

# 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.

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 [blocked URL](#) > **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 [Manual Deduplication](#).

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

Exporter IP	Interface In	Interface Out
<input type="text" value="X.Y.4.38"/>	<input type="text" value="2"/>	<input type="text" value="5"/>

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](#)



- 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

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 3

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 [blocked URL](#) > **Settings** > **NetFlow Settings** > **Patterns**
2. **Add** new or **Edit** existing pattern
3. Click the **Service** tab.

Screenshot below shows the an example of service filter.

Address	Exporter	Service	AS	Protocol	Quis	Next Hop
Service filters parameters:						
Source ports: <input type="text"/>						
<input type="text"/>						
Destination ports: <input type="text"/>						
<input type="text"/>						
<input type="checkbox"/> Include <input type="checkbox"/> Exclude <input type="button" value="+ Add"/> <input type="button" value="X Reset"/>						
Source Port				Destination Port		
All				All		
All				All		



To cancel any changes to the filter, click **Reset**.



If you do not know the service you wish to include/exclude, go to [blocked URL](#) > **Settings** > **Display Names** > **Service** tab and do a search on the desired service port.

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**

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:

Address	Egnetur	Service	AS	Protocol	QoS	Next Hop
AS criteria parameters: Source AS number(s) <input type="text"/>						
Destination AS number(s) <input type="text"/>						
<input type="checkbox"/> Include <input type="checkbox"/> Exclude <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> None						
Source AS			Destination AS			
100			AS			
1243			AS			
4244			AS			
5765			AS			
AS			1242			
AS			1243			
AS			4244			
AS			5765			



- 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 [blocked URL](#)  
**> Settings > Display Names > AS** tab and do a search on the desired ASN

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:



If you do not know the Protocol Number of the protocol you wish to include/exclude, go to [blocked URL > 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:



If you do not know the exact ToS for the QoS level you want to monitor, go to [blocked URL > 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:



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](#).