

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 you company's IP address range and exclude your data center's IP range in Internal Network, and include you 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.