# Stage ESTIG, IPBEJA

## Realisatieverslag

**Stage**

Pauline Valgaeren 3CCS02

Academiejaar 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

# INHOUDSTAFEL

# LIJST MET AFBEELDINGEN

# 1 INTRODUCTIE

Met trots presenteer ik hierbij mijn realisatiedocument, samengesteld tijdens mijn stageperiode bij ESTIG, IPBEJA in Portugal. Als student Cloud en Cyber Security aan Thomas More Hogeschool Geel kreeg ik de unieke kans om mijn kennis en vaardigheden op het gebied van netwerktechnologieën uit te breiden en te verdiepen.

Gedurende mijn stage heb ik me voornamelijk gericht op de netwerktak van onze opleiding. Mijn reis begon met een diepgaande verkenning van MikroTik routers, switches en access points. Door het opzetten van mijn eigen testnetwerk in MikroTik kon ik hands-on ervaring opdoen en alle aspecten van deze systemen verkennen, van Winbox tot de command-line interface.

Met de begeleiding van ervaren professionals, zoals Joao Santos en José Jasnau Caeiro, heb ik niet alleen de basisbeginselen van MikroTik onder de knie gekregen, maar heb ik ook uitgebreide documentatie gemaakt om anderen te helpen bij het begrijpen en configureren van deze systemen.

Na deze periode van intensieve studie heb ik mijn horizon verbreed door me te verdiepen in WireGuard, een opkomende technologie voor veilige communicatie. Ik heb WireGuard zowel op computers als op mobiele apparaten onderzocht en gedocumenteerd, waardoor ik een dieper inzicht kreeg in de implementatie en configuratie ervan.

Verder kreeg ik de kans om mijn kennis uit te breiden naar virtualisatieomgevingen, met de mogelijkheid om virtuele machines aan te maken en te beheren in Proxmox. Hier heb ik systemen zoals IPfire en OpnSense verkend en gedocumenteerd, wat resulteerde in heldere handleidingen voor beginners.

Mijn stagebegeleider daagde me uit om ook nieuwe systemen te verkennen, zoals Netbox en EVE-NG, en zelfs de overstap te maken naar GNS3 toen zich technische uitdagingen voordeden. Elk nieuw systeem bracht zijn eigen leercurve met zich mee, maar dankzij mijn vastberadenheid en begeleiding slaagde ik erin om ze te begrijpen en te documenteren voor toekomstige referentie.

Dit realisatiedocument biedt een gedetailleerd verslag van mijn ervaringen, ontdekkingen en prestaties tijdens mijn stageperiode. Ik ben ervan overtuigd dat de kennis en vaardigheden die ik heb opgedaan, een waardevolle aanvulling zullen zijn op mijn academische en professionele reis in de wereld van Cloud en Cyber Security.

# 2 STAGEPLAATS

Tijdens mijn stage ben ik geplaatst bij IPBEJA in het ESTIG-gebouw, waar ik werkzaam was in het Sepsi Lab. IPBEJA, oftewel Instituto Politécnico de Beja, is een vooraanstaand instituut voor hoger onderwijs en onderzoek gevestigd in Beja, Portugal. Het ESTIG-gebouw is een dynamische omgeving waar innovatie en kennis samenkomen.

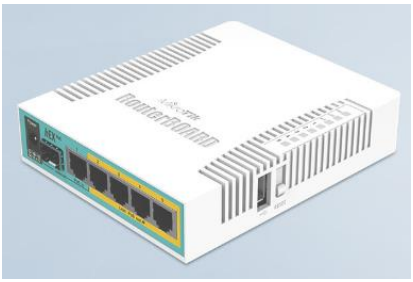
Mijn stagebegeleider, José Jasnau Caeiro, is een ervaren professional binnen het vakgebied en fungeert als mijn directe aanspreekpunt en mentor gedurende mijn stageperiode. Zijn expertise en begeleiding zijn van onschatbare waarde geweest bij het navigeren door complexe vraagstukken en het ontwikkelen van mijn vaardigheden. Daarnaast werk ik regelmatig samen met Joao Santos, een collega binnen het Sepsi Lab, waardoor ik de kans krijg om te leren van verschillende perspectieven en samen te werken aan diverse projecten.

De keuze voor een Erasmus-stageplaats bij IPBEJA was voor mij een bewuste beslissing, gedreven door mijn verlangen om mijn zelfstandigheid te vergroten en mijn taalvaardigheid te verbeteren. Door te kiezen voor een internationale stageomgeving heb ik de mogelijkheid om te werken en te communiceren in een andere taal en cultuur, wat mijn persoonlijke en professionele ontwikkeling ten goede komt. Het is een kans om mijn horizon te verbreden, nieuwe mensen te ontmoeten en mijn vaardigheden op zowel technisch als interpersoonlijk vlak te versterken.

# 3 MIKROTIK

In de eerste drie weken heb ik me voornamelijk gericht op het verkennen van de MikroTik-systemen, zoals beschreven in het plan van aanpak. Aangezien dit een geheel nieuw systeem voor mij was, kostte het enige tijd om alle functionaliteiten te ontdekken.

## 3.1 hEX PoE



*Figuur 1*

Als eerste heb ik de functionaliteiten en configuratiemogelijkheden van de hEX PoE grondig onderzocht. Mijn focus lag op het verkennen van de diverse toepassingen van dit apparaat, het identificeren van optimale gebruiksrichtlijnen en het vaststellen van effectieve configuratieprocedures.

### 3.1.1 Wat is de hEX PoE?

De hEX PoE (RB960PGS) is een Gigabit Ethernet-router met vijf poorten, ontworpen voor locaties waar draadloze connectiviteit niet vereist is. Het apparaat heeft een USB 2.0-poort en een SFP-poort voor optische connectiviteit. Poorten 2 tot en met 5 kunnen andere PoE-compatibele apparaten van stroom voorzien met dezelfde spanning als het apparaat zelf.

Dit model is betaalbaar, compact en gemakkelijk te gebruiken. Ondanks zijn compacte formaat wordt hij geleverd met een krachtige 800 MHz CPU die alle geavanceerde configuraties van RouterOS ondersteunt. Dit betekent dat u zich minder zorgen hoeft te maken over adapters en kabels. De maximale stroom van elke poort is 1A en de netwerkpoort is afgeschermd.

Bovendien ondersteunt het apparaat passieve PoE-invoer en passieve of 802.3af/at PoE-uitvoer. Ethernet-poorten 2 tot en met 5 kunnen andere PoE-compatibele apparaten van stroom voorzien met dezelfde spanning als de router. Dit vermindert het aantal benodigde adapters en kabels. Bij gebruik van een ingangsspanning van 48-57V kan het apparaat apparaten voeden die compatibel zijn met AT/AF-modus B (4,5+) (7,8-).

### 3.1.2 Werkwijze en implementatie

#### 3.1.2.1 Onderzoeksmethoden

Mijn aanpak omvatte een grondige verkenning van verschillende informatiebronnen, waaronder YouTube-video's en de officiële documentatie van MikroTik. Ik ben ook dankbaar voor de begeleiding van Joao Santos, die niet alleen de basisconfiguraties heeft gedemonstreerd, maar ook waardevolle studiematerialen heeft verstrekt. Zijn bijdrage omvatte het delen van een uitgebreide studiemap op Zotero, waar ik toegang had tot relevante video's en documenten over MikroTik. Deze gecoördineerde aanpak heeft mijn begrip van het MikroTik-besturingssysteem aanzienlijk vergemakkelijkt en versneld.

#### 3.1.2.2 Verkenning van configuratiemogelijkheden

Ik heb bewust zowel de command line-interface (CLI) als de grafische interface (Winbox) van MikroTik verkend om een grondig begrip van beide benaderingen te ontwikkelen. Hoewel Winbox intuïtief is en een visuele weergave biedt van

het netwerk, heb ik de voorkeur gegeven aan de CLI vanwege de efficiëntie en schaalbaarheid bij grootschalige configuraties.

#### 3.1.2.3 User story’s

1. Als gebruiker wil ik de mogelijkheid hebben om de router volledig te resetten voorafgaand aan de eerste configuratie, om een schone basis te garanderen.

2. Als gebruiker wil ik de standaardbeheerdersaccount kunnen verwijderen om beveiligingsrisico's te minimaliseren.

3. Als gebruiker wil ik in staat zijn om onnodige services zoals telnet uit te schakelen, om potentiële beveiligingsrisico's te verminderen.

4. Als gebruiker wil ik de mogelijkheid hebben om standaardpoorten zoals SSH te wijzigen om externe toegang te beperken en de blootstelling aan potentiële bedreigingen te verminderen.

5. Als gebruiker wil ik DHCP kunnen opzetten om IP-adressen dynamisch toe te wijzen aan aangesloten apparaten, om het netwerkbeheer te vereenvoudigen.

6. Als gebruiker wil ik een bridge-netwerk kunnen configureren om alle netwerkinterfaces te verbinden en adresconflicten te minimaliseren.

7. Als gebruiker wil ik de mogelijkheid hebben om via een domeinnaam te zoeken naar de gewenste website, zodat ik snel en gemakkelijk toegang kan krijgen tot de benodigde informatie.

8. Als gebruiker wil ik dat mijn privé IP-adres niet automatisch wordt gedeeld met externe verbindingen buiten mijn netwerk, om mijn privacy en veiligheid te waarborgen.

#### 3.1.2.4 Implementatie van basisconfiguraties

1. Routerinitialisatie en gebruikersbeheer: Voorafgaand aan de eerste configuratie heb ik de router volledig gereset om een schone basis te garanderen. Vervolgens heb ik mijn eigen gebruikersaccount aangemaakt en beheerdersrechten toegewezen, waarbij ik de standaardbeheerdersaccount heb verwijderd om beveiligingsrisico's te minimaliseren.

2. Beveiligingsmaatregelen: Een cruciale stap was het implementeren van beveiligingsprotocollen, waaronder het uitschakelen van onnodige services zoals telnet en het wijzigen van standaardpoorten zoals SSH om externe toegang te beperken. Door deze maatregelen te treffen, wordt de blootstelling aan potentiële bedreigingen verminderd en wordt de algehele netwerkintegriteit versterkt.

3. Netwerkconfiguratie: Het opzetten van DHCP en het configureren van een bridge-netwerk waren essentiële stappen om alle netwerkinterfaces te verbinden en IP-adressen dynamisch toe te wijzen aan aangesloten

apparaten. Door een gestructureerde IP-adresrange te definiëren, kon ik het netwerkbeheer vereenvoudigen en het adresconflict minimaliseren.

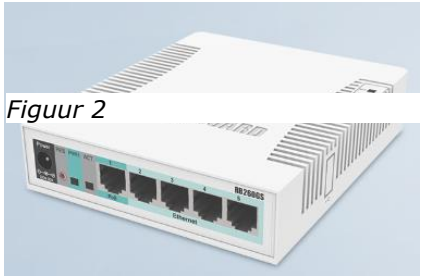
4. Domeinnaamservice (DNS): Het instellen van een interne DNS-server stelde het netwerk in staat om domeinnamen naar IP-adressen te vertalen, waardoor communicatie tussen apparaten mogelijk was en gebruikersvriendelijke toegang tot netwerkbronnen werd geboden.

5. Netwerkadresvertaling (NAT) en firewallfilterregels: Door NAT te implementeren met masquerading, kon ik meerdere privé-IP-adressen omzetten naar een enkel openbaar IP-adres, waardoor de interne netwerkstructuur verborgen bleef voor externe bronnen. De firewallregels werden zorgvuldig geconfigureerd om alleen geautoriseerd verkeer toe te staan en ongeautoriseerde toegang te blokkeren, waardoor de veiligheid van het netwerk werd gewaarborgd.

#### 3.1.2.5 Back-upprocedures

Om de operationele continuïteit te waarborgen, heb ik na elke werksessie back-ups van de configuratie gemaakt. Deze proactieve benadering stelde me in staat om snel te herstellen in het geval van onvoorziene gebeurtenissen of configuratiefouten, waardoor downtime werd geminimaliseerd en de algehele betrouwbaarheid van het netwerk werd verzekerd.

## 3.2 RB260GSP



*Figuur 2*

In het volgende deel van mijn stageonderzoek heb ik me gericht op de RB260GSP. Mijn doel was om een diepgaand begrip te ontwikkelen van de mogelijkheden van dit apparaat en hoe ik het kon integreren met mijn reeds geconfigureerde hEX PoE-router.

### 3.2.1 Wat is de RB260GSP?

De RB260GS is een compacte SOHO-switch met vijf Gigabit Ethernet-poorten en een SFP-aansluiting. Het wordt aangedreven door Atheros-switchchips en draait op een aangepast besturingssysteem genaamd SwOS, dat speciaal is ontworpen voor MikroTik-switchproducten. SwOS biedt uitgebreide configuratiemogelijkheden via een webbrowserinterface. Met deze interface kunt u niet alleen de basisfunctionaliteit van uw beheerde switch beheren, maar ook meer geavanceerde taken uitvoeren, zoals port-to-port forwarding, MAC-filtering, VLAN-configuratie, verkeersmonitoring, bandbreedtebeheer en het aanpassen van headervelden voor bepaalde MAC en IP.

### 3.2.2 Werkwijze en implementatie

#### 3.2.2.1 Onderzoeksmethoden

Mijn onderzoek begon met het raadplegen van diverse educatieve bronnen, zoals tutorials, om een praktisch begrip van de materie te krijgen. Daarna zocht ik naar gedetailleerde documentatie over de RB260GSP switch waar ik mee werkte, hoewel deze beperkter was dan de informatie die beschikbaar was voor de hEX PoE-router. Hierdoor heeft het ook wat langer geduurd om juiste en volledige informatie over de RB260GSP switch te vinden.

### 3.2.2.2 Verkenning van configuratiemogelijkheden

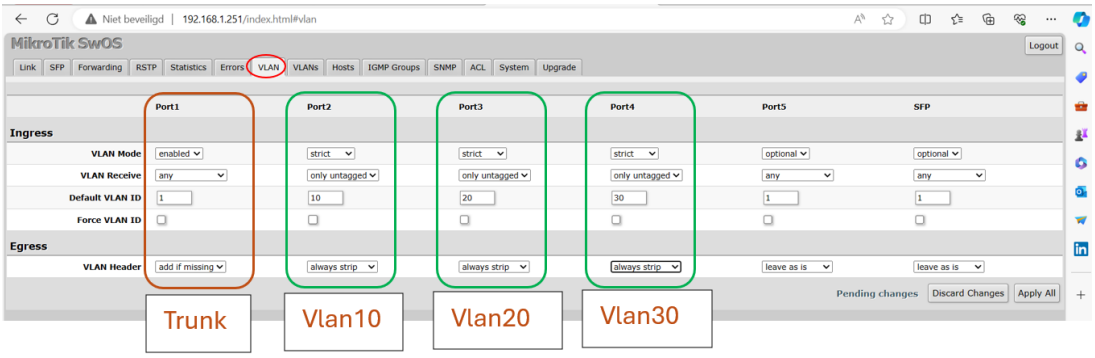
Een grondige verkenning van de configuratiemogelijkheden van de RB260GSP switch was essentieel voor het correct opzetten van mijn test netwerk. Het werd al snel duidelijk dat de configuratie via de webbrowserinterface verliep, aangezien er geen informatie beschikbaar was over de Command Line Interface (CLI).

### 3.2.2.3 User story’s

1. Ik wil toegang hebben tot verschillende netwerksegmenten via de VLAN's
2. Ik wil zonder problemen kunnen communiceren met andere gebruikers en apparaten binnen hetzelfde VLAN.
3. Ik verwacht dat mijn netwerktoegang soepel verloopt, ongeacht de achterliggende VLAN-configuratie.
4. Ik wil niet worden belast met het opzetten of wijzigen van VLAN-configuraties, maar wil er wel van profiteren voor een verbeterde netwerkervaring.

### 3.2.2.4 Implementatie van basisconfiguraties

Mijn initiële focus lag op het configureren van VLAN's op de switch, gevolgd door het instellen van een trunk om deze VLAN's te vervoeren naar mijn hEX PoE-router. Deze aanpak was essentieel om mijn netwerk te segmenteren en te organiseren, wat resulteerde in een betere beheersbaarheid en efficiëntie. Met behulp van de trunk kon ik meerdere VLAN's transporteren naar mijn vooraf geconfigureerde router, waardoor ik een solide basis legde voor verdere netwerktopologie en -functionaliteit.




*Figuur 3*

### 3.2.2.5 Back-upprocedures

Ik heb ervoor gezorgd dat ik na elke wijziging een back-up van de configuratie van mijn switch maakte. Deze voorzorgsmaatregel was noodzakelijk, aangezien ik had opgemerkt dat elke keer wanneer ik de stroom van de switch 's avonds

uitschakelde bij het verlaten van het labo, mijn configuratie verloren ging. Door regelmatig back-ups te maken, kon ik mijn configuratie eenvoudig herstellen in het geval dat deze opnieuw verloren zou gaan.

## 3.3 wAP R

*Figuur 4*

Als derde heb ik mij toegelegd op de configuratie van de wAP R. Vanwege de overeenkomsten in configuratie met de hAP PoE-router verliep dit proces al vlotter. Desondanks ondervond ik enige uitdagingen bij het instellen van het draadloze netwerk.

### 3.3.1 Wat is de wAP R?

De wAP R is een compact draadloos access point dat weerbestendig is op de 2,4 GHz frequentie. Het heeft een miniPCI-e-slot en een LTE-antenne. Voor bekabelde apparaten is één enkele 10/100 Ethernet LAN-poort beschikbaar.

Dit weerbestendige apparaat is geschikt voor een verscheidenheid aan buiten- en mobiele toepassingen, waaronder installatie buitenshuis, in voertuigen, op veranda's en overal waar draadloze toegang vanaf een mobiele telefoon of computer vereist is. Er wordt een tafelstandaard meegeleverd voor gebruik binnenshuis, bijvoorbeeld bij een raam.

Er zijn meerdere voedingsopties beschikbaar, waaronder 9-30V PoE-invoer via Ethernet-poort, DC-aansluiting en autostekker. Deze opties zijn handig voor mobiele toepassingen zoals auto's, bussen of treinen.

Let op: Dit apparaat heeft in eerste instantie geen ingebouwd LTE-modem. Het SIM-slot is alleen beschikbaar als er een LTE-modem is geïnstalleerd, aangezien dit modem niet bij het product wordt geleverd.

### 3.3.2 Werkwijze en Implementatie

#### 3.3.2.1 Onderzoeksmethoden

Door de gelijkenissen in configuratie met de hAP PoE-router, vereiste het instellen van dit draadloze toegangspunt minder onderzoek. Desalniettemin heb ik aanzienlijke inspanningen moeten leveren om een goede tutorial te vinden waarin duidelijk werd uitgelegd hoe ik het draadloze gedeelte correct kon implementeren op deze router.

#### 3.3.2.2 Verkenning van configuratiemogelijkheden

Op de wAP R werden twee methoden van configuratie toegepast, waarbij zowel de grafische interface via WinBox als de Command Line Interface beschikbaar waren. Dit was dus hetzelfde als bij de hEX PoE router.

#### 3.3.2.3 User story’s

1. Ik wil een eenvoudige manier hebben om de router te initialiseren en de fabrieksinstellingen te herstellen.

2. Ik wil in staat zijn om gebruikersaccounts aan te maken, te wijzigen en te verwijderen.

3. Ik wil de mogelijkheid hebben om onnodige services uit te schakelen om het aanvalsoppervlak te verminderen.

4. Ik wil standaardpoorten kunnen wijzigen om te voorkomen dat potentiële aanvallers gemakkelijk toegang krijgen tot het netwerk.

5. Ik wil dat routers effectief met elkaar kunnen communiceren door routing tussen routers in te stellen.

6. Ik wil de mogelijkheid hebben om een draadloos netwerk op te zetten voor draadloze apparaten, zodat alle gebruikers toegang hebben tot internet.

7. Als gebruiker wil ik de mogelijkheid hebben om via een domeinnaam te zoeken naar de gewenste website, zodat ik snel en gemakkelijk toegang kan krijgen tot de benodigde informatie.

8. Als gebruiker wil ik dat mijn privé IP-adres niet automatisch wordt gedeeld met externe verbindingen buiten mijn netwerk, om mijn privacy en veiligheid te waarborgen.

#### 3.3.2.4 Implementatie van basisconfiguraties

1. Routerinitialisatie en gebruikersbeheer: Voorafgaand aan de eerste configuratie heb ik het access point volledig gereset om een schone basis te garanderen. Vervolgens heb ik mijn eigen gebruikersaccount aangemaakt en beheerdersrechten toegewezen, waarbij ik de standaardbeheerdersaccount heb verwijderd om beveiligingsrisico's te minimaliseren.

2. Beveiligingsmaatregelen: Een cruciale stap was het implementeren van beveiligingsprotocollen, waaronder het uitschakelen van onnodige services zoals telnet en het wijzigen van standaardpoorten zoals SSH om externe toegang te beperken. Door deze maatregelen te treffen, wordt de blootstelling aan potentiële bedreigingen verminderd en wordt de algehele netwerkintegriteit versterkt.

3. Netwerkconfiguratie: Ik heb een DHCP-client ingesteld op het draadloze toegangspunt, zodat het een IP-adres kon verkrijgen van de hAP PoE-router. Daarnaast heb ik een routing opgezet tussen beide routers om effectieve communicatie mogelijk te maken. Bovendien was het noodzakelijk een bridge te configureren, aangezien ik anders problemen ondervond bij het tot stand brengen van de draadloze verbinding. Verder heb ik een draadloos netwerk opgezet, waardoor ik ook andere apparaten die niet rechtstreeks via een kabel zijn verbonden, kon voorzien van internettoegang en een IP-adres.

4. Domeinnaamservice (DNS): Het instellen van een interne DNS-server stelde het netwerk in staat om domeinnamen naar IP-adressen te vertalen, waardoor communicatie tussen apparaten mogelijk was en gebruikersvriendelijke toegang tot netwerkbronnen werd geboden.

5. Netwerkadresvertaling (NAT) en firewallfilterregels: Door het toepassen van NAT met masquerading, kon ik meerdere privé-IP-adressen converteren naar één enkel openbaar IP-adres, waardoor de interne netwerkstructuur afgeschermd bleef voor externe bronnen. De firewallregels werden nauwkeurig geconfigureerd om enkel geautoriseerd verkeer toe te laten en ongeautoriseerde toegang te blokkeren, met als resultaat het waarborgen van de netwerkbeveiliging. Bovendien werd specifiek verkeer van de hAP PoE-router toegestaan, om ervoor te zorgen dat communicatie ongehinderd kon verlopen zonder enige belemmering door de firewallfilterregels.

## 3.4 Troubleshooting en problemen

Tijdens het configuratieproces van de router ondervond ik aanvankelijk enkele uitdagingen. Een foute configuratie leidde tot het ontoegankelijk worden van de router, waardoor ik gedwongen was om het systeem te resetten en opnieuw te beginnen. Deze herstartprocedure vergde aanzienlijke tijd.

Een poging om een Raspberry Pi aan te sluiten op het testnetwerk met als doel een aanvullende firewall te implementeren, bleek onsuccesvol vanwege stroomproblemen. De Raspberry Pi ontving niet voldoende stroom, wat resulteerde in overbelasting van de router, waardoor de hoofdrouter in de problemen kwam. Daarnaast bleek de installatie van IPFire op de Raspberry Pi problematisch, aangezien deze firewall niet volledig compatibel is met het Raspberry Pi-platform. Dit onvoorziene obstakel vergde eveneens aanzienlijke inspanningen en tijd.

Daarnaast ondervond ik moeilijkheden met het wifi-netwerk dat ik had opgezet. Incidenteel viel de verbinding weg, wat uiteindelijk te wijten bleek aan een loszittende netwerkkabel, waardoor de internetverbinding naar de router werd onderbroken.

Tot slot, bij mijn poging om MQTT te implementeren, stuitte ik op diverse problemen. Het toevoegen van brokers en het tot stand brengen van verbindingen met het gespecificeerde netwerk op RouterOS bleek uitdagend. Ondanks uitgebreid onderzoek en inspanningen om de oorzaak van de problemen te achterhalen, resulteerde de implementatie van MQTT telkens in het wegvallen van de internetverbinding. Door een nieuwe opdracht en het ontbreken van een oplossing voor dit specifieke probleem, was het uiteindelijk niet mogelijk om MQTT succesvol te implementeren in MikroTik.

# 4 WIREGUARD

Na afronding van mijn werk met de MikroTik systemen, heb ik mijn focus verlegd naar WireGuard. In eerste instantie stond dit niet in mijn plan van aanpak, omdat het systeem pas later in beeld kwam tijdens mijn verkenning van de MikroTik systemen. Desondanks hebben José en Joao mij toestemming gegeven om meer over WireGuard te leren. Hoewel ik dit systeem eerder op school had gezien, was het voor mij niet volledig nieuw om ermee te werken. Niettemin heb ik tijdens dit proces veel nieuwe kennis opgedaan over dit systeem.

## 4.1 Wat is WireGuard?

WireGuard is een snel, modern en veilig VPN-protocol dat is ontworpen om gemakkelijk te gebruiken en zeer prestatiegericht te zijn. Het werkt op het kernelniveau, waardoor het een lichtgewicht maar robuuste oplossing biedt voor het creëren van veilige tunnels over het internet. In tegenstelling tot traditionele VPN-protocollen streeft WireGuard naar eenvoud in zowel zijn codebase als configuratie, waardoor het een uitstekende keuze is voor zowel beginners als ervaren gebruikers.

## 4.2 Werkwijze en Implementatie

Tijdens mijn stage heb ik me ook even helemaal toegewijd aan het verkennen en implementeren van WireGuard. Mijn aanpak omvatte zorgvuldige onderzoeksstappen en praktische experimenten om een diepgaand begrip van de technologie te verkrijgen en deze effectief toe te passen in een netwerkomgeving.

### 4.2.1 Onderzoek en Kennisverwerving

Mijn inzet begon met grondig onderzoek naar WireGuard. Ik maakte gebruik van verschillende bronnen, waaronder YouTube-tutorials, officiële documentatie van de WireGuard-website en relevante filmpjes gedeeld door Joao Santos via Zotero. Deze diverse bronnen gaven me een uitgebreid inzicht in de werking en implementatie van WireGuard.

### 4.2.2 User story’s

1. Als een netwerkbeheerder wil ik een stevige basis van kennis hebben over WireGuard-verbindingen zodat ik praktisch aan de slag kan met het opzetten van verbindingen.

2. Als een netwerkbeheerder wil ik ondersteuning bieden aan mijn collega's zodat zij zelfs op afstand kunnen helpen bij eventuele problemen in het testnetwerk.

3. Als een netwerkbeheerder wil ik een uitgebreid begrip hebben van WireGuard in verschillende besturingssystemen zodat ik succesvolle verbindingen kan tot stand brengen tussen verschillende apparaten.

### 4.2.3 Implementatie van basisconfiguraties

Met een stevige basis van kennis begon ik met het praktisch opzetten van WireGuard-verbindingen. Mijn eerste experiment omvatte het tot stand brengen van een succesvolle connectie tussen twee routers in mijn testnetwerk, specifiek

de hAP PoE-router en de wAP R-router. Deze initiële implementatie vormde de basis voor verdere exploratie.

### 4.2.4 Uitbreiding van Experimenten

Om de mogelijkheden van WireGuard volledig te benutten, besloot ik mijn experimenten uit te breiden naar andere scenario's. Ik configureerde een WireGuard-verbinding tussen mijn hAP PoE-router en mijn laptop, waardoor ik vanaf mijn studentenkamer kon werken in mijn testnetwerk. Daarnaast onderzocht ik ook de haalbaarheid van het opzetten van een WireGuard-verbinding op mijn mobiele telefoon, waardoor ik zelfs onderweg toegang had tot het testnetwerk.

### 4.2.5 Ondersteuning voor Collega's

Naast mijn eigen experimenten stond ik ook klaar om ondersteuning te bieden aan mijn collega's. Ik zette een WireGuard-verbinding op voor Joao, zodat hij, zelfs als hij niet fysiek aanwezig was in het lab, vanuit huis nog steeds kon helpen bij eventuele problemen in mijn testnetwerk.

### 4.2.6 Verdieping in Besturingssystemen

Om een uitgebreid begrip van WireGuard te krijgen, onderzocht ik ook de werking ervan in verschillende besturingssystemen. Ik testte de implementatie zowel in Windows als in Linux. Voor het testen op Linux gebruikte ik mijn ubuntu Linux-installatie in de proxmox omgeving, waarbij ik succesvolle verbindingen tot stand bracht tussen verschillende apparaten, waaronder mijn telefoon en mijn laptop.

## 4.3 Troubleshooting en problemen

Tijdens de implementatie van WireGuard in mijn testnetwerk stuitte ik op een probleem waarbij ik na het inschakelen van de VPN-verbinding geen toegang meer had tot mijn routers en switches. Dit was een aanzienlijke hinder, aangezien ik op dat moment nog verschillende configuraties op deze apparaten aan het uitvoeren was. Gelukkig kon ik dit probleem oplossen door de verbinding opnieuw op te zetten vanaf het begin en vervolgens in te loggen op Winbox met het verkregen IP-adres. Na deze stappen functioneerde alles weer naar behoren. Het oplossen van deze fout kostte echter wel aanzienlijke tijd.

Een ander probleem deed zich voor bij het verzenden en ontvangen van bytes via WireGuard tussen routers. Aanvankelijk vermoedde ik dat dit te wijten was aan de firewallregels, maar deze bleken al snel uitgesloten als oorzaak. Na grondig onderzoek ontdekte ik dat het leggen van een route tussen de twee WireGuard-verbindingen van de router het probleem oploste.

# 5 PROXMOX

In het laboratorium werd een nieuwe omgeving geïmplementeerd, namelijk een Proxmox-omgeving. Deze nieuwe omgeving vereiste initiële configuratie, wat resulteerde in een lange wachttijd voor het verkrijgen van inloggegevens om toegang te krijgen tot de Proxmox-omgeving. Ook dit is een systeem dat er later pas bijgekomen is en daarom dus ook niet in mijn plan van aanpak staat.

## 5.1 Wat is Proxmox?

Proxmox Virtual Environment, oftewel Proxmox VE, is een open-source virtualisatieplatform dat twee technologieën combineert: KVM (Kernel-based Virtual Machine) voor virtuele machines en LXC (Linux Containers) voor lichtgewicht containergebaseerde virtualisatie. Het biedt een gecentraliseerde beheerinterface via een webgebaseerd dashboard, waarmee gebruikers virtuele machines en containers kunnen maken en beheren op een enkele fysieke host. Met functies zoals live migratie, high availability clustering en flexibele opslagondersteuning is Proxmox VE populair vanwege zijn flexibiliteit en kosteneffectiviteit voor zowel professionele als persoonlijke projecten.

## 5.2 Inrichting en Training

Nadat ik mijn inloggegevens had ontvangen, kreeg ik instructies over het opzetten en beheren van virtuele machines binnen de Proxmox-omgeving. Vanwege mijn beperkte rechten was ik echter niet in staat om alle taken zelfstandig uit te voeren. Bijvoorbeeld bij het creëren van specifieke omgevingen, zoals VLAN's, moest ik hulp vragen aan een van de professoren.

## 5.3 Nieuwe Ervaring en Ondersteuning

Werken in de Proxmox-omgeving bood mij een nieuwe leerervaring. Gelukkig hoefde ik zelf niet veel onderzoek te doen, omdat de professoren mij grondige uitleg gaven over het gebruik van het platform. Dit verminderde de leercurve en zorgde voor een soepele overgang naar het werken binnen deze nieuwe omgeving.

## 5.4 Troubleshooting en problemen

Tijdens het opzetten van een externe verbinding met de Proxmox-omgeving voor werken op afstand tijdens de feestdagen, werden enkele problemen geïdentificeerd. In samenwerking met collega's José en Joao werden deze kwesties geanalyseerd om de oorzaak vast te stellen en passende oplossingen te vinden. Dit proces vergde enkele dagen van intensieve inspanning, waarbij meerdere overleggen plaatsvonden om het probleem te identificeren en op te lossen.

Na uitgebreide troubleshooting slaagden we er uiteindelijk in om de externe verbinding tot stand te brengen. Joao implementeerde enkele aanpassingen in de configuratiebestanden van de Lola-router in het Sepsi-laboratorium, dat gekoppeld is aan de Wotan-server waarop de Proxmox-omgeving draait. Daarnaast heb ik ook configuratiebestanden aangemaakt om een correcte SSH-verbinding te waarborgen.

# 6 IPFIRE

Ondanks dat er andere systemen tussendoor kwamen, ben ik toch in week 4 begonnen met het configureren van de IpFire firewall in de Proxmox-omgeving. Ik ben blij dat, ondanks de extra taken, de planning zoals beschreven in mijn plan van aanpak nog steeds nauwkeurig bleek te zijn.

## 6.1 Wat is IpFire?

IPFire is een open source Linux-distributie die is ontworpen om te dienen als een krachtige, veelzijdige en veilige netwerkfirewalloplossing. Het biedt een breed scala aan functies, waaronder firewallfunctionaliteit, Network Address Translation (NAT), Virtual Private Network (VPN), Inbraakdetectie/preventiesysteem (IDS/IPS), proxyserver en Quality of Service (QoS)-beheer. IPFire is geschikt voor thuisgebruik en kleine tot middelgrote bedrijfsnetwerken en beschikt over een gebruiksvriendelijke interface, modulaire architectuur en een sterke focus op beveiliging.

## 6.2 Werkwijze en implementatie

### 6.2.1 Onderzoek en kennisverwerving

Om de IPFire firewall effectief te kunnen implementeren tijdens mijn stage, heb ik een grondig onderzoek uitgevoerd naar het platform en zijn functionaliteiten. Als eerste stap heb ik me verdiept in de installatieprocedure en het werken met IPFire. Aangezien dit mijn eerste ervaring was met IPFire, heb ik verschillende tutorials en documentatiebronnen geraadpleegd om een diepgaand begrip te krijgen van het systeem. Dit onderzoek was essentieel om een solide basis te leggen voor verdere configuraties.

### 6.2.2 User story’s

1. Als een netwerkbeheerder wil ik URL-filters kunnen instellen op de IPFire firewall, zodat ik specifieke websites kan blokkeren en ongewenst browsen kan voorkomen.

2. Als een netwerkbeheerder wil ik firewallregels kunnen opzetten op de IPFire firewall, zodat ik kan bepalen welk verkeer mag passeren en welk verkeer moet worden geblokkeerd.

3. Als een netwerkbeheerder wil ik IPS kunnen implementeren op de IPFire firewall, zodat ik verdacht verkeer kan detecteren en blokkeren, waardoor potentiële bedreigingen effectief worden aangepakt en de veiligheid van het netwerk wordt versterkt.

4. Als een netwerkbeheerder wil ik de DNS-configuratie kunnen instellen op de IPFire firewall, zodat DNS-verzoeken correct worden verwerkt.

5. Als een netwerkbeheerder wil ik specifieke statische routes kunnen opzetten op de IPFire firewall, zodat ik connectiviteit kan waarborgen tussen de firewall en de MikroTik-router.

6. Als een netwerkbeheerder wil ik de Connection Scheduler-functionaliteit van de IPFire firewall kunnen gebruiken, zodat ik het verkeer binnen bepaalde tijdspannes kan reguleren.

7. Als een netwerkbeheerder wil ik een IP-adres blocklist kunnen aanmaken op de IPFire firewall, zodat ik het netwerk kan beschermen tegen bekende kwaadaardige IP-adressen. Hierdoor kan ik potentiële bedreigingen proactief blokkeren.

### 6.2.3 Implementatie van basisconfiguraties

Na het verzamelen van de benodigde kennis, begon ik met de implementatie van de basisconfiguraties voor de IPFire firewall. Hier volgt een overzicht van de stappen die ik heb genomen:

1. URL-filters opzetten: Om het internetverkeer te kunnen beheren en controleren, heb ik URL-filters ingesteld. Hierdoor kon ik bijvoorbeeld specifieke websites blokkeren om ongewenst browsen te voorkomen.

2. Firewallregels opzetten: Het opzetten van firewallregels was van cruciaal belang om te bepalen welk verkeer mocht passeren en welk verkeer moest worden geblokkeerd. Ik heb regels opgesteld om ICMP en DNS-verkeer toe te staan, externe toegang tot de firewall te verlenen, en alle andere verkeer te blokkeren.

3. Implementatie van IPS (Intrusion Prevention System): Om verdacht verkeer te detecteren en te blokkeren, heb ik IPS geïmplementeerd op de firewall. Hierdoor kon ik potentiële bedreigingen effectief aanpakken en de veiligheid van het netwerk versterken.

4. DNS-configuratie: Om DNS-verzoeken te verwerken, heb ik de DNS-instellingen geconfigureerd op de IPFire firewall. Hierbij heb ik Google ingesteld als de DNS-forwarder om een betrouwbare en snelle DNS-resolutie te garanderen.

5. Statische routes opzetten: Om connectiviteit te waarborgen tussen de IPFire firewall en de MikroTik-router, heb ik specifieke statische routes geconfigureerd. Dit was nodig om ervoor te zorgen dat beide apparaten elkaar konden vinden en communiceren binnen het netwerk.

6. Gebruik van Connection Scheduler: Ik heb de Connection Scheduler-functionaliteit van IPFire verkend en toegepast om het verkeer binnen bepaalde tijdspannes te reguleren. Hiermee kon ik bijvoorbeeld buiten kantooruren de toegang tot het netwerk beperken door verkeer te blokkeren.

7. IP-adres blocklist: Om het netwerk te beschermen tegen bekende kwaadaardige IP-adressen, heb ik een IP-adres blocklist aangemaakt. Deze lijst bevatte IP-adressen die gekend zijn voor kwaadwillige activiteiten, en hierdoor kon ik potentiële bedreigingen proactief blokkeren.

8. Documentatie en handleiding: Gedurende het hele proces heb ik gedetailleerde documentatie bijgehouden, die later diende als een cursus of handleiding voor beginners. Deze documentatie is waardevol voor mij en mijn collega's om te verwijzen naar de configuraties die ik heb geïmplementeerd en om in de toekomst eventuele wijzigingen aan te brengen of problemen op te lossen.

## 6.3 Troubleshooting en problemen

Tijdens mijn werk met IPFire heb ik enkele uitdagingen ondervonden die ik professioneel heb aangepakt. Eén van de uitdagingen betrof het implementeren van intrusion detection. Ondanks uitgebreid zoeken op internet vond ik geen duidelijke richtlijnen. Om deze kwestie op te lossen, heb ik advies ingewonnen bij José, die me adviseerde Suricata te koppelen aan IPFire. Hoewel ik erin slaagde dit te implementeren voor het intrusion prevention systeem van IPFire, bleef ik steken omdat er geen duidelijke bronnen waren over hoe dit te doen voor het IDS in IPFire. Dit benadrukte de noodzaak voor betere documentatie en toegankelijke bronnen voor dergelijke integraties.

Een ander probleem dat ik tegenkwam, was beperkte opties bij het instellen van het URL-filtering. Dit resulteerde in een verminderde functionaliteit en beperkte mogelijkheden. Na het raadplegen van verschillende tutorials en het experimenteren met verschillende instellingen, slaagde ik er uiteindelijk in om de opties uit te breiden en het URL-filtering systeem naar behoren te laten functioneren. Deze ervaring onderstreepte het belang van geduld, doorzettingsvermogen en een grondig begrip van de configuratie-opties binnen IPFire.

# 7 OPNSENSE

Hoewel OpnSense aanvankelijk niet in mijn plan van aanpak stond, hebben de professoren in het laboratorium toch gevraagd om deze beter te leren kennen, omdat OpnSense nauwkeuriger is dan IpFire.

## 7.1 Wat is OpnSense?

Opsense is een firewall- en routerplatform dat is ontworpen om de netwerkbeveiliging te verbeteren door het netwerkverkeer te monitoren en te reguleren. Het biedt een breed scala aan functies, waaronder firewallregels, VPN-ondersteuning, inbraakpreventie, antivirus- en antispamfiltering en meer.Opnsense wordt regelmatig bijgewerkt en onderhouden door een actieve gemeenschap van ontwikkelaars, waardoor het een betrouwbare en actuele oplossing is voor netwerkbeveiliging.

## 7.2 Werkwijze en implementatie

### 7.2.1 Onderzoek en kennisverwerving

Het implementeren van OpnSense in de Proxmox-omgeving vereiste een grondig begrip van zowel netwerkconfiguraties als firewallinstellingen. Om deze taak succesvol uit te voeren, heb ik nauw samengewerkt met een professor uit het labo. We begonnen met het identificeren van de benodigde stappen en het plannen van de implementatie.

Een uitdaging die we tegenkwamen was het toevoegen van een nieuw VLAN om de OpnSense-firewall en de gastmachine in hetzelfde VLAN te plaatsen. Aangezien ikzelf geen toegang had tot het aanmaken van deze VLAN's, moest ik inloggen op het admin-account om de vereiste configuraties uit te voeren.

### 7.2.2 User story’s

1. De gebruiker moet in staat zijn om verbinding te maken met het bedrijfsnetwerk via een beveiligde VPN-verbinding.

2. De firewall moet in staat zijn om ongewenst inkomend en uitgaand verkeer te blokkeren, waardoor mijn thuisnetwerk wordt beschermd tegen cyberaanvallen.

3. Ik moet gemakkelijk kunnen controleren welke apparaten toegang hebben tot het internet en welke worden geblokkeerd.

### 7.2.3 Implementatie van de basisconfiguraties in OpnSense

Na het opzetten van de infrastructuur en het uitvoeren van de nodige VLAN-configuraties, heb ik me gericht op de basisconfiguraties van OpnSense.

1. Firewallregels: Ik heb uitgebreid onderzoek gedaan naar het opzetten van firewallregels om het netwerkverkeer te beheren en te beveiligen. Dit omvatte het definiëren van regels voor inkomend en uitgaand verkeer, evenals het implementeren van NAT-regels.

2. VPN-configuratie: Om een veilige verbinding tussen externe locaties en ons netwerk mogelijk te maken, heb ik VPN's geconfigureerd met behulp

van OpnSense. Dit omvatte het opzetten van een WireGuard-verbinding voor veilige toegang tot het interne netwerk.

3. Intrusion Prevention: Ik heb de opties voor intrusion prevention binnen OpnSense onderzocht en beoordeeld hoe deze konden worden geconfigureerd om de netwerkbeveiliging te verbeteren.

Hoewel de implementatie van OpnSense geen officiële opdracht was van mijn stagebegeleider, heb ik ervoor gekozen om deze taken uit te voeren om mijn begrip van netwerkbeveiliging en firewalltechnologie te vergroten. De kennis en ervaring die ik heb opgedaan tijdens dit proces zullen van onschatbare waarde zijn voor toekomstige projecten en uitdagingen op het gebied van netwerkbeveiliging.

## 7.3 Troubleshooting en problemen

Tijdens mijn ervaring met OpnSense stuitte ik op enkele uitdagingen met de connectiviteit tussen WireGuard en OpnSense. Na meerdere pogingen en het raadplegen van aanvullende tutorials, slaagde ik erin deze problemen op te lossen. Bovendien ondervond ik moeilijkheden bij het initiëren van de OpnSense-machine, omdat ik aanvankelijk niet de juiste rechten had om een VLAN aan te maken, wat essentieel was voor het creëren van een VLAN-netwerk met twee machines. Om dit op te lossen, heb ik, in samenwerking met mijn docent, het admin-account gebruikt om de benodigde configuraties voor de machines en het VLAN op te zetten. Nadat de implementatie en installatie waren voltooid, keerde ik terug naar mijn eigen account om verder te werken.

# 8 NETBOX

Netbox is ook tijdens mijn stage toegevoegd aan mijn takenlijst daarom vindt u ook dit systeem niet terug in mijn plan van aanpak. Het is een management systeem waar José op stuitte en zelf nog niet veel ervaring mee had, maar wel zeer interessant vond. Dit leidde ertoe dat ik de opdracht kreeg om dit systeem te onderzoeken en te documenteren, zodat zij aan de hand van mijn documentatie het systeem ook beter konden leren kennen. Netbox bleek een zeer uitgebreid systeem te zijn, wat veel tijd vergde om het volledig te doorgronden.

## 8.1 Wat is NetBox?

NetBox is een open-source applicatie voor IP-adresbeheer (IPAM) en het beheer van datacenterinfrastructuur. Het is ontwikkeld om te dienen als een centrale database en beheersysteem voor IP-adressen, netwerken, apparaten en andere elementen van een IT-infrastructuur. Met NetBox kunnen organisaties effectief hun netwerkbronnen documenteren, visualiseren en beheren, waardoor ze beter netwerkassets kunnen bijhouden, wijzigingen kunnen plannen en problemen kunnen oplossen. NetBox biedt functionaliteiten zoals IP-adresbeheer, subnetbeheer, apparaatbeheer, rackvisualisatie, kabelbeheer en integratie met andere systemen via een RESTful API. Het is een veelgebruikt instrument in IT-omgevingen voor netwerk- en datacenterbeheer.

## 8.2 Werkwijze en implementatie

### 8.2.1 Onderzoek en kennisverwerving

Mijn eerste stap in het begrijpen en implementeren van NetBox was grondig onderzoek. Zowel mijn stagebegeleider als ikzelf waren nieuw met dit platform. Ik dook diep in de documentatie van NetBox, maar al snel merkte ik dat deze niet altijd even duidelijk was voor mij persoonlijk. Om een beter begrip te krijgen, heb ik me verdiept in tutorials en andere educatieve video's die de gebruiksmogelijkheden en theoretische achtergrond van NetBox helder beschreven.

### 8.2.2 User story’s

1. Als gebruiker wil ik in staat zijn om snel en eenvoudig de informatie van verschillende netwerklocaties te raadplegen in NetBox, zodat ik een overzicht heb van onze wereldwijde infrastructuur.

2. Als gebruiker wil ik de mogelijkheid hebben om de apparaten in ons netwerk te kunnen identificeren en hun kenmerken te bekijken, zoals manufacturer, model en locatie, om effectiever onderhoud te kunnen plannen en asset management te vergemakkelijken.

3. Als gebruiker wil ik via NetBox toegang hebben tot de specificaties van verschillende netwerkapparaten, zodat ik mijn applicaties kan ontwikkelen en testen met inachtneming van de netwerkvereisten.

4. Als gebruiker wil ik alle benodigde informatie over actieve VLAN's kunnen vinden in NetBox, zodat ik snel problemen kan identificeren en oplossen voor wanneer ik met netwerkproblemen kamp.

### 8.2.3 Implementatie van de basisconfiguratie

Tijdens de implementatiefase in NetBox heb ik de volgende entiteiten geconfigureerd en beheerd:

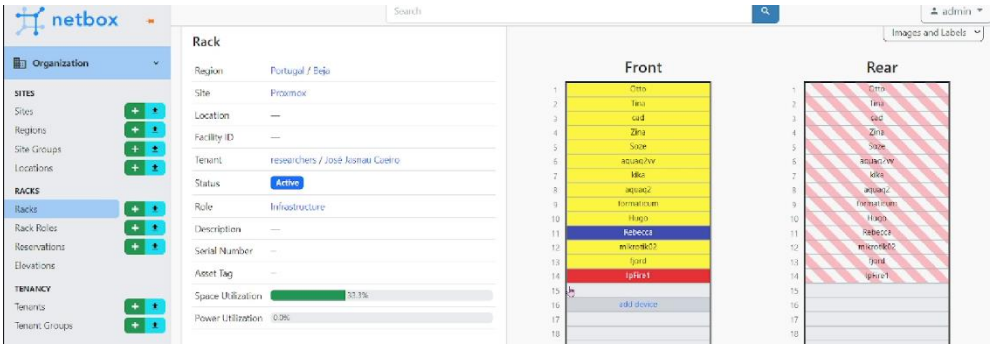
1. Gebruikersconfiguraties: Gebruikers zijn aangemaakt met verschillende toegangsrechten, zodat ze overeenkomen met hun verantwoordelijkheden binnen het netwerk.

2. Entiteitenconfiguraties: Sites, tenants, racks, device roles, regio's, manufacturers, device types, VLAN-groepen en VLAN's zijn geconfigureerd en beheerd om een gestructureerd overzicht van de netwerkinfrastructuur te bieden.

3. Bekabeling en Voeding: De fysieke verbindingen en voedingseenheden zijn geconfigureerd om een nauwkeurige documentatie van de netwerkapparatuur te garanderen.

4. Interfaces: De interfaces van verschillende netwerkapparaten zijn geconfigureerd om de connectiviteit binnen het netwerk te optimaliseren.

Deze instellingen zijn uitvoerig gedocumenteerd in een handleiding, waardoor toekomstige gebruikers een naslagwerk hebben voor het opzetten en beheren van hun netwerkinfrastructuur met behulp van NetBox. Ik heb dit alles opgezet voor het SEPSI-lab, zodat zij NetBox kunnen inzetten als een managementtool voor hun eigen netwerk.




*Figuur 5*

## 8.3 Troubleshooting en problemen

Het begrijpen en effectief gebruiken van NetBox kostte heel wat tijd, aangezien het een complex systeem is met een breed scala aan functionaliteiten. De overvloed aan mogelijkheden maakte het soms verwarrend, wat resulteerde in een leercurve voor mijzelf. Bovendien werd de uitdaging vergroot doordat dit systeem nieuw was voor alle betrokkenen in het SEPSILab, inclusief mijn stagebegeleider, wat het lastig maakte om directe ondersteuning te krijgen bij onduidelijkheden.

Het integreren van de MikroTik plugin bleek een aanzienlijke uitdaging te zijn vanwege het gebrek aan toegankelijke en begrijpelijke documentatie of instructievideo's. Ondanks uitgebreid onderzoek en pogingen om dit te implementeren, bleek het helaas niet mogelijk om tot een succesvolle afronding te komen.

# 9 EVE-NG

Het netwerkdiagram heeft wat vertraging opgelopen omdat de professoren erg druk waren en niet alle details over het netwerk konden verstrekken. Bovendien wilden ze dat ik het diagram maakte in EVE-NG, wat aanvankelijk niet in mijn plan van aanpak stond. Dit gaf mij de kans om de systemen opnieuw te configureren en extra te oefenen met de configuraties. Helaas verliep dit proces niet soepel vanwege problemen met EVE-NG, dus zijn we na een week van pogingen overgestapt naar GNS3.

## 9.1 Wat is Eve-NG?

EVE-NG is een krachtige netwerkvirtualisatietool die wordt gebruikt voor het bouwen en simuleren van complexe netwerken. Met EVE-NG kunnen gebruikers virtuele machines (VM's) van verschillende netwerkapparaten zoals routers, switches, firewalls en servers maken en deze verbinden om echte netwerkomgevingen na te bootsen.

## 9.2 Werkwijze en implementatie

### 9.2.1 Onderzoek en Kennisverwerving

Mijn kennismaking met EVE-NG begon met grondig onderzoek om het systeem te begrijpen, aangezien het nieuw was voor zowel mij als mijn stagebegeleider. Ik heb verschillende bronnen geraadpleegd, waaronder video's en documentatie, om een diepgaand inzicht te krijgen in de installatie en werking van EVE-NG. Dit omvatte het bestuderen van installatieprocedures en het verkrijgen van praktische kennis over het configureren van routers, switches en andere netwerkapparaten binnen de EVE-NG-omgeving.

### 9.2.2 User story’s

1. Als gebruiker wil ik een duidelijk overzicht van mijn netwerk in de vorm van een technisch schema zodat ik gemakkelijk kan terug vinden welke connecties er allemaal aanwezig zijn.
2. Als gebruiker wil ik gemakkelijk nieuwe implementaties testen in de testomgeving al vorens ik het implementeer in mijn fysieke omgeving.

## 9.3 Troubleshooting en problemen

Tijdens het implementatieproces stuitte ik op verschillende uitdagingen, met name bij het toevoegen van routers, switches en andere apparaten aan de EVE-NG omgeving. Ondanks mijn initiële inspanningen en het raadplegen van beschikbare bronnen, waaronder video's en documentatie, bleven foutmeldingen een terugkerend probleem. Zelfs na overleg met mijn stagebegeleider, bleven de oplossingen ongrijpbaar. Uiteindelijk resulteerde dit in een overstap naar GNS3, een vergelijkbaar systeem, in de hoop een werkende omgeving te verkrijgen. Desondanks heb ik de volledige installatieprocedure van EVE-NG gedocumenteerd, inclusief aanvullende uitleg over het systeem zelf, om een waardevolle bron van informatie te creëren voor toekomstige referentie.

# 10 GNS3

Dit systeem is toegevoegd omdat EVE-NG niet functioneerde zoals we hadden gehoopt. Ook dit systeem zult u niet terugvinden in mijn plan van aanpak, omdat dit aanvankelijk geen onderdeel was van mijn stage.

## 10.1 Wat is GNS3?

GNS3, wat staat voor Graphical Network Simulator-3, is een krachtige open-source netwerkemulator die wordt gebruikt voor het simuleren, configureren en testen van netwerken. Het biedt de mogelijkheid om virtuele netwerken te creëren en te beheren met echte netwerkapparaten en besturingssystemen. Met een intuïtieve grafische interface kunnen gebruikers complexe netwerktopologieën bouwen en ze draaien in een gecontroleerde virtuele omgeving.

## 10.2 Werkwijze en implementatie

### 10.2.1 Onderzoek en kennisverwerving

Ik heb uitgebreid onderzoek gedaan naar de installatieprocedure en configuratie-opties omdat dit voor zowel mij als voor mijn stagebegeleider een nieuw systeem was. Dit omvatte het bestuderen van documentatie en tutorials om een diepgaand begrip te krijgen van de benodigde stappen om zo succesvol GNS3 te kunnen installeren en implementeren.

### 10.2.2 User story’s

1. Als gebruiker wil ik een duidelijk overzicht van mijn netwerk in de vorm van een technisch schema zodat ik gemakkelijk kan terug vinden welke connecties er allemaal aanwezig zijn.

2. Als gebruiker wil ik gemakkelijk nieuwe implementaties testen in de testomgeving al vorens ik het implementeer in mijn fysieke omgeving.

### 10.2.3 Implementatie van de basisconfiguratie

Na uitgebreid onderzoek en overleg met mijn stagebegeleider, heb ik besloten om de GNS3-infrastructuur op te zetten binnen de Proxmox-omgeving. Dit vereiste het creëren van een Ubuntu-desktopmachine binnen Proxmox en het volgen van de installatie-instructies van GNS3. Ondanks enkele uitdagingen tijdens de installatie, zoals het ontbreken van vereiste softwarepakketten, kon ik met behulp van mijn stagebegeleider en het gebruik van Synaptic Package Manager de installatie succesvol voltooien. Na het oplossen van wat technische hindernissen, kon ik me concentreren op het bouwen en configureren van de netwerktopologieën, zowel voor mijn persoonlijke testomgeving als voor de specifieke omgeving van het sepsilab. Dit omvatte nauwe samenwerking met mijn stagebegeleider en collega's om een uitgebreide en nauwkeurige weergave van de netwerkinfrastructuur te garanderen. Ondanks enkele wachttijden als gevolg van drukke schema's, slaagde ik erin de gewenste topologieën succesvol te implementeren en te testen. Ook is alles duidelijk en grondig gedocumenteerd in de vorm van een handleiding voor beginners, in deze documentatie kan je alle stappen terug vinden om snel en gemakkelijk te leren werken met GNS3.


*Figuur 6*

## 10.3 Troubleshooting en problemen

Het proces was niet zonder hindernissen, zoals terugkerende foutmeldingen met betrekking tot KVM-acceleratie. Ik moest een configuratiebestand aanmaken in de map van de server en specifieke instellingen toevoegen om deze problemen op te lossen. Af en toe keerde de fout terug, maar door de betreffende regels te verwijderen en opnieuw toe te voegen, kon ik de problemen snel oplossen. Ik heb deze foutmelding ook duidelijk gedocumenteerd in de documentatie omdat ik op het internet heel wat mensen tegen kwam met hetzelfde probleem.

# 11 BESLUIT

Tijdens mijn stageperiode heb ik een aanzienlijke groei doorgemaakt, zowel op professioneel als persoonlijk vlak. Ik ben in aanraking gekomen met diverse nieuwe systemen waar ik voorheen geen ervaring mee had, waardoor mijn leervermogen is vergroot. Daarnaast kreeg ik de kans om projecten van andere professoren te observeren en af en toe een bescheiden bijdrage te leveren, wat mijn begrip van verschillende werkmethoden en benaderingen heeft verrijkt.

Ook heb ik een grondige tour van het IPBEJA-datacenter gekregen, waar ik een gedetailleerde rondleiding kreeg en uitgebreide uitleg over de operationele aspecten ervan ontving. Deze ervaring heeft mijn begrip van datacenterbeheer en infrastructuur aanzienlijk verdiept.

Op het gebied van soft skills heb ik eveneens vooruitgang geboekt. Ik heb geleerd om effectiever te communiceren met mensen van verschillende nationaliteiten. Daarnaast heb ik mijn geduld verder ontwikkeld, aangezien het soms nodig was om langer te wachten op bepaalde zaken, wat een belangrijke eigenschap is in een professionele omgeving.

Een andere opvallende verbetering is mijn Engelse taalvaardigheid. Door de voortdurende interactie met internationale collega's en de vereiste communicatie in het Engels tijdens mijn stage, heb ik mijn taalvaardigheden aanzienlijk verbeterd, wat me zowel professioneel als persoonlijk ten goede zal komen.

Bovendien is het vermogen om effectief te documenteren verbeterd als gevolg van de noodzaak om frequent verslag uit te brengen en procedures vast te leggen tijdens mijn stage. Deze vaardigheid is van onschatbare waarde gebleken en zal me in mijn toekomstige professionele trajecten ten goede komen.

Ten slotte heb ik mijn zelfstandigheid ontwikkeld door vele uren alleen door te brengen in het SEPSILab, waar ik zelfstandig aan mijn toegewezen taken heb gewerkt en mijn tijd effectief heb kunnen beheren.

Al met al heb ik mijn stage-ervaring als zeer leerzaam en plezierig ervaren, en ik ben dankbaar voor de mogelijkheid om te groeien en te leren in een internationale omgeving.

# 12 BIJLAGE

Hier vindt u een voorbeeld van een handleiding die ik heb geschreven. In deze gids heb ik alleen de hEX PeO en de wAP R van MikroTik behandeld, omdat alleen deze systemen voor mij beschikbaar waren in het labo. Aangezien alle systemen van MikroTik op vergelijkbare wijze werken, heb ik echter een goed inzicht in de andere systemen. U ziet ook dat ik de switch niet heb behandeld; dit komt doordat de configuraties hiervan zo beperkt waren dat de professoren en ik hebben besloten dit weg te laten.

Mikrotik  Guide

# 13 BRONNEN

About Plugins - NetBox documentation. (n.d.). https://docs.netbox.dev/en/stable/plugins/

ChatGPT. (n.d.). https://chat.openai.com/c/4242173c-783f-45a9-9ac4-a9feadb2aeac

Christian Lempa. (2020, June 1). WireGuard installation and configuration - on Linux [Video]. YouTube. https://www.youtube.com/watch?v=bVKNSf1p1d0

Community | GNS3. (n.d.). https://gns3.com/community/featured/after-gns3-upgrade-2-0-1-i-am-ge

Contribuidores da Wikipédia. (2023, October 1). OPNsense. https://pt.wikipedia.org/wiki/OPNsense

Donenfeld, J. A. (n.d.). WireGuard: fast, modern, secure VPN tunnel. https://www.wireguard.com/

Getting Started with GNS3 | GNS3 Documentation. (n.d.). https://docs.gns3.com/docs/

GNS3 Linux Install | GNS3 Documentation. (n.d.). https://docs.gns3.com/docs/getting-started/installation/linux/

IPFire.org - IPFire Development Team. (n.d.). Welcome to IPFire Documentation - the IPFire Documentation. IPFire Documentation. https://www.ipfire.org/docs

IT System Admin. (2020, December 2). How to Setup MikroTik RouterOS in GNS3 [Video]. YouTube. https://www.youtube.com/watch?v=IbRrk2wwE2U

Krishna's TechInfo. (2021, February 6). How to Block websites and Monitor user logs in IP Fire Firewall [Video]. YouTube. https://www.youtube.com/watch?v=TNaXRQCYE2o

MikroTik. (2017, June 19). Basic guidelines on RouterOS configuration and debugging [Video]. YouTube. https://www.youtube.com/watch?v=SGoX5Tu80vQ

MikroTik. (2017, June 19). Features and usage examples of wAP device [Video]. YouTube. https://www.youtube.com/watch?v=_gUp6OarSyo

MikroTik. (2022, August 22). MikroTips: serial console [Video]. YouTube. https://www.youtube.com/watch?v=LcM7Ds0p_pA

MikroTik. (2022, December 8). MikroTik Hairpin NAT [Video]. YouTube. https://www.youtube.com/watch?v=1I5FywY6opQ

MikroTik. (2022, January 11). MikroTips: How to firewall [Video]. YouTube. https://www.youtube.com/watch?v=hMj80ZIVBQs

MikroTik. (2022, June 29). Routing basics with MikroTik [Video]. YouTube. https://www.youtube.com/watch?v=ZpAY_6RDuRA

MikroTik. (2022, May 9). How to port forward on MikroTik [Video]. YouTube. https://www.youtube.com/watch?v=a_8AV6vIDYQ

MikroTik. (2022, May 10). Which MikroTik wireless package to use? [Video]. YouTube. https://www.youtube.com/watch?v=EYORYehRwG0

MikroTik. (2022, May 11). How to connect to a MikroTik device [Video]. YouTube. https://www.youtube.com/watch?v=13NvZY7sRlY

MikroTik. (2022, May 16). When not to use QuickSet in MikroTik devices [Video]. YouTube. https://www.youtube.com/watch?v=hQgGzgPOFFY

MikroTik. (2022, November 7). SSH RSA key for your router [Video]. YouTube. https://www.youtube.com/watch?v=8tt7fSvdFRM

MikroTik. (2022, November 29). Let's Encrypt - free & easy TLS certificates [Video]. YouTube. https://www.youtube.com/watch?v=T1Dyg4_caa4

MikroTik. (2023, December 8). What's with all the WiFi packages? [Video]. YouTube. https://www.youtube.com/watch?v=AkBIQxi-VKs

MikroTik. (2023, December 19). Network Address Translation - NAT secrets they didn't teach you [Video]. YouTube. https://www.youtube.com/watch?v=vt819u0QEtg

MikroTik. (2023, January 5). RouterOS CLI features everyone should know [Video]. YouTube. https://www.youtube.com/watch?v=fSt1UrNcx08

MikroTik. (2023, January 20). Install GNS3 on Linux and learn MikroTik networking [Video]. YouTube. https://www.youtube.com/watch?v=tBswpi22q_0

MikroTik. (2023, March 28). Cybercriminal reveals how to hack with MikroTik [Video]. YouTube. https://www.youtube.com/watch?v=_2fqev6NhTY

MikroTik. (2023, November 16). Your first DHCP configuration [Video]. YouTube. https://www.youtube.com/watch?v=kF4b_t6W5fM

MikroTik. (2024, February 14). Port-forwarding in RouterOS [Video]. YouTube. https://www.youtube.com/watch?v=LEjg54S_C0M

MikroTik. (2024, January 17). Dynamic NAT in RouterOS [Video]. YouTube. https://www.youtube.com/watch?v=vIiWSmvjmeE

MikroTik. (2024, January 26). Static NAT in RouterOS [Video]. YouTube. https://www.youtube.com/watch?v=rZh_OePiH0c

Module 2 – Setting up the Organization - NetBox Labs. (2023, October 5). NetBox Labs. https://netboxlabs.com/zero-to-hero/2-setting-up-the-organization/

Netbox Tutorial (Jeremy Cioara). (2022). [Video]. Youtube. https://www.youtube.com/playlist?list=PLGmJrV5excOzNzObe4dkyh9OKBbyIYEW4

NETVN82. (2024, February 12). How to create a WireGuard VPN server on OPNsense Firewall [Video]. YouTube. https://www.youtube.com/watch?v=EBvsmbiNCT8

Nerdy Tech. (2020, April 4). How To Set Up IPFire step by step [Video]. YouTube. https://www.youtube.com/watch?v=4OCqxfUb32M

OPNsense® a true open source security platform and more - OPNsense® is a true open source firewall and more. (2024, January 30). OPNsense® Is a True Open Source Firewall and More. https://opnsense.org/

Rules — OPNsense documentation. (n.d.). https://docs.opnsense.org/manual/firewall.html

SC Tech Academy. (2020, April 2). How to install and configure IPFire [Video]. YouTube. https://www.youtube.com/watch?v=I6MVHhMdEPQ

Surfer. (n.d.). Step by step guide developing a netbox plugin - Fixes.co.za. https://fixes.co.za/network-automation/netbox-plugin-step-by-step-guide/

Viatto. (2021b, November 11). The core of everything your first Netbox site [Video]. YouTube. https://www.youtube.com/watch?v=Ic_tuGBF4lQ

Viatto. (2021b, November 16). Netbox Site Region tenant design Examples [Video]. YouTube. https://www.youtube.com/watch?v=WugtkeMqYaA

Viatto. (2021, November 11). The core of everything your first Netbox site [Video]. YouTube. https://www.youtube.com/watch?v=Ic_tuGBF4lQ

Viatto. (2021, December 28). Netbox Cabling [Video]. YouTube. https://www.youtube.com/watch?v=b-H-tSlZmZA

Viatto. (2022, January 18). Netbox IPAM RIR and aggregates [Video]. YouTube. https://www.youtube.com/watch?v=bhZxMoAVqWw

ZacsTech. (2022, November 13). How to install GNS3 on Ubuntu 22.04 | 20.04 [Video]. YouTube. https://www.youtube.com/watch?v=PBdHzJOi1Tc

Zero to Hero - NetBox Labs. (2023, October 31). NetBox Labs. https://netboxlabs.com/zero-to-hero/