

Traffic Pattern Settings

NetFlow users can view and NetFlow administrator can add, edit, delete or clone a Traffic Pattern.

Traffic Patterns allow you custom monitoring of any specific traffic type you want, independently of your physical infrastructure. For example:

- All traffic - *comes predefined* (entire network overview)
- Internet traffic (with external network)
- Email traffic (with your email server)
- Social networks (Facebook, YouTube, etc.)
- Blocked traffic (sent to Null interface)

To create new or configure existing Traffic Patterns, go to [blocked URL](#) > **Settings** > **NetFlow Settings** > **Patterns**.



If you are not familiar with Traffic Patterns, go to article [Traffic Patterns](#) and then proceed to [Traffic Pattern Examples](#).

Patterns	Subnets	Subnet Sets	Topik	Alarms	Aggregator Filtering	Exporters	Configuration
ADD	Name	Description	Internal Included	Internal Excluded	External Included	External Excluded	Action
All Blocked Traffic	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	-	-	-	
Proxy1	Proxy	Proxy	1.1.1.1/24	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	
User	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	
Unwanted	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	
OpenPorts	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	
Internet traffic	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	-	-	0.0.0.0/0 0.0.0.0/0 128.0.0.0/1	

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.