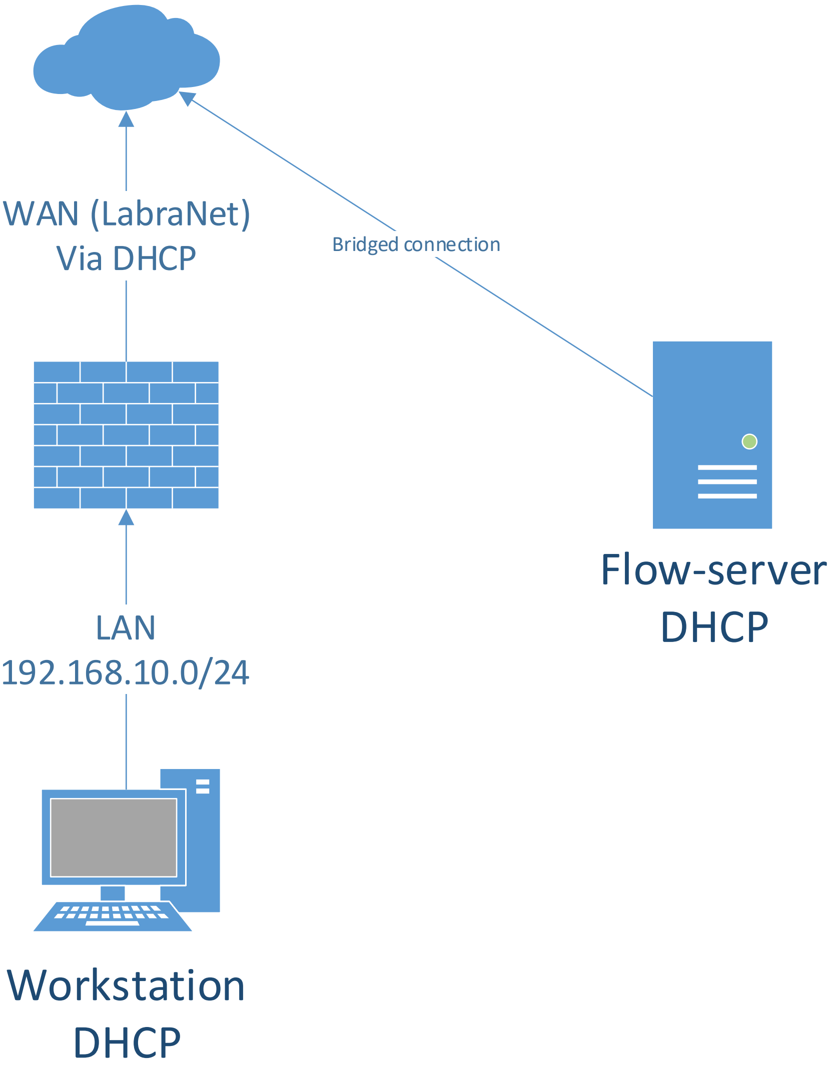
ftLab11 – Traffic Monitoring

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

This lab will use the following topology:

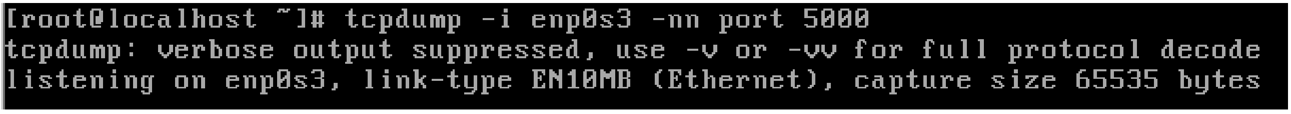


- ## VM config

Fetch the ELK-Flow template from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\ and set the network settings to Bridged. NOTE: In real world situations the Netflow collector would be in a internal/management network segment, but to make the VM easier to use in the lab it is connected to LabraNet directly. Boot the VM and take note of the IP address.

The flow server is readily configured and listens to UDP/5000 for Netflow data. You can monitor the next steps with tcpdump:

```
tcpdump -i enp0s3 -nn port 5000
```

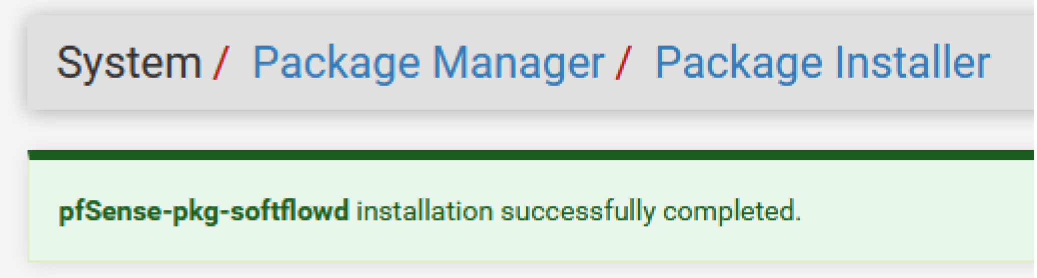


```
[root@localhost ~]# tcpdump -i enp0s3 -nn port 5000
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 65535 bytes
```

You should see incoming flow packets when the softflowd is correctly configured in the next step.

- ## Sending flow-data

Configure the firewall to actually send netflow data to the collector. In Package Manager, find the package softflowd in Available Packages and install it. The configure softflowd under Services with the following settings:

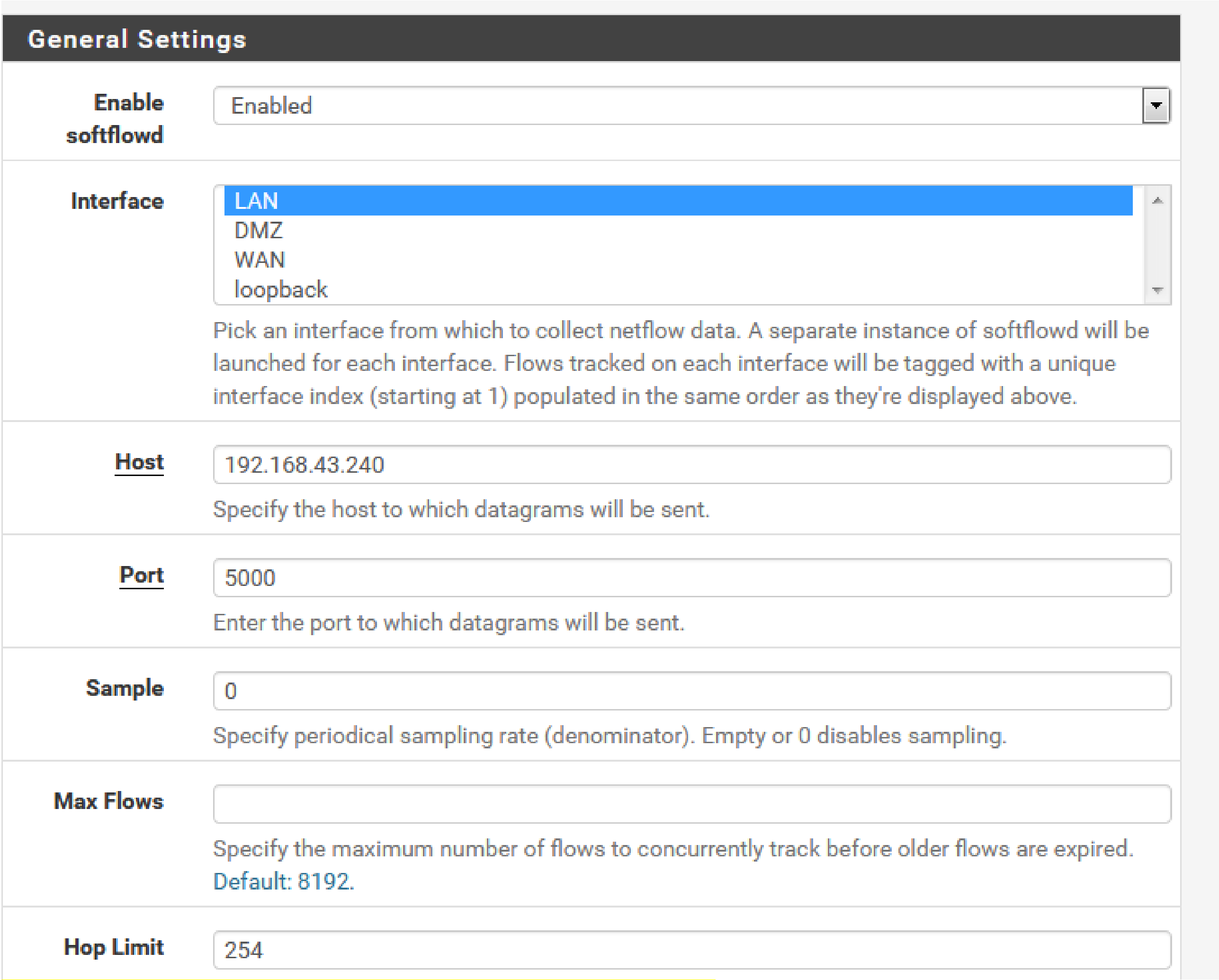


System / Package Manager / Package Installer

pfSense-pkg-softflowd installation successfully completed.

asensin paketin

- Interface: LAN
- Host: IP address of the Flow-server
- Port: 5000
- Hop Limit: 254
- Netflow version: 9
- Flow Tracking Level: Full
- General Timeout Value: 60
- Maximum Lifetime: 0
- Expire Interval: 0



General Settings

Enable softflowd: Enabled

Interface: LAN (selected), DMZ, WAN, loopback

Pick an interface from which to collect netflow data. A separate instance of softflowd will be launched for each interface. Flows tracked on each interface will be tagged with a unique interface index (starting at 1) populated in the same order as they're displayed above.

Host: 192.168.43.240

Specify the host to which datagrams will be sent.

Port: 5000

Enter the port to which datagrams will be sent.

Sample: 0

Specify periodical sampling rate (denominator). Empty or 0 disables sampling.

Max Flows:

Specify the maximum number of flows to concurrently track before older flows are expired. Default: 8192.

Hop Limit: 254

vaihdoin asetuksi , osa ei näy kuvassa mutta nekin on muutettu

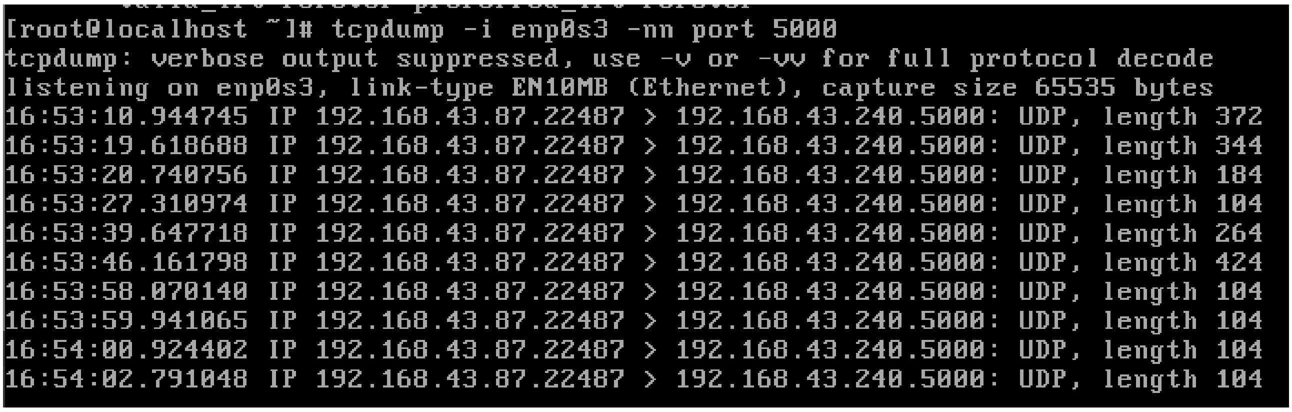
Save the changes.

Browse pages on the Workstation VM. The initial state cache of the softflowd seems to fill up very slowly, so it may take multiple different sites with images and such to get the actual data. Eventually you should start to get a constant stream of traffic in the Flow server tcpdump output.

For troubleshooting, you can try to run the following command on the firewall console (Press 8 for Shell in the menu):

```
softflowctl -c /var/run/softflowd.vtnet1.ctl statistics
```

After a while, the output should contain flow statistics and sent packet amounts etc.

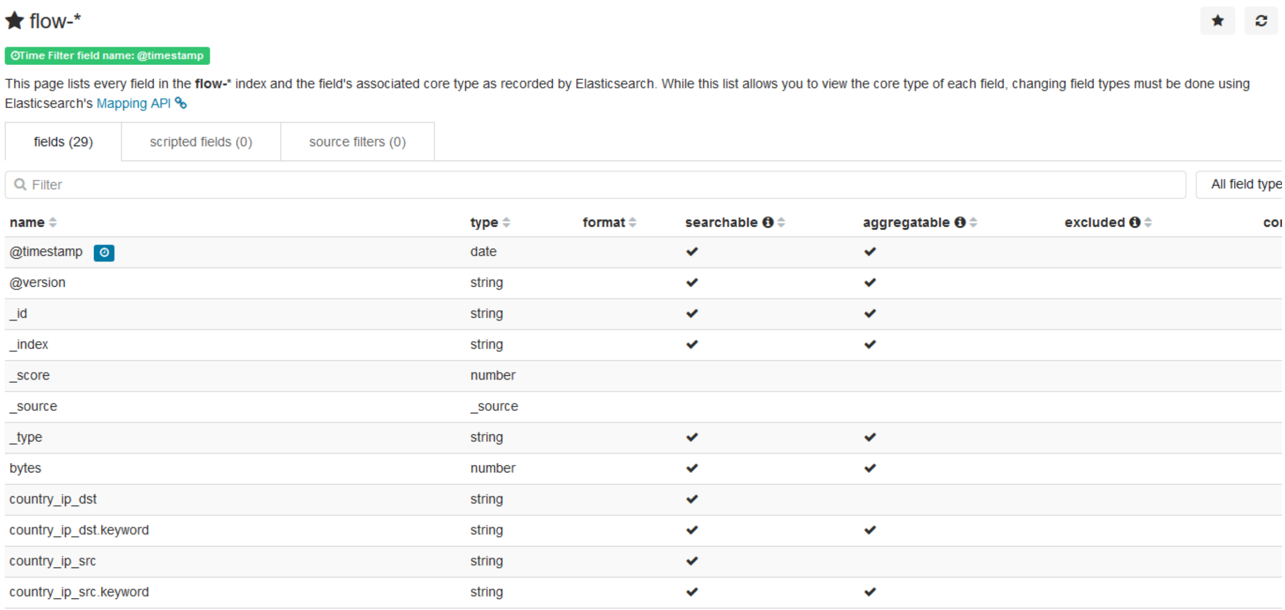


```
    valid_lft forever preferred_lft forever
[root@localhost ~]# tcpdump -i enp0s3 -nn port 5000
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 65535 bytes
16:53:10.944745 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 372
16:53:19.618688 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 344
16:53:20.740756 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 184
16:53:27.310974 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 104
16:53:39.647718 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 264
16:53:46.161798 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 424
16:53:58.070140 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 104
16:53:59.941065 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 104
16:54:00.924402 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 104
16:54:02.791048 IP 192.168.43.87.22487 > 192.168.43.240.5000: UDP, length 104
```

toimii

- ## Flow indexing

Log in to the Flow-server using browser (Firefox is highly preferred). Set the Index pattern as flow-*, you should get a timestamp value and be able to click ok. You should also get a list of fields like in the image:



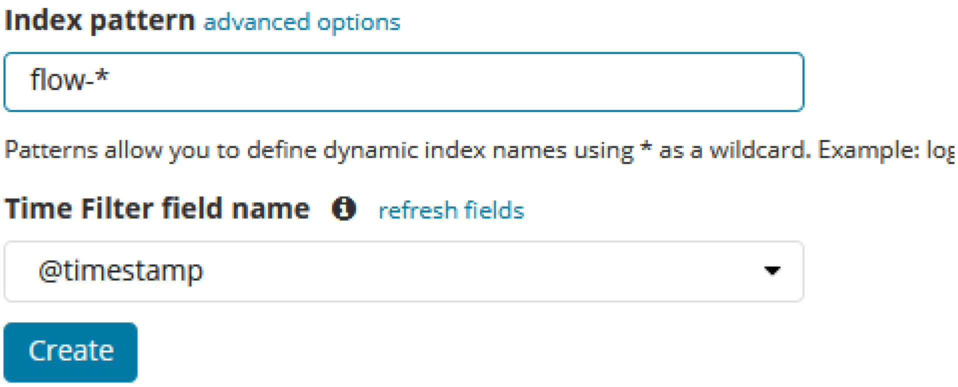
★ flow-*

@Time Filter field name: @timestamp

This page lists every field in the **flow-*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

name	type	format	searchable	aggregatable	excluded	co
@timestamp	date		✓	✓		
@version	string		✓	✓		
_id	string		✓	✓		
_index	string		✓	✓		
_score	number					
_source	_source					
_type	string		✓	✓		
bytes	number		✓	✓		
country_ip_dst	string		✓			
country_ip_dst.keyword	string		✓	✓		
country_ip_src	string		✓			
country_ip_src.keyword	string		✓	✓		

Verify that you can find the 5-tuple fields in the field list. Do NOT load the dashboards until you have the index pattern and fields correctly in the list.



Index pattern advanced options

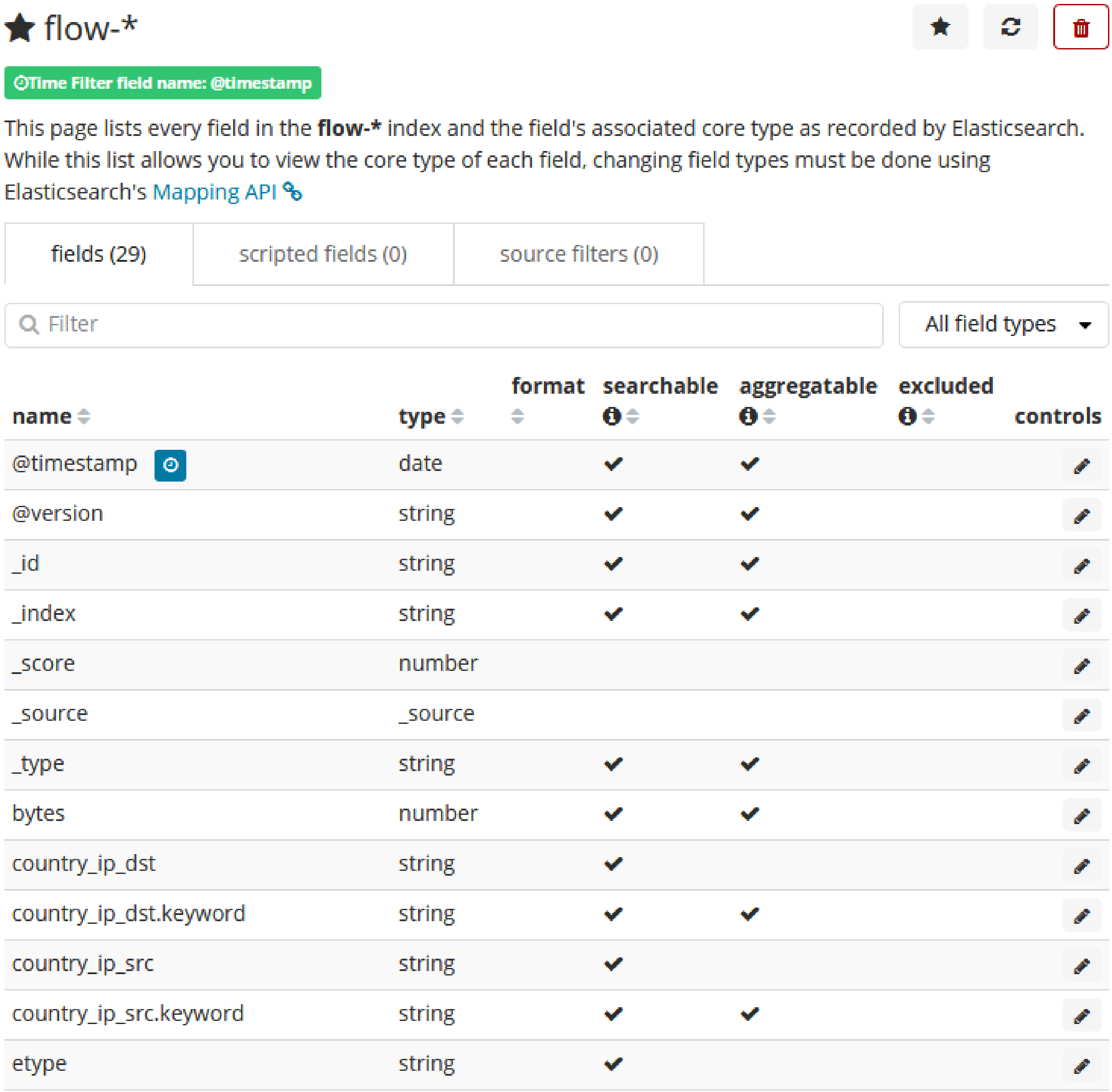
flow-*

Patterns allow you to define dynamic index names using * as a wildcard. Example: log

Time Filter field name refresh fields

@timestamp

timestamp löyty



★ flow-*

Time Filter field name: @timestamp

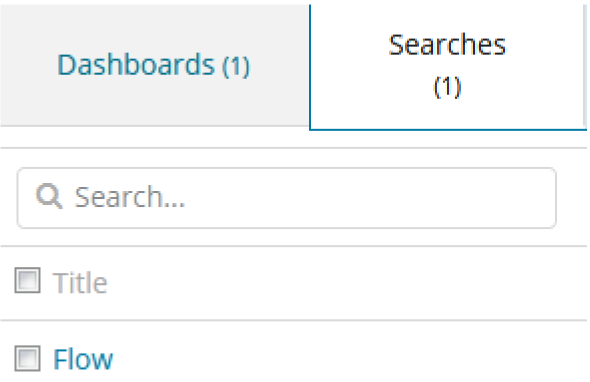
This page lists every field in the **flow-*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

name	type	format	searchable	aggregatable	excluded	controls
@timestamp	date		✓	✓		✎
@version	string		✓	✓		✎
_id	string		✓	✓		✎
_index	string		✓	✓		✎
_score	number					✎
_source	_source					✎
_type	string		✓	✓		✎
bytes	number		✓	✓		✎
country_ip_dst	string		✓			✎
country_ip_dst.keyword	string		✓	✓		✎
country_ip_src	string		✓			✎
country_ip_src.keyword	string		✓	✓		✎
etype	string		✓			✎

Oikeat listat löytyy

Fetch the pre-made dashboards files (*.json in \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\flow-json\ ) and import them in the Flow-server in Management -> Saved Objects. Import the json files in order:

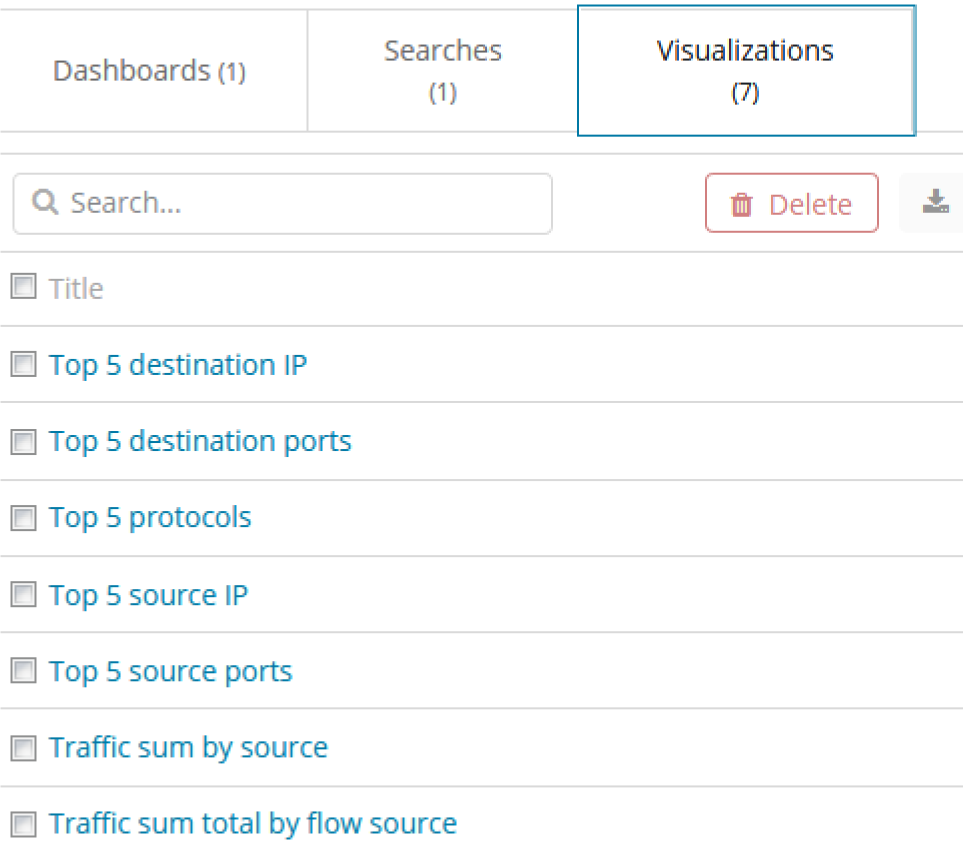
- flow-search.json



□ Title

□ Flow

- flow-viz.json



□ Title

□ Top 5 destination IP

□ Top 5 destination ports

□ Top 5 protocols

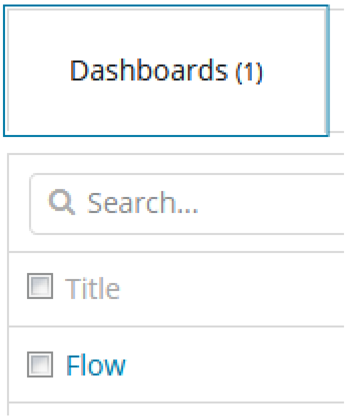
□ Top 5 source IP

□ Top 5 source ports

□ Traffic sum by source

□ Traffic sum total by flow source

- flow-dashboard.json


Dashboards (1)

Search...

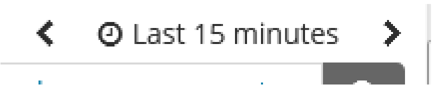
□ Title

□ Flow

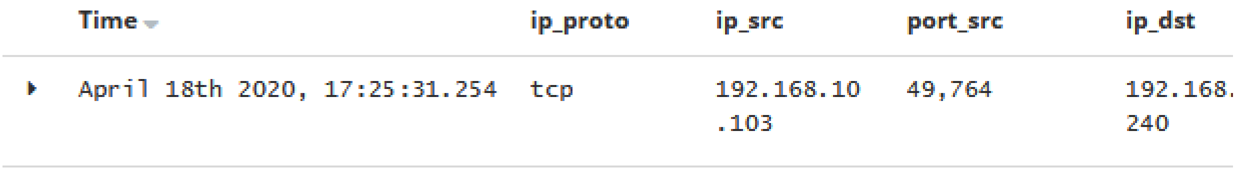
- **Flow analysis**

Generate traffic from/to your VM. Use for example YouTube videos as they quickly generate a lot of traffic.

Find out the NetFlow 5-tuple values for the traffic going from your VM to the YouTube or other site using the Discover-tab. The upper right corner has option to select data start and end times, use the quick meny to select *Last 15 minutes*. To make sure you get an up-to-date view of the traffic.


Last 15 minutes

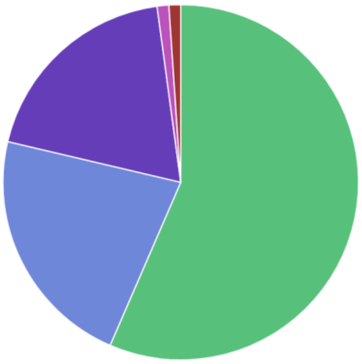
valitsin oikean ajanjakson



Time	ip_proto	ip_src	port_src	ip_dst
April 18th 2020, 17:25:31.254	tcp	192.168.10.103	49,764	192.168.240

liikennettä

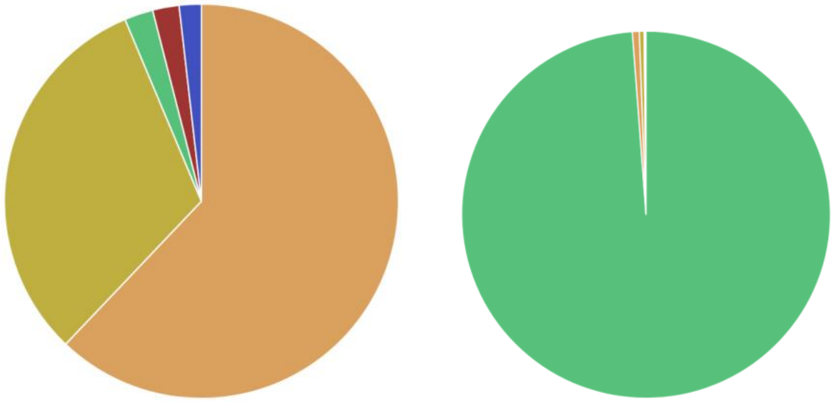
Visualize-tab can be used to quickly find top talkers and protocols/port numbers. Find out where your DNS queries go (top destination IP). You can add a filter with port_dst = 53 to show only DNS traffic.



dns liikenne

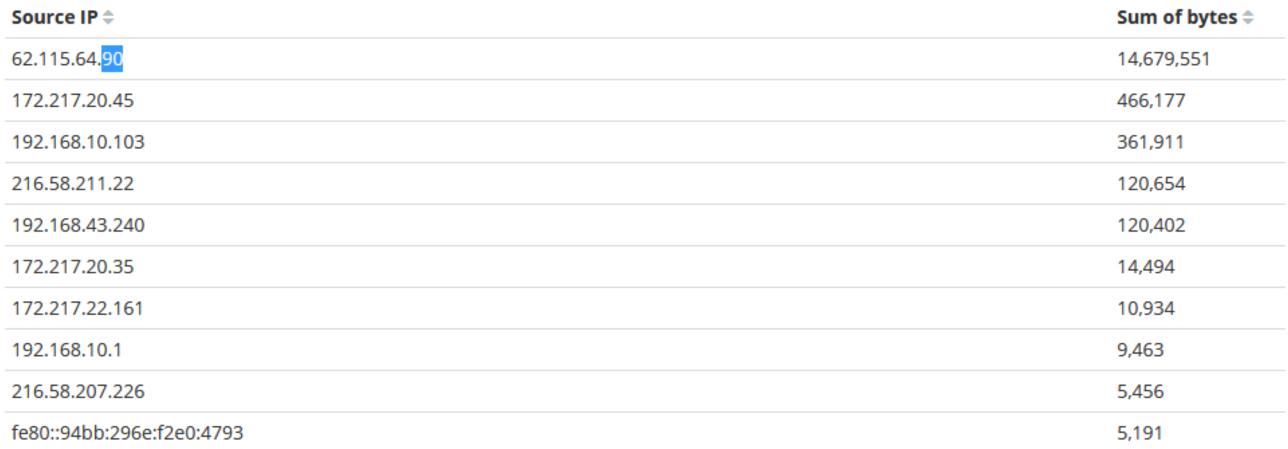
piirakka ilman filtteriä ja filtterin kanssa

By default the pie charts consist of packet count, which is useless for summarized flow-data. Go to Visualize -> Top 5 source IP and change the metric from *Count* to *Sum* of *bytes.* Save the chart from the top panel. Now the Pie chart shows the IPs that have sent the most traffic in bytes. Do the same for the *Top 5 source ports* -visualisation.



vasemmalla source ip bitteinä ja oikella source portit bitteinä

Finally find where the Youtube video traffic mostly comes from (Hint: Traffic sum by source). Take a screenshot of this.



Source IP ⇕	Sum of bytes ⇕
62.115.64.90	14,679,551
172.217.20.45	466,177
192.168.10.103	361,911
216.58.211.22	120,654
192.168.43.240	120,402
172.217.20.35	14,494
172.217.22.161	10,934
192.168.10.1	9,463
216.58.207.226	5,456
fe80::94bb:296e:f2e0:4793	5,191

suurin liikenne tulee kohde ipstä 62.115.64.90

- ## Extra work for the fastest

Find out how much of the traffic is HTTP vs HTTPS? Using this data, create a visualisation (pie) from the traffic using sum of bytes sorted by source port (80/443).