Beschrijving van de huidige en toekomstige situatie

Den Haag, oktober 2024
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Versie	Datum	Auteur	Wijzigingen
0.9	07-08-2024	[]	

INHOUDSOPGAVE

Figuren

Tabellen

Legenda

De volgende afkortingen zullen in dit document worden gebruikt:

Afkorting	Beschrijving	
BGP	Border Gateway Protocol	
DACL	Dynamic Access Control List	
DNS	Domain Name System	
HA	High Availability	
HLD	High Level Design	
IP	Internet Protocol	
LAN	Local Area Network	
LLD	Low Level Design	
MER	Main Equipment Room	
MSP	Multi Service Port	
NBD	Next Business Day	
OSPF	Open Shortest Path First	
PoE	Power over Ethernet	
SER	Satellite Equipment Room	
SFP	Small form-factor pluggable	
VLAN	Virtual Local Area Network	
VM	Virtual Machine	

Tabel 1: Afkortingen

1 INTRODUCTIE

Het High Level Design (HLD) beschrijft het globaal technisch ontwerp van de nieuw te ontwerpen netwerk infrastructuur ten behoeve van de netwerkswitches. Het HLD geeft in deze inzicht in de huidige situatie (IST) en de gewenste situatie (SOLL).

Wat dit document niet is

Binnen dit document zijn de volgende onderdelen niet uitgeschreven:

- HLD van de gehele netwerkinfrastructuur en bijbehorende componenten van NWO.
- Details inrichting/configuratie van het netwerk ontwerp
- Cloud netwerk en netwerk security ontwerp

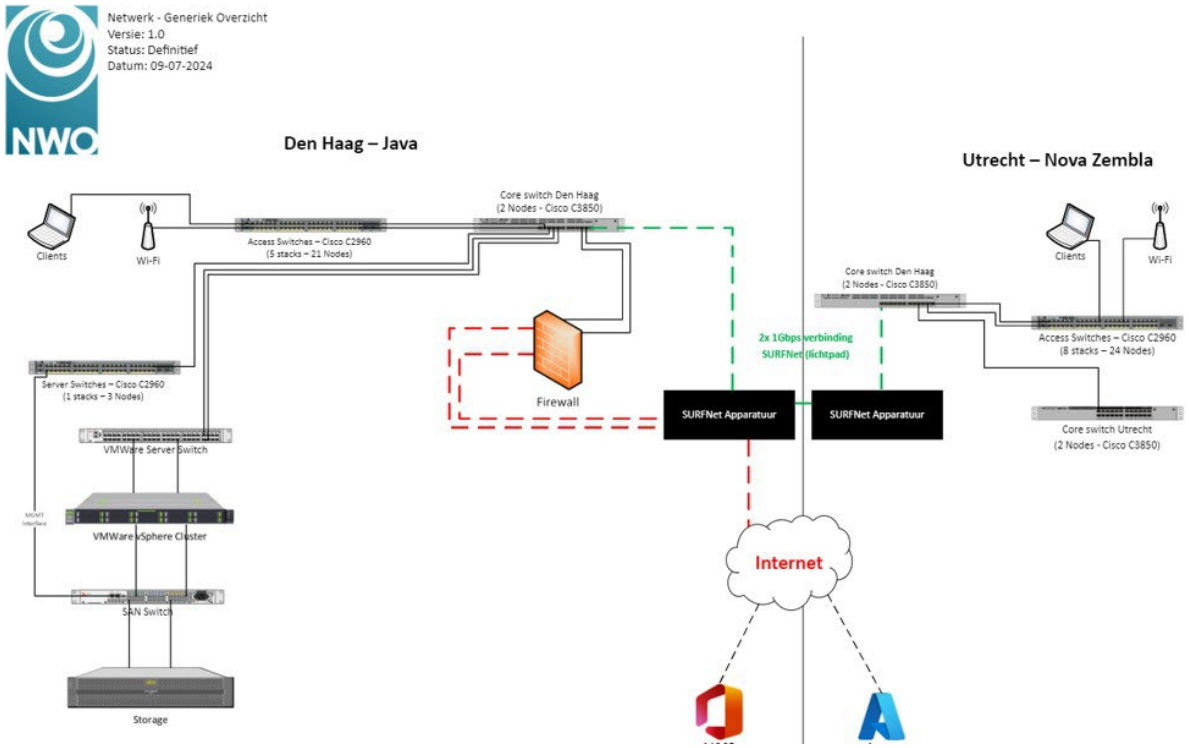
1.1 UITGANGSPUNTEN

Tijdens het schrijven van dit document is rekening gehouden met de volgende uitgangspunten:

- De IST-situatie is gebaseerd op informatie uit interview sessies en documenten die door NWO zijn verstrekt welke mogelijk niet volledig zijn.
- De SOLL-situatie is gebaseerd op informatie voortkomend uit geïnventariseerde uitgangspunten en design principes.

2 HUIDIGE SITUATIE (IST)

NWO beoogt middels deze aanbesteding de netwerkswitches op de NWO-locaties in Den Haag en in Utrecht te vervangen, hierbij wordt de huidige netwerkinfrastructuur gehandhaafd. Zie figuur onderstaand voor een globale weergave van de netwerkswitches binnen de netwerkinfrastructuur landschap van NWO.



Figuur 1: Generiek overzicht LAN/WAN netwerkinfrastructuur

Op zowel locatie Den Haag als locatie Utrecht is een Local Area Network (LAN) opgebouwd. Het LAN bestaat uit fysieke Cisco netwerk componenten welke geplaatst zijn in 'Main Equipment Room' (MER) en 'Satellite Equipment Room' (SER) op beide locaties. Op elke locatie is er 1 MER en meerdere SER's. SER's zijn verspreid over de verschillende etages per locatie.

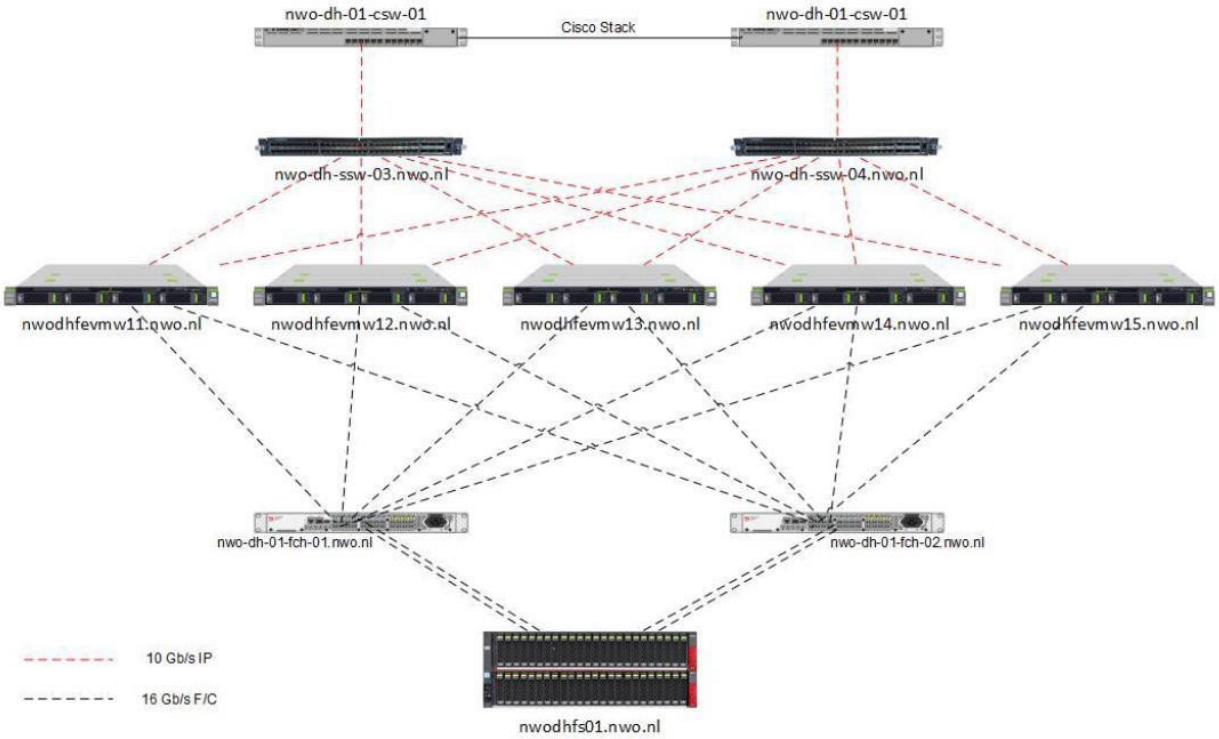
In de MER, voor zowel Den Haag als Utrecht, zijn de core switches geplaatst. Deze core switches zorgen voor de interne routeringen per locatie waarbij de core switches in Den Haag ook voorziet in de routering en de koppeling naar externe netwerken via het centrale Palo Alto firewall cluster.

Elke etage heeft een aantal access switches in de SER. Deze etage gebonden access switches zijn als 'stack' geconfigureerd. De access switches binnen één stack functioneren als één logische switch. Alle access switches ondersteunen POE (Power over Ethernet) voor access points en audiovisuele panelen. De access switches zijn weer verbonden aan de core switches middels Multimode glasvezel (Den Haag en Utrecht OM3 50/125).

De huidige server omgeving binnen NWO Den Haag is technisch opgedeeld in twee stukken:

- Cisco server stack waarop fysieke server/appliances gekoppeld zitten zoals Wireless Lan Controllers en NTP server.
- Fujitsu compute omgeving incl. Fujitsu netwerk en Brocade fiberchannel switches waarop de centrale VMWare omgeving met alle virtuele VM's voor NWO draaien.

De Cisco server stack is direct redundant gekoppeld op de Cisco core stack zoals, de Fujitsu server switches zijn



Figuur 2: Fujitsu compute omgeving incl. Fujitsu netwerk en Brocade fiberchannel switches

Binnen NWO Utrecht zijn enkel Cisco server switches waarop fysieke server/appliances gekoppeld zitten zoals een NTP server.

3 UITGANGSPUNTEN VOOR DE NIEUWE SITUATIE

NWO heeft voor de nieuwe LAN netwerk infrastructuur onderstaande specifieke wensen, eisen en uitgangspunten opgesteld. Deze dienen als grondslag voor het uitwerken dan het nieuwe netwerk infrastructuur design.

De uitgangspunten onderstaand vormen de basis voor de selectie en implementatie van de nieuwe netwerkswitches en zorgen ervoor dat de toekomstige netwerkoplossing voldoet aan de verwachtingen van NWO.

ID	Algemene design principes
AD1	**Beschikbaarheid** De netwerk infrastructuur dient 24x7 beschikbaar te zijn. De LAN en WAN netwerk infrastructuur dient volledig redundant opgezet te worden om een zo hoog mogelijke beschikbaarheid te garanderen. Een redundant uitgevoerde netwerkinfrastructuur is zodanig ingericht dat een verstoring geautomatiseerd wordt afgehandeld. De netwerk infrastructuur wordt zo ingericht dat de beschikbaarheid per locatie ten minste 99,9% is, gemeten over 24 uur per dag, over alle dagen per jaar, exclusief gepland onderhoud
AD2	**Locatie onafhankelijk** De netwerk infrastructuur op locatie Utrecht en Den Haag dient onafhankelijk operationeel te kunnen zijn. Dit betekent dat eventuele netwerk verstoringen op één van de NWO locaties, geen invloed mag hebben op het netwerk van de andere NWO locaties.
AD3	**Schaalbaarheid** De netwerk architectuur moet schaalbaar kunnen zijn. Bij uitbreiding van een gebouw, locatie en aantallen gebruikers moet de architectuur niet de remmende factor zijn. De gekozen oplossingen dienen zonder veel aanpassingen te herhalen zijn of uit te breiden zijn.
AD4	**Solutions** De netwerk infrastructuur moet de mogelijkheid bieden om de laatste technologieën te ondersteunen, echter wordt de keuze gemaakt om enkel “proven technology” te implementeren vanwege beschikbaarheid en security redenen. Hardware en software oplossingen van vendoren die geïmplementeerd worden bij NWO, dienen door Gartner beoordeeld te zijn binnen Gartner Quadrant als Leaders in de betreffende Hardware en Software oplossingen.
AD5	**Uniformiteit** Uniformiteit is te behalen door standaard bouwblokken en configuraties uit te rollen binnen de netwerk infrastructuur. Uniformiteit heeft als doel om beheer en wijzigingen/uitbreidingen, kosten efficiënt uit te kunnen voeren.
AD6	**Segmentatie** Het netwerk dient multi-level gesegmenteerd opgezet te worden zodat een beveiligingslaag eenvoudig geïntegreerd kan worden in de netwerk infrastructuur. We onderscheiden hierin macro en micro segmentatie waarbij macro scheiding tussen de verschillende virtuele netwerken is en micro de scheiding tussen de verschillende end points is. Doel is om met deze macro en micro segmentatie ook het impact domein te verkleinen doordat dataverkeer niet direct tussen bepaalde functionaliteiten/groepen/segmenten kan plaatsvinden.
AD7	**Security beleid** Het NWO beveiligingsbeleid dient eenvoudig over de nieuwe netwerk infrastructuur uitgerold te kunnen worden. Hierbij dient op macro als micro segmentatie niveau onderscheid gemaakt te kunnen

	worden tussen vertrouwde en niet-vertrouwde systemen/functionaliteit, authenticatie van personen en systemen uitgevoerd kunnen worden en rechten/policy's toegepast te kunnen worden.
AD8	**Beheersbaarheid** De netwerk infrastructuur dient door NWO efficiënt en centraal te kunnen worden onderhouden. Er dient een management platform beschikbaar te zijn voor monitoring, proactieve meldingen, historische data en troubleshooting, rapportages, diagnose tools. Beheer tooling kan eventueel centraal binnen locatie Den Haag of toekomstig in Azure IAAS geplaats worden echter is het algemeen ICT-beleid binnen NWO "cloud dienstverlening of anders".
AD10	**Open standaarden** Binnen de netwerk infrastructuur dient gebruik gemaakt te worden van standaard (open) technologieën en worden proprietary technieken of protocollen zoveel mogelijk vermeden. Het gebruik van open standaard technologie biedt vele voordelen, waaronder compatibiliteit met eventuele andere systemen.
AD11	**Maintenance** Het is mogelijk om wekelijks/maandelijks maintenance windows te plannen voor eventuele wijzigingen of beheerwerkzaamheden op de netwerk infrastructuur. Het uitsluitend "in service" wijzigingen of beheerwerkzaamheden uitvoeren is geen eis.
AD12	**Hardware support** De access laag binnen de netwerk infrastructuur dient zoveel mogelijk gestandaardiseerd te worden op één hardware platform zodat doormiddel van 8x5xNBD hardware support en spare parts herstel snel uit te voeren is. Core componenten dienen in een 24x7x4 hardware support contract te zitten zodat herstel van redundancy snel uit te voeren is.
AD13	**Software support** Alle hardware dient in een support contract bij de vendor ondergebracht te zijn. Enerzijds voor recht op de laatste software versies, anderzijds voor eventuele support op software bij incidenten. Het is daarnaast van groot belang dat de netwerkapparatuur beschikt over de laatste major stabiele softwareversie. Dit is belangrijk omdat elke softwareversie bugs, kwetsbaarheden en beveiligingsproblemen kan bevatten die kunnen worden uitgebuit door kwaadwillende actoren.
AD14	**Beheer/Regie** De nieuwe netwerk infrastructuur dient volledig in eigendom en in eigen beheer te kunnen worden genomen door NWO. Echter dient de mogelijkheid er te zijn om ondersteunende supportdiensten af te nemen. Wel is behoefte aan duidelijkheid en transparantie over de te leveren ondersteuning vanuit de beoogde Leverancier om zorg te dragen dat de afbakening van de verantwoordelijkheden tussen NWO en de leverancier helder en gedocumenteerd zijn.
AD16	**Naamconventie** Het toewijzen van naamconventie binnen de netwerk infrastructuur dient volgens de standaard binnen NWO te gebeuren.
~~AD17~~	~~**Monitoring**~~ ~~Alle oplossingen dienen middels een third party tool gemonitord kunnen worden op basis van SNMP, SSH, SFTP of API.~~ Vervalt n.a.v. vraag 17, Nota van Inlichtingen 1.
~~AD18~~	~~**Quality of Service**~~ ~~In het algemeen is traditioneel QoS niet een vereiste binnen de LAN infrastructuur wanneer de volgende criteria van toepassing zijn:~~ • ~~Recente aangeschafte apparatuur met features als jitter buffers, processor buffers en memory buffers~~ • ~~Voldoende bandbreedte beschikbaar, voornamelijk op interlinks binnen het netwerk~~ • ~~Firewall cluster die applicatie bewust is en voorrang geeft aan latency gevoelige data naar WAN~~ ~~QoS configuraties zouden pas als de noodzaak er is, wel overwogen, geïmplementeerd moeten worden.~~ Vervalt n.a.v. vraag 17, Nota van Inlichtingen 1.

AD19	**Vendor keuze** NWO wil deels vasthouden aan de vendor keuze die in het verleden gemaakt is: • Wired op basis van een merk switch wat valt binnen het Gartner Quadrant als Leaders in de betreffende Hardware en Softwareoplossingen NWO heeft hierbij de afweging gemaakt om: 1. Verregaande integratie binnen één eco systeem/platform van één vendor. Er is gekozen voor het tweede punt.

Tabel 2: Algemene design principes

De hieronder beschreven design principes vormen de basis voor de eisen waaraan het type netwerkswitch moet voldoen. Deze principes, ofwel eisen, zorgen onder meer ervoor dat de netwerkswitches compatibel zijn met de bestaande infrastructuur, voldoen aan de prestaties- en beveiligingseisen, en schaalbaar zijn voor toekomstige uitbreidingen. Zie ook Bijlage E, Programma van Eisen, voor een volledige beschrijving van de eisen behorend tot deze aanbesteding.

ID	LAN design principes
LD1	Binnen de access laag worden switches ingezet die minimaal de volgende zaken ondersteunen: - 48 poorten - Mix van 1G t/m 10G access poorten - Minimaal 10G SFP uplink poorten - UPOE of POE++ (IEEE 802.3bt) - Interne redundante voedingen - Stacking technologie, MLAG of vergelijkbaar - Fully manageable - Geavanceerde securityfeatures - SFP-modules van fabrikant - Ondersteuning van centrale monitoring/beheer tool Op beiden NWO-locaties dient een hot spare aanwezig te zijn.
LD2	Binnen de core laag worden switches ingezet die minimaal de volgende zaken ondersteunen: - Minimaal 10G SFP uplink poorten - Interne redundante voedingen - Stacking technologie, MLAG of vergelijkbaar - Fully manageable - Geavanceerde securityfeatures - SFP-modules van fabrikant - Ondersteuning van centraal monitoring/beheer tool
LD3	Waar meerdere switches in dezelfde kast worden geïnstalleerd, dienen deze gestacked te worden als één logische entiteit.
LD4	Binnen de netwerk infrastructuur worden enkel originele SFP's gebruikt vanwege verlenen van operationele support vanuit de fabrikant.
LD5	Alle LAN-componenten dienen IPv4, IPv6 en dual-stack te ondersteunen.
LD6	Wanneer dynamic routing noodzakelijk binnen de LAN infrastructuur noodzakelijk is: • Interne routing op basis van OSPF • Externe routing op basis van BGP
LD7	Het Default VLAN dient niet te worden gebruikt, netwerk apparatuur dient via afgeschermd management VLAN benaderd te worden.
LD8	VLAN stretching over netwerk infrastructuur Den Haag en Utrecht moet mogelijk zijn voor redundantie/uitwijk oplossingen binnen LAN/WAN/Compute netwerken. Vlan stretching op access laag voor end points is niet toegestaan.

LD9	Macro segmentatie dient doormiddel van security zones en VLAN's geïmplementeerd te worden. Hierbij dient het aantal security zones en VLAN's wel overwogen te worden om complexiteit te beperken.
LD10	Micro segmentatie dient doormiddel van DACL geïmplementeerd te worden.
LD11	IP subnets/broadcast domeinen, dienen niet groter te zijn dan /23 subnets
LD12	Binnen de LAN infrastructuur mogen zich VLAN's bevinden die, via de centrale firewall, directe toegang naar internet hebben. Deze internet VLAN's mogen onder geen enkele voorwaarde kunnen communiceren met andere segmenten binnen de LAN-infrastructuur.
LD13	Binnen de LAN-infrastructuur dient zoveel mogelijk DNS naming plaats te vinden
LD14	De huidige beschikbare poorten zijn voldoende voor de toekomstige behoefte van NWO. Voor nu zijn er geen redenen vanuit de overige designs binnen het NDF programma dat deze behoefte wijzigt bijvoorbeeld door een wireless-only beleid.
LD15	Alle hardware zal volgens de markt en vendor standaarden gehardend moeten zijn waarmee de beveiliging wordt verbeterd ter voorkoming van oneigenlijk gebruik.
LD16	Toegang tot hardware dient via protocollen te gaan die encryptie ondersteunen. Toegang dient centraal geregeld te zijn waarbij ook inzicht is wie en wanneer heeft ingelogd.

Tabel 3: LAN design principes

ID	Omgeving design principes
OD1	Nieuwe interne bekabeling dient minimaal CAT6A UTP bekabeling en OS2/OM4 glas bekabeling te zijn. Bestaande UTP bekabeling dient minimaal CAT5E te zijn. Bestaande glas bekabeling dient minimaal OS2/OM3 te zijn.
OD2	Patch bekabeling dient minimaal CAT6A bekabeling te zijn. Bij patching dient zoveel mogelijk de juiste kabellengte gebruikt te worden voor verminderen risico's op beschikbaarheid.
OD3	Alle hardware dient een redundante voeding te hebben en gekoppeld te worden met één voeding op de UPS en één voeding op de netspanning. Wenselijk is dat er ook twee spanningsgroepen zijn.
OD4	Alle MER/SER ruimtes en racks dienen fysiek gesloten, geconditioneerd en stofvrij te zijn.
OD5	Alle hardware binnen de netwerk infrastructuur dient gelabeld te zijn met hostname en/of NWO ID voor herkenning.
OD6	Alle MER/SER ruimtes dienen geconditioneerd te zijn vanwege meer warmteontwikkeling met moderne POE++ switches.

Tabel 4: Omgeving design principes

4 Nieuwe situatie (SOLL)

Op basis van deze uitgangspunten en de design principes is in een vooronderzoek een oplossingsrichting voorgeschreven. Dit onderzoek heeft geleid tot de aanbeveling van een specifiek type netwerkswitch (zie kitlijst, tabel 5) dat voldoet aan de gestelde uitgangspunten en eisen. De kitlist sturen we mee als indicatie waaraan de netwerkcomponenten minimaal v.w.b. functionaliteit en specificaties moeten voldoen, de keuze van het merk laten we echter vrij onder de voorwaarden dat de door de Leverancier voorgeschreven type netwerkswitches voldoen aan de eisen beschreven in Bijlage N "Programma Van eisen".

Artikel	Beschrijving	Aantallen	Info
C9500-40X-A	Catalyst 9500 40-port 10Gig switch, Network and DNA Advantage	4	Core laag (Advantage voor BGP)
CON-SNTP-C95004XA	Smartnet SNTC-24X7X4 Catalyst 9500 40-port	4	Smartnet support 24X7X4 5 jaar
PWR-C4-950WAC-R/2	950W AC Config 4 Secondary Power Supply front to back cooling	4	Secondaire voeding

C9300-48UXM-E	Catalyst 9300 48-port Network and DNA Essentials	30	Access laag, members met uplink module
CON-SNT-C93E048X	Smartnet SNTC-8X5XNBD Catalyst 9300 48-port	30	Smartnet support 8X5XNBD 5 jaar
PWR-C1-1100WAC-P/2	1100W AC 80+ platinum Config 1 Secondary Power Supply	30	Secondaire voeding
C9300-NM-8X	Catalyst 9300 8 x 10GE Network Module	30	Uplink module access - core
C9300-48UXM-E	Catalyst 9300 48-port Network and DNA Essentials	16	Access laag, members zonder uplink module
CON-SNT-C93E048X	Smartnet SNTC-8X5XNBD Catalyst 9300 48-port	16	Smartnet support 8X5XNBD 5 jaar
PWR-C1-1100WAC-P/2	1100W AC 80+ platinum Config 1 Secondary Power Supply	16	Secondaire voeding
STACK-T1-3M	3M Type 1 Stacking Cable	11	Lange stack kabels voor stacks > 3
SFP-10G-SR	10GBASE-SR SFP Module	60	SFP uplinks Access - Core
QSFP-40G-SR4	40GBASE-SR4 QSFP Transceiver Multimode Module	8	QSFP core SVL link
SFP-10G-SR	10GBASE-SR SFP Multimode Module	4	SFP core DAD link
SFP-10G-LR	10GBASE-LR SFP Single mode Module	4	SFP uplink surfnet lichtpad
SFP-10G-SR	10GBASE-SR SFP Multimode Module	4	SFP uplink firewalls - core
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	6	UTP uplink firewall HA1/2 en MGMT
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	2	UTP uplink Surfnet Internet en MSP
PAN-SFP-PLUS-SR	Palo Alto 10GBASE-SR SFP Multimode Module	4	SFP uplink firewalls - core
SFP-10G-SR	10GBASE-SR SFP Multimode Module	4	SFP uplinks Fujitsu - core
SFP-10G-SR (Fujitsu)	Fujitsu 10GBASE-SR SFP Multimode Module	4	SFP uplinks Fujitsu - core

Tabel 5: Kitlijst