# Using Alarms in NetFlow Module

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)
- several traffic types (total, host, conversation...)
- for bps, pps, fps traffic or its combination
- for different direction of traffic (total, in, out, src in...)

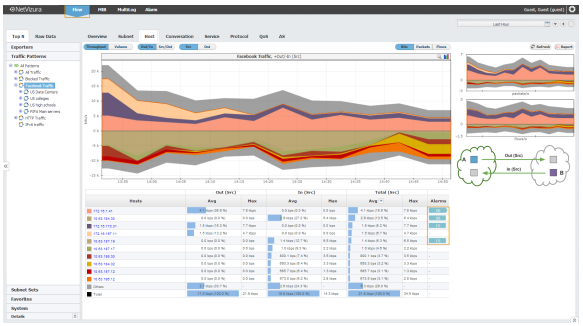
Alarms can be sent to certain users to speed up notification of the right person.

**On this page:**



## Viewing Alarms in NetFlow module

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.

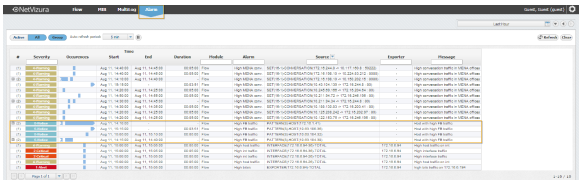


Click on the alarm indicator will take you to more detailed view of the alarm in the Alarm module.

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.

Here you can see the list off 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. 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.

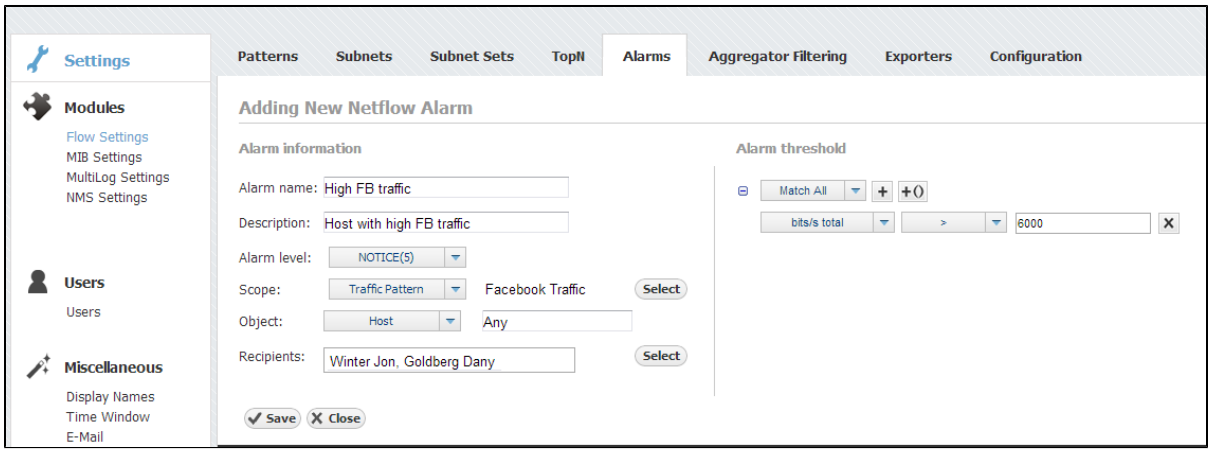



Figure above shows an example of an Alarm. This alarms triggers if any host in the network has more than 6 kbps of Facebook traffic in 5 minutes. Facebook traffic is identified via Facebook Traffic Pattern. On alarm trigger an email will be sent to Winter Jon and Goldberg Dany.