Understanding Traffic Patterns

Traffic Pattern Concept

What is a Traffic Pattern? It is a logical structure you create in order to analyze the network traffic you are interested in. Traffic Patterns are completely independent of the physical infrastructure. This enables you to focus on logical properties of your traffic instead focusing on physical links, network devices and their interfaces.

Traffic Pattern is a part of the totally collected network traffic. It represents the traffic between two networks, namely:

- **Internal Network** - usually represents the whole or part of your internal network (company network) from which the NetFlow data are exported and collected
- **External Network** - can be an arbitrary network – other part of your network (such as a network in another city, database center etc), Internet provider's network, or the entire Internet.

The traffic between the Internal Network and External Network is always bidirectional. This means that the Traffic Pattern will match the traffic going from the Internal Network to External Network, and from the External Network to Internal Network. The statistics are generated for the traffic between Internal and External Networks separately in two opposite directions, referenced from the Internal Network perspective:

- **Outgoing (Out**) traffic – going out of the Internal network or, in other words, traffic sourced from the Internal Network and destined to the External Network.
- **Incoming (In)** traffic – coming into the Internal network or, in other words, traffic sourced from the External Network and destined to the Internal Network.

Types of Traffic Patterns

There are three types of Traffic depending on the direction of traffic in regards to you Internal network:

- **Self Traffic** - within one network. In other words, source and destination of the traffic are both within a single network. Naturally, the network in question has to be within your internal network. In this case, your internal network (or its part) is both Internal Network and External Network. In the case of Self Traffic, outbound traffic volume is the same as the inbound traffic volume.
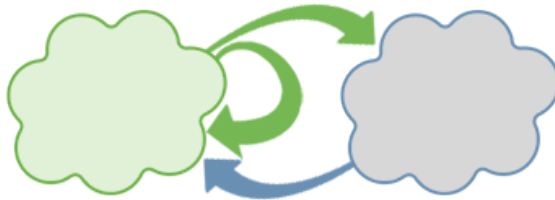

- **Normal Traffic** - between two different networks (network IP ranges do not overlap). Usually, one of these network is your company' network (or its part) and some external network such as the whole Internet or some specific network like Facebook.
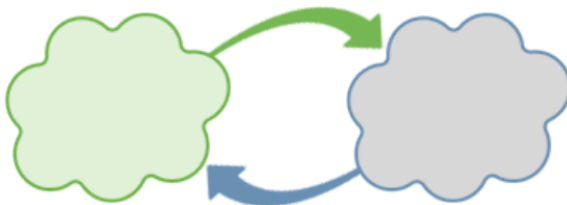
- **Custom Traffic** - a combination of Self-Traffic and Normal Traffic. For example, if you want to track the entire network communication of your PR department. This means tracking (1) to witch part of your company network did they communicate with and (2) to which networks outside of your company network did they communicate with. The Internal Network is your PR department and the External Network is all networks except PR department network.

> ⓘ Traffic Pattern's Internal and External networks are defined by IP address ranges and other parameters collected by the NetFlow and similar protocols can be used as filters to further specify Traffic Patterns. Learn more about Traffic Pattern Settings.

Differences between Exporter Traffic and Traffic Pattern

	Exporter Traffic	Traffic Pattern
Setup	✅ provided by default	✅ requires custom setup
Based on	✅ physical infrastructure	✅ logical definition
Nodes	✅ exporters and interfaces	✅ traffic patterns, subnet sets and subnets
Monitors	✅ traffic on routers, L3 switches and interfaces	✅ specific (custom defined) traffic
Analysis focus	✅ whole traffic on specific physical infrastructure	✅ specific traffic between two network ranges
Level of expertise	✅ fast setup and easy to understand	✅ complex setup and harder to understand

In general you will use:

- Exporter Traffic when you are interested in monitoring the bandwidth of an interface or exporter (whole traffic passing through the physical infrastructure)
- Traffic Patterns to isolate a specific type of traffic (traffic via specific ports, protocols, AS etc.): YouTube Traffic, certain service traffic, blocked traffic etc.
- Traffic Patterns with Subnet Sets to monitor whole or specific traffic per logical unit: company departments, regional company offices, member organizations, data center traffic etc.