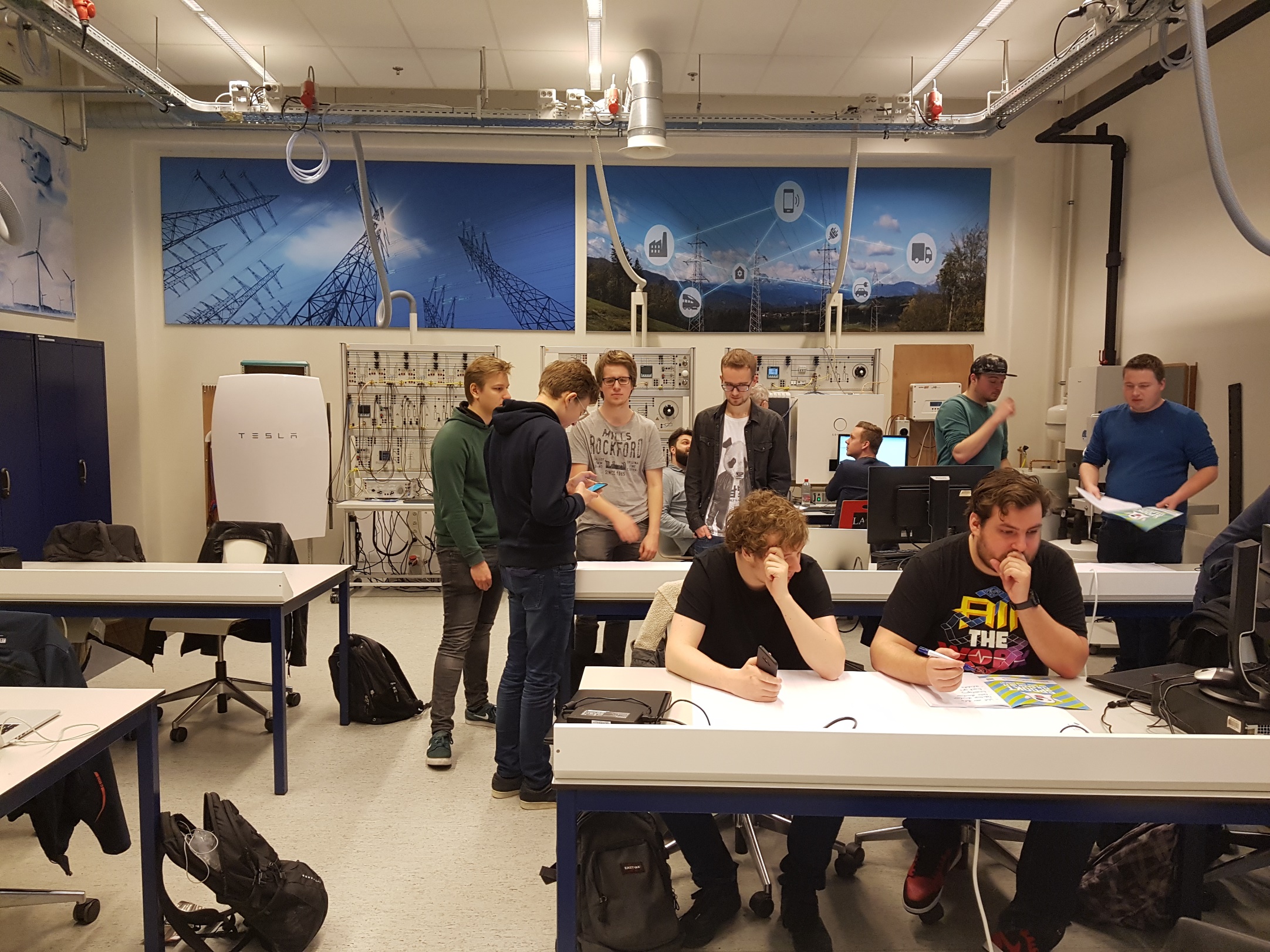
**Expertisecentrum Technische Innovatie**

Lectoraat Smart Energy



**DOCUMENTATIE**

**SENDLAB CLOUD**

**ICT Infrastructuur, database, API, meetpunten en visualisatie**

Technische Informatica

|  |  |  |
| --- | --- | --- |
| Datum | : |  |
| versie | : | 0.2 |
| status | : | Concept |
| docent(en) | : | Maurice Snoeren |

Versiegeschiedenis

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Omschrijving** | **Datum** | **Auteur** |
| 0.1 | Initiële versie van de documentatie. | 03-11-2019 | Maurice Snoeren |
| 0.2 | Afschakel en opstartprocedure toegevoegd. | 26-11-2020 | Maurice Snoeren |
|  |  |  |  |

Inhoudsopgave

[1 Inleiding 4](#_Toc57407564)

[2 SENDLAB Cloud 5](#_Toc57407565)

[2.1 Lectoraat Smart Energy 5](#_Toc57407566)

[2.2 Achtergrond 5](#_Toc57407567)

[2.3 Probleemstelling 5](#_Toc57407568)

[2.4 Wensen SENDLAB 6](#_Toc57407569)

[2.5 Doelstellingen 7](#_Toc57407570)

[2.6 Differentiatie planning 7](#_Toc57407571)

[2.7 De opdracht 7](#_Toc57407572)

[3 Hardware 9](#_Toc57407573)

[3.1 Opstelling serverrack 9](#_Toc57407574)

[3.2 Inschakelen en uitschakelen hardware 10](#_Toc57407575)

[4 Architectuur 11](#_Toc57407576)

[5 Netwerk 12](#_Toc57407577)

[5.1 Architectuur 12](#_Toc57407578)

[5.2 Praktische implementatie 13](#_Toc57407579)

[5.3 Firewall globale regels 13](#_Toc57407580)

[5.3.1 DMZ 13](#_Toc57407581)

[5.3.2 LAN 14](#_Toc57407582)

[5.3.3 WiFi 14](#_Toc57407583)

[5.3.4 Utility 14](#_Toc57407584)

[5.4 Realisatie 14](#_Toc57407585)

[5.4.1 Systeemontwerp 14](#_Toc57407586)

[5.4.2 Openstaande punten 14](#_Toc57407587)

[6 Internet toegang 16](#_Toc57407588)

[7 Systemen 17](#_Toc57407589)

[7.1 Virtuele omgeving 17](#_Toc57407590)

[7.1.1 SENDLAB CLOUD 17](#_Toc57407591)

[7.1.2 DMZ 17](#_Toc57407592)

[7.2 Server: gateway 18](#_Toc57407593)

[7.3 Server: router 18](#_Toc57407594)

[7.4 Server: jumphost 18](#_Toc57407595)

[7.4.1 Architectuur 18](#_Toc57407596)

[7.4.2 Cybersecurity implementatie 18](#_Toc57407597)

[7.4.3 Systeem details 19](#_Toc57407598)

[7.4.4 Installed software 19](#_Toc57407599)

[7.4.5 Users 19](#_Toc57407600)

[7.4.6 SSH Tunnels 19](#_Toc57407601)

[7.4.7 Startup 19](#_Toc57407602)

[7.5 Server: zonneboot 20](#_Toc57407603)

[7.5.1 Systeem details 20](#_Toc57407604)

[Verwijzingen 22](#_Toc57407605)

# Inleiding

Het SENDLAB naar een hoger plan! Binnen Avans Hogeschool doet het lectoraat Smart Energy, van het expertisecentrum Technische Innovatie, onderzoek naar de energietransitie. In deze transitie staat decentrale energieopwekking en duurzame opwekking centraal. Nederland heeft als doel gesteld, vastgelegd in de energieagenda, om in 2050 de energievoorziening een CO2 arme energievoorziening ingericht te hebben (Ministerie van Economische zaken, 2016). Om deze doelstelling te halen is het doel van de energietransitie om in 2030 de broeikasgassen met 49% te verlagen. De partijen die deze doelstelling moeten realiseren is de industrie, gebouwde omgeving, mobiliteit, landbouw en de energiesector (Bracht, 2019).

Fundamentele stappen zullen er gezet moeten worden om van fossiele brandstoffen naar duurzame bronnen te gaan. De vraag naar energie blijft bestaan en mogelijk groeien. Er komen nieuwe energiesystemen op verschillende niveaus: Woning, wijk, regio, nationaal en internationaal. Nieuwe spelers zullen zich gaan inmengen in de huidige energiemarkt. Om deze energievoorziening goed te regelen en op elkaar af te stemmen, is er tevens (real-time) communicatie tussen de componenten belangrijk. Kortom, het energiesysteem wordt veel complexer. Het is noodzakelijk dat we een betrouwbaar, veilig en betaalbaar energiesysteem behouden.

Er gaat veel veranderen en er is veel kennis nodig op het gebied van “het” nieuwe energiesysteem van de toekomst. Deze kennis en opleidingen bestaan vaak nog niet en zullen in de komende tijd gerealiseerd moeten worden. Om dit gelijktijdig te laten gaan, heeft Topsector energie ingezet op learning communities. Binnen deze communities gaan scholen (Universiteiten, Hogescholen en MBO’s) samen met het bedrijfsleven aan de slag met de huidige en toekomstige uitdagingen. In deze projecten wordt de kennis opgebouwd en levert dit meteen mensen op met de juiste kennis.

Het lectoraat Smart Energie geeft gehoor aan de uitdagingen van Nederland. Het onderzoek richt zich op energiebesparing en de inpassing van duurzame energie, waarbij het gebruik van technologische ontwikkelingen centraal staat. Er zijn drie onderzoekslijnen uiteengezet: Meten & weten, inpassen & koppelen en consuminderen & prosumeren (Doomernik, 2017). In 2018 is het SENDLAB opgericht om onderzoek te kunnen doen naar energiebesparing en inpassing van duurzame energie. Het doel is om het lokaal LA1.21 energieneutraal te maken en hierbij kennis op te doen dat relevant is voor de energietransitie. Begin 2019 is het lectoraat in de energy learning community (ELC) project gestapt om samen met Universiteiten en MBO’s samen te werken aan de uitdagingen van de energietransitie. Het SENDLAB speelt hierin een cruciale rol om de verschillende ideeën en experimenten verder te kunnen onderzoeken.

Technische Informatica heeft, in opdracht van het lectoraat voor het ELC project, het project opgepakt om de eerste stap te kunnen zetten voor het SENDLAB. In dit project wordt een ICT infrastructuur opgebouwd, een centrale database ingericht, API gerealiseerd, SENDLAB meetpunten geïmplementeerd en een eerste visualisatie van de opgeslagen data. Het project werd uitgevoerd door derdejaars studenten in periode 3.3 en 3.4 van de differentiatie Internet of Things (IoT) onder begeleiding van Diederich Kroeske en Maurice Snoeren.

De SENDLAB Cloud is gerealiseerd. Om deze installatie goed te kunnen beheren, is er een goede documentatie nodig. Dit document beschrijft de verschillende aspecten van de SENDLAB Cloud en dient als bijgehouden te worden bij wijzigingen.

# SENDLAB Cloud

De SENDLAB Cloud is een computer rack met computers, dat er voor zorgt dat de data van het lab en het lokaal worden opgeslagen.

## Lectoraat Smart Energy

Onze maatschappij wordt steeds afhankelijker van energie. De uitputting van fossiele energiebronnen dwingt ons te zoeken naar duurzame energievoorzieningen. Het lectoraat Smart Energy levert een bijdrage aan de ontwikkeling.

Elk onderzoek bij het lectoraat Smart Energy is gericht op energiebesparing en het inpassen van duurzame energie, met gebruikmaking van technologische ontwikkelingen. Onderzoek gebeurt via drie onderzoekslijnen:

1. Meten & Weten: geeft consumenten, bedrijven en overheden meer inzicht in hun energieverbruik, zodat zij de juiste beslissingen kunnen nemen over hun energiehuishouding.
2. Inpassen & Koppelen: decentrale duurzame energiebronnen met een niet-stuurbaar aanbodpatroon en conversie- en opslagsystemen in de energie-infrastructuur in en om het huis toepassen. Zowel in het distributienetwerk als in de industrie. Het doel is het verduurzamen van het energiesysteem.
3. Consuminderen & Prosumeren: gericht op de mogelijkheden om energiezuinig gedrag en gebruik van duurzame energie door consumenten, bedrijven en overheden te faciliteren met technische hulpmiddelen, met als doel de overgang naar een duurzame energiehuishouding te versnellen.

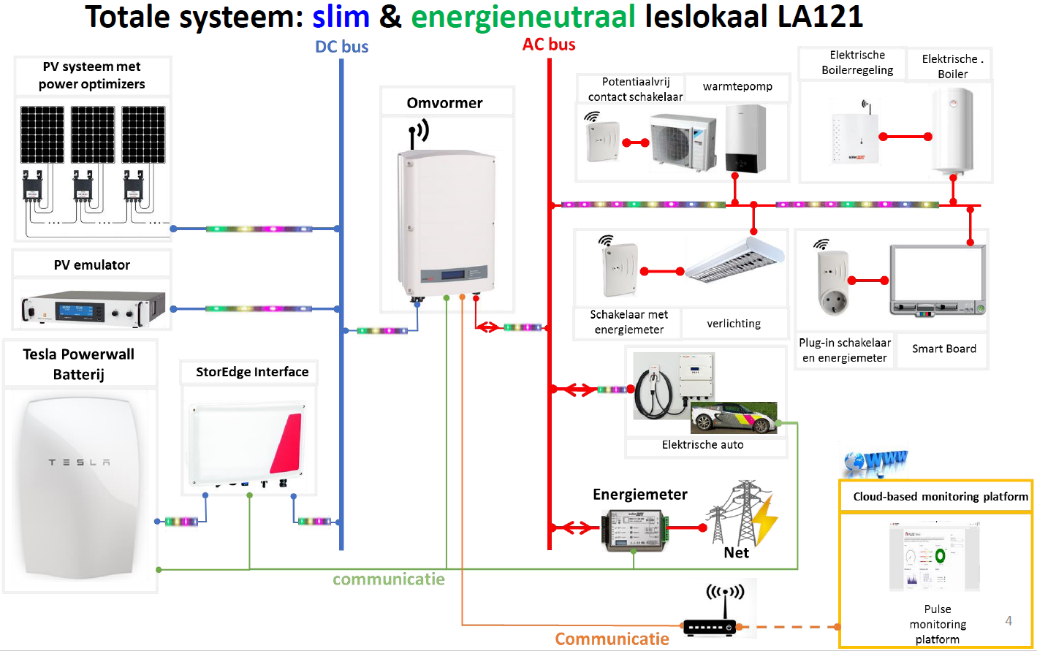
## Achtergrond

Op de Lovensdijkstraat 61, ruimte LA1.21, is het Smart Energy Delivery Lab (SENDLAB) gerealiseerd door de Opleiding Elektrotechniek van de Academie Engineering en ICT samen met het lectoraat Smart Energy. Dit lab heeft als doel enerzijds het onderwijs te faciliteren en anderzijds toegepast onderzoek met studenten en docenten te faciliteren op het gebied van energievraagstukken. Het SENDLAB zal dan ook een prominente rol vervullen binnen de huidige en toekomstige projecten van het lectoraat.

## Probleemstelling

Het SENDLAB is nog niet klaar! Op dit moment kunnen er al wel verschillende onderzoeken uitgevoerd worden. Hierbij kan mee denken aan het onderzoeken van de efficiëntie van zonnepanelen als functie van de instraling van de zon. Het simuleren van zonnepanelen om de effecten te bekijken van de energiehuishouding en regelingen die geïmplementeerd zijn in de energieomvormers en -opslag. Figuur 1 geeft de componenten van het SENDLAB weer, die voor het onderzoek ingezet kunnen worden. De belangrijkste componenten zijn:

* Zonnepanelen op het dak
* Omvormer (teruglevering naar het net)
* Energiestorage
* Energiemeters
* Warmtepomp
* Monitoringsysteem
* Tesla Powerwall batterij
* Elektrische auto (staat bij de hoofdingang van LA)



Figuur 1 Componenten SENDLAB leslokaal LA1.21

## Wensen SENDLAB

Het SENDLAB is net aangeschaft. De eerste projecten zijn vanuit Elektrotechniek uitgevoerd. Voor de korte termijn is het noodzakelijk om het SENDLAB op het niveau te krijgen waarbij onderzoeksprojecten goed het onderzoek kunnen uitvoeren in het SENDLAB. Dit betekent dat docenten en studenten het systeem op de volgende wijze kunnen gebruiken:

1. Onderzoeksvragen formuleren.
2. Verschillende testscenario’s definiëren.
3. Modeleren van een testscenario en de verschillende systemen correct instellen.
4. Opslaan van meetdata.
5. Uitvoeren van de verschillende testen.
6. Verkrijgen en visualisatie van meetdata.
7. Analyse uitvoeren op de verkregen data.
8. Conclusies opmaken.
9. Rapport opleveren conclusies experiment.

Op dit moment zijn de verschillende componenten niet met elkaar gekoppeld. Er is geen ICT netwerk aanwezig om dit op een goede en veilige manier te faciliteren. Daarnaast hebben de verschillende componenten verschillende manieren hoe de meetgegevens uitgelezen moeten worden. Om te zorgen dat de meetgegevens beschikbaar worden gemaakt, is het op korte termijn belangrijk om een database te realiseren. Voor ieder component is het belangrijk dat deze de data in de database schrijft. Later kunnen de onderzoekers deze data gebruiken binnen het onderzoek. Visualisatie kan helpen met het tussentijdse inzicht te verkrijgen wat er gebeurd tijdens het experiment. Visualisatie is dan ook een belangrijk aspect voor een stuk zichtbaarheid van het SENDLAB en ondersteuning tijdens de experimenten.

Het SENDLAB heeft de behoefte om zijn data adequaat op te slaan en de mogelijkheid deze data later te kunnen gebruiken in andere applicaties of onderzoeken. Binnen Avans Hogeschool is er een studententeam dat werkt aan de zonneboot. Dit team heeft dezelfde behoefte, namelijk het opslaan van meetgegevens van de zonneboot, deze real-time beschikbaar te maken en te visualiseren. In de toekomst mogelijk de races te optimaliseren op basis van de meetdata. Het project richt zich daarom op een centrale database dat via verschillende interfaces beschikbaar wordt gesteld. In de toekomst is de verwachting dat er meer meetdata en andere project dezelfde behoefte gaan krijgen. Met het oog op dataengineering is het voor Avans Hogeschool interessant om een dergelijke data-cloud te realiseren. Zodoende is voor het SENDLAB de volgende eerste stappen gedefinieerd:

1. Datalogging functionaliteit (alle SENDLAB componenten)
2. Visualisatie van de data (actueel en historisch)
3. Netwerk realiseren

## Doelstellingen

Met dit project zet het lectoraat de volgende stap met het SENDLAB. Hierbij is het doel om het lab verder volwassen te maken, zodat onderwijs en projecten uitgevoerd kunnen worden. De doelstellingen, van deze eerste stap voor het SENDLAB, zijn als volgt gedefinieerd:

* Centrale dataopslag van de metingen van het SENDLAB
* Centrale API (Application Programming Interface) voor het ophalen van data.
* Aansluiten van de meetpunten: Zonnepanelen, omvormer, energieopslag, energiemeters, warmtepomp, Tesla batterij, elektrische auto.
* Visualisatie van de data van de metingen van het SENDLAB
* Veilig netwerk en ontsluiting van de data.

## Differentiatie planning

Periode 2 (3 d/w)

Periode 1 (1 dag/week)

Figuur 2 Planning differentiatie Technische Informatica.

Zoals weergegeven in de figuur hierboven, start de differentiatie met theoretische vakken. Er is op dat moment één dag in de week beschikbaar voor het project. De focus ligt in die periode op de start van het project, het inlezen in de componenten van het SENDLAB en het ontwerpen van de verschillende onderdelen. In de tweede periode, hebben de studenten drie dagen in de week om aan het project te werken. De focus ligt dan op de realisatie van de verschillende onderdelen volgens het ontwerp. Daarnaast zullen er drie docenten meewerken één dan in de week aan deze projecten, om de studenten mee te helpen in de realisatie van de verschillende onderdelen.

## De opdracht

De studenten krijgen een vrije opdracht dat ze zelfstandig oppakken en onderzoeken. De studenten hebben de doelstellingen gekregen en het plan van aanpak van het SENDLAB (Snoeren, 2018). Daarbij een omgeving neer te zetten die zowel voor onderzoek als voor onderwijs ingezet kan worden. In de eerste weken hebben de studenten de opdracht geformuleerd, op basis van de gestelde doelstellingen, door een centrale onderzoeksvragen en deelvragen op te stellen.

Studenten hebben groepen gemaakt en onderwerpen gekozen, waarmee zij graag aan de slag wilden gaan. De volgende groepen zijn gerealiseerd:

1. API (Application Programming Interface)
2. Dataopslag
3. Warmtepomp
4. Lotus
5. Zonneboot
6. Visualisatie

Iedere studentengroep heeft de opdracht verder uitgewerkt en de onderzoeksvragen geformuleerd. Vervolgens hebben de studenten in de eerste periode (3.3) een analyse en ontwerp opgeleverd. De tweede periode (3.4) stond in het teken van de realisatie en testen. Hierbij hebben de studenten de opdracht gerealiseerd op basis van het gemaakte ontwerp.

# Hardware

In dit hoofdstuk gaan we in op de hardware die in het SENDLAB staat opgesteld. Het SENDLAB bevat een ICT infrastructuur dat bestaat uit netwerkapparatuur, servers en AI reken computers.

## Opstelling serverrack

In het SENDLAB staat een 19inch serverrack. De figuur hieronder geeft aan hoe deze geïnstalleerd is en op welke wijze het rack is ingedeeld. Het Avans netwerk wordt verbonden met de Gateway, die bovenin het rack zit. Vervolgens wordt een DMZ omgeving ingericht. Deze omgeving ontsluit de Utility en Cloud omgevingen. Vanuit de Utility omgeving wordt het lokale lab netwerk ontsloten. De inrichting is dan ook weergegeven in de fysieke installatie. Hierbij is de main switch geconfigureerd om alle onderliggende netwerken te ontsluiten.



Figuur 3 Opstelling serverrack.

## Inschakelen en uitschakelen hardware

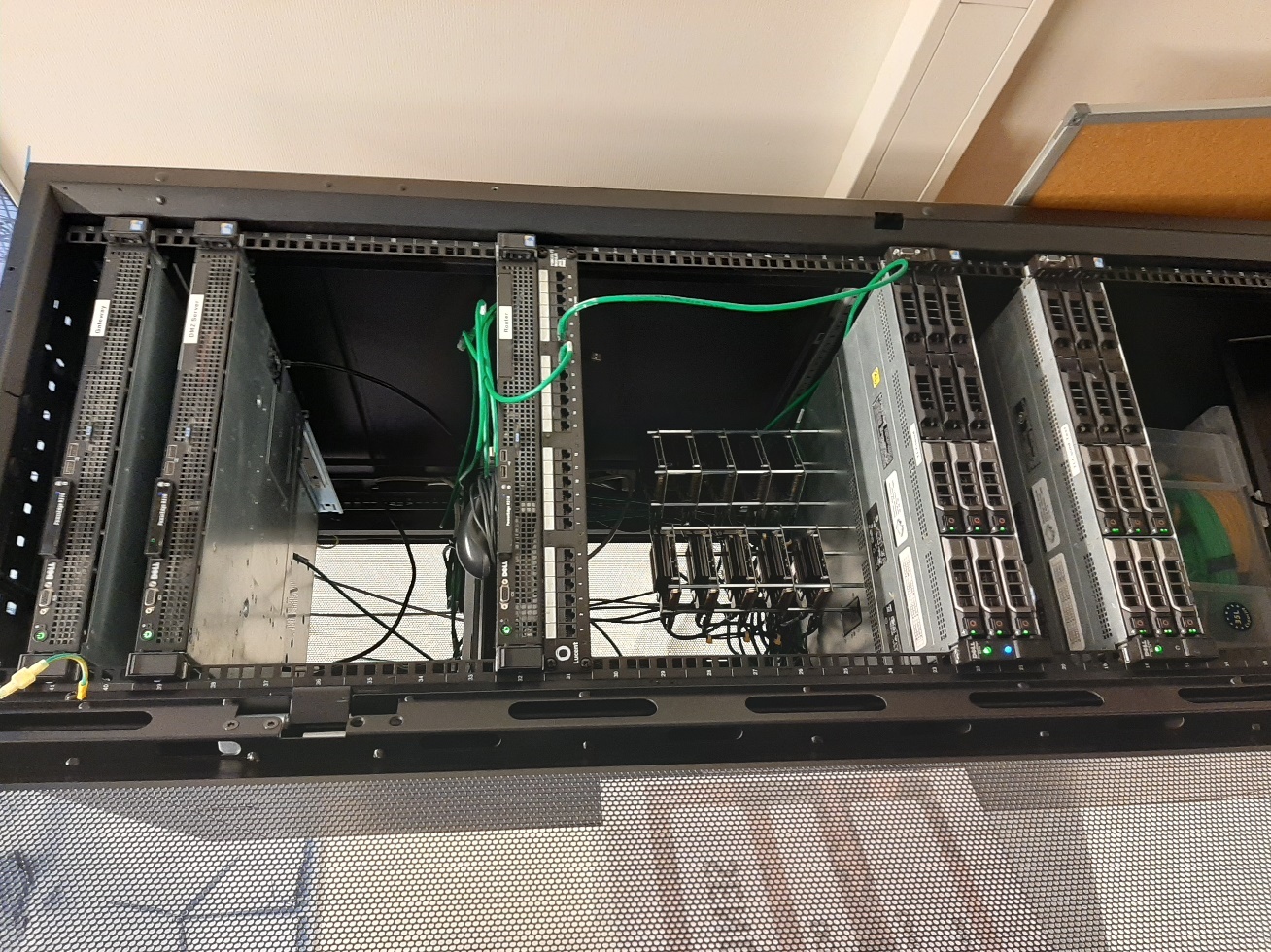
De procedure van het in- en uitschakelen is exact hetzelfde. Op het moment dat de servers uitgezet moeten worden, dient deze procedure gevolgd te worden. Zorg er altijd voor dat de contactpersoon op de hoogte is van deze gebeurtenis, zodat alle projecten en studenten op de hoogte gesteld kunnen worden.

**Uitschakelen:**

1. Stuur een Whats-app bericht aan de contactpersoon (staat op het serverrack)
2. Start bij de bovenste server en druk op de aan/uit-knop (groene lampje, zie blauwe pijl)
3. Druk op alle aan/uit-knoppen van de servers eronder van boven naar beneden
4. Wacht tot alle server zichzelf hebben uitgeschakeld
5. **Bel contactpersoon op wanneer de server niet stoppen en volg de instructies op**
6. Haal de spanning van het serverrack eraf.

**Inschakelen:**

1. Zet de spanning op het serverrack
2. Start bij de bovenste server en druk op de aan/uit-knop (groene lampje, zie blauwe pijl) – **het kan zijn dat een aantal servers automatisch starten**
3. Druk op alle aan/uit-knoppen van de servers eronder van boven naar beneden
4. Wacht tot alle server zichzelf hebben ingeschakeld
5. **Bel contactpersoon op wanneer niet alle servers aan schakelen**
6. Stuur een Whats-app bericht aan de contactpersoon (staat op het serverrack)



Figuur 4 Foto serverrack t.b.v. in- en uitschakel procedure.

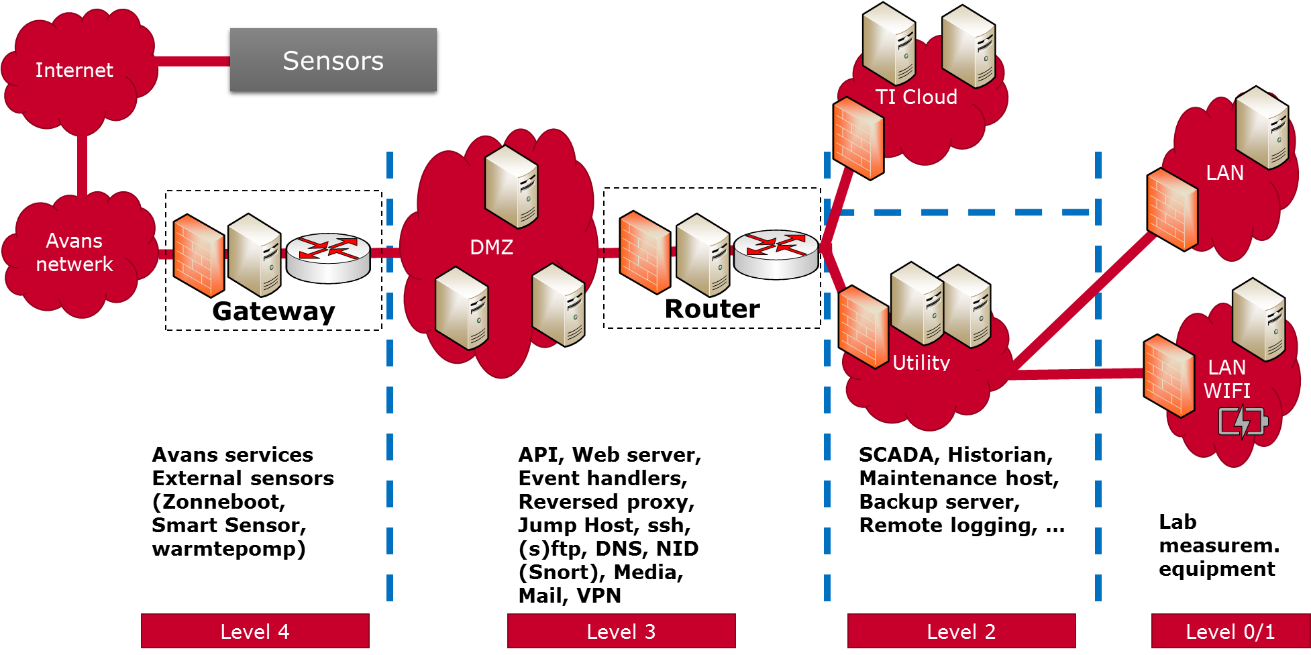
# Architectuur

# Netwerk en configuratie

Tijdens het project is tevens de ICT infrastructuur gerealiseerd. Dit netwerk is door Sam Nicknam en Thijs Wijnen opgezet naast hun eigen opdracht van de Lotus. Zij waren het winnende team dat tijdens de module Netwerktechnologie het beste ontwerp hadden gerealiseerd. Dit hoofdstuk beschrijft hoe het netwerk is opgezet.

## Architectuur

Omdat het lab gebaseerd is op een SCADA systeem, is het architectuurprincipe van automatiseringssystemen (SCADA) toegepast. De standaarden die deze architectuurprincipes beschrijven zijn de IEC62264 en IEC62443. Hierin wordt het gehele automatiseringslandschap meegenomen van actuatoren en sensoren tot het kantoornetwerk en het Internet. Figuur 8 toont het netwerkarchitectuur principe dat wordt gehanteerd voor het SENDLAB.



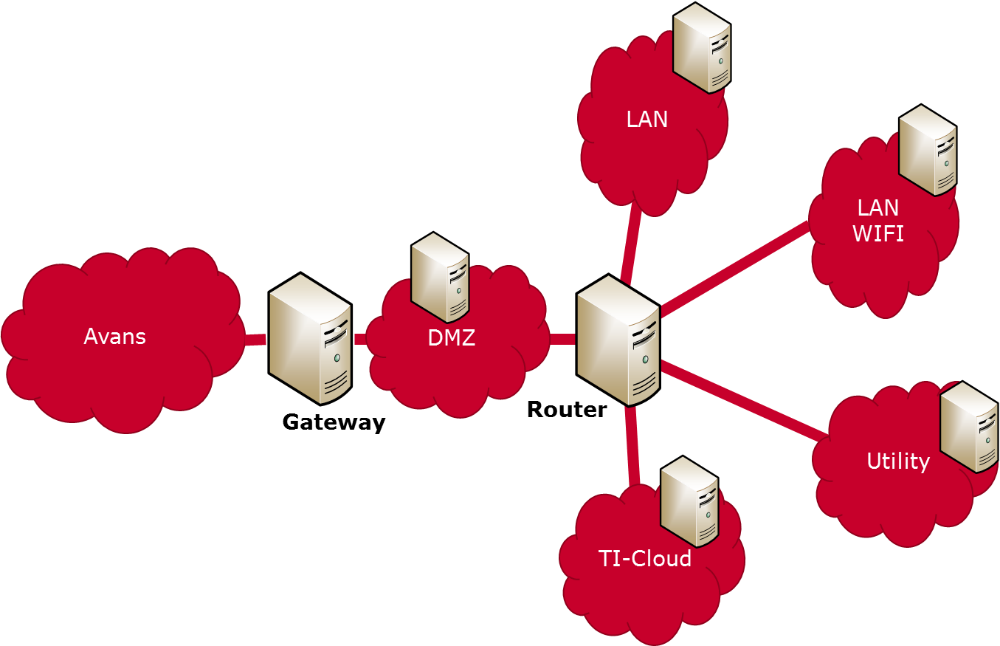
Figuur 5 SENDLAB netwerk architectuur.

Binnen IEC62264 worden er verschillende niveaus (levels) gedefinieerd. Ieder niveau bevat een bepaald type automatisering. Niveau 0 en 1 bevatten de actuatoren, sensoren en PLC’s die verantwoordelijk zijn voor de regelingen op het laagste niveau. In het geval van het SENDLAB zijn dit de sensoren van de proefopstelling. De warmtepomp valt hier ook onder. Echter is het mogelijk om vanuit het Internet ook sensoren aan te sluiten. Niveau 2 gaat over lokale regelingen die verschillende PLC’s aansturen. Vaak zijn dit SCADA systemen, die samen met een historische database, de gebruiker in staat stelt het hele systeem te monitoren en te besturen. In het SENDLAB is dat het SCADA system, waarmee de gebruiker de gehele opstelling kan regelen. Niveau 3 gaat nog een stap verder. In dit geval is dit de DMZ waarin verschillende diensten worden geleverd om de regelingen op laag niveau te kunnen ontsluiten. Voorbeelden hiervan zijn remote toegang, web servers of VPN aspecten. Het laatste niveau, niveau 4, is de buitenwereld. In dit geval is dat het Avans netwerk en uiteindelijk de internet toegang die het verschaft.

De TI-Cloud hebben we veilig geïntegreerd na de DMZ voor een goede ontsluiting van de TI Cloud naar het Internet. Deze cloud functioneert op zich zelf en staat los van de SCADA systemen.

## Praktische implementatie

Er zijn verschillende manieren waarop de architectuur gerealiseerd kan worden. Om de kosten te drukken, is er gekozen voor een twee-machine-ontwerp. Figuur 9 toont het werkelijke ontwerp. Hierin worden twee servers gebruikt die de firewalls en routering realiseren, zoals in de architectuur wordt aangegeven. De eerste server, gateway, is verantwoordelijk voor het inkomende en uitgaande verkeer naar het Internet/Avans. Deze implementeert de firewall en verzorgt het verkeer naar de DMZ. De andere server, router, is verantwoordelijk voor de realisatie van de verschillende onderliggende netwerken en hoe deze met elkaar kunnen en mogen communiceren. Eén belangrijke regel is dat er geen directe communicatie mag plaatsvinden van het Avans netwerk naar het LAN, LAN WIFI, Utility en TI Cloud. Dit dient ten alle tijden via de DMZ te gaan.



Figuur 6 Werkelijke implementatie van de architectuur.

## Firewall globale regels

De onderstaande tabel geeft weer of er verkeer tussen de verschillende systemen is toegestaan, gebaseerd moet zijn op regels of dat het niet toegestaan is. Over het algemeen geldt dat verkeer, over de verschillende netwerken heen, niet is toegestaan. Tussen de netwerken, die direct met elkaar verbonden zijn, is wel toegestaan.

Tabel 6 Firewall globaal ontwerp.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Internet** | **DMZ** | **TI Cloud** | **Utility** | **LAN** | **LAN WIFI** |
| **Internet** | - | Regels | Nee | Nee | Nee | Nee |
| **DMZ** | Ja/Regels | - | Regels | Regels | Nee | Nee |
| **TI Cloud** | Ja/Regels | Ja/Regels | - | Nee | Nee | Nee |
| **Utility** | Ja/Regels | Ja/Regels | Nee | - | Ja | Ja |
| **LAN** | Nee | Nee | Nee | Nee | - | Nee |
| **LAN WIFI** | Nee | NEe | Nee | Nee | Nee | - |

### DMZ

In de De-Militarized Zone (DMZ) staan servers die zowel vanaf Internet/Avans-netwerk als vanuit het interne netwerk (via een beperkt aantal poorten) benaderd moeten kunnen worden. In de DMZ bevindt zicht minimaal een webserver die dynamische webpagina’s kan genereren en een Intrusion Detection System (IDS) dat het complete netwerk bewaakt.

### LAN

In het LAN zijn in het SENDLAB alle devices aangesloten met een vaste netwerkinterface.

### WiFi

In het WiFi-netwerk zijn in het SENDLAB alle devices aangesloten met een wireless

netwerkinterface.

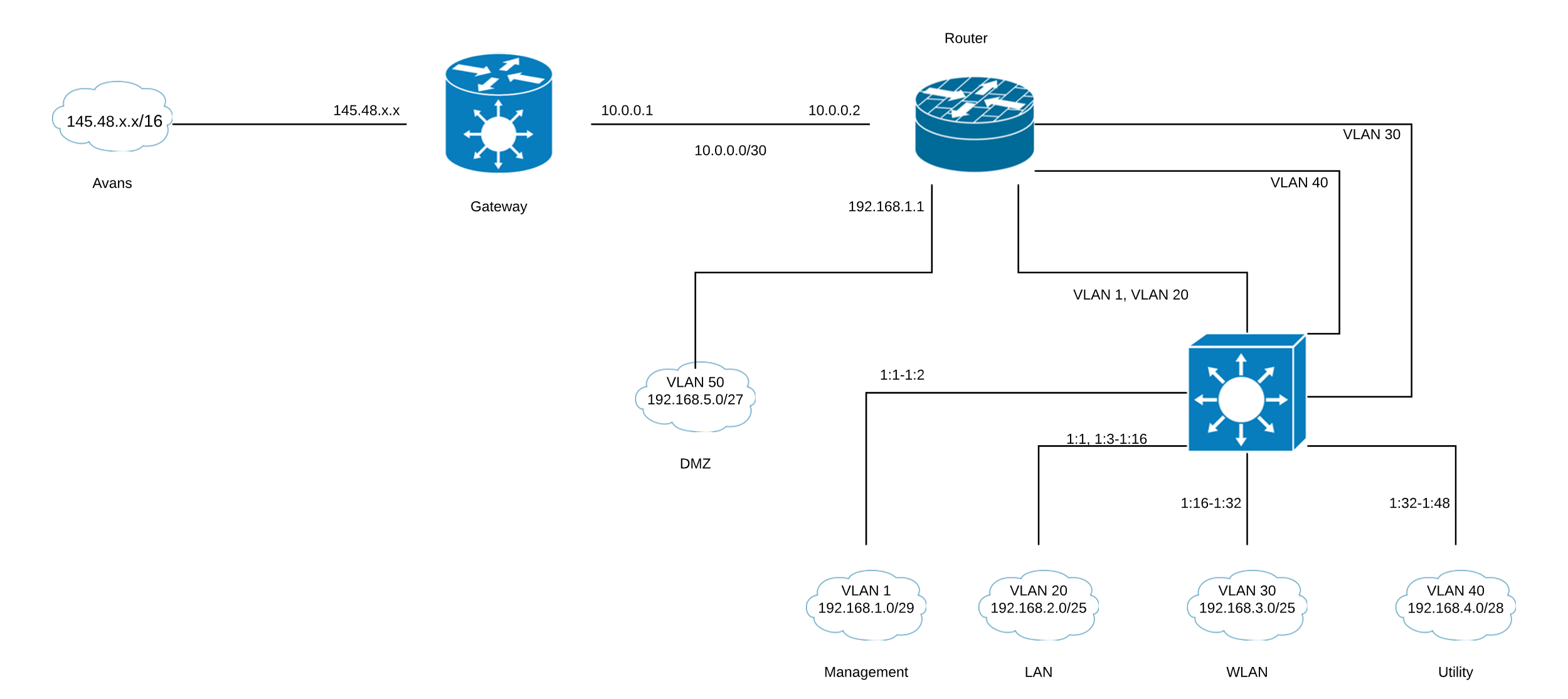
### Utility

In het Utility-netwerk zijn alle hosts opgenomen waarmee devices in het LAN en/of het WiFi-netwerk beheerd kunnen worden. Het Utility-netwerk is alleen vanaf het Internet/Avans-netwerk bereikbaar via de DMZ.

## Realisatie

In dit hoofdstuk wordt beschreven hoe het netwerk van het SENDLAB werkelijk is gerealiseerd. Dit kan afwijken van de architectuur.

### Systeemontwerp



Figuur 7 Netwerkontwerp SENDLAB.

In de bovenstaande figuur wordt weergegeven hoe het huidige netwerk van het SENDLAB is gerealiseerd met de verschillende componenten. Hierin is goed te zien dat het ontwerp gebaseerd is op twee servers, namelijk de gateway en de router. Er is een netwerkswitch toegepast om Virtual LAN’s (VLANs) te realiseren en uiteraard veel netwerkpoort ter beschikking te krijgen. De Router is verantwoordelijk voor de verschillende deelsystemen. In dit geval is de DMZ als een apart netwerk gerealiseerd. In de architectuur wordt het tussenliggende netwerk (in dit geval 10.0.0.0/30) niet als zodanig gebruikt.

Beide servers zijn geïnstalleerd met het Linux operating system pfSense. Deze distributie biedt de mogelijkheid om op een eenvoudige en veilige wijze een netwerk te realiseren met alle mogelijkheden die er zijn op het gebied van veiligheid.

### Openstaande punten

Het diagram is op dit moment de enige beschikbare documentatie van het netwerk. Het is niet gelukt om de poorten toe te voegen aan de DMZ VLAN op de Cisco DMZ switch. Wanneer dit gerealiseerd is, dient op de router ervoor gezorgd te worden dat de interface naar de DMZ, dat de twee VLANS (DMZ en Management) onderscheiden wordt en de juiste firewall-regels worden toegepast. In pfSense kan men bekijken welke firewall-regels zijn ingesteld.

# Internet toegang

Het SENDLAB Cloud dient vanaf het Internet beschikbaar te zijn. De systemen zijn diep weggestopt binnen het Avans netwerk. Om deze systemen beschikbaar te maken wordt op dit moment SSH port forwarding gebruikt vanaf de DMZ.

SSH Client : 192.168.0.12 ( Fedora 21 )

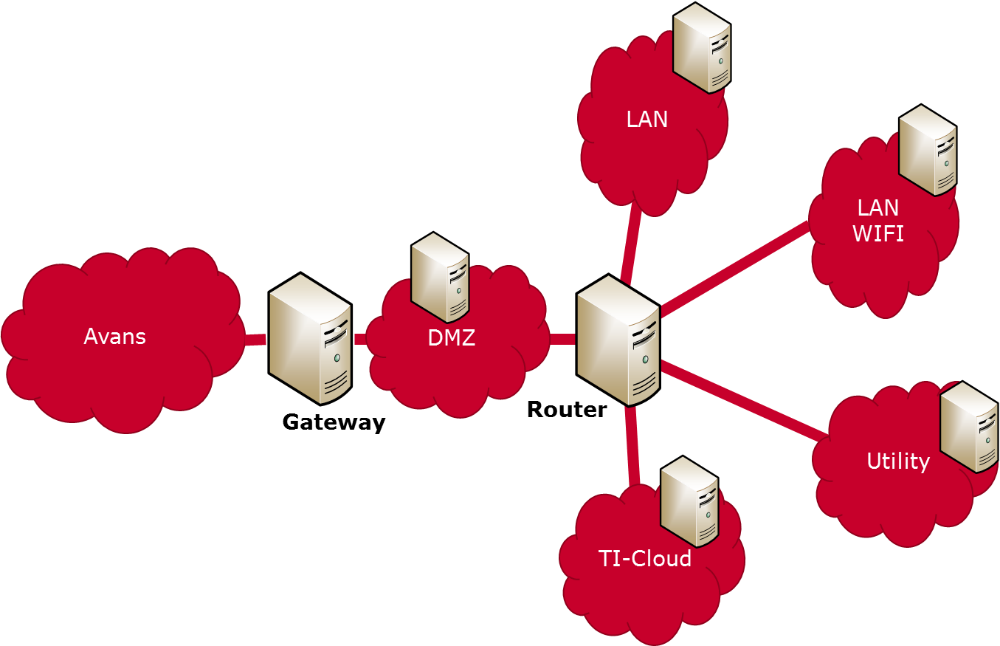
SSH Remote Host : 192.168.0.11 ( CentOS 7 )

Login into the SSH Client: ssh-keygen -t rsa

Create on remote host the .ssh directory with permissions 700

Copy the public key to the remote host:

cat .ssh/id\_rsa.pub | ssh sendlab-cloud@ti-live.avans.nl 'cat >> .ssh/authorized\_keys'



Op de DMZ:

#!/bin/sh

# Create a seperate tunnel for the SSH server, so if things needs to change we can leave this one alone!

autossh -M 0 -o ServerAliveInterval 30 -o ServerAliveCountMax 3 -f -N -T -R 10022:192.168.5.28:22 sendlab@ti-live.avans.nl

# Create a tunnel for the different applications!

# 1883 -> 11883 (MQTT), 443 -> 10443 (HTTPS)

autossh -M 0 -o ServerAliveInterval 30 -o ServerAliveCountMax 3 -f -N -T -R 11883:192.168.5.28:1883 -R 10443:192.168.5.28:443 sendlab@ti-live.avans.nl

# Systemen

## Virtuele omgeving

Een virtuele omgeving is handig voor verscheidende redenen. Ten eerste is het makkelijk nieuwe servers te realiseren. Voor studenten is dat handig om zelf aan de slag te kunnen met de server, zonder dat er vervelende dingen kunnen gebeuren. Daarnaast kunnen de servers eenvoudig geback-upt worden. Verder is het mogelijk een productie-omgeving te realiseren die alleen aangepast wordt op het moment dat alles goed is getest. Virtuele omgeving biedt een eenvoudige mogelijkheid om verschillende servers aan te maken voor verschillende onderdelen. Kortom, het biedt flexibiliteit, veiligheid, experimenteerbaarheid en robuustheid. Omdat VMWare omgevingen vrij prijzig zijn, is in dit geval gekozen voor een opensource oplossing Proxmox.

### SENDLAB CLOUD

De SENDLAB CLOUD bestaat uit een Proxmox cluster van twee nodes. De eerste node host de productie-servers en de tweede node de rest.

#### Node 1

Node 1 wordt gebruikt om productie-servers op te draaien. Servers die een belangrijke rol spelen, zullen continue aan moeten staan. Hierbij kunnen we denken aan het dataplatform dat real-time data verzameld van sensoren binnen Avans Hogeschool.

|  |  |
| --- | --- |
| Item | Value |
| OS | Proxmox ?? |
| MAC address |  |
| IP address |  |
| DNS | pm1.sendlab.avans.nl |

#### Node 2

Node 2 wordt gebruikt om niet-productie-servers op te draaien. Deze node kan ook worden gebruikt als back-up voor node 1. Op deze node zullen de studenten een server toegewezen krijgen voor het project om alles te kunnen doen wat er nodig is.

|  |  |
| --- | --- |
| Item | Value |
| OS | Proxmox ?? |
| MAC address |  |
| IP address |  |
| DNS | pm2.sendlab.avans.nl |

### DMZ

#### Node 1

In de DMZ is er op dit moment één node beschikbaar. Dit is een kleine server waarop verschillende kleine servers gedraaid kunnen worden. De DMZ verzorgd de veilige overgang tussen het Internet de cloud of de SENDLAB servers.

|  |  |
| --- | --- |
| Item | Value |
| OS | Proxmox ?? |
| MAC address |  |
| IP address |  |
| DNS | pm1.sendlab.avans.nl |

## Server: gateway

De gateway server is de ingang van de SENDLAB en verzorgt een belangrijke functie om te zorgen dat kwaadwillende geen toegang krijgen tot het SENDLAB CLOUD netwerk.

## Server: router

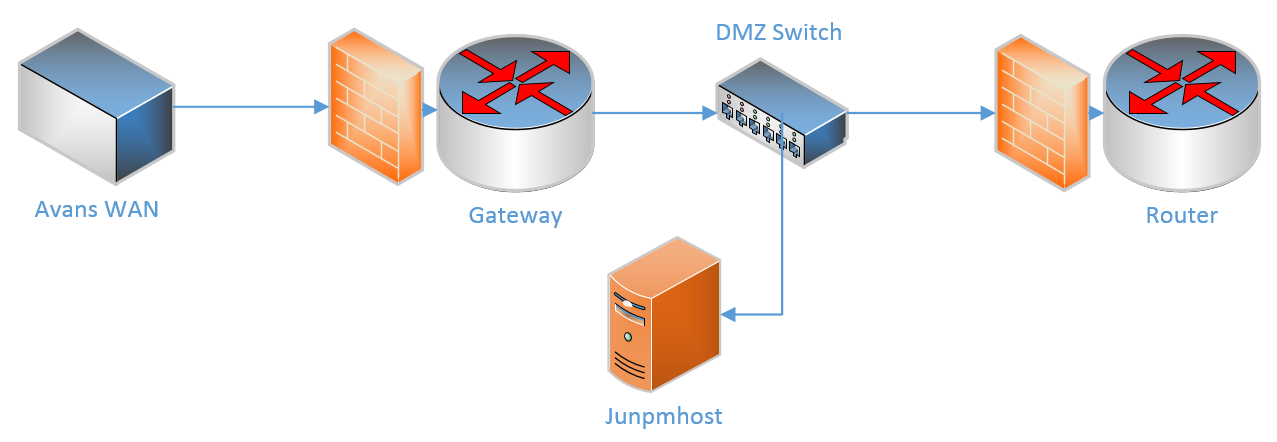
De router server zorgt voor de verschillende netwerken, scheiding van deze netwerken en de firewall tussen deze netwerken, binnen de SENDLAB CLOUD.

## Server: jumphost

Voor de veiligheid worden niet alle systemen met het Internet verbonden. Er zijn maar een aantal services die uiteindelijk vanuit het Internet bereikbaar zijn. Remote toegang tot het SENDLAB CLOUD is een grote aanvalsvector en dient heel goed ingeregeld te worden. Om de veiligheid te borgen, wordt gebruikt gemaakt van een “jumphost”. Deze server bevindt zich in de DMZ zone en kan vanuit het Internet benaderd worden. Remote toegang tot de systemen van het SENDLAB CLOUD verloopt via deze jumphost. Men logt in via SSH en kan van daaruit inloggen op de andere systemen.

### Architectuur

De jumphost bevindt zich in de DMZ zone. Vanuit het Internet bereikbaar. De jumphost mag bij de andere systemen aan de andere kant van de router.



Figuur 8 Architectuur jumphost.

### Cybersecurity implementatie

De jumphost is de server die als eerste aangevallen wordt van buitenaf. Dat betekent dat deze veilig geconfigureerd moet zijn. De volgende aspecten dienen te worden geïmplementeerd:

1. SSH hardening
2. Linux OS Hardening
3. Host based intrusion detection
4. Two-factor authentication
5. System monitoring
6. Automatic updates (cron)

### Systeem details

|  |  |
| --- | --- |
| Item | Value |
| OS | Linux Debian Buster 10.1 |
| MAC address | 46:14:25:e4:21:60 (ens18) |
| IP address | 192.168.5.22/24 |
| DNS | jumphost.sendlab.avans.nl |

### Installed software

|  |  |
| --- | --- |
| Software | Notes |
| Debian base system | Lean and small version of Debian buster. |
| SSH | Remote secure shell |
| iptables | Firewall software |
| OSSEC | Host based intrusion detection |

### Users

|  |  |  |
| --- | --- | --- |
| Full name | Username | Email |
| Maurice Snoeren | maurice | [mac.snoeren@avans.nl](mailto:mac.snoeren@avans.nl) |
| Diederich Kroeske | diederich | [dm.kroeske@avans.nl](mailto:dm.kroeske@avans.nl) |
| Michel Megens | michel | [mtm.megens@Student.avans.nl](mailto:mtm.megens@Student.avans.nl) |
| TI Live | ti-live | - |

### SSH Tunnels

De jumphost verzorgt op dit moment ook wat Internet tunnels, zodat men van buitenaf de jumphost kan bereiken. In dit geval realiseert de gebruiker ‘ti-live’ deze tunnels. De volgende tunnels worden vanuit de jumphost opgebouwd:

|  |  |
| --- | --- |
| Tunnel | Notes |
| Jumphost remote connection | autossh -p 12002 -fNT -R 10022:localhost:22 sendlab@vmacman.jmnl.nl |
| ETI servers | autossh -p 12002 -fNT -R 11883:192.168.5.29:1883 -R 11080:192.168.5.29:80 -R 11443:192.1685.29:443 [sendlab@vmacman.jmnl.nl](mailto:sendlab@vmacman.jmnl.nl) |
| Proxmox | autossh -p 12002 -fNT -R 8006:192.168.5.3:8006 -R 8007:192.168.5.4:8006 -R 8008:192.168.5.2:8006 sendlab@vmacman.jmnl.nl |

### Startup

#!/bin/sh

#/etc/init.d/tunnels

#

### BEGIN INIT INFO

# Provides: tunnels

# Required-Start: $remote\_fs $syslog

# Required-Stop: $remote\_fs $syslog

# Default-Start: 2 3 4 5

# Default-Stop:

# Short-Description: Creating the tunnels to get contact with SENDLAB CLOUD

### END INIT INFO

touch /var/lock/tunnels.lock

# Carry out specific functions when asked to by the system

case "$1" in

start)

echo "Starting script tunnels.sh "

/sbin/runuser ti-live -s /bin/bash -c "/home/ti-live/tunnels/tunnels.sh"

;;

stop)

echo "Stopping script tunnels.sh"

;;

\*)

echo "Usage: /etc/init.d/tunnels.sh {start|stop}"

exit 1

;;

esac

exit 0

## Server: zonneboot

Deze server is de ontwikkelserver voor de zonneboot. Studenten kunnen hierop experimenteren.

### Systeem details

|  |  |
| --- | --- |
| Item | Value |
| OS | Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-66-generic x86\_64) |
| MAC address | 86:61:18:62:f2:e1 (ens18) |
| IP address | 192.168.5.21/24 |
| DNS | zonneboot-dev.sendlab.avans.nl |

Kopieer dit script naar /etc/init.d/tunnels.

# Verwijzingen

Bracht, M. v. (2019). *Naar een Robuust Geïntegreerd energiesysteem (NRG).* Amersfoort: Topsector Energie.

Doomernik, J. (2017). *Lectorale reden: Empowerment, Regie over je eigen energie.* Breda: Avans Hogeschool.

Ministerie van Economische Zaken. (2016). *Energieagenda, Naar een CO₂-arme energievoorziening.* Den Haag: Ministerie van Economische Zaken. Opgehaald van Rijksoverheid.

Snoeren, M. (2018). *Plan van aanpak: Smart Energy Delivery Lab versie 0.3.* Breda: Avans Hogeschool, Technische Informatica.