NETWORK SECURITY
GotITech

Studenten: *Weyers Axel, Verbist Jef*
Studentennummer: s159667 , *s159845*
Opleidingsonderdeel: Network Security
Opleidingsinstelling: AP Hogeschool Antwerpen
Docent: Manderyck Isaac
Academiejaar: 2025–2026

1. GotITech

GotITech is een start-up. Aanvankelijk gebruikten ze ‘homemade’ servers die bij de oprichters thuis draaiden maar ze gebruiken nu steeds meer en meer gebruik van cloud applicaties en cloud storage. Ze hebben tal van systemen zoals laptops, servers en smartphones. Hier moet wel in het achterhoofd worden gehouden dat sommige van deze systemen outdated zijn.

Het bedrijf is ondertussen sterk afhankelijk geworden van cloudapplicaties en online meetings. Tot nu toe hadden ze geluk: er zijn nog geen grote cyberaanvallen geweest. Maar er is grote schrik voor ransomware, omdat zo’n aanval het bedrijf financieel waarschijnlijk niet zou overleven.

Huidige Situatie

- geen centrale beveiliging of firewall
- medewerkers zitten op onbeveiligde home-netwerken
- oude toestellen worden nog gebruikt → EOL = geen updates = kwetsbaar
- een paar zelfgemaakte “homelab” servers draaien bij oprichters thuis
- geen monitoring of logging
- grote angst voor ransomware

Visie:
GotITech wil binnen één jaar volledig migreren naar een professioneel cloudplatform en een future-proof beveiligingsarchitectuur invoeren.

Behoefte van het bedrijf

- alsof iedereen “lokaal” kan samenwerken
- veilig online meetings kunnen doen
- bescherming tegen ransomware
- binnen 12 maanden overstappen naar een veiligere infrastructuur
- eenvoudige oplossing (start-up, dus laag budget)

3. Analyse van de huidige kwetsbaarheden

3.1 EOL-systemen

Oude apparaten krijgen geen beveiligingsupdates meer dit verhoogt de kans op exploits.
Hierdoor kan een aanvaller binnen via gekende kwetsbaarheden.

3.2 Geen zero trust

Thuisnetwerken vertrouwen doorgaans alle apparaten impliciet. Daardoor bestaan er weinig interne beveiligingsmaatregelen of netwerksegmentatie. Wanneer één toestel via bijvoorbeeld phishing met ransomware wordt besmet, kan de malware zich hierdoor eenvoudig verspreiden naar andere apparaten in het netwerk. Op eenzelfde lijn kan een aanvaller door het gebrek aan netwerksegmentatie ook aan lateral movement doen (bv via een IOT apparaat binnengeraken en zo doorschuiven naar een apparaat met meer waardevolle gegevens).

3.3 Geen uniforme beveiliging

Iedereen gebruikt zijn eigen router, wifi en pc-configuratie.
Geen firewallregels, geen segmentatie, geen monitoring.

3.4 Homemade servers thuis

In een thuisomgeving met zelfgebouwde servers ontbreekt vaak de professionele hardening die in bedrijfsnetwerken standaard is. Er is doorgaans geen DMZ aanwezig om publieke diensten van interne systemen te scheiden en ook detectie mechanismen zoals IDS/IPS ontbreken. Hierdoor ontstaat een situatie waarin één succesvolle hack direct kan leiden tot een volledig datalek. Zodra een aanvaller één systeem weet te compromitteren, kan hij zich door het gebrek aan netwerksegmentatie ongehinderd lateraal door het hele netwerk bewegen. Dit vergroot de impact van een incident aanzienlijk, omdat alle verbonden systemen en gegevens in potentie bereikbaar worden voor de aanvaller.

3.5 Geen centrale authenticatie

Er is geen identiteitsbeheer. Iedere gebruiker logt in met eigen credentials, vaak zonder MFA. Hierdoor is credential theft extreem risicovol.

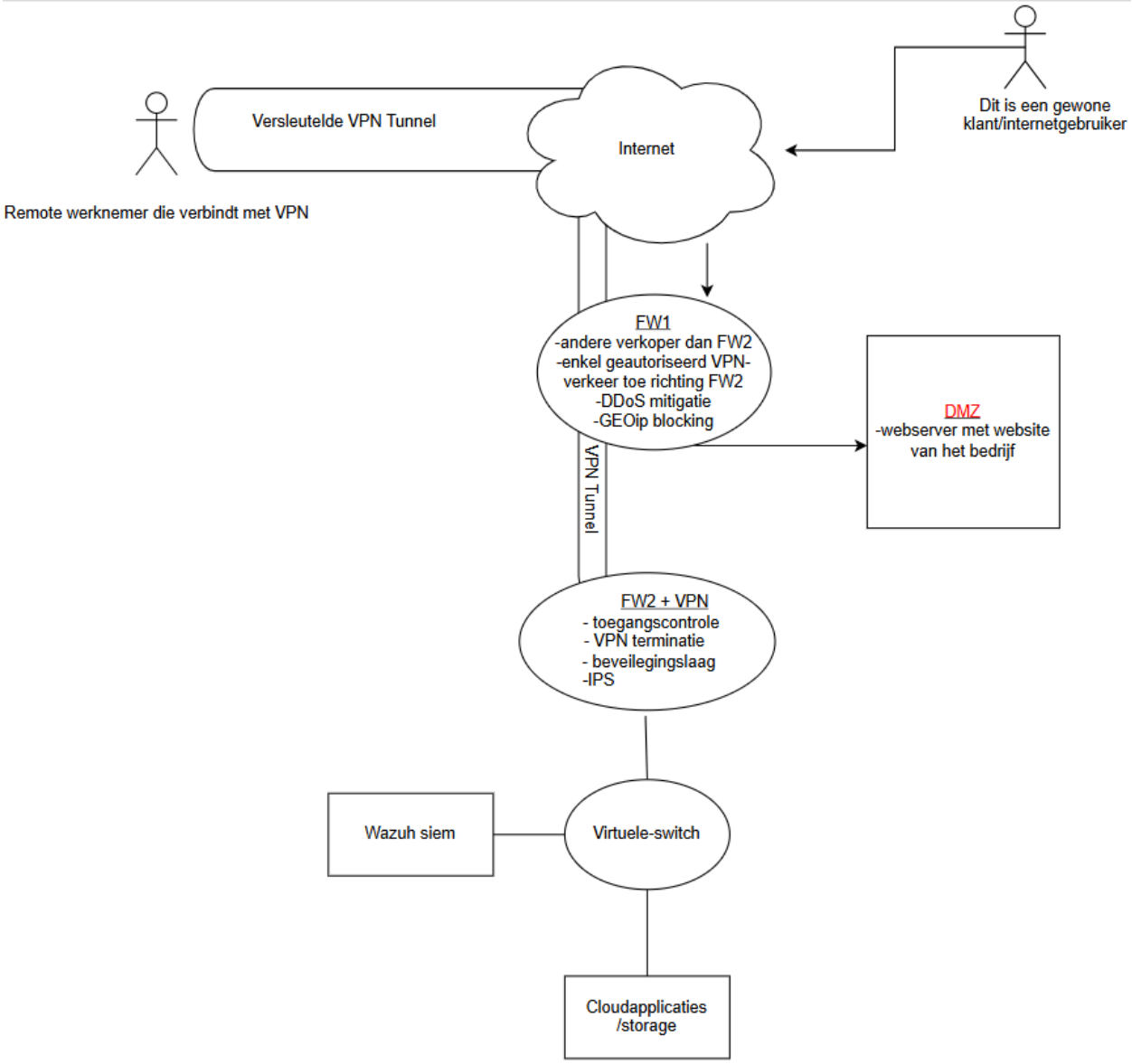
3.6 Kwetsbaarheden typisch voor remote start-ups

- phishing
- gestolen wachtwoorden
- social engineering
- cloud-misconfiguraties
- zwakke wifi
- ongepatchte apparaten
- risico op ransomware-verspreiding via thuisnetwerken

Doelstellingen van dit project

1. Een volledig nieuw netwerk ontwerpen dat ransomware voorkomt of sterk beperkt.
2. Veilige toegang tot bedrijfsdata en applicaties.
3. Segmentatie en isolatie toepassen zodat één besmet toestel niet het volledige netwerk verwoest.
4. Centrale firewall, IDS/IPS en SIEM in een gesimuleerd bedrijfsnetwerk.
5. Werken volgens Zero Trust-principes.
6. Een ontwerp dat eenvoudig is voor een start-up, maar toch professioneel.

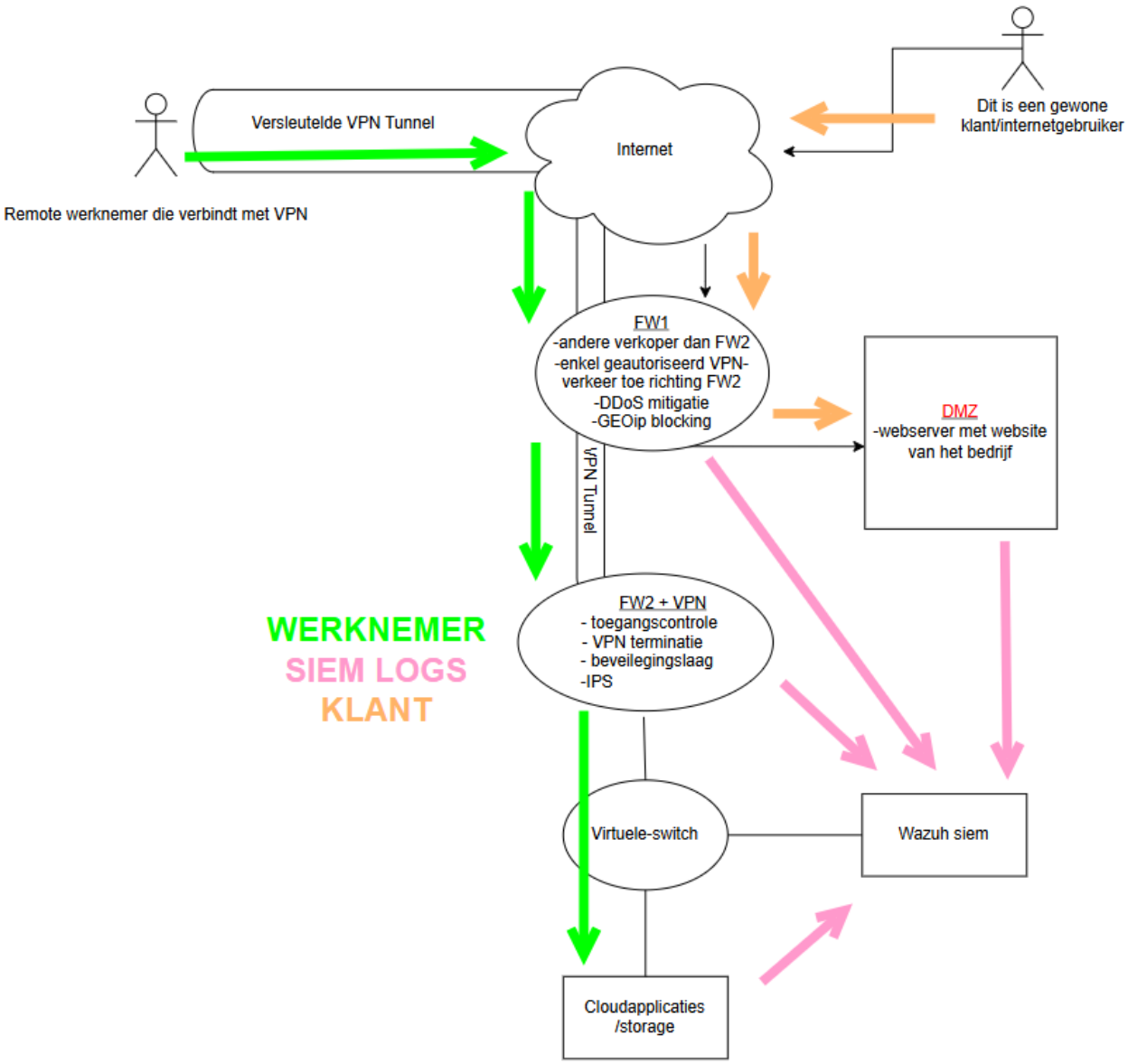
5. Definitief Security Ontwerp (To-Be)



Onze gekozen architectuur is een simulatie van hoe GotITech eruit zou zien als het een klein, professioneel netwerk had. Hoewel het bedrijf remote werkt, gebruiken we een virtueel on-prem model om te tonen hoe beveiliging wordt gerealiseerd.

De virtuele switch in het schema wordt uitsluitend gebruikt in de testomgeving (EVE-NG) om de interne netwerksegmentatie en verkeersstromen te simuleren. In de productieomgeving van GotITech wordt deze functionaliteit niet gerealiseerd via een klassieke virtuele switch, maar via netwerktechnologieën zoals subnets binnen een virtueel netwerk (VPC/VNet). De virtuele switch dient in het schema dus enkel als conceptuele voorstelling om de werking en segmentatie van de testomgeving inzichtelijk te maken. Evenzo hebben we in EVE-NG een switch gebruikt om het verkeer van end-device over het internet naar ons bedrijfsnetwerk te visualiseren aangezien een uitgebreide oplossing onhaalbaar was met de toegekende resources in EVE-NG en buiten het bestek van deze opdracht valt.

Verkeerstroom



5.1 Firewalls

FW1 – Perimeter firewall

FW1 is de perimeter firewall en vormt de eerste beveiligingslaag tussen het pubkieke internet en de cloudomgeving. Het doel van FW1 is om ongewenst en potentieel kwaadaardig verkeer zo vroeg mogelijk te blokkeren, nog vóór dit de interne beveiligingslaag bereikt.

FW1 voert geen VPN-terminatie uit, maar laat enkel expliciet toegestaan VPN-verkeer door naar FW2. Op die manier wordt de VPN-firewall beschermd tegen scanning en misbruik.

Daarnaast:

- past FW1 geo-blocking toe om verkeer uit niet-relevante regio's te blokkeren
- beperkt FW1 DDoS-aanvallen en abnormale verkeerspieken
- scheidt FW1 de DMZ (publieke website) strikt van de interne cloudomgeving

FW1 fungeert dus als een filterende en beschermende randlaag, die het aanvalsoppervlak verkleint en ervoor zorgt dat enkel gecontroleerd verkeer FW2 en de interne cloud bereikt.

FW2 – Interne beveiligings firewall & VPN-gateway

FW2 vormt de interne beveiligingslaag van de cloudomgeving en is verantwoordelijk voor het controleren van wie toegang krijgt tot welke interne resources. In tegenstelling tot FW1 richt FW2 zich niet op algemeen internetverkeer, maar op geauthenticeerde en gecontroleerde verbindingen.

FW2 fungeert als VPN-gateway en verzorgt de VPN-terminatie voor remote werknemers. Pas nadat gebruikers correct geauthenticeerd zijn, krijgen zij toegang tot de interne cloudapplicaties.

Daarnaast:

- voert FW2 strikte toegangscontrole uit tussen de verschillende interne segmenten
- inspecteert FW2 het verkeer met een **Intrusion Prevention System (IPS) op basis van Suricata** om verdachte of kwaadaardige activiteiten te detecteren en actief te blokkeren
- beperkt FW2 laterale beweging binnen de cloudomgeving

FW2 beschermt zo de cloudapplicaties en opslag tegen misbruik van gecompromitteerde accounts of systemen, en vormt de laatste actieve beveiligingslaag vóór de interne services.

5.2 DMZ-zone

De DMZ is een afgeschermde netwerkzone die bedoeld is voor systemen die publiek bereikbaar moeten zijn, zoals de bedrijfswebsite. In dit ontwerp bevat de DMZ uitsluitend de webserver van het bedrijf.

Waarom DMZ?
Moest een webserver gehackt worden, raakt de aanvaller niet meteen in het interne netwerk.

VPN-toegang

Remote werknemers maken verbinding met de cloudomgeving via **OpenVPN met Multi-Factor Authentication (MFA)**, dat een versleutelde tunnel opzet over het internet. Hierdoor worden vertrouwelijkheid en integriteit van de communicatie gegarandeerd, ongeacht het netwerk van waaruit de werknemer werkt.

De VPN-verbinding wordt beëindigd op FW2, waar gebruikers eerst moeten worden geauthenticeerd voordat zij toegang krijgen tot interne cloudapplicaties. Pas na succesvolle authenticatie wordt verkeer doorgelaten naar de interne netwerken.

IPS – Suricata

1. Op FW2 is een Intrusion Prevention System (IPS) actief op basis van Suricata. Het IPS inspecteert netwerkverkeer na VPN-authenticatie, dus op verkeer dat afkomstig is van geauthenticeerde gebruikers.

Het doel van het IPS is het detecteren en blokkeren van kwaadaardig gedrag, zoals:

- malware-communicatie
- exploitpogingen
- verdachte netwerkpatronen
- command-and-control verkeer

Dit is vooral belangrijk bij remote workers:

> *Indien een remote toestel besmet zou zijn met malware, kan Suricata dit gedrag detecteren en het verkeer blokkeren voordat het de cloudapplicaties bereikt.*

Zo wordt voorkomen dat één geïnfecteerd toestel de volledige cloudomgeving compromitteert.

Netwerksegmentatie

In het schema worden VLAN's gebruikt als logische voorstelling van netwerksegmentatie. In een public cloud omgeving worden deze VLAN's geïmplementeerd als afzonderlijke subnets binnen een virtueel netwerk (VPC/VNet).

De segmentatie dient om:

- laterale beweging te beperken
- impact van incidenten te verkleinen
- beveiligingsregels per zone af te dwingen

Typische segmenten zijn:

- DMZ (publieke webserver)
- VPN / beveiligingslaag
- interne cloudapplicaties
- logging / monitoring (SIEM)

Deze scheiding is essentieel om ransomware en andere aanvallen te beperken

Waarom netwerksegmentatie met meerdere subnets noodzakelijk is

Onderdeel	Eén subnet (onveilig)	Meerdere subnets (veilig ontwerp)
Segmentatie	**Alle systemen bevinden zich in één netwerksegment**	**Systemen worden opgesplitst in afzonderlijke subnets per functie**

Toegangscontrole	**Elk systeem kan in principe elk ander systeem bereiken**	**Toegang tussen subnets wordt strikt afgedwongen door de firewall**
Bescherming van SIEM	**Interne systemen kunnen SIEM rechtstreeks bereiken of scannen**	**SIEM bevindt zich in een apart subnet en is enkel bereikbaar voor logging**
Verkeer inspecteren	**Moeilijk onderscheid maken tussen types verkeer**	**Firewall kan verkeer per subnet inspecteren en controleren**
Laterale beweging	**Een geïnfecteerd systeem kan het volledige netwerk verkennen**	**Laterale beweging is beperkt tot het eigen subnet**
Impact van incidenten	**Eén incident kan het volledige netwerk treffen**	**Impact blijft beperkt tot één subnet**
Logging en monitoring	**Moeilijk om relevante events te filteren**	**Logs zijn beter te correleren per subnet en functie**

Ransomware-risico	**Hoge kans op verspreiding binnen het netwerk**	**Verspreiding wordt sterk beperkt door segmentatie**

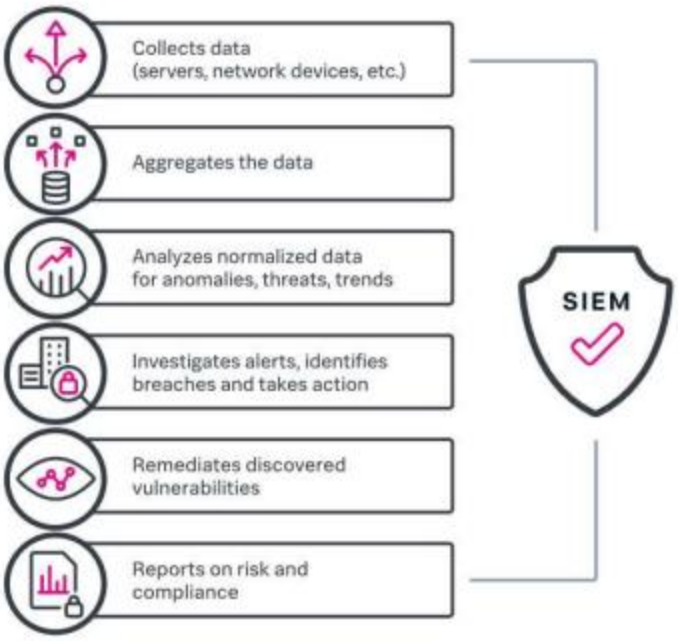
5.7 SIEM

Voor centrale logging en monitoring wordt Wazuh SIEM ingezet. Deze SIEM-oplossing verzamelt en correleert loggegevens van de perimeter firewall (FW1), de interne beveiligingsfirewall (FW2) en de interne cloudapplicaties. Hierdoor ontstaat een volledig overzicht van zowel extern als intern netwerkgedrag, waaronder perimeter-events zoals geo-blocking en DDoS-pogingen, VPN-authenticaties en IPS-detecties, evenals activiteiten op

interne systemen.

(Foto uit T06_siem.pdf van AP hogeschool geraadpleegd op 30/12/2025)

Het doel van Wazuh is het **tijdig detecteren van verdachte of afwijkende activiteiten**, het herkennen van aanvalspatronen en het ondersteunen van incident response. Door logs te correleren over meerdere beveiligingslagen heen kan sneller worden vastgesteld of er sprake is van een gerichte aanval of van misbruik van gecompromitteerde accounts of systemen. Daarnaast ondersteunt Wazuh forensisch onderzoek door het bewaren en analyseren van historische loggegevens.



(Foto uit T06_siem.pdf van AP hogeschool geraadpleegd op 30/12/2025)

Waarom in een aparte zone?

- SIEM moet veilig en geïsoleerd staan
- een aanvaller mag logs niet kunnen verwijderen

5.8 QoS

Quality of Service (QoS) wordt toegepast om ervoor te zorgen dat kritiek bedrijfsverkeer voorrang krijgt op minder belangrijk verkeer. Dit is van groot belang voor GotITech, aangezien het bedrijf volledig remote werkt en sterk afhankelijk is van cloudapplicaties, online samenwerking en realtime communicatie.

Zo wordt niet alleen veiligheid, maar ook **beschikbaarheid en gebruikservaring** gegarandeerd.

6. Waarom we bepaalde technieken NIET gebruiken

802.1X

802.1X wordt niet toegepast omdat deze techniek bedoeld is voor het beveiligen van toegang tot **fysieke netwerken** via beheerde switches en netwerkpoorten. In de context van GotITech, dat volledig cloud-gebaseerd werkt en geen eigen netwerktoegangsinfrastructuur beheert, kan 802.1X niet op een zinvolle manier worden afgedwongen.

SD-WAN

SD-WAN is ontworpen voor omgevingen met meerdere locaties en complexe WAN-verbindingen die dynamisch beheerd moeten worden.

Deze techniek wordt niet ingezet omdat:

- de netwerkarchitectuur geen meerdere vestigingen of WAN-links bevat
- veilige connectiviteit reeds wordt gerealiseerd via VPN
- SD-WAN extra beheer, configuratie en kosten introduceert zonder duidelijke meerwaarde

Private Cloud

Een private cloud wordt niet gekozen omdat het opzetten en beheren van eigen cloudinfrastructuur een hoge operationele en financiële kost vereist. Het heeft geen proportionele meerwaarde.

WAF (Web Application Firewall)

Een WAF wordt niet toegevoegd omdat de publieke webomgeving beperkt is in complexiteit en zich in een strikt afgeschermde DMZ bevindt. Netwerkgebaseerde beveiliging via de perimeter firewall volstaat om het huidige aanvalsvlak te beschermen. Een WAF kan in de toekomst overwogen worden indien de webapplicatie kritieker of functioneel uitgebreider wordt.

7. Risicoanalyse

Nr	Risico	Probability (1–10)	Impact (1–10)	PI-index	Preventie
1	Ongeautoriseerde toegang tot cloudapplicaties	3	9	**36**	VPN-authenticatie via FW2, strikte firewallregels, netwerksegmentatie, IPS
2	Malware-infectie via remote werknemer	5	8	**56**	Inspectie van VPN-verkeer met Suricata IPS, segmentatie, monitoring via SIEM
3	Ransomware-aanval op cloudomgeving	5	10	**50**	IPS-detectie, beperking van laterale beweging via subnets, SIEM-alerting
4	Compromittering van gebruikersaccount (phishing)	6	8	**48**	MFA op VPN-authenticatie, firewall policies, detectie en correlatie via SIEM

5	Aanval op publieke website (DMZ)	8	4	**32**	DMZ-isolatie, perimeter firewall (FW1), geo-blocking, DDoS-beperking
6	Onvoldoende of vertraagde detectie van incidenten	4	7	**28**	Centrale logging en correlatie via Wazuh SIEM
7	Netwerkcongestie of verminderde beschikbaarheid	5	5	**25**	QoS voor kritisch VPN- en applicatieverkeer, filtering op FW1

8. Implementatieplan

Het implementatieplan bestaat uit vijf grote fases, netjes gescheiden tussen wat we eerst in de testomgeving uitwerken en hoe dit daarna wordt doorgetrokken naar de echte productieomgeving van GotITech.

Fase 1 – Aanmaken van een volledige testomgeving

De implementatie van de beveiligingsarchitectuur gebeurt in opeenvolgende fases. Eerst wordt het ontwerp gevalideerd in een testomgeving (EVE-NG). Pas na succesvolle testen wordt het ontwerp stapsgewijs uitgerold naar de productieomgeving van GotITech. Deze aanpak beperkt risico’s en garandeert een gecontroleerde overgang.

8.1 Fase 1 – Voorbereiding en validatie (EVE-NG)

Stap 1: Opzetten van de testomgeving

In EVE-NG wordt een representatieve netwerktopologie opgebouwd die het eindontwerp weerspiegelt. De focus ligt op het correct scheiden van netwerksegmenten en het voorzien van alle noodzakelijke beveiligingscomponenten.

Stap 2: Basisconnectiviteit en routing

Eerst wordt nagegaan of alle netwerksegmenten correct met elkaar kunnen communiceren volgens het ontwerp. Ongewenste verbindingen worden bewust geblokkeerd om te verifiëren dat segmentatie correct afgedwongen wordt.Tijdens de implementatie wordt Multi-Factor Authentication (MFA) geactiveerd op de OpenVPN-authenticatie om misbruik van gecompromitteerde credentials te voorkomen.

Stap 3: Toegangscontrole testen

Vervolgens wordt gecontroleerd of toegang tot interne netwerken enkel mogelijk is via de voorziene VPN-toegang. Pogingen tot rechtstreekse toegang vanaf het internet of vanuit de DMZ worden getest en moeten falen.

Stap 4: Detectie en preventie valideren

Daarna worden gesimuleerde aanvalsscenario's uitgevoerd (bv. verdachte netwerkpatronen, foutieve logins) om te controleren of deze correct worden gedetecteerd en geblokkeerd. De focus ligt op het correct functioneren van detectie- en preventiemechanismen.

Stap 5: Logging en monitoring controleren

Tot slot wordt nagegaan of alle relevante events correct worden doorgestuurd en zichtbaar zijn in de SIEM-omgeving. Enkel wanneer logging en alerting betrouwbaar werken, wordt de testomgeving als geslaagd beschouwd.

8.2 Fase 2 – Overgang naar productie

Stap 6: Vertaling naar cloudomgeving

De gevalideerde configuraties uit de testomgeving worden vertaald naar cloud-native componenten. Logische segmentatie wordt omgezet naar subnets binnen een virtueel netwerk, met behoud van dezelfde beveiligingsprincipes.

Stap 7: Gefaseerde activering van beveiligingsmaatregelen

Beveiligingsmaatregelen worden stapsgewijs geactiveerd in productie. Eerst wordt basisconnectiviteit opgezet, daarna toegangscontrole, en pas op het einde actieve detectie en preventie. Dit voorkomt onverwachte verstoringen.

Stap 8: Productietesten en validatie

Na activatie worden functionele testen uitgevoerd met een beperkte groep gebruikers. Hierbij wordt gecontroleerd of normale werking mogelijk is en of beveiligingsmaatregelen geen ongewenste blokkeringen veroorzaken.

8.3 Fase 3 – Nazorg en optimalisatie

Stap 9: Monitoring en fine-tuning

In de eerste periode na livegang worden logs en alerts actief opgevolgd. Op basis hiervan kunnen drempelwaarden, regels en prioriteiten bijgestuurd worden.

Stap 10: Documentatie en overdracht

Tot slot worden configuraties en beslissingen gedocumenteerd zodat het ontwerp beheersbaar blijft en later kan worden uitgebreid of aangepast.

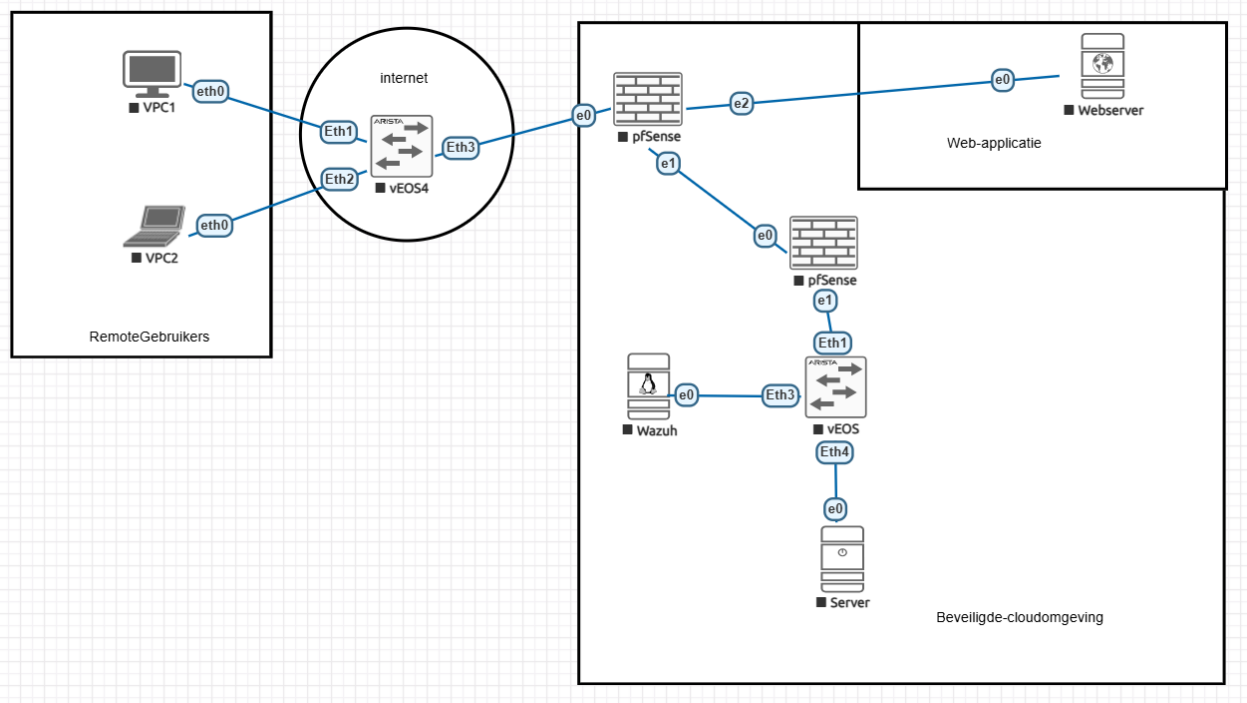
Implementatie – Testfase in EVE-NG

Vooraleer de voorgestelde beveiligingsarchitectuur in een echte cloudomgeving zou worden uitgerold, is ervoor gekozen om het volledige ontwerp eerst te valideren in een gesimuleerde testomgeving. Hiervoor werd EVE-NG gebruikt.

De testfase heeft drie concrete doelen:

1. Aantonen dat het netwerk functioneel werkt volgens het ontwerp
2. Controleren dat segmentatie en toegangscontrole correct worden afgedwongen
3. Verifiëren dat logging, detectie en preventie effectief functioneren

Heel schema:



Het schema is logisch opgedeeld in verschillende zones, elk met een duidelijke beveiligingsfunctie:

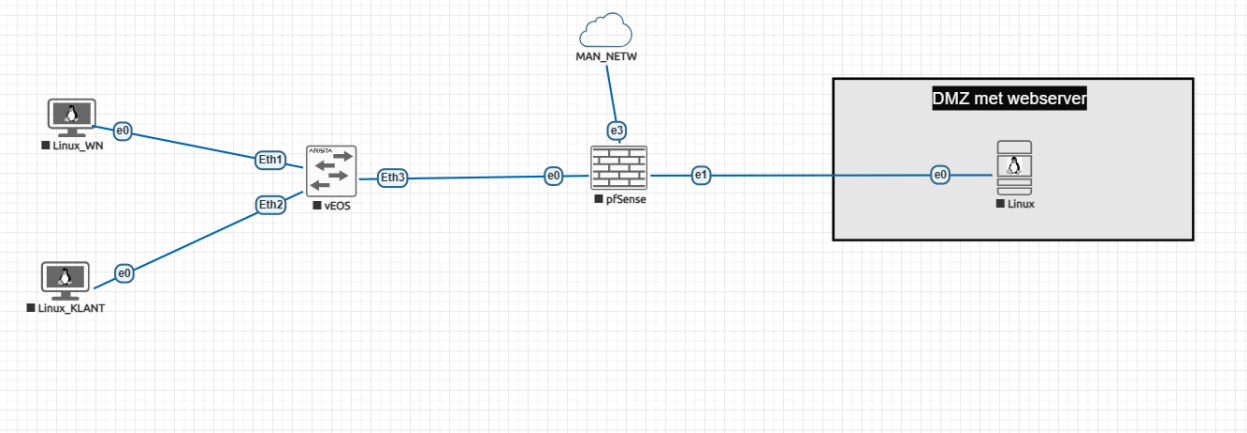
- **Internetzone**: simuleert externe gebruikers en klanten
- **Perimeter firewall (FW1 – pfSense)**: eerste beveiligingslaag
- **DMZ**: bevat een publieke webserver
- **Interne firewall / VPN-gateway (FW2 – pfSense - IPS)**
- **Interne cloudomgeving**: applicaties en server
- **SIEM-zone**: Wazuh voor logging en monitoring

Deze opdeling weerspiegelt exact de principes die in het hoofdstuk *Definitief Security Ontwerp (To-Be)* werden vastgelegd.

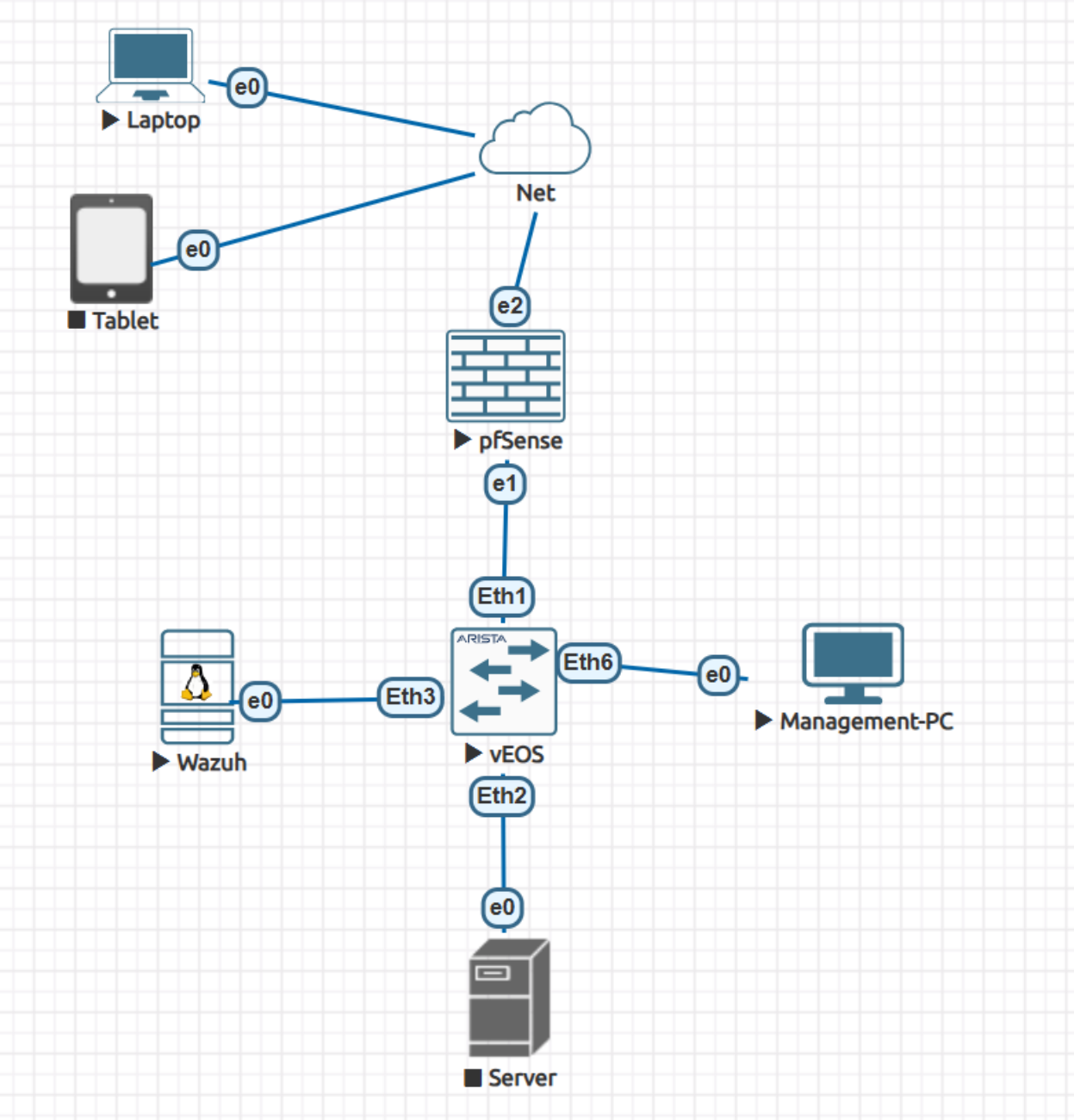
Voor de testen uit te voeren splitsen we ons schema op in twee delen.

Schema 1:

Voor de configuratie zie het extra document


MAN_NETW
DMZ met webserver
Linux_WN
e0
Eth1
vEOS
Eth3
e0
e3
pfSense
e1
e0
Linux
Eth2
e0
Linux_KLANT

Schema 2:



Management-PC is tijdelijk toegevoegd om testen uit te voeren.

10. Conclusie

Dit ontwerp biedt GotITech een moderne, toekomstgerichte en veilige IT-architectuur, afgestemd op een remote-start-up. Dankzij firewalling, segmentatie, VPN, IDS-detectie, SIEM-monitoring en duidelijke policies:

- worden aanvallen sneller gedetecteerd
- blijft ransomware beperkt tot één zone
- krijgt het bedrijf veilige toegang tot cloudapplicaties
- is er volledige zichtbaarheid via centrale logging

Door eerst een volledige testomgeving uit te bouwen, kunnen alle beveiligingslagen zorgvuldig worden getest en geoptimaliseerd voordat ze in de echte omgeving worden uitgerold.

Het resultaat is een helder, logisch en toekomstgericht security-ontwerp waarmee het bedrijf veilig kan blijven werken terwijl het blijft groeien.