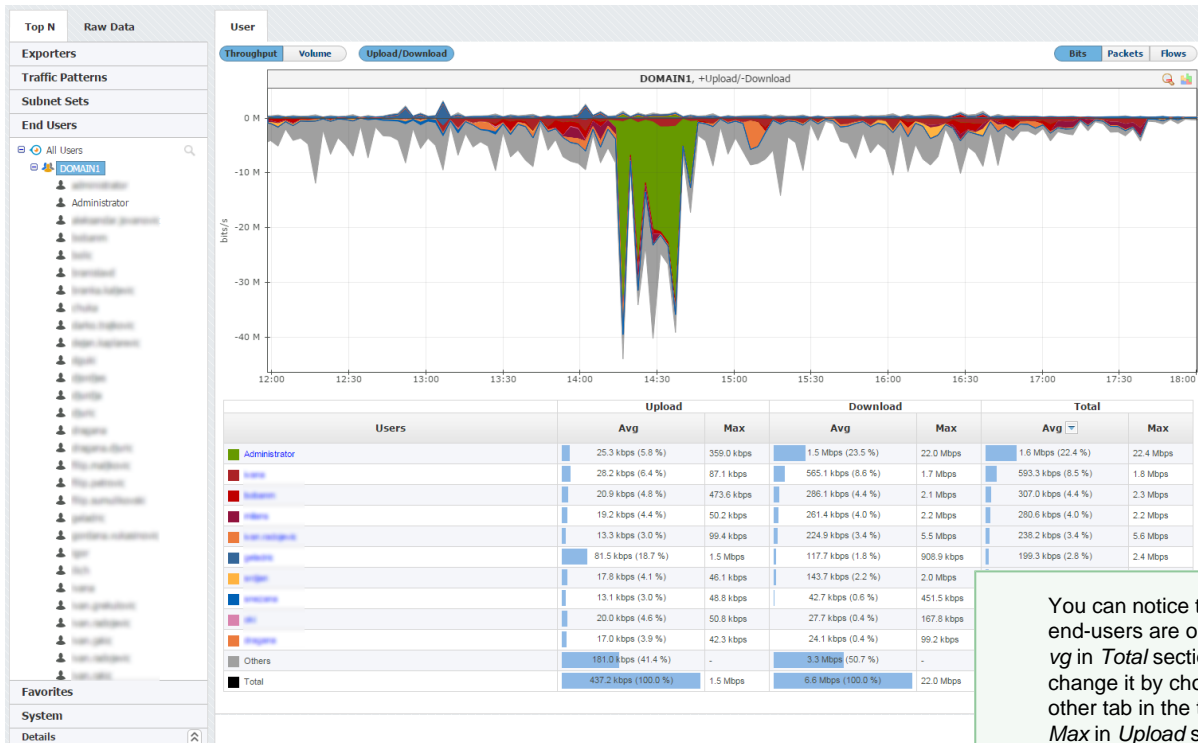
You can notice that user "Administrator" had significantly higher traffic then other users between 2pm and 3pm. Clicking on user "Administrator" will open single user's view, where you can deeply inspect his/hers traffic.



Domain Users Traffic

Domain Users View shows end-users with the most traffic in one domain.

To see this view, go to **Top N > End Users** option and select certain domain within **All Users** node



You can notice that top end-users are ordered by *Avg* in *Total* section. You can change it by choosing any other tab in the table (e.g. *Max* in *Upload* section).

Figure above shows example of top end-user traffic from domain *DOMAIN1* in time period of 6-hours, ordered by Total Average traffic.

This view helps to see how much traffic passing through a specific domain. Main Panel can show *T throughput* or *Volume* measured in bits, packets or flows.

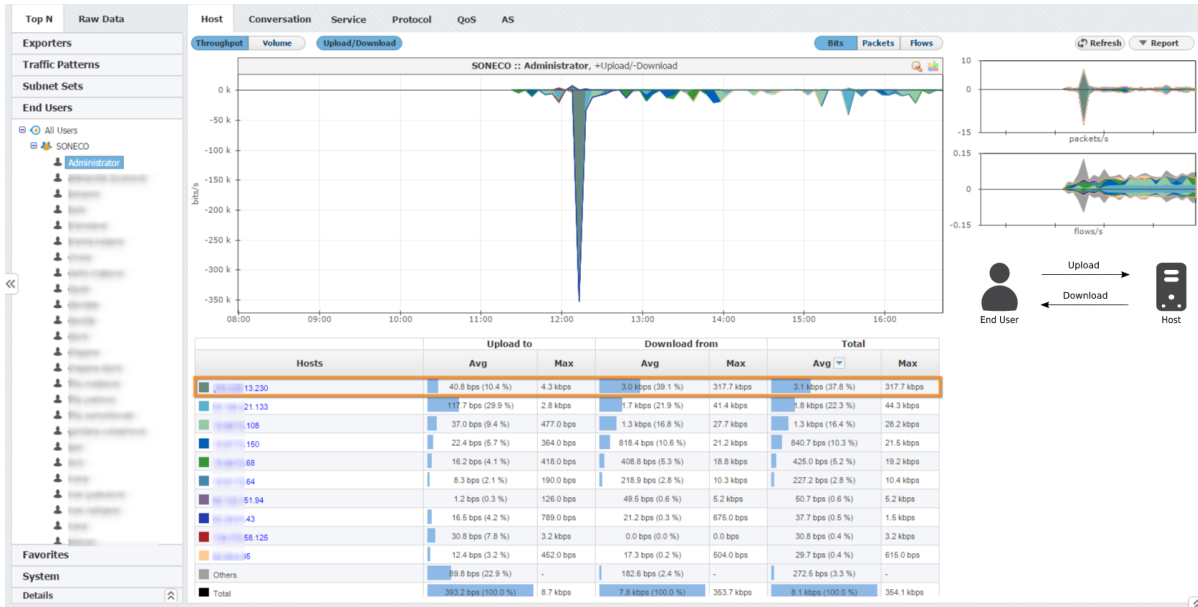
End User Traffic by Hosts

End user traffic distribution by hosts shows the contribution of top hosts (individual IP addresses) to the traffic made by specific end user. Data which was sent by the End user is classified as Upload traffic, while data which was received by the end user is classified as Download traffic.

Traffic for one user is presented as the sum of the traffic from all IP addresses he used during the certain time window.

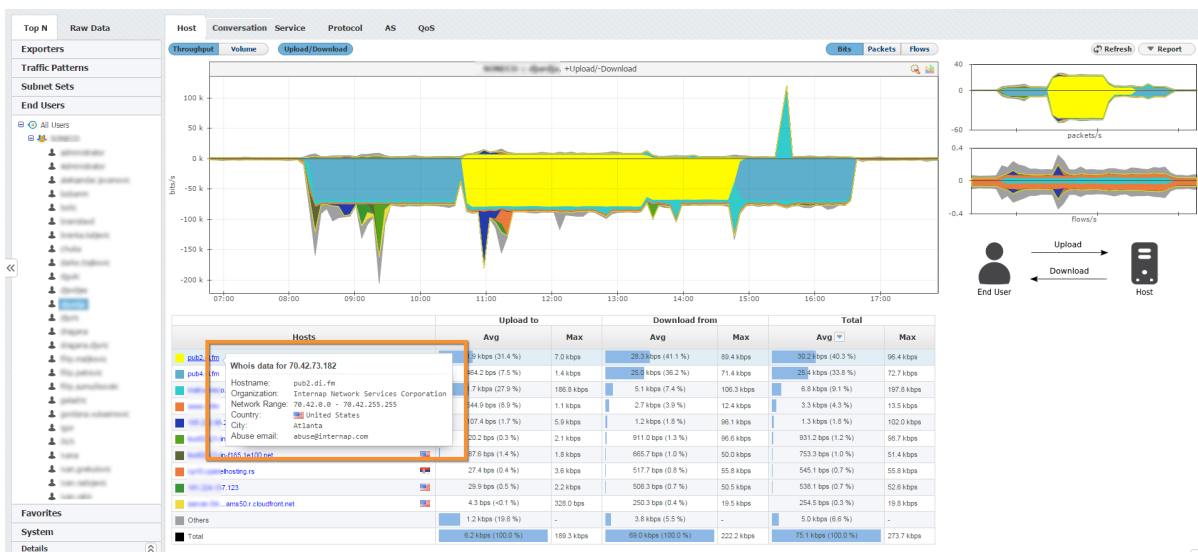
To view this traffic:

1. Choose a node type **End Users** from the accordion in the Menu Panel
2. Select desired domain and username from the Node Tree
3. Choose **Host** from the Tab panel



In the screenshot above, we see that Administrator logged on to the network at 11:30 and had a huge download from X.X.13.230. at 12:15.

Each host IP address is resolved to corresponding hostname over DNS, and for each non-private IP address Whois lookup is performed. Data can be viewed in a tooltip, displayed when hovering over specific host. Whois data contains information about the organization which owns the IP subnet the host is part of, as well as the AS number, additional descriptions, country and other location related information for that host.



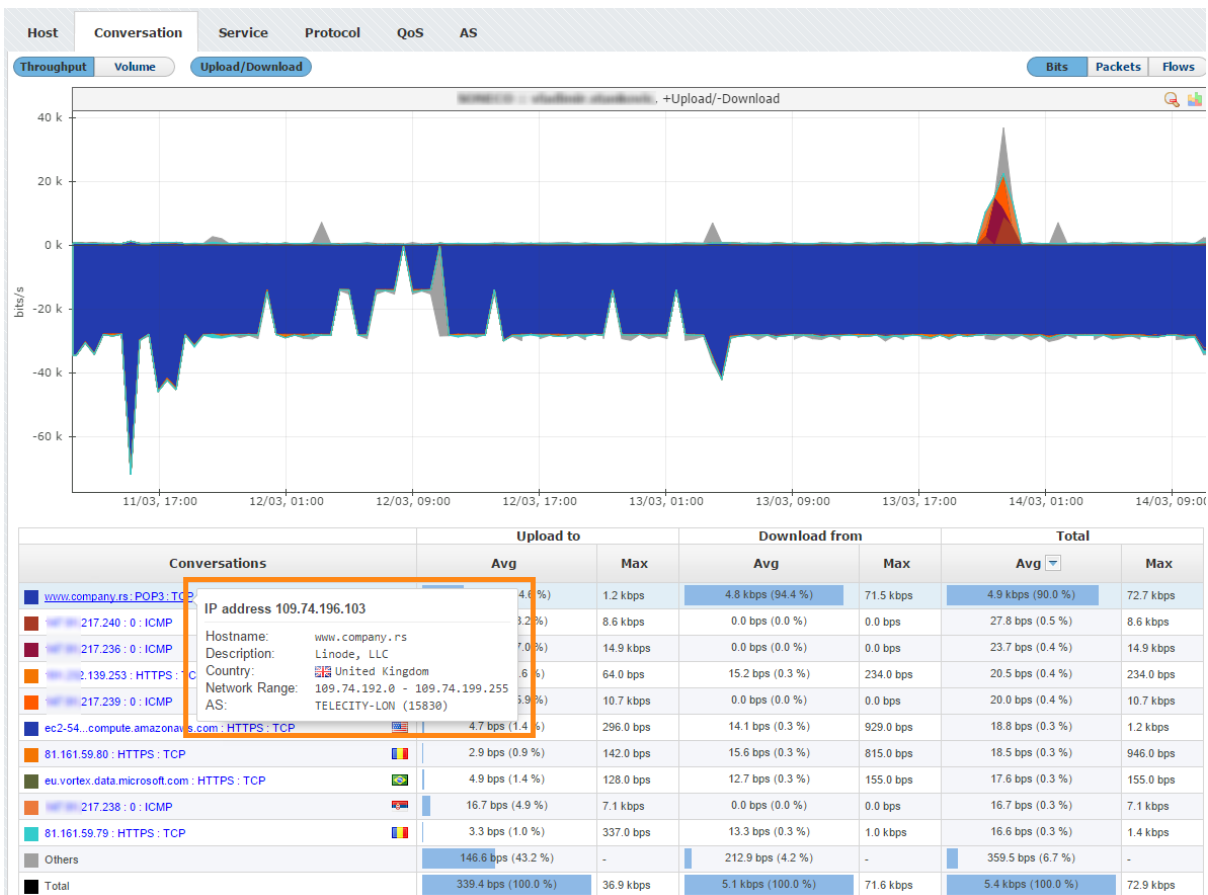
To understand host traffic in general, read more at [Distribution by Hosts](#).

End User Traffic by Conversations

Distribution of end user traffic by conversation shows with whom, over what service and protocol did the user talked to during specified time window. This is useful if you want to look into how much traffic has been generated by end to end conversation by a certain user. Data which was sent by the End user is classified as Upload traffic, while data which was received by the end user is classified as Download traffic.

To see traffic by conversation for specific user:

1. Choose **End Users** node from the accordion in the Menu Panel
2. Search and select desired user from the Node Tree
3. Choose **Conversation** from the Tab panel



In the screenshot above you can see that the selected user mostly use mail service, since POP3 protocol consumes most of the traffic.

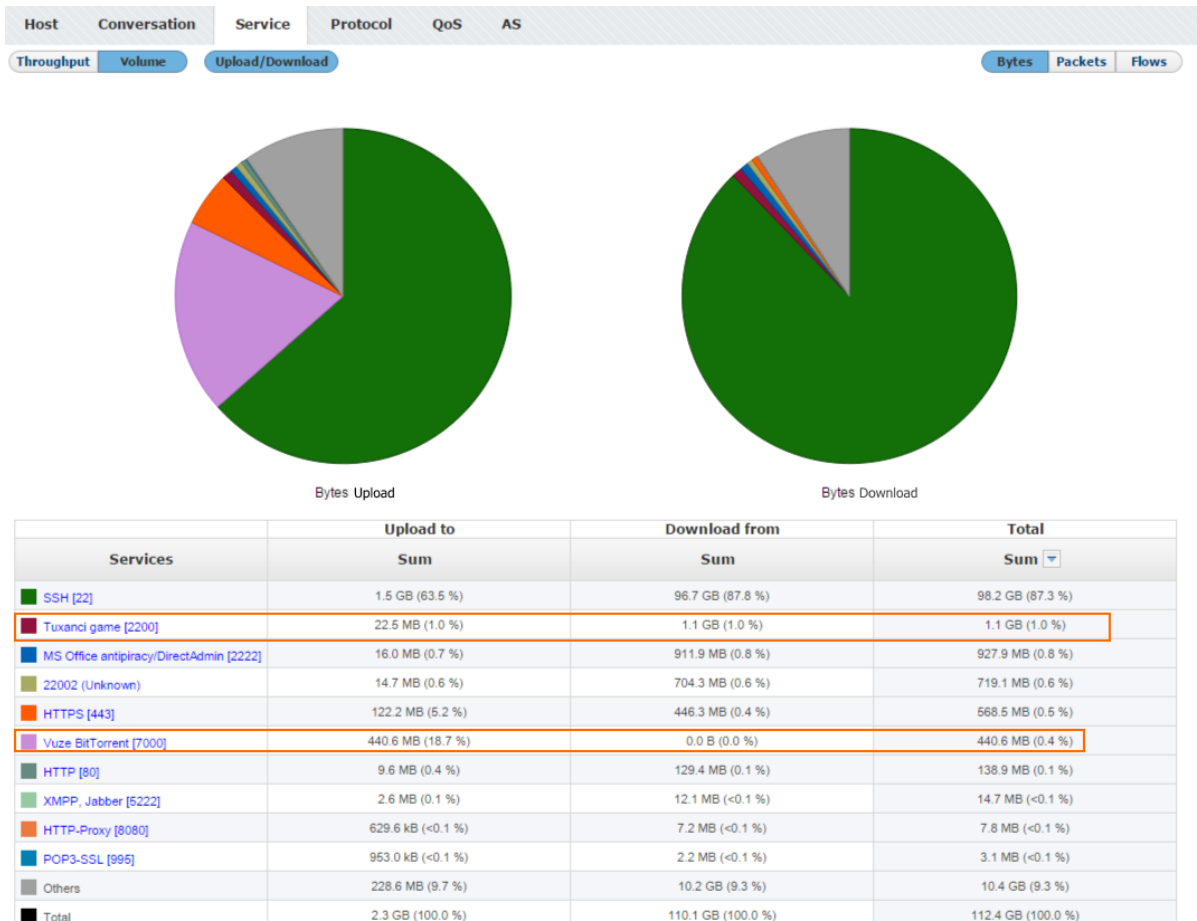
To understand conversation traffic in general, read more at [Distribution by Conversations](#).

End User Traffic by Services

End user traffic distribution by services shows the contribution of top services to the traffic made by specific end user. Data which was sent by the End user is classified as Upload traffic, while data which was received by the end user is classified as Download traffic.

To view this traffic:

1. Choose a node type **End Users** from the accordion in the Menu Panel
2. Select desired domain and username from the Node Tree
3. Choose **Service** from the Tab panel



In the screenshot above, we see that during the selected time window one user made traffic with some undesirable services - 1.1 GB with Tuxanci game and 440 MB with Vuze BitTorrent.

To understand services traffic in general, read more at [Distribution by Services](#).

End User Traffic by Protocols

End user traffic distribution by protocol shows the contribution of top protocols to the traffic made by specific end user. Data which was sent by the End user is classified as Upload traffic, while data which was received by the end user is classified as Download traffic.

To view this traffic:

1. Choose a node type **End Users** from the accordion in the Menu Panel
2. Select desired username from the Node Tree
3. Choose **Protocol** from the Tab panel



In the screenshot above, we see that this user was logged on to the network from 09:00 till 17:00, but also from 23:30 till 00:30. He mostly made TCP downloads but also made one larger UDP download at 11:30.

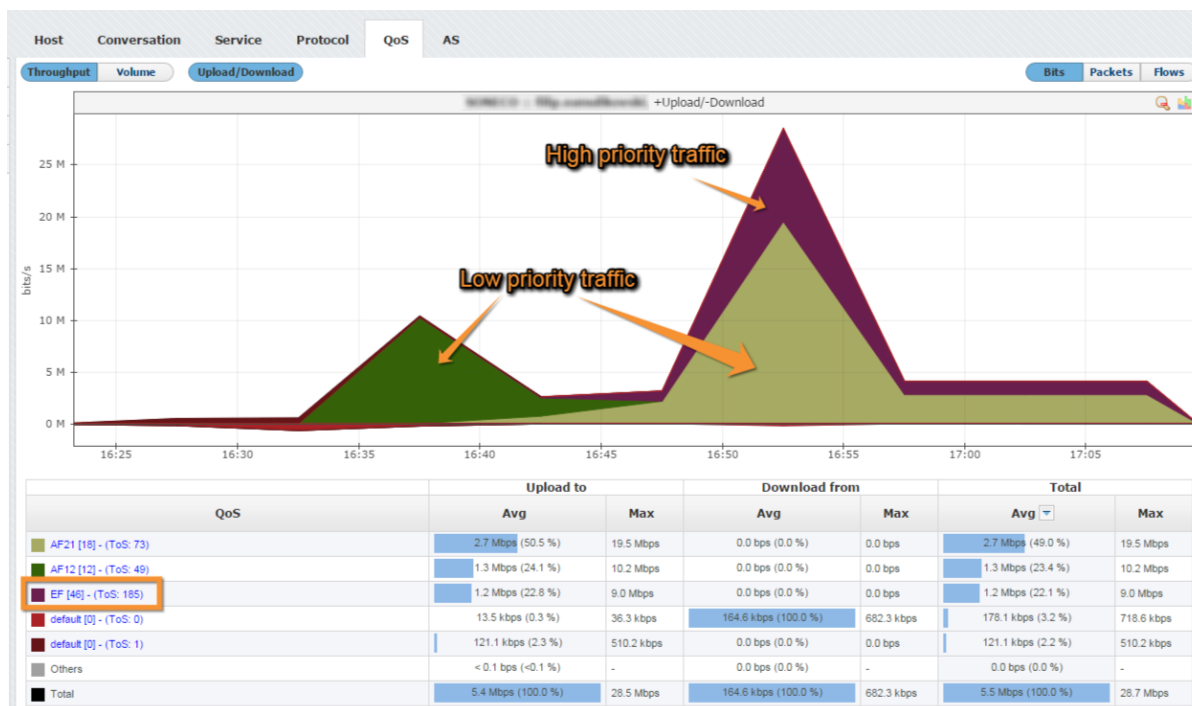
To understand protocol traffic in general, read more at [Distribution by Protocols](#).

End User Traffic by QoS

Distribution by QoS shows end user traffic in the terms of service quality, giving high troubleshooting capabilities in cases of high packet loss, notable latency and jitter, especially concerning real time communication. This is particularly interesting to companies that provide a QoS based service or use such services themselves. Data which was sent by the End user is classified as Upload traffic, while data which was received by the end user is classified as Download traffic.

To view traffic distribution by QoS:

1. Choose **End Users** node from the accordion in the Menu Panel
2. Search and select desired user from the Node Tree
3. Choose **QoS** from the Tab panel



As shown in the image above, traffic that belongs to this user is classified with different QoS markers and therefore being differently treated while routed through the network. Traffic marked with EF(46) marker is highly prioritized over other classes of traffic shown in this image, and has guaranteed bandwidth, which is very suitable for services that require low latency, low packet loss and negligible jitter. It is noticeable in the example image that the sudden increase of high priority traffic affected the overall throughput of other classes of traffic causing higher latency and packet drops for traffic with low priority markers.

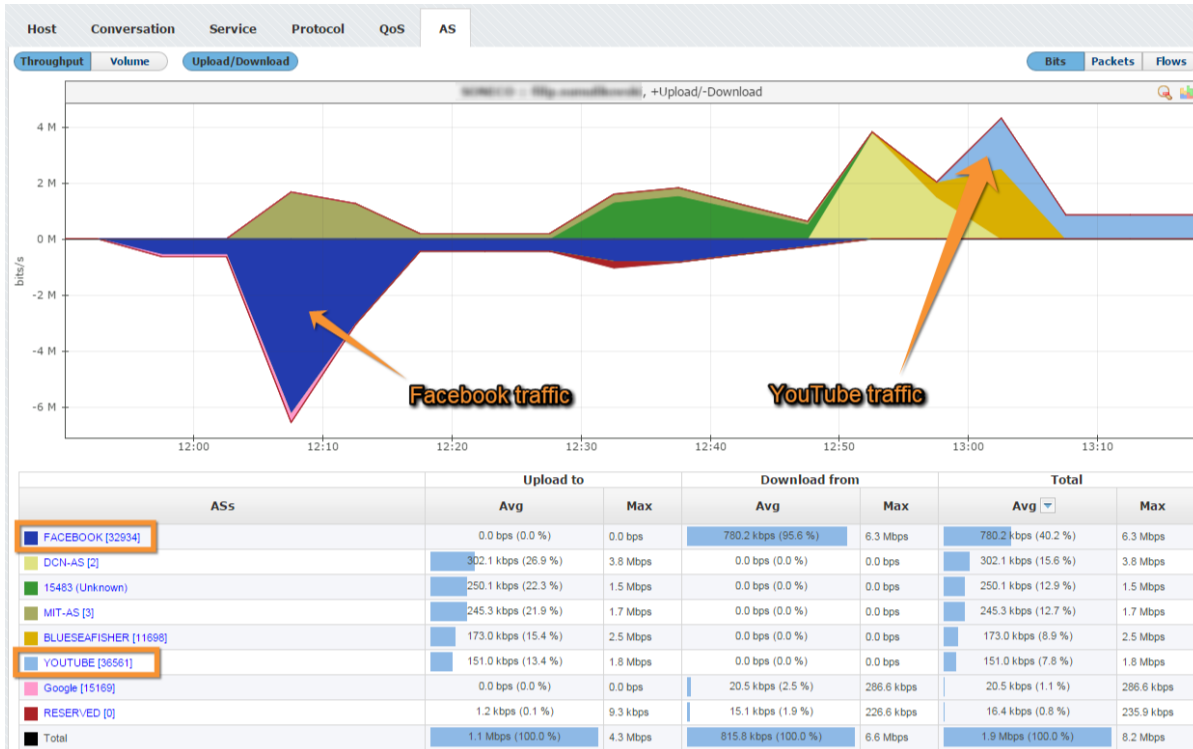
To understand QoS traffic in general, read more at [Distribution by QoS](#).

End User Traffic by AS

Distribution by AS shows traffic for specific end user by autonomous systems. Being aware of traffic users in your network generate towards other autonomous systems i.e. networks is of great importance in terms of preventing and resolving various situations concerning network security and reliability.

To view traffic distribution by AS:

1. Choose **End Users** node from the accordion in the Menu Panel
2. Search and select desired user from the Node Tree
3. Choose **AS** from the Tab panel



In the image above, you can see that this user has notable amount of Facebook traffic in download direction, consuming large portion of available bandwidth between 12:03 p.m. and 12:15 p.m. as well as YouTube traffic in upload direction around 13:02 p.m.

To understand AS traffic in general, read more at [Distribution by AS](#).

Using NetFlow Alarms

You can setup alarms to trigger if traffic goes over defined threshold. Alarms can trigger:

- on any node type (Exporter, Interface, Traffic Pattern, Subnet, Subnet Set, End Users)
- several traffic types (total, host, conversation...)
- for bps, pps, fps traffic or its combination
- for different direction of traffic (total, in, out, src in...)

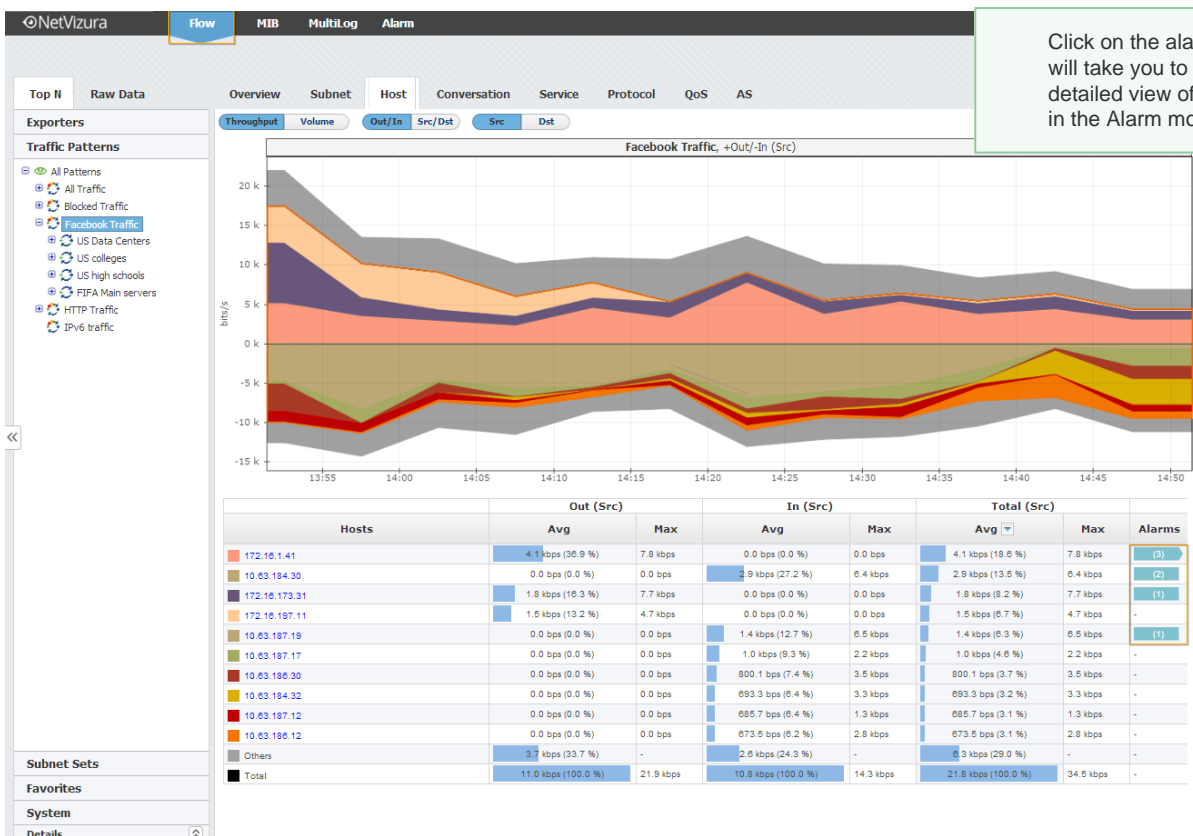
Alarms can be sent to certain users to speed up notification of the right person.

On this page:

- Viewing Alarms in NetFlow module
- Viewing All Alarms (Alarm Module)
- Creating NetFlow Alarms

Viewing Alarms in NetFlow module

Alarms that occurred during Time Window specified are visible as indicators in the Flow Module within the Top talker table. For example, we can see below alarms for Facebook Traffic by hosts.



Click on the alarm indicator will take you to more detailed view of the alarm in the Alarm module.

Alarms that have an arrow to the right are active alarms (trigger condition is still active). Only alarm of the highest severity will be showed. The number in the Alarm table indicates how many alarms occurred for that table entry during the Time Window.

Viewing All Alarms (Alarm Module)

To view all alarms, go to Alarm Module.

Click on the Source link will take you to statistics for the defined scope and object for this alarm. In case of NetFlow alarm, it will jump to NetFlow module and show the corresponding node and traffic chart.

#	Severity	Occurrences	Time	Duration	Module	Alarm	Source	Exporter	Message
(1)	4 Warning	1	Aug 11, 14:40:00 - Aug 11, 14:45:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(172.16.244.0 -> 10.117.00.8 - 20222)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:40:00 - Aug 11, 14:45:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(172.16.158.10 -> 10.224.93.212 - 20300)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:40:00 - Aug 11, 14:40:00	-	Flow	High MENA conv.	SET(16)-CONVERSATION(172.16.158.10 -> 10.150.202.15 - 20300)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 15:15:00 -	00:03:51	Flow	High MENA conv.	SET(16)-CONVERSATION(10.43.104.130 -> 172.16.244.8 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:20:00 - Aug 11, 14:25:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.248.80.196 -> 172.16.204.84 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:20:00 - Aug 11, 14:25:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.211.84.72 -> 172.16.240.105 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:30:00 - Aug 11, 14:45:00	00:15:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.211.84.34 -> 172.16.244.8 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:30:00 - Aug 11, 14:35:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.188.138.83 -> 172.16.203.41 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:20:00 - Aug 11, 14:25:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.122.208.242 -> 172.16.202.97 - 80)	-	High conversation traffic in MENA offices
(1)	4 Warning	1	Aug 11, 14:20:00 - Aug 11, 14:25:00	00:05:00	Flow	High MENA conv.	SET(16)-CONVERSATION(10.122.453.75 -> 172.16.240.105 - 80)	-	High conversation traffic in MENA offices
(2)	6 Notice	1	Aug 11, 14:10:00 -	-	Flow	High FB traffic	PATTERN(S)HOST(172.16.1.41)	-	Host with high FB traffic
(1)	6 Notice	1	Aug 11, 15:10:00 -	00:03:51	Flow	High FB traffic	PATTERN(S)HOST(10.63.180.30)	-	Host with high FB traffic
(1)	6 Notice	1	Aug 11, 15:05:00 - Aug 11, 15:10:00	00:05:00	Flow	High FB traffic	PATTERN(S)HOST(10.63.184.30)	-	Host with high FB traffic
(2)	6 Notice	1	Aug 11, 14:10:00 -	-	Flow	High FB traffic	PATTERN(S)HOST(10.63.184.30)	-	Host with high FB traffic
(1)	4 Warning	1	Aug 11, 15:00:00 - Aug 11, 15:05:00	00:05:00	Flow	High host traffic	INTERFACE(172.16.6.84-20)-TOTAL	172.16.6.84	High host traffic on int
(1)	4 Warning	1	Aug 11, 15:00:00 - Aug 11, 15:05:00	00:05:00	Flow	High int traffic	INTERFACE(172.16.6.84-96)-TOTAL	172.16.6.84	High interface traffic
(1)	2 Critical	1	Aug 11, 15:00:00 - Aug 11, 15:05:00	00:05:00	Flow	High int traffic	INTERFACE(172.16.6.84-20)-TOTAL	172.16.6.84	High interface traffic
(1)	4 Warning	1	Aug 11, 15:00:00 - Aug 11, 15:05:00	00:05:00	Flow	High host traffic	INTERFACE(172.16.6.84-20)-TOTAL	172.16.6.84	High host traffic on int
(1)	1 Alert	1	Aug 11, 15:00:00 - Aug 11, 15:05:00	00:05:00	Flow	High bits	EXPORTER(172.16.6.84)-TOTAL	172.16.6.84	High bits traffic on 172.16.6.194

Here you can see the list of all alarms that occurred within the selected Time Window. In our case, we see that there are several hosts with high FB traffic. Occurrence indicators visualize time when alarm started and ended. If the occurrence indicator blinks it means that the alarm did not end yet (it is still active).

You are also able to filter, sort, group alarms by source and view only active alarms according to your need.

Creating NetFlow Alarms

To add a new alarm in NetFlow Analyzer:

1. Click **Add**
2. Set **Alarm information** (name, description, level, scope, object and optionally mail-to recipients)
 - **Scope** determines on which nodes an alarm will be applied: any or specific exporter, interface, subnet, Subnet Set or Traffic Pattern.
 - **Object** determines what type of traffic will be matched against the alarm threshold criteria: total, interface, subnet, protocol, host, AS, conversation etc.
 - **Recipients list** (optional) determines to whom will an email be sent if the alarm triggers. **i** Only users with emails associated to their user account can be recipients.
3. Set **Alarm threshold**.
Threshold can be in flows, packets or bits. It is possible to combine more threshold criteria by using AND, OR and NOT logical operands.
4. Click **Save**

Adding New Netflow Alarm

Alarm information

Alarm name: High FB traffic

Description: Host with high FB traffic

Alarm level: NOTICE(5)

Scope: Traffic Pattern Facebook Traffic

Object: Host Any

Recipients: Winter Jon, Goldberg Dany

Alarm threshold

Match All + (+0)

bits/s total > 6000

Save Close

Figure above shows an example of an Alarm. This alarm triggers if any host in the network has more than 6 kbps of Facebook traffic in 5 minutes. Facebook traffic is identified via Facebook Traffic Pattern. On alarm trigger an email will be sent to Winter Jon and Goldberg Dany.

Understanding NetFlow System Traffic

System tab shows performance and system traffic for NetFlow module. Traffics available are:

- UDP packets collected
- Flows processed
- Performance metrics

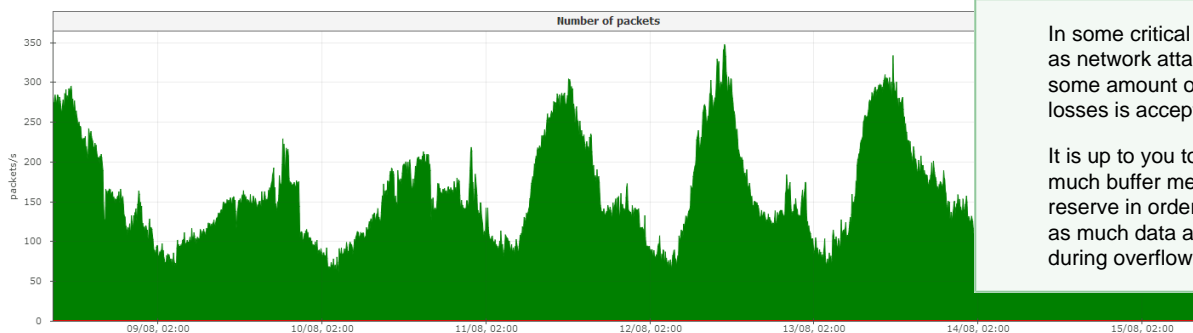
On this page:

- UDP Packet Collected
- Flows Processed
- Performance Metrics

UDP Packet Collected

UDP Packets show number of received and discarded packets. Viewing packet collection is useful for checking if your NetFlow Analyzer experienced some packet losses.

To access this view, go to **Top N > System > UDP Packets**.



In some critical events such as network attack, having some amount of packet losses is acceptable.

It is up to you to decide much buffer memory to reserve in order to collect as much data as possible during overflows.

Packets	Avg	Min	Max
Received	164.5 pps (100.0 %)	59.9 pps	347.1 pps
Discarded	0.0 pps (0.0 %)	0.0 pps	< 0.1 pps
Total	164.5 pps (100.0 %)	59.9 pps	347.1 pps

Discarded UDP packets mean that your buffer is full - some of the packets sent by exporters are not collected and will not be included as traffic information.

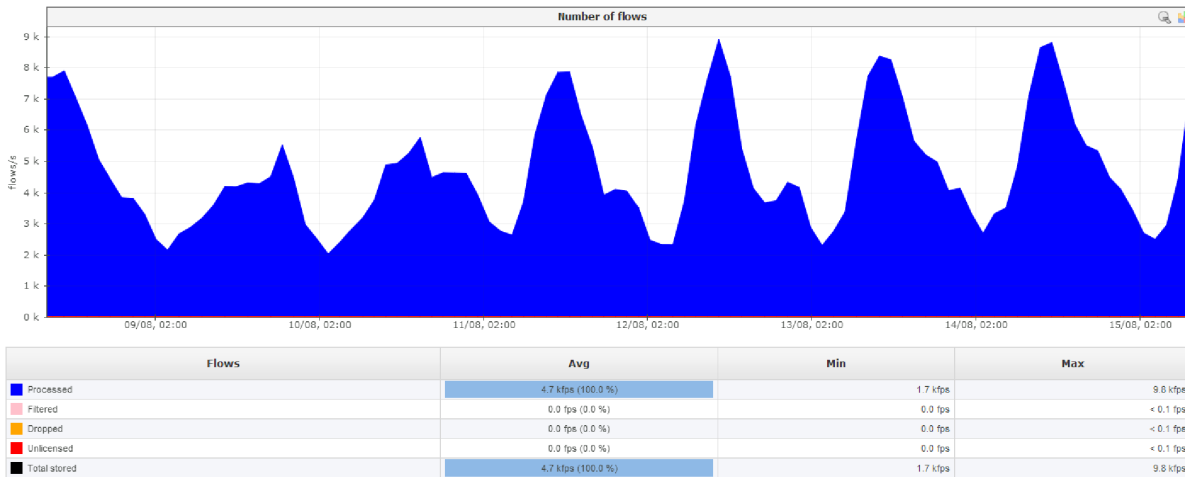
Flows Processed

Number of flows gives you statuses on the data processing.

Flows are categorized into:

- **Processed** - flows that are not filtered out, dropped or unlicensed
- **Filtered** - flows not processed due to filters set in Flow Settings > Aggregator Filtering
- **Dropped** - flows rejected due to full buffer
- **Unlicensed** - flows not processed due to license limitation
- **Total stored** - total number of flows received (processed + filtered + dropped)

To view flow processing, go to **Top N > System > Flows**.



Dropped flows mean that your buffer is full - some of the packets sent by exporters are not collected and will not be included as traffic information.

Unlicensed flows (dark red on the graph) mean that your network devices are exporting more flows than your license allows. These flows will not be processed by aggregator and, therefore, information provided by them will not be included when creating and displaying traffic. In this case, you should upgrade your license. Read more about [Upgrading License](#).

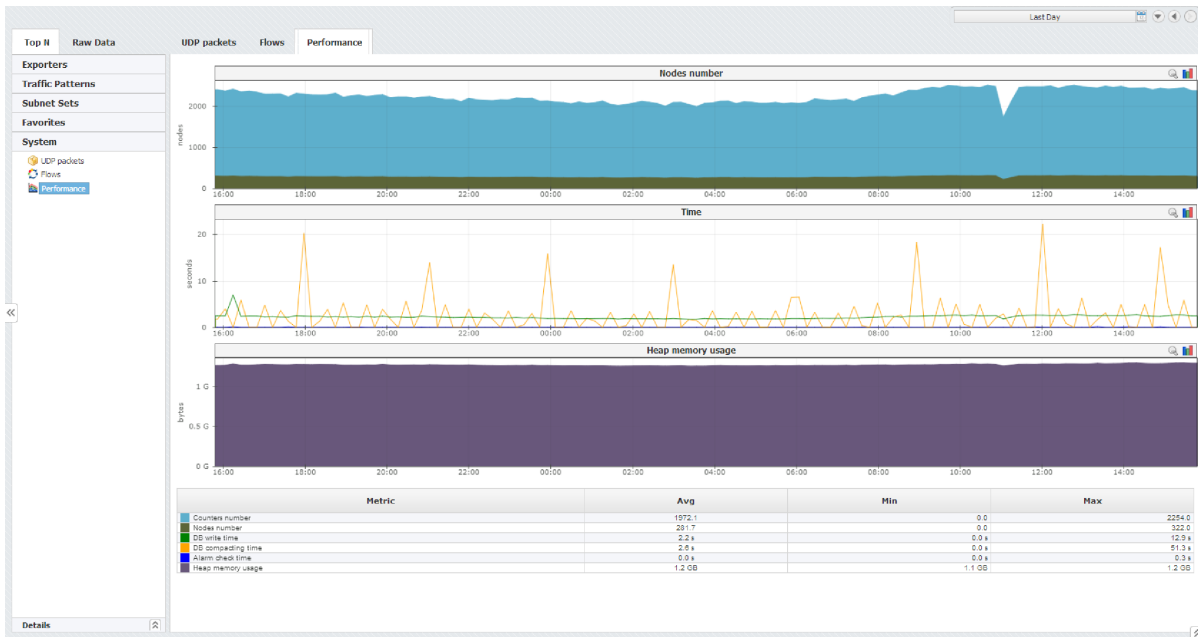
Performance Metrics

Within Performance overview you can see various metrics that show how efficient is your application.

Available metrics are:

- **Counters number** - number of traffic monitoring counters (AS traffic, Service traffic etc.)
- **Nodes number** - number of traffic monitoring nodes (exporters, interfaces, subnets, Traffic Patterns and Subnet Sets)
- **DB write time** - time spent on writing counters to the database
- **DB aggregation time** - time spent on compacting the database (creating grains)
- **Alarm check time** - time spent checking and triggering alarms
- **Heap memory use** - memory use after traffic is written to the database

If you have insufficient memory on the server remember to consult with our post-installation guide on how to assign RAM to NetFlow services (Tomcat and PostgreSQL).



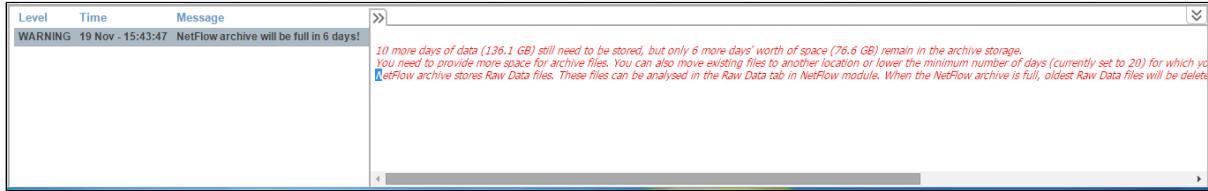
Keep an eye on the Heap memory and how it is affected by the increase in monitored nodes and counters (each time you add a node or create a TopN rule this numbers are modified).

Using Activity Log

Activity Log shows the list of active application notifications (error, system, license and other messages).

To view activity log, click on **Show log** arrow in the bottom right corner of the application.

One log includes information such as level, time, message and description.



Level	Time	Message
WARNING	19 Nov - 15:43:47	NetFlow archive will be full in 6 days! <i>10 more days of data (136.1 GB) still need to be stored, but only 6 more days' worth of space (76.6 GB) remain in the archive storage. You need to provide more space for archive files. You can also move existing files to another location or lower the minimum number of days (currently set to 20) for which you NetFlow archive stores Raw Data files. These files can be analysed in the Raw Data tab in NetFlow module. When the NetFlow archive is full, oldest Raw Data files will be deleted.</i>

EventLog Usage

In this chapter you will find out how to use EventLog module to see and analyze syslog and SNMP traps.

- [Viewing Syslog Messages](#)
- [Inspecting Syslogs](#)
- [Viewing SNMP Traps](#)
- [Understanding Eventlog System Traffic](#)
- [Using EventLog Alarms](#)
- [Syslog How to...](#)

Viewing Syslog Messages

To view syslog go to EventLog module and click Syslog tab. Here you can see syslog messages sent from different exporters for a chosen Time Window.

1. Show Options
2. EventLog Chart
3. Severity Table
4. Exporter Table
5. EventLog Table

On this page:

- Show Options
- Syslog Chart
- Severity Table
- Exporter Table
- Syslog Table

Table and charts will show logs that have (1) the same severity as set in Severity Table (2) for the time set in Time Window. For these logs Exporter table will show distribution by exporters and Severity Table will show distribution by log's severity.



For example, on the screenshot to the left, you can see that logs that occurred during the selected Time Window and severity 0 to 5 are shown. You can also see that there was 523,918 such logs (Severity Table) of which most numerous were Warnings (55%) and Errors (29%).

You can also see the distribution of these logs by exporters in the Exporter table: exporter x.x.6.201 generated the most logs (139,130).

Show Options

Show Options:

1. Refresh Data – manually refresh data on charts and tables
2. Clear filters – clear all filters
3. Show Exporter Names – show names of exporters (routers) instead of their IP address

Syslog Chart

EventLog Chart shows distribution of syslog messages (logs) by severity:

1. Logs per bar (y-axis)
2. Time axis (x-axis)
3. Bar width
4. Zoom out

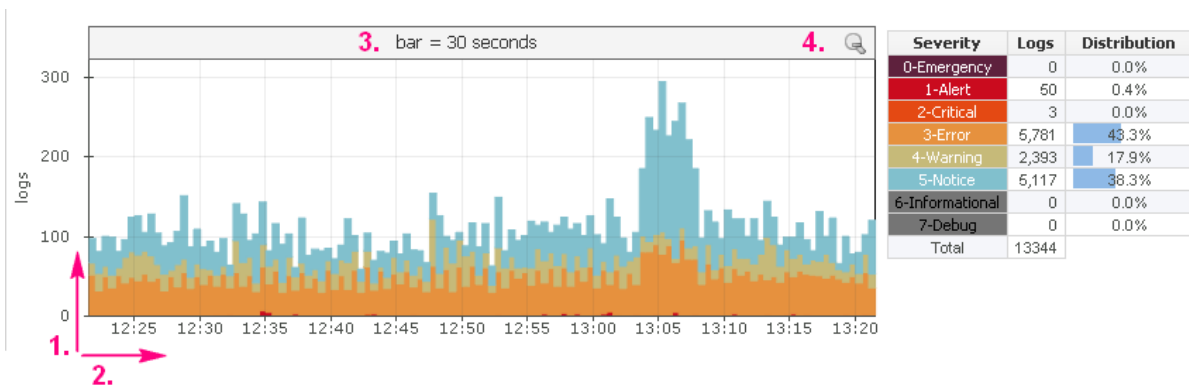


Chart shows number of logs in certain time chunks (1 minute, 1 day, 1 hour). Width of the chart bars and number of bars depends on the Time Window selected. See table below:

Time Window	Bar Width	Number of Bars
Last hour	30 seconds	120
Last 6 hours	5 minutes	72
Last 12 hours	5 minutes	144
Last day	15 minutes	96
Last week	1 hour	168
Last month	6 hours	120

Chart has two axis: numerical y-axis and time x-axis. Numerical axis shows the number of logs per bar. Time shown on the x-axis of the chart is the same time as set in the Time Window. Next to the Syslog Chart is the Severity Table in which you can select if syslog messages of the certain severity will be displayed on the chart or not. Colors on the chart correspond with the colors of the syslog Severity in the Severity Table.

On the EventLog Chart above you can see that one bar on the chart represents logs during 30 seconds (bar = 30 seconds).

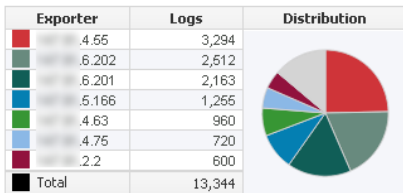
Severity Table

Severity Table shows log distribution by severity, for the logs of selected severity that occurred in the selected Time Window. On screenshot to the right currently selected severity levels are 0, 1, 2 and 3. This means that Syslog chart and tables will show only logs with this severity levels. By clicking on the corresponding severity in the Severity Table you can switch on/off logs of that severity. Switched off severity is shown with a gray background and logs with that severity are not shown on the carts and graphs.

Severity	Logs	Distribution
0-Emergency	0	0.0%
1-Alert	959	1.3%
2-Critical	39	0.1%
3-Error	71,679	98.6%
4-Warning	0	0.0%
5-Notice	0	0.0%
6-Informational	0	0.0%
7-Debug	0	0.0%
Total	72,677	

Exporter Table

Exporter Table shows log distribution by exporter, for the logs of selected severity that occurred in the selected Time Window. Top 7 exporters have a color assigned, while other exporters are grey and under Others on the pie chart. To see other exporters, scroll down the exporter list.



Clicking on an exporter will show only logs for that exporter on the charts and table. By clicking on it again, you can switch back to seeing logs for all exporters.

Syslog Table

EventLog Table shows messages with selected severity (in Severity Table) that were received during time set in the Time Window. For each message Date, Exporter, Severity, Facility and Message content is displayed. Severity levels are shown with the corresponding color, as in the chart and Severity Table. 9/19 Figure 7: Exporter Table Figure 6: Severity Table Syslog Table can be filtered by Exporter, Severity, Facility and Message content. Note that the filters can be activated by selecting items in the Severity and Exporter Tables, as described above. To clear all filters, click the Clear button above the Syslog chart. To show exporter DNS names, click the Show Names button above the Syslog chart.

Date	Exporter	Severity	Facility	Message
Jul 29 2013, 18:16:19.288	7.106, 4.75	0,1,2,3,4,5		
Jul 29 2013, 18:16:17.464	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Connection closed: 11468 bytes sent to SSL, 138 bytes sent to socket
Jul 29 2013, 18:16:14.246	7.106	4 - Warning	23 - Local Use 7	1379813: Jul 29 18:16:16: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from .10.6, Vlan76
Jul 29 2013, 18:16:14.244	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Post check: verification level is low, skipping check
Jul 29 2013, 18:16:07.465	7.106	4 - Warning	23 - Local Use 7	1379812: Jul 29 18:16:06: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from .10.6, Vlan76
Jul 29 2013, 18:15:57.465	7.106	4 - Warning	23 - Local Use 7	1379811: Jul 29 18:15:56: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from .10.6, Vlan76
Jul 29 2013, 18:15:47.472	7.106	4 - Warning	23 - Local Use 7	1379810: Jul 29 18:15:46: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from .10.6, Vlan76
Jul 29 2013, 18:15:44.231	4.75	3 - Error	10 - Security/Authorization	stunnel: LOG3[7582:3072637840]: SSL_read: Connection reset by peer (104)
Jul 29 2013, 18:15:44.231	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Connection reset: 11425 bytes sent to SSL, 138 bytes sent to socket
Jul 29 2013, 18:15:44.181	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG5[7582:3072637840]: Post check: verification level is low, skipping check

Page 1

Inspecting Syslogs

You can filter out unwanted logs based on log's severity, exporter, facility, date and time, and message content.

NetVizura EventLog has three main types of syslog filters:

- quick filters: severity and exporters
- table filters
- time filters (Time Window)

Quick filters are activated/deactivated by clicking on the corresponding severity in the Severity Table, or clicking on the corresponding exporter in the Exporter table. Inactive severity/exporters are marked with gray color, while active severity/exporters are colored. Logs from inactive exporters and logs with inactive severity levels are not shown in the charts and tables, and are not counted in the on-screen statistics.

Activating/deactivating severity or exporter filters will:

- update Syslog Table filters for the corresponding exporter or severity level
- refresh charts and Syslog Table,
- refresh statistics in the Exporter Table and Severity Table

Note: Filters and data in Syslog Table, Exporter Table, Severity table always match each other.

Figure 10: Using filters in Syslog Table shows Syslog Table and Severity Table, and you can see that the Severity filter in the table matches the active (colored) severity levels in the Severity Table.

Table filters are used to filter syslog messages by log's severity, exporter, facility and message text body. To activate or change a filter simple type the value in the corresponding filter text field and press Enter. This will update the data on all chats and tables.

Note: Multiple filter values are separated by commas.

To filter out the logs based on the time and date, change the Time Window value by clicking on it and (1) choosing a value from the drop menu or (2) selecting from and to dates in the calendar. Updating the Time Window will update the data on all chats and tables.

Viewing SNMP Traps

To view SNMP Traps go to EventLog module and click SNMP Trap tab. Here you can see SNMP Trap messages sent from different exporters for a chosen Time Window. Up to 30 traps will be shown per page.

Data shown:

- Date
- Exporter
- Trap OID
- Trap details
- Alarms

You can resolve OID and exporter IP names by clicking on the "Show names" button above Trap table, as shown in the screenshot below. Exporter names are resolved via DNS, and OID names are resolved by extracting data from the MIB modules.

Trap details column contains information about variable bindings for each trap message.

Hovering over any OID in Trap OID and Trap Details columns will display that OID's description in a tool-tip.

If OIDs are not resolved, add the corresponding MIB module for that OID in Settings > MIB Settings > Modules.

Date	Exporter	Trap OID	
Oct 23 2015, 07:34:22.354		1.3.6.1.6.3.1.1.5.4	1.3.6.1.2.1.1.3.0 = 278 days, 10:44:14 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.1! 1.3.6.1.2.1.2.2.1.1.86 = 86 1.3.6.1.2.1.2.2.1.2.86 = Tunnel330 1.3.6.1.2.1.2.2.1.3.86 = 131 1.3.6.1.4.1.9.2.2.1.1.20.86 = Tunnel U
Oct 23 2015, 07:34:20.267		1.3.6.1.6.3.1.1.5.4	1.3.6.1.2.1.1.3.0 = 278 days, 10:27:26 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.1! 1.3.6.1.2.1.2.2.1.1.86 = 86 1.3.6.1.2.1.2.2.1.2.86 = Tunnel330 1.3.6.1.2.1.2.2.1.3.86 = 131

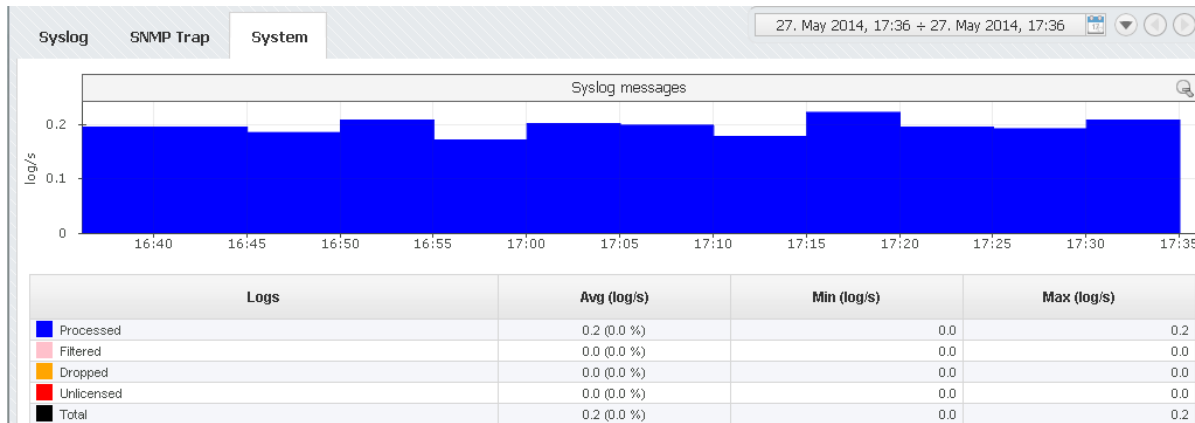
Date	Exporter	Trap OID	
15, 07:34:22.354		linkUp	ifIndex.86 = 86 ifType.86 = 131 ifDescr.86 = Tunnel330 sysUpTime.0 = 278 days, 10:44:14.77
15, 07:34:20.267		linkUp	ifDescr.86 = Tunnel330 snmpTrapOID.0 = 1.3.6.1.6.3.1.1.5.4 locIfReason.86 = Tunnel Up

A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and ...

Understanding Eventlog System Traffic

To view NetVizura EventLog system state, click System tab while in View Mode.

System tab shows NetVizura EventLog system traffic. Tab is organized in two sections: Syslog and SNMP Trap. Each section has a chart and a corresponding table as shown on the Figure 11: System tab - Syslog messages.



Syslog messages:

- Processed - logs processed by the service
- Filtered - logs rejected by the service due to filtering
- Dropped - logs dropped by the service due to high load
- Unlicensed - obfuscated logs due to license limitations

Logs sent to NetVizura server are put in the buffer before processing. Logs are taken from the buffer and matched against the license and Syslog filters. If the the number syslog exporters exceeds the license limit - the log's message will be obfuscated (Unlicensed logs). If a filter marks a log to be reject it will be not be stored or processed (filtered logs). If the buffer is full (to many logs are being sent), incoming packets will not be stored or processed (Dropped logs). Logs that are not dropped, obfuscated or filtered are counted as Processed log.

To manage your Syslog filters, go to Settings > EventLog Settings > Syslog filtering. To learn more about Syslog filters, go to

SNMP Trap messages:

- Processed - traps processed by the service
- Filtered – traps rejected by the service due to filtering
- Unlicensed - obfuscated logs due to license limitations

Traps sent to NetVizura server are forwarded to SNMP4J library. Traps are matched against the license and SNMP Trap filters. If the the number trap exporters exceeds the license limit - the trap's message will be obfuscated (Unlicensed traps). If a filter marks a trap to be reject it will be not be stored or processed (Filtered traps). Traps that are not obfuscated or filtered are counted as Processed traps.

To manage your SNMP Trap filters, go to Settings > EventLog Settings > SNMP Trap filtering.

Using EventLog Alarms

You can setup alarms to trigger if a specific condition is met on a syslog or trap message:

- For Syslogs, threshold is based on source IP, severity, facility and message content
 - For SNMP traps, threshold is based on source IP, OID and variable bindings.
- i** It is possible to combine more threshold criteria (AND logical operand is implied).

On this page:

- Viewing All Alarms (Alarm Module)
- Creating EventLog Alarms

Each alarm has its severity and you can override the severity of the syslog alarm. This is useful if the default severity of a syslog does not correspond to alarm severity. For example, a fan is malfunctioning in the data center. Usually, syslog for this event will have a severity warning, but in this case data center is critical so it is wise to set the alarm severity higher.

Viewing All Alarms (Alarm Module)

To view all EventLog alarms, go to **Alarm Module**.

#	Severity	Occurrences	Start	End	Duration	Module	Alarm	Source	Exporter	Message
(461)	1-Alert		Dec 04, 16:29:32	Dec 05, 15:35:53	-	EventLog	Test Auth	SYSLOG-EXPORTER(147.91.7.1)-SEVERITY(3)	147.91.7.1	necu description !
(1)	4-Warning		Dec 05, 15:26:17	Dec 05, 15:26:17	00:00:00	EventLog	Auth. warning	SYSLOG-EXPORTER(147.91.7.65)-SEVERITY(3)	147.91.7.65	Authentication failure warning for 147.91.7.65
(7)	0-Emergency		Dec 05, 15:23:06	Dec 05, 15:23:08	-	EventLog	Test trap alarma	SNMP_TRAP-EXPORTER(172.16.2.36)	172.16.2.36	Test trap alarma
(7)	0-Emergency		Dec 05, 15:23:08	Dec 05, 15:23:08	00:00:01	EventLog	Test trap alarma	SNMP_TRAP-EXPORTER(172.16.2.36)	172.16.2.36	Test trap alarma
(32)	0-Emergency		Dec 05, 13:33:20	Dec 05, 13:30:56	-	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:38:56	Dec 05, 13:38:56	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(4)	0-Emergency		Dec 05, 13:38:02	Dec 05, 13:38:12	00:00:10	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:37:27	Dec 05, 13:37:27	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(3)	0-Emergency		Dec 05, 13:37:20	Dec 05, 13:37:24	00:00:04	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(2)	0-Emergency		Dec 05, 13:36:43	Dec 05, 13:36:45	00:00:03	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:36:31	Dec 05, 13:36:31	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(3)	0-Emergency		Dec 05, 13:36:13	Dec 05, 13:36:20	00:00:07	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:35:56	Dec 05, 13:35:56	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(4)	0-Emergency		Dec 05, 13:35:12	Dec 05, 13:35:20	00:00:08	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(2)	0-Emergency		Dec 05, 13:35:01	Dec 05, 13:35:11	00:00:10	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(4)	0-Emergency		Dec 05, 13:34:20	Dec 05, 13:34:26	00:00:06	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:34:00	Dec 05, 13:34:00	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(4)	0-Emergency		Dec 05, 13:33:42	Dec 05, 13:33:47	00:00:05	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:33:31	Dec 05, 13:33:31	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic
(1)	0-Emergency		Dec 05, 13:33:20	Dec 05, 13:33:20	00:00:00	EventLog	Testni alarmic	SYSLOG-EXPORTER(147.91.1.39)-SEVERITY(8)	147.91.1.39	Testni alarmic

Here you can see the list of all alarms that occurred within the selected time period. In our case, we can see Auth. warning alarm that we previously defined in Settings.

Occurrence indicators visualize approximate time (withing selected time window) when alarm occurred.

You are also able to filter, sort alarms and view only active alarms according to your need.

Creating EventLog Alarms

To add a new alarm in EventLog:

1. Click **Add**
2. Set **Alarm information** (type, name, description and level)
3. Set **Alarm threshold**

- i** For Syslogs, threshold is based on source IP, severity, facility and message content
- i** For SNMP traps, threshold is based on source IP, OID and variable bindings.
- i** It is possible to combine more threshold criteria (AND logical operand is implied).

If you do not define a value to a certain criterion, that criterion will not be included in the Alarm condition.

Syslog filtering **SNMP Trap filtering** **Alarms** **Configuration**

Adding New Eventlog Alarm

Alarm information

Alarm type: Syslog SNMP Trap

Alarm name:

Description:

Alarm level:

Save Close

Alarm threshold

Source IP:

Severity:

Facility:

Message contains:

Screenshot above shows an example of an Alarm configuration. This alarms will trigger if syslog message is sent from 147.91.7.65, with severity level 3 and message containing Authentication failure.

Syslog How to...

See logs for a specific device only

Click on the device name or IP address in the Exporter Table or type the device's IP address in the Exporter filter in the Syslog Table (text field under the Exporter column).

See logs for specific devices (more than one)

Type the IP addresses of the specific devices in the Exporter filter in the Syslog Table (text field under the Exporter column) separated by comma.

See logs for all exporters

Click on the Total in the Exporter Table or clear the Exporter filter in the Syslog Table (text field under the Exporter column).

See logs of specific severity level

Click on the wanted severity level in the Severity Table to make it active (colored), click on the unwanted active severity levels to switch them off (they will turn gray); or, type the severity number in the Severity filter in the Syslog Table (text field under the Severity column). Multiple severity numbers must be separated by comma.

See logs with all severity levels

Clear the Severity filter in the Syslog Table (text field under the Severity column); or, click on the inactive severity levels (gray) in the Severity table to make them active.

Set default severity levels shown

Go to Settings > EventLog Settings > Configuration and under Service options set the Maximum Severity Level Shown parameter. For example, if the parameter is set to 3, shown severity levels will be 0, 1, 2, and 3.

Erase all filters quickly

Click on the Clear button above the Syslog chart.

See logs with specific facility

Type the facility number or name in the Facility filter in the Syslog Table (text field under the Facility column).

See logs that contain specific text in the message text body

Type the specific text in the Message filter in the Syslog Table (text field under the Messages column).

Filter out unwanted logs

Go to Settings > EventLog Settings > Syslog Filters and make your filter. To learn more on making filters, go to chapter Error: Reference source not found Error: Reference source not found on page Error: Reference source not found.

Set the collection port for syslog messages

Go to Settings > EventLog Settings > Configuration and set the Syslog socket port parameter.

Change database settings

Go to Settings > EventLog Settings > Configuration and set the database maintenance

parameters. To learn more on database maintenance configuration, go to chapter Error: Reference source not found Error: Reference source not found, Error: Reference source not foundError: Reference source not foundError: Reference source not foundError: Reference source not found on page Error: Reference source not found.

See my license details

Click on the Settings and Configuration icon (gear wheel, upper right corner of the screen) and choose About.

MIB Usage

In this chapter you will find out how to use MIB module to see browse the MIB tree and get OID values from your devices.

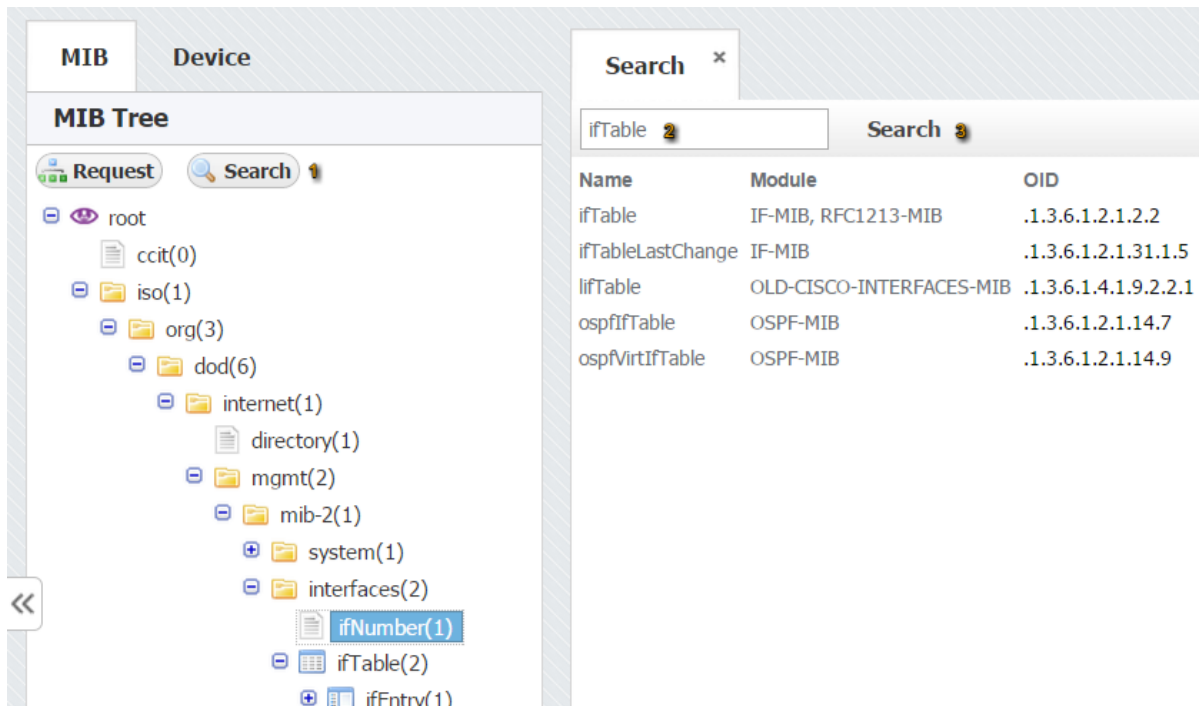
- [Searching OIDs](#)
- [Setting a Current Device](#)
- [Making SNMP Request](#)
- [Managing MIB Favorites](#)
- [Reading MIB Details](#)

Searching OIDs

To find a specific OID in the MIB Tree:

1. Click Search in the MIB Tree
2. Type the name (full or partial) or OID number in the text field of the Search tab
3. Press Enter or click Search in the Search tab

The search results will be shown in the Search tab. Name, (MIB) Module and OID number are shown for each OID found. Clicking on an OID in the Search tab will select it in the MIB tree.



The screenshot displays the MIB Tree and Search interface. The MIB Tree on the left shows a hierarchical structure with 'ifNumber(1)' selected. The Search tab on the right shows a search for 'ifTable' with results for 'ifTable', 'ifTableLastChange', 'lifTable', 'ospfIfTable', and 'ospfVirtIfTable'.

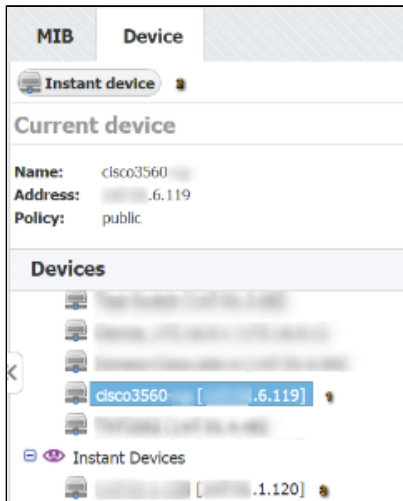
Name	Module	OID
ifTable	IF-MIB, RFC1213-MIB	.1.3.6.1.2.1.2.2
ifTableLastChange	IF-MIB	.1.3.6.1.2.1.31.1.5
lifTable	OLD-CISCO-INTERFACES-MIB	.1.3.6.1.4.1.9.2.2.1
ospfIfTable	OSPF-MIB	.1.3.6.1.2.1.14.7
ospfVirtIfTable	OSPF-MIB	.1.3.6.1.2.1.14.9

By default, up to 50 OIDs will be shown. To change the maximum number of OIDs shown, go to **Settings > MIB Settings > Configuration** and change the **Search results** parameter.

Setting a Current Device

Current device is a device to which the SNMP requests are sent. You can set a Current device by:

1. Selecting a device from the application database
2. Adding Instant device
3. Selecting previously added Instant device



To select a device from the application database, simply select it from the DB devices list in the Device Tab (1). If the device you want is not in this list you can create it by going to Settings > MIB Settings > Devices. For more information on adding a device, go to article [Configuring Devices](#).

Alternately, you can create an instant device by clicking the Instant device button (2). You need to enter IP address and SNMP community string. Instant devices have SNMPv2c and SNMP port 161.

All instant devices you add will be added to the Instant device list (3).

Instant devices will not be saved to application database and they will be cleared after you log out. Current device is displayed in the Device in Use section of the Device panel.

Making SNMP Request

To request SNMP query:

1. Select the desired OID
2. Click **Request**

On this page:

- Table Request
- List requests
- OID Value Setting

index	ifIndex	ifDescr	ifType
.1	1	GigabitEthernet0/1	ethernetCsmacd(6)
.2	2	GigabitEthernet0/2	ethernetCsmacd(6)
.3	3	GigabitEthernet0/3	ethernetCsmacd(6)
.4	4	GigabitEthernet0/4	ethernetCsmacd(6)
.5	5	GigabitEthernet0/5	ethernetCsmacd(6)
.6	6	GigabitEthernet0/6	ethernetCsmacd(6)
.7	7	GigabitEthernet0/7	ethernetCsmacd(6)
.8	8	GigabitEthernet0/8	ethernetCsmacd(6)
.9	9	GigabitEthernet0/9	ethernetCsmacd(6)
.10	10	GigabitEthernet0/10	ethernetCsmacd(6)
.11	11	GigabitEthernet0/11	ethernetCsmacd(6)
.12	12	GigabitEthernet0/12	ethernetCsmacd(6)
.13	13	Null0	other(1)
.14	14	Vlan1	propVirtual(53)
.15	15	Loopback0	softwareLoopback(24)

Result will display in the main panel (3) in a new tab. Title of the tab will be the OID name and it will contain the device to which the SNMP request was sent to (the Current device).

On the screenshot we can see that SNMP query was sent to device cisco3550-xx (3) for the ifTable.

If there is no Current device set, the application will prompt you to enter an instant device. You can request the SNMP query from MIB tree or Favorites.

OID values returned by the SNMP request can be displayed as a list (OIDs and their values) or table, depending on the type of the selected node in the MIB Tree.

MIB tree node types as shown in the screenshot to the left:

1. Folder – returns a list of OIDs
2. Leaf – returns a single OID
3. Table – returns OIDs organized into table
4. Table header - returns a list of OIDs

Table Request

An example of SNMP query result table is shown on figure below. SNMP table contains name and value for each OID corresponding with the same index. SNMP table has the following information and options:

1. Title – shows the MIB requested
2. Device – shows the device that returned the table (Current device)
3. Settable OIDs (marked in blue)
4. Pivot – pivoting the table
5. Next/Refresh – next table page / refresh

index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts
.1	1	GigabitEthernet0/1	ethernetCsmacd(6)	1500	1000000000	00:11:5c:82:96:00	up(1)	up(1)	4 days, 5:58:37.47	2505601206	156161969
.2	2	GigabitEthernet0/2	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:02	up(1)	down(2)	0:01:43.51	0	0
.3	3	GigabitEthernet0/3	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:03	up(1)	down(2)	0:01:43.51	0	0
.4	4	GigabitEthernet0/4	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:04	up(1)	down(2)	0:01:43.51	0	0
.5	5	GigabitEthernet0/5	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:05	up(1)	down(2)	0:01:43.51	0	0
.6	6	GigabitEthernet0/6	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:06	up(1)	down(2)	0:01:43.51	0	0
.7	7	GigabitEthernet0/7	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:07	up(1)	down(2)	0:01:43.51	0	0
.8	8	GigabitEthernet0/8	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:08	up(1)	down(2)	0:01:43.51	0	0
.9	9	GigabitEthernet0/9	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:09	up(1)	down(2)	0:01:43.51	0	0
.10	10	GigabitEthernet0/10	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:0a	up(1)	down(2)	0:01:43.51	0	0
.11	11	GigabitEthernet0/11	ethernetCsmacd(6)	1500	10000000	00:11:5c:82:96:0b	up(1)	down(2)	0:01:43.51	0	0
.12	12	GigabitEthernet0/12	ethernetCsmacd(6)	1500	1000000000	00:11:5c:82:96:0c	up(1)	up(1)	0:01:49.21	239706110	150591690
.13	13	Null0	other(1)	1500	4294967295		up(1)	up(1)	0:00:20.27	0	0
.14	14	Vlan1	propVirtual(53)	1500	1000000000	00:11:5c:82:96:00	up(1)	up(1)	0:02:17.21	10531848	80212
.15	15	Loopback0	softwareLoopback(24)	1514	4294967295		up(1)	up(1)	0:01:43.91	0	0

The table will show up to 100 rows by default. If the table has more rows, the Next option will be displayed. Click next to get next 100 rows.

Refresh option will show if there is less than 100 rows, or you reached the last page of the table (after clicking Next). Click Refresh to send the SNMP request again.

To change the maximum number of rows displayed, go to **Settings > MIB Settings > Configuration** and change the **Table response limit** parameter.

List requests

Examples of list requests are shown on screenshot below:

The screenshot shows a network management interface. On the left, the 'MIB Tree' is expanded to 'interfaces(2)'. Below it, 'Favorites' shows details for 'ifEntry(1)'. The main area displays a table for 'interfaces' on a 'cisco3550' device. The table has two columns: 'oid' and 'value'. The 'oid' column lists interface indices from ifIndex.0 to ifIndex.15. The 'value' column lists interface descriptions from GigabitEthernet0/1 to GigabitEthernet0/6. A pop-up window shows a detailed view of the 'ifNumber' entry, listing 'oid' and 'value' for ifNumber.0 to ifNumber.7.

The list will show up to 50 rows by default. If the list has more rows, the Next option will be displayed. Click next to get next 50 rows.

Refresh option will show if there is less than 50 rows, or you reached the last page of the list (after clicking Next). Click Refresh to send the SNMP request again.

To change the maximum number of rows displayed, go to **Settings > MIB Settings > Configuration** and change the **List response limit** parameter.

OID Value Setting

You can set an OID value if it is marked in blue in the table returned by the SNMP request. To set the OID value:

1. Click on the OID value
2. Select an OID value or type a value
3. Click OK

ifTable ×					
cisco3550-mnt				Pivot	Refresh
ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOct
1000000000	00:11:5c:82:96:00	up(1)	up(1)	4 days, 5:58:37.54	2598228
10000000	00:11:5c:82:96:02	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:03	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:04	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:05	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:06	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:07	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:08	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:09	up(1)	down(2)	0:01:43.58	
10000000	00:11:5c:82:96:0a	up(1)	down(2)	0:01:43.58	

Select value

up(1) ▾

OK Cancel

To set an OID value and SNMP SET change to be successful on a device, you need to have:

1. WRITE or ADMIN permission for MIB module
2. READ_WRITE access level on device's SNMP policy
3. Enabled device remote SNMP setting

Managing MIB Favorites

To access Favorites click on the **MIB** tab and then click on **Favorites**.

On this page:

- Favorite OIDs
- Adding OID to Favorites
- Removing OID from Favorites

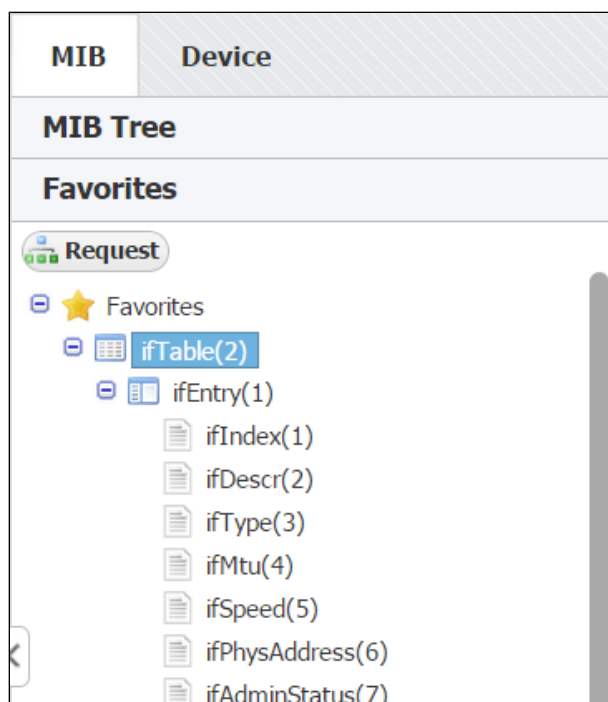
Favorite OIDs

You can access you favorite OID from the Favorites. To request a SNMP Query on the Current device:

1. Select on the desired OID in the Favorites tree
2. Click Request

Result will display in the main panel in a new tab. Title of the tab will be the OID name and it will contain the device to which the SNMP request was sent to (the Current device).

If there is no Current device set, the application will prompt you to enter an instant device.



An example of Favorites are shown on the screenshot. The Favorites shown are the result of adding IfTable to favorites.

we can see that the Favorites are organized hierarchically like the MIB tree.

Adding OID to Favorites

To add an OID to Favorites right-click on it in the MIB Tree and select **Add to Favorites**.

When you add an OID to Favorites you add every OID contained in branch of the MIB tree that starts with that OID, too. On the screenshot above we see that adding the ifTable also added ifEntry, and its belonging ifIndex, ifDescr, etc.

Adding a Favorite will add that OID to your Favorites list only, it will not affect the Favorites list of other users.

Removing OID from Favorites

To remove an OID from Favorites right-click on it in the Favorites Tree and select **Remove from Favorites**.

When you remove an OID from Favorites you remove entire branch of MIB tree that starts with that OID. For example, on screenshot above removing ifTable from Favorites also removes ifEntry, and its belonging nodes ifIndex, ifDescr, etc.

Removing a Favorite will remove that OID from your Favorites list only, it will not affect the Favorites list of other users.

Reading MIB Details

Details panel shows more information for the OID selected in the MIB Tree or Favorites. Information shown depends on the type of the MIB tree node type.

On the figure below we can see the details for ifTable: Name, OID number, Status, Access, Value Type and Description.

Details	
Type	Object
Name	ifTable
OID	.1.3.6.1.2.1.2.2
Status	mandatory
Access	not-accessible
Value Type	SEQUENCE OF ifEntry
Description	A list of interface entries. The

To hide the details panel, click on the double arrow icon in the top right corner of the Details panel.

Configuration

This chapter covers NetVizura configuration. Articals are grouped in:

- General Configuration
- NetFlow Configuration
- EventLog Configuration
- MIB Configuration

General Configuration

In this chapter you will learn how to configure NetVizura:

- [Managing Users](#)
- [Configuring SNMP Policies](#)
- [Configuring Devices](#)
- [Managing License](#)
- [Configuring E-Mail](#)
- [Configuring Display Names](#)
- [Configuring Time Window](#)

Note: For some configuration administrator privileges are needed.

Managing Users

Administrator can view, add, edit, delete users and set their permissions.

To manage users accounts, go to **Settings > Control Panel > Users**.

Name	Username	E-mail	Address	Phone	Mobile	Status	Action
Guest, Guest	guest	guest@domain.com				Active	
User, User	User	user@domain.com				Active	
Admin, Admin	admin	admin@domain.com				Active	

Page 1 of 1

There are three user types:

- **Guest** - shared account
- **User** - normal user
- **Admin** - administrator (can view system tab and Raw Data, manage license, users etc.)

Permissions for specific application features depend on the selected user type:

Feature / User	My Account	Favorites	Control Panel	Module permissions	View System tab	Change Display Names	Change Time-Window
Guest	Read	None	None	None/Read	No	No	No
User	Write	Write	None	None/Read/Write	No	No	Yes
Admin	Write	Write	Write	None/Read/Write	Yes	Yes	Yes

- Selection of User Type implies pre-defined permissions for My Account, Favorites, System tabs, Control Panel, Display Names and Time-Window.
- Control Panel manages users, license, email settings, etc.
- Permissions for Modules are allowed for custom selection.

Module permissions are used to choose user's privilege level for a specific module.

For all modules in general:

- **None** - user can not view module and its Settings
- **Read** - user can view module and its Settings
- **Write** - user can view module and edit its Settings

For NetFlow module specifically:

- **Read** - user can also schedule Reports and view Report Settings
- **Write** - user can also view Raw Data, edit Report Settings, view End Users and edit End User Settings

To add a new user:


1. Click **+Add**
2. Insert user's **Login and Contact Information** into appropriate fields
3. Choose the **Permissions** from the drop-down lists
4. Click **Save**.

Info

- First name, Last name, Username and Password are mandatory fields.
- Email is needed for receiving emails (alarms and system emails).
- Administrators (user type admin) will receive system critical alarms and warnings via email.

To change an existing user:

1. Select desired user from the User table
2. Click **Edit** (pen icon)
3. Change **Login or Contact Information** text in the desired fields
4. Change **Permissions** level in the drop-down lists, if needed.
5. Click **Save** to apply changes.

 Username can not be changed once the user is added.

To remove a user:

1. Select a user from the User table
2. Click **Remove** (-).
3. Click **Yes** to confirm removal.

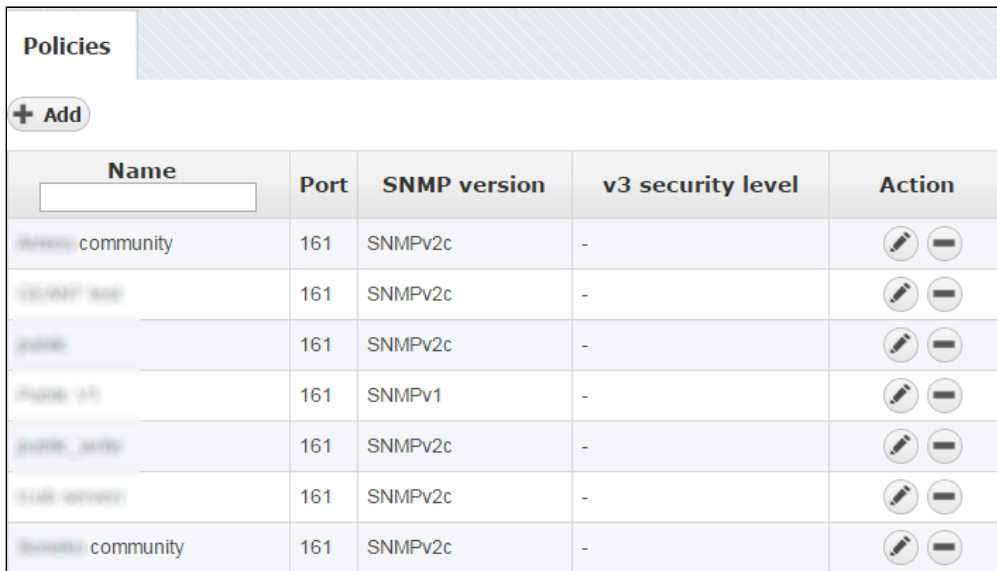
Configuring SNMP Policies















Policies are used for discovery of devices in Traffic Statistics (exporters and interfaces) for NetFlow Analyzer module and sending SNMP requests to devices in MIB Browser module etc.

Policy for a certain device in NetVizura has to match that actual SNMP configuration of that device in order for to get SNMP reports for particular MIB or OID for that device.

Administrator can view, add, edit or delete SNMP policies.

To access Policies, go to **Settings > Control Panel > SNMP Policies**.



Name	Port	SNMP version	v3 security level	Action
community	161	SNMPv2c	-	 
community	161	SNMPv2c	-	 
community	161	SNMPv2c	-	 
community	161	SNMPv1	-	 
community	161	SNMPv2c	-	 
community	161	SNMPv2c	-	 
community	161	SNMPv2c	-	 

On the screenshot to the left we can see Policy table together with some policy examples. As you can see, table shows basic policy parameters:

1. Name
2. Port
3. SNMP version
4. v3 security level

Looking at the first policy “community” we can see that the port used for SNMP is 161, and that SNMP version is v2c. Naturally, since it is v2c there are no associated v3 security levels.

Adding a SNMP Policy

To Add a new policy, click the **+ Add** button at the top of the Policy table.

Editing a SNMP Policy

To edit a policy, click on the pen (edit icon) or double click on the policy table row.

Policies

Editing policy *Access* community

Name:	<input type="text" value="Access community"/>	Username:	<input type="text" value="Access@192.168.1.1"/>	SNMPv3 options
Port:	<input type="text" value="161"/>	Security level:	<input type="text" value="AUTH_PRIV"/>	
Timeout (milliseconds):	<input type="text" value="1000"/>	Authentication protocol:	<input type="text" value="SHA"/>	
Retries:	<input type="text" value="1"/>	Authentication password:	<input type="text" value="*****"/>	
Repeaters:	<input type="text" value="20"/>	Privacy protocol:	<input type="text" value="DES"/>	
SNMP version:	<input type="text" value="SNMPv3"/>	Privacy passphrase:	<input type="text" value="*****"/>	
Access level:	<input type="text" value="READ"/>			

Available policy parameters are: Name, Port, Timeout, Retries, Repeaters, SNMP version, Access level, Username and SNMPv3 security level options (authentication protocol and password, privacy protocol and password).

SNMPv3 security level options are only visible if SNMP version is set to SNMPv3.

When an SNMP request is sent to a device associated with a protocol the request will be sent to the policy UDP port using the policy username as SNMP community and version. In order for request to be successful the policy has to match the SNMP configuration of the target device.

Successful request will result in a number of packets each containing a number of OIDs set by the Repeaters parameter (this is a number of SNMP request repeats in one SNMP Query). If the request is unsuccessful, there will be a number of retries (Retries parameter) with a certain timeout between each request based on the Timeout parameter (timeout incrementally grows after each request).

In the example shown in the screenshot above the SNMP request in view mode will result in a SNMPv3 request to a device on UDP port 161 with the above set security parameters. If the device doesn't reply, there will be one more retry after 1000ms.

Removing a SNMP Policy

To remove a policy, click - (remove icon) in the Action column.

Configuring Devices

To access Devices, go to **Settings > Control Panel > Devices**.

Name	IP	Port	SNMP policy	SNMP version	Action
CISCO7201-xx	192.168.6.114	161	community	SNMPv2c	
cisco2950g-xx	192.168.3.84	161	public	SNMPv2c	
cisco3550-xx	192.168.0.107	161	public	SNMPv2c	
cisco3560-xx	192.168.6.119	161	public	SNMPv2c	
cisco3560-xx	192.168.6.117	161	public	SNMPv2c	
CISCO7201-xx	192.168.3.13.92	161	community	SNMPv2c	
Device_192.168.215.125	192.168.215.125	-	-	-	
Device_192.168.29.245	192.168.29.245	-	-	-	
Device_192.168.3.130	192.168.3.130	-	-	-	

Screenshot above shows the Device table. As you can see, table shows a list of devices with their basic parameters:

1. Name
2. IP address
3. Port
4. SNMP Policy
5. SNMP version

Looking at the first device "cisco2950-xx" you can see that its IP address is x.x.3.84 and that the policy used on the device is "public". Furthermore, you can see that the said policy is SNMP v2c and that the UDP port used for SNMP is 161.

Devices are automatically added when device discovery is made in NMS and NetFlow module. It is not possible to manually add a new device.

Read more about Device Discovery and Exporter and Interface Discovery.

Devices

Editing device cisco2950g-xx

Name: Policy:

IP:

On the screenshot "Editing device" above you can see device parameters: name, IP address and policy. Name is used to identify the device in the application, and IP to identify the device in the network.

To change device name or policy:

1. Click on pen (edit icon), or double click on the Device table row
2. Set name or policy
3. Click Save

Choosing a policy:

-
- If you know the SNMP configuration of the device and the corresponding policy, you can choose the policy from the **Policy** drop-down list.
 - If you do not know the SNMP configuration of the device and the corresponding policy, click on the **Detect** and the application will try each policy defined in the application on the device specified. If successful, the Policy field will be automatically updated.
 - Additionally, you can test if the set device works on the device by clicking on the **Test** button.

Managing License

Administrator can view license information and manage license keys.



To view your NetVizura license, go to **Settings > Miscellaneous > License**.

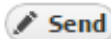
It shows useful information such as:

- License type
- Application version
- Expiration and support end date
- Installation code

To learn about how to update or upgrade your license, read more at [Licensing](#).

License

License type	PERPETUAL
Licensed to	icdev
Name and version	NetVizura 4.1
License expiration date	-
Support expiration date	Wednesday, 25 Feb 2015
Installation code	AA3E-2C46-525E-C647-8449-5F76-BC75-76D 

Installation code is needed for generating commercial license key. You can send it by clicking the **Send** button (opens email client).

License is upgraded with a new license key by clicking the **Upload**.

Configuring E-Mail

Email account setup is needed in order to receive notifications via email (such as system warnings, NetFlow alarms, license messages etc.).

Administrator can set SMTP server, Sender and SMTP password.

To do so, go to **Settings > E-Mail**.

E-mail

SMTP Server

Sender

SMTP Password

If you have multiple installations of NetVizura it is wise for sender name to correspond to the server's name: NVtest@domain.com or NV-production@domain.com.

Include password only if it is required by your SMTP (outgoing) mail server. If not, password should be omitted.

Configuring Display Names

Administrator can set, and user can view DSCP, AS number, Service port and Protocol names and descriptions. These names are used in the application instead of numbers to provide more human friendly statistics.

Configuring DSCP

NetFlow Analyzer has a searchable built-in register of DSCP names and numbers. You can change DSCP name and description. DSCP numbers are not changeable.

To configure DSCP, go to **Settings > Display Names > DSCP**.

On this page:

- Configuring DSCP
- Configuring AS
- Configuring Service
- Configuring Protocol

DSCP	AS	Service	Protocol
Editing DSCP 46			
DSCP Number: <input type="text" value="46"/>			
DSCP Name: <input type="text" value="EF"/>			
Description: <input type="text" value="Expedited Forwarding"/>			
<input type="button" value="✓ Save"/> <input type="button" value="✗ Close"/>			

Configuring AS

NetFlow Analyzer has a searchable built-in register of AS names and numbers. AS register is taken from IANA.org. AS numbers (ASN) are not changeable, but new autonomous systems can be added. In the unlikely event of NetFlow Analyzer built-in register not having the ASN you are looking for, you can retrieve it by visiting IANA.org. You can change AS name and description.

To configure AS, go to **Settings > Display Names > AS**.

DSCP	AS	Service	Protocol
Editing As 1313			
AS Number:		<input type="text" value="1313"/>	
AS Name:		<input type="text" value="ADOBE1-AS-AS"/>	
Description:		<input type="text" value="Adobe Systems Inc."/>	
<input checked="" type="button" value="Save"/>		<input type="button" value="Close"/>	

Configuring Service

NetFlow Analyzer has a searchable built-in register of Service names and numbers. You can change Service name and description. Service numbers are not changeable, but new services can be added.

To configure Service, go to **Settings > Display Names > Service**.

DSCP	AS	Service	Protocol
Editing Service AdobeFlash socket			
Service Name:		<input type="text" value="AdobeFlash socket"/>	
Service Ports:		<input type="text" value="843"/>	
Description:		<input type="text" value="Adobe Flash socket policy server"/>	
<input checked="" type="button" value="Save"/>		<input type="button" value="Close"/>	

Configuring Protocol

NetFlow Analyzer has a searchable built-in register of Protocol names and numbers. You can change Protocol name and description. Protocol numbers are not changeable, but new services can be added.

To configure Protocol, go to **Settings > Display Names > Protocol**.

DSCP	AS	Service	Protocol	
Editing Protocol 41				
Protocol Number: <input type="text" value="41"/>				
Protocol Name: <input type="text" value="Ipv6"/>				
Description: <input type="text" value="Ipv6"/>				
<input type="button" value="✓ Save"/> <input type="button" value="✗ Close"/>				

Configuring Time Window

Each user can set his Time Window preference:

- **Default Time Window** - time period that will be selected each time you log-in to application.
- **Date preference** - format in which date ranges will be presented

To configure Time Window, go to **Settings > Miscellaneous > Time Window**.

Time Window

Default Time Window

Date preference

NetFlow Configuration

This chapter explains how to configure NetFlow Analyzer:

- Configuring Traffic Patterns
- Configuring Subnets
- Configuring Subnet Sets
- Configuring End Users
- Configuring TopN Rules
- Configuring NetFlow Alarms
- Configuring Aggregator Filters
- Configuring NetFlow Sampling
- Configuring NetFlow System

Configuring Traffic Patterns

NetFlow users can view and NetFlow administrator can add, edit, delete or clone a Traffic Pattern.

To create new or configure existing Traffic Patterns, go to **Settings > NetFlow Settings > Patterns**.

Patterns	Subnets	Subnet Sets	TopN	Alarms	Aggregator Filtering	Exporters	Configuration
Name	Description	Internal Included	Internal Excluded	External Included	Ext		
All Blocked Traffic	-	0.0/16 0.0/16 128.0/19 128.0/18	-	-	-		
Proxy1	Proxy	1.40/29	-	-	128.0/19 28.0/18		
Viber		0/26 1.0/24 128/25	-	-	36.0/26 188.0/24 217.128/25		
WhatsApp		0/26 1.0/24 128/25	-	-	36.0/26 188.0/24 217.128/25		
OpenVpn	-	0/16	-	-	0.0/16		
Internet traffic		228.128/25	-	-	228.128/25		

If you are not familiar with Traffic Patterns, go to article [Basic Traffic Patterns](#) and then proceed to the article [Advanced Traffic Pattern Examples](#) for advance usage and examples.

To create a new Traffic Pattern, click **+Add**.

Adding a Traffic Pattern consists of four steps:

- [Defining the Traffic of Interest](#)
- [Setting IP Address Ranges](#)
- [Fine-tuning a Traffic Pattern](#)
- [Manual Deduplication](#)

It usually takes 10 minutes for NetFlow Analyzer to aggregate and show the statistics for the new Traffic Pattern.

In case Exporter filter is used in the Traffic Pattern definition and the Exporter IP address changes, you will have to manually update it in the Traffic Pattern definition.

Defining the Traffic of Interest

First think about the traffic you are interested in. Ask yourself:

- Who is talking to whom? In which networks or subnets are the end points?
- Are both sides of the conversation in your network (Self-Traffic), is one outside of your network (Normal), can one side of the conversation be both in your network and outside of it (Custom)? (This will help you to choose the Traffic Pattern type.)
- Where are these networks located – inside or outside of your company network? (This will help you define the Internal and External Network.)
- Is there something very specific about the traffic in question, such as the destination AS, used service port or protocol or some specific QoS marker? (This will help you choose the necessary filter.)

After this you should have a clear understanding of how to build your Traffic Pattern: Internal and External IP address ranges, and additional filtering by exporter, interface, service port, QoS, protocol etc.

Setting IP Address Ranges

Internal and External Networks are defined with their IP address ranges. Determine which IP addresses belong to these networks to define them. You can both include and exclude IP address range from the network definition, giving you flexibility and more freedom in shaping the definition of Internal and External Networks.

Screenshot below shows the Address tab which is used for setting the IP address ranges:

The screenshot shows the 'Adding new Pattern' dialog box in the NetFlow Analyzer. The 'Address' tab is active, and the 'Internal address ranges' field contains four subnets: 0.0.0.0/16, 128.0.0.0/16, 128.0.0.19, and 128.0.0.18. The 'External address ranges' field is empty. The 'Include' button is highlighted in blue. The 'Self-Traffic' radio button is selected. The 'Save' and 'Close' buttons are at the bottom.

In this screenshot you can see a Traffic Pattern where Internal network consists of 4 subnets and External network with no subnets defined (effectively this is any subnet). This Traffic Pattern will monitor traffic between these four subnets and any other network, including internal traffic (traffic between IPs that belong to any four subnets in the Internal Network).

To help you in Traffic Pattern creation, NetFlow Analyzer offers three types of Traffic depending on the direction of traffic in regards to your Internal network. These three types will also help you create Traffic Patterns more quickly because they will include or exclude some address ranges from the Internal or External Network automatically. These Traffic types are:

- Normal Traffic
- Self Traffic
- Custom Traffic

Self Traffic

If you wish to monitor traffic that originates from and ends in your network or its part (your network is both the source and the destination of the traffic), then you choose the Self Traffic, assuming that you previously correctly configured all subnets that exist in your network. If, for example, you wish to monitor the traffic that originates from the 10.0.0.0/8 network (which can be divided in multiple subnets) and ends up in the same network, we simply enter 10.0.0.0/8 in the Internal address ranges field and click on the Include command. The same address will be automatically entered in the include section of the External address ranges field on the right-hand side of the panel. Defined in this way, the Traffic pattern will collect information on all traffic that originates from the 10.0.0.0/8 network and ends up within the 10.0.0.0/8 network. If we wish to monitor only a specific service or protocol, it is possible to add additional filters as mentioned earlier.

Normal Traffic

A Normal Traffic is used when we wish to monitor traffic which originates from an internal network and ends up in an external network, such as the Internet. If, for example, we wish to monitor the traffic that originates within the 10.0.0.0/8 network and ends up outside of that network we enter 10.0.0.0/8 in the Local Address Range field and click on the Include command. On the right-hand side of the panel, in the External Address Range field, the same 10.0.0.0/8 network will be automatically entered in the excluded section. This Traffic Pattern will monitor all the traffic originating within the 10.0.0.0/8 address range and ending up outside that address range. Additional filters can be set up to further filter out the traffic.

Custom Traffic

A Custom Traffic is used when you wish to monitor traffic which is a combination of two previous cases. In the case of such Traffic Pattern, there is no correlation between Internal and External address ranges fields.

Fine-tuning a Traffic Pattern

Mandatory criteria needed for creating a Traffic Pattern is the IP address criteria. Namely, it is mandatory to enter at least one address range in the Internal Address range field.

Also, it is possible to set up additional filters using the include and/or exclude commands. Additional filters are based on:

- Exporter and its interfaces
- Service
- AS
- Protocol
- QoS
- Next Hop

These filters can be freely combined to make very specific Traffic Patterns which are matching the traffic you are interested in. For instance, by combining first three filters, you can monitor the traffic from a single network device that uses a specific service in communication with a specific Autonomous System.

On this page:

- [Filtering Based on Exporter and its Interfaces](#)
- [Filtering Based on Service](#)
- [Filtering Based on AS](#)
- [Filtering Based on Protocol](#)
- [Filtering Based on QoS](#)
- [Filtering Based on Next Hop](#)

Related pages:

- [Setting IP Address Ranges](#)

Bare in mind that this filters are for fine-tuning your Traffic Patterns. In particular, this means that the filter is applied only to the traffic matched by a given Traffic Pattern IP address range. In other words, an IP address from the Traffic Pattern definition is applied first, and then the filters are applied.

Therefore, if you want to monitor all traffic that goes from your internal network via certain exporter/service/AS/protocol/QoS, you need to apply that filter to a Traffic Pattern that covers all traffic (such as All traffic Traffic Pattern). Likewise, if you want to monitor the traffic from a particular Traffic Pattern via certain exporter/service/AS/protocol/QoS, apply that filter to that Traffic Pattern.

Filtering Based on Exporter and its Interfaces

To create a filter based on the IP address of the exporter or its interface:

1. Go to **Settings > NetFlow Settings > Patterns**
2. **Add** new or **Edit** existing pattern
3. Click the **Exporter** tab.

You can monitor the traffic that has been exported by a single device (exporter) or that has entered/exited a specific interface of that particular device (exporter). The Exporter IP field is used to specify the IP address of the exporting device, while Interface In and Interface Out fields are used to specify the SNMP ID of one or more interfaces of the device. Use the Include and Exclude options to include or exclude several interfaces of the exporter from the filter.

This filter is most commonly used to remove duplicate flows. Read more at [Resolving Duplicated Export](#).

To cancel any changes to the filter, click Reset.

An Exporter filter example is given on the figure below: the Traffic Pattern with this filter will only match flows that pass through exporter X.Y.4.38 and only if the flow passed through interface 2 in ingress (In) direction and passed through interface 5 in egress (Out) direction.

Address Exporter Service AS Protocol QoS Next Hop

Exporter criteria parameters:
 Exporter IP: Interface In: Interface Out:

Include Exclude **+ Add** **X Reset**

Exporter IP	Interface In	Interface Out
10.1.1.4.38	2	5

Save **X Close**

- You can either include one or more exporters, or exclude one or more exporters. It is not possible to have included and excluded exporters in a single Traffic Pattern.
- Device must be an exporter (actually export netflow data to the NetFlow Server) in order for filtering to have any effect.
- IP address used to identify the exporter is the IP address the router has been configured to export the netflow data from.

Example 1

We want to monitor all traffic exported by a network device with the IP address 10.1.1.1. Furthermore, we are only interested in the traffic that has entered through interfaces with SNMP IDs 1 or 2 and exited through interface 4.

Here is how to make the filter:

1. Type in **10.1.1.1** into Exporter IP field
2. Type in **1,2** into Interface In field
3. Type in **4** into Interface Out field
4. Select **Include** radio button (default)
5. Click **Add**
6. Click **Save**

This filter translates to “traffic must pass through router 10.1.1.1, entering through interface 1 or 2, and exiting through interface 4”.

Example 2

We want to monitor all traffic from a single physical link. This link is on a network device with the IP address 10.1.1.1, interface with SNMP ID 1. This means that interface 1 is both In and Out interface. The device is an exporter.

Here is how to make the filter:

1. Type in **10.1.1.1** into Exporter IP field.
2. Type in **1** into Interface In field.
3. Leave the Interface Out field empty

Do not set Interface Out field to 1 here. This would make an invalid filter, since flow can not enter and exit the exporter on the same interface at the same time.

4. Select **Include** radio button (default)
5. Click **Add**
6. Type in **10.1.1.1** into Exporter IP field, again
7. Leave the Interface In field empty
8. Type in **1** into Interface Out field
9. Select **Include** radio button (default)
10. Click **Add**
11. Click **Save**

This filter translates to “traffic must pass through router 10.1.1.1, entering through interface 1, or pass through router 10.1.1.1, entering through interface 1”.

Example 3

To monitor the traffic that entered through the Interface with SNMP ID 1 on any/all exporters:

1. Leave the Exporter IP field empty
2. Type in **1** into the Interface In field
3. Leave the Interface Out field empty
4. Select **Include** radio button (default)
5. Click **Add**
6. Click **Save**

Exporter table added an entry "Exporter IP: all Interface In: 1". This indicates that interfaces In with the SNMP ID 1 of all network devices are included in this filter.

Example 4

To exclude the traffic entering through a specific interface on a specific exporter:

1. Type in **10.1.1.1** into the Exporter IP field, where 10.1.1.1 is Exporter's IP address
2. Type in **1** into the Interface In field, where 1 is SNMP ID of interface we are not interested in
3. Leave the Interface Out field empty
4. Select **Exclude** radio button (default)
5. Click **Add**
6. Click **Save**

Exporter table added an entry Exporter IP: 10.1.1.1 Interface In: 1 Interface Out: all and that Exclude and Include radio buttons are disabled, while the Exclude radio button is active. This indicates that the only traffic that will be excluded from the Traffic Pattern will be the traffic entering through the Interface 1 on the network device with the IP address 10.1.1.1.

Filtering Based on Service

To create a filter based on the service:

1. Go to **Settings > NetFlow Settings > Patterns**
2. **Add** new or **Edit** existing pattern
3. Click the **Service** tab.

You can filter traffic based on services by including or excluding one or more service ports. Filtering is done by inserting service port numbers for the source and destination AS. This enables you to monitor the traffic utilizing certain service ports or services only.

Screenshot below shows the an example of service filter.

To cancel any changes to the filter, click Reset.

Service criteria parameters:

Source port(s):

Destination port(s):

Include Exclude

Source Port	Destination Port
All	80
80	All

If you do not know the service you wish to include/exclude, go to **Settings > Display Names > Service** tab and do a search on the desired service port.

Example

We want to monitor all traffic exported by a network device with IP address 10.1.1.1. Furthermore, we are only interested in the traffic that has entered through interfaces 1 and 2 and exited through interface 4:

1. Type in **10.1.1.1** into the Exporter IP field
2. Type in **1,2** into the Interface In field
3. Type in **4** into the Interface Out field
4. Click on the **Include** radio button (default)
5. Click **Add** to add this filter to the filter list
6. Click **Save**

Filtering Based on AS

You can filter traffic based on AS, by including or excluding one or more Autonomous Systems. Filtering is done by inserting AS numbers (ASN) for the source and destination AS. This enables you to monitor the traffic between going to or coming from a certain AS or AS group and the traffic between two AS or AS groups.

Screenshot below displays an example of AS filter:

AS criteria parameters:

Source AS number(s):

Destination AS number(s):

Include Exclude

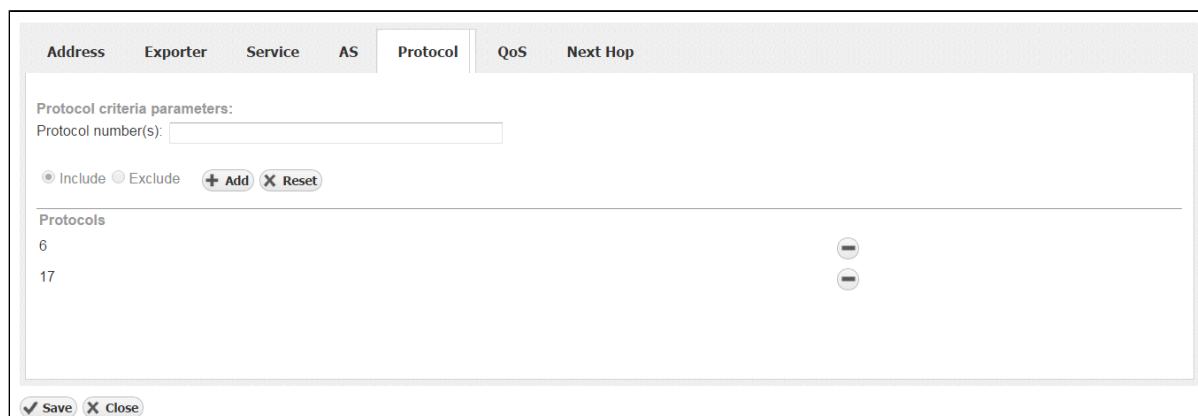
Source AS	Destination AS
5242	All
5243	All
4244	All
9785	All
All	5242
All	5243
All	4244
All	9785

- Leaving the Source/Destination AS Number(s) field empty will have a meaning equal to inserting all Autonomous Systems
- If you do not know the ASN of the AS you wish to include/exclude, go to **Settings > Display Names > AS** tab and do a search on the desired AS name

Filtering Based on Protocol

You can filter the traffic based on the protocol, by including or excluding one or more protocols. Filtering is done by inserting protocol numbers into the Protocol Number(s) field. This enables you to only monitor the traffic including a certain protocol or protocols, or to monitor the traffic excluding a certain protocol or protocols.

This screenshot shows the configuration of the protocol filter:



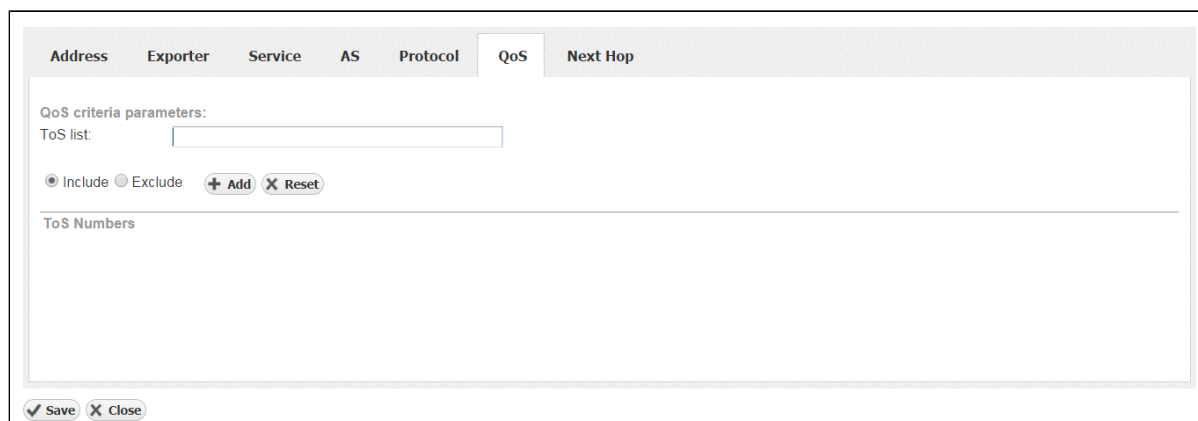
The screenshot shows a configuration window with tabs: Address, Exporter, Service, AS, Protocol, QoS, and Next Hop. The 'Protocol' tab is active. Under 'Protocol criteria parameters:', there is a 'Protocol number(s):' text input field. Below it are radio buttons for 'Include' (selected) and 'Exclude', along with '+ Add' and 'X Reset' buttons. A table titled 'Protocols' contains two rows: '6' and '17', each with a minus sign icon to its right. At the bottom are 'Save' and 'Close' buttons.

If you do not know the Protocol Number of the protocol you wish to include/exclude, go to **Settings > Display Names > Protocol** tab and do a search on the desired protocol name or locate the protocol in the Protocol table.

Filtering Based on QoS

You can filter the traffic based on QoS, by including or excluding one or more QoS markers. Filtering is done by inserting the ToS field into the ToS list field. This enables you to only monitor the traffic including or excluding a certain level(s) of QoS, or in other words including or excluding certain ToS fields.

The configuration of the QoS filter:



The screenshot shows a configuration window with tabs: Address, Exporter, Service, AS, Protocol, QoS, and Next Hop. The 'QoS' tab is active. Under 'QoS criteria parameters:', there is a 'ToS list:' text input field. Below it are radio buttons for 'Include' (selected) and 'Exclude', along with '+ Add' and 'X Reset' buttons. A table titled 'ToS Numbers' is currently empty. At the bottom are 'Save' and 'Close' buttons.

If you do not know the exact ToS for the QoS level you want to monitor, go to **Settings > Display Names > DSCP** tab and locate the desired DSCP number in the table.

Filtering Based on Next Hop

You can filter the traffic based on next hop, by including or excluding one or more next hop IP addresses. Filtering is done by inserting the IP address for next hop field into the Next Hop IP field. This enables you to monitor only traffic including or excluding a certain next hop.

The configuration of the Next hop filter:

Address Exporter Service AS Protocol QoS **Next Hop**

Next hop criteria parameters:
Next hop IP:

Include Exclude

Next hops

A case when the Next Hop filtering is particularly useful is when the network architecture and configuration forces you to have double netflow export. This situation is further explained in the article [Manual Deduplication](#).

Manual Deduplication

In general, if you correctly configured exporters (ingress/egress) and decided to enable automatic deduplication by exporting from all devices in flow continuity then all flows in your Traffic Patterns should be automatically deduplicated. Read more in [Configuring NetFlow Export \(Ingress vs. Egress\)](#) and [Enabling Automatic Deduplication](#).

However, if this is not the case then it is also possible for you to adjust Traffic Pattern configuration in a way to achieve flow deduplication.

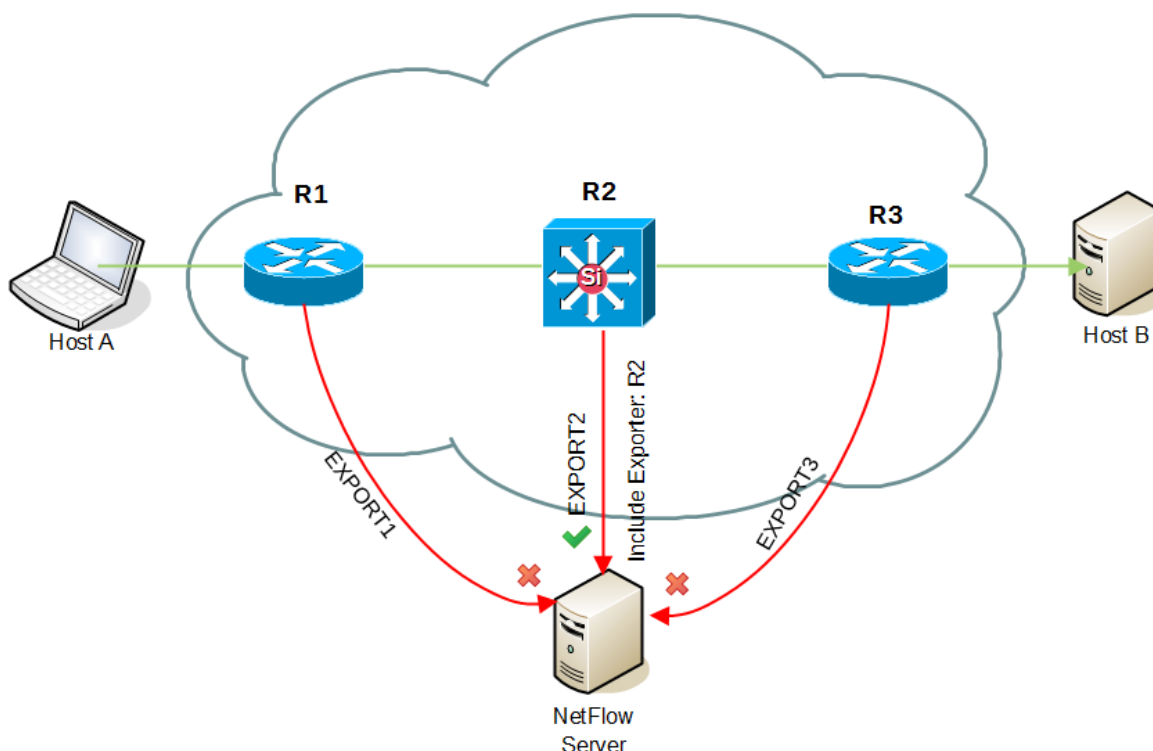
Before proceeding, pay attention to first disable automatic deduplication (at **NetFlow Settings > Configuration**).

On this page:

- Deduplication based on the central exporter
- Deduplication based on exporters and their interfaces
- Deduplication based on next hop

Deduplication based on the central exporter

If you have a central exporter (a netflow exporter through which all desired traffic is passing through) then preventing duplicated Traffic Pattern traffic is easy. You just need to add a filter to the Traffic Pattern in the Exporter section of the Traffic Pattern definition. Add the IP address of the central exporter while include option is set. This will result in Traffic Pattern matching only netflow that was exported by the central exporter.



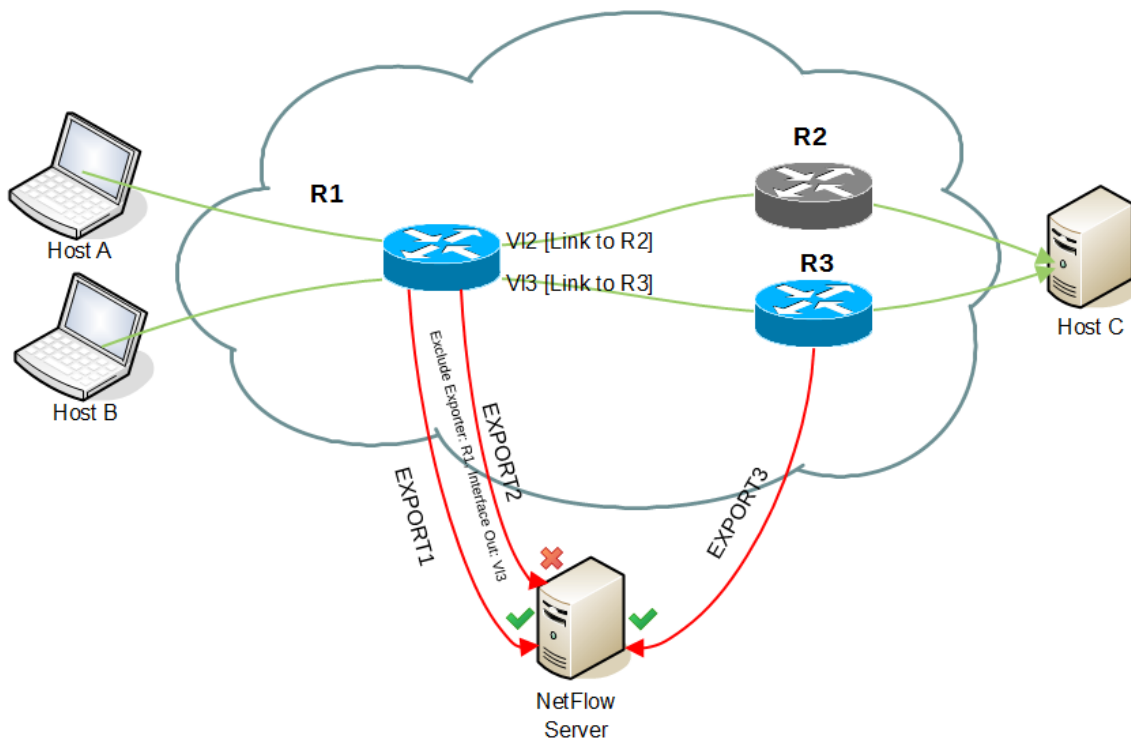
In our example above, flow that passes and is exported by three routers (R1, R2 and R3) will be taken into account and processed only from central router (R2) since Traffic Pattern includes its IP address in Exporter filter.

Have in mind that all other traffic (that does not pass via central exporter) will not be captured.

Learn more about [Filtering Based on Exporter and its Interfaces](#).

Deduplication based on exporters and their interfaces

If you do not have a central exporter and/or your network topology is more complex you can prevent duplicated Traffic Patterns by entering exporters and their specific interfaces from which you will either include or exclude traffic when matching traffic to a Traffic Pattern. In this way you can exclude specific interfaces on exporters that would duplicate the traffic.



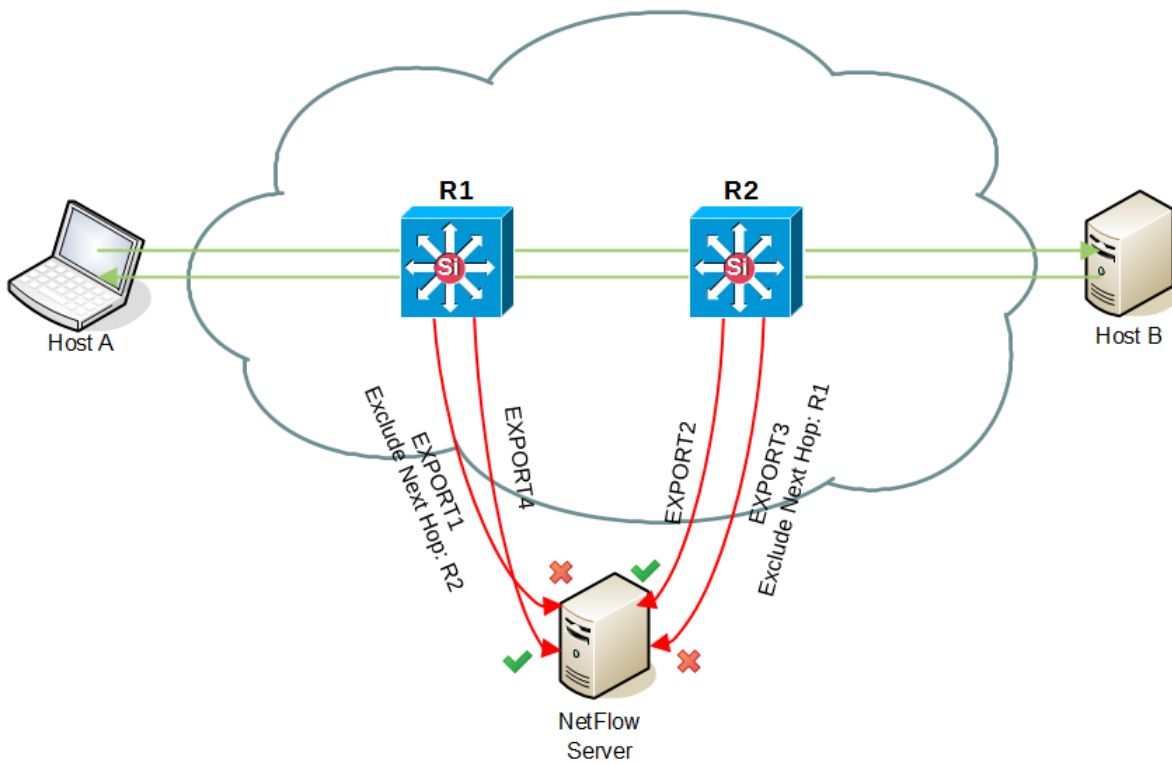
In the example above, flow travelling via R1 and R2 will not be duplicated since R2 is not an exporter, however flow travelling via R1 and R3 will be duplicated. By excluding Interface Out: VI3 on Exporter R1 only export from exporter R3 will be processed.

Have in mind that all other traffic (that passes via included exporters and interfaces) will be captured.

Learn more about [Filtering Based on Exporter and its Interfaces](#).

Deduplication based on next hop

In the example below, a flow travelling from Host A to Host B passes via two central routers R1 and R2. As a consequence, one flow is exported and processed to a netflow server twice (by R1 and R2). This should be overcome by adding next hop filter.



The solution is to exclude R2 as Next Hop IP address. This will simply skip all the flows passing from router R1 to R2. Flows will be then matched and processed only by router R2. The same applies for flows from Host B to Host A - excluding R1 as Next Hop IP address will skip all the flows passing from router R2 to R1. These flows will be processed only by R1.

Have in mind that all other traffic (that does not have R2 and R1 as next hop) will be captured.

Learn more about [Filtering Based on Next Hop](#).

Configuring Subnets

Subnets are used in charts to show the distribution of the traffic within a Traffic Pattern. Created subnets will be automatically displayed under a Traffic Pattern if its IP address range is included in the Traffic Pattern's Internal Network.

NetFlow users can view and NetFlow administrator can add, edit or delete Subnets.

To configure subnets, go to **Settings > NetFlow Settings > Subnets** tab.

Name	Address	Description
Sarnet- 130.0/24	130.0/24	-
Sarnet- 131.0/24	131.0/24	-
Sarnet- 132.0/24	132.0/24	-
Sarnet- 133.0/24	133.0/24	-
Sarnet- 134.0/24	134.0/24	-
Sarnet- 135.0/24	135.0/24	-
Sarnet- 136.0/24	136.0/24	-
Sarnet- 137.0/24	137.0/24	-
Sarnet- 138.0/24	138.0/24	-
Sarnet- 139.0/24	139.0/24	-
Sarnet- 140.0/24	140.0/24	-
Sarnet- 141.0/24	141.0/24	-
Sarnet- 142.0/24	142.0/24	-
Sarnet- 143.0/24	143.0/24	-
Sarnet- 144.0/24	144.0/24	-
Sarnet- 145.0/28	145.0/28	-
Sarnet- 145.64/28	145.64/28	-
Sarnet- 145.80/28	145.80/28	-

Tip

To get a precise display of traffic distribution it is a good practice to define subnets covering entire IP address range of a bigger subnet. If one or more subnets are not defined, their traffic will be added to "Others" (gray in charts and tables) even if they would be in top talkers otherwise. If Others entry covers a lot of traffic in your Traffic Pattern, you should add more subnets.

To add a new subnet:

1. Click **Add**
2. Type in subnet_name into the **Name** field (optional)
3. Type in subnet_ip_address_and_mask into the **Address** field.
4. Click **Save**.

Note that any new subnet will be automatically added in the subnets hierarchy, and in all Traffic Patterns if its IP address range belongs to the Internal Network of the Traffic Pattern.

To remove a subnet from the database:



















1. Select the desired subnet from the table
2. Click **Remove**
3. Click **Yes** to confirm removal

Configuring Subnet Sets



Subnet Sets are a set of subnets grouped by some logical criteria you define, independent to the IP address range. To read more, go to [Subnet Sets](#).

NetFlow users can view and NetFlow administrator can add, edit or delete Subnet Sets.

To configure subnet sets, go to **Settings > NetFlow Settings > Subnet Sets** tab.

Patterns	Subnets	Subnet Sets	TopN	Alarms	Aggregator Filtering	Exporters	Configuration
+ Add							
Name		Description	Action				
AlphaCom		Offices in Europe, MENA and US	 				
Benelux offices			 				
Europe offices			 				
France offices			 				
Germany and Austria			 				
InoTech			 				
MENA offices		Middle East and North Africa	 				
Spain offices			 				
US offices			 				
Page 1 of 1							1-9 / 9

To add a new Subnet Set to the database:

1. Click **Add**
2. Type in subnetset_name into the **Name** field
3. Type in subnetset_description into the **Description** field (optional)
4. Add subnets from the Available Subnets list to your SubnetSet
 -  Available Subnets list displays all subnets you previously defined that are not members of any Subnet Set, while the Available Subnet Sets list displays all Subnet Sets that are already created.
 -  A subnet can be a member of only one Subnet Set.
5. Add Subnet Sets from the Available SubnetSets list to your Subnet Set
6. Click **Save**.

Note that new Subnet Sets will be automatically displayed under a Traffic Pattern if its IP address range is included in the Traffic Pattern's Internal Network.

To remove a subnet from the database:

1. Select the desired subnet set from the SubnetSet table
2. Click **Remove**
3. Click **Yes** to confirm removal

Configuring End Users

NetVizura is capable of detecting end user activity in the company network. Mapping user's actual username with IP addresses allows to keeping *logon events* tracks of end users. Logon events could be generated by Domain Controllers or Work Stations relayed via Syslog to NetVizura server. We use Windows Domain Controller in our example.

NetVizura comes with predefined matching rules for Snare Open Source Syslog agent. For detailed explanation on how to install and configure Snare Syslog agent see [Installing and Configuring Syslog Agent for End User Traffic](#).

On this page:

- Step 1. Select appropriate message (logon event):
 - Match String
- Step 2. Setup rule:

Example of correct match string

```
* MSWinEventLog * 4624 Microsoft-Windows-Security-Auditing * Success Audit * Logon  
Type: 3 * Account Name: <USERNAME> * Account Domain: <DOMAIN> * Source  
Network Address: <USER-IP> *
```

Step 1. Select appropriate message (logon event):

Navigate to Netvizura **Eventlog** module and choose **Syslog** tab. Identify syslog message with logon information. This log should contain:

1. **IP address** of domain controller that exports Syslogs - *type IP address into Exporter text box and press Enter*
2. Windows code **4624** that designates successful logon event - *type 4624 into Message filter text box and press Enter*
3. Select, copy and paste text message in some text editor (Wordpad or similar)
4. Create appropriate **Match string** in text editor

The screenshot shows the NetVizura Syslog interface. At the top, there are tabs for 'Syslog', 'SNMP Trap', and 'System'. Below the tabs is a 'Refresh' button and a 'Show names' button. A bar chart shows log activity over time. On the right, there is a 'Severity' table and a 'Distribution' pie chart. The main area displays a list of log messages. The first message is selected, and its details are shown in a text box. The details include the date, time, exporter IP, severity, facility, and the full log message text. The message text is highlighted with a red box, and three numbered callouts (1, 2, 3) point to specific parts of the message: 1 points to the exporter IP '172.16.0.108', 2 points to the event ID '4624', and 3 points to the log message text.

Match String

Steps for creating correct match string :

1. Find *Account Name* within the message and put **<USERNAME>** instead of real account name (please refer to picture below)
2. Find *Account Domain* within the message and put **<DOMAIN>** instead of real account domain (please refer to picture below)
3. Find *Source Network Address* within the message and put **<USER-IP>** instead of real IP address (please refer to picture below). **i** No need for this step in case of Work Station type of rule.
4. Find additional information that can help in matching message more precisely like: **MSWinEventLog, 4624 Microsoft-Windows-Security-Auditing, Success Audit, Logon Type: 3**
5. **IMPORTANT:** Delete any other text and put ***** as a wildcard instead of deleted text (refer to [Example of correct match string](#))

Dec 9 16:57:48 dc.mycompany.com MSWinEventLog [Security 299108 Thu. Dec. 09 16:57:47
 4624 Microsoft-Windows-Security-Auditing MyDomain\john N/A Success Audit
 dc.mycompany.com Logon An account was successfully logged on. Subject: Security ID: S-1-0-
 0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level:
 Delegation New Logon: Security ID: S-1-5-4104 Account Name: john Account Domain:
 MyDomain Logon ID: 0x2A8DB41A Logon GUID: {B50C1E00-1688-A170-5068-84D2F9A016D3}
 Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation
 Name: Source Network Address: 172.16.4.23 Source Port: - Detailed Authentication
 Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: -
 Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is
 created. It is generated on the computer that was accessed. The subject fields indicate the
 account on the local system which requested the logon. This is most commonly a service such
 as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type
 field indicates the kind of logon that occurred. The most common types are 2 (interactive)
 and 3 (network). The New Logon fields indicate the account for whom the new logon was
 created, i.e. the account that was logged on. The network fields indicate where a remote
 logon request originated. Workstation name is not always available and may be left blank in
 some cases. The impersonation level field indicates the extent to which a process in the
 logon session can impersonate. The authentication information fields provide detailed
 information about this specific logon request. - Logon GUID is a unique identifier that can be
 used to correlate this event with a KDC event.]

Step 2. Setup rule:

In upper right corner of Netvizura application navigate to **cogwheel > Settings > NetFlow Settings > End Users:**

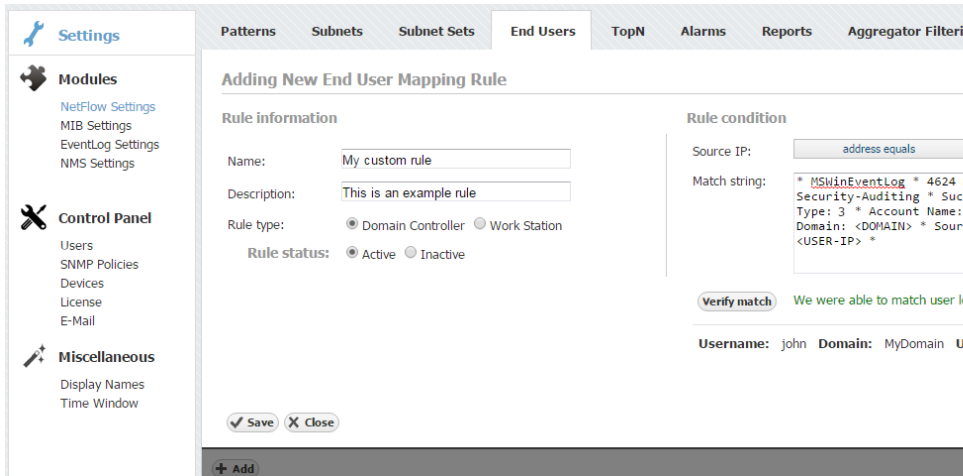
1. Click on **+ Add** button
2. Enter your own **Rule Name and Description**
3. Set **Rule type** (in this example set *Domain Controller*)
4. Set **Rule status** (in this example set *Active*)
5. Enter **Source IP** (IP address of Domain Controller)
6. Copy and paste **Match string** from text editor into the *Match string area*
7. Click on **Verify match** button
8. Click on **Save** button to save your rule (if verification is successful)

In order to improve user mapping and system performance, we recommend to set status as inactive for all rules that are not in use.

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.

Use help button: Move your cursor under the question mark on the screen for additional help.

You can easily verify the rule by clicking **Verify** button. Your rule will be automatically applied to check if any Syslog message received during the last 24 hours matches the rule.



To check results of your work, navigate to **NetFlow > End Users**. If the three is empty, refresh your web browser with ctrl+F5.

Configuring TopN Rules

By default, the number of top talkers that appear in the chart and table for any node and statistic is set to 10. This is defined by the Default TopN rule. In addition to a default rule, you can create specific rules for specific nodes i.e. rise or lower top talkers followed for certain type of traffic the that node affected by the rule.

NetFlow users can view and NetFlow administrator can add, edit or delete TopN rules.

To configure TopN rules, go to **Settings > NetFlow Settings > TopN tab**.

To change default TopN rule:

1. Choose **Edit** Default rule (click on pen icon button, or double click on table row)
2. Update the **TopN shown** fields as wanted
3. Confirm with **Save**

To add a new TopN rule:

1. Click **Add**
2. Give a **Rule Name**
3. Choose Node for which the rule will apply to
 - a. Choose **Note type** (Exporter, Interface, Traffic Pattern, Subnet, Subnet Set, All Users, End User, Domain)
 - b. Click **Select** to choose a node (popup showing all available nodes will show)
4. In **TopN shown** section change the topN count for a traffic distribution (host, conversation, service...)

The screenshot shows the 'Editing TopN Rule' configuration page. The breadcrumb navigation is 'Patterns > Subnets > Subnet Sets > End Users > TopN > Alarms > Reports > Aggregator Filtering > Sampling > Configuration'. The page title is 'Editing TopN Rule "Exporter GNS3"'. The form is divided into two main sections: 'Rule information' and 'TopN shown'. In the 'Rule information' section, the 'Rule name' field contains 'Exporter GNS3'. The 'Node type' is set to 'Exporter' and the selected node is 'GNS3-R1 [172.16....' with a 'Select' button next to it. At the bottom left of the form are 'Save' and 'Close' buttons. The 'TopN shown' section contains a list of categories with input fields for their respective counts: Interfaces (8), Host (8), Conversation (8), Service (8), Protocol (8), QoS (8), AS (8), and Set all to (10). There are 'Set' and 'Set to default' buttons at the bottom right of this section.


You need to login/logout to be able to view these changes on charts and tables.

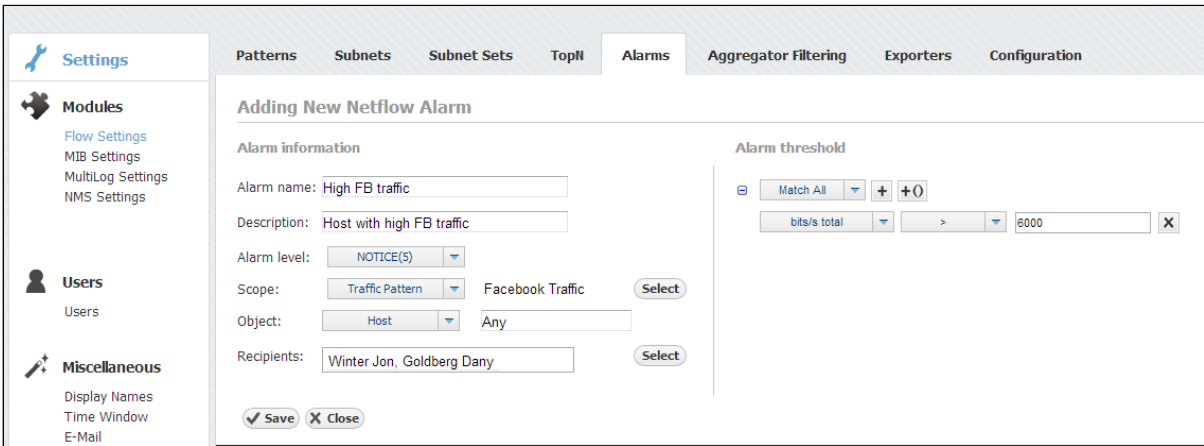
Configuring NetFlow Alarms

NetFlow users can view and NetFlow administrator can add, edit or delete alarms.

To configure NetFlow alarms, go to **Settings > NetFlow Settings > Alarms**.

To add a new alarm in NetFlow Analyzer:

1. Click **Add**
2. Set **Alarm information** (name, description, level, scope, object and optionally mail-to recipients)
 - **Scope** determines on which nodes an alarm will be applied: any or specific exporter, interface, subnet, Subnet Set or Traffic Pattern.
 - **Object** determines what type of traffic will be matched against the alarm threshold criteria: total, interface, subnet, protocol, host, AS, conversation etc.
 - **Recipients** list (optional) determines to whom will an email be sent if the alarm triggers.  Only users with emails associated to their user account can be recipients.
3. Set **Alarm threshold**.
Threshold can be in flows, packets or bits. It is possible to combine more threshold criteria by using AND, OR and NOT logical operands.
4. Click **Save**



The screenshot shows the 'Adding New Netflow Alarm' configuration page in the NetFlow Analyzer. The page is divided into several sections:

- Navigation:** A top bar with tabs for Patterns, Subnets, Subnet Sets, TopN, Alarms (selected), Aggregator Filtering, Exporters, and Configuration.
- Left Sidebar:** Contains 'Settings' (with a wrench icon) and three main categories: 'Modules' (Flow Settings, MIB Settings, MultiLog Settings, NMS Settings), 'Users' (Users), and 'Miscellaneous' (Display Names, Time Window, E-Mail).
- Alarm Information:**
 - Alarm name: High FB traffic
 - Description: Host with high FB traffic
 - Alarm level: NOTICE(S)
 - Scope: Traffic Pattern (selected), Facebook Traffic (selected)
 - Object: Host (selected), Any (selected)
 - Recipients: Winter Jon, Goldberg Dany
- Alarm threshold:**
 - Match All (selected)
 - bits/s total (selected)
 - Operator: >
 - Value: 6000
- Buttons:** Save and Close.

Figure above shows an example of an Alarm. This alarms triggers if any host in the network has more than 6 kbps of Facebook traffic in 5 minutes. Facebook traffic is identified via Facebook Traffic Pattern. On alarm trigger an email will be sent to Winter Jon and Goldberg Dany.

Configuring Aggregator Filters

Aggregator filtering sets filters for all received flows on application level in order to filter unnecessary flows from processing.

NetFlow users can view and NetFlow administrator can add, edit, delete or reorder aggregator filters.

To configure aggregator filtering, go to **Settings > NetFlow Settings > Aggregator Filtering** tab.

You are able to accept or reject any traffic coming via:

- Source IP
- Destination IP
- Source port
- Destination port
- Protocol
- Exporter IP
- Interface in
- Interface out

The screenshot shows the 'Adding New Filter' configuration page. At the top, there is a navigation bar with tabs: Patterns, Subnets, Subnet Sets, TopN, Alarms, Aggregator Filtering (selected), Exporters, and Configuration. The main content area is divided into two sections: 'Filter information' and 'Filter expression'.
In the 'Filter information' section, there is a 'Filter name:' text input field and a 'Description:' text area. Below these, there are radio buttons for 'Filter status:' with 'Active' selected and 'Inactive' unselected. At the bottom left of this section are 'Save' and 'Close' buttons.
The 'Filter expression' section contains a 'Match All' dropdown menu, a '+' button, and a '+()' button. Below this is a list of filter criteria: Source IP, Destination IP, Source port, Destination port, Protocol, Exporter IP, Interface in, and Interface out. The 'Source IP' option is currently selected. To the right of the list is an 'address equals' dropdown menu and an empty text input field with a close 'X' button. Below the list, there are radio buttons for 'Action:' with 'ACCEPT' selected and 'REJECT' unselected.

Note that filters are executed in their order. Default filter is always applied last.

If you add filters, you can have two filter strategies:

- Set default filter to reject all flows and create specific filters that explicitly accept certain flows
- Set default filter to accept all flows and create specific filters that explicitly reject certain flows

In case Exporter IP is used to create a filter and that netflow exporter changes its export IP address, you will have to manually update the filter.

Configuring NetFlow Sampling

When core network devices have a very large amount of traffic passing through them, you may decide that your exporter device sends sampled netflow data to lower CPU load. In this case, sample ratios enable you to multiply metric values and get a more realistic traffic in the graphs.

NetFlow users can view and NetFlow administrator can add, edit or delete exporter sampling rules.

To configure sampling rules, go to **Settings > NetFlow Settings > Sampling** tab.

To add an exporter sampling rule:

1. Click **Add**
2. Enter IP address of the exporter you want to multiply data for
3. Enter sample ratios (Bytes, Packets and Flows)
4. Click **Save**

If you don't want to multiply a metric, simply enter ratio 1.

Patterns	Subnets	Subnet Sets	TopN	Alarms	Aggregator Filtering	Sampling	Configuration
Adding new sampling rule							
IP address:	<input type="text" value="1.1.1.1"/>						
Bytes sample ratio:	<input type="text" value="100"/>						
Packets sample ratio:	<input type="text" value="100"/>						
Flows sample ratio:	<input type="text" value="100"/>						
<input type="button" value="✓ Save"/> <input type="button" value="✗ Close"/>							

Configuring NetFlow System

NetFlow users can view and NetFlow administrator can manage:

- NetFlow Service Options
- NetFlow Database Maintenance
- Archiving Raw Data
- Importing/Exporting Configuration
- Automatic Deduplication

To access NetFlow system configuration, go to **Settings > Flow Settings > Configuration**.

NetFlow Service Options

To configure service options, go to **Settings > NetFlow Settings > Configuration** tab.

Here, you can define:

- **Service socket port** - port used by the application to receive the netflow data. The value has to be the same as the value set on your network devices which export the netflow data (Exporters). Default value is 2055.
- **Socket timeout** - UDP socket timeout in seconds

NetFlow Database Maintenance

Flow database stores the data needed for chart and alarms in Flow module. You can configure NetFlow database in **NetFlow Settings > Configuration** with the following parameters:

- **Maximum database size** - oldest data will be removed first
- **Minimum database size in weeks** - the system will warn you before database space runs out

NetFlow Analyzer will warn you if your storage space is full and tell you exactly what actions are advised. Warnings are sent by email to NetVizura administrators and displayed when you log-in. Warning message is triggered when application concludes that Maximum database size will be reached without storing minimum amount of traffic in weeks (Minimum database size in weeks).

The screenshot shows the 'Configuration' tab of the NetFlow Settings interface. The left sidebar contains 'Settings', 'Modules' (Flow Settings, MIB Settings), 'Users', and 'Miscellaneous' (Display Names, Time Window, License). The main content area has tabs for 'Patterns', 'Subnets', 'Subnet Sets', 'TopN', 'Alarms', 'Aggregator Filtering', 'Exporters', and 'Configuration'. Under the 'Configuration' tab, there are 'Import' and 'Export' buttons. The 'Service options' section includes: 'Service socket port' (2055), 'Socket timeout' (5 seconds), 'Temp folder' (/var/lib/icmynet/flow/temp), 'Archived files folder' (/var/lib/icmynet/flow/archive), and 'Legacy raw files folder' (/var/lib/icmynet/flow/legacy). The 'Maximum database size' is set to 30 GB, and the 'Minimum database size in weeks' is set to 52. Both of these fields are highlighted with orange boxes. At the bottom, there are 'Save' and 'Cancel' buttons.

Example of storage warning message for Maximum database size set to 30 GB and Minimum database size in weeks set to 52 weeks:

9 weeks of data (5.5 GB) still needs to be stored, but only 5 more weeks' worth of space (3 GB) remain in the database storage.

You need to provide more space for Flow database (currently set to 30 GB), or lower the minimum number of weeks (currently set to 52 weeks) for which you would like to keep the data. 52 weeks is approximately 33 GB.

Flow database stores the data needed for chart and alarms in Flow module. When the database size increases beyond configured limit, oldest entries will be deleted although those entries would fall within configured minimum number of weeks - consequently charts and alarms corresponding to deleted entries would be missing.

Archiving Raw Data

Flow archive stores Raw Data files. These files can be analyzed in the Raw Data tab in Flow module. Archiving data is configured in **Flow Settings > Configuration** by setting:

- **Temp folder** - folder in which NetFlow Analyzer will temporary unpack Raw Data files
- **Archived files folder** - folder in which NetFlow Aggregator stores processed files
- **Legacy raw files folder** - folder in which NetFlow stores Raw Data files from previous versions
- **Minimum free disc space** - minimum free hard disk space is a value that needs to be free on the NetFlow Server in GB. Once saving of new Raw Data file threatens to lower free hard disk spaces below this value, NetFlow will delete the oldest Raw Data files freeing up the disk space. Default value is 30.00 GB.
- **Minimum archive size in days** - the system will warn you up to 7 days before archive space runs out

NetFlow Analyzer also warns you if your archive space is full and tells you exactly what actions are advised. Warnings are sent by email to NetVizura administrators and displayed when you log-in. Warning message is triggered when application concludes that Minimum free disc space will be reached before minimum amount of Raw Data files in days is stored (Minimum archive size in days).

The screenshot shows the 'Configuration' tab in the NetFlow Analyzer interface. It features a navigation bar with tabs for Patterns, Subnets, Subnet Sets, TopN, Alarms, Aggregator Filtering, Exporters, and Configuration. Below the navigation bar are 'Import' and 'Export' buttons. The main area is titled 'Service options' and contains several configuration fields:

- Service socket port: 2055 (UDP port number listening for NetFlow data)
- Socket timeout: 5 seconds (UDP socket timeout)
- Temp folder: /var/lib/icmynet/flow/temp (Folder in which ICMyNet.Flow will temporary unpack Raw Data files)
- Archived files folder: /var/lib/icmynet/flow/archive (Folder in which ICMyNet.Flow Aggregator stores processed files)
- Legacy raw files folder: /var/lib/icmynet/flow/legacy (Folder in which ICMyNet.Flow stores Raw Data files from previous versions)
- Maximum database size: 30 GB (Oldest data will be removed first)
- Minimum free disk space: 2000 MB (When free space on the Raw Data storage is less than configured oldest files will be removed)
- Minimum database size in weeks: 52 (The system will warn you before database space runs out)
- Minimum archive size in days: 30 (The system will warn you up to 7 days before archive space runs out)

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Example of archive warning message for Minimum number of days set to 30 and Minimum disk space set to 2 GB:

10 more days of data (30 GB) still need to be stored, but only 7 more days' worth of space (21 GB) remains in the archive storage.

You need to provide more space for archive files. You can also move existing files to another location, or lower the minimum number of days (currently set to 30) for which you would like to keep the archive files. (30) days of archive files is approximately 90 GB.

Flow archive stores Raw Data files. These files can be analyzed in the Raw Data tab in Flow module. When the Flow archive is full, oldest Raw Date files will be deleted, although those Raw Data files would fall within configured minimum number of days.

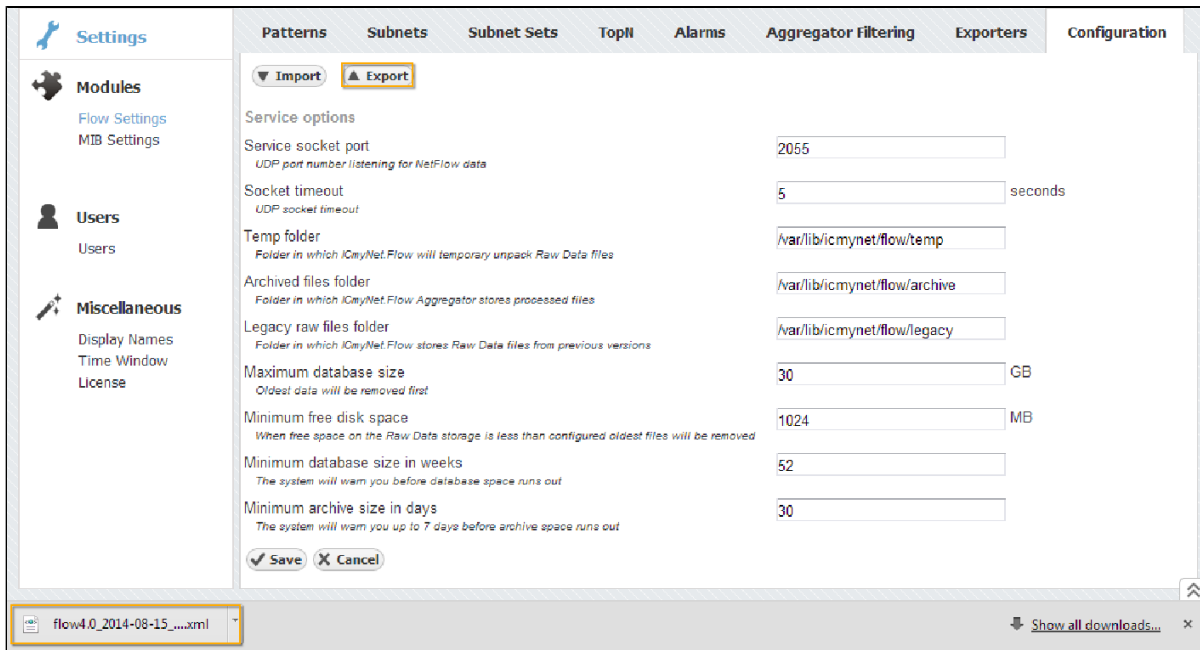
- Space estimation is based on the average size of your raw data file.
- Remaining space for the archive is calculated by deducting Minimum free disk space from the current available free disk space.
- In the above example, if Minimum free disk space is 2GB, the warning message will trigger when free disk space goes under 23GB.

Importing/Exporting Configuration

If you are upgrading software, you might want to transfer your previous configuration from old version to new version of your NetFlow Analyzer. This is possible by configuration export and import.

To export your configuration:

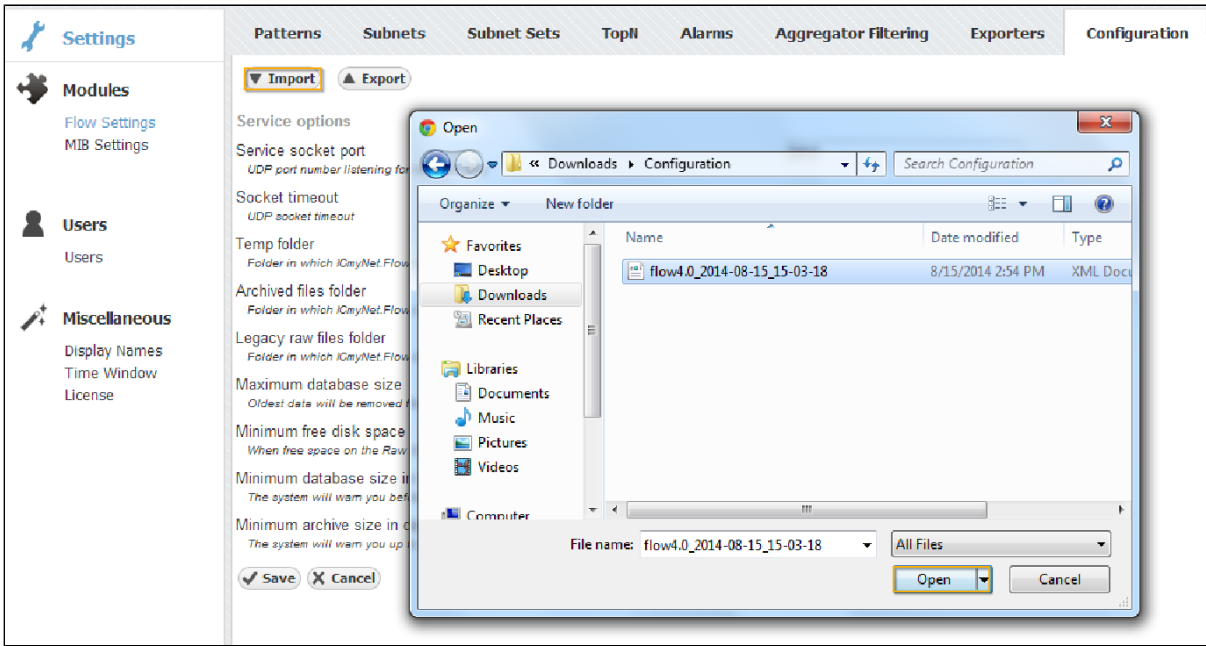
1. **Log-in** to old NetFlow Analyzer version
2. Go to **Settings > Flow Settings > Configuration** and click **Export**
3. Your configuration parameters will be downloaded in a XML file



If you already added Traffic Patterns, Subnets, Subnet Sets, alarms etc. to new version of NetFlow Analyzer, you will need to remove all entries before proceeding further to avoid duplication.

To import your configuration:

1. **Log-in** to new NetFlow Analyzer version
2. Go to **Settings > Flow Settings > Configuration** and click **Import**
3. Select the **XML file** and click **Open**
4. Verify that all your configuration parameters is correct

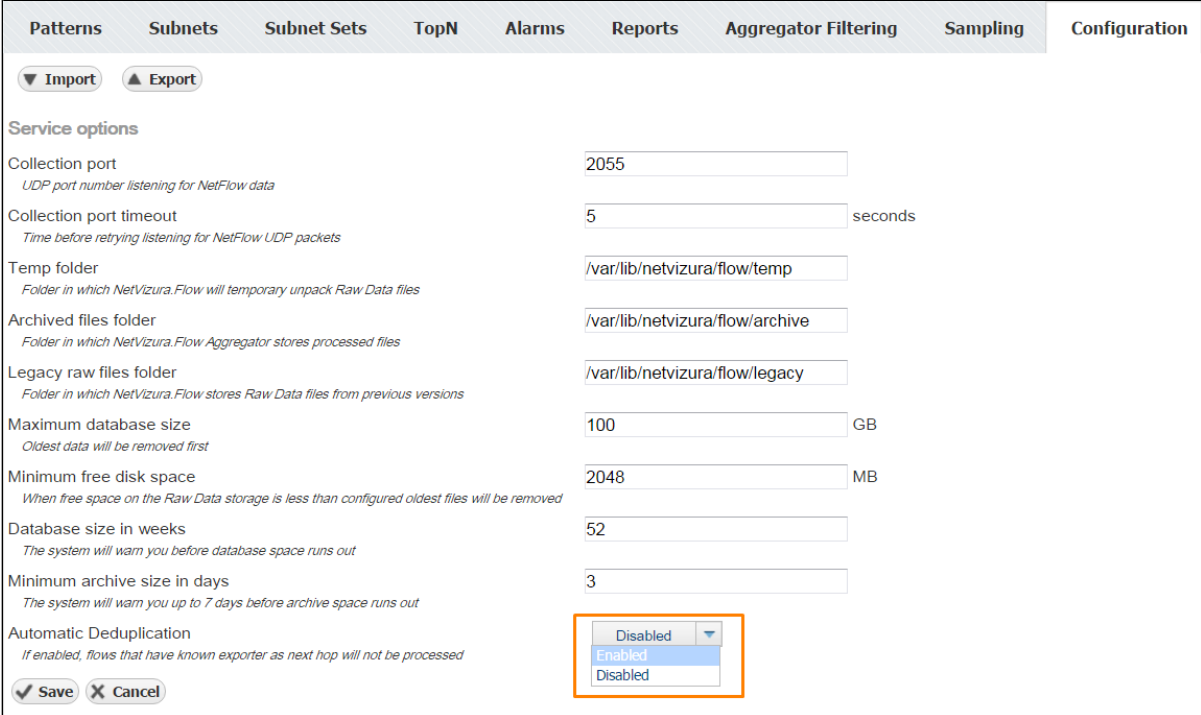


Automatic Deduplication

To understand duplication problem and how automatic deduplication is used, read article [Deciding Whether to Use Automatic Deduplication](#).

To enable automatic deduplication:

1. Go to **NetFlow Settings > Configuration > Automatic Deduplication**
2. **Select Enable**



The screenshot shows the 'Configuration' tab in the NetFlow settings interface. The 'Automatic Deduplication' dropdown menu is open, showing 'Enabled' selected. The interface includes various configuration fields for service options, such as collection port, timeout, and storage paths.

Field	Value	Unit
Collection port	2055	
Collection port timeout	5	seconds
Temp folder	/var/lib/netvizura/flow/temp	
Archived files folder	/var/lib/netvizura/flow/archive	
Legacy raw files folder	/var/lib/netvizura/flow/legacy	
Maximum database size	100	GB
Minimum free disk space	2048	MB
Database size in weeks	52	
Minimum archive size in days	3	
Automatic Deduplication	Enabled	

In order to achieve automatic flow deduplication in Traffic Patterns and Subnet Sets, it is required that ALL devices in flow continuity are configured as exporters.

EventLog Configuration

To access NetVizura EventLog settings go to Settings > EventLog settings.

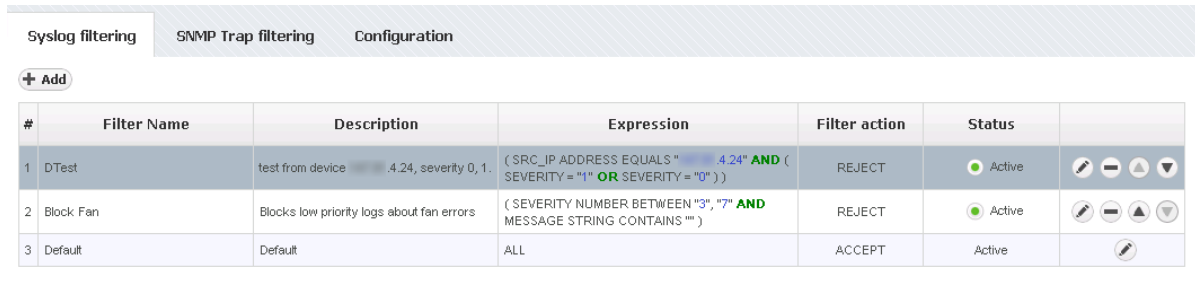
You have the option to configure Syslog filtering, SNMP Trap filtering and to configure NetVizura EventLog service and database maintenance options.

- [Syslog and SNMP Trap Filtering](#)
- [Configuring EventLog Alarms](#)
- [Configuring Eventlog System](#)










Syslog and SNMP Trap Filtering

Syslog Filters

Syslog Filters are used to make explicit rules to filter out unwanted syslog messages. Filtered out messages will not be processed, stored and showed in the EventLog charts and tables. To access Syslog Filters, go to Settings > EventLog Settings > Syslog filtering.



The screenshot shows a web interface for Syslog filtering. At the top, there are tabs for 'Syslog filtering', 'SNMP Trap filtering', and 'Configuration'. Below the tabs is a '+ Add' button. The main content is a table with the following columns: '#', 'Filter Name', 'Description', 'Expression', 'Filter action', 'Status', and a set of icons for editing, deleting, and moving. The table contains three rows:

#	Filter Name	Description	Expression	Filter action	Status	
1	DTest	test from device 10.4.24, severity 0, 1.	(SRC_IP ADDRESS EQUALS "10.4.24" AND (SEVERITY = "1" OR SEVERITY = "0"))	REJECT	Active	   
2	Block Fan	Blocks low priority logs about fan errors	(SEVERITY NUMBER BETWEEN "3", "7" AND MESSAGE STRING CONTAINS "fan")	REJECT	Active	   
3	Default	Default	ALL	ACCEPT	Active	

By default, there is only one Syslog Filter named Default that accepts all syslog messages. On the Figure 15: Syslog Filter Table you can see Syslog Filter list together with some filter examples. As you can see, each filter has:

1. Filter number
2. Description
3. Filter expression – condition for the filter expressed in text format
4. Filter action - reject or accept messages that match filter expression
5. Status – filter can be active or inactive

Looking at the second filter named "Block Fan" you can see that it is used to block (reject) fan related logs (log message contains the word "fan") of low priority (severity levels between 3 and 7) from any device.

Filter table is ordered which means that filters are applied in the order of the table: filter with the filter number 1 will be applied first, then rest will follow. Note that default filter is always the last one to be applied.

Ordering and Default filter allows you to have two filter strategies:

- Explicit reject: default filter accepts all messages, filters reject specific messages
- Explicit accept: default filter rejects all messages, filters accept specific messages

Default filter is always active, always the last to be applied, and the only change you can make to it is to change its Filter action (to accept or reject all messages).

Filter table has several quick options:

1. To make a filter active/inactive, click the Inactive/Active icon
2. To edit filter, click the edit icon., or double click on the filter table row
3. To remove filter, click remove icon
4. To change the position of the filter in the table, use the Up and Down icons

To Add a new filter, click the Add button at the top of the Filter table.

Adding New Filter

Filter information

Filter name:

Description:

```
Blocks fan messages if Severity is
not 0,1 or 2
```

Filter status: Active Inactive

Filter expression

Severity

Facility

Message

Action: ACCEPT REJECT

#	Filter Name	Description	Expression	Filter action	Status	
1	Default	Default	ALL	ACCEPT	Active	<input type="button" value="edit"/>

Filter expression is a set of conditions that need to be met in order for filter action to be triggered. Condition are based on the syslog message severity, facility, message content or device(s) that sent it (based on source IP address). Each condition type has several condition operands depending on the possible values, for instance Severity has options >, <, =, !=, >=, <= and "between" operands.

The conditions are added by clicking on the "+" icon and composite conditions are added by clicking on the "+()" icon. Composite conditions will appear in the filter expression in the brackets, and are generally used if you need a condition in the form of Cond1 AND (Cond2 OR Cond3).

Logical operator between condition are set by the drop-down list next to "+" and "+()" options: Match All (AND), Match Any (OR), Match None (NAND).




By default, filter action is set to Accept and filter status to Active.

Configuring EventLog Alarms

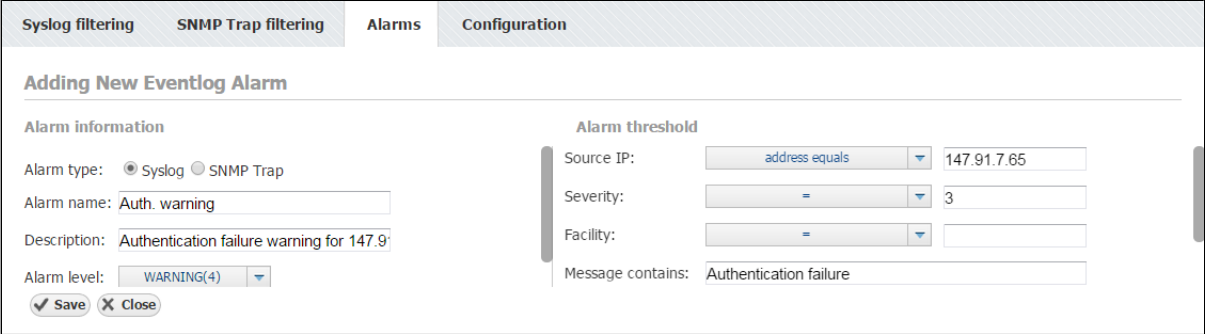
EventLog users can view and EventLog administrator can add, edit or delete alarms.

To configure EventLog alarms, go to **Settings > EventLog Settings > Alarms**.

To add a new alarm in EventLog:

1. Click **Add**
2. Set **Alarm information** (type, name, description and level)
3. Set **Alarm threshold**
 -  For Syslogs, threshold is based on source IP, severity, facility and message content
 -  For SNMP traps, threshold is based on source IP, OID and variable bindings.
 -  It is possible to combine more threshold criteria (AND logical operand is implied).

If you do not define a value to a certain criterion, that criterion will not be included in the Alarm condition.



The screenshot shows a web interface for configuring an alarm. At the top, there are four tabs: 'Syslog filtering', 'SNMP Trap filtering', 'Alarms', and 'Configuration'. The 'Alarms' tab is active. Below the tabs is the title 'Adding New Eventlog Alarm'. The form is divided into two main sections: 'Alarm information' and 'Alarm threshold'. In the 'Alarm information' section, there are radio buttons for 'Syslog' (selected) and 'SNMP Trap'. Below that is a text input for 'Alarm name' containing 'Auth. warning', a text input for 'Description' containing 'Authentication failure warning for 147.9', and a dropdown for 'Alarm level' set to 'WARNING(4)'. At the bottom left of this section are 'Save' and 'Close' buttons. The 'Alarm threshold' section contains four rows of configuration: 'Source IP' with a dropdown set to 'address equals' and a text input '147.91.7.65'; 'Severity' with a dropdown set to '=' and a text input '3'; 'Facility' with a dropdown set to '=' and an empty text input; and 'Message contains' with a text input 'Authentication failure'.

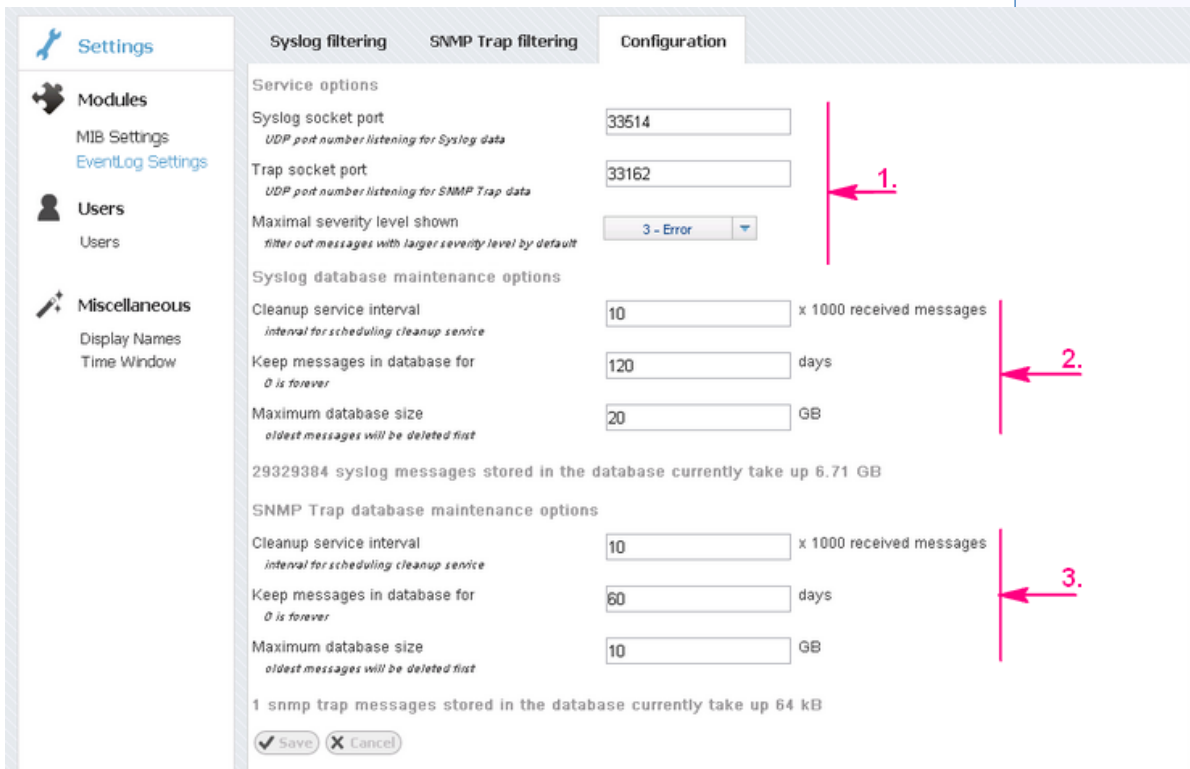
Screenshot above shows an example of an Alarm configuration. This alarms will trigger if syslog message is sent from 147.91.7.65, with severity level 3 and message containing Authentication failure.

Configuring Eventlog System

On this page:

- Service Options
- Database Maintenance

To access NetVizura EventLog settings go to **Settings > EventLog settings > Configuration**.

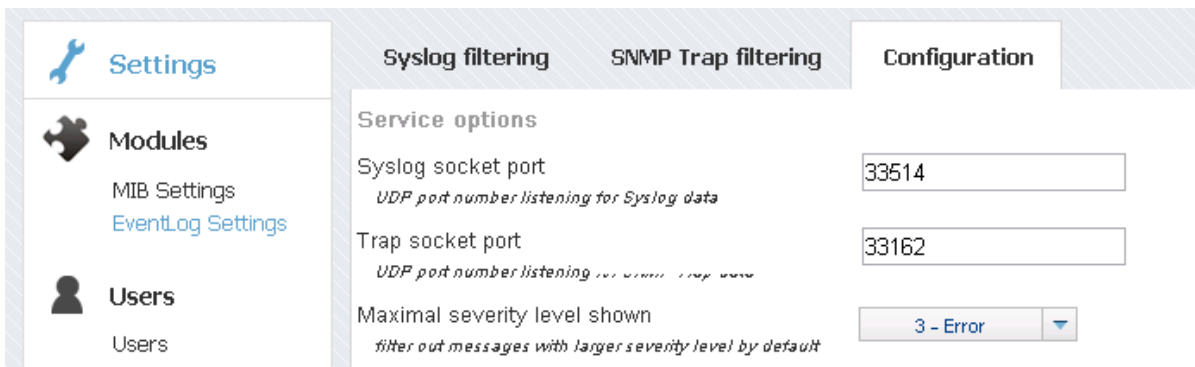


You have the option to configure:

1. NetVizura EventLog service options
2. Syslog database maintenance options
3. SNMP Trap database maintenance options

Service Options

To access Service options, go to **Settings > EventLog Settings > Configuration**.



In service options you can set listening port for syslog and trap messages, and view preferences.

To set *Syslog socket port*, change the value in the corresponding text field and click Save. Note that devices exporting syslog messages need to target this port (explicitly or via redirection).

To set *Trap socket port*, change the value in the corresponding text field and click Save. Note that devices exporting trap messages need to target this port (explicitly or via redirection).

By default, syslog messages are exported from the devices to port 514, while NetVizura listens on the port 33514. You need to (1) redirect syslog messages to the 33514, or (2) export syslog messages to 33514, or (3) change NetVizura EventLog configuration. Same applies to trap socket port.

Maximal severity level shown is by default set to 3 – Error which means that when you open EventLog module severity levels 0, 1, 2, 3 will be active in the Severity Table. To change the value, click on the drop down menu and choose a different value.

Database Maintenance

To access Database Maintenance, go to **Settings > EventLog Settings > Configuration**.

Syslog database maintenance options

Cleanup service interval <i>interval for scheduling cleanup service</i>	<input type="text" value="10"/>	x 1000 received messages
Keep messages in database for <i>0 is forever</i>	<input type="text" value="120"/>	days
Maximum database size <i>oldest messages will be deleted first</i>	<input type="text" value="20"/>	GB

On screenshot above you can see an example of database maintenance configuration: cleanup is triggered after every 10,000 messages and the cleanup service will delete messages that are either more than 120 old, or the oldest messages if the database size is more than 20GB.

To change database maintenance parameters, edit the corresponding text fields and click Save.

Setting the Keep messages in database for parameter to zero will switch off deletion of the messages in regards to their age. In other words, cleanup service will only delete messages if the maximum database size is exceeded.

MIB Configuration

To access MIB Browser settings go to **Settings > MIB settings**. Settings is accessible by clicking on the gear icon located in the upper right corner of the application.

You have the option to configure MIB modules, SNMP queries and search options.

- [Configuring MIB Modules](#)
- [Configuring MIB Options](#)

Configuring MIB Modules

On this page:

- Adding MIB Module
- Bulk MIB Module Import
- Removing MIB Module

In order to populate the MIB Tree and be able to send SNMP requests to devices, OID definitions need to be in the application database. If the MIB Tree does not have OIDs you need, you need to add the module that defines them.

To access MIB Modules, go to **Settings > MIB Settings > Modules**.

Modules		Configuration	
+ Add			
BGP4-MIB	05 Jan 1994	⊖	Counter32, Gauge32, Integer32, IpAddress, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE from SNMPv2-SMI; mib-2 from RFC1213-MIB;
BRIDGE-MIB	19 Jan 2005	⊖	MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP from SNMPv2-CONF; Counter32, Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE, TimeTicks, mib-2 from SNMPv2-SMI; InterfaceIndex from IF-MIB; MacAddress, TEXTUAL-CONVENTION from SNMPv2-TC;
CHARACTER-MIB	26 Jan 1994	⊖	MODULE-COMPLIANCE, OBJECT-GROUP from SNMPv2-CONF; Counter32, Gauge32, Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE, TimeTicks from SNMPv2-SMI; AutonomousType, DisplayString, InstancePointer, TEXTUAL-CONVENTION from SNMPv2-TC; InterfaceIndex from IF-MIB; mib-2, transmission from RFC1213-MIB;

On the screenshot to the left we can see MIB module table together with default MIBs. As you can see, table shows basic MIB parameters:

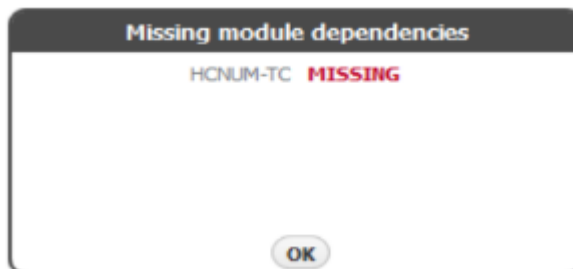
1. Name
2. Release date
3. Imports

Looking at the first MIB named "xxxx" we can see that it was released on 6th of January 1994 and that its imports mib-2 located in the MIB called RFC1213-MIB. This means that in order for BGP4-MIB to be added to the database, RFC1213-MIB had to be added before that.

Adding MIB Module

To add a new MIB module, click the **+ Add** button at the top left of the Module table.

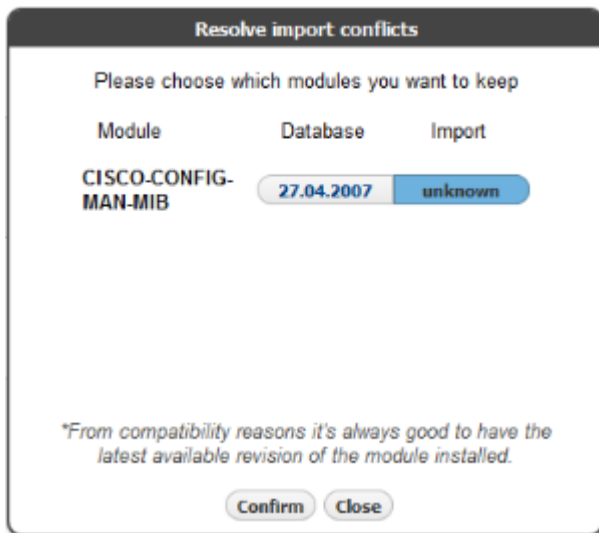
If you try to add a MIB and it fails, the application will show a list of imports needed for that MIB and the missing MIBs will be marked red.



For instance, if you want to add CISCO-CLASS-BASED-QOS-MIB you will have to add HCNUM-TC first. If you do not, you will get the message shown on screenshot to the right.

Bulk MIB Module Import

When importing, multiple MIB Module files may be chosen for import. All selected files will be imported successfully in case MIB Modules, you are importing, have not yet been uploaded. If that is not the case, appropriate dialog will be displayed, and you will be asked to resolve existing MIB Module conflicts. By default, the module you are trying to import will be selected for import, only if it is newer revision comparing to the module already in database. On the other hand, if the module you are trying to import has unknown or older revision comparing to one already in database, you can resolve import conflict by choosing the revision of the module you want to keep.



From compatibility reasons it's always good to have the latest available revision of the module installed.

Make sure not to select multiple MIB Module files with the same name when importing modules in bulk. In that case, there is no guarantee which module will be imported.

Removing MIB Module

To remove a MIB, click - (remove icon) in the Action column.

If some other MIB Module depends on the module you are trying to remove, application will show a list of all dependent modules and you will not be able to remove selected module until you remove all dependent modules. Otherwise, remove action will be successful.

Configuring MIB Options

To access MIB options settings go to **Settings > MIB settings > Configuration**.

Modules	Configuration
MIB options	
Search results <small>Number of MIB elements returned by a search</small>	<input type="text" value="50"/>
List response limit <small>Number of items returned by SNMP list request</small>	<input type="text" value="50"/>
Table response limit <small>Number of rows return by SNMP table request</small>	<input type="text" value="100"/>
<input checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>	

You have the option to configure:

1. Search results
2. List response limit
3. Table response limit

Search results sets the limit to the number of results returned using the Search option. When the number of found OIDs reaches the limit set here, the Search action will stop.

List response limit sets the limit of OID values returned and showed on a page as a result of SNMP request on a MIB tree element. When the number of found OID values reaches the limit set here, the SNMP walk will stop and the found OID values will be displayed. This limit is used to break very large SNMP request into several smaller ones.

For example, if you click Request on the MIB tree element that can return 200 OIDs and the List response limit is 50, in view mode first 50 results will show. When you click the Next button above the table, next 50 results will show etc. Effectively, this SNMP request has been broken down into 4 smaller SNMP requests.

If a MIB tree element is a table List response limit is ignored.

Table response limit sets the maximum number of table rows shown on a page as a result of SNMP request on the MIB tree element that is a table. Result of the request will be shown as a table with multiple columns and successive rows are displayed by clicking on the Next button above the table.

For example, if you have a MIB table containing 1000 OIDs organized in the 5 columns, we will have in total 200 rows. If the Table response limit is set to 50 then the resulting table after a SNMP request will shows first 50 rows (containing $5 \times 50 = 250$ OIDs). When you click the Next button above the table, next 50 rows will show etc. Effectively, a very large table is shown in 4 steps.

Troubleshooting

- General Troubleshooting
 - NetVizura is slow
 - Web interface not running
 - How to recover from Exception caught: 500 The call failed on the server
 - How to recover from RPC failure error
 - How to restart the application
 - How to submit a request
- NetFlow Troubleshooting
 - No NetFlow traffic captured
 - End User traffic impact on NetVizura performance
- EventLog Troubleshooting
 - I do not receive any Syslog messages
 - I set the Syslog socket port to 514 but I am still not receiving syslog messages (Linux)
- MIB Troubleshooting
 - SNMP request lasts too long
 - SNMP request fails on a device
 - I can not add a MIB to Modules
 - I can not find an OID in the MIB tree
 - I can not set the OID value on a device

General Troubleshooting

- NetVizura is slow
- Web interface not running
- How to recover from Exception caught: 500 The call failed on the server
- How to recover from RPC failure error
- How to restart the application
- How to submit a request

NetVizura is slow

Problem

NetVizura is slow: long time for loading graphics, tables etc.

This usually happens if RAM is not allocated to NetVizura services: PostgreSQL and Tomcat. After installation it is needed to tweak the configuration files in order to utilize the installed RAM to the fullest extent.

Solution

To tweak PostgreSQL and Tomcat memory allocation follow the instructions on links below:

1. For DEB Linux installation: [Linux DEB \(Debian&Ubuntu\) Installation#Postinstallsteps](#)
2. For RPM Linux installation: [Linux RPM \(CentOS\) Installation#PostInstallSteps](#)

If the memory is already fully allocated, add more memory to the server and re-tweak PostgreSQL and Tomcat to use the extra memory.

Related articles

- [NetVizura is slow](#)
- [Web interface not running](#)
- [No NetFlow traffic captured](#)
- [How to restart the application](#)
- [How to recover from RPC failure error](#)

6 related results

Web interface not running

Problem

Web interface is not responding.

Solution

Web interface is started via browser using Tomcat and PostgreSQL service. The interface is access by typing `http://netvizura_server_ip:8080/netvizura`.

Follow these steps:

1. Check if your IP is correct
2. Check if port 8080 is open on the NetVizura server
3. Check if tomcat service is up (using `top` command)
 - a. if not, try to start it (`service tomcat6 start`)
 - b. if it can not be started check which services are installed:
 - i. The listing of `/etc/init.d`
 - ii. The listing of command `service --status-all`
 - iii. The listing of command `chkconfig -list`
4. Check if PostgreSQL is up (`service postgresql-9.3 status`)
 - a. if not, try to start it: `service postgresql-9.3 start`

Note

`tomcat6` and `postgresql-9.3` are examples of Tomcat and PostgreSQL installation. Name of services and their versions on your server may differ.

If the problem persists please contact us at support@netvizura.com and send us the following:

1. On which virtual (or physical) platform have you installed NetVizura (VMWare Workstation, Proxmox, Xen, physical machine...)
2. The listings of commands ran in step 3.b. above
3. Entire zipped directory `/var/log/tomcat6/`
4. File `/var/log/pgsql`
5. Entire zipped directory `/var/lib/pgsql/9.3/data/pg_log/`
6. Entire zipped directory `/var/log/netvizura/`

How to recover from Exception caught: 500 The call failed on the server

Problem

When trying to login, application displays the following error: "Exception caught: 500 The call failed on the server". This can happen if the browser window with the application stayed open during update or if the browser session has expired or if database is not running.

Solution

1. Refresh browser (Ctrl+F5) and then log in again OR log out and log in manually.

If this doesn't work, access the server via ssh and execute the following commands:

1. Check the status of database and start the postgresql service
 - a. `service postgresql-9.3 status`
 - b. `service postgresql-9.3 start`
2. Restart tomcat6 service (to register the application on the database)
 - a. `service tomcat6 stop`
 - b. `service tomcat6 start`

Info

Names of Tomcat and PostgreSQL services in these article are an example. Check which version of these services are installed on your server and use those names in the commands listed above. For example, if you have installed Tomcat 7 the command 2a will be `service tomcat7 stop`

How to recover from RPC failure error

Problem

Application displays RPC failure error. This happens if session has expired in browser you use to access the application.

Solution

Refresh browser (Ctrl+F5) and then log in again OR log out and log in manually.

How to restart the application

Problem

Application is not collecting or processing data (syslog, netflow). This is manifested by empty charts and presence of dropped packets in System view of the corresponding application module. This can happen due to low memory, power outage on the server.

Solution

Access the server via ssh and execute the following commands:

Execute commands in strict order to avoid improper application restart. Tomcat service must be started after PostgreSQL for instance.

1. `service tomcat6 stop`
2. `service postgresql stop`
3. `service postgresql start`
4. `service tomcat6 start`

Check the names of your services before attempting stop and start commands.. Names of Tomcat and PostgreSQL services may differ on different installations. For Example Tomcat may be tomcat6 or tomcat7 and PostgreSQL may be postgresql-9.2 or postgresql-9.3

How to submit a request

Contact Us

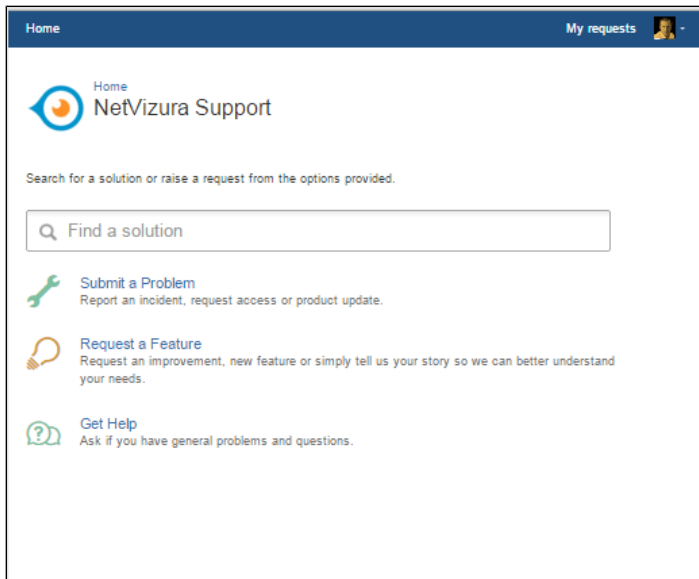
If you need to report a problem, request a new feature or ask for help, you can contact NetVizura team in two ways: submit a customer request on our Support portal or email us.

1. **Customer Portal**

Go to web page <http://jira.netvizura.com/servicedesk/customer/portal/1> and login to your account.

On this page:

- Contact Us
 - Customer Portal
 - Email
- Submit a Problem



Here you can see previous request tickets, their statuses and correspondence. You will get notified on status changes and NetVizura team replies via email.

i If you don not have an account:

- a. Send initial email to support@netvizura.com
- b. You will receive automatic reply with the link to the portal page
- c. Enter password to complete registration and enter your account


2. **Email**

Send an email to support@netvizura.com. This will automatically open a ticket on our Customer Portal. After support agent reviews your request, you will receive notification reply that support ticket is in progress.

Tue 14/04/17 03:08 AM

Jack Lousma <no-reply@jira.netvizura.com>
 [JIRA] [NetVizura Support] Houston, we've had a problem! [NVSUP-13]

To jim.lovell@apollo13.com

 If there are problems with how this message is displayed, click here to view it in a web browser.

NetVizura Support - Submit a Problem Reference: NVSUP-13

Houston, we've had a problem! IN PROGRESS

Your request status changed to **In Progress**.

Today 03:08


Roger. MAIN B UNDERVOLT.

Okay, stand by, 13. We're looking at it.

You can [view the full request](#)

Previous activity

Jim Lovell
 Today 03:08



Details

Description	Houston, we've had a problem. We've had a MAIN B BUS UNDERVOLT.
Version	7
Build	103
Priority	Critical


You can continue to reply via email (ticket will be updated automatically) or start using the Customer Portal.

Please do not change the Subject line (eg. "[JIRA] (NetVizura Support) Houston, we've had a problem! [NVSUP13] "). This will ensure that all relevant information (emails, comments etc.) are synchronized with the ticket on our Customer Portal.


Submit a Problem

Before submitting a problem, please try to find a solution in the search box provided at <http://jira.netvizura.com/servicedesk/customer/portal/1>.


If none of the provided resources help, we kindly ask you to send necessary information so that we can quickly analyze, diagnose and provide solution to your problem:

1. Summary and Description of problem
2. Version and Build of the application (**About** in the upper right corner of the application)
3. Screenshot of the problem
4. `/var/log/tomcat6(7)` ( **whole directory**, not just the last file)
5. System tab > Performance, Flow screenshots (if problem is performance related)
6. Environment
 - a. HW: CPU, RAM, HDD (if problem is performance related)
 - b. SW: OS, Java, PostgreSQL, Tomcat, browser (if problem is dependence related)
7. Priority (optionally)

Example:

Home My requests 

Home / NetVizura Support
Submit a Problem


Raise this request on behalf of
 Jim Lovell

Summary

Description

Version

Build

Attachment

Apollo13_spacelog.out
[Choose file\(s\)](#)

Environment (optional)

Priority (optional)

NetFlow Troubleshooting

- No NetFlow traffic captured
- End User traffic impact on NetVizura performance

No NetFlow traffic captured

Problem

NetFlow export is started on the devices but there is no NetFlow traffic in the application.

Solution

NetFlow traffic may not show due to several reasons:

- Firewall and access lists are blocking netflow packets
- Collection port is not opened
- Collection port has already being used by a different application
- Bad netflow exporter configuration
- Aggregation filter is filtering out the traffic
- License has expired
- NetFlow packets are being dropped

To determine the cause and solution please do the following:

1. Go to System tab:
 - a. check the Packets chart (netflow packets that the application collected)
 - i. if there are no UDP packets received go to steps 2 to 3.
 - ii. if there are dropped packets restart Tomcat service for temporary quick fix and go to step 1c to resolve the core problem
 - b. check Flows chart:
 - i. if there are no flows this means that no netflow data is received by the application, go to steps 2 to 3.
 - ii. if all flows are unlicensed, your license is invalid or expired - contact us for resolving this
 - iii. if all flows are filtered, go to Settings > NetFlow Settings > Aggregation filtering and remove the filter rejecting all flow
 - iv. if all flows are dropped, try restarting the tomcat service and contact us if the problem persists
 - c. check Performance chart:
 - i. if Heap utilisation is high try adding more RAM to Tomcat and PostgreSQL services (consult Post installation steps)
 - ii. if DB write time is high try adding more CPU cores to the server
 - iii. if you are not sure what to do contact us at support@netvizura.com
2. Check if NetFlow data is received by the server:
 - a. in command shell on the server execute `tcpdump port 2055 command` - you should see steady stream of packets received by the server (2055 is the default NetFlow port)
 - i. if there is no netflow packets check your firewalls, access lists to enable packets to be received by NetVizura server;
 - b. in command shell on the server execute `watch -n1 "ls -l /var/lib/netvizura/flow/temp"` - after several seconds you should see that `tmp.bin` file size is increasing
 - i. if `tmp.bin` file size is not increasing, but `tcpdump` shows that netflow packets are reaching the server check your local firewall configuration (usually iptables) or NetVizura NetFlow Collection port (see below).

3. Check if Collection port on the server is open and that NetVizura is listening on that port
 - a. Check that firewall is allowing packets on NetFlow port (the default is 2055)
 - i. Execute command `service iptables status` to view firewall configuration. There has to be a line present which is allowing traffic on NetFlow port (2055)
 - b. Check that NetVizura is listening on NetFlow port
 - i. Execute command `netstat -noap | grep 2055` and verify that there is a line present similar to following:

```
udp          0          0 :::2055
:::*
28004/java   off (0.00/0/0)
```

It is important that *java* process is the one that occupied NetFlow port - not some other process. If some other process already occupied NetFlow port you need to reconfigure that other process to use a different port.

- c. Check that Collection port is accessible outside the NetVizura server
 - i. on a remote host execute command `nmap netvizura_ip_address -sU -p 2055` where `netvizura_ip_address` is the address of NetVizura server. In the output of the command you should see that the port is open.
4. Check netflow exporter configuration:
 - a. Check if netflow device is configured to send netflows to the NetVizura server IP address and collection port
 - i. Collection port in NetVizura application can be set in Settings > NetFlow Settings > Configuration
 - ii. Default Collection port is 2055
 - b. Try installing a netflow generator and set it to export data to the NetVizura server
 - i. if there is traffic on the chart then netflow exporter configuration is not good
 - ii. if there is no traffic on the chart, check if the traffic is being blocked (access lists, firewalls)

End User traffic impact on NetVizura performance

In general, NetVizura performance primarily depends on the inherited number of counters (nodes) and number of users you want to monitor. End User traffic does not significantly affect CPU, HDD and DB write time. However, it may have impact on:

1. RAM usage
2. Shared Syslog db usage

RAM increase

Depending on the RAM availability it increases it more or less (when RAM is less available it can increase by only a couple of percentages, when RAM is more available it can increase up to 100%).

There is a way to optimize NetVizura RAM usage by tweaking JAVA. Read more about Post-install steps within specific [Installing](#) article.

Shared Syslog database increase

If you use also NetVizura EventLog Analyzer, end user syslog logon messages share database storage with the rest of syslog messages and might increase disk usage thus triggering removal of old syslog messages sooner.

Consider increasing Maximum database size within [Syslog Database Maintenance Options](#).

EventLog Troubleshooting

- I do not receive any Syslog messages
- I set the Syslog socket port to 514 but I am still not receiving syslog messages (Linux)

I do not receive any Syslog messages

There are several possible reasons for not receiving syslog messages:

1. Syslog export port and NetVizura Syslog socket port do not match
2. NetVizura server has firewall (port is not opened)
3. Devices exporting syslog and NetVizura server are not connected

Syslog export port and NetVizura Syslog socket port do not match

Syslog socket port in Settings > EventLog Settings > Configuration needs to match the port on which you are sending syslog messages. You need to (1) redirect syslog messages to the 33514, or (2) export syslog messages to 33514, or (3) change NetVizura EventLog configuration so that the export port (devices or redirection) match the Syslog socket port in the configuration. Check the IP table to see if redirection is applied.

On Linux systems ports lower than 1024 can not be used by application. Tomcat web server running NetVizura EventLog needs to be started by root user to allow NetVizura EventLog service to listen on ports lower than 1024.

NetVizura server has firewall (port is not opened)

Port to which syslog messages are exported to (Syslog socket port in Settings > EventLog Settings > Configuration) might not be opened during installation process, if so, you need to manually open that port. Check your software firewall on the NetVizura server and open the port. Iptables is an example of firewall on CentOS and RedHat systems.

Devices exporting syslog and NetVizura server are not connected

Contact your system and network administrators and make sure that all devices exporting syslog messages have network connection to the server running NetVizura EventLog.

I set the Syslog socket port to 514 but I am still not receiving syslog messages (Linux)

Problem

Port lower than 1024 on Linux systems can only be used by root.

Solution

If NetVizura doesn't have root privileges then you need to set the port to one higher than 1024 and redirect the Syslog messages to that port.

MIB Troubleshooting

- SNMP request lasts too long
- SNMP request fails on a device
- I can not add a MIB to Modules
- I can not find an OID in the MIB tree
- I can not set the OID value on a device

SNMP request lasts too long

SNMP request can take too long if the number of SNMP request retries and timeout are set to high for the policy used to access the device.

Go to **Settings > Control Panel > SNMP Policies** and check the parameters **Retry** and **Timeout** for the policy used on the device. You can see which policy is configured on the device by going to **Settings > Control Panel > Devices**.

For more information, go to chapter [Configuring SNMP Policies](#).

SNMP request fails on a device

There are several possible reasons for SNMP request to fail on a device:

- Policy used to access device is wrong
- Access list doesn't allow access to the device
- SNMP not enabled on the device
- Device is not available

Policy used to access device is wrong

Policy of the device has to match SNMP configuration on that device. Policy is defined in the **Settings > Control Panel > SNMP Policies**, and policy is set to a device in the **Settings > Control Panel > Devices**. Check SNMP version and Community string first.

For further information, go to articles [Configuring SNMP Policies](#) and [Configuring Devices](#).

A quick way to check if a policy is working on a device is to go to **Settings > Control Panel > Devices**, double click on a device and then clicking on the **Test** button.

Access list doesn't allow access to the device

Check if the access list allows access to the device from NetVizura server (server's IP has to be permitted).

Multiple access list might need to be checked.

SNMP not enabled on the device

Check if the SNMP is enabled on the device, if not – enable it.

Device is not available

Device might not be available because network is not working properly, SNMP access is not permitted or the device is down (no power for instance). Try to ping the device to check it's availability or contact your network engineers.

I can not add a MIB to Modules

There are two possible reasons for not being able to add a MIB to Modules:

- MIB is dependent on other MIBs
- MIB has a syntax error

MIB can only be added to Modules if all MIBs that it is dependent on are already added in the Modules. Application will inform you of the list of missing MIBs. You need to download all the missing MIBs from the list and add them before trying to add the desired MIB again.

For more info on adding a MIB, go to article [Configuring MIB Modules](#).

In some cases the MIB file can contain syntax error(s) that does not allow the application to parse it. You can try to fix the file yourself, or rise a support case by sending an email to support@netvizura.com.

I can not find an OID in the MIB tree

There are two possible reasons for not being able to find an OID in the MIB tree:

- OID number or name is mistyped
- MIB containing the OID is not in the application database

Double check the OID number or name first.

If this is OK, then you need to add a MIB containing the OID to the application. Download the MIB (from vendor website for instance) and then add it to the database by going to **Settings MIB Settings > Modules**.

For more info on adding a MIB, go to article [Configuring MIB Modules](#).

I can not set the OID value on a device

There are two possible reasons for not being able to set the OID value on a device:

- Policy used to access device is READ instead of READ_WRITE (application settings)
- SNMP configuration on a device itself has no write privileges

To check privileges of a policy go to **Settings > Control Panel > SNMP Policies** and double click on the policy.

If the problem persist, contact your network engineers to check if the SNMP configuration on a device is READ only.

In order to get the Set OID option, you need to have write or administrator privileges.

FAQ

- [License FAQ](#)
- [NetFlow FAQ](#)

License FAQ

Can I switch from Trial to commercial version without reinstalling NetVizura?

Yes. Upon purchase you will be given a new license key which will activate modules and features according to your license pack. This enables you to keep all the data and configuration.

What can I do with the NetVizura Trial version?

NetFlow Analyzer Free Trial was made for evaluation on any network, regardless of network topology or complexity. Evaluation period is 30 days from the day of installation. NetFlow AnalyzerFree Trial will process up to 10.000 flows per minute. There are no other functional restrictions. If you want to extend the evaluation period, please contact us at support@netvizura.com

Can I prolong the trial period?

You can find these useful statistics in the System Tab of NetFlow Analyzer. Number of total flows received, number of flows processed, as well as the number of flows missed due to license limitation are shown. This data is calculated and refreshed periodically every 5 minutes.

How do I upgrade?

You can find these useful statistics in the System Tab of NetFlow Analyzer. Number of total flows received, number of flows processed, as well as the number of flows missed due to license limitation are shown. This data is calculated and refreshed periodically every 5 minutes.

My support period has expired. How do I renew it?

You can find these useful statistics in the System Tab of NetFlow Analyzer. Number of total flows received, number of flows processed, as well as the number of flows missed due to license limitation are shown. This data is calculated and refreshed periodically every 5 minutes.

How do I choose a license pack?

You can find these useful statistics in the System Tab of NetFlow Analyzer. Number of total flows received, number of flows processed, as well as the number of flows missed due to license limitation are shown. This data is calculated and refreshed periodically every 5 minutes.

How can I buy NetVizura?

Please contact us at sales@netvizura.com and we will find the best licensing and payment model that suites your requirements and business.

NetFlow FAQ

What is an IP flow?

IP flow is an unidirectional stream of IP packets of a certain network protocol, traveling between two network points. IP flow is identified by the source and destination IP address, source and destination port, protocol and DSCP field, within a certain period of time. Within an IP flow all IP packets have identical:

- Source and destination IP addresses
- IP header protocol number
- IP header ToS field (DSCP)
- Source and destination ports if the TCP or UDP protocols are used

What is IP flow accounting?

IP flow accounting is a feature of a router enabling it to create IP flows collection, count IP flows passing through it and to export the traffic via NetFlow® protocol. The collection itself consists of the following data:

- Number of packets in IP flow
- Number of bytes in IP flow
- Timestamps

What is NetFlow?

NetFlow is a network protocol, developed by Cisco Systems, used for exporting collected IP flow traffic. This data is exported to a server, where it is collected, processed, aggregated and archived. It can then be reviewed in a more user-friendly form. NetFlow Analyzer performs all of these functions. There are numerous NetFlow protocol versions, most important of which are versions 5 and 9. Version 5 is commonly used on most Cisco NetFlow enabled devices. NetFlow version 9 is the latest version, created to support advanced technologies such as MPLS, IPv6, Multicast, VLANs, etc.

Which devices support NetFlow?

NetFlow® technology was developed by Cisco Systems, so all of the Cisco IOS routing platforms can export NetFlow data. From Cisco Catalyst switching platforms, only Catalyst 6500 series multilayer switches support NetFlow data export. Other vendors are also offering NetFlow-like capabilities on their network devices. These similar technologies are named differently by different vendors, for example J-Flow® by Juniper, NetStream® by Huawei, IPFIX® by Nortel etc.

Which versions of NetFlow protocols are supported by NetFlow Analyzer?

NetFlow Analyzer is based on Cisco NetFlow protocol versions 5 and 9. NetFlow Analyzer also supports IPFIX. The system is capable of recognizing protocol formats from other vendors, which are compatible with NetFlow protocol versions 5 and 9 such as Juniper J-Flow, Huawei NetStream.

However, NetFlow Analyzer has been tested to support NetFlow enabled Cisco devices and IPFIX from Juniper devices only.

NetFlow Analyzer utilizes Traffic Patterns which are based on IP addresses and not on physical interfaces, this allows NetFlow Analyzer to support netflow probes - software generated NetFlow-like protocol. One such (free) software is Softflowd, available at <http://code.google.com/p/softflowd/>.

Indirectly, sFlow is supported if you convert it to NetFlow, using free tool such as sFlow Toolkit, available at <http://www.inmon.com/technology/sflowTools.php>.

What is the network traffic overhead generated by the NetFlow data export?

NetFlow data overhead is expected to be less than 0.5% of the total network traffic included in the charts. This means, for instance, that 1 Mbps user traffic will produce approximately 50 kbps of additional traffic exported from routers to NetFlow Server.