# KWAADAARDIG INTERNETVERKEER ONDERSCHEPPEN

**Een firewall ontwikkeld in Python**

Een project om het inzicht in de werking van een firewall en de ineractie met malware te verbeteren.

## Inleiding

Het doel van het project is om een educatieve bijdrage te leveren aan de opleiding Bachelor Elektronica-ICT. Het brengt inzicht in de werking van een firewall. Het project met zijn onderzoek naar malware en het ontwikkelen van de firewall, bieden een meerwaarde in de algemene beroepskennis.
Als programmeertaal voor de applicatie werd voor python gekozen. Er werd ook gekozen voor een webapplicatie. De gebruikers kunnen dus communiceren met de firewall door middel van een webpagina.

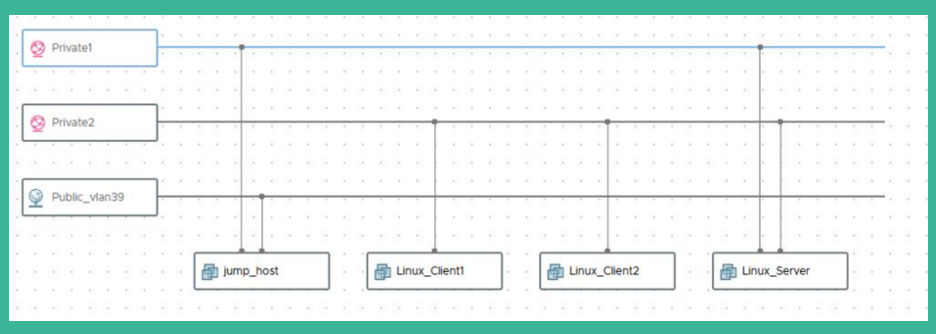
## Werking

De firewall werkt laag per laag. Als een pakket binnen komt zal door gebruik te maken van enkele lussen gecontroleerd worden of het pakket toegelaten mag worden. Het komt terecht in een lus die alle modules zo nagaan. Hier zal het pakket in een lus van regels terechtkomen. Die zullen de relevante data testen tegenover alle regels binnen een module.Enkel als alle regels van alle modules uit alle lagen doorlopen zijn wordt het pakket geaccepteerd. Het block diagram is hier een schematische voorstelling van.

## Infrastructuur

Voor dit project wordt er gekozen voor een gesloten omgeving, zodat er geen gevaar ontstaat voor zelfbesmetting bij het testen met bestaande malware. De virtuele machines met als prefix “Linux” behoren tot de testomgeving. De “jumphost” is nodig om via SSH (secure shell) verbinding te maken met de firewall server. Het verkeer van de twee computers in het netwerk wordt gerouteerd door de firewall server zelf.

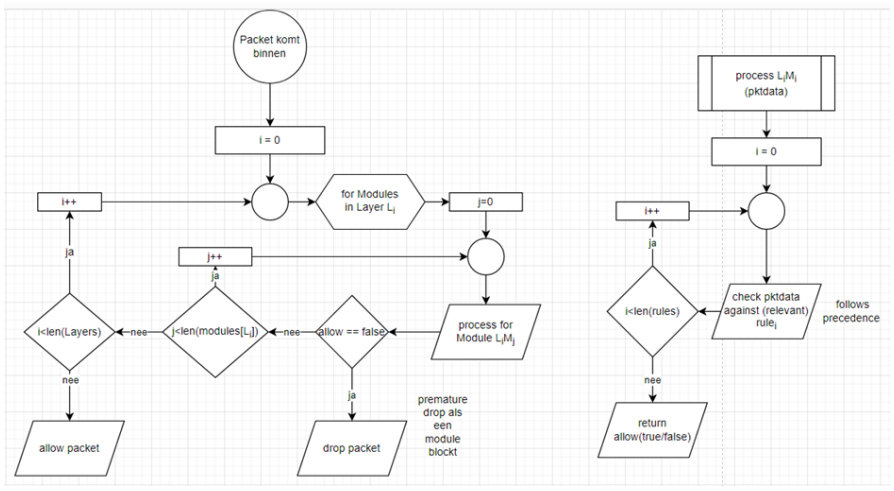
## Netwerk



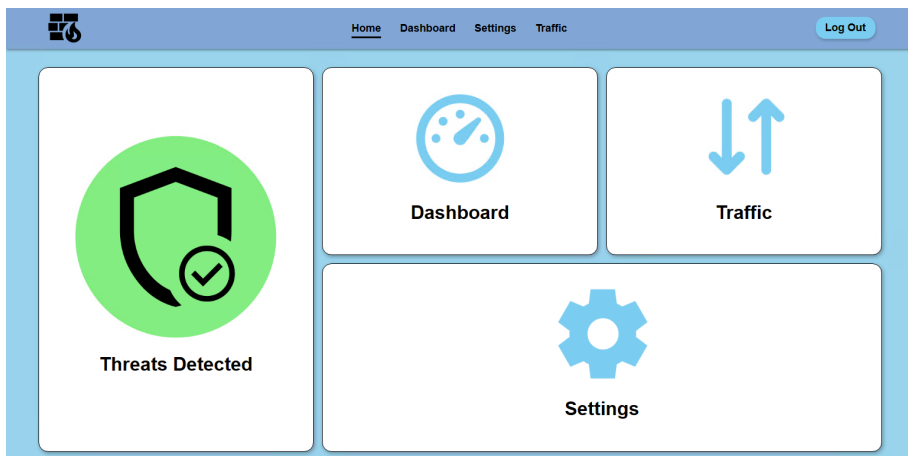

## Userinterface

De userinterface wordt zodanig ontwikkeld dat deze toegankelijk is voor iedereen. Op de homepagina wordt gekozen voor grote duidelijke knoppen met de meest frequente en belangrijkste gebruikte functionaliteiten. De status van de firewall wordt hier ook getoond. Het geeft aan of er dreigingen gevonden werd en er pakketten werden geblokkeerd.

## Block diagram




## Homepagina




## Output

```
[student@localhost Code]$ sudo python main.py -s -f
[sudo] password for student:
Frontend/flaskkey.pem
could not load module example_module
module 'Backend.modules.Layer3.example_module' has no attribute 'config'
starting backend
starting queue 1
starting queue 2
starting queue 3
starting frontend
 * Serving Flask app 'Frontend.frontend'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on https://127.0.0.1:8080
 * Running on https://192.168.0.10:8080
Press CTRL+C to quit
10.129.32.6 - - [04/Jun/2023 10:04:08] "GET / HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:08] "GET /static/CSS/login.css HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:08] "GET /static/CSS/common.css HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:08] "GET /static/JS/login.js HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:13] "POST / HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /?token=8ab3cb7fa2c7ff2fbbee433574caec28a2cfb4e3cb3edbdb17cda9f2e34b53f2 HTTP/1.1" 3
02 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /home?token=8ab3cb7fa2c7ff2fbbee433574caec28a2cfb4e3cb3edbdb17cda9f2e34b53f2 HTTP/1.
1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/CSS/common.css HTTP/1.1" 304 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/CSS/firewall.css HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/JS/script.js HTTP/1.1" 404 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/ASSETS/Protected.png HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/ASSETS/Dashboard.png HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/ASSETS/Traffic.png HTTP/1.1" 200 -
10.129.32.6 - - [04/Jun/2023 10:04:14] "GET /static/ASSETS/Settings.png HTTP/1.1" 200 -
```

Odisee
DE CO-HOGESCHOOL