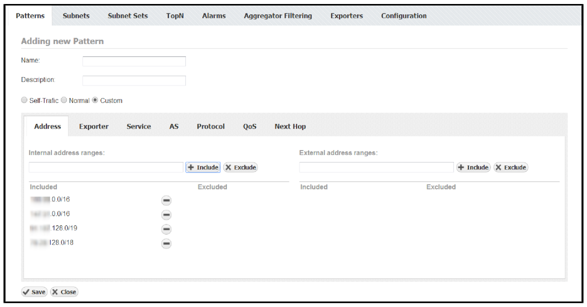
Setting IP Address Ranges

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:



Adding new Pattern

Name:

Description:

○ Self-Trafic ○ Normal ● Custom

Internal address ranges:

Included	Excluded
[redacted].0.0/16	
[redacted].0.0/16	
[redacted].128.0/19	
[redacted]128.0/18	

External address ranges:

Included	Excluded

In this screenshot you can see a Traffic Pattern were Internal network consist 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 you Internal network. These three types will also help you create Traffic Patterns more quickly because they will include or exclude some address ranges form 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.