Traffic Logging

- Traffic Logging Config
- rsyslog server settings for receiving logs

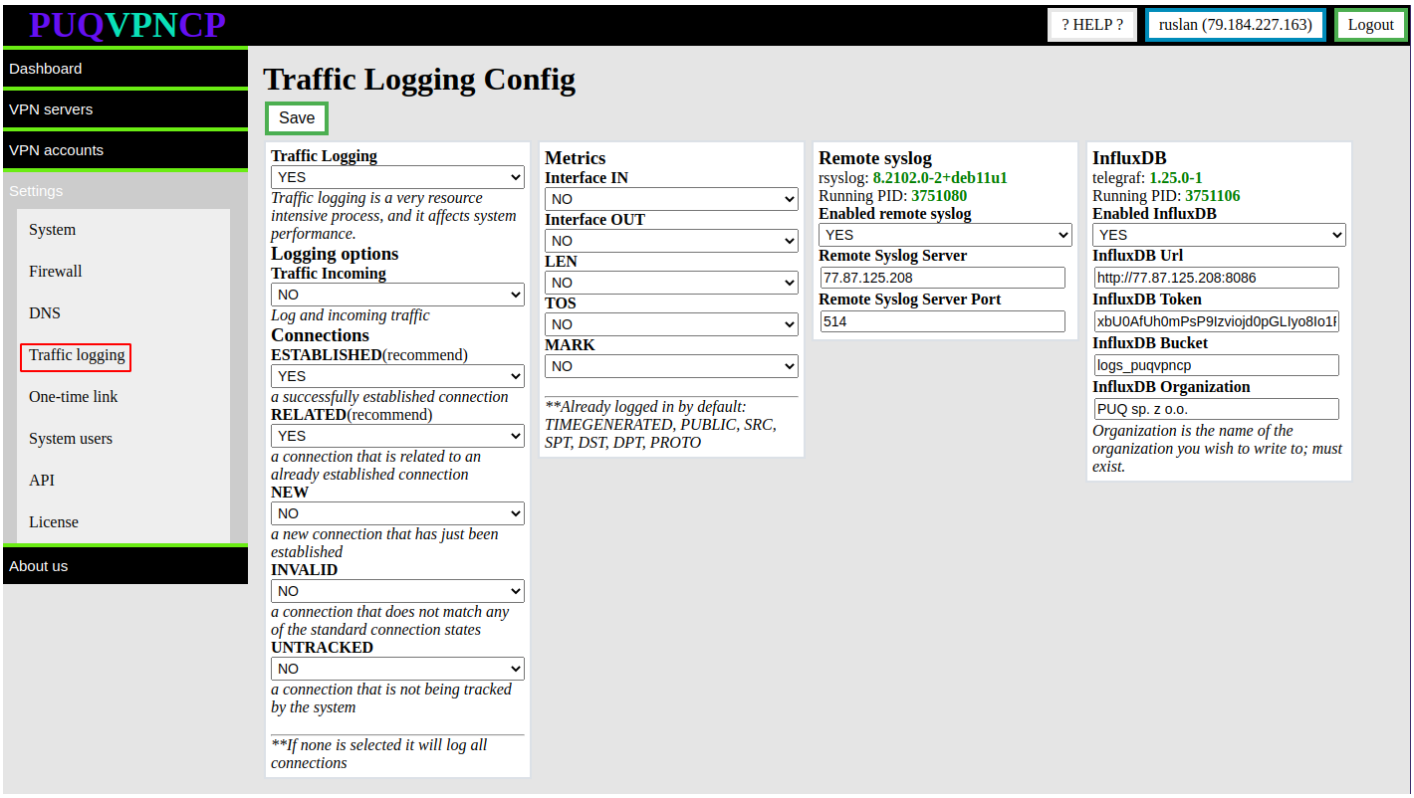
Traffic Logging Config

To enable and configure traffic logging go to **Settings->Traffic logging**

Logging all traffic passing through a server can be very resource intensive and can have a significant impact on the performance of the server. This is because logging requires the server to process and store a large amount of data, which can consume a significant amount of CPU, memory, and disk resources. In addition, logging all traffic can generate a large number of log messages, which can further strain the server's resources.

As a result, it is important to carefully consider the need for logging all traffic and to balance this need with the potential impact on the performance of the server. In some cases, it may be more appropriate to only log a subset of traffic or to use sampling or filtering techniques to reduce the volume of logs generated. It is also important to consider the hardware resources of the server and to ensure that the server has sufficient capacity to handle the load of logging all traffic.

In summary, while logging all traffic can be useful for certain purposes, it is important to be aware of the potential impact on the server's performance and to carefully evaluate the need for this level of logging.



Remote syslogTraffic logging section

you can enable logging of client traffic passing through the server

Logging options

You can choose the following logging options:

1. Traffic Incoming - Log also incoming traffic. By default, only outgoing traffic is logged.
2. Connections - What connection types to log (ESTABLISHED and RELATED are recommended)
   - **ESTABLISHED -** a successfully established connection
   - **RELATED -** a connection that is related to an already established connection
   - **NEW -** a new connection that has just been established
   - **INVALID -** a connection that does not match any of the standard connection states
   - **UNTRACKED -** a connection that is not being tracked by the system

> **If none is selected it will log all connections**

Metrics

What data will be collected and transmitted to a remote server

Already logged in by default: TIMEGENERATED, PUBLIC, SRC, SPT, DST, DPT, PROTO

Remote syslog

Remote syslog server configuration options

InfluxDB

Remote InfluxDB server configuration options

To use logging to the InfluxDB server, you need to install telegraf

https://docs.influxdata.com/telegraf/v1.21/introduction/installation/

rsyslog server settings for receiving logs

Here are the steps you can follow to configure rsyslog to receive logs from remote servers:

1. Install rsyslog on the machine that you want to use as the central log server. On a Debian-based system, you can install rsyslog with the following command:

```
sudo apt-get install rsyslog
```

2. Open the rsyslog configuration file in a text editor. On a Debian-based system, this file is typically located at /etc/rsyslog.conf.

```
sudo nano /etc/rsyslog.conf
```

3. In the configuration file, uncomment the line that reads "module(load="imudp")" and "input(type="imudp" port="514")". This will configure rsyslog to listen for incoming log messages on UDP port 514. If you want to use a different port, you can specify it here.
4. Save and close the configuration file.
5. Restart the rsyslog service to apply the new configuration. On a Debian-based system, you can do this with the following command:

```
sudo service rsyslog restart
```

To view the logo, use the command

```
sudo less /var/log/syslog
```

You should get something like this

```
Dec 28 15:42:50 dev.softkeel.com [2265632.987952] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265632.988013] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.020799] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
```

```
Dec 28 15:42:50 dev.softkeel.com [2265633.071709] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.081883] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.081972] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.239150] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.245651] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.245738] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.336217] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.339190] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.345274] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.345456] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.430714] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:43:19 dev.softkeel.com [2265661.777196] TIMEGENERATED=2022-12-28 15:43:19
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=48566 DST=172.217.16.37 DPT=443 PROTO=TCP
Dec 28 15:43:19 dev.softkeel.com [2265661.784642] TIMEGENERATED=2022-12-28 15:43:19
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=48566 DST=172.217.16.37 DPT=443 PROTO=TCP
Dec 28 15:43:20 dev.softkeel.com [2265662.835952] TIMEGENERATED=2022-12-28 15:43:20
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=45142 DST=216.58.215.74 DPT=443 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.853984] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.893813] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.921793] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
```