|  |  |
| --- | --- |
| Innovatief netwerk is snel en dichtbij | Veerman ICT  Plan van aanpak  Netwerk technologie | Ties Tienhoven en Chiem Stevens  14-03-2021 |

Inhoud

[Achtergronden & Aanleiding 2](#_Toc66626386)

[Opdrachtomschrijving / probleemstelling 3](#_Toc66626387)

[Projectresultaat 5](#_Toc66626388)

[Ontwerp  6](#_Toc66626389)

[Gateway 7](#_Toc66626390)

[Operating system: Ubuntu server LTS 20.04 7](#_Toc66626391)

[DHCP server: DNSMasq 7](#_Toc66626392)

[DNS: DNSMasq 7](#_Toc66626393)

[TFTP: DNSMasq 7](#_Toc66626394)

[PXE: DNSMasq 8](#_Toc66626395)

[NFS: nfs-kernel-server 8](#_Toc66626396)

[Firewall: NFTables 8](#_Toc66626397)

[NAT: NFTables 8](#_Toc66626398)

[TSLR 8](#_Toc66626399)

[Operating system: Ubuntu server LTS 20.04 8](#_Toc66626400)

[Host-apd 8](#_Toc66626401)

[Firewall: NFTables 8](#_Toc66626402)

[NAT: NFTables 8](#_Toc66626403)

[Operating system 9](#_Toc66626404)

[Inrichten firewalls 9](#_Toc66626405)

[Security 10](#_Toc66626406)

[Projectactiviteiten 12](#_Toc66626407)

[Kwaliteit borging 14](#_Toc66626408)

[Planning 0](#_Toc66626409)

[Risico’s 0](#_Toc66626410)

[Bibliografie 1](#_Toc66626411)

# Achtergronden & Aanleiding

Voor het vak netwerktechnologie dient er een nieuw netwerk gebouwd te worden. Het SENDLAB netwerk wordt gemaakt om de competenties voor het vak netwerktechnologie te toetsen en het beste netwerk wordt ook daadwerkelijk in het SENDLAB geïmplementeerd.

Computers zonder netwerken zijn vandaag de dag bijna niet meer voor te stellen. Tijdens deze periode wordt er dieper ingegaan in de wereld van netwerken. In periode 2.1 is dit deels al gedaan, deze kennis dient hergebruikt te worden bij het maken van het netwerk.

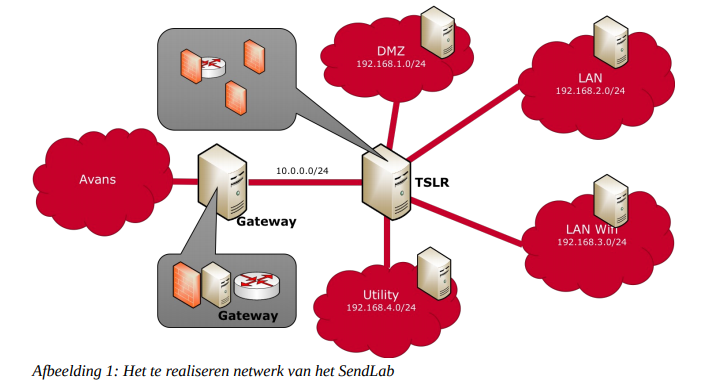
Tijdens de hoorcolleges wordt er uitleg gegeven over het project en wordt de kennis opgefrist van voorgaande periodes.

Ook cybersecurity gaat een steeds grotere rol spelen. Er wordt tegenwoordig met alle mogelijke soorten aanvallen rekening gehouden. Binnen deze module wordt er dieper ingegaan op cyber security en hoe dat toegepast kan worden in een netwerk.

Na vier weken van onderzoek is het vervolgens tijd om het netwerk te bouwen.

# Opdrachtomschrijving/ probleemstelling

De opdracht is een netwerk te realiseren waarvan de architectuur deels is gegeven. Het ontwerp van dit netwerk is te zien in figuur 1.



Het netwerk is onderverdeeld in drie sub netwerken: DMZ, LAN/ Wifi en Utility. Deze netwerken worden opgezet vanuit de TSLR (Thin Server Linux Router). De DMZ staat voor demilitarized zone, dit is een sub netwerk dat zich tussen het internet en het privé netwerk bevindt. Het voegt een extra beveiligingslaag toe om de gevoelige gegevens die op interne netwerken zijn opgeslagen te beschermen door firewalls te gebruiken om verkeer te filteren. Het LAN/WiFi netwerk is bedoeld voor apparaten zoals telefoons en laptops die draadloos met het netwerk willen verbinden. Het Utility netwerk is bedoeld voor alle hosts waarmee devices in het LAN/WiFi netwerk beheerd kunnen worden. Het Utility netwerk is alleen vanaf het internet/ Avans netwerk bereikbaar via de DMZ.

Het netwerk bevat is ingericht volgens secure-by-design principes. Zo bevindt er een DMZ tussen het internet en het SENDLAB netwerk, dit voegt een extra beveiligingslaag toe. Ook worden apparaten op het LAN/ WiFi netwerk beheerd vanaf het Utility netwerk. Hierdoor is het niet mogelijk voor een gebruiker van het WiFi om andere apparaten op het netwerk in te zien. Doordat er een gateway is geplaats tussen de TSLR en het internet is het ook niet mogelijk om de TSLR vanaf buiten het Avans netwerk te benaderen.

De probleemstelling luidt: Er dient een netwerk gerealiseerd te worden dat veilig is en het verkeer adequaat routeert en de benodigde diensten levert. Vanuit deze probleemstelling is de volgende hoofdvraag geformuleerd: **Hoe kan er een netwerk gerealiseerd worden dat veilig is en de benodigde diensten levert terwijl het verkeer adequaat gerouteerd wordt.** De doelstellingen die na het project behaald willen worden zijn:

* Een gateway die verbonden is met het thuis/ Avans netwerk.
* De TSLR verbindt met de gateway en kan diskless opstarten
* Internet op sub-netwerken verloopt via de gateway.
* Secure-by-design aspecten zijn toegepast in het netwerk.
* Firewall regels zijn geïmplementeerd.

De deelvragen die bij deze doelstellingen horen:

* Hoe wordt een raspberry pi verbonden met het internet?
* Hoe werkt de communicatie tussen twee raspberry pi’s via een ethernet kabel?
* Hoe start een raspberry pi op zonder opslag, via het netwerk?
* Wat is er nodig om een internet connectie te verkrijgen op de TSLR.
* Welke secure-by-design aspecten zijn er te vinden in het netwerk?
* Welke firewall regels dienen er te worden opgesteld.

# Projectresultaat

Aan het eind van het project is er een nieuw netwerk gerealiseerd voor het SENDLAB. Het netwerk bestaat uit twee raspberry pi’s (de gateway en de TSLR) die verbonden zijn met een ethernet kabel. De gateway zorgt voor de verbinding tussen het SENDLAB netwerk en het Avans netwerk. De TSLR is een raspberry pi waar verschillende sub netwerken op draaien. Het is mogelijk om met een telefoon/ laptop te verbinden met het SENDLAB (LAN/ WIFI) netwerk, ook kunnen andere apparaten verbinden met het Utility sub netwerk.

Om aan te tonen wat het netwerk wel en niet moet kunnen doen is er gekozen om een MoSCoW lijst op te stellen.

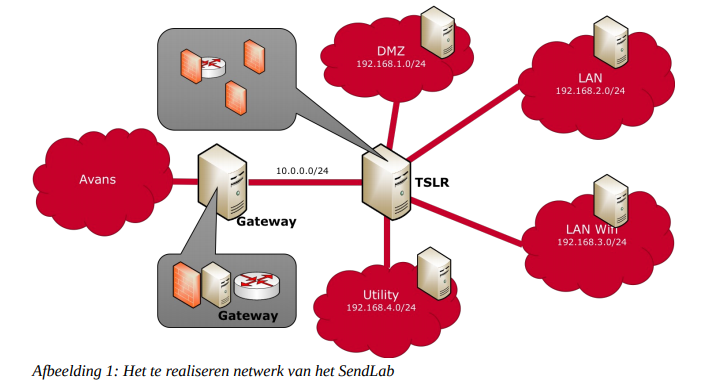
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Naam | Must | Should | Could | Won’t |
| Het netwerk wordt gemaakt met twee raspberry pi’s | X |  |  |  |
| Gateway |  |  |  |  |
| Netwerk bevat een gateway. | X |  |  |  |
| Gateway routeert inkomend internetverkeer naar SENDLAB netwerk. | X |  |  |  |
| Gateway opereert als DNS server om Tl’s te gebruiken in SENDLAB netwerk. | X |  |  |  |
| Gateway opereert als DHCP server om ip adressen uit te delen aan de rest van het SENDLAB netwerk. | X |  |  |  |
| Gateway maakt gebruik van een firewall regels om niet toegestaan internet verkeer te blokkeren. | X |  |  |  |
| De gateway maakt gebruik van NAT om het SENDLAB netwerk toegang te geven tot het internet. | X |  |  |  |
| TSLR |  |  |  |  |
| Netwerk bevat een TSLR (Thin server Linux router) | X |  |  |  |
| TSLR bevat geen opslag (diskless). | X |  |  |  |
| TSLR moet kunnen opstarten via het netwerk (gateway). | X |  |  |  |
| De TSLR realiseert een DWZ. | X |  |  |  |
| De TSLR realiseert een LAN Wifi. | X |  |  |  |
| De TSLR realiseert een Utility subnet | X |  |  |  |
| Het netwerk bevat een intrusion detection system (IDS) |  | X |  |  |

# Ontwerp

Voor het vernieuwde SENDLAB netwerk wat opgezet gaat worden in dit project is een ontwerp gemaakt. Een deel van dit ontwerp was al gegeven in de vorm van de netwerkarchitectuur voor het SENDLAB netwerk, deze is onder het kopje architectuur overzicht te zien.

**Architectuur overzicht**

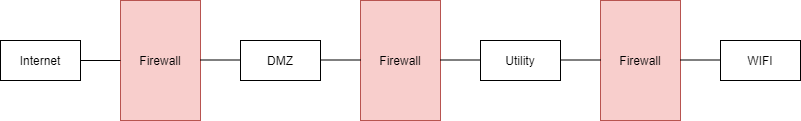
Hieronder is de architectuur te zien die is ontworpen voor het SENDLAB netwerk.



In dit figuur zijn verschillende netwerk node’s te zien, deze worden hier verder toegelicht.

* Gateway: De gateway van dit netwerk zorgt voor verbinding tussen het Avans netwerk/thuisnetwerk en het SENDLAB netwerk. Hiernaast maakt de gateway het mogelijk om de TSLR diskless op te kunnen starten.
* TSLR: De Thin Server Linux Router gaat in dit netwerk het mogelijk maken om de verschillende subnet’s op te zetten. Deze subnet’s zijn de DMZ, LAN/LAN Wifi en Utility. Deze TSLR moet volledig diskless kunnen opereren.

Als netwerk met verkeer ziet dit er als volgt uit:

**

Figuur 1: Het internetverkeer over het SENDLAB netwerk:

Hierin is te zien dat al het internetverkeer dat het SENDLAB netwerk binnenkomt via het internet via een firewall naar de DMZ gaat, waarna het via een firewall naar het Utility netwerk waarna het tot slot via een firewall naar het WIFI netwerk gaat.

Voor het realiseren van dit netwerk worden de Gateway en TSLR geïmplementeerd met raspberry pi’s (RPi 3b+). De Gateway gaat via de onboard wifi (wlan0) verbonden zijn met het Avans netwerk/thuisnetwerk en via het vaste ethernet interface(eth0) met een lan kabel verbonden zijn aan de TSLR.

De lan kabel vanuit de gateway komt bij de TSLR binnen op het ingebouwde ethernet interface (eth0). Hiernaast zijn er op de TSLR twee usb-netwerkinterfaces aangesloten voor de subnets. Dit zijn de DMZ (op eth1) en Utility (op eth2). Als laatste draait er op de onboard wifi (wlan0) het subnet voor LAN Wifi.

## Gateway

### Operating system: Ubuntu server LTS 20.04

Als operating system voor de gateway wordt gebruik gemaakt van Ubuntu LTS 20.04.

### DHCP server: DNSMasq

De verschillende apparaten in het netwerk moeten communiceren met elkaar, die hebben IP-adressen nodig. Deze IP-adressen worden uitgedeeld door de DHCP server. De DHCP server gaat IP-adressen uitdelen aan apparaten in het netwerk. Een apparaat stuurt een DHCP broadcast bericht, die door de DHCP server wordt opgevangen en erop reageert.

Om IP-adressen uit de delen moet een DHCP-range ingesteld worden, hiermee wordt bepaald hoeveel IP-adressen er uitgedeeld kunnen worden aan het netwerk. Er is gekozen om 20 IP-adressen uit te delen om het netwerk niet te veel te belasten.

De DNSMasq  server heeft een IP-adres nodig. Ook moet tijdens het instellen het IP-adres van de router worden toegevoegd aan de settings van DNSMasq. De DNS en DHCP services moeten toe worden gevoegd aan de firewall, anders is er geen connectie tot DNSMasq mogelijk.

### DNS: DNSMasq

DNS wordt gebruikt om ip adressen te koppelen aan hostnamen. Dit wordt gebruikt om apparaten te bereiken via een hostnaam, maar ook om domeinnamen zoals google.com te vertalen naar ip adressen. De nameserver 8.8.8.8 wordt gebruikt om domeinnamen van het internet te koppelen aan IP-adressen, er dient een eigen nameserver aangemaakt te worden om zelf apparaten te koppelen aan hostnamen. Deze nameserver heeft hetzelfde ip als de gateway. Poort 53 dient open te staan om DNS verkeer toe te staan.

### TFTP: DNSMasq

TFTP (Trivial File Transfer Protocol) is een protocol dat gebruikt kan worden via DNSMasq. Het maakt het mogelijk om een bestand te delen met een extern apparaat, dit wordt gebruikt om de TSLR op te starten via de gateway. Poort 69 wordt gebruikt voor TFTP.

### PXE: DNSMasq

PXE (Preboot Execution Environment) is een ander protocol dat geïnstalleerd wordt via DNSMasq. PXE wordt in combinatie met TFTP en NFS gebruikt om de TSLR op afstand op te starten.

### NFS: nfs-kernel-server

NFS (Network File System) wordt gebruikt om bestanden/ mappen te delen met andere apparaten over het netwerk. Hiervoor wordt nfs-kernel-server gebruikt, deze service wordt aangeleverd door Ubuntu.

### Firewall: NFTables

Op de gateway moet een firewall worden geïmplementeerd die het netwerkverkeer filtert wat het SENDLAB netwerk in wil en alleen maar de pakketten toelaat die naar het DMZ sub netwerk gaan.

### NAT: NFTables

NAT wordt gebruikt om verschillende privé ip adressen van apparaten te koppelen aan het publieke ip adres van de router zodat niet alle publieke ip adressen opraken. Dit moet toegepast worden in het SENDLAB netwerk om de verschillende sub netwerken van het SENDLAB te koppelen aan het internet. Hiervoor moet op de Gateway het privé adres van de TSLR gekoppeld worden aan het publieke adres van de Gateway.

## TSLR

### Operating system: Ubuntu server LTS 20.04

Als operating system voor de gateway wordt gebruik gemaakt van Ubuntu LTS 20.04.

### Host-apd

Deze service wordt op de TSLR gebruikt om een WiFi hotspot aan te maken. Dit wordt gebruikt om apparaten zoals telefoons en laptops te laten verbinden met het lan/wifi netwerk. Als alleen host-apd geconfigureerd wordt zonder een DHCP server krijgt het apparaat geen IP-adres. Om dit werkend te krijgen zal er dus een verbinding moeten zijn tussen de TSLR en de DHCP server op de gateway.

### Firewall: NFTables

Op de TSLR moeten firewall regels toegevoegd worden om alleen het internetverkeer tussen de DMZ en het Utility sub netwerk en tussen het Utility en WIFI sub netwerk toe te laten.

### NAT: NFTables

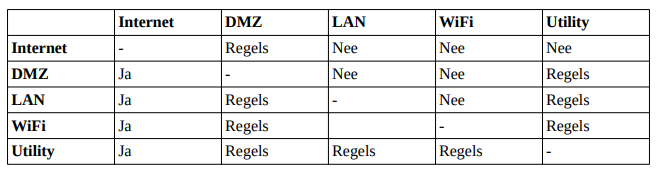
Op de TSLR moeten de verschillende ip adressen van de sub netwerken gekoppeld worden aan het ip adres van de TSLR die op de Gateway getransleerd wordt met het publieke adres van de gateway.

## Operating system

Voor het operating system wordt er gebruik gemaakt van Ubuntu server LTS (long term support) 20.04. Hier is voor dit gekozen omdat het goed samenwerkt met de raspberry pi, ook is er een grote community die Ubuntu server gebruikt, waardoor er veel online hulp beschikbaar is. Uit het vooronderzoek is ook gebleken dat veel Linux services die gebruikt gaan worden voor dit netwerk, beschikbaar zijn voor Ubuntu server LTS. Tot slot is er voor versie 20.04 gekozen omdat dit de nieuwste versie is van Ubuntu server en minimaal tot 2025 ondersteund wordt.

## Inrichten firewalls

Er wordt voor het assessment gestreefd om de firewalls in te richten volgens de volgende regels. Mocht dit niet lukken dient in ieder geval een deel van deze regels geïmplementeerd te zijn.



Figuur 2: Firewall regels

# Security

In week 4 is er een securityriskassesment uitgevoerd volgens de bow-tie methode. Het resultaat hiervan is te zien in afbeelding 2. Er zijn verschillende aanvalsvectoren genoemd, deze staan hieronder nog een keer beschreven.

* Inbraak via draadloze toegang

Een van de aanvalsvectoren die tegen het netwerk gebruikt kan worden is de draadloze toegang via het netwerk, hierbij is het in bezit krijgen van het Wi-Fi wachtwoord al voldoende. Als het mogelijk moet zijn om in te loggen via een admin panel kan dit problemen opleveren. Daarom hebben wij ervoor gekozen om dit niet mogelijk te maken! Er moet met een draad verbonden worden tot een van de Pi’s.

* Malware infectie

Een besmetting met malware zou grote gevolgen kunnen hebben voor het netwerk, tot zover dat het netwerk ook niet meer werkt. Om hier een reactie op te hebben zullen er om de tijd back-ups gemaakt moeten worden van het systeem.

* DDoS

Als het netwerk slachtoffer wordt van een DDoS aanval is dit erg vervelend en is het netwerk tijdelijk niet bereikbaar. Om dit te voorkomen wordt er goed gekeken naar welke firewall poorten er open worden gezet, om het aanvallers niet te makkelijk te maken.

* Toegang tot hardware

Dit is een van de vervelendste dingen die kan gebeuren. Als iemand met kwade bedoelingen bij het fysieke netwerk komt is het een kwestie van een kabel uit de Pi’s halen om het netwerk offline te halen. Ook kan deze persoon dan toegang krijgen tot de pi’s en bekijken wat er op het netwerk gebeurt. Daarom wordt er een wachtwoord ingesteld om toegang te krijgen tot de Pi’s. Ook wordt er sterk aangeraden om het netwerk op te bergen achter een gesloten deur, zodat niet iedereen toegang heeft tot de Pi’s.

* Man in the middle

Bij een man in the middle aanval heeft een persoon toegang gekregen tot het netwerk en kunnen berichten worden uitgelezen. Om dit te voorkomen worden berichten die tussen het netwerk verstuurd worden versleuteld. Berichten kunnen daardoor niet worden uitgelezen.

Ubuntu server wordt gebruikt als operating system voor de raspberry pi’s. Voor software is er gekozen voor Suricata, een IDS (intrusion detection system) dat de Pi’s moet beveiligen tegen niet toegestane verbindingen.

De volgende veiligheidsmaatregelen worden gebruikt om het netwerk te beveiligen.

* IDS

Een IDS wordt gebruikt om indringers op het netwerk te herkennen. Een IDS houdt het netwerkverkeer in de gaten en is op zoek naar verdachte activiteit op het netwerk.

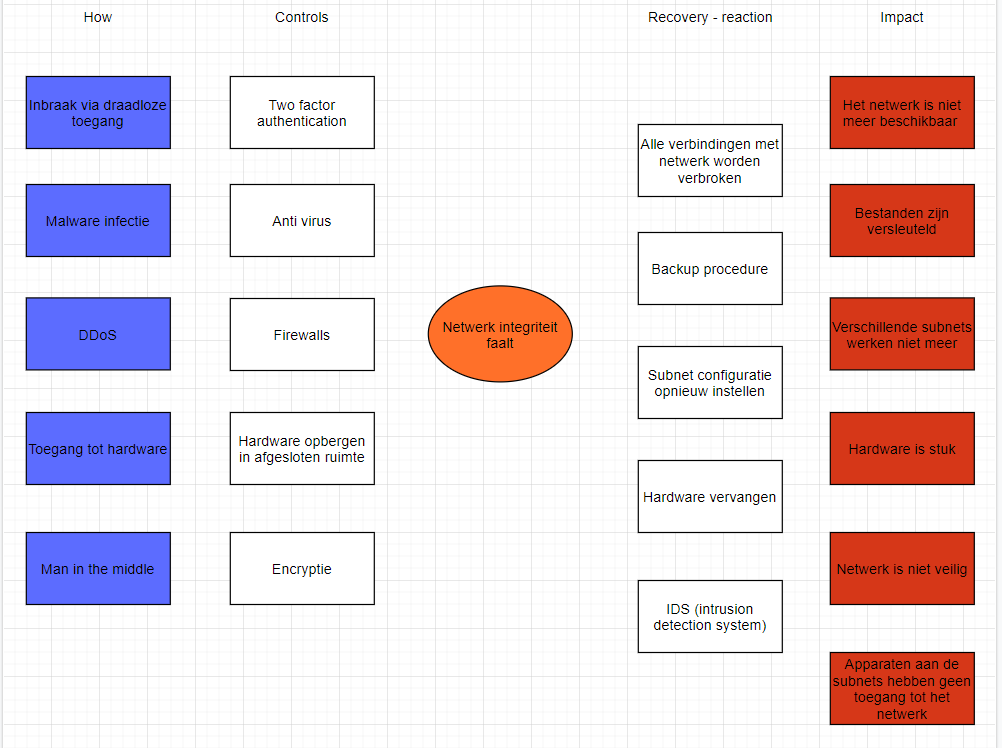
* Firewalls

Firewalls worden gebruikt om netwerk toe te staan, maar ook om netwerkverkeer uit te sluiten. Er wordt gebruik gemaakt van NFTables.

* Authenticatie

De Pi’s zijn voorzien van een wachtwoord waardoor niet iedereen zomaar toegang heeft als er een USB aansluiting wordt gebruikt in de Pi’s. Bij het aansluiten van een USB kan dit gedetecteerd worden en naar een aparte server gelogd worden, echter is dit geen maatregel om niet toegestane authenticatie tegen te gaan.

Alle bovenstaande veiligheidsmaatregelen worden geïmplementeerd.



Figuur 3: Bow-tie methode uitgewerkt

# Projectactiviteiten

Dit hoofdstuk beschrijft de projectactiviteiten die worden uitgevoerd tijdens het project.

* 1. Security riskassesment

In week 4 van de huidige periode wordt er onderzoek gedaan naar de security risico’s van het netwerk. De resultaten van dit onderzoek worden opgenomen in het plan van aanpak.

* 1. Pi’s installeren met Ubuntu server

Wanneer het plan van aanpak wordt goedgekeurd kan er begonnen worden met het bouwen van het netwerk. Als eerste activiteit staat het installeren van Ubuntu server op de raspberry pi’s.

* 1. Pi’s koppelen en communicatie tussen Pi’s werkend maken

Wanneer beide Pi’s voorzien zijn van een operating system worden deze aan elkaar gekoppeld om communicatie tussen deze twee apparaten werkend te krijgen zal er ook wat configuratie plaats moeten vinden

* 1. Opzetten DHCP server (DNSMasq) op gateway

De eerste service die geïnstalleerd wordt op de gateway is DNSMasq. Deze service wordt ook gebruikt voor andere protocollen, het is daarom een logische eerste stap.

* 1. Opzetten DNS (DNSMasq) op gateway

Na het opzetten van de DHCP server wordt ook de DNS opgezet. Dit zal ongeveer tegelijk gebeuren omdat deze twee protocollen gebruik maken van dezelfde service.

* 1. Opzetten NAT op gateway

Het opzetten van het NAT wordt gebruikt om domein namen te koppelen aan ip adressen.

* 1. Opzetten NFS op gateway

NFS wordt gebruikt om bestanden te delen met de TSLR. Als dit werkt kan er begonnen worden aan PXE.

* 1. Opzetten PXE op gateway

PXE wordt gebruikt voor het netwerk booten van de TSLR. Hier kan ook nog wat configuratie van de TSLR bij komen kijken. Als er veel moet worden opgezet op de TSLR kan deze activiteit ook op een later moment gedaan worden.

* 1. Opzetten NAT op TSLR

Voor de TSLR kan wordt er begonnen met het opzetten van het NAT. Dit zal op dezelfde wijzen gebeuren als op de gateway.

* 1. Opzetten host-apd op TSLR

Voor het opzetten van WIFI wordt host-apd gebruikt.

* 1. Opzetten NFTables op TSLR

De firewall regels worden hier opgezet voor de TSLR.

* 1. Opzetten NFTables regels op gateway

De firewall regels worden hier opgezet voor de gateway.

* 1. Voorbereiden assessment

Om tijdens het assessment een goede demo te geven dient er het een en ander getest worden.

* 1. Assessment

Tijdens het assessment wordt het netwerk beoordeelt en hebben examinatoren de mogelijkheid tot het stellen van vragen.

# Kwaliteit borging

Om de kwaliteit te borgen tijdens dit project worden er verschillende stappen ondernomen bij de verschillende fasen van het project.

Tijdens het onderzoeken en schrijven van het PVA worden de bronnen die zijn gebruikt voor het onderzoek opgenomen in het hoofdstuk bronvermelding. Hierdoor kan er makkelijk teruggezocht worden naar de informatie en makkelijk verwezen worden naar deze bronnen.

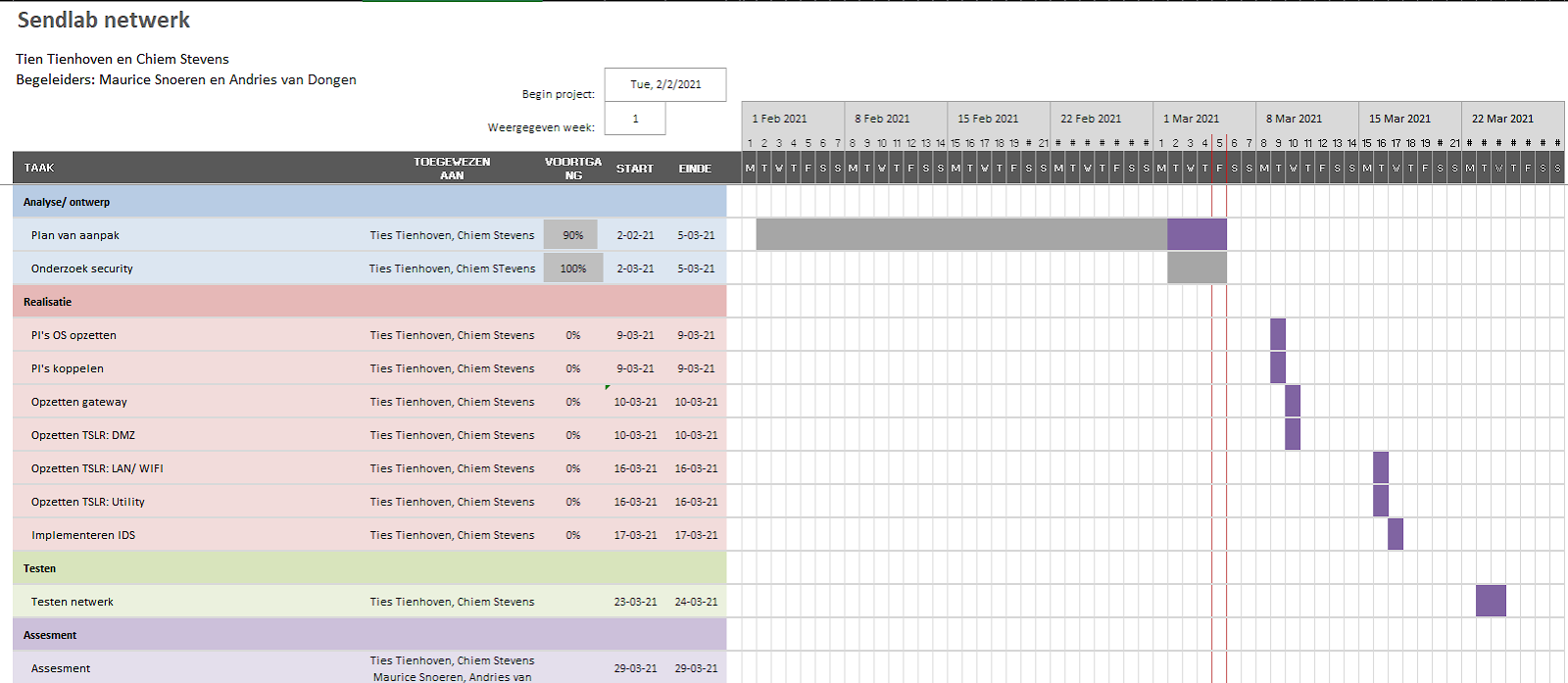
Tijdens het ontwikkelen aan het netwerk en de Pi’s houden we een document bij waarin wordt beschreven welke stappen zijn ondernomen om de verschillende services onder Linux in te stellen. Hierdoor kan er makkelijk terug gekeken worden naar welke stappen eerder zijn ondernomen.

Hiernaast wordt er tijdens de volledige ontwikkeling van dit project een lijst bijgehouden van vragen voor Maurice en Andries zodat er verzekerd kan worden dat alle vragen die ontstaan gesteld worden aan de begeleiders.

# Planning

Dit hoofdstuk beschrijft de planning die is gemaakt voor het uitvoeren van het project.

Er is gekozen om de planning te maken in Excel, hieronder is een schermafbeelding opgenomen om een beter beeld te geven van de planning.



Figuur 2: Planning uitgewerkt in Excel

# Risico’s

Dit hoofdstuk beschrijft de risico’s van het project. Het gaat hierbij om de risico’s die voor kunnen komen tijdens het maken van het project en niet zo zeer over de beveiliging van het project. Er wordt ook een cijfer gegeven aan de risico’s, dat cijfer wordt gerekend volgens kans x impact. Hoe hoger het risico cijfer, des te meer impact het heeft op de voortgang van het project.

* Falende hardware.

Het kan voorkomen dat tijdens het implementeer van het netwerk een van de raspberry pi’s kapot gaat. Ook kan een kabel het niet meer doen. Als dit gebeurt kan dit worden opgelost door nieuwe hardware op te halen op Avans.

Kans: 2 Impact: 3 Risico: 6

* Studenten niet ervaren met de verschillende Linux services waardoor mogelijk doel van dit project niet behaald kan worden.

Het bouwen van een netwerk is compleet nieuwe leerstof voor de projectgroep. Ook het werken met Linux is redelijk nieuw. Daarom kan het voorkomen dat het voor de projectgroep lastig om sommige dingen te realiseren. Als dit gebeurt wordt er contact gezocht met een begeleidend docent, waardoor de projectgroep hopelijk snel weer door kan met het project.

Kans: 3 Impact: 3 Risico: 9

* Verschillende gekozen Linux services werken mogelijk niet goed samen waardoor doel van dit project niet behaald kan worden.

Het kan voorkomen dat Linux services niet werken zoals de projectgroep van tevoren had bedacht. Hierdoor zou functionaliteit van het netwerk niet goed geïmplementeerd worden. Er moet in dit geval opnieuw onderzoek gedaan worden naar Linux services.

Kans: 1 Impact: 3 Risico: 3  

* Fouten in configuratie netwerk waardoor thuisnetwerk niet meer werkt.

Tijdens het configureren van de gateway kan er wat fout gaan met het uitdelen van IP-adressen. Als dit gebeurt kan het zijn dat het thuisnetwerk niet meer werkt. Dit lever wat vertraging op met het bouwen van het netwerk en het kan zijn dat een van de begeleidende docenten om advies wordt gevraagd om het netwerk te herstellen.

Kans: 1 Impact: 5 Risico: 5

# Bibliografie

DMZ. (n.d.). *linux demilitarized zone* . Retrieved from cyberciti: https://www.cyberciti.biz/faq/linux-demilitarized-zone-howto/

*dnsmasq conf*. (n.d.). Retrieved from docs oracle: https://docs.oracle.com/cd/E37670\_01/E41137/html/ol-dnsmasq-conf.html

*ids*. (n.d.). Retrieved from suricata: https://suricata-ids.org/docs/

*install and configure dnsmasq on ubuntu*. (n.d.). Retrieved from computingforgeeks: https://computingforgeeks.com/install-and-configure-dnsmasq-on-ubuntu-18-04-lts/

*quick reference nf tables*. (n.d.). Retrieved from wiki nftables: https://wiki.nftables.org/wiki-nftables/index.php/Quick\_reference-nftables\_in\_10\_minutes

*service nfs*. (n.d.). Retrieved from ubuntu: https://ubuntu.com/server/docs/service-nfs

Ubuntu. (n.d.). *how to install ubuntu on your rasberry pi*. Retrieved from ubuntu.com: https://ubuntu.com/tutorials/how-to-install-ubuntu-on-your-raspberry-pi#1-overview

wennyprastiwi98. (n.d.). *ids intrusion detection system with using snort in ubuntu*. Retrieved from medium.com: https://medium.com/@wennyprastiwi98/ids-intrusion-detection-system-with-using-snort-in-ubuntu-16-04-3a5862fed91f