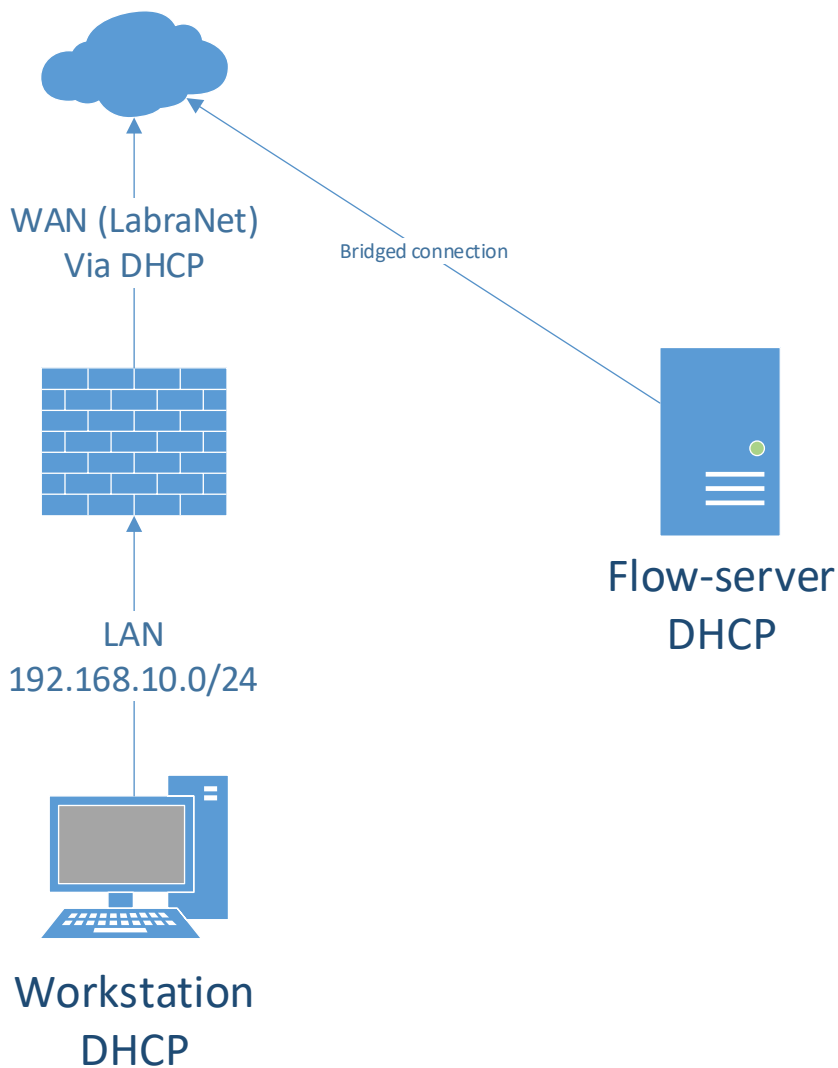


Lab11 – Traffic Monitoring

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\](https://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.

- 192.168.1.188

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
```

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:

- 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	<div>LAN DMZ WAN loopback</div> <div>Pick an interface from which to collect netflow data. A separate instance of softflowd will be launched for each interface. Flows to interface will be tagged with a unique interface index (starting at 1) populated in the same order as they're displayed above.</div>
Host	<div>192.168.1.188</div> <div>Specify the host to which datagrams will be sent.</div>
Port	<div>5000</div> <div>Enter the port to which datagrams will be sent.</div>
Sample	<div>0</div> <div>Specify periodical sampling rate (denominator). Empty or 0 disables sampling.</div>

- softflowd asetukset

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
```

Shell Output - softflowctl -c /var/run/softflowd.vtnet1.ctl statistics

```
softflowd[1266]: Accumulated statistics since 2020-04-01T11:57:59 UTC:
Number of active flows: 178
Packets processed: 23493
Fragments: 0
Ignored packets: 2 (2 non-IP, 0 too short)
```

- pfsensen command promptissa ajettu komento

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

• 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](#).

fields (29) | scripted fields (0) | source filters (0)

Q Filter All field type

name	type	format	searchable	aggregatable	excluded	core type
@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.

Fetch the pre-made dashboards files (*.json in [\\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\flow-json\](https://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

- flow-viz.json
- flow-dashboard.json

Dashboards (1)	Searches (1)	Visualizations (7)
<input type="text" value="Search..."/>		
<input type="checkbox"/> Title		
<input type="checkbox"/> 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.

```

March 31st 2020, 20:47:06 Q Q iface_in: 1 ip_proto: tcp iface_out: 1 peer_ip_src: 192.168.1.69 ip_src: 192.168.10.102 port_dst: 443 port_src: 46,798 ip_dst: 216.58.207.214
packets: 543 @timestamp: March 31st 2020, 20:47:06.747 bytes: 40,567 country_ip_src: etype: 800 country_ip_dst: US _id: LM20MXESVxV0dVU_OFOL _type:
flow _index: flow-2020.03.31 _score: -

```

5 tuple data

192.168.10.102 – 216.58.207.214

46,798 – 443

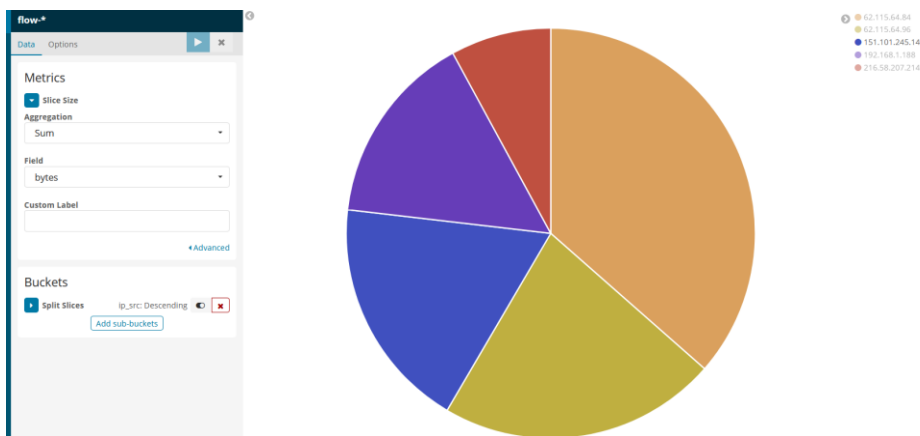
TCP

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.

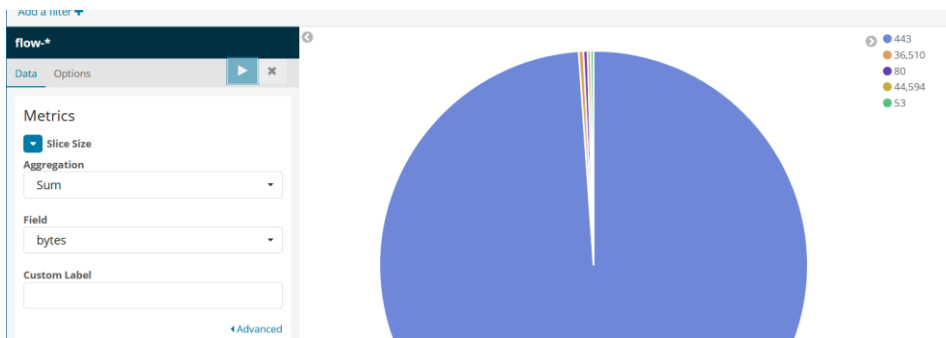
field	value	Count
Destination IP	192.168.10.1	363 (100%)

- saan dns kohde ip:ksi ainoastaan 192.168.10.1 eli pfsensen ip

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.



- top 5 source ip osoitteet



- Top 5 source portit

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
172.217.21.182	6,040,300
62.115.64.92	3,261,201

- **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).