AP HOGESCHOOL ANTWERPEN

<Toegepaste Informatica / Elektronica-ICT

Blueprint
Project SASE

ondersteund door de

AP Hogeschool

begeleid door het bedrijf

New Wave Group

Akira Neeus

Axel Weyers

Begeleider: Dimitri Weayaert

Academiejaar 2025-2026 (1ste semester)

Inhoudstafel

Termen en Afkortingen

[De termen en afkortingen die worden gebruikt in de blueprint, worden hier opgelijst en omschreven. Wanneer een afkorting voor de eerste keer wordt gebruik in de blueprint, dan wordt deze ook daar kort verklaard.]

Term	*Omschrijving*
SASE	*Een cloud-gebaseerd beveiligingsmodel dat netwerk- en security functies (zoals firewall, SWG, CASB, ZTNA en SD-WAN) integreert in één centraal platform.*
SWG	*Beveiligingsoplossing die internetverkeer filtert, malware blokkeert en ongewenste of schadelijke websites tegenhoudt.*
CASB	*Een beveiligingslaag die het gebruik van cloud applicaties (SaaS) monitort, controleert en beveiligt, inclusief gegevensbescherming en toegangsbeheer.*
ZTNA	*Een beveiligingsmodel waarin geen enkele gebruiker of bron standaard vertrouwd wordt; toegang wordt per sessie en context gecontroleerd.*
SD-WAN	*Een netwerkoplossing die WAN-verkeer dynamisch en intelligent verdeelt via meerdere verbindingen (bijv. internet, MPLS), vaak met focus op prestaties, kosten en beveiliging.*
PoC	*verbindingen (bijv. internet, MPLS), vaak met focus op prestaties, kosten en beveiliging.* *Een kleinschalige testopstelling waarmee wordt aangetoond dat een voorgestelde oplossing of technologie praktisch uitvoerbaar is.*

Breakout	*Een breakout is een netwerkconfiguratie waarbij internetverkeer direct naar de cloud of het internet gaat, zonder eerst terug te hoeven naar een datacenter. Dit vermindert latency en verbetert de prestaties van cloudapplicaties.*
DLP	*DLP = Data Loss Prevention/Het doel van DLP is te voorkomen dat gevoelige informatie per ongeluk of opzettelijk het bedrijf verlaat.*
SAAS	*Software As A Service, een manier om software via internet aan te bieden als een dienst.*

I. Bedrijfscontext

A. Opdrachtgever

[Beschrijf de organisatie en belangrijkste drijfveren van de opdrachtgever(s).]

[Beschrijf ook de functie van de betrokken personen én hun rol in het project. Die kunnen verschillend zijn.]

New Wave Group is een internationale kleding- en textielgroep die actief is in verschillende landen. Het bedrijf ontwikkelt, produceert en distribueert promotiekleding, bedrijfskleding, sport- en vrijetijdskleding, aangevuld met lifestyle- en geschenk producten. Ze beheren en hosten hun kritieke applicaties en data in datacenters in Zweden en Nederland. Hun infrastructuur ondersteunt zowel remote sites als mobiele gebruikers, met beveiliging via firewalls, VPN, IPS, anti-malware en webfiltering.

Belangrijkste drijfveren

1. **Veiligheid**
   De organisatie wil overal een betrouwbare, uniforme en veilige toegang tot gevoelige data en applicaties. Het doel is één consistent security-model dat zowel interne als remote gebruikers beschermt.

2. **Verminderen van complexiteit**
   De huidige infrastructuur bestaat uit losse VPN-verbindingen, verschillende firewalls en versnipperde policies, wat beheer over meerdere landen moeilijk maakt.
   De drijfveer is dus niet dat de oplossing complex moet zijn, maar net dat de huidige complexiteit moet verdwijnen.

3. **Prestaties**
   Veel verkeer moet vandaag onnecessarily terugkeren naar de datacenters in Zweden of Nederland, wat leidt tot vertragingen. Een modern model moet snellere toegang tot cloudapplicaties en minder latency mogelijk maken.

Daarom willen ze migreren naar een full SASE-oplossing op basis van open source, om centrale beveiliging, schaalbaarheid en betere prestaties te realiseren.

Functies

- Opdrachtgever: Bepaalt de noden en verwachtingen rond de SASE-migratie.
- Studenten: Zoeken en ontwerpen een gepaste oplossing.
- Lector: Communiceert met de klant en biedt ondersteuning tijdens het project.

B. Samenvatting

[Korte samenvatting van het project en context, 1 of 2 alinea's]

In dit project zorgen we ervoor hoe we hoe de huidige beveiligingsarchitectuur van New Wave Group kunnen evolueren naar een modern full SASE-model. De huidige situatie van het bedrijf draait voornamelijk op datacenter beveiliging met Next-Generation Firewalls, IPS(beveiligingssysteem dat netwerken actief analyseert), anti-malware, sandboxing en webfiltering, aangevuld met SD-WAN en always-on VPN voor remote en mobiele gebruikers. Dit zorgt wel al voor goede beveiliging voor de interne infrastructuur , maar mist een volledige integratie van cloudbeveiliging , Zero Trust-principes en uniforme policies.

C. Huidige Situatie (AS-IS)

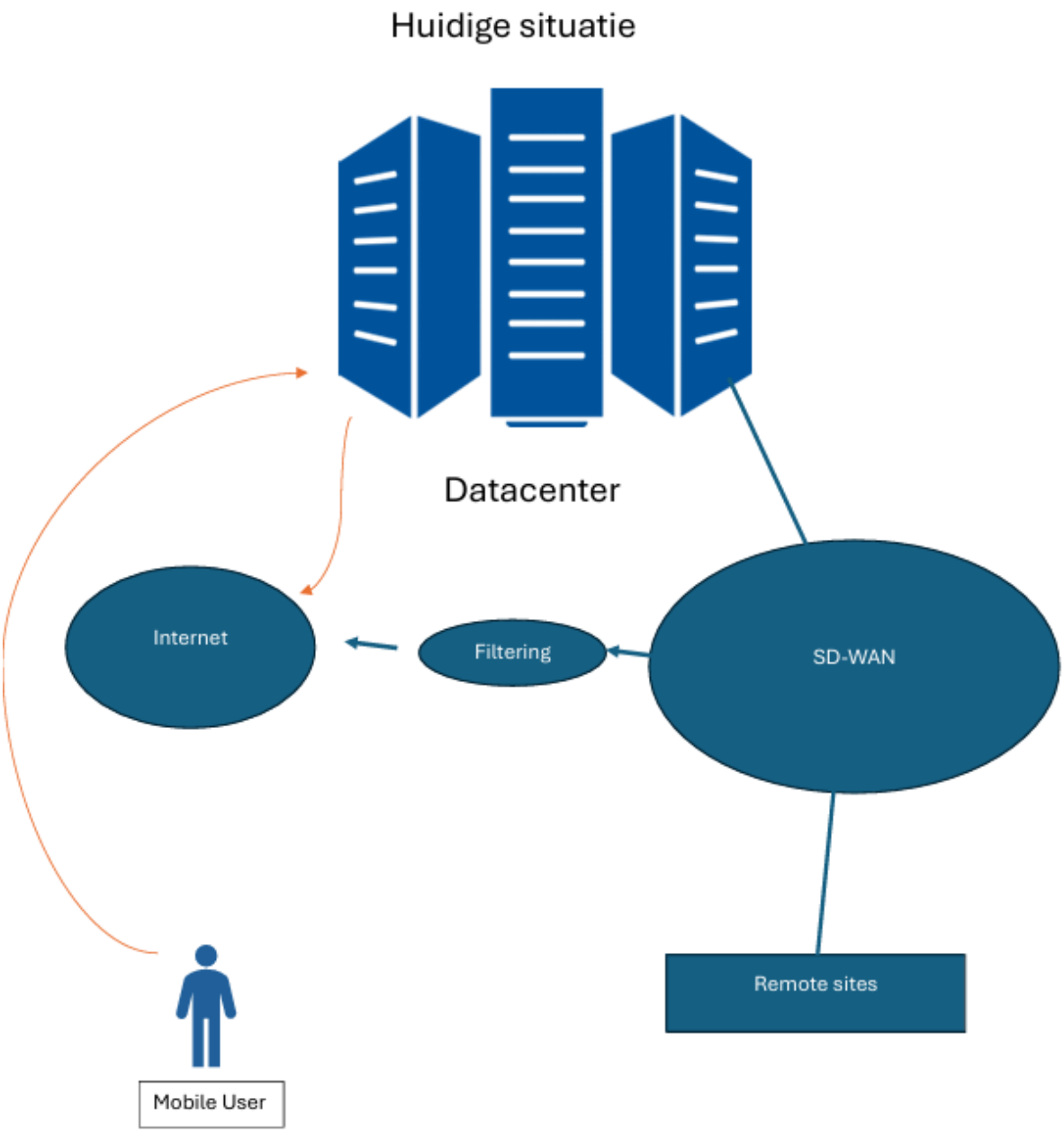
[Beschrijf de huidige werkwijze en oplossing functioneel. Lijst de problemen en/of opportuniteiten op. Maak hier los van tekst gebruik van (een) gepaste visuele voorstelling(en). Dit kan bijv. een netwerkschema zijn en/of een aangeleerd diagram tijdens het vak analysis

Omschrijf ook de verschillende betrokken partijen. Denk ook hier aan gepaste visuele voorstellingen zoals bijv. een sequentiediagram.]

Bij New Wave Group ligt de focus van de beveiliging vooral op het datacenter en interne systemen. Belangrijke onderdelen zijn: Next-Generation Firewalls, IPS om aanvallen te blokkeren, anti-malware met cloud-based sandboxing, web filtering, SD-WAN voor remote sites en een always-on VPN voor mobiele gebruikers.

Problemen zijn dat cloudapplicaties nog niet goed beschermd zijn, Zero Trust ontbreekt en policies niet overal uniform zijn. Ook is er geen centraal platform voor volledige monitoring van het netwerk en de gebruikers. Dit biedt wel een kans: door over te stappen naar een full SASE-model kunnen zowel cloud als interne systemen beter beveiligd worden en wordt het beheer eenvoudiger.

***Betrokken partijen:** IT-beheerteam, System Administrators, mobiele gebruikers, Klanten.*



In het huidige model moet verkeer van mobiele gebruikers altijd eerst door het datacenter lopen (oranje lijn), ongeacht of ze interne applicaties of cloud applicaties gebruiken. Dit creëert extra hops, verhoogde latency en onnodig netwerkverkeer.

Het huidige model is robuust voor traditionele datacenter gebaseerde workloads, maar voldoet niet langer aan moderne vereisten zoals:

- uniforme cloudbeveiliging
- Zero Trust-toegang
- gecentraliseerd beleid
- performante cloud verbindingen

- ❖ schaalbaarheid

D. Toekomstige Situatie (TO-BE)

[Beschrijf de gewenste toekomstige situatie en beschrijf/visualiseer waar er aanzienlijke afwijkingen zijn ten opzichte van de huidige situatie]

De doelstelling is om een functioneel en technisch ontwerp uit te werken dat toont hoe open-source oplossingen zoals SWG (Secure Web Gateway, voor het filteren en beveiligen van internetverkeer), CASB (Cloud Access Security Broker, voor controle en bescherming van cloudapplicaties), ZTNA (Zero Trust Network Access, voor context-gebaseerde toegangscontrole) en SD-WAN (Software-Defined Wide Area Network, voor geoptimaliseerde en veilige netwerkconnectiviteit) geïntegreerd kunnen worden in een SASE-architectuur (Secure Access Service Edge, een cloud-gebaseerd platform dat netwerk- en beveiligingsfuncties combineert). Het project omvat een analyse van de huidige situatie, een vergelijking met commerciële oplossingen, een risicoanalyse en de rol van AI (Artificial Intelligence, voor detectie en automatisering) in de beveiliging. Uiteindelijk wordt een blueprint en Proof of Concept (PoC, een testopstelling om de praktische uitvoerbaarheid aan te tonen) opgesteld waarmee New Wave Group veilig en toekomstgericht kan migreren naar een full SASE-omgeving.

II. Oplossing

A. Doelstelling

[Welke problemen en/of opportuniteiten worden er opgelost? Lijst ze op en formuleer ze op een duidelijke en meetbare manier.]

Problemen:

1. *Cloudapplicaties en SaaS zijn nu nog niet goed beveiligd.*
    - *Oplossing: alle cloudapps worden beschermd via CASB en SWG.*

2. *Zero Trust ontbreekt, interne gebruikers worden soms automatisch vertrouwd.*
    - *Oplossing: toegang wordt per sessie gecontroleerd via ZTNA.*

3. *Beveiligingsregels zijn niet overal hetzelfde, waardoor er inconsistenties zijn.*
    - *Oplossing: uniforme security policies voor alle gebruikers en locaties.*

4. *Er is geen centraal overzicht van netwerkactiviteiten of incidenten.*
    - *Oplossing: een geïntegreerd dashboard met logging, monitoring en AI-ondersteuning.*

Opportuniteiten:

1. *Cloud en interne systemen beter integreren via full SASE.*
    - *Resultaat: alle netwerk- en security functies zitten in één platform.*

2. *Automatisering en AI inzetten voor detectie van bedreigingen.*
    - *Resultaat: afwijkend of verdacht gedrag wordt automatisch herkend en gerapporteerd.*

Doelstelling:

Alles samen brengen tot één gecentraliseerd cloudplatform, één beleidssysteem voor alle gebruikers, apps en locaties. Automatisch schaalbaar en eenvoudiger te beheren.

B. Functionele Scope

Scope

- *[Opsommen van de functionaliteit en onderdelen die bij het uitvoeren van het project horen. Probeer dit zo sluitend mogelijk te doen, dit voorkomt discussies.]*
- *[Maak enkel assumpties als het niet anders kan.]*

- *[Expliciet vernoemen wat niet tot de draagwijdte (scope) van het project hoort, bv. het aanleveren van onderdelen, opleiding, maintenance, onderhoud van servers, …]*

[Samengevat: Afbakening van de te realiseren functionaliteiten.]

Het project start met een volledige analyse van de bestaande beveiligings omgeving, waaronder SWG-functionaliteit, SIEM/SOAR, VPN, webfiltering en logging. Deze inventarisatie vormt de basis voor het ontwerp van de nieuwe open-source SASE-architectuur. Binnen de scope valt ook het verbeteren van monitoring en incident detectie, het uitbreiden van de CASB-beveiliging voor cloud applicaties, en het opstellen van uniforme security policies die gelden voor alle gebruikers en locaties. Daarnaast onderzoeken we hoe de huidige always-on VPN kan worden vervangen door een Zero Trust-benadering via ZTNA.

De functionele scope omvat eveneens het bouwen van een Proof of Concept waarin de integratie van ZTNA, CASB, SWG, SIEM/SOAR, SD-WAN en FWaaS wordt getest. In deze PoC wordt nagegaan hoe deze componenten samenwerken, welke beveiligingsfuncties ze bieden en hoe ze bijdragen aan een schaalbare, moderne en veilige omgeving.

Voor dit project maken we uitsluitend gebruik van open-source oplossingen of bestaande interne systemen. We gaan ervan uit dat de huidige application firewall correct werkt en zonder aanpassing geïntegreerd kan worden in de toekomstige SASE-architectuur.

Niet inbegrepen in de scope zijn het aanleveren of installeren van fysieke hardware, het uitvoeren van onderhouds- of beheertaken, het geven van opleidingen aan beheerders of eindgebruikers en het uitvoeren van operationele taken na oplevering. Ook de volledige productie-implementatie van SASE en de migratie van alle medewerkers naar ZTNA vallen buiten deze opdracht.

Samengevat levert dit project een blauwdruk en Proof of Concept van een open-source SASE-omgeving, maar geen productie-uitrol, onderhoud of operationele ondersteuning.

C. Functioneel design

[*Beschrijf hier wat er in het ontwerp reeds opgenomen moet worden m.b.t. functionaliteit]*

***Use cases**: Scenario's of beschrijvingen van hoe de gebruiker het systeem zal gebruiken.*

***Functionaliteiten**: Gedetailleerde beschrijvingen van wat het systeem moet kunnen.*

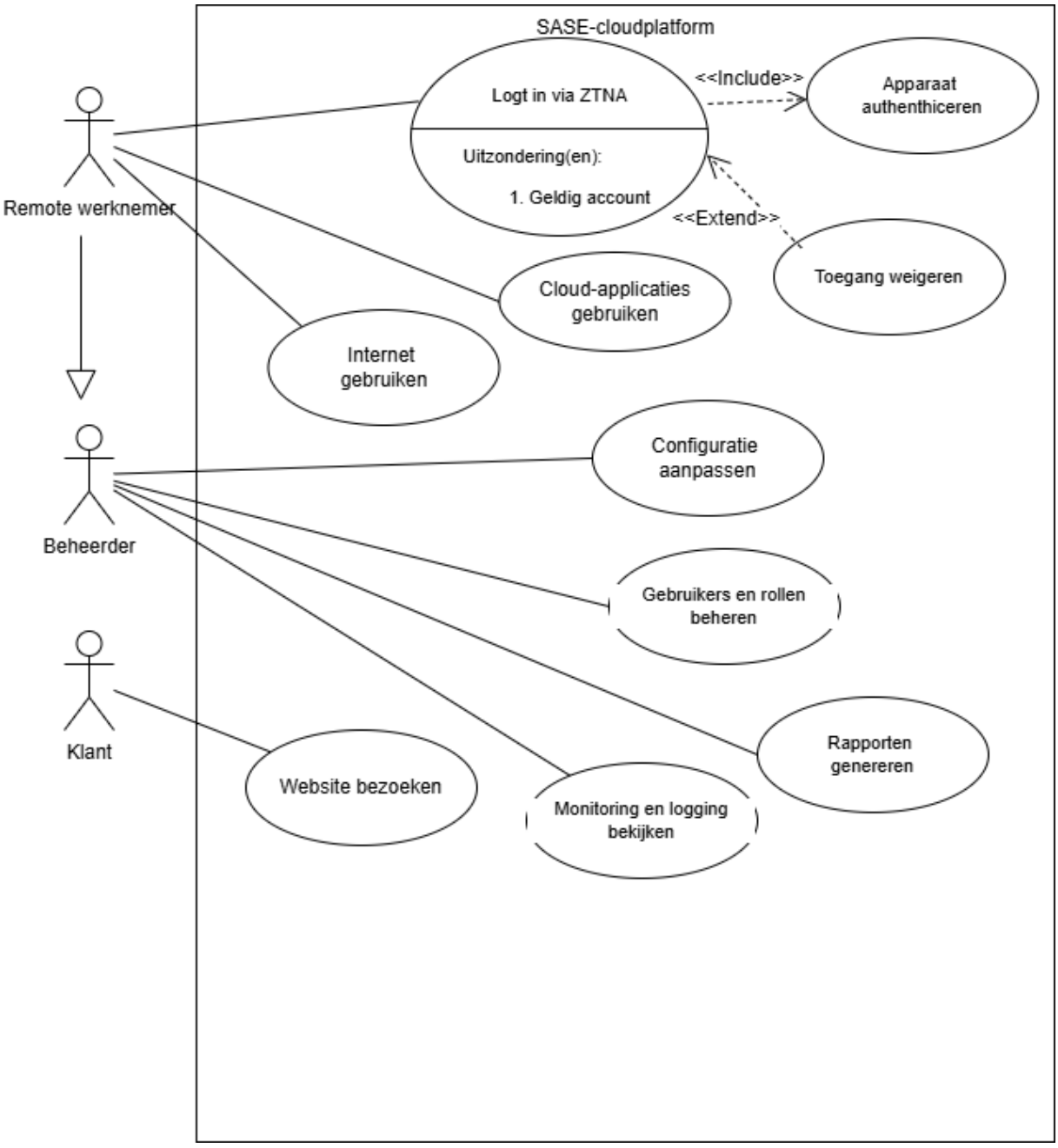
***Systeemgedrag**: Specificaties van hoe het systeem op bepaalde acties van de gebruiker of gebeurtenissen moet reageren.*

***Business rules**: De regels en voorwaarden waaraan het systeem moet voldoen.*

[TIP ! Denk aan wireframes,mock-ups, toestandsdiagrammen, beslissingstabellen, activitydiagrammen.]

[Samengevat: Gedetailleerde beschrijving van hoe het systeem moet werken om aan de eisen van de gebruikers te voldoen.]

Use case



Het use case-diagram stelt de belangrijkste interacties voor tussen de drie betrokken actoren => Remote Gebruiker, Beheerder en Klant.

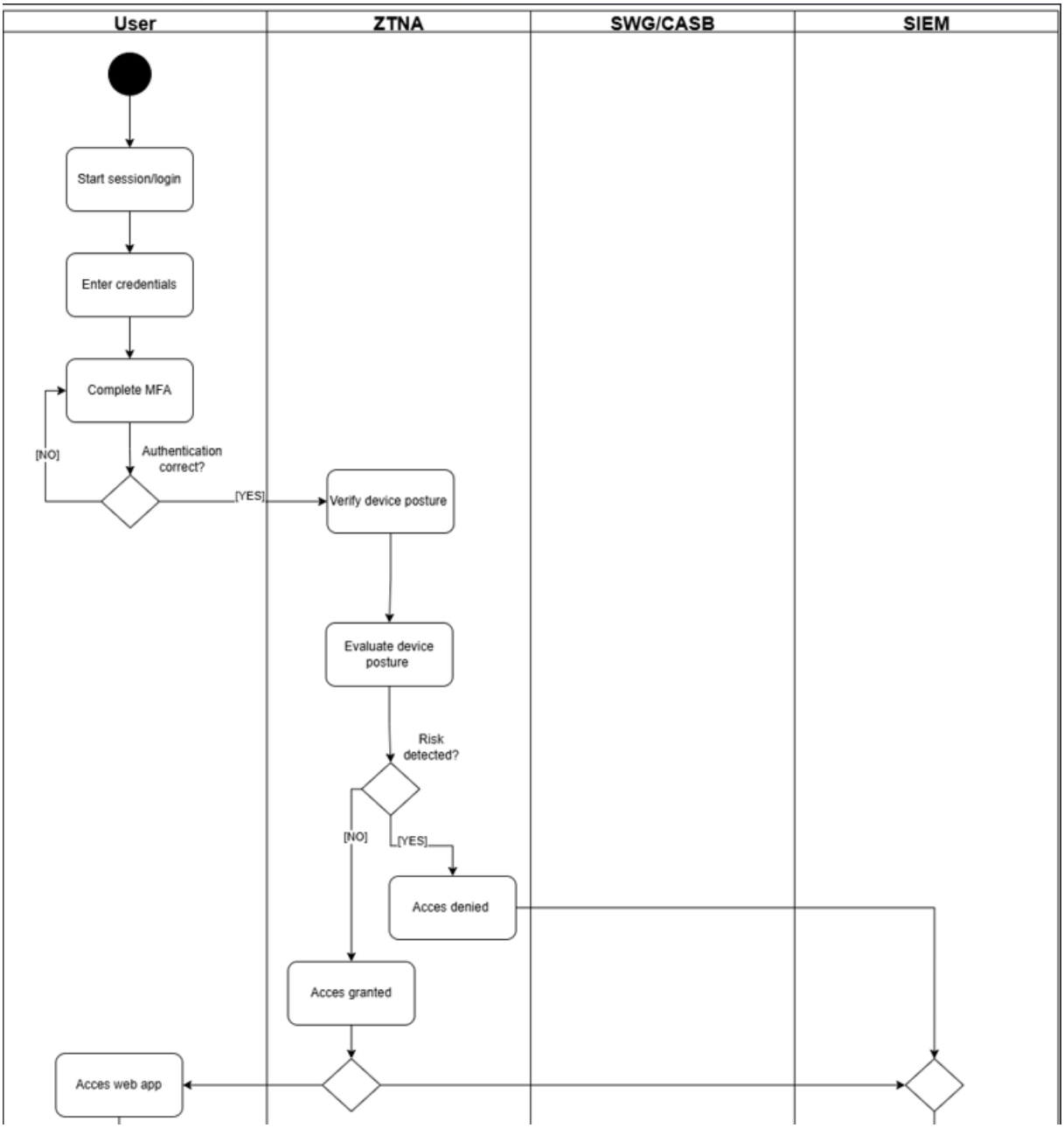
- **Remote gebruiker**
  De remote gebruiker meldt zich aan via Zero Trust Network Access (ZTNA).
  Deze controleert de identiteit, locatie en het apparaat, en vereist Multi-Factor Authenticatie (MFA) voordat toegang wordt verleend.
  Na succesvolle verificatie kan de gebruiker:

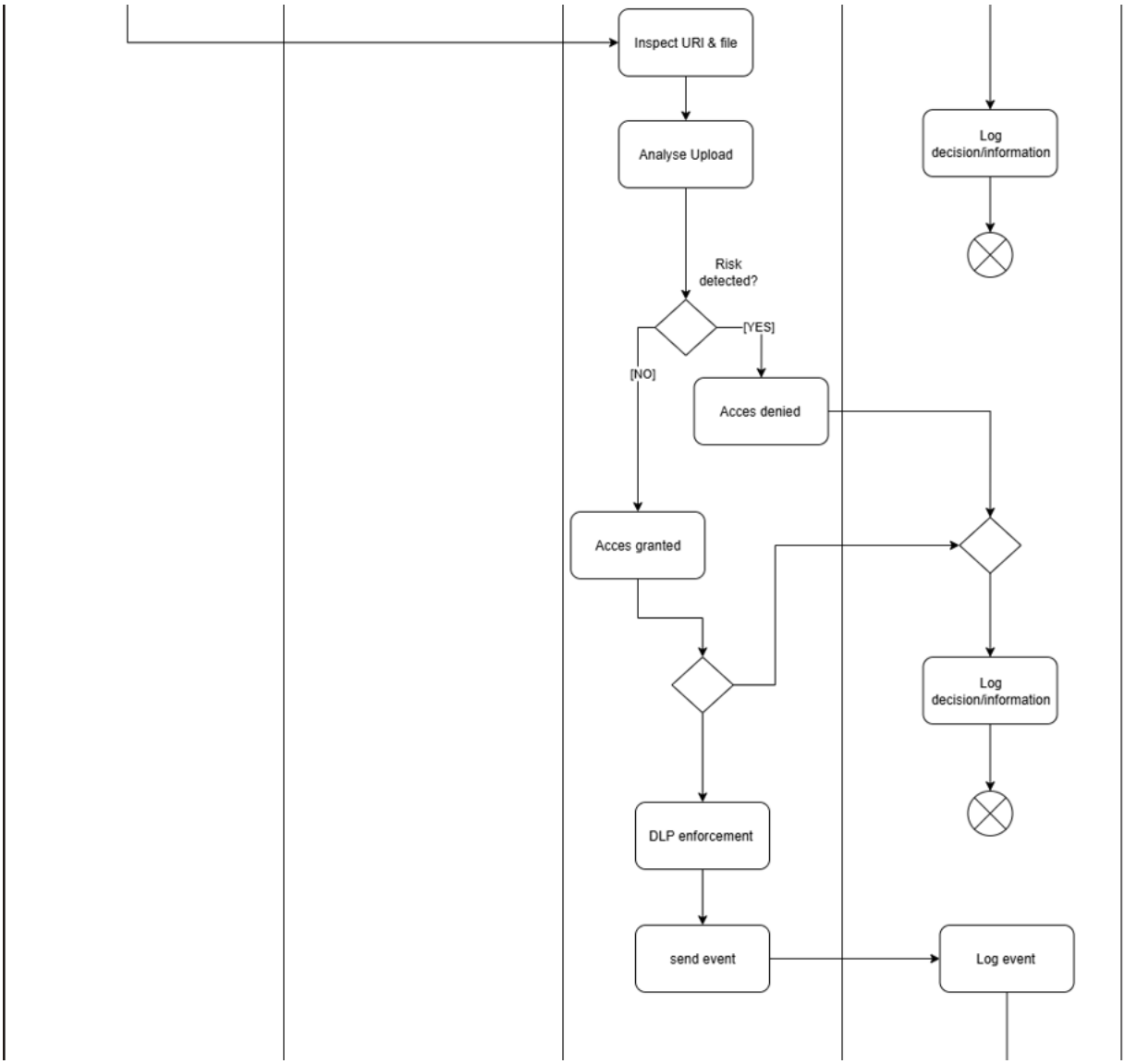
    - Cloudapplicaties openen via CASB, die controleert of de app veilig en toegestaan is.
    - Internettoegang gebruiken via SWG, die al het webverkeer filtert en malware of ongewenste websites blokkeert.
    - Verkeer verzenden via SD-WAN, dat automatisch de meest efficiënte en veilige route kiest.

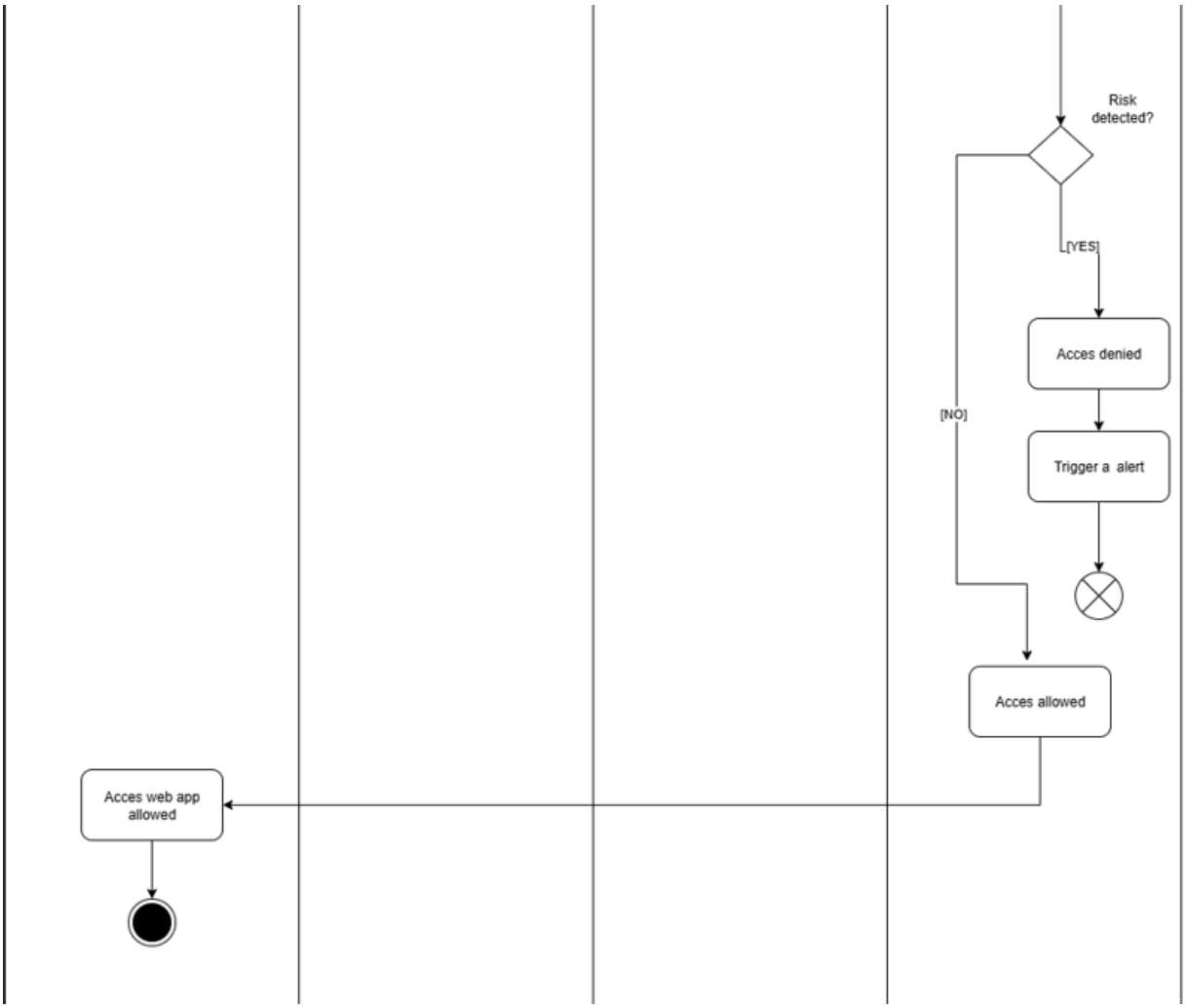
- **Beheerder**
  De beheerder beheert het centrale SASE-platform. Hij kan policies aanmaken, gebruikersrechten beheren en netwerkverkeer opvolgen via het centrale dashboard.
  Hij ontvangt ook waarschuwingen van het systeem bij verdachte activiteiten of blokkeringen.
- **Klant**

  Bezoekt de publieke website.

Activity Diagram




Inspect URI & file
Analyse Upload
Log decision/information
Risk detected?
[YES]
[NO]
Acces denied
Acces granted
Log decision/information
DLP enforcement
send event
Log event



Het activity-diagram beschrijft de volgorde van acties die plaatsvinden wanneer een remote gebruiker verbinding maakt met het netwerk en beveiligd toegang krijgt tot applicaties of het internet.
De activiteiten illustreren de **volledige flow binnen de SASE-architectuur**.

1. **Start – Remote gebruiker wil verbinden**
   De gebruiker opent de verbinding met het SASE-portaal.
2. **Authenticatie via ZTNA**
   Wanneer een gebruiker inlogt, verloopt dit via ZTNA, dat controleert of het apparaat geautoriseerd is en zich niet op een onbevoegde locatie bevindt. Daarnaast wordt Multi-Factor Authentication (MFA) gebruikt om de veiligheid te waarborgen.
   - *Is de authenticatie geldig?*
     - Nee → verbinding wordt geweigerd.
     - Ja → ga verder.
3. **Zero Trust controle**
   Toegang wordt enkel verleend als de gebruiker voldoet aan de context regels.
   Niet-goedgekeurde sessies worden onmiddellijk afgesloten.

4. **CASB-controle op cloudtoepassingen**
   Wanneer de gebruiker een cloudapplicatie opent, controleert de CASB of deze applicatie is toegestaan en of er geen risico is op datalekken of shadow IT.
   - *Is de app veilig en goedgekeurd?*
     - Nee → verbinding geblokkeerd, melding naar beheerder.
     - Ja → verkeer doorgestuurd.

5. **SWG-filtering van webverkeer**
   Al het internetverkeer loopt via de Secure Web Gateway, die malware en ongewenste sites blokkeert en verdachte patronen meldt.
6. **SD-WAN-routing**
   Het netwerkverkeer wordt door SD-WAN automatisch geoptimaliseerd.
   Dit zorgt voor de snelste en veiligste route. Bij storingen wordt automatisch overgeschakeld naar een alternatieve route (failover).
7. **Monitoring en rapportering**
   Alle stappen worden gelogd en weergegeven in het centrale dashboard. De beheerder kan de sessies opvolgen.
8. **Einde**
   De gebruiker werkt in een beveiligde omgeving of krijgt melding van een geblokkeerde sessie.

Functionaliteiten

Component	**Functionaliteit**
ZTNA	Authenticatie via MFA, contextgebaseerde toegang, sessielogging
SWG	Web verkeer filteren, malware detectie, blokkeren van ongewenste sites
CASB	Cloudapplicaties monitoren, data-exfriltratie voorkomen, Shadow IT detecteren
SIEM	Verzamelen van logs uit ZTNA, SWG en CASB
SD-WAN	slimmer routing, failover, bandbreedte optimalisatie

Business rules

Toegangscontrole
Iedereen moet altijd inloggen via ZTNA. De toegang hangt niet gewoon af van een wachtwoord, maar ook van het toestel dat je gebruikt, waar je bent en hoe de sessie verloopt. Zero Trust dus: nooit zomaar vertrouwen.

Cloudapplicaties
We gebruiken alleen de cloudapps die vooraf toegestaan zijn.
CASB houdt een oogje in het zeil, vooral om datalekken te voorkomen en om verdachte dingen sneller op te merken. Shadow IT wordt automatisch tegengehouden en alles wat er gebeurt wordt gelogd.

Webverkeer
Al het internetverkeer gaat via het SWG. Dat zorgt ervoor dat malware of ongewenste sites er niet zomaar doorkomen. Als een website onveilig is of niet is toegestaan, wordt die gewoon meteen geblokkeerd.

Netwerkbeheer
SD-WAN zorgt voor slimme routing, zodat het netwerk niet onnodig traag wordt.
Als er iets uitvalt, schakelt het systeem automatisch over (failover).
Alle prestaties en incidenten worden doorgestuurd naar één centraal dashboard.

Beleid en compliance
De security regels zijn overal hetzelfde, ongeacht waar iemand zit of welke app er gebruikt wordt.
Als er iets aan het beleid verandert, moet dat centraal worden gedocumenteerd en eerst goedgekeurd.

Monitoring en logging
Alles wat gebruikers doen, en wat er op apps of het netwerk gebeurt, wordt standaard gelogd.
Als er iets verdacht is, markeert het systeem dat automatisch zodat het kan worden onderzocht.

Breakouts en prestaties
Voor mobiele gebruikers gaat het internetverkeer direct naar de cloud of het internet (breakout).
Het is wel belangrijk dat de SASE-oplossing de snelheid van het netwerk of de cloudapps niet vertraagt.

Schaalbaarheid en onderhoud
Het systeem moet makkelijk kunnen meegroeien als er nieuwe gebruikers of locaties bij komen.
De PoC en de blueprint zijn enkel voor het ontwerp en om te testen. Serverbeheer en training van gebruikers horen daar niet bij.

D. Technisch design

a) Architectuur

[Beschrijf de voorgestelde architectuur (HOE gaan we het bouwen?]

[Een voorbeeld van een architectuur kan zijn: Database-Firewall-Applicatieserver-Frontend)]

Gebruiker/device *→ logt in via* ***ZTNA/OpenZiti*** *→ Zero Trust check, MFA, apparaat & locatietest*

SD-WAN Edge (FlexiWAN) *→ routeert verkeer slim naar PoP(Point of Presence), datacenter of cloud*

FWaaS (pfSense/OPNsense) *→ inspectie, filtering en policy enforcement*

SWG *→ controleert webverkeer, blokkeert malware en ongewenste sites*

IDS/IPS (Suricata) *→ detecteert aanvallen of verdachte patronen*

Monitoring/Dashboard *(wazuh)→ verzamelt logs, toont alerts en performance metrics*

b) Integraties

[Beschrijf de eventuele integraties met (externe) systemen, omschrijf zowel de input data als output data. Bv. bij een API, DFD, ...]

Binnen het project gebruiken we een full SASE-architectuur . Hieronder vindt je SASE onderdelen met hun input en output data.

SD-WAN:

Het netwerkverkeer wordt via SD-WAN-edges naar de cloud-SASE-omgeving gestuurd voor optimalisatie en beveiliging.

-INPUT:

- *applicatievekeer*
- *qos en routing configuratie*

-OUTPUT:

- *latency, packetloss*
- *Routing & path selection data*

FWaaS:

Het systeem gebruikt SASE's cloud-gehoste firewall voor netwerkbeveiliging.

-INPUT :

- *Verkeer (IP, poort, protocol)*
- *Firewall- en segmentatieregels*

-OUTPUT:

- *Allowed/denied logs*
- *Threat detection events*
- *Session data*

Secure Web Gateway (SWG)

Het internetverkeer wordt gefilterd via de Secure Web Gateway.

-INPUT:

- *HTTP/HTTPS-verkeer*
- *Security policies (webfiltering, malwarefilters)*

-OUTPUT:

- *Toegangverdicts (toegestaan/geblokkeerd)*
- *URL-classificatie*

CASB:

Een CASB bewaakt en controleert het gebruik van cloudapplicaties, detecteert risico's en policy-overtredingen, en beschermt zo gevoelige data in de cloud.

-INPUT:

- *bestanden en data*
- *gebruikersinformatie*
- *API-logdata*
- *Cloud-applicatie-activiteiten*

-OUTPUT:

- *beslissingen*
- *alerts*
- *logs*
- *DLP-events (DLP = Data loss Prevention)*
- *risicoscores*

DLP:

CASB is het primaire DLP-systeem binnen de SASE-architectuur: het detecteert en blokkeert ongeautoriseerde toegang tot gevoelige cloud data en rapporteert overtredingen.

ZTNA (met breakout):

ZTNA verleent veilige toegang tot applicaties op basis van identiteit en context, en voert breakout uit door verkeer direct naar cloud- of internetservices te routeren wanneer toegestaan.

-INPUT:

- *gebruikersinfo*
- *device-status*
- *toegangsaanvraag*
- *policies*
- *breakout-context*

-OUTPUT:

- *toegangsbeslissingen*
- *logs*
- *security alerts*
- *breakout-routing*

c) Technologie

[Beschrijf de voorgestelde technologie en onderbouw de keuze met argumenten.Zoek voor elk van de componenten in de architectuur minimaal 2 opensource-oplossingen.f

HIER IS ZIEN OM TE ZEGGEN WAAROM WE DIE OPENS_SOURCE TOOL GEBRUIKEN

1. FWaaS (pfSense vs. OPNsense)

Firewall as a Service (FWaaS) is een cloudgebaseerde firewall-oplossing die fysieke hardware overbodig maakt. Bij de vergelijking tussen pfSense en OPNsense is gekeken naar stabiliteit, community-ondersteuning, functionaliteiten en gebruiksgemak.

- *pfSense: Beschikt over een volwassen community en uitgebreide documentatie. De updates zijn minder frequent, maar zeer stabiel, wat het risico op downtime in enterprise-omgevingen verlaagt. Het is de standaard voor core routing en VPN-oplossingen.*

- *OPNsense: Biedt een modernere interface, flexibel pluginbeheer en snellere security-updates (wekelijks). De integratie met Suricata IDS/IPS is intuïtiever, wat het aantrekkelijk maakt voor gebruikers die de nieuwste features zoeken.*

Conclusie: *Wij kiezen voor pfSense. De bewezen stabiliteit en de enorme hoeveelheid beschikbare praktijkvoorbeelden maken implementatie en troubleshooting*

betrouwbaarder. Voor onze PoC is deze robuustheid cruciaal voor de basisfeatures (VPN, NAT, DHCP).

2. ZTNA (OpenZiti vs. Pritunl Zero)

Zero Trust Network Access (ZTNA) hanteert het principe dat geen enkele gebruiker of apparaat standaard wordt vertrouwd, ongeacht de locatie in het netwerk. Toegang wordt strikt verleend op basis van identiteit en context.

- *OpenZiti: Een volledig open-source stack die zero-trust op applicatieniveau toepast via SDK's. Dit stelt ontwikkelaars in staat om beveiliging rechtstreeks in de code te verweven, waardoor het onzichtbaar wordt voor het publieke internet.*
- *Pritunl Zero: Een gebruiksvriendelijke oplossing die sneller op te zetten is voor kleinere teams. Het blinkt uit in out-of-the-box integraties met Identity Providers zoals Google en Okta (SSO/MFA).*

***Conclusie:** De keuze valt op OpenZiti. De mogelijkheid om zero-trust via SDK's direct in applicaties te integreren biedt een superieur beveiligingsniveau en voorkomt vendor lock-in bij commerciële partijen.*

3. SD-WAN (flexiWAN)

Software-Defined Wide Area Network (SD-WAN) optimaliseert en beveiligt het verkeer tussen verschillende locaties, datacenters en de cloud via een centrale softwarelaag.

Hoewel OpenZiti en Pritunl Zero raakvlakken hebben met netwerkbeheer, biedt flexiWAN een specifieke open-source benadering voor SD-WAN.

***Conclusie:** Wij integreren flexiWAN. Het is modulair, vereist geen diepgaande SDN-kennis en is specifiek ontworpen om snel inzetbaar te zijn binnen een SASE-architectuur (Secure Access Service Edge) voor kleine tot middelgrote omgevingen.*

4. SWG (BunkerWeb vs. SafeLine WAF)

Een Secure Web Gateway (SWG) filtert al het uitgaande webverkeer om malware, phishing en ongeoorloofd websitebezoek tegen te gaan.

- *BunkerWeb: Werkt als een realtime filter dat downloads sandboxed en beleid (policies) afdwingt op basis van websitecategorieën. Het is volledig open-source en biedt uitgebreide monitoring-dashboards.*

- *SafeLine WAF: Is primair een Web Application Firewall. De focus ligt hier op het beschermen van inkomend verkeer (zoals SQL-injecties en XSS) in plaats van het controleren van het surfgedrag van gebruikers.*

***Conclusie**: BunkerWeb is de geselecteerde oplossing. Het sluit nauwer aan bij de definitie van een SWG door de focus op verkeersfiltering en sandboxing, wat essentieel is voor een veilige SASE-stack.*

5. SIEM/SOAR + AI

Voor de centrale loganalyse en automatische incidentrespons (SIEM/SOAR) zijn twee paden onderzocht:

- *Wazuh met externe AI (OpenAI API): Wazuh fungeert als logverzamelaar, waarna externe AI-modellen patronen en anomalieën analyseren. Dit is uiterst flexibel, maar vereist maatwerk (Python-scripts/API-koppelingen) en brengt lichte latency met zich mee.*

- *ELK Stack met Elastic ML: Een alles-in-één platform waarbij Elastic Machine Learning direct anomaliedetectie uitvoert op de verzamelde data. Dit is sneller, maar vereist aanzienlijke hardwarebronnen (RAM/CPU).*

***Conclusie:** We kiezen voor Wazuh in combinatie met externe AI. Deze setup biedt de meeste vrijheid om specifieke AI-algoritmes te testen, wat essentieel is voor de leerdoelen van deze PoC.*

6. CASB (ELK vs. Osquery)

Een Cloud Access Security Broker (CASB) beveiligt het gebruik van cloudapplicaties en detecteert 'Shadow IT' en datalekken (DLP).

- *ELK Stack: Kan logs van SaaS-apps (zoals Microsoft 365 of Google Workspace) centraal aggregeren en via Machine Learning ongebruikelijk gedrag detecteren.*

- *Osquery: Richt zich op telemetrie van het eindpunt (endpoint). Hoewel krachtig voor apparaatinzicht, biedt het onvoldoende direct zicht op cloudverkeer en SaaS-transacties.*

Conclusie: *ELK wordt ingezet als CASB-oplossing vanwege de mogelijkheid om logdata van diverse cloudplatformen te correleren aan beveiligingsincidenten in één dashboard.*

7. DLP (OpenDLP vs. MyDLP)

Data Loss Prevention (DLP) voorkomt dat gevoelige informatie het netwerk verlaat.

- *OpenDLP: Uitstekend voor het scannen van 'data-at-rest' (opgeslagen bestanden en databases) voor compliance-audits zoals GDPR. Het mist echter krachtige realtime blokkeringsfuncties.*
- *MyDLP (Community Edition): Focust op 'data-in-motion'. Het kan actief web-, e-mail- en USB-verkeer monitoren en blokkeren voordat een datalek optreedt.*

Conclusie: *De keuze is MyDLP. Binnen een SASE-architectuur is de bescherming van bewegende data (realtime blokkering) de hoogste prioriteit om de veiligheid van de cloudomgeving te waarborgen.*

[Samengevat: Hier komt dus een vergelijkend onderzoek tussen componenten met uiteindelijke keuzes die duidelijk geargumenteerd zijn.]

d) Impact op de huidige infrastructuur

[Beschrijf de vereiste infrastructuur. Dienen er servers aangekocht te worden, geherinstalleerd, of gewijzigd? Worden er andere systemen in het landschap voorzien of verwijderd? Wat zijn de kosten hierbij? Indien de infrastructuur niet wijzigt, graag een beschrijving van de huidige situatie]

Huidige infrastructuur

De huidige omgeving bestaat nog altijd uit Next-Generation Firewalls, IPS-systemen, anti-malware, sandboxing, webfiltering en de SD-WAN-verbindingen. We gebruiken de bestaande virtualisatie-omgeving. Er moeten geen nieuwe fysieke servers aangekocht worden. We voegen enkel extra virtuele machines toe voor de open-source componenten. Vandaag loopt al het verkeer, ook van remote gebruikers, verplicht via het datacenter. Dat veroorzaakt omwegen, trage cloudtoegang en extra belasting op VPN en firewalls.

Nieuwe componenten

Binnen de bestaande virtuele infrastructuur worden een aantal extra open-source componenten toegevoegd. Het gaat onder andere om:

- pfSense / OPNsense voor Firewall-as-a-Service (FWaaS)
- FlexiWAN voor SD-WAN-beheer en dynamische routing
- OpenZiti voor ZTNA en context gebaseerde toegangscontrole

- Suricata voor IDS/IPS-detectie van verdacht netwerkgedrag
- Wazuh en de ELK-stack voor centrale logging, monitoring en AI-ondersteunde analyses

Deze tools worden uitgerold op virtuele servers of aparte test-VM's binnen de huidige omgeving. Er moet niets opnieuw geïnstalleerd worden, de bestaande systemen blijven staan. Het enige dat nodig is, zijn configuratie-aanpassingen en integratie in het huidige netwerklandschap.

Beheer en beleid

De grootste wijziging situeert zich op beheer- en beleidsniveau. Alle security policies en toegangsrechten worden voortaan gecentraliseerd via één cloud gebaseerd platform. Hierdoor verdwijnt de versnippering van regels over verschillende firewalls en VPN-oplossingen, en ontstaat een uniform beveiligingsbeleid voor alle gebruikers, locaties en applicaties.

Kostenimpact

e) Analyse van security

[Beschrijf de methode en aanpak van de security. Welke stappen ga je nemen om je systeem zelf te beschermen? Als het om een externe component gaat, leg dan uit hoe het extern platform dit aanpakt.]

Om het systeem te beschermen, wordt een gelaagde aanpak gehanteerd die zowel interne als externe componenten omvat:

FWaaS (pfSense)

a. Beschermt netwerkverkeer, voert firewalling, NAT, VPN en policy enforcement uit.
b. Updates en patches worden volgens een gepland schema uitgevoerd om kwetsbaarheden te minimaliseren.

ZTNA (OpenZiti)

c. Toegang wordt verleend op basis van identiteit, context en apparaatstatus.
d. Multi-Factor Authentication (MFA) en sessielogging zorgen dat alleen geautoriseerde gebruikers toegang krijgen.

SD-WAN (FlexiWAN)

e. Optimaliseert netwerkverkeer en voert failover uit bij storingen, zodat beschikbaarheid gegarandeerd blijft.

SWG (BunkerWeb / SafeLine WAF)

f. Filtert webverkeer, blokkeert malware, phishing en ongeautoriseerde sites.

DLP – OpenDLP (Data Loss Prevention)

- Scant endpoints, bestanden en databases op gevoelige informatie (PII, credentials, financiële data).
- Blokkeert of logt pogingen om data te kopiëren, up te loaden of extern te delen.
- Policies bepalen welke data niet mag verlaten (GDPR compliance).
- Integreert met SIEM voor realtime incidentmelding.

SIEM + AI (Wazuh + AI API)

g. Verzamelt logs van alle componenten en voert anomaliedetectie uit.
h. AI detecteert verdacht gedrag en genereert alerts voor de beheerder.

◦ *Welke security-risico's loopt de oplossing die jullie aan het bouwen zijn?*
▪ *Hoe kan de CIA (Confidentialiteit, Integriteit en Availability oftewel beschikbaarheid in gevaar komen ?*
▪ *Maak hiervoor een risico-analyse en een plan-van-aanpak hoe je met deze risico's gaat omgaan.*

- *Penetratietesten: simuleren van aanvallen op ZTNA, SWG en FWaaS.*
- *Anomalie Detectie testen: injecteren van onregelmatige patronen in logs om AI-detectie te controleren.*
- *Failover testen: SD-WAN en FWaaS redundanties controleren bij storingen.*
- *Policy compliance testen: controleren of security policies consistent worden toegepast.*

▪ *Hoe ga je de veiligheid van je applicatie testen ?*

- ***Penetratietesten:** simuleren van aanvallen op ZTNA, SWG, en FWaaS.*
- ***Anomalie Detectie testen:** door AI onregelmatige patronen injecteren in logs om detectie te controleren.*
- ***Failover testen:** SD-WAN en FWaaS redundanties controleren bij storingen.*
- ***Policy compliance:** controleren of uniforme security policies consistent worden toegepast.*

Worden er persoonsgegevens verwerkt?

ja, er worden persoonsgegevens verwerkt , zoals:

- *identiteitsgegevens van gebruikers (naam,e-mail)*
- *Eventueel gevoelige bedrijfsdata (credentials,financiële data)*

f) Autorisatierollen

[Beschrijf de verschillende autorisatierollen en wat ze kunnen in het systeem. Gebruik hiervoor een matrix]

In dit project worden vier autorisatierollen gebruikt. Elke rol heeft duidelijk afgebakende rechten binnen de SASE-omgeving. Dit zorgt ervoor dat gebruikers enkel de functies kunnen uitvoeren die voor hun taak noodzakelijk zijn (principle of least privilege).

Remote Gebruikers

Remote gebruikers maken via het SASE-platform verbinding met cloudapplicaties, interne applicaties en het internet. Zij kunnen inloggen via ZTNA en gebruiken het systeem uitsluitend als eindgebruiker. Ze hebben geen toegang tot configuratie-instellingen of beheertaken.

Beheerders

Beheerders staan in voor het functionele beheer van de volledige SASE-omgeving. Zij beheren security policies, toegangsrechten, monitoring, logging en incidentopvolging. Ze werken op applicatieniveau binnen CASB, SWG, ZTNA, SD-WAN en het centrale dashboard. Ze voeren geen systeem- of infrastructuurtaken uit.

System Administrators

System Administrators beheren de infrastructuur waarop de SASE-oplossing draait. Zij staan in voor het installeren, configureren en onderhouden van servers, VM's, netwerkcomponenten (pfSense, FlexiWAN), monitoringservers (Wazuh) en andere achterliggende systemen. Ze passen geen security policies, gebruikersrechten of compliance-regels aan.

Klanten

Klanten kunnen enkel de publieke website raadplegen. Zij hebben geen toegang tot het SASE-platform of interne systemen.

Verschil tussen Beheerders en System Administrators

De Beheerder werkt volledig binnen het SASE-platform. Hij houdt zich bezig met zaken zoals policies, toegangsrechten, monitoring en beveiligingsinstellingen. Hij raakt de onderliggende infrastructuur niet aan en voert geen systeemwijzigingen uit.

De System Administrator beheert de technische omgeving waarop SASE draait. Dit omvat de virtuele machines en componenten zoals pfSense, FlexiWAN en Wazuh. Hij werkt op systeem- en netwerkniveau, maar verandert geen security policies, gebruikersrechten of toegangsbepalingen.

Functionaliteit/ Component	Remote Gebruikers	Beheerders	System-Administrator	Klanten
Publieke Website raadplegen	✅	✅	✅	✅

Inloggen op SASE-portaal	✓	✓	✓	✗
Toegang tot interne applicaties	✓	✓	✗	✗
Toegang tot dashboard / monitoring	✗	✓	✓	✗
Gebruikers-en rollenbeheer	✗	✓	✗	✗
Bekijken security logs en alerts	✗	✓	✗	✗
Behandelen van security incidenten	✗	✓	✗	✗
Installatie, updates en onderhoud van SASE-componenten	✗	✗	✓	✗
Beheer van VM's, servers, netwerkconfiguratie en back-ups voor de PoC-omgeving	✗	✗	✓	✗
Wijziging van securitybeleid / compliance-regels	✗	✓	✗	✗

E. Risicoanalyse (Algemeen en Security)

[Beschrijf risico's aan de hand van probabiliteit, hun impact, …]

Binnen de toekomstige SASE-architectuur worden zowel netwerk- als securityfuncties gecentraliseerd in één cloudgebaseerd platform. Hierdoor ontstaan nieuwe risico's op vlak van configuratie, beschikbaarheid, beleidsbeheer en databeveiliging. In deze risicoanalyse worden alle relevante risico's beoordeeld op Probability (P) en Impact (I) volgens een schaal van 1–10, waarna de PI-index wordt berekend.

Nr.	Risk	Probability	Impact	PI-index	Beschrijving	Mitigerende acties
1	Misconfiguratie van SASE-componenten	7	8	56	Foutieve policies in ZTNA, CASB of SWG kunnen toegang blokkeren of te veel toelaten.	Testomgeving gebruiken
2	Verliest van connectiviteit bij overgang van VPN naar ZTNA	4	9	36	Gebruikers kunnen tijdelijk geen toegang krijgen bij omschakeling	Gefaseerde migratie per gebruikersgroep, fallback-VPN voorzien, uitgebreide communicatie.
3	Security-lek in open-source software	4	9	36	Kwetsbaarheid in een component kan worden misbruikt.	Regelmatige updates en patchmanagement
4	Conflicterende policies tussen legacy en nieuwe SASE-regels	6	6	36	Overlapping tussen NGFW, SWG, CASB, ZTNA kan legitiem verkeer blokkeren.	Policy-consolidatie, documentatie, audit van bestaande regels, centraal beheer.
5	Onvoldoende logging of verkeerde interpretatie van AI-alerts	4	8	32	SIEM-regels testen; AI-alerts valideren met handmatige analyse	Handmatige validatie, tuning van AI-regels, detectie-tests, alert-triageproces.
6	beschikbaarheid van de PoC-omgeving	3	7	21	Overbelasting van VM's of crashes kunnen testresultaten beïnvloeden.	Back-ups van virtuele machines & voldoende CPU/RAM toewijzen
7	Foutieve integratie tussen verschillende SASE-componenten	3	7	21	integratie kan mislukken, waardoor inconsistent gedrag ontstaat.	Integratietesten, standaardconfiguraties, duidelijke API-documentatie.

Probability & Impact: Scale between 1-10
PI-index: Probability x Impact

F. Documentatie

[Welke documentatie plan je te maken (van configuratie, in code, gebruikershandleiding, …)? Geef een overzicht van de verschillende soorten documentatie. Argumenteer en beschrijf telkens je doelpubliek.]

Binnen dit project wordt alle documentatie opgesplitst in vier duidelijke categorieën:

- **technische documentatie**
- **functionele documentatie**
- **beheer documentatie**
- **gebruikersgerichte documentatie**.

1. Technische documentatie

Doelpubliek:
System engineers, netwerkbeheerders, security administrators, lectoren en toekomstige teams die de Proof of Concept of volledige SASE-omgeving willen reproduceren.

Doel:
Dit document is bedoeld om alles wat nodig is om de SASE-omgeving op te zetten, uit te leggen. Van installatie en configuratie tot monitoring en onderhoud zodat engineers het systeem precies kunnen opbouwen en gebruiken, zonder dat ze constant hoeven te raden wat er bedoeld wordt.

Inhoud:

- **Architectuurdocument**
- **Installatiehandleidingen**
- **PoC-documentatie**
- **CLI-referentie & API-overzicht**
- **Netwerkconfiguratie**

Waarom dit document bestaat:
Het idee is dat iemand dit document kan volgen en de hele SASE-oplossing kan opzetten of aanpassen, zelfs zonder dat de originele projectgroep erbij betrokken is. Alles staat duidelijk uitgelegd zodat engineers snel kunnen debuggen, uitbreiden of opschalen.

2. Functionele documentatie

Doelpubliek:
Security officers, IT-managers, projectleiders, auditors, lectoren en interne stakeholders.

Doel:
Uitleggen *wat* het systeem doet en *waarom* bepaalde keuzes gemaakt zijn. Deze documentatie ondersteunt audits, risico-analyses, beleidsafspraken en strategische beslissingen.

Inhoud:

- ★ **Use-case documentatie**
- ★ **Activity-diagrammen**
- ★ **Business rules** (Zero Trust policy, cloudaccess policies, DLP-regels)
- ★ **Securitybeleid**
  - ZTNA-verplicht MFA
  - App-based toegangsregels
  - SWG-categorieën
  - CASB-policy-violations
- ★ **Risicoanalyse + PI-index**
- ★ **TO-BE architectuurvisie**
  - Waarom SASE
  - Waarom open-source
  - Waarom breakout
- ★ **Autorisatierollen + matrix**

Waarom dit document bestaat:
Functionele documentatie is nodig voor beleidsmakers en security-teams die moeten begrijpen hoe de SASE-oplossing werkt, welke risico's bestaan en welke regels/afspraken moeten worden nageleefd.

3. Beheer Documentatie

Doelpubliek:
Beheerders die de omgeving dagelijks zullen monitoren, bijsturen of incidenten opvolgen.

Doel:
Het bieden van richtlijnen voor onderhoud, updates, back-ups en incident respons met betrekking tot de SASE-architectuur.

Inhoud:

- ★ **Dagelijkse beheertaken**
- ★ **Incident Response Plan**
- ★ **Backup- en herstelprocedures**
- ★ **Update- & patchmanagement**
- ★ **Monitoring Richtlijnen**

Waarom dit document bestaat:
Deze documentatie zorgt ervoor dat het beheer veilig, gestructureerd en herhaalbaar verlopen kan. Het voorkomt fouten, downtime en misconfiguraties, risico's die ook naar voren komen in jullie risicoanalyse.

4. Gebruikersgerichte documentatie

Doelpubliek:
Eindgebruikers: remote medewerkers, interne werknemers, eventueel partners.

Doel:
Helpen bij het veilig en correct gebruiken van het platform zonder technische voorkennis.

Inhoud:

III. **Handleiding "Hoe aanmelden via ZTNA"**
   A. Eerste keer inloggen
   B. Hoe MFA werkt
   C. Hoe problemen te melden

IV. **Cloudapplicatie-toegang**
   A. Wat mag wel / niet volgens CASB-policy

V. **Internetgebruik via SWG**

VI.
   A. Uitleg waarom bepaalde sites geblokkeerd zijn
   B. Omgang met downloads

VII. **FAQ voor remote workers**

   A. "Waarom werkt mijn VPN niet meer?"
   B. "Waarom moet ik MFA doen?"
   C. "Waarom is mijn site geblokkeerd?"

VIII. **Security-awareness mini-gids**

A. Phishing
B. Shadow IT
C. Veilig omgaan met bedrijfsdata

Bronvermelding

[Vermeld hier al je bronnen volgens de APA-stijlgids (https://apastyle.apa.org/). Denk eraan dat elk brontype (website/rapport/wetenschappelijk artikel/hoofdstuk uit boek/…) zijn eigen stijl heeft.]

[1] Jan, A. (2023-04-12). De titel van deze pagina. Opgehaald van http://xxxxxxxxx.

Chaitin, A. (z.d.). *SafeLine WAF – Web Application Firewall*. Opgehaald van https://github.com/chaitin/SafeLine

Elastic, A. (z.d.). *Elastic Stack (ELK): Elasticsearch + Logstash + Kibana*. Opgehaald van https://www.elastic.co/elastic-stack Elastic

Osquery Project, A. (z.d.). *osquery – operating system instrumentation framework*. Opgehaald van https://osquery.io/ osquery.io

Zorz, M. (2024, 4 december). *SafeLine: Open-source web application firewall (WAF)*. Help Net Security. https://www.helpnetsecurity.com/2024/12/04/safeline-open-source-web-application-firewall-waf/

BunkerWeb. (z.d.). *BunkerWeb – open-source web application firewall* [Webpagina]. https://www.bunkerweb.io/

Zenarmor. (z.d.). *pfSense – What is it?* [Network security tutorial]. https://www.zenarmor.com/docs/network-security-tutorials/pfsense

OPNsense. (z.d.). *Introduction* [Documentation]. https://docs.opnsense.org/intro.html

Pritunl. (z.d.). *Authenticated Web VSCode Server* [Knowledge base article].Pritunl. https://docs.pritunl.com/kb/zero/general/zero-vscode-web

OpenDaylight. (z.d.). *About OpenDaylight*. https://www.opendaylight.org/about

NetFoundry.(z.d.).*OpenZiti:Features*.NetFoundry. https://netfoundry.io/docs/openziti/learn/introduction/features

OpenAI. (2025, 11 november). ChatGPT 5 [Large language model]. https://chat.openai.com/

FlexiWAN.(z.d.). *SD-WAN open source*. FlexiWAN. https://flexiwan.com/sd-wan-open-source/