

Sociale Verzekeringsbank
Bijlage O
Beschrijving huidige en toekomstige situatie

**Europese aanbesteding WAN- en internetconnectiviteit en
aanverwante dienstverlening**

Versie 1.1

*Niets uit dit document mag zonder schriftelijke toestemming vooraf van de Sociale Verzekeringsbank worden
verveelvoudigd, openbaar gemaakt of voor andere doelstellingen gebruikt worden.*

Inhoudsopgave

1.	Inleiding	3
2.	Huidige situatie	4
2.1.	Access verbindingen	4
2.2.	WAN connectiviteit	4
2.3.	Internet connectiviteit	6
2.3.1.	Centrale Internet connectiviteit.....	6
2.3.2.	Lokale Internet connectiviteit	6
2.4.	Datacenter–datacenter koppeling	6
2.5.	Overzichtsplaat.....	6
2.6.	Beheer	7
3.	Beoogde situatie na gunning	8
3.1.	Access Verbindingen	8
3.2.	WAN connectiviteit	8
3.3.	Internet connectiviteit	9
3.3.1.	Centrale Internet connectiviteit.....	9
3.3.2.	Lokale internet breakout kantoorlocaties	9
3.3.3.	Overige lokale Internet connectiviteit	11
3.3.4.	IP nummering.....	11
3.4.	Datacenter–datacenter koppeling	11
3.5.	Capaciteit	12
3.6.	Overzichtsplaat logische verbindingen	13
4.	Mogelijke ontwikkelingen komende jaren.....	14

1. Inleiding

In dit document zijn de volgende onderdelen opgenomen:

- Hoofdstuk 2 “Huidige situatie”: Omschrijving van de wijze waarop op dit moment de WAN en Internetconnectiviteit zijn ingericht;
- Hoofdstuk 3 “Beoogde situatie na gunning”: Verwachte inzet van WAN en internet verbindingen bij implementatie van de nieuwe Overeenkomst en de mogelijke veranderingen daarin t.o.v. de huidige situatie;
- Hoofdstuk 4 “Mogelijke ontwikkelingen komende jaren”: Dit zijn de mogelijke ontwikkelingen en plannen voor de komende jaren. Tevens worden hierin enkele opties benoemd die aan de orde zouden kunnen zijn gedurende de looptijd van de Overeenkomst. De SVB is geheel vrij om deze opties wel of niet in opdracht te geven conform het gestelde in het Beschrijvend Document en de Overeenkomst.

Hoofdstuk 3 en hoofdstuk 4 beschrijven de verwachtingen naar huidig inzicht; Deelnemers kunnen hier geen rechten aan ontleen.

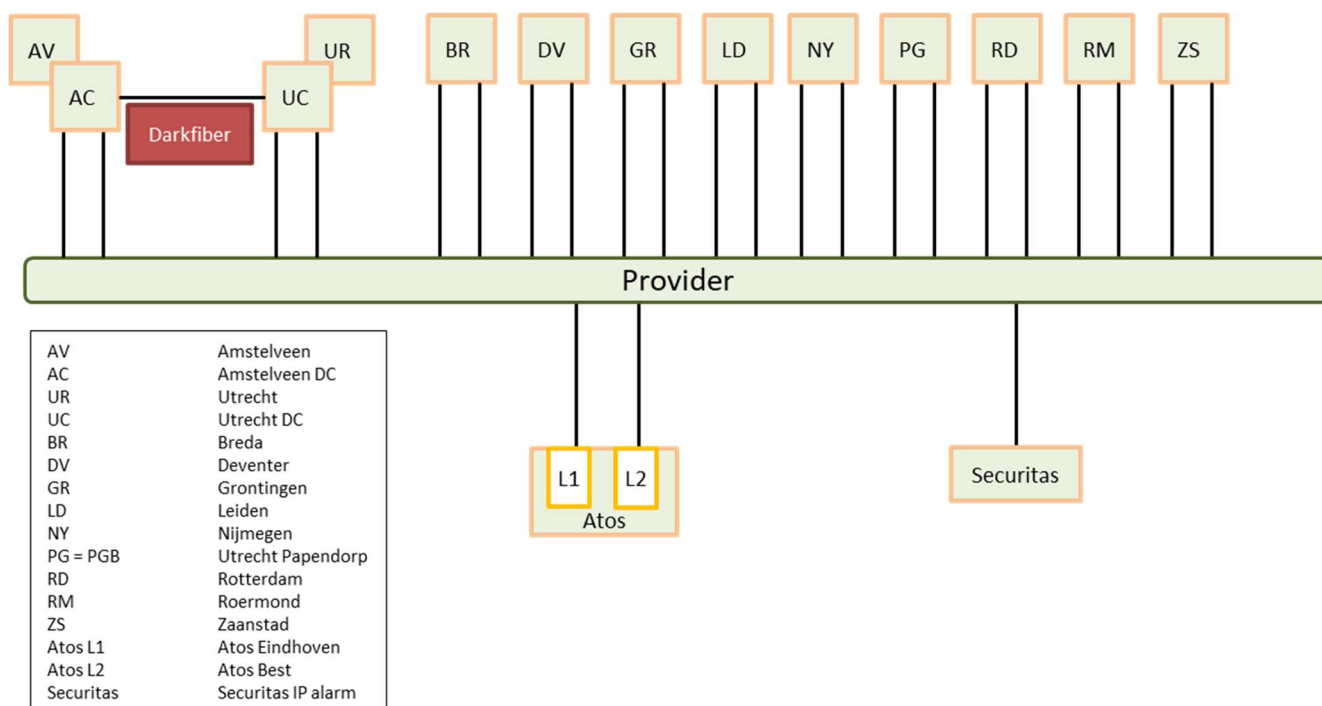
2. Huidige situatie

2.1. Access verbindingen

In de huidige situatie onderscheiden we een drietal logische connectiviteitsdiensten die bij één provider worden afgenomen:

1. WAN connectiviteit: vormt de koppeling tussen de diverse vertrouwde locaties van de SVB en haar ESP's.
2. Internet connectiviteit: wordt op diverse manieren ontsloten voor het aanbieden en bereiken van externe diensten.
3. DC-DC koppeling: Deze laag-2 koppeling verzorgt specifiek verkeer (backup, redundantie, beheer, e.d.) tussen de eigen rekencentra van de SVB in Utrecht en Amstelveen.

De 3 diensten zijn gerealiseerd op dezelfde fysieke fiber infrastructuur, zoals hieronder aangegeven. Alle SVB-locaties zijn op basis van geografisch redundante fiber infrastructuur verbonden met de provider. De ESP-locaties (2 Atos locaties) zijn enkelvoudig aangesloten.



Figuur 1: Access verbindingen

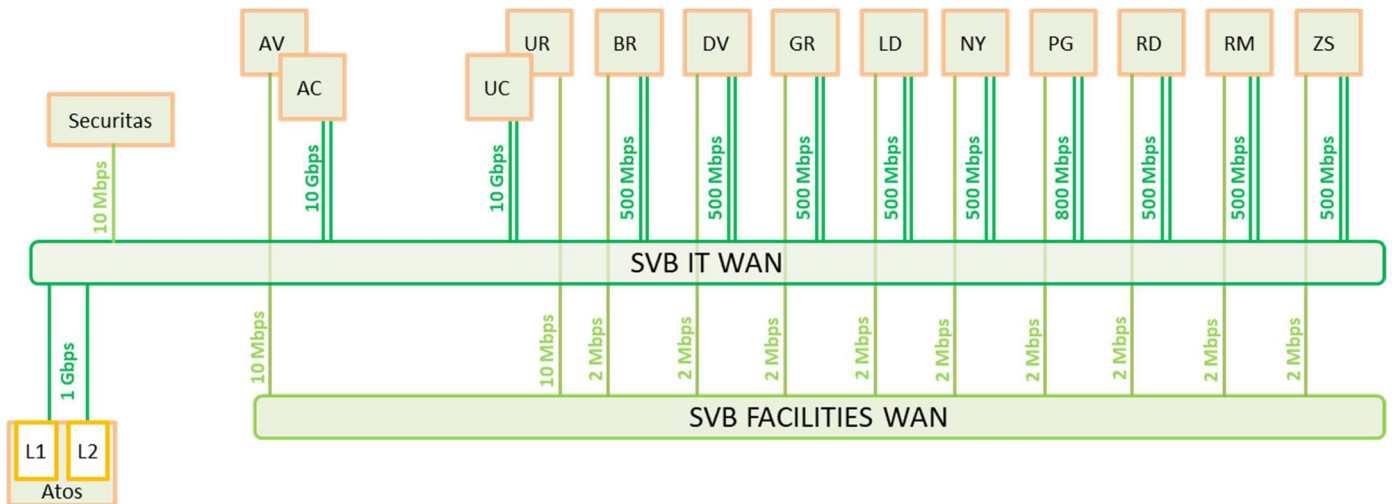
2.2. WAN connectiviteit

Het "SVB IT WAN" is opgezet als een any-to-any netwerk, waarbij alle SVB locaties logisch met elkaar verbonden zijn, zodat er geen afhankelijkheid is van een centrale SVB locatie of een willekeurig knooppunt.

Het betreft een elftal SVB-locaties, waarbij op een tweetal SVB-locaties naast een kantoorfunctie ook datacenterdiensten worden geleverd, en negen (9) locaties met uitsluitend een kantoorfunctie. Daarnaast is er een tweetal ESP-locaties, waar alleen datacenter diensten worden geleverd.

T.b.v. de gebouw-toegangssytemen op de elf SVB-locaties is een separaat "Facilities WAN" gerealiseerd.

Verkeer naar Securitas t.b.v. een IP-Alarm dienst wordt via het SVB IT WAN gerouteerd.



Figuur 2: WAN connectiviteit

IP-netwerk

Het WAN betreft een laag-3 netwerk (o.b.v. IPVPN over MPLS). Het WAN ondersteunt alleen verkeer op basis van TCP/IP, zodat op laag-3 alleen IP-routing tussen de genoemde IP-subnetten mogelijk hoeft te zijn. De routing is middels dynamische protocollen (BGP, OSPF, HSRP) ingesteld.

Omdat ook telefonieverkeer wordt getransporteerd is een gegarandeerde bandbreedte vereist, wat door ondersteuning van CoS/QoS is ingesteld. De QoS parametrisering wordt vanuit de lokale VLAN's aan het WAN aangeboden.

Redundantie

Alle SVB-locaties zijn via de glasinfrastructuur redundant op het WAN aangesloten. Hiermee is bereikt dat de kans op een langdurige verstoring (bijv. i.v.m. las- en graafwerkzaamheden, alsmede enkelvoudige uitval van apparatuur) minimaal is.

De ESP is op 2 locaties met enkelvoudige verbindingen gekoppeld. De redundantie is daar geregeld o.b.v. de twin-datacenter infrastructuur van de betreffende ESP.

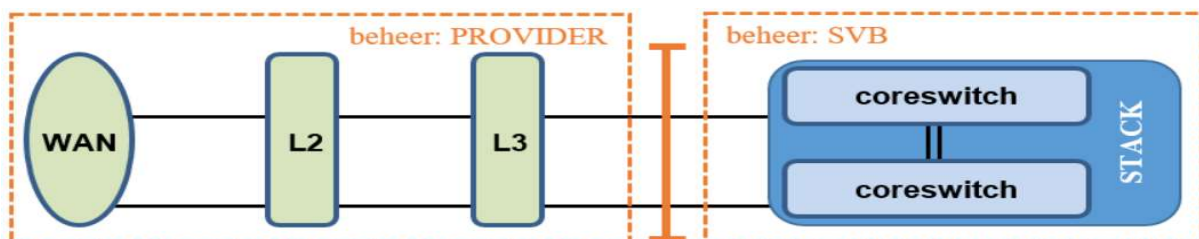
De logische WAN verbindingen zijn active/passive redundant uitgevoerd.

Koppelingen

Het SVB IPVPN WAN wordt o.b.v. ethernetconnectiviteit van de huidige provider afgenomen.

Het koppelvlak op de locaties t.b.v. de verbinding is op basis van ethernet multi-mode fiber. De fysieke verbindingen en bijbehorende apparatuur zijn in beheer bij de provider. Er wordt o.b.v. standaard protocollen en interfaces gekoppeld met de LAN-apparatuur van de SVB en haar ESP's. Koppeling van het WAN is op alle locaties direct op een LAN-switch (stack) in het klantdomein gerealiseerd.

Onderstaand is globaal aangegeven welke componenten bij de koppeling betrokken zijn, waarbij de groene en blauwe kleuren respectievelijk het domein van de provider en het domein van de SVB aangeven.



Figuur 3: koppelvlak provider - SVB

2.3. Internet connectiviteit

2.3.1. Centrale Internet connectiviteit

Op de beide datacenters van de SVB in Amstelveen en Utrecht wordt op dit moment een upgrade van de centrale internet connectiviteit gerealiseerd van 2 naar 5 Gbps.

De centrale internetverbindingen worden gebruikt voor inbound verkeer naar de SVB werkplek-applicaties, inbound verkeer naar de SVB-website, remote access, extern e-mail verkeer. Ook worden ze gebruikt voor outbound verkeer vanaf de SVB-werkplekken, waarbij verkeer vanaf de kantoorlocaties over het WAN naar de centrale locaties wordt geleid. Om die reden zijn de kwaliteitseisen, bijvoorbeeld m.b.t. capaciteit en beschikbaarheid, hoog.

Redundantie

De centrale internetverbindingen worden ook op de glasinfrastructuur geleverd, maar zijn enkelvoudig uitgevoerd. De verbindingen in Amstelveen en Utrecht zijn beiden actief. O.b.v. een laag-2 verbinding tussen beide locaties is redundantie gerealiseerd. De huidige provider verzorgt de dynamische routing (BGP) vanuit het internet over beide verbindingen zodat bij uitval van één verbinding de diensten beschikbaar blijven.

Koppelingen

Via een eigen fysieke interface zijn deze verbindingen aangesloten op de DMZ's van beide DC locaties.

Anti-DDoS

De anti-DDoS dienst wordt geleverd door de huidige provider als onderdeel van de centrale internetaansluiting op beide SVB datacenters. DDoS bescherming is ingericht t/m laag 4 (volume aanvallen). De anti-DDoS dienst is geïmplementeerd in de omgeving van de huidige provider.

2.3.2. Lokale Internet connectiviteit

Op alle elf SVB locaties is voorzien in lokale internetvoorzieningen voor het gebruik van apparatuur die geen onderdeel uitmaakt van de SVB core-IT (denk aan Gast-internet, BYOD, internet-radio, camera's, e.d.). Deze verbindingen worden ook op de redundante glasinfrastructuur geleverd, maar zijn enkelvoudig uitgevoerd zonder speciale eisen aan verdeling over de infrastructuur. De capaciteit varieert tussen 40 en 200Mbps.

2.4. Datacenter–datacenter koppeling

Tussen de datacenter locaties Amstelveen en Utrecht beschikt de SVB over een redundante laag-2-verbinding. Redundantie is gerealiseerd met een kanaal over een darkfiber en een ethernet point-to-point verbinding. De darkfiber wordt belicht met apparatuur onder beheer van de SVB.

Over deze laag 2 verbinding routeert de SVB meerdere VLAN's t.b.v. telefonieoplossing, DC-DC replicatie en DC management verkeer.

Over de darkfiber is een separaat kanaal gerealiseerd voor de internetredundantie zoals genoemd onder de centrale internetconnectiviteit.

2.5. Overzichtsplaat

Hieronder wordt een grafische voorstelling van de beschreven situatie weergegeven. Hierin zijn de WAN, internet en Laag-2 verbindingen weergegeven.



Figuur 4: Logische verbindingen en bandbreedtes. N.B. De verbindingen t.b.v. “Lokale internet connectiviteit” zijn niet ingetekend.

2.6. Beheer

IP-adres beheer

De SVB is verantwoordelijk voor het beheer van het IP-management (IP-adressen, DNS, DHCP e.d.) van het gehele netwerk.

Binnen de IPVPN-wolk worden in de huidige situatie publieke IP-adressen gebruikt van de provider. Voor noodzakelijke koppeling met het netwerk van de provider worden (private) IP-ranges ter beschikking gesteld door de SVB. Deze ranges mogen niet conflicteren met de IP-adressen die al in gebruik zijn binnen de SVB-omgeving; daaronder vallen ook de adressen die t.b.v. de SVB in gebruik zijn bij de ESP.

Beheer vanuit SVB

Het netwerk is zodanig ingericht dat de SVB-specialisten de mogelijkheid hebben om rudimentaire sanity-checks uit te voeren en standaard hulpmiddelen kunnen inzetten om fout- en/of verbetersituaties te kunnen inschatten c.q. opsporen. Dit is onafhankelijk van de status van een verbinding of eventuele werkzaamheden van de provider.

Op alle verbindingen is het mogelijk om (een rudimentair) inzicht te krijgen in het capaciteitsgebruik. Dit capaciteitsgebruik kan door de SVB zelf (ook grafisch) inzichtelijk gemaakt worden via een portaldienst van de provider.

3. Beoogde situatie na gunning

Hieronder is de mogelijke situatie beschreven die de SVB op dit moment voorziet bij implementatie van de nieuwe Overeenkomst. Daar waar dit afwijkt van de beschrijving van de huidige situatie wordt dit aangegeven, en wordt aangegeven wat de SVB hiermee beoogt. De eisen die voortvloeien uit deze beschrijving zijn geconcretiseerd in het Programma van Eisen.

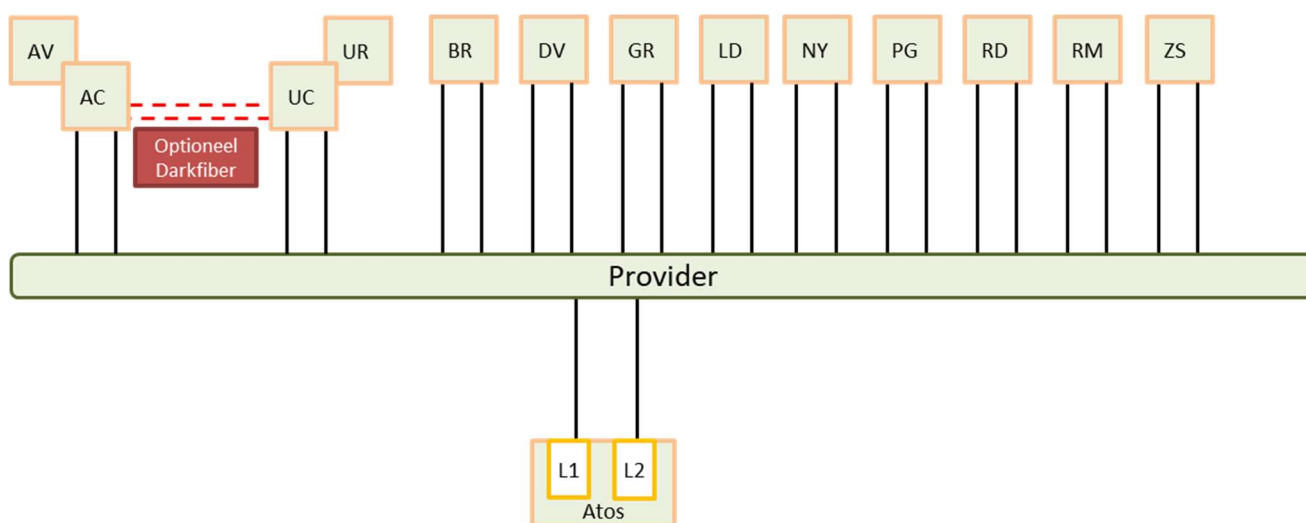
3.1. Access Verbindingen

Gelijkwaardig aan de glas-infrastructuur zoals in de beschrijving van de huidige situatie, worden de Access Verbindingen gerealiseerd als een gemeenschappelijke glas-infrastructuur, waarover de verschillende internet- en WAN Diensten kunnen worden aangeboden. De huidige glasinfrastructuur wordt door SVB als een optimale oplossing ervaren op gebied van veiligheid, performance, schaalbaarheid, flexibiliteit en storingsgevoeligheid.

Logische verbindingen moeten naar wens redundant of enkelvoudig kunnen worden afgenomen. De glas-infrastructuur op de 11 (elf) SVB locaties wordt hiertoe volledig redundant uitgevoerd¹, zodanig dat de kans op een langdurige verstoring (bijv. i.v.m. las- en graafwerkzaamheden, alsmede enkelvoudige uitval van apparatuur) minimaal is.

De bandbreedte van logische verbindingen moet eenvoudig en snel aanpasbaar zijn, en extra logische verbindingen moeten eenvoudig en snel kunnen worden gerealiseerd. De logische verbindingen worden onderling logisch gescheiden, maar komen bij het koppelvlak met het on-premise SVB netwerk wel uit op separate fysieke poorten.

In het kader van garantie op bandbreedte wordt als netwerkdrager geen gebruik gemaakt van draadloze dataverbindingen.



Figuur 5: Access verbindingen – glas-infrastructuur

3.2. WAN connectiviteit

Het “SVB IT WAN” wordt opgezet als een any-to-any laag 3 (IP) netwerk, waarbij alle locaties logisch met elkaar verbonden zijn, zodanig dat er geen afhankelijkheid is van een centrale SVB locatie of een willekeurig knooppunt. Het betreft een elftal SVB-locaties, waarbij op een tweetal SVB-locaties naast een kantoorfunctie ook datacenterdiensten

¹ Voor de locatie Breda geldt de bijzonderheid dat deze omringd is door water en er in de huidige situatie ter hoogte van de brug maar één nutsvoorziening invoer het pand in gaat. De diensten tot aan de brug en in het pand zijn wel volledig redundant. Het continueren van deze SPOF ter hoogte van de brug is acceptabel. In de voorbereidingsfase zullen tekeningen worden gedeeld en mogelijkheden en impact van het elimineren van de SPOF worden besproken.

worden geleverd, en negen locaties met uitsluitend een kantoorfunctie. Daarnaast is er een tweetal ESP-locaties, waar alleen datacenter diensten worden geleverd.

De (logische) WAN verbindingen met de netwerkprovider worden op elk van de SVB locaties redundant uitgevoerd. De ESP Atos wordt op 2 locaties enkelvoudig gekoppeld. Redundantie is daar geregeld middels de twin-datacenter infrastructuur van de betreffende ESP.

Ten behoeve van telefonieverkeer is een gegarandeerde bandbreedte vereist, wat door ondersteuning van CoS/QoS wordt ingesteld. De QoS parametrisering wordt vanuit de lokale VLAN's aan het WAN aangeboden.

Op de elf SVB-locaties wordt een separaat "Facilities WAN" gerealiseerd t.b.v. gebouw-toegangssystemen. Dit netwerk kent een lage bandbreedte en lagere beschikbaarheidseisen en wordt enkelvoudig uitgevoerd.

Daarnaast is de intentie dat ten opzichte van de huidige situatie de afhankelijkheid van de IP alarm dienst naar het SVB IT WAN komt te vervallen. Deze wordt vervangen door een internet gebaseerde dienst.

3.3. Internet connectiviteit

3.3.1. Centrale Internet connectiviteit

Op de beide datacenters van de SVB in Amstelveen en Utrecht wordt een verbinding met het internet gerealiseerd.

Deze centrale internetverbindingen worden gebruikt voor inbound verkeer naar de SVB werkplek-applicaties, remote access en extern e-mail verkeer. Daarnaast worden ze gebruikt voor outbound verkeer vanaf de SVB-werkplekken in Amstelveen en Utrecht (local breakout). Internetverkeer vanaf de SVB-werkplekken in overige kantoorlocaties wordt in de toekomstige situatie dus niet langer over het WAN naar de centrale locaties geleid, maar maakt gebruik van lokale internet breakouts op de betreffende kantoorlocaties (zie 3.3.2).

Redundantie

De centrale internetlijnen worden zowel in Amstelveen als in Utrecht redundant uitgevoerd. Redundantie wordt hierbij voortaan als standaard dienst van de dienstverlener afgenomen, waarbij een enkelvoudige storing binnen 1 Datacenter kan worden opgevangen. De huidige Datacenter-datacenter koppeling t.b.v. failover over de huidige enkelvoudige internetlijnen vervalt hierdoor.

Anti-DDoS

De centrale internetconnectiviteit wordt door de WAN leverancier voorzien van DDoS bescherming t/m laag 4 (volume aanvallen).

3.3.2. Lokale internet breakout kantoorlocaties

Als onderdeel van deze netwerkaanbesteding worden voor het werkplekverkeer lokale internet breakouts gerealiseerd op de kantoorlocaties. Op elk van de 9 kantoorlocaties van de SVB wordt hiertoe een verbinding met het internet gerealiseerd t.b.v. lokale internet breakout. Ook deze verbindingen worden redundant uitgevoerd.

Hiermee worden de volgende doelen beoogd:

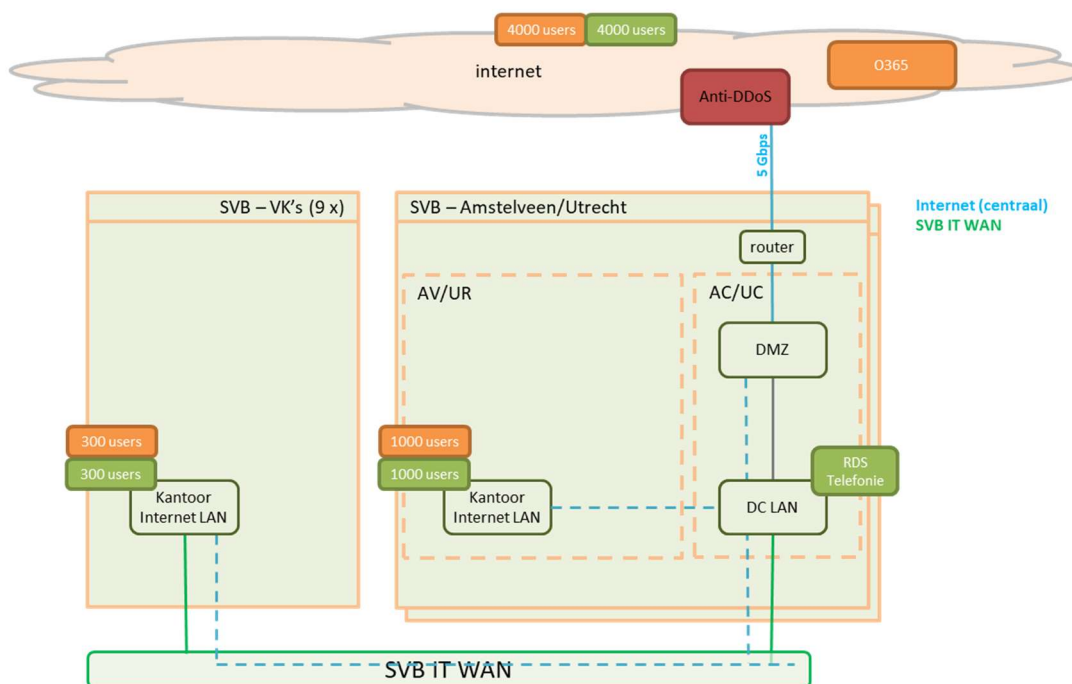
- Endpoints worden conform de vanuit Microsoft O365 aanbevolen architectuur² zo direct mogelijk gekoppeld aan het Internet om de eindgebruikersdiensten in de O365 cloud optimaal te kunnen gebruiken.
- Kostenbesparing door het afschalen van relatief dure WAN capaciteit. Omdat internetverkeer niet langer naar het centrale datacenter wordt geleid is een lagere WAN capaciteit nodig en wordt het op termijn zelfs mogelijk het WAN geheel uit te faseren ('internet-only', zie hoofdstuk 4).
- Lokale breakout is in lijn met de verwachte uitbesteding van het huidige datacenter, waarbij de huidige centrale breakout voorziening zal verdwijnen (zie hoofdstuk 4).

² Zie bijvoorbeeld <https://docs.microsoft.com/nl-nl/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide>

- Lokale breakout is in lijn met de doelarchitectuur van de SVB werkplek, waarbij voor de beveiliging van de SVB werkplek niet langer wordt vertrouwd op de centrale netwerk-beveiligingsvoorzieningen.

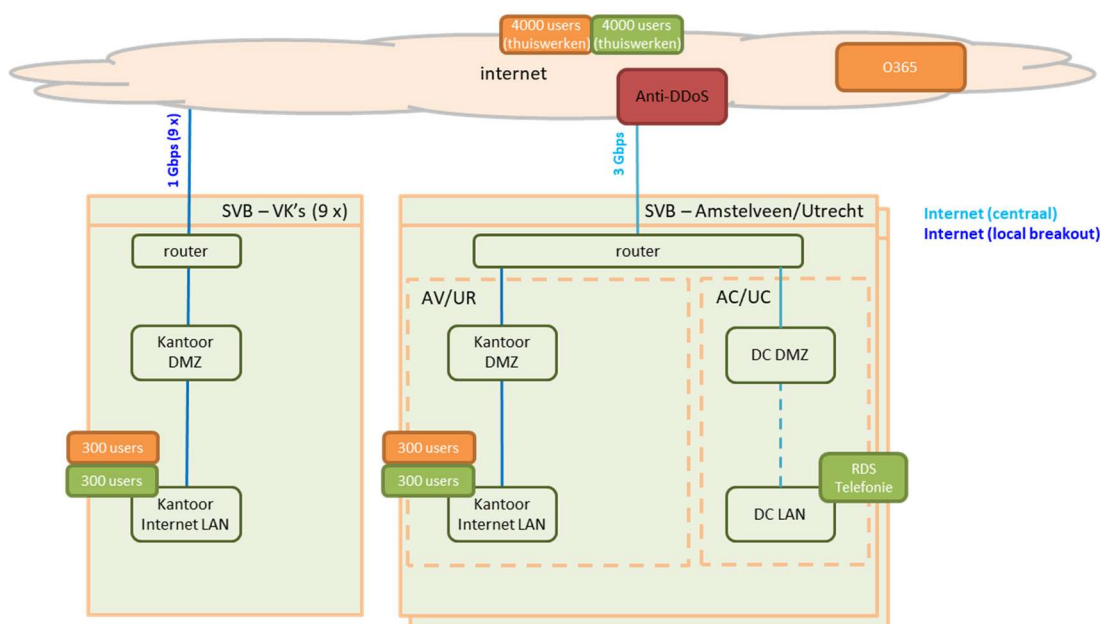
Op de locaties Amstelveen en Utrecht worden de centrale internetverbindingen ook ingezet als lokale internet breakout voor deze locaties. Hierbij is de verwachting dat door hergebruik van deze lijnen kosten worden bespaard ten opzichte van separate lokale internet breakouts op de locaties Amstelveen en Utrecht.

Internet breakout – Voor transitie



Figuur 6: Belangrijkste gebruik van centrale internet breakouts in de huidige situatie

Internet breakout – Na transitie



Figuur 7: Belangrijkste gebruik van lokale internet breakouts in de toekomstige situatie

Beveiliging Lokale internet breakout

De SVB zal op alle SVB locaties een “Kantoor DMZ” realiseren t.b.v. beveiliging van de lokale breakouts.

Ook voor de lokale breakouts in Amstelveen en Utrecht wordt een “Kantoor DMZ” gerealiseerd, naast de bestaande datacenter DMZ. Hierdoor wordt de netwerkarchitectuur voor de kantooromgevingen op alle locaties inclusief Amstelveen en Utrecht geüniformeerd.

3.3.3. Overige lokale Internet connectiviteit

Op alle SVB locaties wordt voorzien in lokale internetconnectiviteit voor het gebruik van apparatuur die geen onderdeel uitmaakt van de SVB core-IT (denk aan Gast-internet, BYOD, internet-radio, camera's, e.d.).

Uitgangspunt is dat deze verbindingen ook via de redundante glasinfrastructuur worden geleverd, maar over het algemeen enkelvoudig worden uitgevoerd.

Ten opzichte van de huidige situatie is de intentie om op moment van transitie een aantal internetlijnen dat nu bij een andere partij wordt afgenomen ten behoeve van Videoconference oplossing, te migreren naar de nieuwe WAN provider. **Het betreffen de volgende verbindingen / lokaties:**

- 1 * 300 Mbps SVB locatie Nijmegen
- 1 * 300 Mbps SVB locatie Deventer
- 1 * 300 Mbps SVB locatie Breda
- 1 * 300 Mbps SVB locatie Zaandam
- 1 * 300 Mbps SVB locatie Roermond
- 1 * 300 Mbps SVB locatie Amstelveen
- 1 * 300 Mbps SVB locatie Leiden
- 1 * 300 Mbps SVB locatie Groningen

3.3.4. IP nummering

De lijnen t.b.v. centrale internet connectiviteit zullen worden geconfigureerd met publieke adressen uit SVB IP ranges, waarvan er voldoende beschikbaar zijn.

De lokale breakout lijnen moeten worden geconfigureerd met publieke adressen uit leveranciers IP ranges.

De verbindingen moeten kunnen worden geconfigureerd met meerdere publieke adressen, zodat ze kunnen worden ingezet voor meerdere diensten (consolidatie van losse internetlijnen).

3.4. Datacenter–datacenter koppeling

Tussen de datacenter locaties Amstelveen en Utrecht wordt een redundante laag-2 verbinding gerealiseerd. De SVB gebruikt deze laag-2 verbinding voor de routing van meerdere VLAN's t.b.v. replicatie- en managementverkeer tussen de datacenters. Datacenter-failover en -uitwijk scenario's worden hiermee gefaciliteerd.

De aanbieder mag de verbinding op basis van point-to-point ethernet of (conform de huidige situatie) als een combinatie van darkfiber en point-to-point ethernet aanbieden.

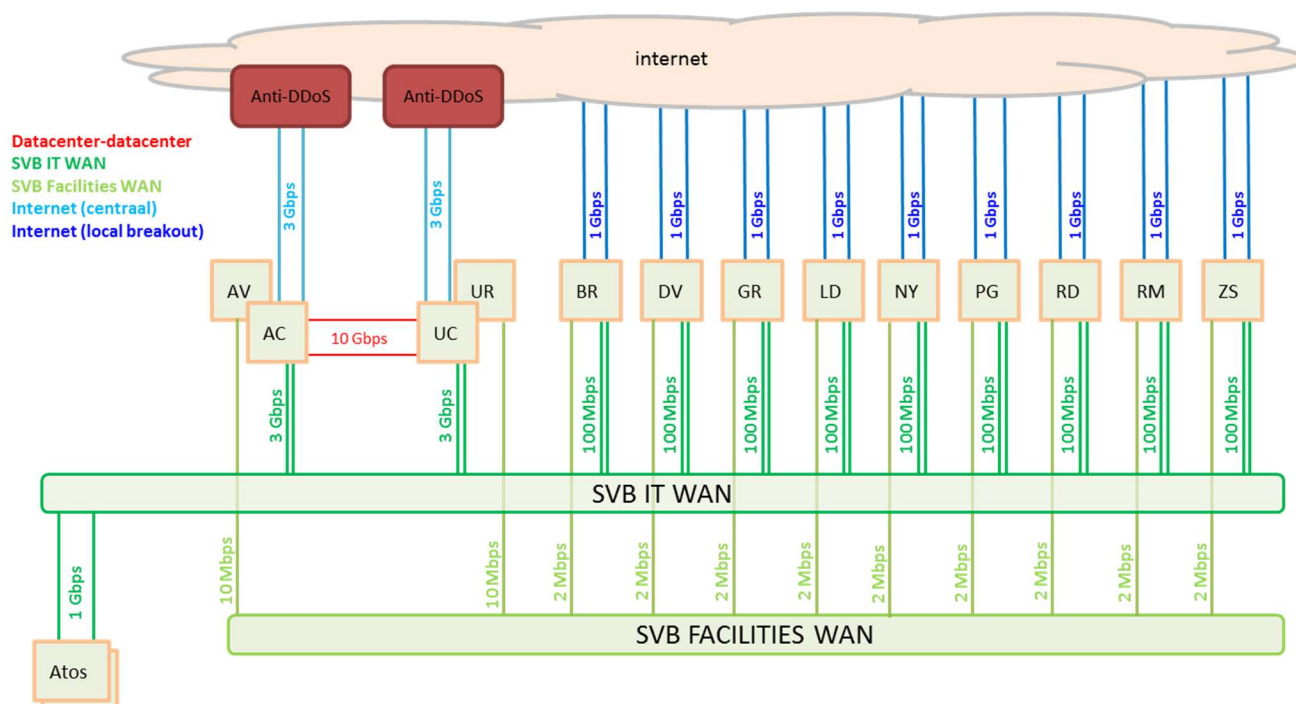
De huidige Datacenter-datacenter koppeling t.b.v. failover over de huidige enkelvoudige internetlijnen vervalt, omdat de internetlijnen per locatie redundant worden afgenomen.

3.5. Capaciteit

Als gevolg van de genoemde Interne ontwikkelingen zullen de benodigde bandbreedtes wijzigen ten opzicht van de huidige situatie. In onderstaande tabel is ter indicatie de verwachte bandbreedte voor de verschillende lijnen inzichtelijk gemaakt. Dit kan tot het moment van transitie nog wijzigen als gevolg van ontwikkelingen en bevindingen, waarbij er met name onzekerheden zijn over de gevolgen van Office365 voor de bandbreedte.

Type verbinding	Locatie	Huidige bandbreedte	Verwachte bandbreedte	Toelichting op verwachte bandbreedte
Access verbindingen	Amstelveen/Utrecht	Ca. 30Gbps	30Gbps	Minimum bovengrens voor schaalbaarheid totale bandbreedte van de logische verbindingen per locatie
Access verbindingen	Kantoren	Ca. 3Gbps	5Gbps	Minimum bovengrens voor schaalbaarheid totale bandbreedte van de logische verbindingen per locatie
IT WAN	Amstelveen/Utrecht	10Gbps	3Gbps	Internetverkeer van de kantoren verloopt niet meer over het WAN naar centrale internet breakout
IT WAN	Kantoren	500Mbps	100Mbps	Internetverkeer van de kantoren verloopt niet meer over het WAN naar centrale internet breakout
IT WAN	Atos	1Gbps	1Gbps	Geen verandering
Facilities WAN	Amstelveen/Utrecht en Kantoren	2 Mbps voor kantoorlocaties 10 Mbps voor datacenterlocaties	2 Mbps voor kantoorlocaties 10 Mbps voor datacenterlocaties	Geen verandering
Centraal internet breakout	Amstelveen/Utrecht	5 Gbps	3Gbps	Internetverkeer van de kantoren verloopt niet meer over het WAN naar centrale internet breakout
Lokale internet breakout	Kantoren	n/a	1Gbps	Internetverkeer van de kantoren verloopt voortaan via lokale breakout
Overige internet koppelingen	Alle locaties	19*100Mbps 8*300Mbps	19*100Mbps 8*300Mbps	Extra lijnen t.b.v. Videoconference
DC-DC koppeling	DC-DC Amstelveen/Utrecht	10Gbps	10Gbps	Geen verandering

3.6. Overzichtsplaat logische verbindingen



Figuur 8: Logische verbindingen en bandbreedtes. N.B. De verbindingen t.b.v. "Overige lokale internet connectiviteit" zijn niet ingetekend.

4. Mogelijke ontwikkelingen komende jaren

De SVB wil het aantal WAN en internetverbindingen, als wel de bandbreedtes daarvan, kunnen laten meebewegen (zowel meer als minder) met haar behoeften gedurende de looptijd van de Overeenkomst. In deze paragraaf wordt een aantal mogelijke ontwikkelingen gegeven die van invloed kunnen zijn op de afname van connectiviteitsdiensten binnen de Overeenkomst.

Opdrachtnemer dient deze bewegingen te onderkennen en daar flexibel mee om te gaan. Hierbij kan het zijn dat indien een ontwikkeling actueel wordt en de SVB daartoe opdracht geeft, Opdrachtnemer samen met de SVB de consequenties daarvan op de connectiviteitsdiensten in kaart brengt (tijd, geld en kwaliteit) en/of uitvoert, op basis van de afgesproken tarieven.

1. Hybride werken. Na het grootschalige thuiswerken afgelopen tijd a.g.v. de Corona pandemie is het de verwachting dat medewerkers, eventueel een deel van hun tijd, structureel vanaf huis zullen blijven werken.
2. Uitbesteding Datacenters & hosting ten behoeve van de primaire en secundaire processen. Vanuit de SVB sourcingstrategie is de intentie om de Datacenters uit te besteden. De huidige datacenter locaties Amstelveen en Utrecht ontwikkelen zich daarna tot reguliere kantoorlocaties. De Datacenter-Datacenter koppeling en “Centraal internet” verbindingen vervallen hiermee uiteindelijk in deze locaties.
3. Verdere toename van de inzet van public cloud diensten. Dit voor zowel hostingfuncties als voor SAAS applicaties. Dit zal mogelijk gevolgen hebben voor de bandbreedte van de centrale en lokale internet breakouts. Ook kan de behoefte ontstaan voor een (tijdelijke) directe ontsluiting van (één van) de grote public cloud providers vanuit het netwerk van de WAN leverancier.
4. De huidige on-premise telefonie oplossing zal worden vervangen door een mogelijk cloud gebaseerde oplossing. De afhankelijkheid van de huidige telefonie oplossing naar het private WAN netwerk en de inrichting van CoS/QoS zal in dat geval komen te vervallen.
5. Als gevolg van bovenstaande ontwikkelingen zal het belang van het private WAN afnemen en van het Internet toenemen. De SVB voorziet dat kantoorlocaties naar ‘internet only’ zullen gaan. Voordelen van internet-only liggen met name in een vereenvoudiging van de architectuur en een kostenoptimalisatie door consolidatie van verbindingen. Doordat internetverbindingen private WAN verbindingen gaan vervangen worden deze steeds meer bedrijfskritisch.
6. SDWAN / SASE. SD-WAN vereenvoudigt het beheer en de werking van een WAN door de netwerk hardware los te koppelen van het besturingssysteem. Het vormt een overlay (overlappend/bovenliggend) op de WAN en internetverbindingen waarmee pad optimalisatie, netwerk redundantie en netwerk zonering ingeregeld kunnen worden. Als gevolg van marktontwikkelingen op dit gebied, de toenemende inzet van clouddiensten en verdergaande eisen aan cyberweerbaarheid voorziet SVB een mogelijke migratie naar een SDWAN / SASE netwerkarchitectuur.
7. Verhoging cyberweerbaarheid. Verhoging van de cyberweerbaarheid en het tegengaan van actuele cyberdreigingen kan noodzaak geven om aanvullende diensten van de WAN leverancier af te nemen indien het dreigingsbeeld voor de SVB hier aanleiding toe geeft. Hierbij worden onderscheiden:
 - a. DDoS bescherming (t/m laag 4) op de internetconnectiviteit op kantoorlocaties
 - b. **Tekst verwijderd n.v.t.**

Deze diensten zijn als optie in deze aanbesteding opgenomen.