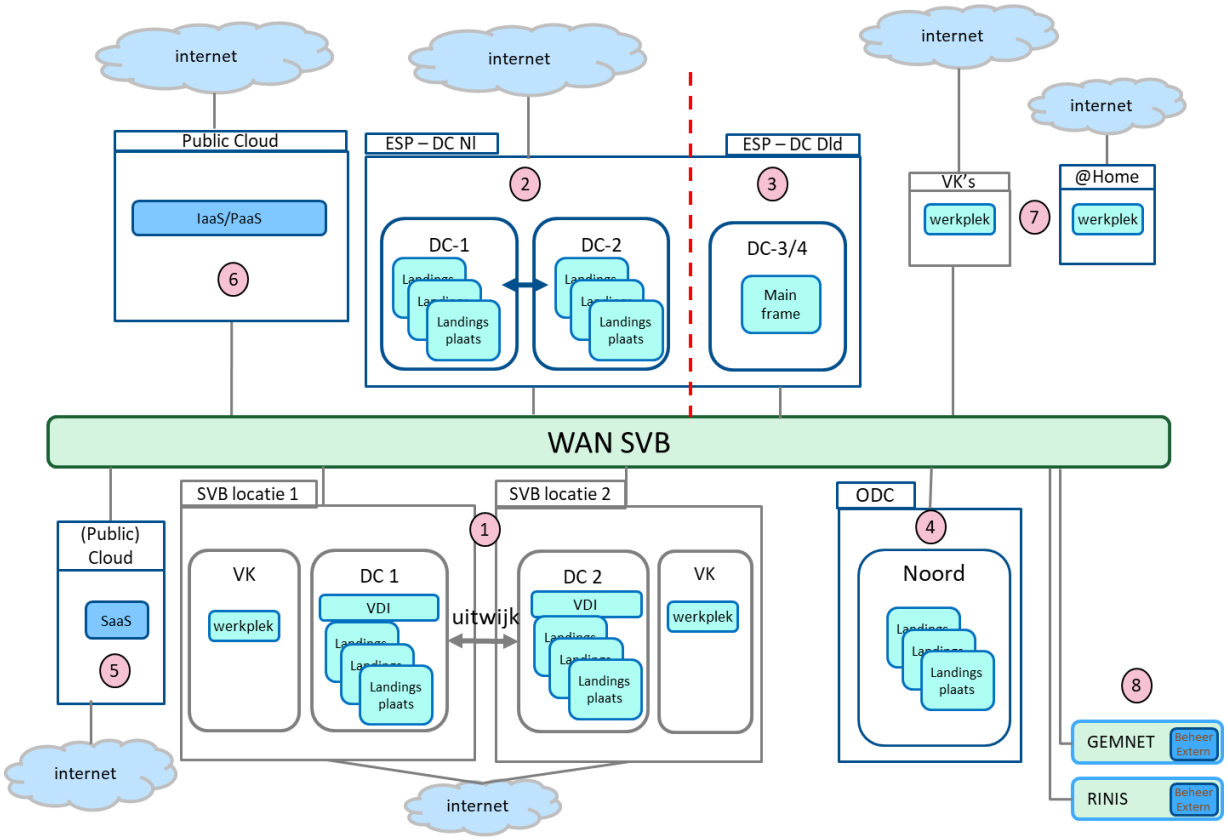
Bijlage D. Infrastructuurlandschap SVB en relevante volumes

1.1 Infrastructuurlandschap SVB

Door de SVB zijn in de loop der jaren diverse ICT-Infrastructuur- en applicatieplatformen ingezet voor de ondersteuning van bedrijfsapplicaties. Voor deze platformen zijn zowel eigen keuzes gemaakt voor specifieke ICT-Infrastructuur ter ondersteuning van zelf ontwikkelde maatwerksoftware, als ook voorgeschreven ICT-Infrastructuur door ESP's (External Service Providers) van standaard of generieke softwarepakketten. Een globaal overzicht van het infrastructuur landschap in de huidige situatie is in het volgende overzicht weergegeven.



Figuur 1: globaal overzicht huidig infrastructuur landschap

Hierin zijn de volgende hoofdonderdelen onderscheiden (nummers corresponderen met de nummers in figuur 5):

1. De interne SVB datacenter ruimtes gevestigd op 2 SVB locaties met ook een kantoorfunctie (VK, vestigingskantoren). Hier draaien voornamelijk secundaire en generieke applicaties. Ook draait hier de infrastructuur van PGB1.0.[1] De omgeving is grotendeels gevirtualiseerd op een Microsoft Hyper-V virtualisatieplatform met een totale installed base van zo'n 170 fysieke servers waarop +/- 1700 VM's actief zijn. Dit zijn Windows/Linux servers, appliances of Windows VDI's. Ook de virtuele werkplek op basis van Microsoft RDS draait binnen deze infrastructuur. Redundantie wordt geboden in de vorm van clustering (lokaal) en replicatie t.b.v. uitwijk tussen beide datacenters (RTO: 5 min).

[1] Binnen het domein Zorg wordt de toekomstbestendigheid van het PGB systeem geborgd door overgang naar een nieuw PGB2.0- systeem, in opdracht en onder regie van het ministerie van VWS. Tijdens de transitiefase borgen we de continuïteit door het actief onderhouden van het huidige PGB1.0-systeem.

2. Door een ESP worden diverse gedistribueerde systemen geleverd die ondersteunend zijn aan het primair landschap. Deze worden geleverd vanuit een dual datacenter in Nederland en betreffen naast de voor de SVB ingerichte netwerk en beveiligingsinfrastructuur ca. 350 VM's. De storage t.b.v. opslag (excl back-up) in verschillende klassen heeft een omvang van ca. 210 Tb.
3. De mainframe hostingdiensten zijn ondergebracht bij dezelfde ESP en worden geleverd vanuit een dual datacenter set up in Duitsland. Dit betreffen de kernsystemen van de sociale verzekeringen die verschillende regelingen ondersteunen (AOW, kinderbijslag (AKW), weduwen &wezen (ANW) waaronder de mainframe applicaties AKW, AnW, AOW, TOG en bijbehorende webportalen (MijnSVB) en ondersteunde voorzieningen als ontwikkel/ test/acceptatie/educatie-omgevingen van alle mainframe applicaties (OTAP+E).
4. Bij ODC-Noord draait een deel van het systeem voor de verwerking van PGB2.0 (het zogenaamde PGB-Z domein).
5. Een deel van de applicatiesystemen met name voor bedrijfsvoering (HR & Facilitair – Finance & Control – Inkoop) draait bij SaaS ESP's en wordt ontsloten voor SVB werkplekken via het internet.
6. De SVB maakt op dit moment gelimiteerd gebruik van publieke cloud obv Azure. Enkele toepassingen waarvoor public cloud (Azure) wordt ingezet zijn Azure AD, MS365, MCAS en Intune.
7. De SVB werkplekken zijn mobiel en kunnen zowel thuis (via internet) als op een vestigingskantoor (VK) (via SVB LAN en WAN) de SVB applicaties bereiken. De SVB heeft een cloud (MS365) gebaseerde werkplek waarmee flexibel werken wordt gefaciliteerd voor de ca. 4100 medewerkers. Bedrijfsapplicaties worden in hoofdzaak ontsloten via RDS en MyApps.
8. Voor samenwerking met (overheids)ketenpartners wordt gebruikt gemaakt van specifieke koppelvlakleveranciers die zorgdragen voor de juiste connectiviteit en formattering. Belangrijkste daarvan zijn GEMNET en RINIS.

A.g.v. verschillende ontwikkelingen is dit landschap in beweging. Zo is vanuit de sourcing strategie SVB de intentie om de Datacenter en hostingdiensten (tot en met het niveau van het technisch platform beheer) de komende jaren verder uit te besteden. Als gevolg hiervan zullen de applicaties die nu binnen het eigen DMZ van de SVB draaien (op termijn) worden verplaatst naar een landingsplaats bij een ESP (ofwel als legacy hosting, ofwel private cloud hosting) ofwel verschuiven naar een publieke cloud.

1.2 Volumes logdata en complexiteit landschap

De security monitoring van het SOC is in de huidige situatie gerelateerd aan de de bovenstaande hoofdonderdelen 1, 3, 6, en 7. Het SOC ontvangt ca. 7500 Events per second vanuit het landschap met de volgende kenmerken.

Log sources	Aantallen
Windows Servers	800 VM's.
Linux Servers	200 VM's
Database	344
Laptops / VM's met Windows 10	5000
Application firewall	2x merk A
Anti-virus	MS Defender op Windows platform + 4x merk B op netwerk infrastructuur
Firewalls	20x merk C + 2x merk D
Web proxy	2 merk E
Reverse Proxy	4

E- mail gateways	1x merk F en Microsoft Office 365
DHCP	16
DNS/Passive	16
Web servers	3x merk G + 4x merk H

Gezien de vertrouwelijk aard van de (defense in depth) architectuur zijn de merken van de security appliances onherkenbaar gemaakt.