CCS Project Concept & Analyse Rapport Skills 2/2

Beschrijving van het probleem

De klant wilt een platform om een webapplicatie te hosten. Deze applicatie bedient 20-40 gebruikers in pieken. Op deze momenten dient de applicatie vlot beschikbaar te zijn.

Toepassingsgebied van het project

Hier worden de grenzen onderscheid van wat het bedrijf zeker zal implementeren, alsook wat er mogelijk is. De implementaties van wat er out of scopes is worden op het einde vermeld.

Must have: Applicatie op een platform, security, SFTP-server, PHP ondersteunen

Should have: Gitlab, java ondersteunen, Logging dashboard voor admins, automatisatie

Could have: logging dashboard voor klant

Won't have: eigen website (wij maken geen websites voor de klant)

Stakeholder analyse

Alle individuen of groepen die interesse hebben in het project, zullen geïdentificeerd worden. Er is een overzicht over hun rollen en verantwoordelijkheden.

Er zijn 3 belangrijke stakeholders. De klanten zelf, eindegebruikers en het development team vertegenwoordigen deze stakeholders.

Het ontwikkelingsteam zorgt voor een beveiligd platform waar klanten hun applicatie op kunnen hosten. Er wordt sterk ingezet op security. Het bedrijf neemt hierin de rol op zich door hun expertise toe te passen. Hierdoor zijn zij verantwoordelijk voor het veilig opzetten van deze infrastructuur.

De klanten profiteren van sterke beveiliging, aangeboden door het hostingplatform. Door een efficiënte workflow en gestroomlijnde implementatie processen, kunnen zij zich extra focussen op de ontwikkeling van hun applicatie. Zo is de enige verantwoordelijk van de klant zijn eigen webapplicatie voorzien en onderhouden.

De eindgebruikers hebben als voordeel dat ze op een zeer beveiligde omgeving terecht komen. Zo zijn ze beveiligd van mogelijke risico's die hun, of hun systeem, in gevaar kunnen brengen zonder hier zelf verantwoordelijk voor te zijn.

Analyse van de behoeften

Functionele eisen

Er worden functionele eisen gespecificeerd wat het systeem moet doen, door gebruik te maken van een lijst van alle functionaliteiten die het systeem moet uitvoeren.

- **Hosting van web applicaties:** Het platform moet een web applicatie kunnen hosten.
- **Accountmanagement:** Klant moet een account kunnen aanmaken.
- **Beheer van domeinen:** Het bedrijf beheert alle domeinen.
- **Geautomatiseerde backups:** Het systeem automatisch en op vraag backups.
- **Git-Integratie:** Het systeem voorziet integraties voor Git

Niet-functionele eisen

Er worden niet-functionele eisen bepaald hoe het systeem een functie vervult. Dit omvat beperkingen en kwaliteiten zoals beveiliging, betrouwbaarheid en prestaties.

- **Overdraagbaarheid:** Eenvoud voor de klant om te wisselen van hosting provider
- **Efficiency:** Het systeem wordt voorzien van shared hosting zodat dit door meerdere gebruikers gebruikt kan worden
- **Betrouwbaarheid:** Het systeem is betrouwbaar en voldoet aan de security vereisten
- **Beschikbaarheid:** Automatisch schalen om piekbelasting van het verkeer aan te kunnen zonder handmatige tussenkomst.

Analyse van beveiligingsrisico's

Identificatie van top assets

Hier wordt er geïdentificeerd wat het meest moet worden beschermd, zoals gegevens, systemen of services.

Wat moet er beschermd worden:

- Persoonsgegevens van gebruikers
- Hardware (servers in het datacenter)
- Netwerk
- Configuratie van servers
- Configuratie van applicaties

Onderstaand vindt u een threat model terug. Hierin wordt beschreven welk dreigingsscenario er is en welke maatregels er hiervoor ondernomen worden. Bijkomend wordt er een graad van waarschijnlijkheid (hoe vaak komt dit voor?), risico en impact toegevoegd volgend volgde waarde:

Kritiek	Hoog	Gemiddeld	Laag	INFO
Zeer hoog risico	Hoog risico	Risico	Weinig tot geen risico	Geen risico's

Dreigingsscenario	**Waarschijnlijkheid**	**Impact**	**Risico**	**Maatregelen voor risicobeperking**
Datalek	Gemiddeld	Hoog	Hoog	Geëncrypteerde databse.
Service downtime	Laag	Gemiddeld	Gemiddeld	HA op Proxmox en in K8 cluster
Malware	Hoog	Hoog	Hoog	Crowdsec tool voor continuous vulnerability management
Disaster Recovery	Laag	Kritiek	laag	Extra NAS Backups en configuratie op git.

Het concept

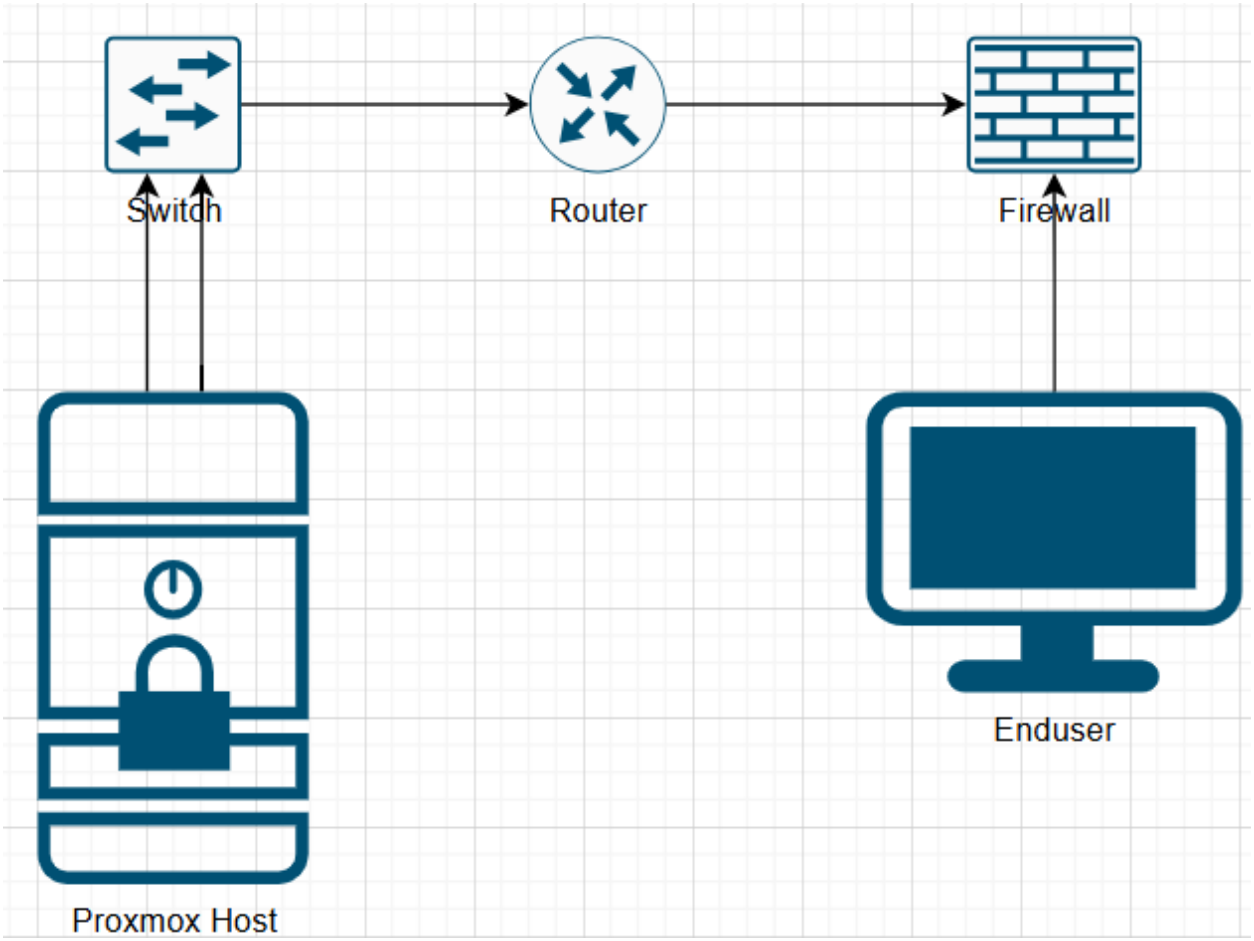
De klant heeft nood aan een platform waar hij zijn applicatie op kan hosten. Het bedrijf biedt zijn expertise in het voorzien een van beveiligd en secure hostingplatform. Aan de hand van de CIS control wordt er security geïmplementeerd, alsook andere frameworks zoals het OWASP model en tools zoals Crowdsec en Grafana Loki.

Op een Proxmox server zal er een virtuele management machine voorzien worden die de andere machines en services zal opstarten, naar wens van de klant. Er wordt een NAS voorzien voor alle opslag. Bijkomend wordt er een 2de NAS voorzien ter backup.

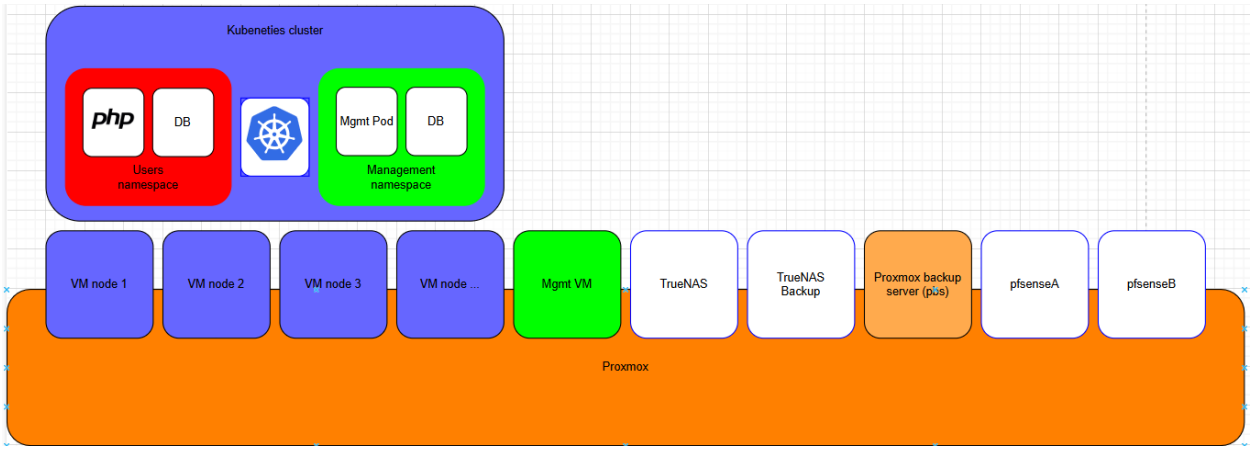
Per klant zal er een aparte pod/pods voorzien worden in een Kubernetes cluster. Deze zal de gepersonaliseerde stack per klant draaien.

Definitief conceptontwerp

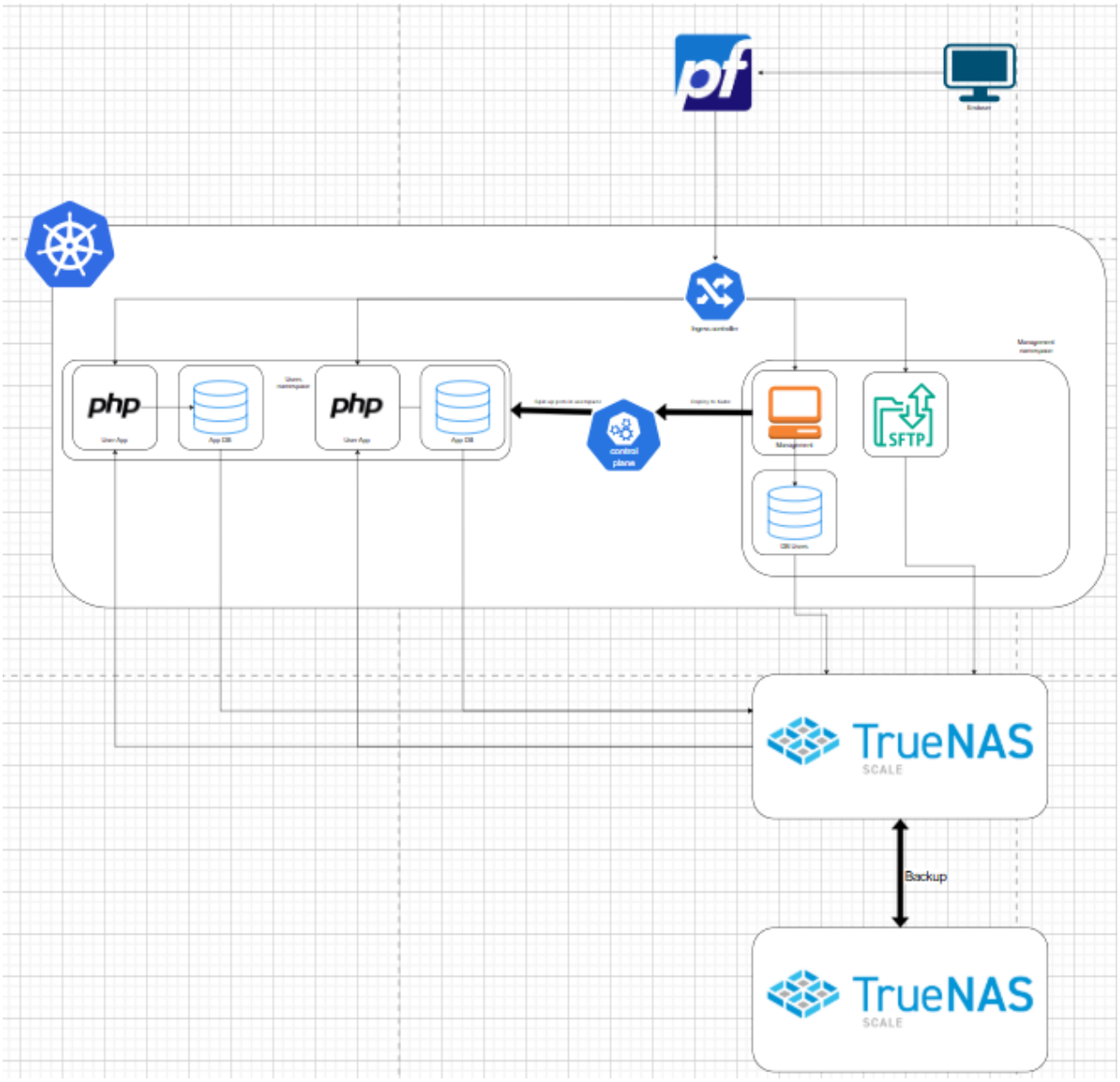
Fysiek design



Virtueel design



Logic design



Testplan

Dit onderdeel dient nog aangevuld te worden.