Functioneel Ontwerp Netwerk

DEF

Inhoudsopgave

1. INLEIDING

1.1 Doel van dit document

Dit document beschrijft de ontwerp keuzes voor het netwerk. Hierbij wordt niet de vraag hoe, maar vooral waarom belicht. Het netwerk is ondersteunend aan de applicaties die worden gebruikt binnen Heliomare. Deze applicaties hebben in de huidige situatie een gegeven risicoprofiel. Uitgangspunt is dat de risico's in de huidige situatie onacceptabel worden geacht. In dit document wordt daarom vooral gekeken naar het verlagen van deze risico's middels een nieuwe infrastructuur.

1.2 Uitgangspunten

Voor de design keuzes die in dit document worden beschreven zijn de volgende uitgangspunten gebruikt:

1. Risicoprofiel van de huidige in scope zijnde diensten is in overeenstemming met de wensen van Heliomare;
2. De beschikbaarheid van infrastructuur moet voldoen aan de zwaarste applicatie eisen;
3. Belangrijkste applicatie is afhankelijk van locatietype;
4. Diverse bedrijfskritische applicaties zijn ingericht in private datacentra;
5. Inhoudelijke gegevens aangeleverd t.b.v. de IST-situatie zijn juist en consistent.

Het geheel van deze componenten moet ervoor zorgen dat aan de functionele eisen van het netwerk met betrekking tot beschikbaarheid, continuïteit, en veiligheid wordt voldaan. Waarbij gebruik gemaakt wordt netwerk architectuur principes prestaties, beschikbaarheid en veiligheid.

1.3 Toelichting beschikbaarheid begrippen

Veel zorgprocessen zijn direct afhankelijk van ICT. De bedrijfsvoering van Heliomare en de clientveiligheid die zij bedient, is afhankelijk van de beschikbaarheid en prestaties van ICT. De netwerk infrastructuur kan de beschikbaarheid en prestaties beïnvloeden. Zowel positief als negatief.
100% Beschikbaarheid bestaat niet. Zowel geplande (onderhoud) als ongeplande (incidenten) uitval zorgen voor tijdelijke onderbrekingen. De beschikbaarheidseis van applicaties kan worden uitgedrukt in een aantal KPI's:

- Beschikbaarheid (%), hoeverre een ICT-dienst, systeem of component toegankelijk is voor gebruikers, uitgedrukt in een percentage van een periode (veelal een jaar);
- RTO (uren/mins), Recovery Time Objective, de tijdsduur binnen welke de dienst hersteld moet zijn na falen;
- RPO (uren/mins), Recovery Point Objective, de tijdsduur waarover dataverlies als gevolg van een incident wordt geaccepteerd.

Vanuit het netwerkperspectief zijn beschikbaarheid en RTO relevant. Wanneer het netwerk als geheel een lagere beschikbaarheid of RTO biedt dan op applicatieniveau noodzakelijk is, zijn aanvullende maatregelen op applicatieniveau noodzakelijk. Beschikbaarheid wordt uitgedrukt in een percentage uptime. In onderstaande tabel is dit percentage uitgedrukt in tijd per jaar dat een applicatie niet beschikbaar is.

Beschikbaarheid	Totale geoorloofde tijd per jaar dat een applicatie niet beschikbaar mag zijn (24*7*365)
99,6%	1 dag, 11 uur en 3 minuten
99,6%	1 dag, 11 uur en 3 minuten
99,9%	8 uur en 45 minuten

99,99%	52 minuten
99,999%	5 minuten

Bij het bepalen van de beschikbaarheid wordt "dubbel falen" uitgesloten. Hierbij wordt het falen van twee verschillende componenten of verbindingen tegelijk niet meegenomen. Ook bij een beschikbaarheidseis van 99,999% is nog altijd sprake van een geaccepteerde uitval van 5 minuten. Daarnaast is het mogelijk dat de gewenste beschikbaarheid niet behaald wordt. Voor een goede en veilige behandeling van cliënten is het van belang dat Heliomare de afhankelijkheden van ICT binnen (zorg)processen in kaart brengen.

1.4 Scope van dit document

Dit document beschrijft alle netwerk gerelateerde onderdelen die moeten worden aangepast of verplaatst om de beschikbaarheid van applicaties te verhogen. Hieronder vindt u een in scope/out of scope lijst t.b.v. de Heliomare netwerk infrastructuur voor dit document:

In scope:

- WAN verbindingen
- SD-WAN / SASE
- LAN
- Wi-Fi
- 2e en 3e lijns beheer van in scope zijnde netwerk infrastructuur
- Active monitoring van in scope zijnde netwerk infrastructuur

Out of scope:

- 1e lijns beheer van in scope zijnde netwerk infrastructuur
- KPN mobiele & vaste telefonie
- Clients en werkstations
- Zorgcommunicatie
- Medisch/Verpleegkundig Oproep Systeem (VOS/MOS)

1.5 Pre-requisites

Het is noodzakelijk dat alle lopende projecten die van invloed zijn en raakvlakken hebben bekend zijn. Documenten die worden aangeleverd t.b.v. het bepalen van de design keuzes Heliomare of andere partijen worden geacht volledig en consistent met de werkelijkheid te zijn.

1.6 Raakvlakken met andere projecten

Lopende en bekende projecten en programma's binnen Heliomare die op dit moment actief of in voorbereiding zijn en raakvlakken hebben met dit project zijn:

1. Implementatie van een nieuw EPD van NEXUS;
2. Migratie van Citrix naar Azure Virtual Desktop en implementatie Azure Landing Zone;
3. Verhuizing private datacenter naar nog te bepalen locatie (fysiek of virtueel).

1.7 Keuzemomenten en ontwerpbesluiten

De informatie in de groene blokken geeft een globaal overzicht van te nemen beslissingen en feiten die van belang zijn voor de implementatie van de oplossing. Deze blokken kunnen ook als een samenvatting worden gezien van wat er in de paragraaf is besproken.

OB0X Hier wordt dan een keuzemoment of een ontwerp besluit nader toegelicht

1.8 Disclaimer

Dit document is tot stand gekomen met de gegevens die op het moment van schrijven bekend waren. Gegevens die nodig waren om dit document te vervaardigen zijn aangeleverd door Heliomare of haar externe leveranciers. Alle cijfers en berekening zijn tot stand gekomen op basis van deze gegevens.

1.9 Gerelateerde documenten

Document	Auteur	Datum
Architectuur v1.0.vsdx	Externe adviseur	21-02-2025
Locatieoverzicht v1.0 xls	Emiel Käller	21-11-2024

2. AANLEIDING EN ACHTERGROND

In dit document wordt een nieuwe netwerk architectuur beschreven. In dit hoofdstuk worden de redenen voor deze nieuwe architectuur benoemd. De nieuwe netwerk architectuur (SOLL-architectuur) moet de grootste pijnpunten wegnemen. Wanneer dit niet mogelijk is, worden de risico's en mitigerende maatregelen in dit document benoemd.

2.1 Wie is Heliomare

De opdrachtgevers zijn in deze 'Stichting Heliomare Onderwijs' en 'Stichting Heliomare' gezamenlijk, waarbij Onderwijs fungeert als penvoerder voor deze aanbesteding. Stichting Heliomare is niet aanbestedingsplichtig, maar doet vrijwillig mee in deze aanbesteding aangezien Stichting Heliomare Onderwijs wel aanbestedingsplichtig is.

'Niemand aan de zijlijn. Iedereen doet mee.'

Bij Heliomare hebben kinderen, jongeren en volwassenen met een beperking meer kans om weer mee te doen in de maatschappij. Heliomare ondersteunt hen zodat zij nu en in de toekomst zo zelfstandig mogelijk kunnen leven. Werkzaam op ruim 20 locaties is Heliomare de enige zorg- en onderwijsinstelling in Noord-Holland waar u voor een totaaloplossing terecht kunt. Onze expertisegebieden onderwijs, arbeidsintegratie, revalidatie, bewegen en sport zijn vaak onderdeel van dit totaalpakket. 'Niemand aan de zijlijn. Iedereen doet mee'. Voor ons is dat de belangrijkste drijfveer bij alles wat we doen

2.2 Versnipperde netwerkarchitectuur

Door versnipperde implementatie en het ontbreken van een change proces is er geen eenduidige netwerkarchitectuur. Netwerkcomponenten hebben op verschillende locaties een andere configuratie en documentatie is onvolledig. Heliomare maakt op diverse locaties gebruik van netwerkinfrastructuur van derden. Hierdoor heeft Heliomare geen totaal overzicht van haar netwerkomgeving, onvoldoende grip op prestaties, beschikbaarheid en veiligheid. In de eindsituatie voert Heliomare regie over alle netwerkinfrastructuur op alle locaties. Dat kan via eenmalige aanschaf (CAPEX) of as-a-service dienstverlening (OPEX).

OB1	Eenduidige netwerk architectuur, onafhankelijk van locatie.
OB2	Heliomare voert regie over de netwerkinfrastructuur op alle locaties.

2.3 Versnipperde security policy

Doordat componenten op verschillende locaties een andere configuratie hebben, is er geen eenduidige security policy. Network Access Control is niet op alle locaties beschikbaar, niet op alle netwerkpoorten ingericht en maakt gebruik van een niet gecentraliseerde database (Azure AD vs Microsoft AD). Netwerksegmentatie is niet consistent ingericht.

OB3	Eenduidige security architectuur, onafhankelijk van locatie.
OB4	Security architectuur moet voldoen aan wet- en regelgeving.

2.4 End-of-Support

Diverse netwerkcomponenten op diverse locaties zijn reeds end-of-support. Zie bijlage 4 *Locatieoverzicht v1.0.xls* voor een overzicht. Bij incidenten kan er geen beroep gedaan worden op fabrikant. Waardoor het herstellen van een dienst bij incidenten niet gegarandeerd kan worden. Dit vormt een gevaar voor de bedrijfsvoering van Heliomare en is niet acceptabel.

OB5	Er mag geen end-of-support apparatuur gebruikt worden in het netwerk van Heliomare.

2.5 Wi-Fi beperkt beschikbaar

Het Wi-Fi netwerk is op diverse Heliomare locaties beperkt beschikbaar. De beschikbaarheid van (zorg) applicaties kan niet op alle plaatsen binnen Heliomare gegarandeerd worden.

OB6	Heliomare beschikt in de eindsituatie over een volledig dekkend Wi-Fi netwerk op alle locaties.

3. ALGEMEEN

Heliomare heeft dit document opgesteld voor het ontwerpen van een concept nieuw netwerkinfrastructuur. Waarbij beschikbaarheid, prestaties en veiligheid worden verhoogd. Dit document beschrijft in grote lijnen de inrichting van netwerkcomponenten en afhankelijkheden. Deze inrichting is afhankelijk van het locatietype. Hierdoor beschikt Heliomare over een standaard netwerkinfrastructuur, welke de beschikbaarheid verhoogd en RTO verlaagt.
Tevens vormt dit document een naslagwerk welke als basis dient voor toekomstige wijzigingen aan de netwerkinfrastructuur.

3.1 Locatie type

Heliomare beschikt over diverse locaties. Iedere locatie is toegewezen aan een locatie type. De wensen en eisen aan het netwerk zijn afhankelijk van het type locatie en worden separaat opgesteld.

Locatie type	Omschrijving
A. Groot 24x7	Grote locatie waar 24x7 zorg wordt verleent
B. Groot 8x5	Grote locatie waar 8x5 onderwijs wordt gegeven
C. Midden 8x5	Middelgrote locatie waar 8x5 zorg wordt verleent met maximaal 10 werkplekken
D. Klein 8x5	Kleine locatie waar 8x5 zorg, onderwijs en/of dagbesteding wordt verleent met maximaal 2 a 3 werkplekken

3.2 Locatie overzicht

Locatiecode	Naam	Adres
HM01	Wijk aan Zee	Relweg 51, 1949 EC, Wijk aan Zee
HM02	De Velst	De Velst 1, 1963 KL, Heemskerk
HM03	De Alk	Van Harenlaan 23, 1813 KE, Alkmaar
HM04	Het HCA	Amstelstraat 5, 1823 EV, Alkmaar
HM05	REA/Arbeid	Flevoweg 11, 2318 BZ , Leiden
HM06	Babbels	Dudockweg 69, 1703 DC, Heerhugowaard
HM07	REA College	Amsterdamsevaart 268, 2032 EK, Haarlem
HM08	Amsterdam	Baarsstraat 35 - 39, 1075 RV , Amsterdam
HM09	Krommenie	Zuiderhoofdstraat 14, 1561 AL, Krommenie
HM10	Obdam	Overweg 7, 1713 HX, Obdam
HM11	De Ruimte	Het Schild 2a, 1704 EK, Heerhugowaard
HM12	Klas op Wielen BO	Kofschipstraat 12, 1826 CG, Alkmaar
HM13	Klas op Wielen VO	Lorentzstraat 3, 1821 BR, Alkmaar
HM17	Alkmaar	Frieseweg 13, 1823 CA Alkmaar
HM18	Heemstede (Praktijk Deen)	Handelslaan 2a, 2102 CW, Heemstede
HM19	Heemskerk (Reva centre)	Steenhouwerskwartier 29b, 1967 KD, Heemskerk
HM20	Amsterdam Zuid-Oost	Hoptille 465-467, 1102 PJ Amsterdam
HM21	Hoorn, Leef!	Nieuwe Steen 25b, 1625 HV, Hoorn
HM22	Heerhugowaard, Leef!	Beukenlaan 23 unit 129A, 1701 DA, Heerhugowaard
HM23	Heerhugowaard, REA	Stationsplein 75, 1703 WE, Heerhugowaard
HM24	Azure	Azure omgeving van Heliomare

In bijlage 4 *Locatieoverzicht v1.0.xlsx* is iedere locatie toegewezen aan een locatietype. Inclusief een indicatie van beschikbare netwerkapparatuur per locatie.

3.3 Componenten algemeen

De belangrijkste applicaties welke op de netwerkinfrastructuur zijn aangesloten zijn zorg, telefonie en werkplekken. Deze applicaties bestaan uit verschillende componenten die met elkaar verbonden worden middels de netwerkinfrastructuur. Hierdoor is de beschikbaarheid van deze applicaties direct afhankelijk van de onderliggende infrastructuur.

Een overzicht van zorg, telefonie en werkplek componenten van de IST situatie is in onderstaande tabel opgenomen, inclusief korte beschrijving.

Applicatie	Functie	Beheerpartij
Werkplek	Werkplekken voor medewerkers van Heliomare	Heliomare
COW	Computer on Wheels	Heliomare
Printers	Printen	Uniflow
Internet	Internet connectiviteit	KPN
EVPN	Verbindingen om locaties met elkaar te ontsluiten	KPN
LAN	Bedrade netwerkinfrastructuur	Huawei Bright / Maxcare
Wi-Fi	Draadloze netwerkinfrastructuur	Huawei Bright / Maxcare
Edge Firewall	Beveiliging internet toegang	Fortinet Bright
EPD	Electronisch Patient Dossier	SDB Group SPS Nexus
CLB	Zorgalarmering Heliomare	CLB
ONS	Elektronisch Cliënten Dossier	Nedap
Telefonie vast	Vaste telefoontoestellen op Heliomare locaties	KPN EEN
Somtoday en Parnassys	Leerling Volg Systeem	Topicus Somtoday
Telefonie mobiel	Mobiele telefonie voor medewerkers Vast-mobiel integratie middels ‘KPN Mijn Gesprek’	KPN EEN

Binnen Heliomare zijn meerdere beheerpartijen actief. Dit veroorzaakt mogelijk vertraging bij het oplossen van verstoringen. Om dit te voorkomen, stelt Heliomare duidelijke kaders op welke bij alle partijen bekend zijn. Wanneer nodig werken onderlinge partijen samen om een verstoring op te lossen.

OB7 De beschikbaarheid van het netwerk wordt bepaald door de strengste applicatie eisen.

OB8 Heliomare stelt duidelijke (beheer) kaders op welke bij alle partijen bekend zijn. Wanneer nodig werken onderlinge partijen samen om een verstoring op te lossen.

3.4 Architectuur concepten

Dit hoofdstuk beschrijft de functionele eisen waaraan zorg, telefonie en werkplek omgeving moet voldoen en geeft richting aan de technische implementatie die moet aansluiten bij de infrastructuur van Heliomare.
Door te werken met duidelijke, eenvoudige en afgebakende bouwblokken, welke het totale landschap vormen, kan een betrouwbare en beheersbare omgeving worden neergezet. Hierbij wordt tevens zo veel mogelijk naar standaardisatie gestreefd. In de volgende paragrafen worden alle bouwblokken benoemd, inclusief onderbouwing van wensen en eisen.

3.4.1 Zorg

De primaire bedrijfsvoering van Heliomare, en de veiligheid van haar cliënten, is volledig afhankelijk van de werking van zorgsystemen. Zonder deze systemen worden zorgmedewerkers niet genotificeerd wanneer cliënten hulp nodig hebben. Zorgsystemen moeten dan ook hoog beschikbaar zijn. Binnen zorgsystemen zijn er verschillende functionele bouwblokken, elk met eigen eisen aan beschikbaarheid.

3.4.1.1 Zorgoproepen cliënten

Cliënten kunnen op verschillende manier zorgoproepen plaatsen:

- Oproep module in kamer cliënt;
- Hals/pols zender;
- Slimme sensoren.

Deze oproepen worden middels Wi-Fi afgeleverd bij zorgmedewerkers welke voorzien zijn van een Wi-Fi toestel. De melding geeft voldoende informatie voor de zorgmedewerker om adequaat op de oproep te reageren.
Zorgoproepen van cliënten is het belangrijkste bouwblok binnen zorg en moet de allerhoogste beschikbaarheid bieden. Daarbij moet de tijd tussen het maken van een zorgoproep en afleveren hiervan op een handset zo kort mogelijk zijn. Dit stelt prestatie eisen aan de individuele bouwblokken.

OB9 ‘Zorgoproepen cliënten’ heeft een beschikbaarheid van 99,9% met een RTO van 120 minuten.

OB10 De maximale tijd tussen een zorg aanvraag en aflevering bij een eerste zorgmedewerker bedraagt 10 seconden.

3.4.1.2 Spreek-luister verbindingen

Wanneer zorgmedewerkers een zorgoproep op een handset ontvangen, kunnen zij middels VoWi-Fi een spreek-luister verbinding opbouwen met de cliënt. Hierdoor kan de zorgmedewerker de prioriteit van de zorgaanvraag bepalen en op basis hiervan reageren.
Wanneer spreek-luister verbinding niet mogelijk is, moet een zorgmedewerker alle aanvragen met hoge prioriteit behandelen. Dit gaat ten koste van de efficiëntie, maar een lagere beschikbaarheid is acceptabel.
Onderliggende infrastructuur moet voldoende prestaties bieden voor een spreek-luister verbinding met hoge kwaliteit. Spraakkwaliteit in een IP-netwerk wordt gemeten in Mean Opinion Score (MOS). Hierbij staat MOS 5 voor de hoogste en MOS 1 voor de laagste spraak kwaliteit. ISDN heeft een gesprekskwaliteit van MOS 4.0.

OB11 Spreek-Luister verbinding heeft een beschikbaarheid van 99,0% met een RTO van 240 minuten.

OB12 Spreek-Luister verbinding heeft een minimale gesprekskwaliteit van MOS 4.0.

3.4.1.3 Camerabeelden

Heliomare maakt nog geen gebruik van camerabeelden. Maar camerabeelden zullen in de nabije toekomst naar verwachting geïntroduceerd worden. Door het gebruik van slimme camera's kunnen zorgmedewerkers efficiënter werken. Wanneer camerabeelden niet beschikbaar zijn, moet een zorgmedewerker mogelijkerwijs alle oproepen met hogere prioriteit behandelen. Dit gaat ten koste van de efficiëntie, maar een lagere beschikbaarheid is acceptabel.
Onderliggende infrastructuur moet voldoende prestaties bieden voor camerabeelden met acceptabele kwaliteit. Kwaliteit van camerabeelden wordt bepaald door resolutie en frame rate.

OB13 Camera beelden hebben een beschikbaarheid van 99,0%, een RTO en RPO van 240 minuten

OB14 Het netwerk moet geschikt zijn voor het gebruik van Camerabeelden met een minimale resolutie van 1280x960 en frame rate van 12 FPS

3.4.2 Onderwijs

De primaire bedrijfsvoering van Heliomare op onderwijslocaties is volledig afhankelijk van internet toegang. Zonder internettoegang kan er geen onderwijs worden gegeven.

OB15 Internet heeft een beschikbaarheid van 99,9% met een RTO van 120 minuten.

3.4.3 Telefonie

Een centraal telefonie platform verzorgt de telefonische bereikbaarheid van Heliomare. Deze omgeving verzorgt tevens de spreek-luister verbindingen in de zorg omgeving. Telefonie is belangrijk, maar de bedrijfsvoering van Heliomare is hiervan niet direct afhankelijk. Een lagere beschikbaarheid is acceptabel.
Onderliggende infrastructuur moet voldoende prestaties bieden voor een spreek-luister verbinding met hoge kwaliteit. Spraak- en videokwaliteit in een IP-netwerk wordt gemeten in Mean Opinion Score (MOS). Hierbij staat MOS 5 voor de hoogste en MOS 1 voor de laagste spraak kwaliteit. ISDN heeft een spraakkwaliteit van MOS 4.0.

OB16 'Telefonie' heeft een beschikbaarheid van 99,6% met een RTO van 120 minuten.

OB17 Telefoongesprekken hebben een minimale gesprekskwaliteit van MOS 4.0.

3.4.4 Videobellen

Videobellen en/of -vergaderen middels Microsoft Teams wordt binnen Heliomare gebruikt voor interne en externe communicatie. Dit is belangrijk, maar de bedrijfsvoering van Heliomare is hiervan niet direct afhankelijk. Een lagere beschikbaarheid is acceptabel.
Onderliggende infrastructuur moet voldoende prestaties bieden voor een video verbinding met hoge kwaliteit.

OB18 'Videobellen' heeft een beschikbaarheid van 99,6% met een RTO van 120 minuten.

OB19 Videogesprekken of -vergaderingen hebben een minimale gesprek- en videokwaliteit van MOS4.

3.4.5 Werkplek

Alle medewerkers van Heliomare hebben de beschikking over een Microsoft werkplek. Middels deze omgeving hebben medewerkers toegang tot systemen en informatie welke zij nodig hebben in hun dagelijks werk. Wanneer werkplekken niet beschikbaar zijn raakt dit de bedrijfsvoering van Heliomare.
De prestaties van de Microsoft werkplek moeten aansluiten wij de werkzaamheden van de medewerker. Systemen en informatie moet snel beschikbaar zijn, zonder wachttijden.

OB20 Microsoft werkplek heeft een beschikbaarheid van 99,6% met een RTO van 120 minuten.

OB21 Om prestaties te garanderen wordt voor iedere Microsoft werkplek 2 à 3 Mbps bandbreedte gereserveerd.

3.4.6 Internet

Het geven van onderwijs is sterk afhankelijk van SaaS applicaties en de onderliggende internet infrastructuur. Hierdoor is de primaire bedrijfsvoering van onderwijs locaties (locatietypen B, C en D) afhankelijk van internet connectiviteit.
SaaS applicaties moeten snel beschikbaar zijn, zonder wachttijden.

OB22 Internet connectiviteit op locatietype A & B heeft een minimale beschikbaarheid van 99,9% met een RTO van 120 minuten.

OB23 Internet connectiviteit op locatietype C & D heeft een minimale beschikbaarheid van 99,6% met een RTO van 240 minuten.

OB24 Om prestaties te garanderen wordt voor iedere Microsoft werkplek 2 à 3 Mbps bandbreedte gereserveerd. Capaciteit WAN verbindingen is gebaseerd op concurrent gebruik.

3.4.7 Partnership

De ontwikkeling van netwerk infrastructuur staat niet stil. Ook voor Heliomare worden continu interessante en relevante nieuwe oplossingen en diensten ontwikkeld en geïntroduceerd. Een partner die meedenkt met deze ontwikkelingen is een noodzaak voor het up-to-date houden van de netwerk infrastructuur die past bij de dienstverlening van Heliomare.

OB25 Heliomare zoekt een partner die meedenkt met de ontwikkelingen op het gebied van netwerk infrastructuur.

3.4.8

4. DESIGN PRINCIPES

Dit hoofdstuk beschrijft de eisen waaraan het netwerk moet voldoen. De eisen voor het ontwerp worden bepaald door applicaties welke afhankelijk zijn van netwerk connectiviteit.

4.1 Prestaties

Netwerkprestaties van het LAN komen met name terug in de bandbreedte van verbindingen. Onderstaand de uitgangspunten van de verschillende typen verbindingen.

- LAN Access – werkplek ontsluiting bedraad:
  - Twisted pair koper bekabeling CAT 6 (max 90 meter)
    Heliomare hergebruikt beschikbare bekabeling, ook wanneer deze beschikt over een lagere norm
  - 1 Gbps
  - PoE+ op alle access poorten
- Uplink – verbinding tussen access en core switch:
  - Type bekabeling; single-mode glas of multi-mode glas afhankelijk van afstanden, met een bandbreedte van 1Gbps.
    Op basis van inventarisatie van huidige omgeving en vergelijkbare omgevingen in andere zorg organisaties is 1Gbps voldoende. In uitzonderlijke gevallen moet deze capaciteit uitgebreid kunnen worden naar 10Gbps.
  - Minimaal 2 uplink verbindingen welke actief-actief in gebruik zijn wat resulteert in een totale bandbreedte van 2Gbps

OB26 Access switches zijn gestandaardiseerd op 1Gbps PoE+
OB27 1Gbps verbindingen tussen core en access switches

De prestaties van het Wi-Fi worden voornamelijk bepaald door de Wi-Fi-signaalkwaliteit van een client. De signaalkwaliteit is sterk afhankelijk van de plaatsing van Wi-Fi-accesspoints. De plaatsing van Wi-Fi-accesspoints wordt in een site survey bepaald. Uitgangspunt voor deze site survey is de meest belangrijke Wi-Fi client met de slechtste Wi-Fi antenne karakteristieken. Het uitvoeren van een Wi-Fi site survey en validatiemeting op iedere locatie maakt deel uit van de uitvraag.
Plaatsing van Wi-Fi-accesspoints is afhankelijk van waarvoor het netwerk wordt gebruikt: data, voice of location based services (LBS). Binnen Heliomare wordt gebruik gemaakt van location based services op locatietype A. Om optimaal voorbereid te zijn op LBS, dienen alle Wi-Fi access points te beschikken over BLE. Voor alle andere locaties wordt ingemeten op basis van data. In uitzonderlijke situaties wordt afgeweken van deze standaarden.

- Wi-Fi Access – werkplek ontsluiting draadloos:
  - Plaatsing Wi-Fi access points:
    - Word bepaald in een on-site Wi-Fi site survey
    - Afhankelijk van locatietype in combinatie met Wi-Fi client
    - Afhankelijk van capaciteit en gewenste bandbreedte van draadloze gebruikers
    - Wi-Fi nameting om gebruikerservaringen te verifiëren
  - Gebruik van 5 en 6 GHz frequentieband voor bedrijfskritische netwerken
  - Gebruik van 2.4 GHz frequentieband voor niet kritische netwerken, bijvoorbeeld gast internet

OB28 Uitgangspunt voor een Wi-Fi site survey is de meest belangrijke Wi-Fi client met de slechtste Wi-Fi antenne karakteristieken.
OB29 Locatietype A: plaatsing Wi-Fi access points op basis van location based services
OB30 Overige locatietypen: plaatsing Wi-Fi access points op basis van data
OB31 Alle Wi-Fi access points moeten beschikken over een BLE radio

4.2 Beschikbaarheid

De beschikbaarheid van het netwerk wordt bepaald door het belang van deze infrastructuur voor uw organisatie. Onderstaand de uitgangspunten welke Heliomare hanteert in het ontwerp van het netwerk.

- Uptime is afhankelijk van locatietype.
- Redundantie voor enkelvoudige fouten. Kritieke componenten en uplink verbindingen zijn redundant (dubbel) uitgevoerd en wanneer mogelijk geografisch gescheiden. Eén fout kan niet leiden tot uitval van het netwerk op een locatie.
- Redundante WAN verbindingen voor locatietypen A en B. 2e verbinding beschikbaar als backup ter voorkoming van uitval.
- Geen actief gebruik van spanning-tree protocol (STP). Door redundant aansluiten van switches en het aggregeren van verbindingen is STP niet actief in gebruik. STP is actief, maar alleen als backup.
- Standaardisatie netwerkcomponenten. Generieke netwerkcomponenten moeten zoveel mogelijk uitwisselbaar zijn tussen de locaties. Bij verstoringen is op de A en B locaties spare voorraad reeds aanwezig. Bij opheffing van een locatie kunnen componenten hergebruikt worden op andere locaties.

OB32	Uptime: locatie A & B: 99,9%, C & D: 99,6%
OB33	Dubbele WAN verbindingen voor locatie A & B ten behoeve van redundantie
OB34	Geen actief gebruik van spanning-tree protocol (STP)
OB35	Standaardisatie netwerkcomponenten; netwerkcomponenten zijn zoveel mogelijk uitwisselbaar

4.3 Veilig

Het netwerk geeft toegang tot vrijwel alle gegevens in uw organisatie. Toegang tot deze gegevens moet beheerd worden. Vanuit bedrijfsvoering maar ook vanuit regelgeving, bijvoorbeeld AVG.

- Netwerk ontwerp gebaseerd op NIST CSF
- Zero-trust
    - Middels Network Access Control (NAC) krijgen alleen geverifieerde gebruikers of netwerkapparaten toegang tot het netwerk (bedraad en draadloos)
    - Gebruikers of netwerkapparaten krijgen automatisch rechten toegewezen. Deze rechten bepalen waarmee wel en niet gecommuniceerd kan worden.
    - Management toegang tot netwerkcomponenten op basis van TACACS
- Beveilig Wi-Fi netwerken met minimaal WPA2-Enterprise beveiliging
- Vermijd complexe netwerkarchitecturen
- Gast verkeer is volledig gescheiden van het productienetwerk van Heliomare
- Captive portal voor gasten van Heliomare

OB36 Inzet van Network Access Control voor alle bedrade en draadloze netwerkapparatuur.
OB37 Automatisch toewijzen van rechten voor alle bedrade en draadloze netwerkapparatuur. Rechten bepalen waarmee wel of niet gecommuniceerd kan worden.

5. ARCHITECTUUR

Dit hoofdstuk beschrijft een architectuur welke voldoet aan de gestelde eisen en design principes.

5.1 Kwaliteit

Gezien de afhankelijkheid van het netwerk voor de bedrijfsvoering stelt Heliomare hoge eisen aan de kwaliteit van netwerkapparatuur. Het Gartner® Magic Quadrant™ is een betrouwbare indicator is voor de kwaliteit en betrouwbaarheid van producten en oplossingen. Producten van fabrikanten in het leiderskwadranten wordt gezien als topproducten welke zich hebben bewezen in de praktijk. Heliomare maakt alleen gebruik van apparatuur van fabrikanten in het leiderskwadrant.

OB38 Leverancier van SD-WAN apparatuur is een leider in 2024 Gartner® Magic Quadrant™ for SD-WAN
OB39 Leverancier van LAN en Wi-Fi apparatuur is een leider in 2024 Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure
OB40 Leverancier van Firewalls is een leider in Gartner® Magic Quadrant™ for network firewalls (op moment van schrijven is de meest recente versie van 2021)

5.2 Internet & SD-WAN/SASE

Internet verzorgt de connectiviteit naar publieke diensten. Applicaties migreren meer en meer naar publieke cloud diensten. In dergelijke gevallen communiceren werkplekken direct met deze internetdiensten. Hierdoor is de bedrijfsvoering van Heliomare direct afhankelijk van de beschikbaarheid en prestaties van de internet ontsluiting.
SD-WAN of SASE zorgt ervoor dat er automatisch VPN verbindingen opgebouwd worden tussen locaties onderling en naar private datacentra en vervangt het huidige IP-VPN. Logisch beschikt iedere locatie over 2 verbindingen: internet voor extern verkeer en VPN voor intern verkeer. Het internetverkeer wordt direct op locatie naar internet ontsloten: local internet break-out. Hierdoor is het aanvalsvlak voor hackers sterk vergroot. In plaats van één centrale internetverbinding zijn er nu meerdere internetverbindingen. Om de veiligheid te garanderen is het noodzakelijk dat alle internetverbindingen beschikken over standaard next-generation firewall faciliteiten, aangevuld met onderstaande security faciliteiten.

- **Application Control**
  Controle uitoefenen over het applicatiegebruik binnen de organisatie middels black- of whitelisten. Inclusief het prioriteren van bedrijfskritische applicaties (traffic shaping).
- **Botnet protection**
  Blokkeren van verkeer van en naar bekende botnet netwerken.
- **Intrusion Prevention System (IPS)**
  Beschermen van netwerken en systemen tegen ongeautoriseerde toegang, malware, aanvallen en andere potentiële bedreigingen.
    - Detectie van aanvallen: IPS bewaakt continu het netwerkverkeer en de systeemactiviteit om potentiële aanvallen te detecteren. Het gebruikt verschillende methoden en handtekeningen om verdachte patronen, gedragingen en bekende aanvalssignaturen te identificeren.

- Preventie van aanvallen: Nadat IDS een verdachte activiteit detecteerd, neemt het IPS actieve maatregelen om de aanval te voorkomen of te blokkeren voordat deze schade kan veroorzaken.
- Logboekregistratie en rapportage: bijhouden van gedetailleerde logboeken van activiteiten en incidenten.

- **IP/Domain Reputation**
  Verkeer van en naar bekende IP adressen of domeinen wordt geblokkeerd op basis van reputatie.
- **Web Filtering**
  Controle uitoefenen op het internetgebruik middels het monitoren en blokkeren van webactiviteiten op basis van classificatie.

OB41 SD-WAN of SASE voor het onderling ontsluiten van Heliomare locaties
OB42 Locatietypen A en B zijn voorzien van redundant
OB43 e verbindingen met gescheiden koppelvlak. Bijvoorbeeld door inzet van 4G/5G routers
OB44 Beveiligen van internet connectiviteit middels: IPS, botnet protection, IP/Domain reputation, application control en web filtering.

5.3 LAN

5.3.1 Core

Type A locaties worden voorzien van 2 fysieke core switches welke, waar mogelijk, geografisch gescheiden opgesteld zijn. Beide core switches zijn voorzien van redundante voedingen en ventilatoren en vormen één logische switch. Vanuit beheers oogpunt wordt er maar een switch beheert, er is geen dubbele configuratie noodzakelijk.
Hierbij word 'enkelvoudige' redundantie gehanteerd; uitval één netwerkcomponent, verbinding, voeding of MER heeft geen impact op de beschikbaarheid. Core switches ondersteunen in-service-software-updates

Type B locaties worden voorzien van 2 minimaal fysieke core switches welke ook dienst doen als access switch. Wat betekend dat deze switches zowel de ontsluiting naar SER ruimten verzorgen als het ontsluiten van client apparatuur. Core-access switches vormen één logische switch. Vanuit beheers oogpunt wordt er maar een switch beheert, er is geen dubbele configuratie noodzakelijk.

Er wordt geen core switches ingezet op type C en D locaties.

OB45 A locatie: geografische scheiding van core switches, 'Enkelvoudige' redundantie, in-service-software-updates
OB46 B locatie: inzet van core-access switches welke ontsluiting SER & client apparatuur verzorgen

5.3.2 Access

Werkplekken worden middels access switches op het netwerk aangesloten.
Alle fysieke switches in een SER dienen voorzien te zijn van redundantie in de aansluiting naar de MER switches. Iedere SER wordt direct met de iedere core switch verbonden met 1x 1Gbps, wat resulteert in een totale bandbreedte van 2Gbps. Deze bandbreedte moet waar nodig uitgebreid kunnen worden naar 4Gbps.

Het aantal apparaten wat middel Power over Ethernet gevoed wordt, neemt toe. Daarnaast neemt het vermogen per apparaat toe. *De hoeveelheid vermogen via PoE dient toekomstbestendig te zijn zodat dit geen belemmeringen oplevert bij toekomstig gebruik van bijvoorbeeld camera's.*

OB47 Alle access switches in een MER/SER worden redundant aangesloten.
OB48 Access switches ondersteunen PoE+ met minimaal 740 watt PoE budget.

5.4 Wi-Fi

5.4.1 Access Point

Heliomare heeft een sterke voorkeur voor inzet van Wi-Fi6E of Wi-Fi7 welke de 6 GHz frequentieband beschikbaar maken. De definitieve keuze van Wi-Fi standaard is afhankelijk van de bijbehorende investering. Heliomare vraagt u om twee voorstellen uit te werken: een op basis van Wifi 6E en een op basis van Wifi 7.

OB49 Heliomare kiest voor Wi-Fi6E of Wi-Fi7 op basis van de bijbehorende investering.

5.4.2 SSID

Onderstaande draadloze netwerken worden ingericht. SSIDs worden niet over meerdere radio frequenties geactiveerd. In de huidige situatie is 5 GHz niet volledig dekkend en is Wi-Fi redesign noodzakelijk.

SSID	Omschrijving	Band	Encryption
Internet	Open netwerk zonder captive portal met enkel internet toegang. Bandbreedte limiet 10 Mb per gebruiker.	2.4 GHz	Open
Heliomare_Data	Beveiligd netwerk voor laptops van medewerkers en MDM managed devices. Op basis van AD attributen worden rechten op het netwerk toegewezen.	5 GHz	WPA2-Enterprise EAP-TLS
Heliomare_IOT	Wi-Fi netwerk voor apparaten welke niet beschikken over een certificaat maar wel verbinding moeten hebben met het netwerk. Op basis van DHCP, fingerprinting en MAC adres worden rollen aan devices toegekend.	2.4 GHz[1] & 5 GHz	WPA2-Personal PSK

[1] Indien IoT apparatuur geen 5 GHz ondersteunt

Op alle draadloze netwerken is client isolatie actief. Hierdoor kunnen clients niet onderling met elkaar communiceren. Het gebruik van Chromecast of andere casting is blijft mogelijk, ook in netwerken met client isolatie.

OB50 Inrichting SSIDs volgens bovenstaande tabel.

5.5 Quality of Service

Netwerkverkeer van realtime applicaties, zoals voice en video, moeten voorrang krijgen om verstoring te voorkomen. Quality of Service (QoS) prioriteert het netwerkverkeer en is beschikbaar in onderstaande standaarden.

- IETF DiffServ (RFC2474) (Layer 3)
- IEEE 802.11e (WME / WMM)
- IEEE 802.1p (Layer 2, Frame priority)
- IEEE 802.1q (Layer 2, 4 bytes header voor VLAN tagging)

In onderstaande tabel zijn de QoS waarden opgenomen binnen het netwerk. Deze waarden worden in alle LAN componenten correct geconfigureerd.

Type	TOS byte (With DiffServe codepoint)		IEEE 802.1 p/q	WMM
	Binair	Decimaal		
VoIP Payload	EF	184	5	
VoIP Signalling	AF31	104	3	Voice

OB51 Quality of Service wordt end-to-end ingericht

5.6 Network Access Control

Iedere gebruiker of apparaat welke op het netwerk wordt aangesloten, bedraad of draadloos, wordt geauthentiseerd door Network Access Control (NAC). Authenticatie op basis van 802.1X of MAC met koppelingen naar een database. Hierbij worden reeds beschikbare gegevens in bijvoorbeeld Microsoft Active Directory of Azure Active Directory gebruikt voor netwerk authenticatie en worden gegevens niet dubbel beheerd.
Wanneer een client geen 802.1X ondersteunt, vindt een fallback naar MAC authenticatie plaats. Waarbij gebruik moet worden gemaakt van 'fingerprinting'. Hierbij wordt niet alleen het MAC-adres, maar ook de chipset, operating software en andere zaken opgeslagen in een fingerprint. Door het gebruik van fingerprinting wordt voorkomen dat ongewenste apparatuur middels MAC-spoofing toegang krijgt tot het netwerk. Wanneer een client in een bepaalde categorie, zoals IP camera, telefoontoestel of printer, toegang heeft tot het netwerk, kan ook nieuwe apparatuur uit dezelfde categorie toegang krijgen tot het netwerk.
Daarnaast toont Network Access Control alle apparatuur die op het netwerk is aangesloten. Dit is belangrijk, daar veel IT aanvallen van binnenuit komen. U kunt uw gegevens alleen goed beveiligen als u weet wat er op uw netwerk is aangesloten.
Network Access Control wordt redundant geplaatst in de Azure omgeving van Heliomare. Dit is een toekomstvaste locatie, daar op middellange termijn naar verwachting het datacenter van Heliomare uitgefaseerd wordt.

OB52 Inzet van Network Access Control (NAC) voor het ontsluiten van alle bedrade en draadloze clients, uitgezonderd gasten/cliënten.

OB53 Redundante NAC omgeving wordt geplaatst in de MS Azure omgeving van Heliomare.

5.7 Universal ports

Na authenticatie door Network Access Control (NAC) wordt de gebruiker of het apparaat automatisch, zonder handmatige interventie, geprofileerd en netwerkrechten toegewezen. Netwerkrechten worden ingericht op basis van functie en de daarbij behorende toegang. Een printer wordt automatisch in het printer netwerk opgenomen en een telefoontoestel in het telefonie netwerk, zonder handmatige tussenkomst van een beheerder. Netwerkbeheer is niet meer betrokken bij verhuizingen wat de operationele kosten verlaagt zonder concessies op beveiliging. Onbekende apparatuur zal bij eerste connectie geïsoleerd worden, toegang wordt gegeven na goedkeuring/toewijzing van een profiel door de beheerder.

OB54	Inzet van universal ports.

5.8 Microsegmentatie

Al het netwerkverkeer van gebruikers, bedraad en draadloos, wordt centraal afgeleverd op een statefull firewal. Op de statefull firewall wordt centraal bepaald waarmee de gebruiker of het apparaat wel of niet mag communiceren. Ook wanneer dit apparatuur in hetzelfde VLAN betreft. Dit wordt micro segmentatie genoemd en brengt een hoger beveiligingsniveau met zich mee. Dit resulteert in een uniform securitybeleid voor bedraad en draadloos verkeer.

Voordelen overlay netwerkarchitectuur:

- Veilig:
  - Centrale Role Based Policy Management & Enforcement
  - Consistente security policy voor bekabelde en draadloze gebruikers
  - Microsegmentatie; beveiligen van east-west verkeer
  - Zero Trust security policy
- Flexibel:
  - Terugdringen van netwerksegmenten
  - Inzet van locatie overstijgende netwerksegmenten (VLANs)
  - Eenvoudig toevoegen van nieuwe netwerken op één centrale omgeving, zonder aanpassingen op onderliggende infrastructuur
- Inzicht:
  - Inzage in applicatiegebruik in uw organisatie
  - Prioritering voor bedrijfskritische applicaties
- Eenvoudige adoptie en migratie:
  - Bestaande VLAN segmentatie kan gebruikt worden als underlay netwerk
  - 'Traditioneel' en 'underlay/overlay' kunnen naast elkaar bestaan zonder uitval van diensten

OB55	Inzet van microsegmentatie voor alle bedrade en draadloze netwerkapparatuur.

5.9 Management

Een centraal beheerplatform voor netwerkapparatuur biedt diverse voordelen:

- Efficiënt beheer: Uniforme configuraties en centrale monitoring vereenvoudigen netwerkbeheer en verminderen menselijke fouten
- Kostenbesparing: Minder handmatige taken en voorspelbare abonnementskosten optimaliseren IT-resources
- Zichtbaarheid en controle: Realtime inzicht in netwerkstatus en trends versnelt probleemoplossing en optimaliseert prestaties
- Schaalbaarheid: Eenvoudige uitbreiding en beheer van netwerken, ongeacht de grootte
- Verhoogde beveiliging: Snelle implementatie van beveiligingsupdates en naleving van regelgeving door centraal beheer
- Automatisering en integratie: Ondersteunt API-koppelingen en automatisering van repetitieve taken

OB56	Alle netwerkapparatuur wordt beheerd middels één centrale beheerportal
OB57	Heliomare heeft een voorkeur voor een cloud based beheer omgeving

6. NETWORK SERVICES

6.1 Dynamic Host Configuration Protocol (DHCP)

DHCP verzorgt uitgifte van unieke IP adressen op het computernetwerk. DHCP is centraal ingericht middels twee Microsoft AD controllers. Op enkele locaties is DHCP ingericht op een lokale firewall.

In de SOLL situatie worden IP adressen uitgegeven door de lokale firewalls/gateways. Hierdoor is er geen afhankelijkheid van een centrale omgeving wat de beschikbaarheid van de dienst verhoogd.

OB58 Lokale firewalls/gateways verzorgen DHCP, Management is Centraal beheerd

6.2 Domain Name Service (DNS)

DNS is centraal ingericht middels twee Microsoft AD controllers. Op enkele locaties is DNS ingericht op een lokale firewall.

Malafide DNS servers kunnen gebruikt worden om bedrijfsinformatie uit het netwerk van Heliomare te versturen. Dit is ongewenst. Alleen vertrouwde DNS servers mogen gebruikt worden. Een whitelist bepaald welke publieke DNS servers gebruikt mogen worden in de omgeving van Heliomare.

Op locaties waar medische apparatuur gebruikt wordt, kan gebruik gemaakt worden van een interne DNS server.

OB59 Heliomare maakt gebruik van publieke DNS servers op basis van whitelist. Op locaties waar medische apparatuur gebruikt word, kan een private DNS server gebruikt worden, evt per VLAN

6.3 Network Time Protocol (NTP)

NTP zorgt ervoor dat alle (netwerk)apparatuur met voorzien is van dezelfde datum en tijd. Dit is met name belangrijk wanneer logging van verschillende systemen geanalyseerd moet worden. Lokale firewalls/gateways verzorgen NTP op een locatie

OB60 Lokale firewalls/gateways verzorgen NTP