Advanced Traffic Patterns

ⓘ This article uses filtering based on netflow parameters. For more information on how to add a specific filter, see chapter Traffic Pattern Settings and article Fine-tuning a Traffic Pattern.

On this page:

Discarded Traffic Pattern

Discarded Traffic is the traffic that your network devices send to the Null interface. On Cisco routers, traffic is sent to the null interface if you have invalid routing (routing tables are not complete) or the traffic is blocked by access lists. So, this traffic can give you information on (1) routing problems and (2) on blocked traffic, which is potentially an attack or an attempt of unauthorized access to your network.

Let us see how to make a Traffic Pattern for this purpose. You are only interested in the traffic within your network, so you should create a Self-Traffic type. This being said, you should only set the Internal Network IP address range to your company network's whereas your company network's range will be automatically included in the External network IP address range (Self-Traffic). As for using filters, since you are interested in the discarded traffic (null interfaces), you need to use the Exporter filter. Furthermore, as you are interested in discarded traffic on all exporters, you need to include all exporters into the filter while setting the Out interface field to 0 (code for the null value).

1. Select Self-Traffic (Traffic Pattern type)
2. IP Address ranges:
    a. Internal: include your company network's range
    b. External: your company network's range is included automatically (Self-Traffic)
3. Filters:
    a. Click on the Exporter:
    b. Add Exporter IP address and set Interface Out value to 0, click Include

    ⓘ It is necessary to repeat this step for each exporters that are sending netflow data to your NetFlow Analyzer.

Internet HTTP Traffic Pattern

In some cases, you might want to take a detailed look at HTTP traffic. Since this traffic is between an outside network and your internal network, you should use the Normal Traffic Pattern type. You need cover the traffic between your whole internal network and any other network (Internet). This being said, you should set the Internal Network IP address range to your company network's range - the External network IP address range will be populated automatically (Normal Traffic). As for using the filters, since you are dealing with a web service which is recognized by its port(s), you need to use an Service filter and enter its Service number, HTTP (80) in this example.

1. Select Normal (default Traffic Pattern type)
2. IP Address ranges:
    a. Internal: include your company network's range
    b. External: your company network's range is excluded automatically
3. Filters:
    a. Exporter or Next Hop: read more about Manual Deduplication
    b. Service:
        i. Include Source port(s) 80 / Destination port(s) empty (All)
        ii. Include Source port(s): empty (All) / Destination port(s) 80

        ⓘ It is necessary to repeat this step for each port that is used for HTTP (eg. 8080, 443, etc.).

Email Traffic Pattern

Your can use NetFlow Analyzer for dedicated monitoring of your Email traffic. You should use the Custom Traffic Pattern type, since IP address ranges overlap. You need to cover the traffic between your whole internal network with mail servers. This being said, you should set the Internal Network IP address range to your company network's range, with exception of your mail server's IP, and set the External network IP address range as your mail server's IP (in this case your email server is treated as "Outside" network). As for using the filters, since you are interested in service which is recognized by its port(s), you need to use an Service filter and add Service number for the service, Email POP3 port (110) in this example.

1. Select Custom (Traffic Pattern type)
2. Address
    a. Internal: include your company network's range, and exclude you mail server's IP
    b. External: include you mail server's IP
3. Filters:

a. Exporter or Next Hop: read more about Manual Deduplication
b. Service
    i. Include Source port(s): 110 / Destination: empty (All)
    ii. Include Source port(s): empty (All) / Destination: 110

It is necessary to repeat this step for each port used for email traffic (eg. 25, 995, ...).

Other examples of the filtering based on service are SMTP, SSH, MS-SQL Traffic, etc.

Facebook Traffic Pattern

You may want to measure the traffic between your network (or its part) and a specific web service such as Facebook. Since this traffic is between an outside network (Facebook) and your internal network, you should use the Normal Traffic Pattern type. You need to cover traffic between your whole internal network and any other network. This being said, you should set the Internal Network IP address range to your company network's range - the External network IP address range will be populated automatically (Normal Traffic). As for using the filters, since you are interested in a web service which is recognized by its AS, you need to use an AS filter and enter AS number for the service, in this example the ASN is Facebook's ASN (32934).

You can also join all major social network traffics in into one Social Network Traffic Pattern.

1. Select Normal (default Traffic Pattern type)
2. IP Address ranges:
    a. Internal: include your company network's range
    b. External: your company network's range is excluded automatically
3. Filters:
    a. Exporter or Next Hop: read more about Manual Deduplication
    b. AS
    a. i. Include Source port(s): 32934 / Destination: empty (All)
        ii. Include Source: empty (All) / Destination: 32934

Other examples of AS filtering are YouTube, Twitter and Skype Traffic Patterns. You can also monitor these services in a same Traffic Pattern.

> It is necessary that your exporters have BGP table included, and that they are configured to export AS numbers.

Unexpected Protocols Traffic Pattern

Some traffic important to you might be small in the terms of volume and, therefore, not easily spotted on charts and graphs, if so - create a separate Traffic Pattern for that traffic. One example of this is when you are interested in traffic made by protocols other then UDP and TCP. Since these two protocols usually take up to 99% of all traffic, it will be hard to spot any other protocol on graphs. Protocols other then TCP and UDP (we will call them unexpected protocols) might indicate a tunneling protocol or a potential attack.

Let us see how to make a Traffic Pattern for this purpose. You need to cover the traffic between your whole internal network and any other network - attacks are usually expected to come from the External Network to Internal Network (your internal network), but keep in mind that your own network security can be compromised and an attack might be launched from your network to some other network (both Internal and External network). You will do that by choosing Custom for the Traffic Pattern type. This being said, you should set the Internal network IP address range to your company's network range and leave the External network IP address range empty, since you want to cover all other networks. As for using the filters, since you are interested in protocols, you need to use the Protocol filter and enter service port numbers for TCP and UDP which are 6 and 17.

1. Select Custom (Traffic Pattern type)
2. IP Address ranges:
    a. Internal: include your company network's range
    b. External: leave empty
3. Filters:
    a. Exporter or Next Hop: read more about Manual Deduplication
    b. Protocol
        i. Exclude Protocol number(s): 6
        ii. Exclude Protocol number(s): 17

Other examples of Protocol filtering are dedicated ICMP, IPv6 and GRE Traffic Patterns.