Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Producten en Diensten Catalogus Netwerken CIV

Uitgegeven door:

Diensten Portfolio Manager	KPN Dedicated Organisatie Rijkswaterstaat (DO RWS)
Service Portfolio Manager	RWS CIV IRN INFRA NETWERKEN

Datum:	30-03-2023
Status:	Definitief
Versie:	11.0

1 Versie- en Distributieblad

1.1 Versie

In deze paragraaf worden de wijzigingen ten opzichte van eerdere versie bijgehouden. Een document wordt altijd in een x.9 versie aangeboden ter accordering en krijgt pas na akkoord de status “definitief” waarbij het versie nummer wordt opgehoogd naar (x+1).0.

1.2 Versiehistorie

Versie	Status	Datum	Auteur	Wijzigingen op vorige versie
0.7	Concept	27-07-2018	Jorinde Zwarts Carola de Ruijg	Volledig herziene versie
0.9	Concept	01-10-2018	Jorinde Zwarts Carola de Ruijg	Toevoeging bestelbare items ten behoeve van RWS CIV IRN Infra Netwerken
1.0	Definitief	01-11-2018	Jorinde Zwarts Carola de Ruijg	Volledig herziene versie
2.0	Definitief	01-7-2019	Jorinde Zwarts	Toevoeging Partner PDC rapportage, VPN aansluiting Connect en Interconnect, IDS IPS 24x7, CVR toegang en omgevingsmonitoring, LEG EPL, verduidelijking
3.0	Definitief	21-01-2020	Keesjan Koning	Toevoeging Draadloze aansluiting (legacy), Digitale Video aansluiting is legacy, Partyline verwijderd, MiniFEP aangepast, Type bestellingen aangepast, reverse Webproxy verwijderd uit dienstenmatrix, Draadloze Werkplek aansluiting is legacy, Tekening CVR Toegang en omgevingsmonitoring aangepast, Bandbreedte optie VPN aansluiting aangepast
4.0	Definitief	02-06-2021	Keesjan Koning	Toevoeging Noodknop Sytwendetunnel (Special), verwijdering Draadloze Werkplek aansluiting, aanpassing tekst MiniFEP, aanpassing naam Diensten Catalogus (DC) in Product en Diensten Catalogus (PDC), wijziging CT RWS in DO RWS, toevoeging uitgangspunt WIFI, aanpassing namen in Bijlage A, aanpassing tekst Netscaler in figuur 8, aanpassing tekst LAN aansluiting type Wegkant/waterkant, levertijd 'Wijzigen Virtual Firewall' aangepast van L10 naar L5, Service Level Dienst TBMS gewijzigd in ‘redelijke effort’, Externe koppeling IPsec ‘legacy’ vervallen en diverse aanpassingen/correcties tekst, nummering en verwijzingen.
5.0	Definitief	03-08-2021	Keesjan Koning	IDS/IPS wijziging, aanvulling Dienst LAN aansluiting CVR/VOR en Wegkant/Waterkant met optische interface, aanpassing Internet

				Access en diverse aanpassingen/correcties in de tekst.
6.0	Definitief	14-12-2021	Keesjan Koning	Wijziging voorwaarden Virtual Firewall; wijziging tekst MiniFEP; vernieuwde dienst RKN toegevoegd; Figuur Webproxy verwijderd; Beschikbaarheid LAN type gebouw en rekencentrum toegevoegd; dienst 'Open WIFI' toegevoegd; diensten Meekijkfunctie, Regierol en ISO27001 vervallen; uitfasering 3G KPN toegevoegd; beschikbaarheid Externe koppeling IPsec aangepast; dienst RijkskantoorRoam toegevoegd; links naar RWS VPR bijgewerkt en diverse aanpassingen/correcties in de tekst/figuren.
7.0	Definitief	17-03-22	Keesjan Koning	Tekst aanpassing Draadloze VPN aansluiting, Glasfunctieherstel en Kantelwalsbord vervallen, SIM Data niet meer bestelbaar, tekst aanpassing LAN aansluiting Type CVR/VOR/Wegkant/Waterkant en Digitale Video aansluiting ivm demarcatie IP Camera en wijziging servicelevel PPP/Draadloze aansluiting in 'redelijke effort' Dienstenmatrix Eindsystemen aangepast.
8.0	Definitief	30-06-22	Keesjan Koning	Inhoudsopgave aanklikbaar; (restant) Diensten Glasvezelfunctieherstel en Losse verbinding verwijderd; Service Level Dienst TBMS, PPP en Draadloos 'redelijke effort' in figuur 62 aangepast; Bijlage A aangepast.
9.0	Definitief	30-09-22	Barbara Koorn	Nieuwe dienst LAN aansluiting type SPAN toegevoegd; Dienst Losse verbinding (restant tekst) verwijderd; SIM Data niet meer bestelbaar gemaakt in figuur 48; Dienst Internet Access verwijderd.
10.0	Definitief	30-12-22	Barbara Koorn	Figuur 27: opmerking toegevoegd inzake netto bandbreedte i.g.v. huurlijnen; Aanpassing tekst Webproxy; SIM Data dienst verwijderd; Missiekritisch vervangen door Missiekritiek conform gebruikelijk bij RWS; Bij dienst Draadloze VPN aansluiting toegevoegd dat deze niet geschikt is voor missiekritieke systemen; Dienst Dark Fiber levering RWS aangescherpt met toevoeging goedkeuring Domeineigenaar Netwerken; door hele document wijzigingen aangebracht om dienstnamen in lijn te brengen met Prijzenblad Gecoördineerde Leveringen Nieuwe Stijl versie 1.1.

11	Definitief	30-03-23		Wijzigen SSID's WiFi nav uitfaseren BYOD via SSID RWS-intern en uitfaseren RWS GAST SSID, Update tekst Partner PDC Rapportages n.a.v. nieuwe afspraken, Dienst dark fiber verplaatst naar deel 1, Beheertarief LAN omgeving bedraad verwijderd, diverse tekstuele aanpassingen.

1.3 Goedkeuring

Dit document vereist de volgende goedkeuringen. De getekende goedkeuringslijst wordt bewaard in het managementdossier.

Functie
Supply Manager RWS
Delivery Manager KPN

1.4 Eigenaarschap

Dit document wordt onderhouden door KPN DO RWS en beschrijft de dienstverlening die KPN levert aan en beheert voor Rijkswaterstaat. CIV RWS INFRA NETWERKEN is eigenaar van deze netwerkdiensten.

Inhoudsopgave

1 Versie- en Distributieblad 2
1.1 Versie 2
1.2 Versiehistorie 2
1.3 Goedkeuring 4
1.4 Eigenaarschap 4
2 Inleiding 7
2.1 Doel 7
2.2 Opbouw 7
2.3 Dienstverlening RWS CIV IRN Infra Netwerken 8
2.3.1 Algemeen 8
2.3.2 Scope 8
2.3.3 Service Desk KPN DO RWS 9
2.4 Leveringsvoorwaarden 9
2.5 Bestellingen (standaard leveringen, tactische leveringen en ontwikkelingen) en verrekening 9
2.6 Partner PDC Rapportages 11
2.7 Definities en afkortingen 11
3 Diensten RWS CIV IRN Infra Netwerken 13
3.1 Inleiding 13
3.2 Categorie Backbone (BB), Core, Centrale Voorzieningen (CV) 13
3.2.1 Dienstenmatrix BB Core CV 13
3.2.2 Bestelbare items en levertijd 23
3.3 Categorie VPN - detailbeschrijving 23
3.3.1 Functionele omschrijving 23
3.3.2 Dienstenmatrix Categorie VPN 23
3.3.3 Virtual firewall 25
3.3.4 DDI 27
3.3.5 DMZ 30
3.3.6 Forward Webproxy 30
3.3.7 Mail relay 30
3.3.8 Bestelbare items en levertijd 30
3.3.9 Verrekening 31
3.4 Categorie Special 31
3.4.1 Beheer Verbindingen LEG-EPL (Lichteiland Goeree – Europlatform) 31
3.4.2 CCM aansluiting 33
3.4.3 Noodknopbediening Sijtwendetunnel 33
3.4.4 Bestelbare items en levertijd 33
3.4.5 Dark Fiber Advies 33
3.4.6 Dark Fiber RWS levering 33
4 Netwerkdiensten CIV Klant 37
4.1 Inleiding 37
4.2 Categorie VPN 37
4.2.1 Functionele omschrijving 37
4.2.2 Bestelbare items en levertijd 38

4.3 Categorie VPN aansluiting 39
4.3.1 Functionele omschrijving 39
4.3.2 Dienstenmatrix VPN Aansluiting 39
4.3.3 Type VPN aansluiting 40
4.3.4 Bestelbare items en levertijd 50
4.4 Categorie LAN aansluiting 50
4.4.1 Functionele omschrijving 51
4.4.2 Dienstenmatrix LAN aansluiting 51
4.4.3 Type LAN aansluiting 52
4.4.4 Bestelbare items levertijd 59
4.5 Categorie Eindsystemen 60
4.5.1 Dienstenmatrix eindsystemen 60
4.5.2 Type eindsysteemtoepassingen 60
4.5.3 Bestelbare items en levertijd 67
4.5.4 Verrekening 67
4.6 Categorie Overig 68
4.6.1 Gepland werk Glas 68
4.6.2 Glasadvies 69
4.6.3 Netwerkadviezen 69
4.6.4 Uurtarieven / Strippenkaart 69
4.6.5 Rijkskantoorroam 70
4.6.6 Bestelbare items en levertijd 70
4.6.7 Verrekening 71
Bijlagen 71
Bijlage A Contactgegevens 72
Bijlage B Afkortingen en Begrippen 73
Afkortingen 73
Begrippen 74
Bijlage C Service Portfolio Management Proces 76
Bijlage D Technische specificatie 78
Bijlage E SLA Matrix storingshersteltijden verstoord / onderbroken 83

2 Inleiding

2.1 Doel

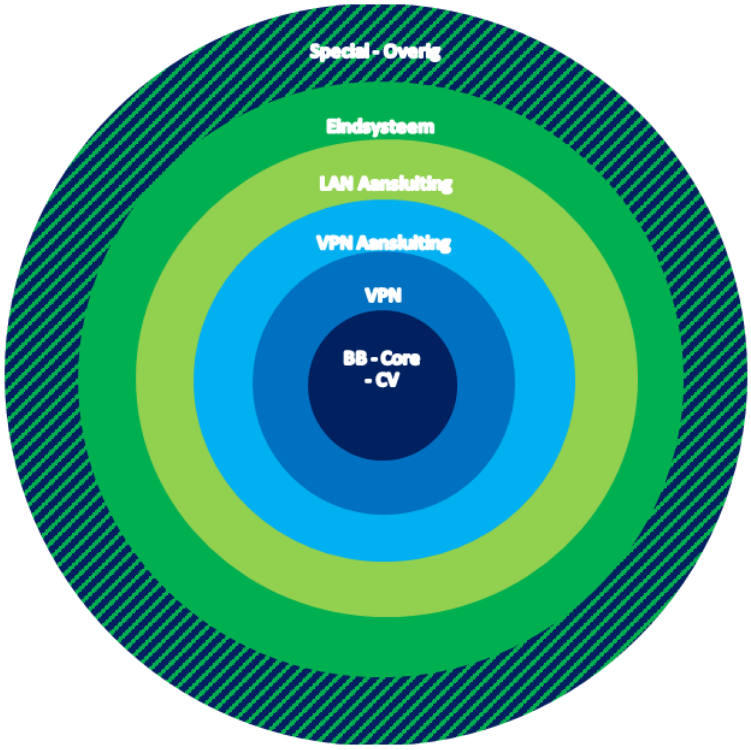
Doel van deze catalogus is het bieden van een overzicht van alle diensten die RWS CIV IRN Infra Netwerken op netwerkgebied afneemt van KPN DO RWS en welke RWS CIV IRN Infra Netwerken biedt aan haar afnemers.

2.2 Opbouw

Deze catalogus bestaat uit de volgende onderdelen:

- Algemeen
    - Toelichting op de scope van de dienstverlening;
    - Ondersteuning via de Service Desk van KPN DO RWS;
    - Leveringsvoorwaarden en bestelprocedure;
    - Het proces voor aanpassing van bestaande diensten en de ontwikkeling van nieuwe diensten;
    - Rapportages
- Catalogus deel 1: Netwerkdiensten RWS CIV IRN Infra Netwerken
    - Een beschrijving van de uitsluitend door/via RWS CIV IRN Infra Netwerken te bestellen diensten in de categorie Backbone, VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Special/Overig.
- Catalogus deel 2: Netwerkdiensten Klant
    - Een beschrijving van de door afnemers te bestellen diensten in de categorie VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Overig.

In **Figuur 1** is de categorisatie van de dienstverlening weergegeven. Deze is te herleiden naar het Prijzenblad.



Figuur 1: Opbouw dienstverlening in categorieën

2.3 Dienstverlening RWS CIV IRN Infra Netwerken

2.3.1 *Algemeen*

Rijkswaterstaat Centrale Informatievoorziening (CIV) zorgt voor de ontwikkeling en beschikbaarheid van informatie binnen Rijkswaterstaat. CIV zorgt voor industriële automatisering bij bruggen, tunnels, rijkswegen en andere objecten. Daarnaast verzorgt CIV de kantoorautomatisering.
RWS CIV IRN Infra Netwerken draagt binnen RWS CIV zorg voor de netwerkinfrastructuur en bijbehorende dienstverlening.

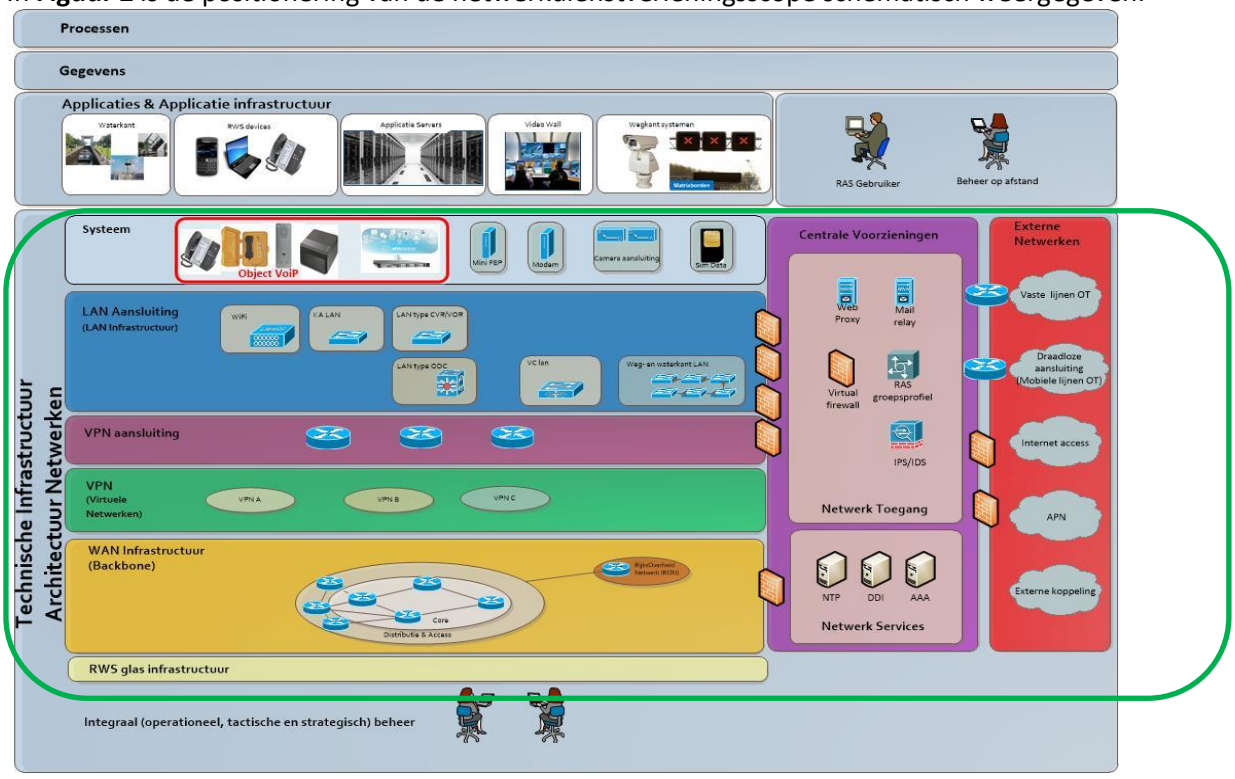
2.3.2 *Scope*

RWS CIV IRN Infra Netwerken is verantwoordelijk voor het beheer, project- en contractmanagement van haar netwerkomgeving. De uitvoering hiervan is belegd bij de outsourcingspartner KPN DO RWS.

De netwerkdienstverlening beslaat de volgende domeinen:

- RWS netwerk;
- KA LAN;
- Object Access Netwerken:
  Netwerken die worden gebruikt om objecten, binnen Rijkswaterstaat ook wel kunstwerken genoemd, maar ook systemen langs weg- en waterwegen, te ontsluiten;
- De WAN verbindingen naar Locaties (kantoren en rekencentra), wegkantsystemen, verkeerscentrales, objecten zoals bruggen, sluizen en tunnels en losse huurlijnen.
- Koppelingen met externe netwerken (internet, mobiel, de Haagse Ring, RON2.0 e.a.);
- Functieherstel glasvezelnetwerk:
  Herstellen van verstoringen op RWS glasvezels;
- Glasvezelbeheer (o.a. vezelbezetting en uitgifte van vezels).

In **Figuur 2** is de positionering van de netwerkdienstverleningsscope schematisch weergegeven.



Figuur 2: Positionering Netwerkdienstverleningsscope

2.3.3 *Service Desk KPN DO RWS*

KPN DO RWS biedt een centrale ingang voor zowel RWS medewerkers als door RWS geautoriseerde contactpersonen in de vorm van de Service Desk. Deze schakelt met de MKO en KA Service Desk van RWS die het eerste aanspreekpunt zijn voor eindgebruikers van RWS dienstverlening.

Enerzijds verwerkt de KPN DO RWS Service Desk, als centrale spil, alle vragen, orders en storingsmeldingen van de afnemers van de Rijkswaterstaat organisatie. Hierbij worden via een gecontroleerd proces de diverse toeleveranciers en derde partijen aangestuurd. Anderzijds verricht de Service Desk alle noodzakelijke registraties ten behoeve van terugkoppeling, rapportage, bijsturing en facturering.

De Service Desk vormt een integraal onderdeel van de KPN DO RWS beheerdienstverlening en omvat de volgende functies:

- Helpdesk: Ondersteunen van de medewerkers/afnemers van Rijkswaterstaat bij vragen over afgenomen diensten;
- Orderdesk: Ingang waar geautoriseerde personen opdrachten en eenmalige diensten (Install, Move, Add en Change (IMAC's)) indienen;
- Melddesk: Voor het melden van storingen, incidenten en klachten.

De Service Desk beantwoordt de vragen van Rijkswaterstaat. Indien KPN de vragen niet kan beantwoorden wordt contact gezocht met de achterliggende supportgroepen of derde contractpartijen om tot een antwoord te komen. Hierover zijn afspraken gemaakt met de achterliggende partijen.

De Service Desk is 24x7 zowel telefonisch als per e-mail bereikbaar:

- Incidenten kunnen 24x7 telefonisch gemeld worden en worden conform geldende SLA afspraak afgerond;
- De afhandeling van orders zal plaatsvinden tijdens kantooruren;
- Informatievragen kunnen 24x7 per e-mail gesteld worden. Tijdens kantooruren kunnen deze vragen ook telefonisch gesteld worden. De afhandeling van informatievragen vindt plaats tijdens kantooruren.

2.4 Leveringsvoorwaarden

- Aansluitvoorwaarden NNV Rijkswaterstaat zijn van toepassing. Deze zijn beschikbaar op de RWS VPR: http://vpr.intranet.rws.nl/Algemeen/vicnet/NNV%20VICnet/Forms/AllItems.aspx
- Het voor de diensten genoemde beschikbaarheidsniveau is gebaseerd op technische beschikbaarheid en afhankelijk van de ketenpartijen;
- Het RWS Enterprise Security Model is van toepassing. Dit is beschikbaar op de RWS VPR: Security Architectuur Rijkswaterstaat

2.5 Bestellingen (standaard leveringen, tactische leveringen en ontwikkelingen) en verrekening

Deze catalogus beschrijft de standaard bestelbare diensten van CIV IRN Infra Netwerken. Afnemers kunnen zonder tussenkomst van CIV IRN Infra Netwerken een standaard levering aanvragen. Een aantal standaard bestelbare items zijn geclassificeerd als "tactische leveringen", hiervoor dient CIV IRN Infra Netwerken akkoord te geven. Levervragen die (nog) niet met de standaard Product en Diensten Catalogus kunnen worden ingevuld worden On hold geplaatst tot een ontwikkeling van een standaard bestelbaar item door CIV IRN Infra Netwerken is afgerond. Indien levering vooruitlopend op ontwikkeling noodzakelijk is, kan met de PDC Uitzonderingen Procedure toestemming gevraagd worden om op basis van een PDC Exceptie de levering op te starten parallel aan een ontwikkeltraject.

Standaard leveringen
De standaard leverbare items uit deze catalogus zijn bestelbaar via de RWS TOPdesk SelfServicePortal via Startpagina > PDC IRN INFRA > Netwerk. Hierbij wordt onderscheid gemaakt tussen een tweetal type leveringen:

1. **Mutaties:** Geautomatiseerd leveren van één of meerdere bestelbare items uit de PDC zonder coördinatie;
2. **Meervoudige PDC project leveringen:** Leveren van één of meerdere bestelbare items uit de PDC onder besturing van een PDC Coördinator o.b.v. een prijsopgaaf.

In geval van twijfel over de te bestellen standaard items kan middels de “Hulp bij mijn PDC bestelling”-tegel in TOPdesk een verzoek tot ondersteuning bij het samenstellen van de juiste bestelling worden ingediend.

Tactische leveringen
Er zijn ook een aantal tactische aanvragen gedefinieerd. Voor de levering hiervan dient contact opgenomen te worden met de Relatie Manager van RWS CIV IRN Infra Netwerken Relatie Manager die bepaald of de aanvraag al dan niet in behandeling wordt genomen.

Ontwikkelingen: het SPM Proces
Indien blijkt dat een levervraag (nog) niet kan worden ingevuld middels een standaard bestelbare dienst, dan dient de functionele behoefte te worden gemeld bij de RWS Relatie Manager. of zijn Service Management collega’s **(**voor contactgegevens zie **Bijlage A)** om middels ontwikkeling te zorgen dat de levervraag kan worden gerealiseerd en als bestelbare dienst in de PDC wordt opgenomen

De Relatie of Service Manager zal een eerste beoordeling doen of ontwikkeling nodig is, en daarmee het SPM Proces gestart (**Bijlage C**) dient te worden. In geval van ontwikkeling zal de Relatie of Service Manager aan de aanvrager/behoeftesteller de actuele versie van het SPM Requirementsdocument beschikbaar stellen, welke de aanvrager/behoeftesteller dient in te vullen. Dit wordt vervolgens in een intake met de RWS Service Portfolio Manager besproken. Bij akkoord van de Service Portfolio Manager voor dienstontwikkeling dient de Service Portfolio Manager een SPM Advies-aanvraag in bij KPN. KPN zal vervolgens op basis van het ingevulde Requirementsdocument een Advies opstellen met de beoogde oplossingsrichting en uitgangspunten / aannames, inclusief een kosteninschatting van de op te leveren deliverables.

Voor dit advies, dat vier gradaties kent, geldt een standaard PDC prijs die ook in rekening wordt gebracht wanneer de aanvrager besluit het advies niet te laten uitvoeren.

Er wordt onderscheid gemaakt tussen vier type adviezen, zoals toegelicht in **Figuur 3**.

Netwerkadvies	
Type	Kenmerken
Eenvoudig	Geen dienst(bouwsteen)ontwikkeling, vooronderzoek om te bepalen of de functionele behoefte kan worden ingevuld met PDC leveringen en/of de inzet van KPN DO RWS medewerk(st)ers.
Normaal	Dienst(bouwsteen)ontwikkeling; Ontwikkelen van een nieuwe bouwsteen, het aanpassen/uitbreiden van bestaande bouwstenen met een nieuwe optie of het combineren van bestaande bouwstenen om te komen tot een nieuwe functionaliteit.
Complex	Dienst(bouwsteen)ontwikkeling als hierboven, inclusief afstemming met meerdere partijen
Maatwerk	Offerte op basis van maatwerk activiteiten en uren, geen vaste prijs

Figuur 3: Type Netwerkadvies

Indien RWS het Advies wil laten opvolgen zal de RWS Programma- & Projectmanager een RFP-aanvraag indienen om de in het Advies beschreven oplossingsrichting verder te specificeren in een offerte, PID en PSA, waarna opdracht gegeven kan worden voor realisatie.

Wanneer dit traject is afgerond wordt de levervraag alsnog middels standaard levering ingevuld.

Verrekening
De eenmalige kosten en abonnementstarieven van de bestelbare items zijn terug te vinden in het Prijzenblad. De actuele versie hiervan is beschikbaar in de RWS Topdesk SelfServicePortal via Startpagina > PDC IRN INFRA > Netwerk

2.6 Partner PDC Rapportages

RWS IRN Infra Netwerken levert een aantal end-to-end diensten aan Partners. Deze partner diensten vormen geen onderdeel van deze catalogus, maar om deze te leveren wordt wel gebruik gemaakt van een aantal netwerkdiensten. Het betreft de dienstbouwstenen VPN, VPN aansluiting (Interconnect en Connect) en Dark Fiber. Over de performance van de geleverde RWS IRN Infra Netwerken Partner dienstverlening wordt maandelijks per geregistreerde partner gerapporteerd op de volgende onderdelen:

- Capaciteit (indien van toepassing en met uitzondering van Dark Fiber);
- Beschikbaarheid.

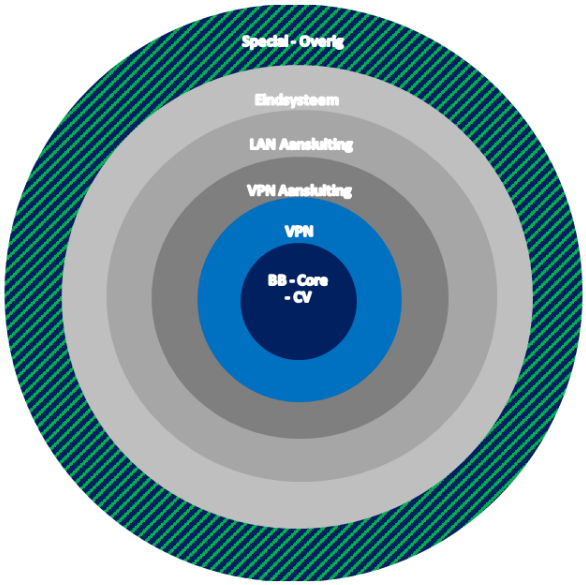
De rapportage wordt geplaatst op de KPN - RWS Collaboration portal en is benaderbaar via de onderstaande link:
RWS - Partner rapportages - All Documents (sharepoint.com)

2.7 Definities en afkortingen

Een overzicht van afkortingen en begrippen is opgenomen in **Bijlage B**.

Catalogus deel 1:

Diensten RWS CIV IRN Infra Netwerken



Figuur 4: Categorieën diensten RWS CIV IRN Infra Netwerken

Backbone - Core – CV
DNS (CV deel)
IDS IPS
NAC (Backbone)
FCoDWDM
Mail relay
(Forward) Webproxy
Centrale WIFI omgeving
CVR Toegang en omgevingsmonitoring
Glasvezelbeheer
VPN
VPN
Virtual Firewall
DDI
DMZ
Forward Webproxy
Mail relay
Special (Niet bestelbaar)
Beheer verbindingen LEG-EPL
CCM aansluiting
Overig
Dark fiber

3 Diensten RWS CIV IRN Infra Netwerken

3.1 Inleiding

De Netwerkdiensten RWS CIV IRN Infra Netwerken zijn uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken. Bij vragen over deze diensten kan contact opgenomen worden met Service Management of de Relatie Manager (contactgegevens in **Bijlage A)**. De netwerkdiensten ten behoeve van afnemers zijn beschreven in deel 2 van deze catalogus: “Netwerkdiensten CIV Klant”.

3.2 Categorie Backbone (BB), Core, Centrale Voorzieningen (CV)

De categorie **BB Core CV** omvat de centrale netwerkdiensten welke betrekking hebben op de backbone van het RWS netwerk, zoals voorzieningen om de veiligheid van het netwerk te garanderen. De backbone van het RWS CIV IRN Infra netwerk is de centrale netwerkinfrastructuur waarlangs het gegevensverkeer van de op de backbone aangesloten netwerken loopt.

De categorie Centrale Voorzieningen betreft de diensten en centrale componenten welke benodigd zijn om klantdiensten te kunnen leveren zoals DNS, IPS IDS, DWDM, Mailrelay, Forward Webproxy, LAN aansluiting draadloos WIFI CV, Vast beheertarief LAN omgeving bedraad, CVR Toegang, omgevingsmonitoring en Glasvezelbeheer.

3.2.1 *Dienstenmatrix BB Core CV*

Onderstaande matrix (**Figuur 5**) geeft een overzicht van de verschillende **BB Core CV** diensten en bijbehorende opties. In de volgende paragrafen worden deze nader toegelicht.
De per dienst afgegeven beschikbaarheid is empirisch bepaald. Dit betekent dat het technisch design zodanig is dat de afgegeven SLA gegarandeerd kan worden.
De weergegeven storingshersteltijd is gebaseerd op incidenten waarbij de dienstverlening onderbroken is (er is business impact). Wanneer er sprake is van verstoorde dienstverlening (geen business impact) geldt het SLA zoals weergegeven in **Bijlage E**.

Dienstenmatrix CV BB								
	Beschikbaarheid				Storingshersteltijd in 95% van de gevallen			
	99,5%	99,9%	99,95%	99,999%	Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
	Onbeschikbaarheid per jaar							
Diensten	ca. 1d20u	ca. 8u45m	ca. 4u28m	ca. 5m15s	K8	K4	E8	E4
DNS			√					√
IDS	√							√
IPS		√						√
NAC								
DWDM				√				√
Mailrelay			√					√
Forward webproxy			√					√
LAN omgeving draadloos Wifi CV	n.v.t.							
Vast beheertarief LAN omgeving bedraad								
Glasvezelbeheer								

Figuur 5: CV BB

3.2.1.1 *Domain Name Services (DNS) CV*

De centrale dienst DNS CV voorziet in het abonnement voor levering van “name services” aan alle eindsystemen die zijn aangesloten op het RWS netwerk op basis van het DNS protocol. Hierbij wordt onderscheid gemaakt tussen een centraal DNS CV abonnement en een aanvullend abonnement per appliance (toepassing).
De dienst voorziet in zowel hosting als resolving van domeinnamen. Daarnaast verzorgt DNS CV samen met Domain Host Configuration Protocol (DHCP) CV een gecentraliseerde IP Address Management (IPAM) functie om het beheer van DNS zones en DHCP scopes en opties efficiënt en effectief uit te kunnen voeren.

De dienst maakt gebruik van High Available DNS, een centraal management systeem en gecentraliseerde logging en levert de volgende functies:

- Centrale DNS dienst ten behoeve van interne- en externe resolving en hosting van DNS domeinen;
- Centraal beheren van gedecentraliseerde DNS resolvers in de RWS verkeerscentrales (POP locaties);
- DNS Forwarding, bedoeld om DNS query's te forwarden voor externe DNS namen op externe DNS servers, buiten het RWS domein;
- Zoveel mogelijk generieke DNS configuratie, waarbij het mogelijk is per zone te kiezen voor voorkeuren maar centraal beheer mogelijk is; Inherent High Available (één virtual DNS IP nummer per cluster);
- Mogelijkheid tot opzetten van een terminal connectie met een seriële poort en een console verbinding;
- Geschikt voor IPv6, geïmplementeerd op basis van Iv4;
- Logging van beheerhandelingen, DNS requests en failures wordt verstuurd naar centrale syslog servers.

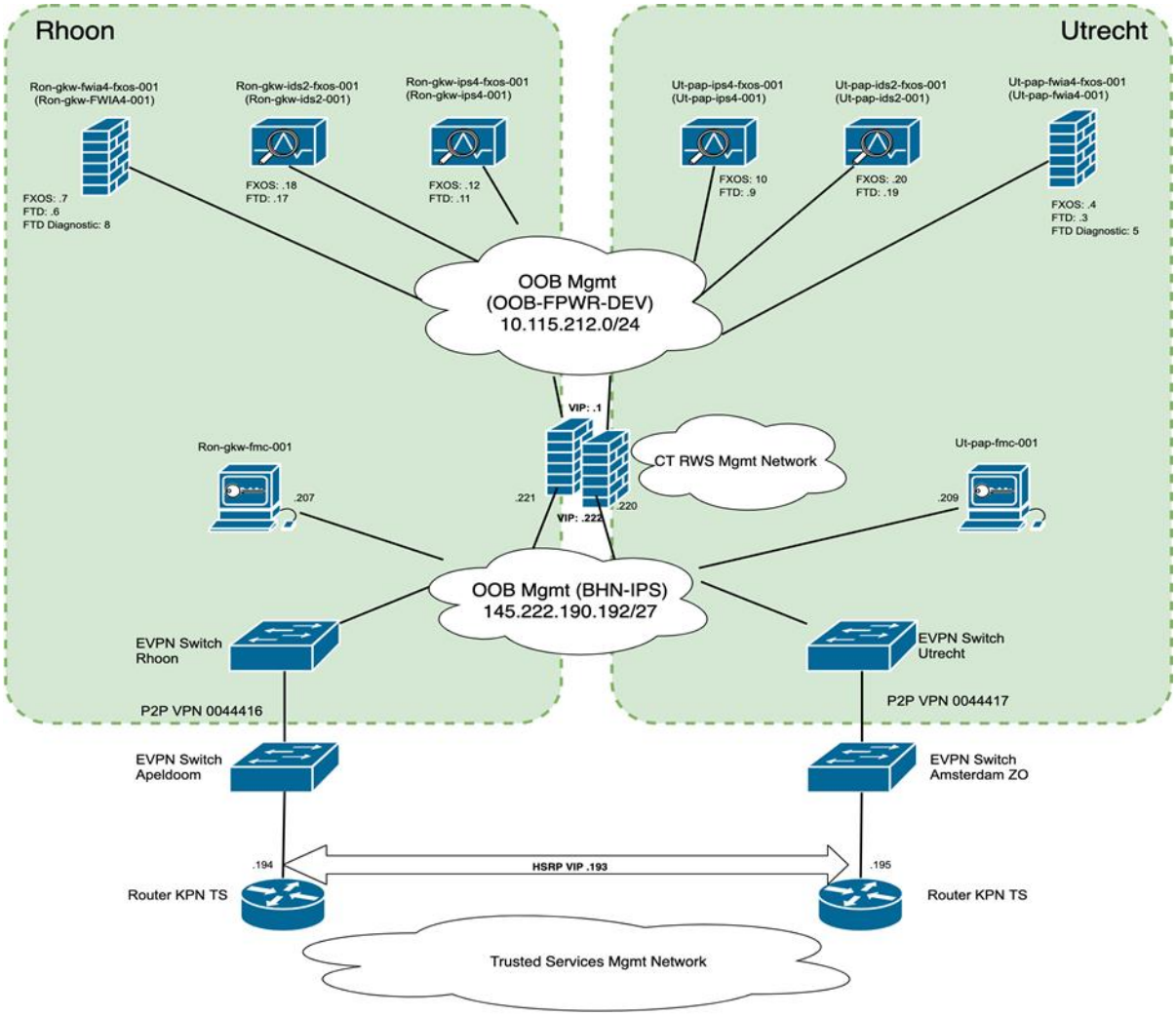
Naast de centrale DNS dienstverlening is het middels de DDI (DNS DHCP IPAM) dienst mogelijk per VPN verschillende DNS en DHCP opties in te stellen en gedelegeerd beheer toe te passen in DNS zones en DHCP scopes. De dienst DDI is beschreven in de Categorie VPN.

3.2.1.2 *IDS/IPS*

IDS/IPS zoals weergegeven in **"Figuur 6: Overzicht IDS-IPS"** biedt een centraal beheerd en bestuurd Intrusion Detection System (IDS) voor verkeer tussen VPN's en voor verkeer van en naar de centrale voorzieningen, en Intrusion Prevention System(IPS) voor al het verkeer van en naar het internet. Doel van deze dienst is om gericht applicatie-, systeem- en netwerkbedreigingen te detecteren en risico's hierop te mitigeren.

IDS/IPS monitort het RWS netwerk en de centrale netwerkdiensten om ongewone/verdachte verkeersstromen, patronen en gebeurtenissen te detecteren en rapporteert deze via een dashboard. Daarnaast evalueert en rapporteert IDS/IPS verdachte verkeersstromen naar of vanuit eindstations bekend als 'malware', 'virale software', 'trojans', 'spyware', portscans en andere afwijkende datapatronen.
IPS blokkeert verdacht verkeer en acteert daarmee als application layered firewall voor al het verkeer van en naar het internet. IPS wordt ook ingezet om intern verkeer vanuit het RWS netwerk richting andere netwerken te filteren en fungeert als centraal punt in het netwerk waar ongewenste verkeersstromen kunnen worden geblokkeerd.
IDS/IPS wordt toegepast om te inspecteren en rapporteren op inter- VPN verkeer van alle RWS VPN's, in- en outbound verkeer met Externe koppeling, DMZ en de centrale voorzieningen en verkeer van en naar beheerinterfaces van beheerde apparatuur. Daarnaast wordt IDS/IPS toegepast om te inspecteren en te acteren op in- en outbound internet verkeer voor het RWS netwerk.
Daarnaast biedt IDS/IPS voor haar beheerders een platform om op gebruikersvriendelijke wijze het systeem te configureren, te laden met 'policies' en 'rules' als ook om gebeurtenissen te categoriseren, te rapporteren en in te richten door middel van 'dashboards' voor het verkrijgen van overzicht en inzicht.

IDS/IPS moet altijd bekend zijn met de te monitoren netwerken (set van IP adressen). Om onterechte meldingen (false positives) te beperken worden nieuwe door KPN DO RWS uitgegeven netwerken automatisch toegevoegd aan de dienst bij aanvraag of wijziging van een VPN. Hiertoe beschikt het IDS-IPS over een profileringsfunctionaliteit waarin de verschillende netwerken opgenomen worden. Netwerken worden toegewezen middels een standaard policy maar het is ook mogelijk een specifieke policy in te richten voor specifieke netwerken.



Figuur 6: Overzicht IDS-IPS

De logging van de IDS sensoren en IPS worden verstuurd naar het centrale management systeem: De Firepower Management Center (FMC). Op basis van de ontvangen informatie kunnen uit het Defence Center verschillende rapportages worden opgevraagd.
Toegang tot het FMC wordt geleverd via het netwerkcomponent BAS (Beheer Access Server). Dit component verzorgt een veilige VPN connectie tot de beheeromgeving van KPN DO RWS en is toegankelijk vanuit het RWS KA netwerk via https://bas.intranet.rws.nl/ in combinatie met een ACS functioneel account met de juiste rechten.

Het component BAS heeft de volgende eigenschappen:

- Sterke gebruikers authenticatie met een hardware token (RSA) + gebruikersnaam/wachtwoord uit de RWS Active Directory (AD) of gebruik te maken van de SMS authenticatie;
- Autorisatie via de DO RWS ACS;
- Zonder aangevraagde permissies heeft een medewerker geen toegang tot het rapportagedashboard van IPS/IDS;
- Afwijkende beschikbaarheid van 97%.

3.2.1.2.1 Policies

IDS/IPS is ingericht met de volgende policies:

- POLICY “EXTERN” (Doel: Beschermen tegen externe dreigingen)

Generieke aanpak voor beveiliging tegen aanvallen vanuit het Internet aan de externe zijde van het netwerk.

- POLICY “INTERN” (Doel: beschermen van interne assets)

Bedoeld om specifieke onderdelen van het netwerk te beschermen. Per type omgeving wordt de mate van analyse en blokkering van verkeersstromen bepaald. In de dienst IDS-IPS is hiertoe in de policies de beschikking over informatie per segment. Dit is ingericht op het niveau van het VPN.

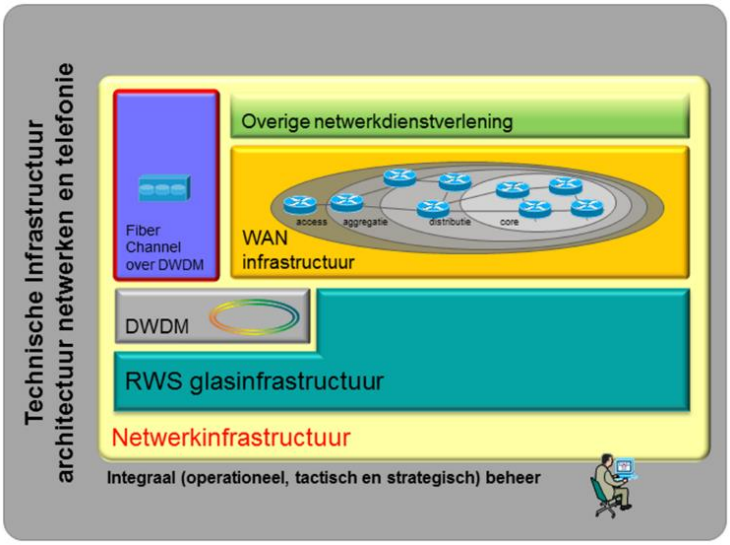
3.2.1.2.2 Interfaces

De dienst kent een aantal interfaces:

- Detectie
  De detectie interfaces van het IDS (sensors) zijn aangesloten op de punten in het netwerk waar de te detecteren verkeerstromen voorbijkomen. Deze IDS detectie interfaces zijn voor devices op die netwerksegmenten niet zichtbaar.
- Preventie
  - De preventie interfaces van de IPS zijn (inline) aangesloten op de internet firewall en het RWS netwerk zodat al het verkeer van en naar het internet automatisch langs de IPS geleid wordt. De IPS detecteert en kan indien het een niet geoorloofde verkeersstroom is automatisch ingrijpen en deze verkeersstroom blokkeren.
- Beheer
  - Voor de IDS/IPS dienstverlening is een, middels een firewall afgeschermd, apart beheernetwerk dat logisch gescheiden is van het productienetwerk. Het beheernetwerk is alleen benaderbaar via de opstap omgeving van KPN DO RWS.
  - Monitoring (SNMP), resolving (DNS) en tijdsynchronisatie (NTP) vindt eveneens plaats via het beheersegment.

3.2.1.3 *FCoDWDM*

De dienst Fibre Channel over Dense Wavelength Division Multiplexing (FCoDWDM) wordt geleverd over glasvezelverbindingen in de RWS infrastructuur. DWDM bestaat uit een point-to-point verbinding tussen bestaande datacenters en onder bepaalde voorwaarden naar nieuwe locaties.
Doormiddel van Fibre Channel over DWDM kan het glas efficiënter gebruikt worden. Het Fibre Channel protocol wordt gebruikt om verschillende locaties te verbinden ten behoeve van data storage synchronisatie.



Figuur 7: DWDM in het netwerk

De dienst DWDM wordt gerealiseerd door twee onafhankelijke verbindingen (unprotected pair) die over gescheiden optische paden en verschillende DWDM-nodes geleverd worden en die beschermd worden door de aangesloten apparatuur. Hiermee kan een hoge beschikbaarheid worden gerealiseerd.

De point-to-point verbinding tussen twee locaties moet voldoen aan de volgende voorwaarden:

- Standaard uitsluitend leverbaar tussen de locaties Datacenter AM2 en Datacenter AM3 (AM1.3 en AM4 zitten respectievelijk achter AM2 en AM4).
- Uitbreiding naar andere locaties mogelijk indien wordt voldaan aan de volgende voorwaarden:
    - Glas beschikbaar over 2 gescheiden routes;
    - Mogelijkheid tot plaatsen DWDM-apparatuur rekening houdend met de latency beperkingen (= afstand) van het Fibre Channelprotocol.
    - Meerdere verbindingen tussen 2 locaties is mogelijk, mits er voldoende ruimte is op de glasvezels.
    - Fibre Channel kan niet omgaan met een verandering van latency door het automatisch omschakelen naar een ander glastraject. Er worden geen *beveiligde* verbindingen aangeboden.
    - Om toch een hoge beschikbaarheid te kunnen bieden, worden Fibre Channel verbindingen altijd per paar geleverd. Een “paar” bestaat uit 2 onafhankelijke verbindingen, die over verschillende glastrajecten worden gerealiseerd.
    - De omschakeling van het primaire pad naar het secundaire pad wordt door de aangesloten Fibre Channel apparatuur (zoals bijvoorbeeld SAN-switches) geregeld.

Over DWDM kunnen de volgende koppelvlakken technisch gerealiseerd worden:

- 8Gbps Fibre Channel
- De koppeling wordt standaard gemaakt met Multi-mode fiber (850nm) via een LC Connector

3.2.1.4 *Mail relay*

De dienst Mail Relay dient als in- en uitgang voor al het e-mailverkeer van en naar het internet. Mail relay wordt ingezet als koppelvlak voor e-mailuitwisseling binnen RWS, met het internet en met organisaties aangesloten op het Rijksweb. Het koppelvlak scant inkomende en uitgaande e-mail op schadelijke of anderszins ongewenste inhoud middels verschillende beveiligingsvoorzieningen:

- Reputatie filtering: Het blokkeren van connecties van nodes op internet die bekend staan om ongewenst gedrag, zoals bekende bronnen van spam en malware;
- Relay bescherming: alleen relayen van uitgaande e-mail vanaf (RWS) hosts die geautoriseerd zijn om email via de relay te mogen uitsturen;
- Afzender controle: wanneer een afzendend domein een SPF DNS record heeft, zal de Mail Relay de daarin opgenomen policy honoreren;
- Bericht integriteitscontrole: via berichtondertekening uit naam van het domein (DKIM) beveiligde berichten worden gecontroleerd op authenticiteit en integriteit;
- Versleuteling van e-mailtransport;
- Adres controle: alleen e-mail voor bestaande RWS domeinen wordt verwerkt. Externe afzenders weren als zij vaak foutieve RWS emailadressen hanteren (bescherming RWS mailomgeving);
- Limiteren van berichtgrootte: maximaal 25MB. Aangesloten e-mailomgevingen kunnen minder groot staan ingesteld;
- Attachment controle: door RWS vastgestelde ongewenste bijlagen kunnen worden geblokkeerd;
- Malware controle: het blokkeren van e-mails met schadelijke inhoud;
- Spam controle:
    - Het in quarantaine plaatsen van mogelijke spamberichten;
    - het blokkeren van spamberichten.

Het onterecht blokkeren van een legitiem bericht (als spam) en het onterecht doorlaten van een spam bericht (als legitiem bericht) dient zo min mogelijk plaats te vinden. Hiervoor is het false positive rate gesteld op 1:1.000.000, wat betekent dat hooguit 1 op de miljoen op spam gecontroleerde berichten onterecht als

spam gekenmerkt mag worden en het false negative rate gesteld op 1:1.000, wat betekent dat hooguit 1 op de duizend op spam gecontroleerde berichten onterecht als legitiem bericht gekenmerkt mag worden.

Verder kent de Mail Relay de volgende functies:

- Quarantaine: berichten die mogelijk spam zijn worden in quarantaine geplaatst. De eindgebruiker kan een bericht desgewenst laten doorsturen naar de eigen mailbox;
- Interne notificaties: in een aantal situaties kunnen medewerkers van RWS een notificatie e-mail ontvangen:
  - Wanneer een schadelijk item is onderschept van of naar de betreffende medewerker;
  - Wanneer een bericht van of naar de betreffende medewerker niet gescand kon worden (bv wachtwoord beveiligde bijlage);
  - Wanneer er nieuwe spamberichten in de quarantaine zijn geplaatst voor de betreffende medewerker.
- Externe notificaties: als een externe zender een e-mail stuurt naar een niet bestaande RWS medewerker (foutief adres), krijgt de externe zender hiervan een notificatie;
- Disclaimer: er wordt door de Mail Relay geen disclaimer toegevoegd aan een e-mail.

De Mail Relay kent drie interfaces: SMTP voor e-mail transport; HTTP voor spam quarantaine en DNS voor afzender controle.

3.2.1.5 *Forward webproxy*

De Forward webproxy dient als uitgang voor al het websurfverkeer door gebruikers naar het internet en externe netwerken (niet naar interne webapplicaties). Dit koppelvlak verzorgt ook het scannen op schadelijke of anderszins ongewenste inhoud. Deze dienst wordt afgenomen wanneer voor een VPN gekozen wordt voor de functie ‘Internet Access’ met als doel om veilig te surfen op het internet.

3.2.1.6 *Centrale WIFI omgeving*

Dit component omvat de basis infrastructuur welke benodigd is om de Access points voor de WIFI dienstverlening te kunnen ontsluiten en bestaat uit het beheer van de centrale Wireless LAN controller (WLC) en de bijbehorende LAN Aansluitingen. Doormiddel van deze LAN Aansluitingen zijn de separate CE routers in Rhoon en Utrecht voorzien van LAN poorten ten behoeve van de Wireless LAN Controllers. Op de CE routers worden VPN Aansluitingen geleverd voor connectiviteit van de Access Points naar de Wireless LAN Controllers en voor ontsluiting van draadloze gebruikers.

3.2.1.7 *CVR toegang en omgevingsmonitoring*

RWS CIV IRN Infra Netwerken maakt voor de CVR-en gebruik van een aantal applicaties ten behoeve van toegangsbeveiliging en omgevingsmonitoring. Middels deze netwerkdienst CVR toegang en omgevingsmonitoring wordt tweedelijns support bij incidentafhandeling van het CVR Toegang en Omgevingsmonitoringsysteem geborgd.

3.2.1.7.1 Scope van de dienstverlening

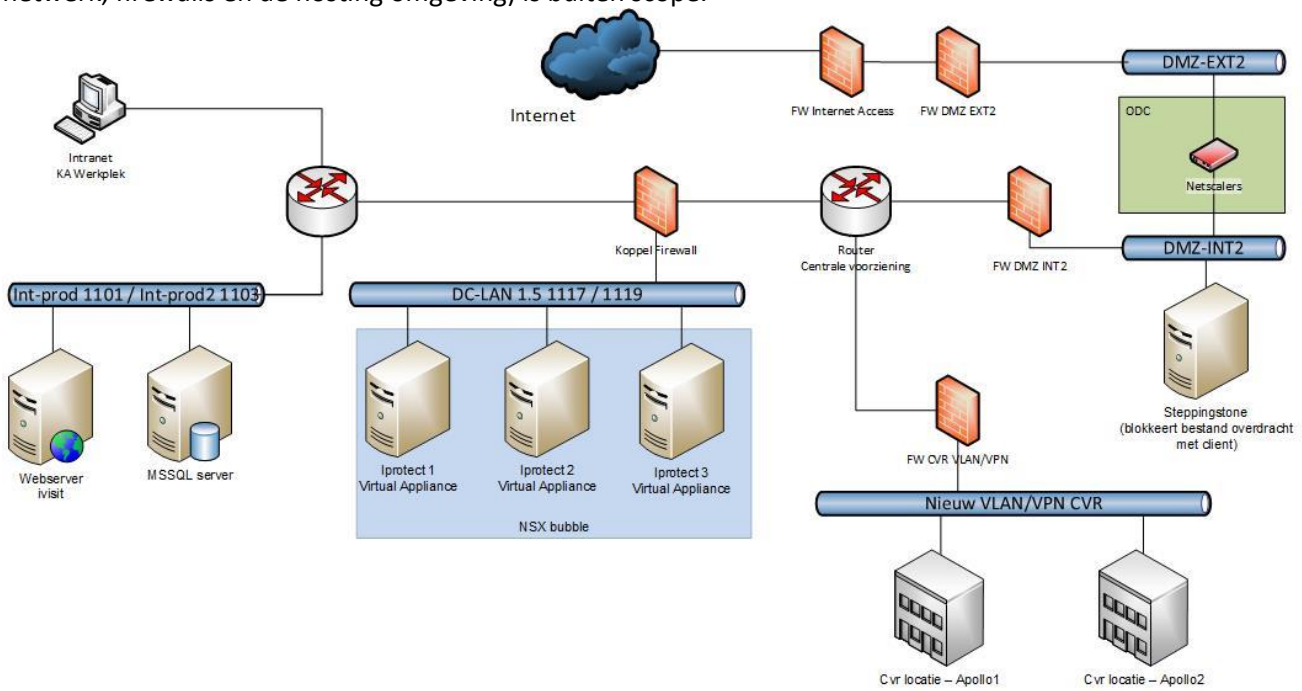
De eerstelijns ondersteuning en dagelijkse monitoring voor deze dienst worden verzorgd door RWS MKO. MKO kan verstoringen via KPN DO RWS aanmelden bij de Servicedesk van SPIE. Na het aanmaken van een melding kan RWS MKO optioneel tijdens kantoortijden telefonisch contact opnemen met SPIE om de melding te bevestigen of te bespreken. De eerste incidentanalyse en kwalificatie van een melding worden door RWS MKO uitgevoerd om KPN/SPIE te voorzien van de juiste informatie, waarna de engineer zich naar de locatie begeeft voor on-site herstel of eventueel remote in kan loggen voor de centrale systemen.

Tweedelijns support bij incidentafhandeling is op basis van een SLA binnen kantoortijden. Hierbij geldt een Next Business Day responsetijd en een hersteltijd van vijf werkdagen vanaf het moment van aanmelding van een incident door RWS CIV IRN Infra Netwerken.

De dienst omvat ondersteuning bij incidenten op zowel de centrale (**Figuur 8**) als decentrale systemen (**Figuur 9**). Een verstoring leidt tot het gedeeltelijk of geheel uitvallen of incorrect werken van de centrale en decentrale systemen. Sensormeldingen vanuit het systeem bij normoverschrijding, zoals brand, water, temperatuur, luchtvochtigheid, automaatstand, toegangsverlening / weigering op locatie en deurstand, zijn buiten scope.
Naast het oplossen van verstoringen kan deze service dienstverlening ook gebruikt worden voor gebruikersvragen. Voor eenvoudig direct op te lossen gebruikersvragen wordt een standaard vast bedrag in rekening gebracht. Voor complexe gebruikersvragen waar het nodige uitzoekwerk voor nodig is dient separaat opdracht gegeven te worden.

3.2.1.7.2 Toelichting omgeving CVR Toegang en omgevingsmonitoring

De CVR toegang en omgevingsmonitoring bestaat uit een centraal en decentraal deel.
Centraal wordt gebruik gemaakt van de “iVisit” applicatie, waarin pasautorisaties worden geregistreerd, en de “iProtect” applicatie die deze pasautorisaties distribueert naar de CVR’s. Daarnaast ontvangt “iProtect” alarmeringen van alle decentrale “Apollo’s”. De alarmeringen worden vertoond op het dashboard van “iProtect” en gelijktijdig per e-mail gemeld aan Rijkswaterstaat MKO. De ODC infrastructuur (o.a. het netwerk, firewalls en de hosting omgeving) is buiten scope.



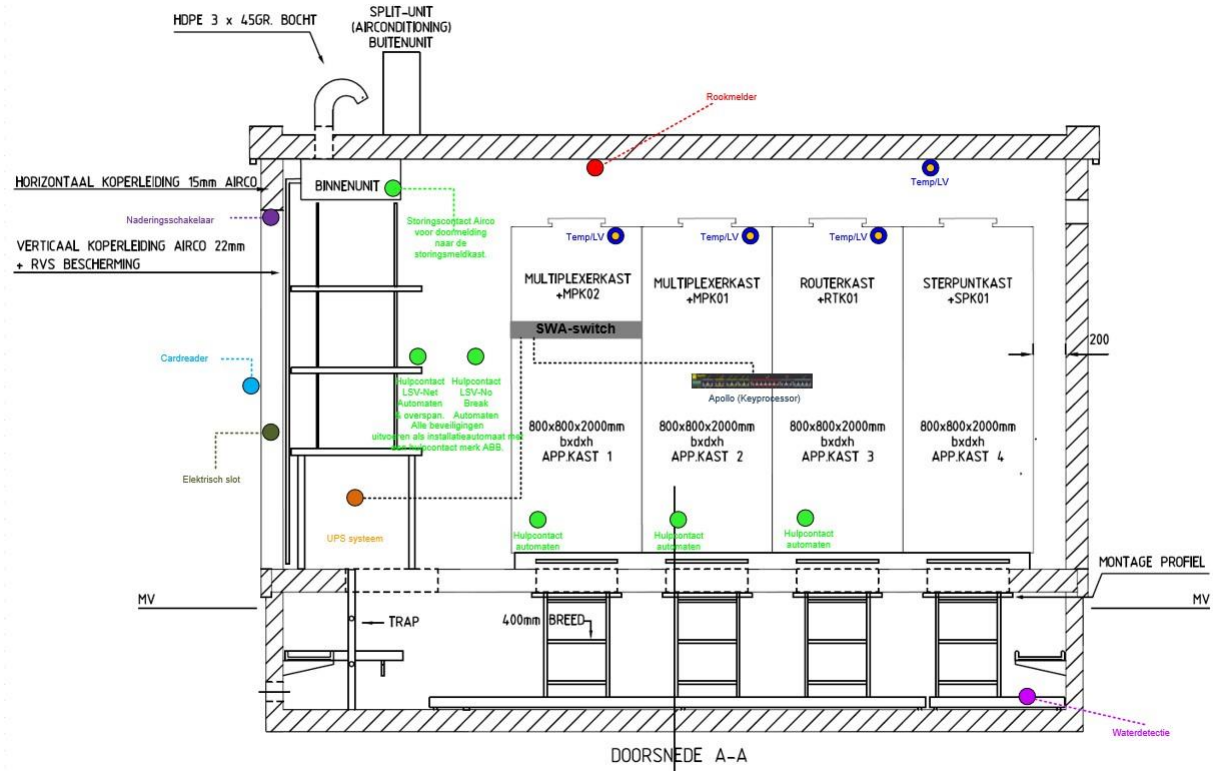
Figuur 9: Centrale omgeving iProtect en iVisit (ODC)

Decentraal wordt in de CVR-ruimte gebruik gemaakt van een “Apollo” welke voorziet in een aantal aansluitingen ten behoeve van Toegang en Omgevingsmonitoring:

- Temperatuur- / luchtvochtigheidssensoren in serie – maximaal 4 stuks (ruimte en apparatuur kasten);
- Kaartlezer buiten ruimte met beschermkap;
- Eén elektrisch slot (motor);
- Rookmelder op plafond;
- Waterdetectie in kelder;
- Naderingsschakelaar toegangsdeur;

- Storingscontact LSV-verdeler NO-BREAK en OSB;
- Storingscontact LSV-verdeler Netvoeding;
- Storingscontact Verdelers apparatuur kasten (MPK en RTK);
- Storingscontact Airconditioning.

De Apollo inclusief bekabeling en componenten (Temperatuur en LV sensoren, kaartlezer, elektrisch motorslot, rookmelder en waterdetector zijn in scope van de dienstverlening. De componenten naderingsschakelaar, verdelers met hulpcontacten, airconditioning, UPS met SNMP management kaart en de cilinder van het deurslot zijn buiten scope. De cilinder van het deurslot blijft de verantwoordelijkheid van de Rijkswaterstaat regio.



Figuur 9: Decentrale omgeving Apollo en aansluitingen (CVR)

3.2.1.7.3 Uitgangspunten

Voor deze dienstverlening gelden de volgende uitgangspunten:

- Er geschiedt geen reparatie van decentrale componenten op locatie. Het betreft “swap” dienstverlening waarbij het defecte component vervangen wordt. Zowel software/hardware resets als swaps maken deel uit van het incidentproces;
- Incidenten op de centrale omgeving worden opgelost om de gebruiker in staat te stellen op acceptabele wijze verder te werken. Het onderliggende probleem wordt via Problem Management structureel opgelost;
- Bij complete uitval van de centrale systemen kan herstel (restore) van de applicaties noodzakelijk zijn. Voor de centrale iVisit applicatie kan door Rijkswaterstaat zelf een snapshot teruggezet worden;
- Bij een complete crash van de iProtect applicatie kan geen garantie worden gegeven dat een snapshot werkend teruggezet kan worden;
- Remote toegang tot het Rijkswaterstaat ODC en de mogelijkheid tot inloggen op de centrale systemen is nodig voor deze dienstverlening. Daarbij moet er een remote omgeving beschikbaar zijn die mogelijkheid

biedt om voldoende technische handelingen uit te voeren voor het onderzoeken en oplossen van storingen aan de decentrale en centrale systemen;

- De dienst is uitgerold voor een installed base van 56 CVR locaties. Andere locaties zijn buiten scope en dienen middels een Non PDC aanvraag te worden toegevoegd aan deze dienstverlening;
- De capaciteits- en beschikbaarheidsplanning is zodanig ingericht dat een aanbod van 5% van de installed base aan storingen binnen SLA kan worden aangenomen en afgehandeld. Dit betekent een gelijktijdige behandeling van het aantal openstaande calls gelijk aan 5% van het aantal CVR locaties, te weten 3 openstaande calls. Zodra een vierde call wordt aangemeld, zal deze als best effort worden opgepakt;
- RWS dient aan te geven wanneer extra werkzaamheden of verkeersmaatregelen noodzakelijk zijn en ook welke werkzaamheden en verkeersmaatregelen het betreft. Hiervoor gelden additionele kosten waarvoor tot maximaal €1.000,- van te voren voor akkoord gevraagd. Voor werkzaamheden waarvan de kosten deze grens overschrijden wordt een separate offerte uitgebracht waarop vooraf akkoord dient te worden gegeven door RWS;
- Indien er geen toegang mogelijk is tot de locatie met de uitgegeven tag, dan bestaat de mogelijkheid om gebruik te maken van de fysieke noodsleutel. Deze is in bezit bij Rijkswaterstaat en hiervoor dient de noodprocedure gebruikt te worden. Uitgangspunt is dat in dit geval toegang door Rijkswaterstaat geregeld wordt met een maximale wachttijd van 15 minuten. Een wachttijd langer dan 15 minuten wordt als meerwerk beschouwd en in overleg verrekend;
- (Preventief) onderhoud kan worden uitgevoerd binnen kantoortijden. De planning dient met SPIE afgestemd te worden en minimaal 10 werkdagen van te voren gemeld te zijn als gepland werk;
- Een reeds met SPIE afgestemde planning wordt minimaal 10 werkdagen voorafgaand aan de werkzaamheden als gepland werk gemeld bij SPIE.
- Voor het oplossen van incidenten zijn soms vervangende materialen en componenten noodzakelijk. Van ieder decentraal component zal een service voorraad aangehouden worden. Alle meldingen veroorzaakt door herhaald of stelselmatig onkundig gebruik van apparatuur en/of programmatuur worden kenbaar gemaakt, zodat dit inzichtelijk wordt en hier structureel een oplossing voor komt;
- Jaarlijks preventief onderhoud en controle van zowel de decentrale Apollo met aangesloten sensoren en het elektrisch motorslot is vereist voor een correcte werking. Voor het oplossen van geconstateerde gebreken tijdens het preventief onderhoud wordt een offerte uitgebracht;
- Om de werking van het complete Apollo systeem te garanderen moet de centrale omgeving (iProtect en iVisit) ten minste één keer per jaar up-to-date gehouden worden (jaarlijkse Software Update);
- Bij het eerste preventief onderhoud worden alle serienummers van de desbetreffende componenten genoteerd en opgeslagen in de CMDB. Bij uitwisseling van componenten op locaties voor het oplossen van incidenten zal er een update in de CMDB.

3.2.1.7.4 CVR locaties in scope

De dienstverlening beslaat de in onderstaand overzicht (**Figuur 11**) weergegeven CVR locaties.

CVR locaties in scope				
Noord Nederland (NN)				
CVR Joure	CVR Hoogeveen	CVR Haren	CVR Werpsterhoek	CVR Zuidbroek
Midden Nederland (MN)				
CVR Deil	CVR Eemnes	CVR Everdingen	CVR Haarrijn	CVR Hoevelaken
CVR Lunetten	CVR Ouderijn	CVR Rijnsweerd		
West Nederland Noord (WNN)				
CVR Hoorn	CVR Watergraafsmeer	CVR Coenplein	CVR Badhoevedorp	CVR Kooimeer
CVR Nieuwe Meer	CVR Raasdorp	CVR De Hoek	CVR Den Oever	CVR Holendrecht
CVR Almere	CVR Amstel			
West Nederland Zuid (WNZ)				
CVR Bodegraven	CVR Gorinchem	CVR Gouwe	CVR Kleinpolderplein	CVR Prins Clausplein 1
CVR Prins Clausplein 2	CVR Ridderkerk	CVR Terbregseplein		
Oost Nederland (ON)				
CVR Azelo	CVR Bankhoef	CVR Barneveld	CVR Beekbergen	CVR Deventer
CVR Hattemerbroek	CVR Lankhorst	Lindeholt	CVR Maanderbroek	CVR Ouddijk

CVR Valburg	CVR Velperbroek		CVR Waterberg	
Zuid Nederland (ZN)				
CVR De Baars	CVR De Stok	CVR Ekkersweijer	CVR Galder	CVR Het Vonderen
CVR Hintham	CVR Hooipolder	CVR Kerensheide	CVR Kruisdonk	CVR Zaarderheiken

Figuur 11: CVR locaties

3.2.1.8 *Glasvezelbeheer*

Met de dienst Glasvezelbeheer voert KPN DO RWS het beheer voor het glasvezelnetwerk van RWS. Dit betreft het aansturen van de werkzaamheden, het registreren van de liggingsinformatie (indien bekend) en het wijzigen van het fysieke glasvezelnetwerk. KPN DO RWS is daarnaast verantwoordelijk voor glasvezelregistratie. Rijkswaterstaat Areaalbeheer
registreert de liggingsgegevens van kabels en leidingen (as-built informatie), dit valt buiten de scope van het Glasvezelbeheer.

De Installed base omvat zowel glasvezelkabel (GVK) als Hoge Dichtheid Polyetheen buis (HDPE).

De dienstverlening bestaat uit de volgende onderdelen:

- **Administratie**

Om operationele glasvezelkabel- en liggingsinformatie uit projecten, incidenten, reconstructies, nieuwbouw en onderhoud te administreren wordt het CMDB Glasbeheersysteem “COntrolled COnsistent Networks” (COCON) gebruikt. Hierin worden complexe glasvezel netwerkstructuren ingevoerd, gemuteerd en geraadpleegd.

- **Leveren van Advies**

Het leveren van advies is nader beschreven in de categorie Overig **paragraaf 4.6.2**.

- **Incidentafhandeling**

DO RWS voert regie bij het oplossen van incidenten. Indien in het incidentmanagement van KPN DO RWS onderzoek of actie nodig is ten aanzien van het glasvezelnetwerk analyseert de incidentcoördinator met behulp van COCON of en waar in het glasvezelnetwerk het incident wordt veroorzaakt. Deze informatie wordt gebruikt voor herstel van patches of om kabelherstel te laten verrichten. De vezelbeheerders van KPN DO RWS verwerken wijzigingen in de glasvezelbezetting als gevolg van de herstelwerkzaamheden in COCON.

- **Uitvoeren geplande werkzaamheden aan de glasinfrastructuur**

De impactanalyse bij Gepland Werk Glas is nader beschreven in de categorie Overig **paragraaf 4.6.1**.

- **Uitvoeren kwaliteitscontrole**

KPN DO RWS voert twee keer per jaar steekproefsgewijs kwaliteitscontroles uit. De locatie waar de controles worden uitgevoerd worden in onderling overleg bepaald.
De kwaliteitscontrole behelst:

  - Controle op de kwaliteit van de glasvezelregistratie;
  - Jaarlijkse controle op de juistheid van de geografische registratie van KPN (COCON) ten opzichte van de registratie in de Kabels & Leidingen administratie van RWS;
  - Controle op de juistheid van de informatie op het label van verdelers en patches in technische objecten (CVR, VC, tunnel);
  - Controle op de kwaliteit van de technische afwerking van glasvezels in technische objecten;
  - Controle op de kwaliteit van de glasvezels doormiddel van Optical Time-Domain Reflector metingen.

Op grond van de uitkomsten van de controles stelt KPN DO RWS een rapport met bevindingen en bijbehorende maatregelen op. In overleg tussen RWS en KPN DO RWS wordt vervolgens bepaald welke maatregelen gerealiseerd worden en wie verantwoordelijk is voor het dragen van bijbehorende kosten.

- **Vezeluitgifte**

KPN DO RWS geeft glasvezels uit aan projecten en houdt reserveringen en de resterende capaciteit bij. Uiteindelijk wordt het definitieve vezelgebruik in Cocon geregistreerd.

3.2.2 *Bestelbare items en levertijd*

De categorie CV BB kent uitsluitend bestelbare items voor IDS/IPS zoals weergegeven in **Figuur 12**.

IDS IPS		
Eenmalige dienst	**Toelichting**	**Levertijd**
IPS Centraal		
Aanvragen	Aanvragen IDS/IPS account *)	L5
Opheffen	Opheffen IDS/IPS account *)	L5
Wijzigen	Wijzigen IDS/IPS account *)	L5
Activeren	Activeren intrusion rule **)	L5
Deactiveren	Deactiveren intrusion rule **)	L5

Figuur 12: Bestelbare items IDS IPS

*) Bij het aanvragen van een account om toegang tot het systeem te krijgen dient aangegeven te worden welke rechten deze gebruiker moet krijgen. Accounts worden niet apart door configuratie management in de CMDB geregistreerd. Via een RFI kan een overzicht van de aanwezige accounts opgevraagd worden. Deze standaard opdrachten kunnen op basis van LNT-Express aangevraagd worden als tactische wijziging. Voor tactische aanvragen dient de afnemer contact op te nemen met de Relatie Manager van RWS CIV IRN Infra Netwerken. De Relatie Manager bepaalt of de aanvraag al dan niet in behandeling wordt genomen.

**) Het betreft voor gedefinieerde intrusion rules die geactiveerd of gedeactiveerd kunnen worden.

3.3 Categorie VPN - detailbeschrijving

Onder de categorie **Virtual Private Network (VPN)** vallen de diensten VPN, DDI, DMZ en DMZ Client, Mail relay, Forward Webproxy en Virtual Firewall.

Dit hoofdstuk bevat de detailbeschrijving van het VPN en de VPN diensten. In Deel 2 van deze catalogus is een generieke beschrijving van de functionaliteiten beschikbaar ten behoeve van afnemers.

3.3.1 *Functionele omschrijving*

Virtual Private Networks (VPN's) zijn landelijk beschikbaar en kunnen middels de diensten VPN Aansluiting en LAN aansluiting tot op LAN access poort niveau op eindlocaties ontsluiting bieden tot systemen. Optioneel kan het VPN via een Virtual Firewall verbonden worden met het internet middels Internet Access. Afhankelijk van het type VPN zijn bepaalde standaardvoorzieningen mogelijk, verplicht of beperkt.

Een VPN biedt de mogelijkheid binnen een besloten en logisch gescheiden netwerk op veilige, betrouwbare wijze bedrijfsinformatie en applicaties te benaderen én informatie te delen tussen geografisch gescheiden netwerken als binnen één dedicated netwerk. Het VPN is randvoorwaardelijk om communicatie tussen eindsystemen op RWS en niet-RWS eindlocaties mogelijk te maken.

3.3.2 *Dienstenmatrix Categorie VPN*

Onderstaande matrix (**Figuur 13**) geeft een overzicht van de diensten in de Categorie VPN en bijbehorende opties. In de volgende paragrafen worden deze nader toegelicht.
De per dienst afgegeven beschikbaarheid is empirisch bepaald. Dit betekent dat het technisch design zodanig is dat de afgegeven SLA gegarandeerd kan worden.
De weergegeven storingshersteltijd is gebaseerd op incidenten waarbij de dienstverlening onderbroken is (er is business impact). Wanneer er sprake is van verstoorde dienstverlening (geen business impact) geldt het SLA zoals weergegeven in **Bijlage E**.

Matrix VPN											
	Beschikbaarheid							Storingshersteltijd in 95% van de gevallen			
	Enkel			Dubbel			VPN	Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
	99,5%	99,9%	99,95%	99,95%	99,98%	99,99%	99,999%				
	Onbeschikbaarheid per jaar										
Diensten	ca. 1d20u	ca. 8u45m	ca. 4u28m	ca. 4u28m	ca. 1u45m	ca. 0u52m	ca. 5m15s	K8	K4	E8	E4
VPN							√				√
Virtual firewall			√								√
DDI - DHCP & DNS*	√					√					√
DDI - IPAM		√									√
DMZ en DMZ Client					√						√
Forward webproxy				√							√
Mail relay				√							√

*De centrale beschikbaarheid van DDI componenten is 99,99%, deze zijn dubbel uitgevoerd en hiertoe geplaatst over twee fysiek geografisch gescheiden locaties. De beschikbaarheid over de gehele keten is afhankelijk van de overige bouwstenen waar de afnemer gebruik van maakt.

Figuur 13: VPN

3.3.2.1 *VPN*

3.3.2.1.1 Functionele omschrijving

Een Virtual Private Network (VPN) stelt RWS in staat (een) besloten en volledig gescheiden netwerk(en) te creëren. Dit maakt het mogelijk om op veilige, betrouwbare wijze informatie te delen tussen geografisch gescheiden netwerken alsof er één dedicated netwerk zou zijn. Een VPN is randvoorwaardelijk om communicatie tussen eindsystemen op RWS en niet-RWS eindlocaties mogelijk te maken. VPN's zijn landelijk beschikbaar en kunnen middels de diensten VPN Aansluiting en LAN aansluiting tot op LAN access poort op eind locaties ontsluiting bieden tot systemen.

3.3.2.1.2 Opties

Er wordt binnen de dienst VPN onderscheid gemaakt tussen eigenschappen waarvan impliciet gebruik wordt gemaakt en functies die expliciet aangevraagd dienen te worden.
De belangrijkste eigenschappen van VPN zijn:

- Any to any IP connectiviteit tussen op het RWS Netwerk backbone ontsloten RWS Netwerk locaties;
- Het netwerk bepaalt optimale routering;
- Het netwerk gedraagt zich als geografisch gedistribueerde router.

De onderstaande tabel beschrijft de standaard en optionele eigenschappen van het VPN.

Eigenschappen VPN	
Eigenschap	**Omschrijving**
VPN (Virtual Routingsdomain)	IP any-to-any routering binnen een virtueel netwerk in de RWS Netwerk backbone met een vrij te kiezen IPv4 adresruimte voor zover beschikbaar binnen het RWS netwerk
Internet Access door middel van Firewall policy en rules	In- en/of uitgaand internet verkeer
IDS/IPS	Inspectie van in- en uitgaand verkeer
NTP	De eigenschap NTP levert een centrale klok waarmee eindsystemen binnen het VPN hun tijd kunnen synchroniseren via het NTPv4 protocol

Figuur 14: Eigenschappen VPN

Met de eigenschap Internet Access wordt veilig en gecontroleerd toegang gegeven tot het internet vanuit RWS, en vice versa. Internet Access is een centrale oplossing die uitsluitend voorziet in de toegang tot het internet en die op aanvraag, middels de dienst Firewall Policy en rules, beschikbaar is voor ieder VPN.
IDS/IPS controleert het verkeer van en naar het internet op schadelijke aspecten.
De afnemer conformeert zich bij afname van Internet Access expliciet aan het beveiligingsbeleid van RWS.
In onderstaande **Figuur 18** is met groen de basis van Internet Access weergegeven en met geel de overige diensten die, afhankelijk van de communicatiebehoefte, verplicht afgenomen dienen te worden.

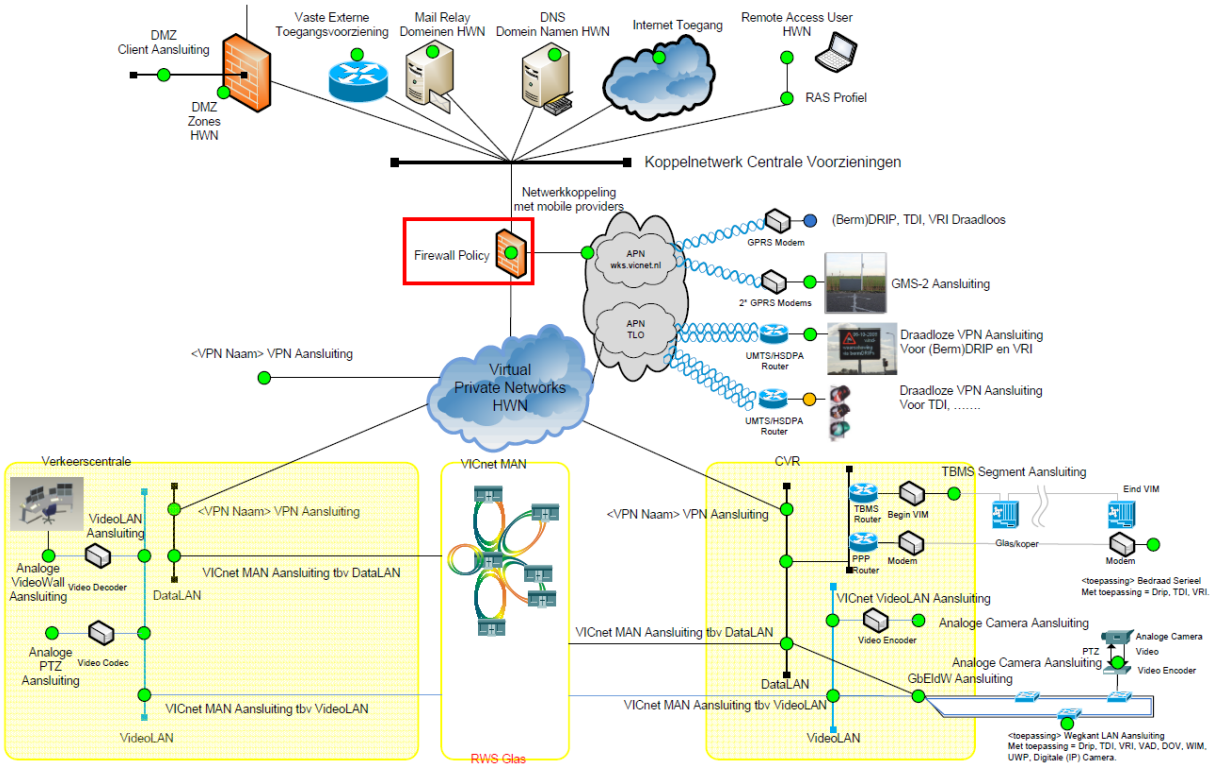
De functies van het VPN zijn weergegeven in **Figuur 15: Functies VPN**.

Functies VPN	
Eigenschap	**Omschrijving**
Mailrelay	Functie voor e-mail uitwisseling buiten het VPN
Forward Webproxy	De functie Webproxy dient als uitgang voor al het websurfverkeer door gebruikers naar het Internet en andere externe netwerken (en dus niet interne webapplicaties).
DHCP	De functie DHCP levert een centrale voorziening om clients (en hosts) binnen het VPN op dynamische wijze van netwerkinstellingen te voorzien middels DHCP (Dynamic Host Configuration Protocol)
DNS	De functie DNS levert name services aan de, binnen het VPN, aangesloten systemen op basis van het DNS protocol
InterVPN comunicatie door middel van Firewall policy en rules	In- en/of uitgaand internet verkeer
Externe koppeling	In- en/of uitgaand verkeer naar aangesloten externe netwerken

Figuur 15: Functies VPN

3.3.3 *Virtual firewall*

Het RWS netwerk beschermt de integriteit en vertrouwelijkheid van de verschillende VPN's en DMZ's door middel van firewalls. Een firewall blokkeert alle communicatie, tenzij expliciet toegestaan. Daarnaast worden specifieke (potentieel schadelijke) communicatiepatronen binnen toegestane communicatie geblokkeerd. Een Firewall Policy bepaalt per VPN, DMZ en het Internet welke communicatiestromen zijn toegestaan.



Figuur 16: Virtual Firewall overzicht

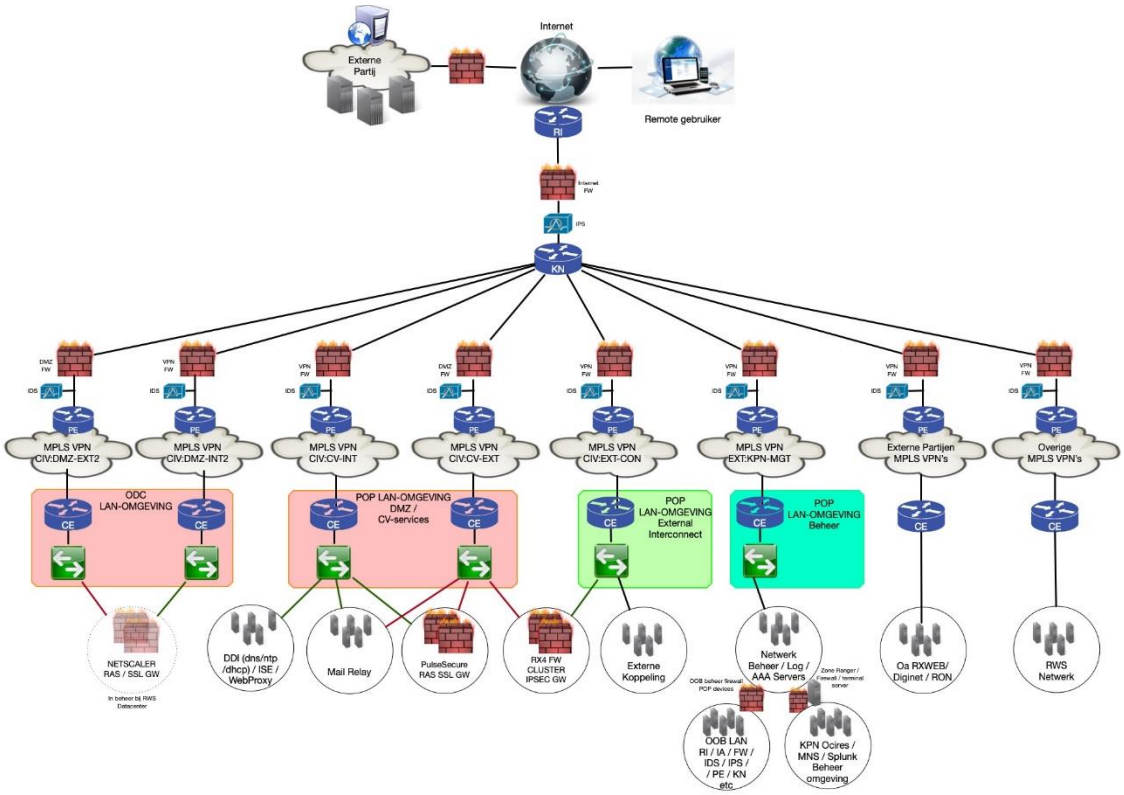
Een Firewall Policy bestaat uit een specificatie van toegestane datastromen waarbij niet meer toegang dient te worden verleend dan strikt noodzakelijk. Per VPN kan een virtual firewall geleverd worden.

Een **datastroom** wordt binnen de dienst Virtual Firewall gespecificeerd middels de volgende voorwaarden:

- Bron IP adres: IP adres waar datacommunicatie opgezet wordt (het beginpunt);
- Bron IP Protocol: TCP, UDP of ICMP;
- Bron Poort: IP poort nummer dat in combinatie met het Bron Protocol de applicatie op het Bron systeem identificeert;

- Doel IP adres: het IP adres waarnaar datacommunicatie opgezet wordt (de eindbestemming);
- Doel Protocol: TCP, UDP of ICMP;
- Doel Poort: het IP poort nummer dat in combinatie met het Doel Protocol de applicatie op het Doel systeem identificeert.

Om meerdere aaneengesloten IP adressen tegelijkertijd aan te duiden, kan in combinatie met het IP-adres ook het bron of doel IP-Subnetmasker aangegeven worden. Een IP-Subnetmasker specificeert het netwerksegment en de systemen in dit netwerksegment.

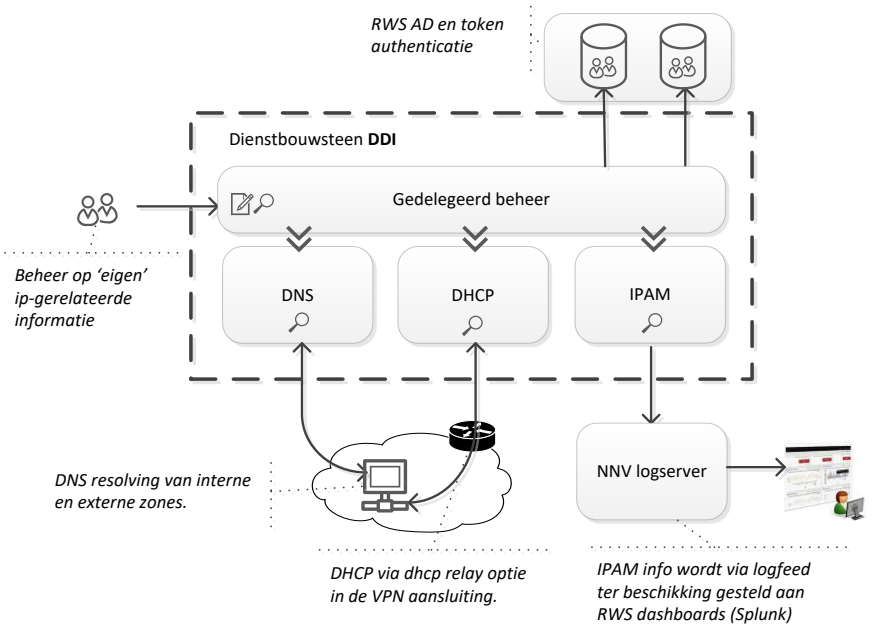


Figuur 18: samenhang dienstbouwstenen categorie VPN

3.3.4 *DDI*

3.3.4.1 *Functionele omschrijving*

DDI (DNS DHCP IPAM) levert de aan IP-adressen gerelateerde services aan de Centrale Voorzieningen van het RWS netwerk. Daarnaast geeft het specifieke RWS medewerkers en onderaannemers van RWS de mogelijkheid om relevante IP-gerelateerde configuraties te onderhouden. De scope van DDI is in **Figuur 19** hieronder weergegeven met een stippellijn.



Figuur 19: onderdelen dienstbouwsteen DDI

De dienst DDI bevat de volgende onderdelen:

- Gedelegeerd beheer voor DDI;
- IP Address Management (IPAM);
- Domain Name Services (DNS);
- Dynamic Host Configuration Protocol (DHCP).

3.3.4.2 *Opties DDI*

3.3.4.2.1 Gedelegeerd beheer

De functie 'gedelegeerd beheer' geeft RWS medewerkers en RWS onderaannemers de mogelijkheid om de 'IP-ruimte' waarvoor zij verantwoordelijk zijn te beheren. Deze functie heeft de volgende kenmerken:

- Sterke gebruikers authenticatie met een hardware token (RSA) + gebruikersnaam/wachtwoord uit de RWS Active Directory (AD)[1] of gebruik te maken van de SMS authenticatie binnen de dienst;
- Autorisatie via groepslidmaatschap in RWS AD. De permissies per groep (lezen, schrijven, en waar op) worden via een standaard aanvraag gerealiseerd;
- Zonder aangevraagde permissies heeft een medewerker geen mogelijkheden tot het gebruik van de 'gedelegeerd beheer' functionaliteit;
- Via 'gedelegeerd beheer' kan men de IPAM , DNS en/of DHCP gegevens muteren voor zover het eigenaarschap op de betreffende IP-ruimte reikt.
- Via 'gedelegeerd beheer' kan men daarnaast, afhankelijk van toegewezen permissies, inzicht krijgen in de inhoud van een DDI-profiel (welke DDI-info en welke permissies zijn toegewezen aan een rol).

[1] Een onderaannemer van RWS dient een AD account te hebben om gedelegeerd beheer te kunnen doen.

- Logging van toegang en toegangspogingen;
- Voor gedelegeerd beheer is het van belang dat een gebruiker slechts lid is van 1 DDI-gerelateerde resourcegroep. De dienst werkt zo dat de permissies worden gekoppeld aan het eerste groepslidmaatschap dat in het kader van DDI wordt aangereikt vanuit de RWS AD omgeving.

3.3.4.2.2 IP Address Management (IPAM)

IPAM geeft geautoriseerde RWS medewerkers de mogelijkheid om IP-gerelateerde informatie vast te leggen om context te kunnen geven aan IP-gerelateerde gegevens zoals fysieke locatie, eigenaar, toepassing etc. Zo wordt IP-informatie beter bruikbaar als ondersteuning bij audits, het uitvoeren van kwaliteitscontrole, het toetsen van KPI's en het onderzoeken van verstoringen/incidenten (onder andere security).

IPAM heeft de volgende kenmerken:

- Een grafische gebruikersinterface;
- Informatievastlegging (eigenaar, toepassing, security classificatie etc.);
- Informatievastlegging per IP reeks of subnet;
- Zoekfunctie binnen velden IPAM database (IP adres, VPN naam, eigenaar, 'next Available IP' etc.);
- Vastlegging DNS naam die bij een IP-adres hoort en automatische synchronisatie met de DNS functie;
- Vastlegging DHCP gegevens van een IP-adres en automatische synchronisatie met de DHCP functie;
- Overerving van op hoger niveau vastgelegde informatie (zoals VPN naam waartoe de IP-ruimte behoort);
- Read only voor gegevens die niet gewijzigd mogen worden en schrijftoegang tot gegevens die gewijzigd mogen worden;
- Beschikbaar stellen IPAM informatie database via RWS Splunk feed (volledige export IPAM database 1x per 24 uur);
- Logging van alle mutaties, inclusief naam van de uitvoerende persoon en het tijdstip.

3.3.4.2.3 Domain Name Services (DNS)

De DNS-functie levert aan het RWS netwerk de centrale DNS functies voor het oplossen van interne RWS DNS zones en externe niet-RWS[2] DNS zones zoals Internet). Deze functie heeft de volgende kenmerken:

- Mutaties zijn mogelijk via aanvraag (per record of in bulk) of via gedelegeerd beheer;
- Zone transfers worden niet ondersteund;
- Voorziet in hosting en resolving van interne DNS domeinnamen;
- Resolving van externe DNS domeinnamen, hetzij generiek (recursief, bijvoorbeeld google.com), hetzij specifiek (Forwarding, bijvoorbeeld naar rijksweb.nl);
- Beschikbaar voor alle RWS MPLS VPN's, mits vanuit security regelgeving toegestaan en het geen gesloten VPN betreft;
- Zone informatie kan beschikbaar worden gesteld aan of worden afgeschermd voor bepaalde source IP subnetten door gebruik te maken van 'DNS views';
- DNSSEC[3]-validatie van DNS responses bij resolving op Internet (externe resolver). DNSSEC signing van RWS domeinen wordt niet ondersteund;
- Logging van DNS requests en failures;
- Dynamische zone updates als gevolg van IP adrestoekenning via DHCP (Dynamic DNS, ofwel DDNS) worden genegeerd.

[2] De externe DNS zones van RWS zelf (bv rws.nl) zijn buiten scope van deze dienst. Deze externe zones worden extern gehost, o.a. bij Prolocation. Verdere informatie bij IRN CIV netwerken.

[3] Is een crypto grafische beveiliging voor het DNS-protocol. Clients die deze uitbreiding ondersteunen, ontvangen van de DNS server adres-informatie met een digitale handtekening. Zo wordt de integriteit van de DNS omgeving en het transport van de DNS data beschermd.

3.3.4.2.4 *Dynamic Host Configuration Protocol (DHCP)*

DHCP levert het RWS netwerk de centrale DHCP functie voor het configureren van IP-instellingen op aangesloten apparatuur. Deze functie heeft de volgende kenmerken:

- De functionaliteit om op dynamische wijze de netwerkinstellingen van op het RWS netwerk aangesloten hosts te configureren (IP-nummers, name servers, gateway adressen, netmask, proxy adres e.d.);
- Aangezien de centrale DHCP gepositioneerd wordt buiten het broadcast domein dient op die delen waar DHCP van toepassing is, DHCP relay/helper op de VPN Aansluiting ingesteld te worden;
- Mutaties mogelijk via aanvraag (per scope met bijbehorende opties, of in bulk) of gedelegeerd beheer;
- Vendor specifieke DHCP options worden ondersteund;
- Het is mogelijk om een vast DHCP IP adres te koppelen aan hetzelfde systeem (MAC adres of Client-ID), standaard wordt een MAC adres gekoppeld aan een IP adres;
- DHCP configuratie is zoveel mogelijk generiek, maar kan per VPN-aansluiting van uitzonderingen worden voorzien na akkoord van CIV IRN Netwerken;
- Logging van DHCP requests en failures;
- Inzicht in de mate van uitnutting van een DHCP scope. Bij naderende (bv.80%) of volledige (100%) uitnutting wordt hierover genotificeerd. Sommige objecten moeten autonoom kunnen draaien en mogen derhalve geen gebruik maken van centrale DHCP.

3.3.4.3 *Uitgangspunten*

De volgende uitgangspunten gelden voor DDI:

- Gebruiker krijgt alleen toegang tot IPAM indien deze in bezit is van een geldig RWS AD account;
- Netwerk connectiviteit dient te zijn ingeregeld om gebruik te kunnen maken van DNS;
- Voor DHCP worden geen scopes geboden met overlappende IP reeksen. Uitgangspunt is dat alle aansluitingen in het RWS netwerk unieke adressen hebben;
- RWS CIV-infra is verantwoordelijk voor de toetsing van aanvragen voor gedelegeerd beheer zodat alleen geautoriseerde personen toegang krijgen tot de data binnen DDI;
- Admin toegang wordt geregeld via centrale BAS service;
- DDI-configs zijn als het ware containers met DNS-, DHCP- en/of IPAM objecten. Men kan een wijziging aanvragen voor objecten in een container, of gedelegeerd beheer krijgen op de objecten in een container. Het beheer op de container zelf is voorbehouden aan KPN DO RWS in diens verantwoordelijkheid voor de netwerk- en netwerkservices dienstverlening;
- DDI profielen worden zo generiek mogelijk ingericht en onderhouden om te voorkomen dat een onoverzichtelijke set van profielen ontstaat. Dit is essentieel voor onder andere auditeerbaarheid van toegangsrechten. Tevens dient maximaal te worden geprofiteerd van overerving uit (default) settings;
- RWS stelt de profielnaam vast;
- De aanvrager (geprocedeerde) is verantwoordelijk voor de inzet c.q. gebruik;
- De gebruiker (bv gedelegeerd beheerder) is verantwoordelijk voor het veilig omgaan met de informatie en de toegangsmiddelen;
- De gedelegeerde beheerder is zelf verantwoordelijk voor verstoringen op de keten die voortvloeien vanuit aanpassingen die worden gedaan door de beheerder zelf;
- RWS is verantwoordelijk voor het aan KPN DO RWS verstrekken van geldige digitale certificaten (PKI) voor de HTTPS ontsluiting van de ‘gedelegeerd beheer’ functie.

3.3.5 *DMZ*

De dienst **DMZ (Demilitarised Zone)** voorziet in een gecontroleerde communicatiezone tussen het interne en het externe netwerk om veiligheidsrisico's te verkleinen. Het externe netwerk, vaak het internet, is "untrusted". Een systeem in de DMZ is relatief vrij toegankelijk vanuit het publieke internet.
Het interne netwerk is echter een beschermd "trusted" deel van het netwerk, zoals een interne VPN, dat uitsluitend toegankelijk is voor geautoriseerde systemen en gebruikers.

3.3.6 *Forward Webproxy*

De dienst Forward Webproxy dient als uitgang voor al het websurfverkeer door gebruikers naar het internet en andere externe netwerken (en dus niet interne webapplicaties) en dient te worden afgenomen om websurfen op externe netwerken via http(s) protocollen mogelijk te maken.

Deze dienst is in detail beschreven in de Categorie Backbone Core CV waar het centrale abonnement wordt doorberekend. Het aanvragen en opheffen van Forward Webproxy is een uitsluitend door RWS CIV IRN Infra Netwerken te bestellen item in de categorie VPN. Hiervoor geldt een maatwerktarief. Voor het wijzigen van de Forward webproxy geldt een standaard tarief.

3.3.7 *Mail relay*

De dienst Mail Relay dient als in- en uitgang voor al het e-mailverkeer van en naar het internet. Mail Relay wordt ingezet als koppelvlak voor e-mailuitwisseling binnen RWS, met het internet en met organisaties aangesloten op het Rijksweb. Het afnemen van de dienst Mail Relay is noodzakelijk om e-mail te kunnen ontvangen van externe netwerken via het smtp protocol en is een functie op het VPN die e-mail uitwisseling buiten het VPN mogelijk maakt.
Deze dienst is in detail beschreven in de Categorie Backbone Core CV waar het centrale abonnement wordt doorberekend. Het aanvragen, opheffen en wijzigen van Mail Relay kan middels een bestelbaar item met standaard tarief worden aangevraagd door RWS CIV IRN Infra Netwerken en haar afnemers.

3.3.8 *Bestelbare items en levertijd*

Voor het VPN gelden de in **Figuur 20** weergegeven bestelbare items met bijbehorende standaard levertijden.

VPN		
Eenmalige dienst	**Toelichting**	**Levertijd**
VPN		
Aanvragen	Leveren nieuw VPN	L20
Opheffen	Opheffen VPN	L20
Wijzigen	Wijzigen instelling bestaand VPN op afstand	L10
Aanvragen VPN QOS Profiel	Realiseren QoS profiel op VPN	L20
Virtual firewall		
Aanvragen	Leveren nieuwe Firewall	L10
Opheffen	Opheffen Firewall	L10
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules (max. 20 rules per aanvraag*)	L5
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules met spoed	L1
DDI – DHCP Scope		
Aanvragen	Aanvragen DHCP scope (IP range centrale distributie)	L10
Opheffen	Opheffen DHCP scope (IP range centrale distributie)	L10
Wijzigen	Wijzigen DHCP scope (IP range centrale distributie)	L10
Aanvragen toegang	Aanvragen toegang op bestaande DHCP scope RW/RO	L10
Opheffen toegang	Verwijderen toegang op bestaande DHCP scope RW/RO	L10

DDI – DNS Domeinnaam		
Aanvragen	Leveren DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L10
Opheffen	Opheffen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L10
Wijzigen	Wijzigen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L5
DDI – Gedelegeerd beheer		
Aanvragen	Aanvragen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
Opheffen	Opheffen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
Wijzigen	Wijzigen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
DDI – IPAM		
Aanvragen	Aanvragen/opvoeren van een (nieuw) netwerk, of nieuwe eigenaren van bestaand netwerk	L10
Opheffen	Opheffen van netwerk informatie van netwerken binnen een VPN	L10
Wijzigen	Opvoeren/update van host informatie binnen een netwerk	L5
DMZ en DMZ Client		
Aanvragen	Aanvragen DMZ	L30
Opheffen	Opheffen DMZ	L10
Aanvragen Client	Aanvragen Client aansluiting	L20
Opheffen Client	Opheffen Client aansluiting	L10
Wijzigen Client	Wijzigen Client aansluiting	L5
Forward Webproxy		
Aanvragen	Aanvragen Forward Webproxy	In overleg
Opheffen	Opheffen Forward Webproxy	In overleg
Wijzigen	Wijzigen Forward Webproxy	In overleg
Mail relay[4]		
Aanvragen	Aanvragen Mail Relay	In overleg
Opheffen	Opheffen Mail Relay	In overleg
Wijzigen	Wijzigen Mail Relay	In overleg

Figuur 20: Overzicht bestelbare items Categorie VPN

*Wanneer er meer dan 20 rules gewijzigd moeten worden adviseren wij u gebruik te maken van een meervoudige PDC project aanvraag.

3.3.9 *Verrekening*

Op basis van de afgenomen diensten wordt een selectie bestelbare items in rekening gebracht. De van toepassing zijnde functionaliteiten zoals hierboven beschreven zijn zichtbaar als line item op de factuur.

3.4 Categorie Special

Onder de categorie **Special** vallen een aantal diensten die vanwege de bijzondere kenmerken van de gewenste oplossing niet binnen de standaard dienstverlening passen. Deze diensten worden beperkt ingezet en kunnen niet worden aangevraagd.

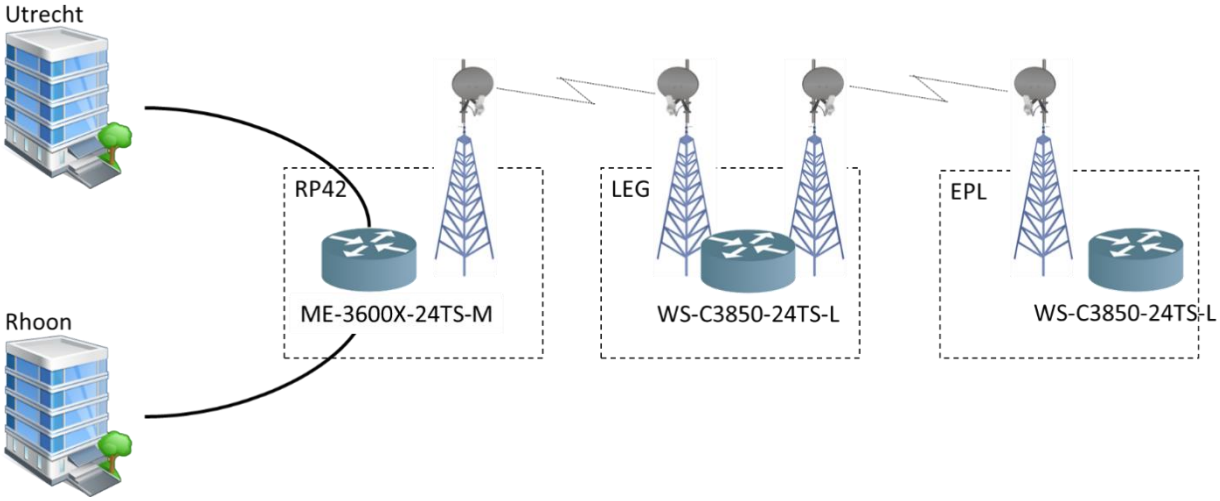
3.4.1 *Beheer Verbindingen LEG-EPL (Lichteiland Goeree – Europlatform)*

KPN DO RWS levert connectiviteit op de RWS platformen voor de kust van Rotterdam.
Ten behoeve van het transport van meetgegevens op de Noordzee wordt gebruik gemaakt van een straalverbinding tussen twee lichteilanden: Lichteiland Goeree (LEG) en Europlatform (EPL).

Vanaf Radarpost 42 (RP42) wordt een straalverbinding opgezet naar LEG en vanaf LEG wordt deze doorgestraald naar EPL. Deze straalverbinding is samen met de router in beheer bij KPN.

RP42 is eigendom van Havenbedrijf Rotterdam, LEG en EPL zijn in beheer van RWS. Met deze partijen zijn door KPN afspraken gemaakt over het gebruik en toegang tot de (technische) ruimtes op deze locaties.

RP42 is aangesloten op de POP locaties Rhoon en Utrecht met een 10Mb ethernet verbinding van Tele2. Vanaf RP42 is een straalpad opgezet van 10Mb naar LEG en 2Mb naar EPL zoals weergegeven in **Figuur 21**.



Figuur 21: LEG EPL dienstverlening

3.4.1.1 *Uitgangspunten*

- De verbinding tussen de Radar Post 42 en LEG en EPL wordt gevormd door een straalverbinding op ethernet basis;
- De switches voor LEG en EPL zijn ge-stackt opgehangen (doorgekoppeld);
- Locatie ontsluiting Dubbel (99,8%) wordt formeel niet toegepast;
- De ingezette router (ME3600X) op RP42 is niet bedoeld voor 10Mb ontsluiting;
- Standaard Service Levels zijn op zee niet van toepassing;
- De bandbreedte van de huidige configuratie kan niet worden uitgebreid. Indien meer bandbreedte gewenst is zal dit nader onderzocht moeten worden en dit kan gepaard gaan met forse investeringen.

3.4.1.2 *Servicelevels*

Voor de LEG EPL Special zijn de SLA afspraken conform **Figuur 22** van toepassing.

Service level element	Service level
Beschikbaarheid	
Doelbeschikbaarheid	99,5%
Servicewindow	E4 (365*7*24)
Openstellingtijden servicedesk	24*7 per e-mail en telefonisch
Storingshersteltijd gerekend vanaf vertrek helikopter	95% binnen 8 uur bij dienst verstoord 95% binnen 4 uur bij dienst onderbroken
Maintenance Window	10:00-15:00 in overleg met MKO
Capaciteit	
Throughput	LEG: 10Mb/s EPL: 2Mb/s
Prestaties	
MTU	1.500 Bytes
Packet loss	< 2%
Delay (RTT) typical	< 2ms

Jitter	Delay+jitter < max delay
Convergentiesnelheid	<60s
Multicast support	Ja

Figuur 22: LEG EPL dienstverlening

3.4.2 *CCM aansluiting*

De CCM aansluiting is een VPN Aansluiting Serieel op de CCM server. Het betreft een server die in VicNet staat ten behoeve van camerabediening PTZ. Deze Special kan niet worden aangevraagd of gewijzigd.

3.4.3 *Noodknopbediening Sijtwendetunnel*

Aansluiting voor serieel overbrengen van contacten. Maakt gebruik van dezelfde technische componenten als de Special CCM. Deze Special kan niet worden aangevraagd of gewijzigd.

3.4.4 *Bestelbare items en levertijd*

Voor de **Specials** gelden de in **Figuur 23** weergegeven bestelbare items met bijbehorende standaard levertijden.

Special		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Beheer Verbindingen LEG-EPL		
Opheffen		in overleg
CCM aansluiting		
Opheffen		in overleg
Noodknopbediening Sijtwendetunnel		
Opheffen		in overleg

Figuur 23: Bestelbare items en levertijd Specials

3.4.5 *Dark Fiber Advies*

Het doel van de dienst Dark Fiber is om RWS in uitzonderlijke gevallen in staat te stellen het Eigen Glas beschikbaar te stellen aan andere (overheids-)partijen in het geval van overcapaciteit. Deze dienst kan alleen worden afgenomen na expliciete goedkeuring van de domeineigenaar van Infra Netwerken, en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken.

Om te bepalen of het op een bepaalde locatie mogelijk is gebruik te maken van de Dark Fiber dienst dient altijd eerst een Dark Fiber Advies te worden aangevraagd. Er wordt onderscheid gemaakt tussen een Dark Fiber Advies type Eenvoudig en type Complex.

3.4.6 *Dark Fiber RWS levering*

Het doel van de dienst Dark Fiber is om RWS in uitzonderlijke gevallen in staat te stellen het Eigen Glas beschikbaar te stellen aan andere (overheids-)partijen in het geval van overcapaciteit. Deze dienst kan alleen worden afgenomen na expliciete goedkeuring van de domeineigenaar van Infra Netwerken en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken

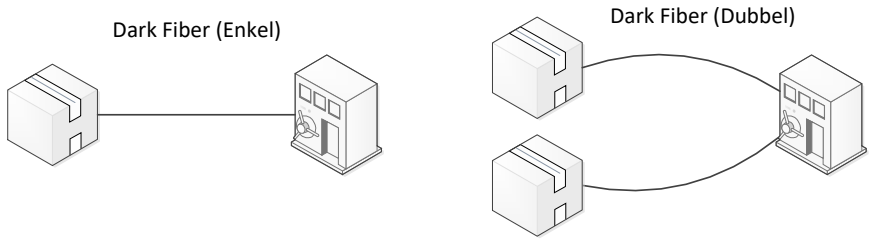
Dark Fibers zijn onbelichte glasvezelverbindingen tussen 2 locaties, bestaande uit een vezelpaar. De capaciteit van Dark Fiber is afhankelijk van het aanwezige type glasvezel, de te overbruggen afstand en de apparatuur die door de afnemer wordt ingezet.
Dark Fibers worden in heel Nederland geleverd. Hierbij wordt alleen gebruik gemaakt van bestaande infrastructuur. Binnen een Dark Fiber levering is geen sprake van aanleg van nieuwe glasvezels.
De Dark Fiber dienst is unmanaged, er vindt geen proactieve bewaking plaats.

3.4.6.1 *Opties*

De Dark Fiber dienstverlening onderscheidt een aantal opties met betrekking tot de uitvoering van de Dark Fiber, demarcatie/eindpunten en aansluitvarianten.

3.4.6.1.1 Enkel / Dubbel uitgevoerde Dark Fiber

Een Dark Fiber-verbinding, weergegeven in **Figuur 51**, bestaat uit twee vezels en kan worden uitgevoerd met een enkele of dubbele verbinding.



Figuur 51: Dark Fiber uitvoering

Dark Fiber (Enkel) = Een vezelpaar tussen twee eindpunten.
Dark Fiber (Dubbel) = Twee geografisch gescheiden vezelparen tussen twee eindpunten, administratief en procedureel onlosmakelijk met elkaar verbonden. Op het moment dat er een storing is op de ene glasvezelverbinding, dan kan de gebruiker door zelf om te schakelen het dataverkeer door laten gaan over de andere glasvezelverbinding. Uiteraard kunnen ook beide verbindingen actief gebruikt worden.

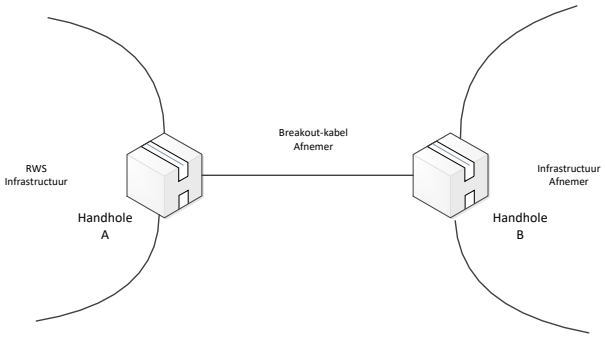
3.4.6.1.2 Demarcatie / Eindpunten

Het demarcatiepunt van de Dark Fiber verbinding kent twee uitvoeringsvormen. Eindpunten kunnen ondergronds (laskoppeling in een glasvezelkabelput) of bovengronds (patchpaneel in RWS-ruimte) zijn. De koppelvlakken van de Dark Fibers zijn ofwel ondergronds (glasvezellassen), dan wel bovengronds (patchpaneel).

3.4.6.1.3 Aansluitvarianten

Er bestaan twee aansluitvarianten (**Figuur 52**):

1. Handhole (ondergronds)



Figuur 52: Aansluitvariant Handhole

Het koppelvlak voor de Dark Fiber-verbinding bevindt zich in Handhole A.

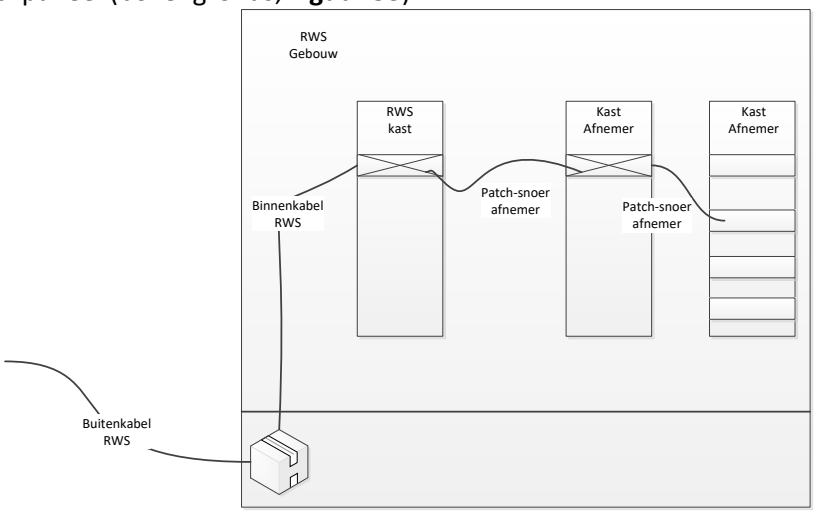
Verantwoordelijkheden RWS-afnemer:

- de aanleg van haar glasvezelinfrastructuur inclusief de Handhole voor koppeling met de RWS-glasvezelinfrastructuur;
- de aanleg van de break-out-kabel tussen beide Handholes;
- het invoeren van de break-out-kabel in Handhole B;
- het koppelen van de glasvezels van de break-out-kabel aan de glasvezelinfrastructuur in Handhole B.

Verantwoordelijkheden RWS:

- het projecteren van de glasvezels in de RWS-infrastructuur (uitgevoerd door KPN DO RWS);
- het invoeren van de break-out-kabel in Handhole A (uitgevoerd door KPN DO RWS aannemer);
- het koppelen van de glasvezels (voorzien van connectoren type E2000/APC) van de break-out-kabel aan de glasvezelinfrastructuur in Handhole A (uitgevoerd door KPN DO RWS aannemer).

2. Patchpaneel (bovengronds; **Figuur 53**)



Figuur 53: Aansluitvariant Patchpaneel

Binnen een gebouw van RWS wordt de Dark Fiber-verbinding opgeleverd op een patchpaneel, welke is gemonteerd in een 19”-kast. Het patchpaneel is de domeinscheiding tussen RWS en de RWS-afnemer.

Binnen de Dark Fiber-dienstverlening valt het:

- Aanbrengen patchpaneel in 19”-kast (indien noodzakelijk);
- Projectering glasvezel-posities op patchpaneel;
- Aanbrengen label op posities op patchpaneel.

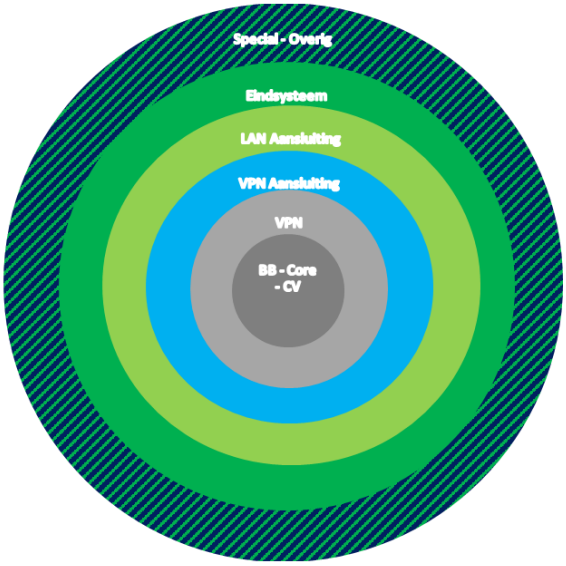
3.4.6.2 *Specifieke leveringsvoorwaarden*

Dark Fiber mag uitsluitend worden gebruikt voor het transport van optische transmissiesignalen.
De systemen die daarvoor door de afnemer worden ingezet, moeten voldoen aan de laserveiligheidseisen in IEC 60825-2 met betrekking tot laser class 1 (maximaal vermogen van 10 mW bij 1550 nm of 16 mW bij 1310 nm).

Als het vanwege afstandsoverbrugging noodzakelijk is om meer vermogen toe te passen, dan mogen ook systemen van laser class 1 M of 3 B worden toegepast. Dit mag alleen als deze zijn uitgerust met een (geactiveerde) voorziening die de laser uitschakelt bij een onderbreking in het lichtcircuit. Deze technieken zijn bekend als Automatic Laser Shutdown (ALS), Automatic Power Reduction (APR) en Intelligent Power Reduction (IPR).

Omdat deze technieken niet altijd vastgelegd zijn in internationale normen dienen de specificaties aan KPN DO RWS ter beoordeling te worden aangeboden. KPN DO RWS behoudt zich het recht voor om in geval van twijfel deze systemen te testen op bovengenoemde normen en indien nodig consequenties te verbinden aan de uitkomst van die testen. Transmissiesystemen die in laser class 4 vallen, mogen nooit worden ingezet op Dark Fiber. Dit in verband met de veiligheid van KPN DO RWS- en andere medewerkers. Er zijn geen eisen gesteld aan de maximale lengte van Dark Fibers.

Catalogus deel 2: Netwerkdiensten CIV Klant



Figuur 24: Categorieën Netwerkdiensten CIV Klant

VPN (functionaliteiten)
VPN
Virtual Firewall
DDI
DMZ
Forward Webproxy
Mail Relay
VPN Aansluiting
VPN aansluiting
Draadloze VPN aansluiting
Externe koppeling
LAN Aansluiting
LAN aansluiting type Gebouw
LAN aansluiting type Verkeerscentrale
LAN aansluiting type CVR/VOR
LAN aansluiting type Weg- / Waterkant
KA LAN incl. callcenter
WIFI
LAN aansluiting type ODC
LAN aansluiting type SPAN
Eindsysteem
Digitale Video aansluiting
MiniFEP
Remote Access groepsprofiel
AAA
PPP aansluiting
TBMS BUS
Draadloze aansluiting
Overig
Glas, , Adviezen, Uurtarieven consultancy, Rijkskantoorroam

4 Netwerkdiensten CIV Klant

4.1 Inleiding

Dit deel van de catalogus biedt een overzicht van de diensten welke door afnemers van CIV IRN Infra Netwerken kunnen worden besteld in de categorie VPN, VPN Aansluiting, LAN Aansluiting en Eindsysteem. De uitsluitend door dan wel via CIV IRN Infra Netwerken te bestellen diensten zijn beschreven in deel 1 “Netwerkdiensten CIV IRN Infra Netwerken”.

4.2 Categorie VPN

Onder de categorie **Virtual Private Network (VPN)** vallen het VPN en de additionele functionaliteiten op het VPN zoals DDI, DMZ en DMZ Client, Mail relay en de Virtual Firewall.

Om gebruik te kunnen maken van verscheidene functionaliteiten uit de categorieën Eindsystemen, LAN aansluiting en VPN aansluiting wordt gebruik gemaakt van een VPN. De aanvrager dient aan te geven op welk VPN hij aangesloten wenst te worden.

4.2.1 *Functionele omschrijving*

Virtual Private Networks (VPN’s) zijn landelijk beschikbaar en kunnen middels de diensten VPN aansluiting en LAN aansluiting tot op LAN access poort niveau op eindlocaties ontsluiting bieden tot systemen. Optioneel kan het VPN via een Virtual Firewall verbonden worden met andere VPN’s en met het internet. Afhankelijk van het type VPN zijn bepaalde standaardvoorzieningen mogelijk, verplicht of beperkt.

Een VPN biedt de mogelijkheid binnen een besloten en logisch gescheiden netwerk op veilige, betrouwbare wijze bedrijfsinformatie en applicaties te benaderen én informatie te delen tussen geografisch gescheiden netwerken als binnen één dedicated netwerk. Het VPN is randvoorwaardelijk om communicatie tussen eindsystemen op twee RWS locaties en tussen RWS en niet-RWS eindlocaties mogelijk te maken. Afhankelijk van het doel van het VPN dienen de in **Figuur 25** weergegeven functionaliteiten verplicht of optioneel afgenomen te worden om gebruik te maken van de diensten beschreven in de categorieën Eindsystemen, LAN aansluiting en VPN aansluiting.

VPN functionaliteiten		
Functionaliteit	**Standaard/ Verplicht/Optioneel**	**Specificatie**
Managed IP-VPN	Standaard	Any to any IP connectiviteit tussen op de RWS backbone ontsloten locaties. IP any to any routering binnen een virtueel netwerk in de RWS backbone met een door de beheerder KPN DO RWS toegewezen IPv4-adresruimte
Externe koppeling	Optioneel	In- en/of uitgaand verkeer naar aangesloten externe netwerken (Categorie VPN Aansluiting)
Internet Access met gefilterd Internet	Standaard	Veilige en gecontroleerde toegang tot het Internet voor in- en/of uitgaand internet verkeer voor interactie met partijen buiten de RWS organisatie.
Virtual Firewall	Verplicht	Beschermt de integriteit en vertrouwelijkheid van het VPN middels een firewall. De Virtual Firewall bepaalt per VPN welke communicatiestromen zijn toegestaan en blokkeert alle niet expliciet toegestane communicatie(patronen). Ieder VPN heeft een eigen Virtual Firewall
IDS/IPS	Standaard	IDS controleert het verkeer tussen VPN’s en van en naar het Internet op schadelijke aspecten en IPS blokkeert volgens ingestelde policies
Mailrelay	Optioneel b	Benodigd om e-mail te ontvangen van en versturen naar externe netwerken via smtp protocol. Mail Relay heeft daarbij verschillende beveiligingsvoorzieningen zoals controle op de reputatie van een systeem op Internet, versleuteling van email transport en inhoudelijke controle van berichten.
DNS (DDI)	Verplicht bij Internet Access	De functie DNS levert ‘name services’ aan de, binnen het VPN, aangesloten systemen op basis van het DNS protocol en voorziet in DNS name resolving van Internet systemen
DHCP (DDI)	Standaard	De functie DHCP levert een centrale voorziening om clients (en hosts) binnen het VPN op dynamische wijze van netwerkinstellingen te voorzien middels DHCP (Dynamic Host Configuration Protocol)

IPAM (DDI)	Standaard	IP Address Management geeft geautoriseerde RWS medewerkers de mogelijkheid om de IP-gerelateerde informatie vast te leggen en hier context aan te geven. Zo wordt IP-informatie beter bruikbaar als ondersteuning bij audits, kwaliteitscontrole en incidenten
Gedelegeerd beheer (DDI)	Standaard	Geeft RWS medewerkers en RWS onderaannemers de mogelijkheid om de 'IP-ruimte' waarvoor zij verantwoordelijk zijn te beheren
Remote Access	Optioneel bij Internet Access	Remote access door personen (Internet) naar RWS systemen ten behoeve van remote beheer
InterVPN communicatie	Optioneel	In- en uitgaand verkeer met een ander VPN
QoS	Optioneel	Congestiebeheersing door end to end Quality Of Service (QoS) binnen een VPN. QoS is niet overal en altijd leverbaar
NTP	Standaard	De functie NTP levert een centrale klok waarmee eindsystemen binnen het VPN hun tijd kunnen synchroniseren via het NTPv4 protocol

Figuur 25: VPN functionaliteiten

4.2.2 *Bestelbare items en levertijd*

Voor het VPN gelden de in **Figuur 26** weergegeven bestelbare items met bijbehorende standaard in werkdagen weergegeven levertijden. De levertijden voor verschillende bestelbare items lopen parallel, niet sequentieel. De dienst VPN is niet apart door afnemers te bestellen.

VPN		
Eenmalige dienst	**Toelichting**	**Levertijd**
VPN		
Aanvragen	Leveren nieuw VPN	L20
Opheffen	Opheffen VPN	L20
Wijzigen	Wijzigen instelling bestaand VPN op afstand	L10
Aanvragen VPN QOS Profiel	Realiseren QoS profiel op VPN	L20
Virtual firewall		
Aanvragen	Leveren nieuwe Firewall	L10
Opheffen	Opheffen Firewall	L10
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules	L5
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules met spoed	L1
DDI – DHCP Scope		
Aanvragen	Aanvragen DHCP scope (IP range centrale distributie)	L10
Opheffen	Opheffen DHCP scope (IP range centrale distributie)	L10
Wijzigen	Wijzigen DHCP scope (IP range centrale distributie)	L10
Aanvragen toegang	Aanvragen toegang op bestaande DHCP scope RW/RO	L10
Opheffen toegang	Verwijderen toegang op bestaande DHCP scope RW/RO	L10
DDI – DNS Domeinnaam		
Aanvragen	Leveren DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L10
Opheffen	Opheffen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L10
Wijzigen	Wijzigen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	L5
DDI – Gedelegeerd beheer		
Aanvragen	Aanvragen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
Opheffen	Opheffen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
Wijzigen	Wijzigen DNS/DHCP/IPAM gedelegeerd beheer groep	L10
DDI – IPAM		
Aanvragen	Aanvragen/opvoeren van een (nieuw) netwerk, of nieuwe eigenaren van bestaand netwerk	L10
Opheffen	Opheffen van netwerk informatie van netwerken binnen een VPN	L10
Wijzigen	Opvoeren/update van host informatie binnen een netwerk	L5
DMZ en DMZ Client		
Aanvragen	Aanvragen DMZ	L30
Opheffen	Opheffen DMZ	L10

Aanvragen Client	Aanvragen Client aansluiting	L20
Opheffen Client	Opheffen Client aansluiting	L10
Wijzigen Client	Wijzigen Client aansluiting	L5
Forward Webproxy		
Aanvragen	Aanvragen Forward Webproxy	In overleg
Opheffen	Opheffen Forward Webproxy	In overleg
Wijzigen	Wijzigen Forward Webproxy	In overleg
Mail relay[5]		
Aanvragen	Aanvragen Mail Relay	In overleg
Opheffen	Opheffen Mail Relay	In overleg
Wijzigen	Wijzigen Mail Relay	In overleg

Figuur 26: Overzicht bestelbare items Categorie VPN
*** Levertijd in werkdagen: L15 staat voor 15 werkdagen levertijd.**

4.3 Categorie VPN aansluiting

De categorie **Virtual Private Network (VPN) aansluiting** beschrijft verschillende type aansluitingen: de VPN aansluiting (middels RWS glasverbindingen of huurlijnen), de Draadloze VPN aansluiting en de VPN Aansluitingen ten behoeve van derde partijen (Externe koppeling).

4.3.1 *Functionele omschrijving*

De VPN ansluiting biedt toegang tot een VPN op een RWS- of RWS klantlocatie met gegarandeerde[6] bandbreedte en beschikbaarheid.
Dit is één veilig en betrouwbaar laag 3 netwerk waarin alle gebruikers op geografisch gescheiden locaties met elkaar kunnen samenwerken en informatie kunnen uitwisselen alsof zij op één locatie zijn aangesloten.

4.3.2 *Dienstenmatrix VPN Aansluiting*

Onderstaande matrix (**Figuur 27**) geeft een overzicht van de verschillende type bestelbare VPN aansluitingen en bijbehorende opties. In de volgende paragrafen worden deze nader toegelicht.
De per dienst afgegeven beschikbaarheid is empirisch bepaald. Dit betekent dat het technisch design zodanig is dat de afgegeven SLA gegarandeerd kan worden.
De weergegeven storingshersteltijd is gebaseerd op incidenten waarbij de dienstverlening onderbroken is (er is business impact). Wanneer er sprake is van verstoorde dienstverlening (geen business impact) geldt het SLA zoals weergegeven in **Bijlage E**.

[6] Uitsluitend voor de bedrade VPN aansluiting en afhankelijk van juiste shaping, de mobiele provider, VODK en het ON2013 contract van Rijkswaterstaat. Voor de draadloze VPN aansluiting wordt geen bandbreedte garantie afgegeven omdat de draadloze drager dit niet ondersteunt.

Dienstenmatrix VPN Aansluiting										
		Beschikbaarheid					Storingshersteltijd in 95% van de gevallen			
		Enkel	Dubbel**	Redundant	Ipsec	Ipsec MCPE	Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
		99,5%	99,8%	99,99%	99,99%	98%				
		Onbeschikbaarheid per jaar								
		ca. 1d20u	ca. 17u30m	ca. 0u52m	ca. 0u52m	ca. 7d7u	K8	K4	E8	E4
Type VPN Aansluiting	**Bandbreedte**									
Bedraad ****	**< = 10Mb** (128/256/384/512/ 640/768/896 Kbps) (1/1.25/1.5/1.75/2/3 /4/5/6/7/8/9 Mbps)	√	√	√						
	10Mb tot 1 Gb (10/20/30/40/50/60/ 70/80/90/100/ 200/300/400/500/60 0/700/800/900 Mbps)	√	√	√				√		√
	1Gb tot en met 10Gb (1/2/3/4/5/6/7/8/ 9 Gbps)	√	√	√						
Draadloos	**2G of 4G*****	√	√*							√
Externe koppeling	Geen garantie	√	√	√	√	√				

Figuur 27: VPN aansluiting

* Beschikbaar als Ruggedized (router geschikt voor ongeconditioneerde ruimtes)

**Deze variant wordt zeer beperkt ingezet. Indien het niet mogelijk is dubbel te ontsluiten, dan is het mogelijk de enkele variant dubbel uit te voeren middels een mobiele back up. Voor de mobiele back up is beschikbaarheid niet gegarandeerd

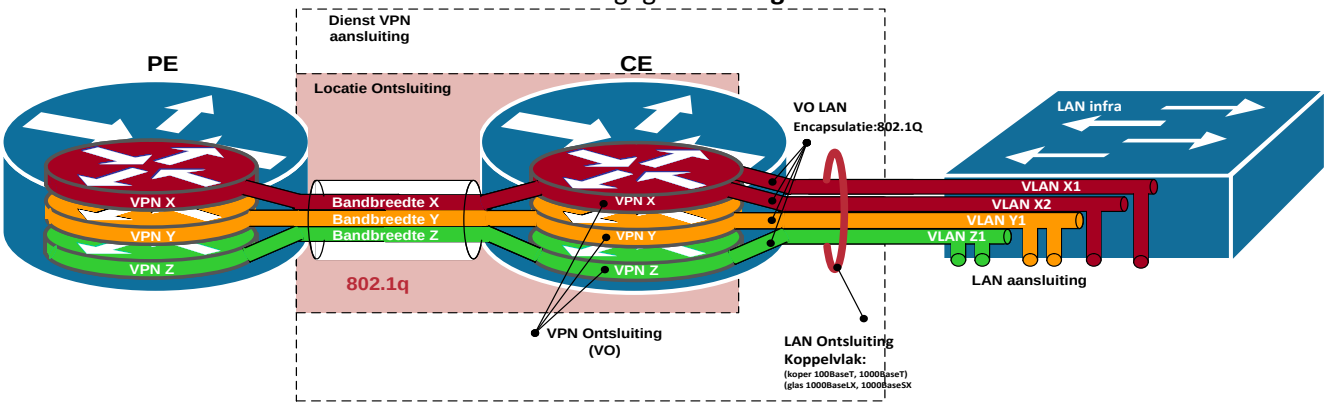
***Afhankelijk van ingezette hardware, geen bandbreedte garantie.

**** Dit betreft een bruto bandbreedte in geval van huurlijnen. De netto bandbreedte bestaat uit de bruto bandbreedte minus een eventuele tunneloverhead van max 8Kbps.

4.3.3 *Type VPN aansluiting*

4.3.3.1 *Bedraad*

De VPN aansluiting omvat de fysieke en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in **Figuur 28**.



Figuur 28: Schematische weergave van de VPN aansluiting

De VPN aansluiting dient als ontsluiting tussen de RWS backbone en de LAN infrastructuur waarop eindsystemen zijn aangesloten. Op dezelfde hardware en transmissie kunnen meerdere VPN aansluitingen geleverd worden. Deze VPN aansluitingen zijn een logisch component op de fysieke hardware.

De VPN aansluiting is de aansluiting middels fysieke transmissie (RWS glas of huurlijnen) en biedt de volgende functies en opties ten behoeve van de LAN infrastructuur op een RWS of RWS klant locatie:

- Toegang tot een bestaand VPN;
- 100MB(UTP), 1GE (UTP of Glas) of 10GE (Glas) fysiek koppelvlak naar LAN infrastructuur;
- DHCP relay functionaliteit ten behoeve van DHCP;
- Wake on LAN;
- Eén of meerdere VLAN's, met per VLAN een IPv4 gateway adres en eventueel routering.

4.3.3.1.1 Functies en opties VPN aansluiting

De verschillende functies en opties voor de VPN aansluiting zijn hieronder beschreven.

4.3.3.1.1.1 Bandbreedte

Op een Router/CE worden naast de Klant-VPN's maximaal 4 Beheer-VPN's geconfigureerd:

- Ten behoeve van de Router [CE:MGT]
- Ten behoeve van KA LAN Switch(es) [LAN:MGT]
- Ten behoeve van Overige LAN Switch(es) [EXT:MGT]
- Ten behoeve van MiniFEP [HWN:MFEP-MGT]

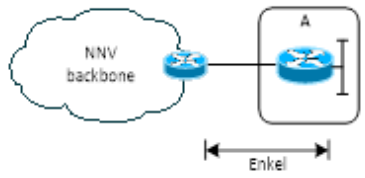
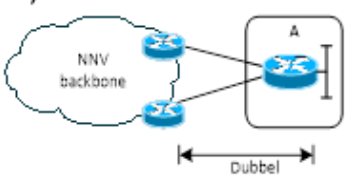
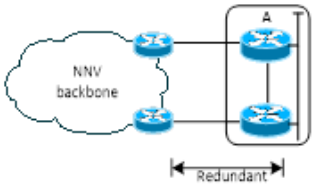
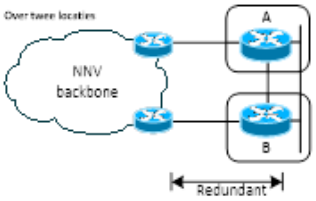
De bandbreedte voor een Beheer-VPN is afhankelijk van de bandbreedte van de VPN Ontsluiting:

- 128Kb voor 2Mb en 10Mb
- 1Mb voor 100Mb
- 10Mb voor 500Mb, 1Gb en 10Gb

De bandbreedte optie komt daadwerkelijk overeen met de geconfigureerde bandbreedte (in geval dat shaping mogelijk is).
Er wordt niet overboekt. Dat betekent dat de optelsom van de Klant-VPN's en Beheer-VPN's bandbreedtes samen kleiner of gelijk aan de bandbreedte van de VPN ontsluiting moet zijn (geldig voor zowel RWS Glas als ontsluiting middels huurlijn).

4.3.3.1.1.2 Beschikbaarheid

De VPN Aansluiting heeft vier beschikbaarheidsopties waarvan er drie zijn weergegeven in **Figuur 29**. De beschikbaarheid op locatie wordt bepaald door de VPN Aansluiting met de hoogste beschikbaarheidseis. Een beschikbaarheid van 99,999% kan uitsluitend worden aangevraagd via RWS CIV IRN Infra Netwerken als maatwerk.

Beschikbaarheid VPN Aansluiting		
Enkel	**Dubbel**	**Redundant**
99,5% 	99,8% 	99,99%  99,99% 
middels één tracé ontsloten naar één backbone router.	middels geografisch gescheiden tracés ontsloten naar twee geografisch gescheiden backbone routers.	

Figuur 29: Beschikbaarheid VPN Aansluiting

4.3.3.1.1.3 DHCP relay

Middels Dynamic Host Configuration Protocol (DHCP) kunnen eindsystemen binnen een LAN segment (VLAN) dynamisch van IP adressen worden voorzien. Met de DHCP relay functie kunnen per LAN segment de hiertoe toegewezen DHCP servers worden ingesteld. Er wordt een maximum van 3 DHCP servers per LAN segment ondersteund.

4.3.3.1.1.4 WoL

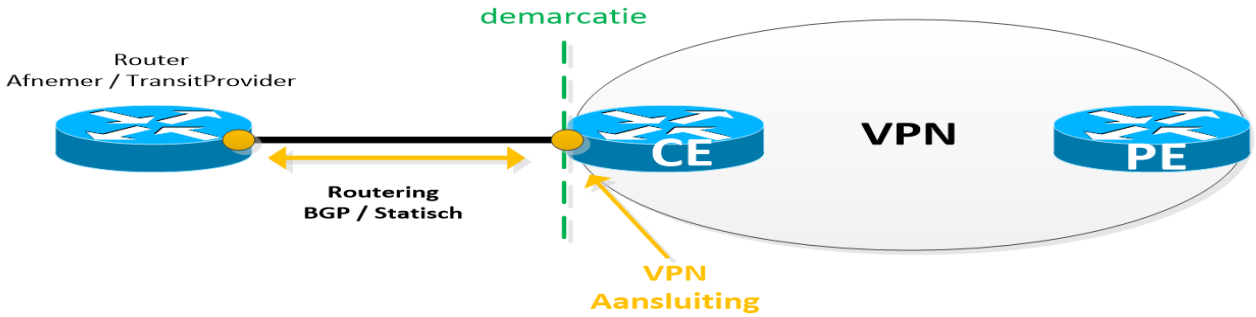
Wake on LAN (WoL) biedt de mogelijkheid netwerk devices op afstand te starten, bijvoorbeeld voor onderhouds- werkzaamheden.

4.3.3.1.1.5 Routering

Doormiddel van een LAN ontsluiting wordt een fysieke koppeling met de LAN infrastructuur tot stand gebracht. Deze wordt geleverd als een laag 3 interface. Elk LAN domein wordt op een gescheiden CE domein gekoppeld met een unieke LAN Ontsluiting.
In de dienstverlening worden vier routeringsopties onderscheiden: standaard, statisch, dynamisch type “Connect” en dynamisch type “InterConnect”. Deze worden hieronder nader toegelicht.

4.3.3.1.1.5.1 Standaard routering

Standaard wordt routering ingericht doormiddel van een VLAN-interface op de LAN aansluiting (VPN Ontsluiting LAN) zoals weergegeven in **Figuur 30**. Er kunnen meerdere VPN Ontsluiting (VO) LANs per VPN Aansluiting worden ingericht. De VPN Aansluiting is beperkt tot een enkel LAN domein.

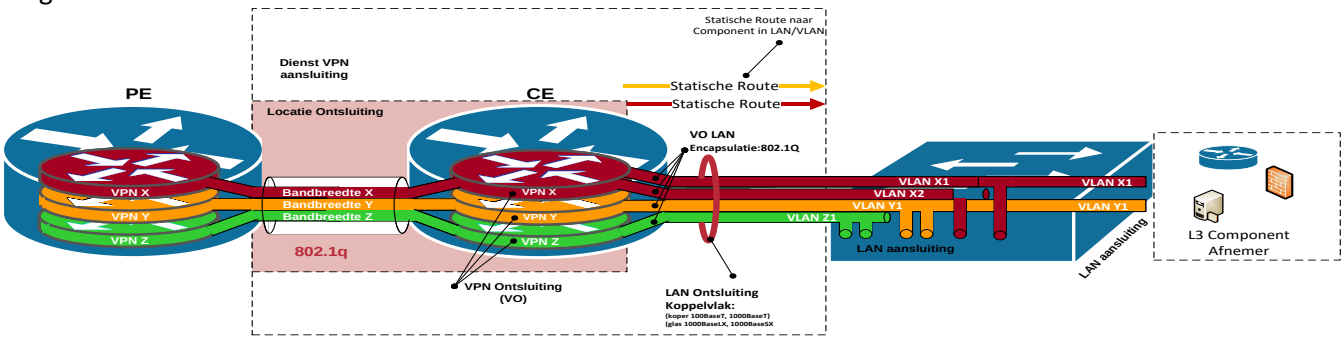


Figuur 30: Standaard routering VPN Aansluiting

Afwijkend kan routering naar een Laag 3 component op het Local Area Network (LAN) van de VPN-Aansluiting ingericht worden. Deze routering kan naar keuze statisch of dynamisch geleverd worden.

4.3.3.1.1.5.2 Statische routering

Indien gewenst is het ook mogelijk routering naar een component achter de VPN Aansluiting toe te passen doormiddel van statische routering zoals weergegeven in **Figuur 31**. Deze optie maakt het mogelijk om een component op het LAN aan te sluiten om zo een extern netwerk te kunnen benaderen. Het is niet toegestaan om tussen RWS netwerken te routeren.

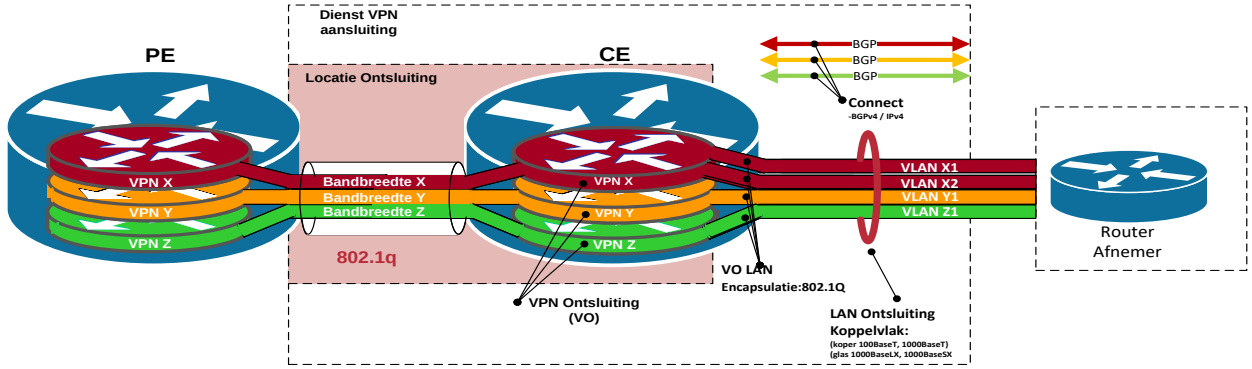


Figuur 31: Statische routering VPN Aansluiting

Voor meer informatie omtrent deze optie kan contact opgenomen worden met Service Management.

4.3.3.1.1.5.3 Dynamisch: VPN Aansluiting Connect

De VPN Aansluiting Connect, zoals weergegeven in **Figuur 32**, maakt het middels dynamische routering mogelijk netwerk-informatie uit te wisselen tussen het VPN en de afnemer. Deze optie is beschikbaar voor afnemers die geen transit-functionaliteit vervullen.



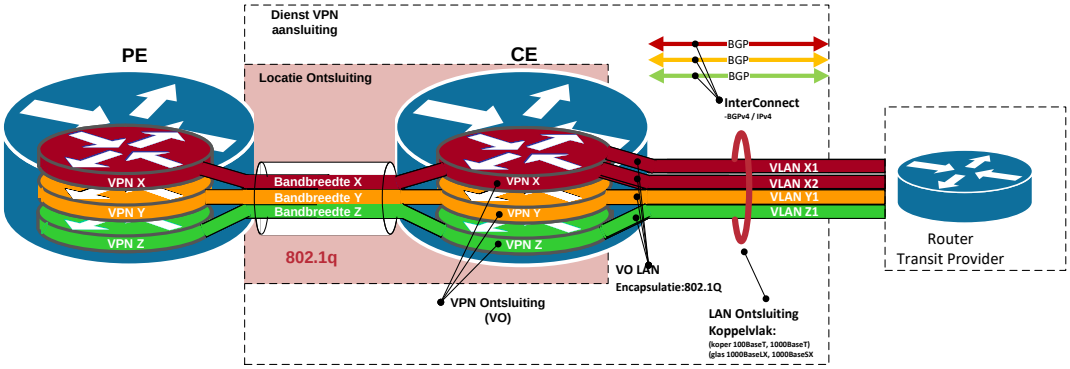
Figuur 32: Dynamische routering - VPN Aansluiting Connect

Voor een VPN-Aansluiting Connect op basis van dynamische routering zijn onderstaande uitgangspunten van toepassing:

- Klantapparatuur wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruikgemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN Aansluiting wordt één BGP-sessie toegestaan;
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De afnemer van de VPN Aansluiting dient gebruik te maken van een Publieke AS. Indien de afnemer hier niet over beschikt wijst de Service Provider van RWS CIV IRN Infra Netwerken (KPN DO RWS) een Private AS toe;
- De afnemer mag niet als ‘transit’ fungeren voor andere partijen;
- Standaard worden max. 100 IPv4 routes van de afnemer geaccepteerd. In overleg kan dit worden aangepast;
- De afnemer van de VPN Aansluiting geeft de IP-netwerken op die worden geadverteerd naar de VPN Aansluiting. De Afnemer kan een ruimer IP-subnet opgeven en daarbinnen kleinere IP-netwerken adverteren (Bijvoorbeeld 172.16.0.0/16 opgeven waarbinnen enkel 172.16.1.0/24 en 172.16.2.0/24 worden geadverteerd door de Afnemer naar RWS);
- De IP-netwerken van de afnemer moeten conformeren aan het IP-plan van het VPN;
- Multicast wordt niet ondersteund.

4.3.3.1.1.5.4 Dynamisch: VPN aansluiting InterConnect

De VPN aansluiting InterConnect, zoals weergegeven in **Figuur 33**, is een optie op de VPN aansluiting om middels dynamische routering netwerk-informatie uit te wisselen met het VPN en wordt gebruikt om het RWS netwerk te koppelen met andere transit/provider netwerken.



Figuur 33: Dynamische routering - VPN Aansluiting InterConnect

De VPN-Aansluiting InterConnect koppelt een VPN op het domein van RWS met een VPN op het domein van de transit-provider. Route uitwisseling vindt plaats middels BGPv4.

De volgende uitgangspunten zijn van toepassing:

- Apparatuur van de transit-provider wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruikgemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN aansluiting wordt één BGP-sessie toegestaan.
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De VPN-aansluiting fungeert als transitkoppeling. Het BGP AS-plan wordt in overleg afgestemd;
- Publieke BGP AS-nummers worden standaard geaccepteerd. Gebruik van Private AS-nummers
- worden vooraf afgestemd;
- Standaard worden maximaal 1000 IPv4-routes per VPN geaccepteerd vanuit de transit-provider. In overleg kan deze waarde verhoogd worden;
- De IP-netwerken die door de transit-partij worden geadverteerd maar RWS dienen aan het IP-plan van het VPN te voldoen;
- Multicast wordt niet ondersteund.

4.3.3.1.1.5.5 RKN aansluiting (Rijkswaterstaat Koppel netwerk)

Rijksoverheden en Overheden maken gebruik van verschillende Wide Area Netwerken met als doel een communicatie-infrastructuur te realiseren. Optimale samenwerking tussen alle (Rijks)overheids-partijen is cruciaal, waarbij overdracht en gebruik van informatie tussen partijen een belangrijk uitgangspunt is.

Het Rijkswaterstaat Koppel Netwerk (RKN) is aangesloten op het centrale Koppelnet Publieke Sector (KPS) en biedt en ontsluiting naar koppelnetwerken van andere (Rijks)overheidspartijen op basis van het Diginetwerk Afsprakenstelsel. Tevens biedt RKN ontsluiting naar het koppelnet van DMO RON2.0 (WAN-I, DCI, Rijksweb en DWR).

Partners van RWS kunnen met de bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) als “aangesloten overheidsorganisatie” aangesloten worden op het Rijkswaterstaat Koppel Netwerk (RKN) en transit aanvragen naar (een) andere aangesloten overheidsorganisatie(s).

De bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) is een integratie-dienst, waarbij de bouwsteen 'VPN' en de bouwsteen 'VPN aansluiting' worden samengevoegd. Alle service management communicatie (eenmalige diensten, incidenten, rapportages, capaciteitsmanagement etc.) vindt plaats o.b.v. de RKN-bouwsteen.

Nieuwe transit providers kunnen via de Service Manager worden toegevoegd op basis van RFI (conform het SPM-proces) en nieuwe transit VPN's kunnen worden aangevraagd op basis van de PDC dienst RKN.

Voor de afnemers van diensten over het RKN-netwerk wordt een VPN aansluiting Enkelvoudig gerealiseerd op één RWS ODC-locatie of een VPN Aansluiting Redundant over de RWS ODC-locaties AM2/AM3. Per afnemer wordt per RWS ODC-locatie één fysieke interface beschikbaar gesteld welke meerdere logische VPN-aansluitingen kan leveren.

De oplossing voorziet in statische of dynamische routering aan de kant van de afnemers. De verantwoordelijkheid van KPN DO RWS eindigt op de patchpanelen waarop de apparatuur van RWS is afgewerkt.

Service Levels
Beschikbaarheid:
Beschikbaarheid van een enkelvoudige RKN-aansluiting: > 99,5% op jaarbasis.
Beschikbaarheid van een redundante RKN-aansluiting: >99,99% op jaarbasis
Storingshersteltijden:
Onderbroken: E4 => Service window 7x24 met hersteltijd 4 uur
Verstoord (geen business impact): K8 => Service window 5x8 met hersteltijd 8 uur (o.b.v. service level VPN)

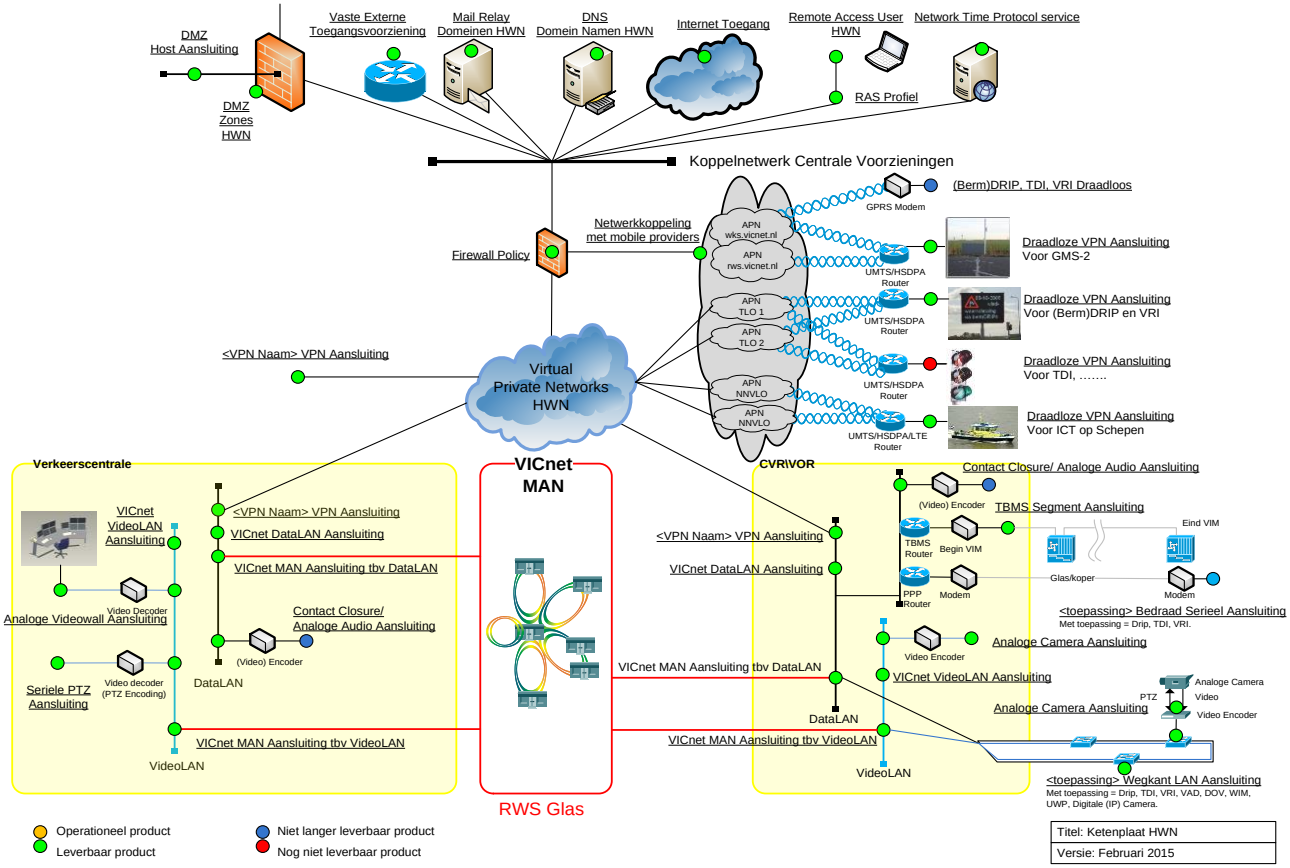
Leveringen
De volgende eenmalige diensten worden onderkend:
- "Aanvraag RKN" (van toepassing wanneer hardware geleverd moet worden of op een nieuw VPN moet worden aangesloten) – 90 werkdagen
- ''Activeren RKN" (activeren extra VPN aansluiting op afstand) – 5 werkdagen
- "Wijziging RKN" (wijzigen instelling bestaande VPN aansluiting op afstand) – 5 werkdagen
- "Deactiveren RKN" (deactiveren VPN aansluiting op afstand) – 5 werkdagen
- "Opheffen RKN" (van toepassing wanneer hardware gede-installeerd moet worden of wanneer door opzegging van de laatste aansluiting tevens een VPN moet worden gedeactiveerd – 10 werkdagen

Eenmalige- en periodieke kosten voor de bouwsteen "RKN" worden gebaseerd op de tarieven in het actuele prijzenblad en bij RWS CIV in rekening gebracht. Deze kosten bestaan uit:
- Kosten voor het generieke deel van de RKN-dienst
- Kosten voor de onderliggende bouwstenen

Maandelijkse rapportage op incident, problem, availability, capacity en changes per deelnemer per koppeling aan de SLM van RWS. Naast een klantrapportage wordt ook een totaalrapportage op de interface aan de providerkant voor capacity management geleverd.

4.3.3.2 *Draadloze VPN aansluiting*

De draadloze VPN aansluiting is de mobiele en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in **Figuur 34** en is inzetbaar om zowel locaties als apparaten aan te sluiten. De aansluiting bestaat uit een draadloze router voorzien van mobiele SIM-kaart(en).



Figuur 34: Schematische weergave draadloze VPN Aansluiting

De Draadloze VPN aansluiting biedt dezelfde functionaliteiten als de VPN aansluiting zoals beschreven in bovenstaande paragraaf met afwijkende beschikbaarheid. De Draadloze VPN aansluiting is niet geschikt voor missiekritieke systemen. Door het gebruik van publieke draadloze infrastructuur kan niet aan BIV- normen worden voldaan. Bovendien is gebruik van Multicast niet toegestaan.

Aanvullend gelden de volgende functionaliteiten:

- Transmissie 2G/4G (op schepen wordt geen gebruik gemaakt van 2G transmissie);
- Single SIM voor standaard beschikbaarheid (legacy, niet bestelbaar) of Dualprovider/ Dual SIM voor hogere beschikbaarheid;
- In ongeconditioneerde omgevingen wordt een Ruggedized router geleverd. Langs de weg kant is dit verplicht.

De dienst kent de volgende eigenschappen:

- Simkaarten worden altijd meegeleverd met de beheerde router, andere Simkaarten mogen niet gebruikt worden;
- Afhankelijk van de dekkingsgraad van mobiel zijn er verschillende antenne opties beschikbaar;
- Afnemer kan er voor kiezen de installatie door de RWS aannemer te laten uitvoeren;

- Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften die beschikbaar zijn op de VPR.

4.3.3.3 *Externe koppeling*

De bouwsteen Externe Koppeling maakt het mogelijk om een niet-RWS-netwerk op een vaste locatie veilig permanent te koppelen met het RWS-netwerk. Hiermee is permanente beveiligde transparante netwerkcommunicatie mogelijk.

Toepassingen hiervoor zijn bijvoorbeeld machine-to-machine communicatie zoals beheersystemen van derde partijen die directe en transparante koppeling tot de door hen beheerde systemen op het RWS-netwerk nodig hebben.

Afhankelijk van de gebruikte transporttechnologie en al dan niet toegepaste redundantie kunnen er SLA's gegeven worden op de beschikbaarheid van en bandbreedte voor deze communicatie.

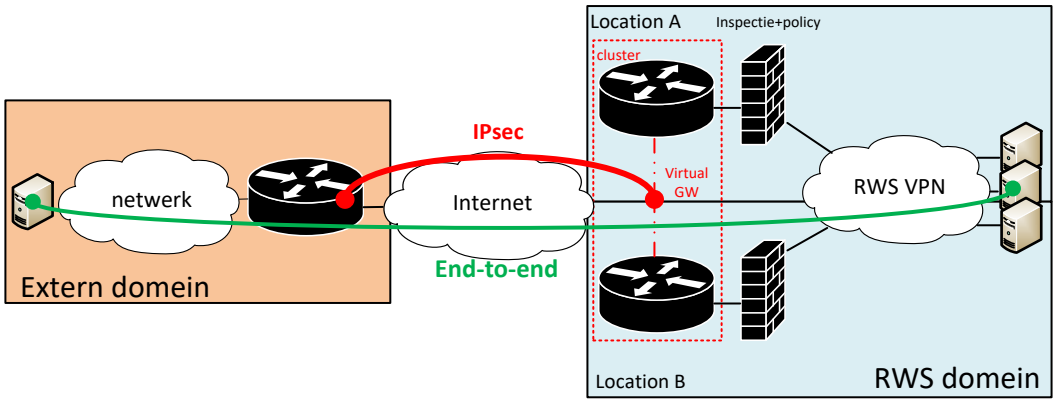
De Externe Koppeling maakt het mogelijk om via een (un)trusted netwerk (bv internet) veilig een niet RWS locatie te ontsluiten naar het RWS netwerk. De vertrouwelijkheid en integriteit van de data wordt gewaarborgd door gebruik te maken van een overlay techniek op basis van IPsec waarin de data versleuteld verstuurd wordt tussen RWS en de aangesloten partij. Er kan ook gekozen worden om een externe koppeling te realiseren via een vaste VPN aansluiting die wordt gekoppeld aan het RWS netwerk.

De externe partij kan er voor kiezen eigen apparatuur in te zetten die logisch wordt aangesloten op het RWS netwerk. Deze partij zal zich wel moeten conformeren aan de interfaces (Zie hfst 3) gesteld vanuit DO RWS, hierbij moet gedacht worden aan de communicatie protocollen en encryptie standaarden om de data veilig te kunnen transporteren. Deze interfaces kunnen van tijd tot tijd worden aangepast als er bv nieuwe standaarden zijn voor de gebruikte encryptiemethoden. Van de aangesloten partij mag worden verwacht dat deze mee gaat met deze nieuwe voorwaarden.

Op dit moment worden er drie opties geboden voor het leveren van een externe verbinding:

IPSEC zonder managed CPE

IPSEC zonder managed CPE is weergegeven in **Figuur 35** en redundant opgebouwd aan de RWS zijde waarbij de apparatuur over twee geografisch gescheiden locaties een cluster vormt. Op deze omgeving worden alleen nog de marktconforme veilige encryptie standaarden gebruikt. Er wordt gebruik gemaakt van een virtual IP adres voor de VPN gateway. Hierdoor is de perceptie van de afnemer dat er slechts één component staat.

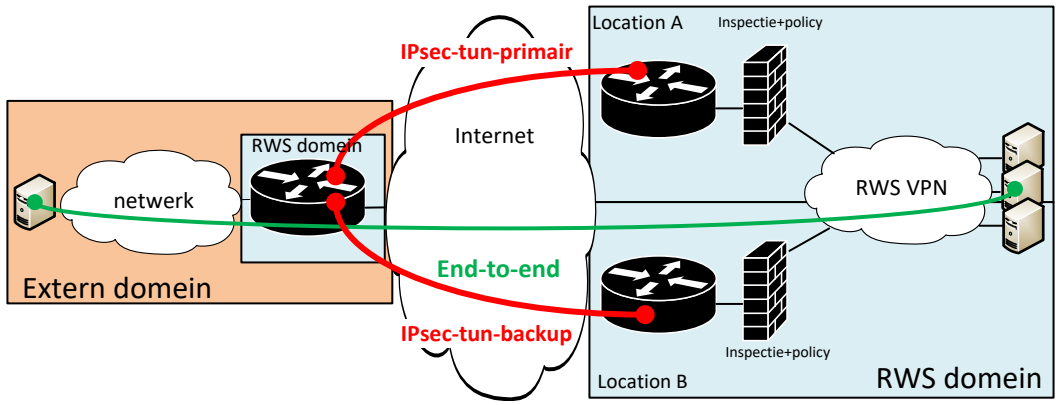


Figuur 35 - IPsec

IPSEC met managed CPE (MCPE)

Bij deze optie, weergegeven in **Figuur 36**, wordt het internet gebruikt als transportmedium tussen het RWS netwerk en de externe partij. De externe partij dient zorg te dragen voor een werkende internet verbinding en een computerruimte waarin de apparatuur geïnstalleerd kan worden. Op locatie van de externe partij wordt een beheerd netwerk device geplaatst vanuit KPN DO RWS. KPN DO RWS draagt zorg voor het opzetten van de veilige logische verbinding waarin het dataverkeer versleuteld wordt. Deze wordt aan de RWS-zijde redundant ontsloten over twee geografisch gescheiden locaties. KPN DO RWS monitort actief de CPE die bij de externe partij staat.

Voordelen	Nadelen
• Flexibel • Veilig • Relatief snel te leveren • Alleen een transparante internet verbinding nodig. • DO RWS zorgt voor een werkende end-to-end verbinding.	• End-to-end geen SLA af te geven • Geen bandbreedte garantie • Standaard alleen leverbaar binnen NL

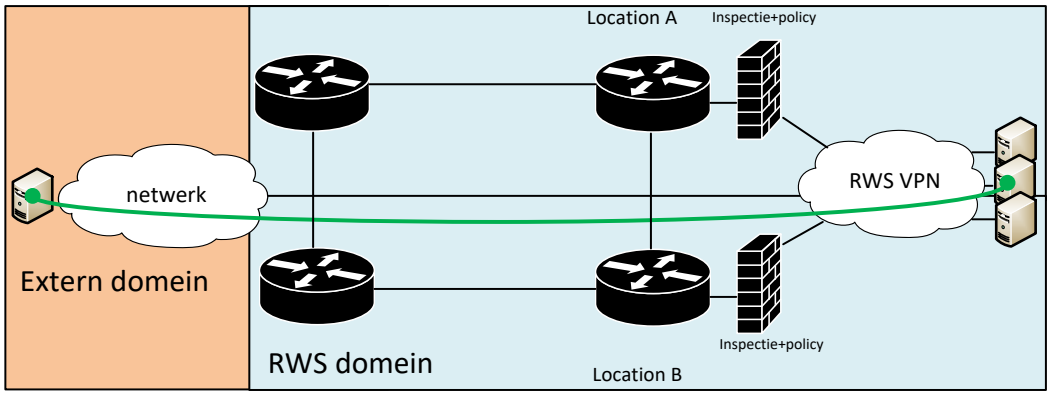


Figuur 36 - IPsec + MCPE

Vaste verbinding

Bij deze optie, weergegeven in **Figuur 37**, wordt een vaste verbinding ingezet vanuit de bouwsteen 'VPN aansluiting'. De VPN aansluiting zal op een veilige manier worden aangesloten op het RWS netwerk. De verbinding t/m de locatie van de afnemer valt onder de verantwoordelijkheid van DO RWS.

Voordelen	Nadelen
• Veilig • End-to-end SLA (zie SLA VPN aansluiting) • Diverse beschikbaarheid opties (zie VPN aansluiting) • Bandbreedte garantie	• Langere levertijd • Standaard alleen leverbaar binnen NL • Extra VPN + VPN Firewall nodig



Figuur 37 - Voorbeeld redundante vaste verbinding, zie voor meer opties 'VPN Aansluiting bouwsteen'

De dienst kent de volgende eigenschappen en uitgangspunten:

- Voor vaste externe toegangsvoorzieningen die geen SLA's vereisen wat betreft beschikbaarheid en bandbreedte, kan er gekozen worden om te koppelen via het internet en IPsec. De randvoorwaarde hiervoor is dat de niet-RWS-locatie beschikt over een eigen internetvoorziening met voldoende beschikbare netwerk capaciteit voor de beoogde communicatie.
- Apparatuur die op locatie bij een derde partij wordt geplaatst, dient te worden geplaatst in een ruimte die voldoet aan de eisen, beschreven in de NNV aansluitvoorwaarden.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[7] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)[8] .
- De systeem eigenaar/ product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang.
- De dienst is alleen voor I&M-onderdelen of externe partners die een contract afgesloten hebben met I&M. Voor het gebruik van de externe koppeling dienen externe partners te voldoen aan de "RWS-voorwaarden Externe koppelingen".
- De klant conformeert zich bij afname van deze dienst expliciet aan het beveiligingsbeleid van Rijkswaterstaat.
- Iedere vaste externe toegangsvoorziening met een derde partij dient een benoemde functioneel beheerder te hebben.
- Vaste externe toegangsvoorzieningen worden bij voorkeur via het internet gerealiseerd via de standaard-beveiligingsfaciliteiten van NNV met gebruik maken van IPsec VPN-technologie.
- De vaste externe toegangsvoorziening voldoet aan de baseline beveiliging BIR2017.
- De vaste externe toegangsvoorziening ondersteunt alleen IPv4 unicast.
- Er kan alleen gebruik worden gemaakt van publieke adressen voor de communicatie tussen de externe partij en RWS.
- Routering tussen de externe partij en DO RWS is op basis van statische routes.

Bij het aanvragen of wijzigen van een vaste externe toegangsvoorziening voor een derde partij dient het "RWS Netwerktoegang voor Derden" proces gevolgd te worden. Dit proces kan opgestart worden door het invullen en bij de Corporate Servicedesk indienen van het "Aanvraagformulier Netwerktoegang voor Derden."

[7] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

[8] Voor een common criteria beoordeling moet een bewuste keuze worden gedaan voor een EAL-niveau en een protection profile dat voldoende is voor de toepassing.

4.3.4 *Bestelbare items en levertijd*

Voor de VPN aansluiting gelden de in **Tabel 38** weergegeven bestelbare items en bijbehorende levertijden.

VPN Aansluiting		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Bedraad		
Aanvragen	Leveren 1e VPN aansluiting (levering en installatie verbinding + apparatuur).	L90
Opheffen	Opheffen laatste VPN aansluiting (opheffen verbinding + verwijderen apparatuur).	L10
Activeren	Activeren nieuwe VPN aansluiting (op afstand) op bestaand apparaat waar al tenminste één andere VPN aansluiting is aangesloten.	L5
Deactiveren	Deactiveren VPN aansluiting (op afstand) waarna er nog minstens één VPN aansluiting op het apparaat overblijft.	L5
Wijzigen	Wijzigen optie instelling(en) bestaande VPN aansluiting (op afstand)	L5
Migreren	Wijzigen diensten/hardware VPN aansluiting(en)	L90
Verhuizen	Verhuizen diensten/hardware per apparaat	L30
Aanvragen back-up Mobiel	Leveren back-up Mobiel	L20
Opheffen back-up Mobiel	Opheffen back-up Mobiel	L10
Wijzigen back-up Mobiel	Wijzigen instelling bestaande back-up Mobiel op afstand	L5
Verhuizen back-up Mobiel	Verhuizen dienst/hardware back-up Mobiel op afstand	L30
VPN Aansluiting Connect en Inter connect		
Activeren - LO Enkelvoudig (99,5%)	Activeren extra VPN aansluiting op afstand	In overleg
Activeren - LO Redundant (99,99%)	Activeren extra VPN aansluiting op afstand	In overleg
Deactiveren	Deactiveren extra VPN aansluiting op afstand	In overleg
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	In overleg
Migreren	Wijzigen diensten/hardware VPN aansluiting(en)	In overleg
Draadloos		
Aanvragen	Leveren 1e VPN aansluiting op apparaat (met en zonder installatie)	L90
Opheffen	Opheffen draadloze VPN-aansluiting (met en zonder installatie)	L90
Wijzigen	Wijzigen configuratie	L5
Activeren	Activeren extra VPN aansluiting op afstand	L5
Deactiveren	Deactiveren extra VPN aansluiting op afstand	L5
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	L10
Migreren	Wijzigen diensten/hardware VPN aansluiting(en) (met en zonder installatie)	L90
Verhuizen	Verhuizen diensten/hardware per apparaat (met en zonder installatie)	L30
Aanvragen Dekkingsmeting Mobiel	Leveren dekkingsmeting mobiele ontvangst inclusief rapport	L5
Externe Koppeling		
Aanvragen IPsec	Leveren IPsec verbinding	L10
Opheffen IPsec	Opheffen IPsec verbinding	L10
Wijzigen IPsec	Wijzigen IPsec verbinding	L5
Aanvragen MCPE	Leveren Managed CPE met apparaat Aanvragen beheerde router Verplicht bij externe koppeling op basis van vaste verbinding, optioneel bij IPSEC	L90
Opheffen MCPE	Opheffen verbinding met en het opruimen van beheerde router	L20
Wijzigen MCPE	Het aanbrengen van wijzigingen in de routering in de MCPE(s)	L10
Aanvragen vaste verbinding	Aanvragen ON2013 verbinding (i.c.m. MCPE)	L90
Opheffen vaste verbinding	Opheffen ON2013 verbinding (i.c.m. MCPE)	L10

Tabel 38: Bestelbare items VPN Aansluiting

4.4 Categorie LAN aansluiting

Een LAN aansluiting maakt het mogelijk om op RWS locaties connecties te maken over het netwerk. De categorie **Local Area Network (LAN) aansluiting** omvat de verschillende type LAN aansluitingen voor Kantoor Automatisering-LAN (KA-LAN), WIFI 3.0, Centrale VicNet Ruimte (CVR) en VicNet Object Ruimte (VOR), Overheid Data Center (ODC), Wegkant/Waterkant systemen, Gebouwen en de Verkeerscentrale (VC).

4.4.1 *Functionele omschrijving*

De dienst LAN aansluiting biedt toegang tot een virtueel netwerk via een fysieke LAN poort.

De LAN aansluiting is opgebouwd uit de volgende componenten:

LAN ontsluiting	dit is de logische koppeling naar een specifiek VPN
VLAN	dit is een virtueel LAN (VLAN) in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN aansluiting	de fysieke poort die toegang biedt naar het virtuele LAN
Ethernet infra	dit is de fysieke infrastructuur (bekabeling en switches)

Het component Ethernet infra is zo opgebouwd dat de dienst LAN aansluiting bijna overal leverbaar is. Hiervoor moet wel bekabeling aanwezig zijn, of aan te leggen zijn, tegen acceptabele kosten.
Deze dienst biedt een fysieke ethernet aansluiting voor een eindsysteem. Deze wordt op een door een VPN ontsloten locatie gerealiseerd middels een VPN aansluiting. en AAA (Authentication Authorization Accounting) eindgebruiker.

4.4.2 *Dienstenmatrix LAN aansluiting*

De categorie LAN aansluiting is opgebouwd uit verschillende type aansluitingen, elk met hun specifieke kenmerken voor wat betreft bandbreedte, beschikbaarheid en storingshersteltijd conform **Figuur 39**.
De per dienst afgegeven beschikbaarheid is empirisch bepaald. Dit betekent dat het technisch design zodanig is dat de afgegeven SLA gegarandeerd kan worden. De weergegeven storingshersteltijd is gebaseerd op incidenten waarbij de dienstverlening onderbroken is (er is business impact). Wanneer er sprake is van verstoorde dienstverlening (geen business impact) geldt het SLA zoals weergegeven in **Bijlage E**.

Dienstenmatrix LAN											
		Beschikbaarheid						Storingshersteltijd in 95% van de gevallen			
		Enkel			Redundant			Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
		99,0%	99,5%	>99,7%	>99,8%**	99,95%***	99,99%***				
		Onbeschikbaarheid per jaar									
Type LAN Aansluiting	Bandbreedte	ca 1d20u	ca 1d20u	ca. 1d2u	ca. 17u30m	ca. 4u28m	ca. 0u52m	K8	K4	E8	E4
Gebouw		√				√			√		√
Rekencentrum		√				√			√		√
SPAN		√				√			√		√
CVR/VOR	Auto (Voorkeurs instelling)		√				√				√
	10 Mbps		√				√				√
	100 Mbps		√				√				√
	1000 Mbps		√				√				√
Callcenter	<= 100 Mbps of		√			√					√
	<= 1Gbps of		√			√					√
	<= 2*1Gbps (Server)		√			√					√
Wegkant/Waterkant*	<=1Gbps			√	√						√
ODC	<= 100 Mbps		√								√
	<= 1Gbps standaard		√								√
	<= 2Gbps (Server/ Blade) redundant					√					√
	<= 4Gbps (Server/ Blade) redundant					√					√
	<= 10Gbps standaard (Server / Blade)		√								√
	<= 20Gbps (Server / Blade) redundant					√					√
	<= 40Gbps (Server / Blade) redundant					√					√
KA LAN	<= 100 Mbps of		√			√		√	√		√
	<= 1Gbps of		√			√		√	√		√
	<= 2*1Gbps (Server/ Blade)		√			√		√	√		√
Wifi*****			√					√			
OpenWifi*****		√						√			

Figuur 39: LAN aansluiting

*maximaal twee storingen per jaar per device
**indien sprake is van geografische redundantie glasvezelinfrastructuur
***over twee switches
***** radiodekking

4.4.3 *Type LAN aansluiting*

4.4.3.1 *RWS Netwerk LAN*

Onder RWS Netwerk LAN worden alle LAN aansluitingen verstaan met uitzondering van Kantoor Automatisering LAN, ODC, WIFI, OpenWIFI en LAN aansluiting type SPAN. Deze specifieke diensten met bijbehorende kenmerken zijn separaat beschreven.

Op basis van de gewenste beschikbaarheid, bandbreedte, robuustheid en functionaliteit zijn er meerdere RWS Netwerk LAN opties mogelijk.

4.4.3.1.1 LAN aansluiting type Gebouw (met uitzondering van kantoren): voor systemen met middelhoge snelheden en data throughput

Dit type LAN aansluiting wordt toegepast voor systemen (onder andere datacollectie-pc's) met middelhoge snelheden en data throughput in RWS gebouwen die geen dienst doen als kantoorlocatie, zoals Industriële Automatisering (IA's) en Object LAN's. De uitvoering is op basis van een RJ45 koppelvlak. Zowel redundantie als loadbalancing zijn niet mogelijk.

4.4.3.1.2 LAN aansluiting type Rekencentrum: voor systemen met hoge eisen aan beschikbaarheid en bandbreedte ten behoeve van Verkeerscentrales

Dit type LAN aansluiting wordt ingezet voor systemen met hoge eisen aan beschikbaarheid en bandbreedte, toegepast in Verkeerscentrales en Verkeersposten. Uitvoering is op basis van een koper (RJ45) of glas-koppelvlak. Schaalbaarheid is in dit type LAN aansluiting mogelijk.

4.4.3.1.3 LAN aansluiting type CVR / VOR: o.b.v. schaalbaarheid, robuustheid en hoge beschikbaarheid

Dit type LAN aansluiting is bedoeld om in CVR/VOR ruimten langs Rijks(water)wegen een connectie te maken met verkeersmanagementsystemen in Verkeerscentrales (VC) en het RWS Overheid Data Center (ODC). De dienst biedt de noodzakelijke LAN functionaliteit ten behoeve van het aansluiten van inwin- en besturingssystemen zoals meetsystemen, camera's, radarsystemen, noodsystemen en signaleringsystemen. Belangrijke kenmerken zijn schaalbaarheid, robuustheid en hoge beschikbaarheid. Redundantie en loadbalancing zijn niet mogelijk.

De volgende voorwaarden gelden voor dit type LAN aansluiting:

- Een geconditioneerde omgeving;
- De LAN aansluiting is uitsluitend bedoeld voor eindsystemen. Het aansluiten van netwerk apparatuur zoals routers, switches en access points op een LAN aansluiting is niet toegestaan;
- Deze dienst biedt uitsluitend ondersteuning voor TCP/IP en Ethernet. Andere protocollen zoals IPX/SPX of veldbus protocollen zoals Profinet, Modbus en SafetyNET worden niet ondersteund.
- Voor het aansluiten van digitale camera's in combinatie met een mediaconvertor kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Dit type aansluiting is alleen bedoeld voor camera's in de directe omgeving van de CVR. Voor het gebruik van RWS glasvezels moet bij de Adviseur Infrastructuur van RWS CIV toestemming worden gevraagd. Het demarcatiepunt van deze aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar de camera en eventuele media convertor zijn geen onderdeel van de dienst.

De duplex instelling van een LAN aansluiting wordt standaard ingesteld op de voorkeursinstelling (Auto) waarbij een onderhandelprotocol zorgt dat beide aangesloten apparaten dezelfde duplex instelling hebben. Hierbij wordt onderscheid gemaakt tussen Half Duplex (eenrichtingsverkeer, om en om zenden en ontvangen) en Full Duplex (tweerichtingsverkeer, tegelijk van beide kanten zenden en ontvangen mogelijk).

Indien de Auto instelling voor beide aangesloten apparaten niet naar behoren werkt kan de aansluiting in sommige gevallen op Half of Full Duplex worden ingesteld.

4.4.3.1.4 LAN aansluiting type Wegkant/Waterkant ten behoeve van ongeconditioneerde ruimtes

Deze LAN aansluiting is bedoeld om ethernet/IP gebaseerde weg- en waterkant toepassingen te koppelen op een VPN. Deze dienst wordt onder andere toegepast bij DRIPs, DOV, TDI, VRI, VAD, Weigh In Motion weegbruggen (WIM), IP-camera's, Digitale Camera aansluitingen en het UWP. Het biedt een hoge beschikbaarheid en betrouwbaarheid waarbij het mogelijk is om onderdelen eenvoudig te vervangen met behoud van functionaliteit.
Afwijkend ten opzichte van andere ethernet/IP gebaseerde LAN producten worden omwille van de relatief grote afstanden de ethernetswitches in cascade (ring-topologie) geschakeld. Standaard is de beschikbaarheid redundant (>99,8%) door een geografisch gescheiden Glasvezelring (loopt via een geheel andere [vaar]weg dan wel aan de andere zijde van de [vaar]weg retour). Indien er geen geografisch gescheiden Glasvezelring mogelijk is, maar wel een fysieke Glasvezelring, kan op verzoek van de Afnemer en met toestemming van CIV Infra deze Dienst geleverd worden met een beschikbaarheid enkelvoudig (>99,7%; loopt via de zelfde [vaar]weg of via dezelfde Glasvezelkabel retour).
Deze dienst is geschikt gemaakt voor het leveren in ongeconditioneerde ruimtes doormiddel van passieve koeling en biedt ten behoeve van de service provider KPN DO RWS remote beheerfunctionaliteit van de apparatuur voor netwerkmanagement.
In het kader van beveiliging worden niet gebruikte poorten dichtgezet, applicatiedomeinen in aparte VLAN's ondergebracht ten behoeve van de scheiding van netwerk services, switches in afgesloten kasten geplaatst, MAC Address filtering toegepast op wegkantswitches, vindt beheeradmin toegang plaats via de centrale AAA Service, is beheer van VLAN/VPN gescheiden van data VLAN's en wordt gebruik gemaakt van Detect en Disable unidirectional links.

Voor dit type LAN aansluiting geldt een aantal aanvullende voorwaarden:

- Plaatsing en montage op DIN rail, 19" rack of 'board' vereist;
- Er worden maximaal 27 switches cascade geschakeld;
- Met een 1000Base-LX interface kan een afstand worden bereikt van 10km en met de ZX variant ca 70km (conform specificaties) per switch;
- Voor het aansluiten van digitale camera's in combinatie met een mediaconvertor kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Aangesloten camera's dienen in de directe omgeving van de wegkant switch te staan. Het demarcatiepunt van deze aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar de camera en eventuele media convertor zijn geen onderdeel van de dienst.

4.4.3.2 *KA LAN en LAN aansluiting type Callcenter*

De KA LAN omgeving is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen en kan alleen worden afgenomen per switch met 24 of 48 KA LAN poorten.

KA LAN is opgebouwd uit de volgende componenten:

LAN aansluiting	Lokale LAN poort, gekoppeld in een VLAN, op de Ethernet infrastructuur
Local Area Network	Laag 2 Ethernet VLAN op de Ethernet infrastructuur
Ethernet infra	Ethernet infrastructuur in gebouwen
Network Access Control (NAC)	Netwerktoegangsbeveiliging op LAN niveau. Gebruikers krijgen pas netwerktoegang na succesvolle authenticatie.

Op basis van de grootte van de locatie en bijbehorende KA omgeving wordt onderscheid gemaakt tussen 3 type KA LAN Aansluitingen waarvan de kenmerken zijn weergegeven in **Figuur 40**. Alle locaties zijn geschikt voor één of meerdere VPN aansluitingen.

Opties type KA LAN Aansluiting												
Type locatie	**Desktop poorten**	**Server poorten**	**LAN**			**MER/SER**			**Routering**	**WAN Router**		**Bladeservers**
			10Base-T	100Base-TX	1000Base-T	Geen	Één	Meerdere		Enkelvoudig	Dubbelvoudig	
Klein	< = 24		√	√		√	√			√		
Middelgroot	√	√*	√	√	√**		√	√		√	√	
Groot	√	√	√	√	√		√	√	√		√	√

Figuur 40: Opties type KA LAN Aansluiting
*Enkele server poorten
**Beperkt aantal 1000Base-T poorten

De KA-LAN omgeving kent de volgende functies:

- Het is mogelijk meerdere VLAN's te creëren op een fysieke poort (trunking). De VLAN's dienen toe te behoren aan één VPN;
- Om de netwerkcapaciteit uit te breiden, is het mogelijk om tussen twee switches port-channeling toe te passen. Hiermee wordt de capaciteit van beide switches gecombineerd;
- Er wordt een spanning-tree protocol toegepast om problemen in het netwerk te detecteren en te voorkomen;
- Het is mogelijk om niet-routeerbare /geïsoleerde VLAN's aan te vragen. Deze VLAN's worden wel administratief gekoppeld aan een VPN Aansluiting;
- Ten behoeve van Call Center omgevingen is het mogelijk Power over Ethernet (PoE) toe te passen. Hiermee kan een aangesloten apparaat zoals een call center server, bedien PC, telefoon of Wall board via de aansluiting op de switch van stroom worden voorzien.

LAN aansluiting Type KA en LAN aansluiting type Call center
De KA LAN omgeving is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen en kan alleen worden afgenomen per switch met 24 of 48 KA LAN poorten.

4.4.3.3 *WIFI*

De dienst WIFI biedt veilige draadloze netwerktoegang op RWS locaties die zijn aangesloten op het RWS netwerk. Er worden vier gebruikersgroepen onderkend:

- RWS medewerkers met een RWS AD account en door RWS beheerde mobile devices:
  Hiermee kunnen de standaard door RWS beheerde mobiele werkplekken draadloos worden verbonden en daarbij logisch dezelfde toegang verkrijgen als via een vaste bedrade kantoor aansluiting (KA).
- Deelnemers van Govroam, zie https://govroam.nl/ voor actuele deelnemers:
  Doormiddel van de overheid brede 'Government roaming Nederland' oplossing wordt veilige internet toegang geboden voor alle overheidsmedewerkers die onderdeel zijn van het Govroam platform.
- Gastgebruikers die middels authenticatie via een tijdelijk uitgegeven gastaccount veilig toegang krijgen tot het publieke internet;
- Gastgebruikers die akkoord gaan met de algemene voorwaarden van RWS en daarmee zonder identificatie toegang krijgen tot het publieke internet op de door RWS CIV aangewezen locaties (zoals WIFI LEF).

Elke groep kent een specifieke, functioneel andere Service Set Identifier (SSID) zoals weergegeven in **Figuur 41.** Het SSID zorgt voor functiescheiding tussen de verschillende logische draadloze netwerken. SSIDs kunnen worden ingesteld per locatie of specifieke ruimte binnen een locatie. Zo kunnen er op een locatie in verschillende ruimten verschillende SSIDs actief zijn. Het aanvragen van een nieuwe functie binnen een SSID of een geheel nieuw SSID kan uitsluitend via CIV RWS IRN INFRA aangevraagd worden bij DO RWS.

Omschrijving	Functie	Identiteit bekend	SSID	VPN	Security Zone
RWS beheerd device en RWS AD account	Toegang tot interne RWS applicaties, toegang tot internet via bouwsteen Webproxy.	Ja	RWS-intern	RWS:RWS	Semi-trusted
Stichting Govroam	Toegang internet voor gastgebruikers en RWS medewerkers die gebruik maken van een BYOD	Ja	Govroam	RWS:Govroam	Untrusted
Rijkskantoorroam voor RWS-panden die tevens rijks-kantoorpand zijn	Toegang tot het bedrijfsnetwerk van de gebruiker	Ja	Rijkskantoor roam	WAN-i	Untrusted
Gastgebruikers zonder account (locatie Westraven-LEF)	Toegang publiek internet	Nee	LEF-LIVE	Live	Untrusted
Gastgebruikers zonder account / Open WiFi (overige locaties)	Toegang publiek internet	Nee	Rijkskantoor Gast		Untrusted

Figuur 41: Overzicht gebruikersgroepen WIFI en Open WIFI

De dienst WIFI voorziet in het ophangen van Access Points (AP's) op locaties waarmee gebruikers een draadloze verbinding kunnen opzetten. Deze AP's zijn verbonden met centrale controllers waarover al het verkeer loopt en welke ook onderdeel uitmaken van de dienst. Op deze manier is geborgd dat alle verkeersstromen binnen het RWS netwerk blijven.

Voor het inrichten van een nieuwe locatie en/of een nieuw gedeelte van een bestaande locatie wordt een dekkingsmeting uitgevoerd om zo te bepalen hoeveel AP's er geplaatst dienen te worden en waar om zo een optimale WIFI dekking te realiseren. Dit is een momentopname, interne verhuizingen kunnen de dekking beïnvloeden. De plaatsing van AP's wordt altijd afgestemd met de gebouwbeheerder.

4.4.3.3.1 Uitgangspunten

Voor WIFI gelden de volgende uitgangspunten:

- WIFI is niet bedoeld voor missiekritieke applicaties!
- WIFI wordt uitsluitend geboden op RWS locaties voorzien van minimaal een vaste VPN aansluiting, aangevuld met een "LAN- of KA-LAN aansluiting";
- Voor het inrichten van WIFI op nieuwe locaties is de afname van een nieuwe VPN aansluiting ten behoeve van het WIFI verkeer vereist;
- De 99,5% beschikbaarheid heeft betrekking op de aanwezige radiodekking op een locatie of in een ruimte. De implementatie van AP's zorgt er voor dat bij uitval van een enkel AP de radiodekking gegarandeerd blijft. Uitval van een enkel AP zal niet tot connectiviteitsverlies leiden, wel zal de

beschikbare bandbreedte tijdelijk afnemen. In overleg met RWS kan worden besloten om de AP's te positioneren met een hogere dichtheid zodat uitval van één of meerdere AP's nagenoeg geen invloed heeft op de eindgebruikerservaring. Dit zal tijdens de inrichting van de locatie worden bepaald met de aanvrager. Verder zal de beschikbaarheid van het AP afhankelijk zijn van 'KA LAN' of de 'LAN aansluiting' waarop het AP fysiek aangesloten wordt;

- Deze dienst is bedoeld voor Data toepassingen. Andere toepassingen zoals spraak en locatie services worden (nog) niet ondersteund;
- Wijzigingen in de omgeving, bijvoorbeeld het plaatsen van wanden of een toename in medewerkers kunnen van invloed zijn op de prestaties van het draadloze netwerk;
- Minimale connectiesnelheid van een client is 12Mbps, lagere snelheden worden niet ondersteund;
- Per AP radio worden maximaal 200 clients ondersteund maar 75 clients wordt als "gezond" gezien;
- WIFI toegang is centraal geregeld via de netwerk dienst AAA;
- De WIFI dienst biedt een veilige, versleutelde verbinding met het netwerk. Om het netwerk te beschermen tegen negatieve externe factoren zijn de volgende veiligheidsmaatregelen genomen:
    - Niet erkende AP detectie: Er worden uitsluitend AP's toegestaan die onder controle staan van KPN DO RWS. Niet erkende AP's worden gedetecteerd en gerapporteerd richting RWS/SOC. Hierbij worden locatie, MAC adres en uitgezonden SSID vermeld.
    - Rapporteren MAC Flooding aanval: Iedere client heeft een eigen uniek MAC adres ID. Aanvallers maken gebruik van speciale systemen die zich voor kunnen doen als honderden clients door het op illegale manier genereren van heel veel MAC adressen. Door zo'n aanval kan het AP "vol" raken waarna er geen nieuwe clients meer worden geaccepteerd. Dit kan niet voorkomen worden. Wel wordt er bij een vermoedelijke MAC Flooding aanval gerapporteerd aan RWS SOC.
    - Ongeoorloofd hergebruik Account: Het is niet toegestaan om een account te delen met andere gebruikers. Om te voorkomen dat dit toch gebeurt, voorziet de dienst erin dat er maximaal twee (2) gelijktijdige inlog sessies mogen zijn per account. Er is voor twee inlog sessies gekozen zodat een gebruiker eventueel een mobiel device en laptop tegelijk kan gebruiken. Het maximaal aantal sessies kan per SSID worden aangepast.
- RWS CIV IRN Infra Netwerken voorziet in de aanlevering van tekeningen/plattegronden van de locaties aan KPN DO RWS en informeert KPN DO RWS tijdig bij wijzigingen in gebruik van locaties zoals verhuizingen e.d. in verband met dekking van het radio spectrum;
- RWS zorgt voor interne bekabeling en stroomvoorziening.

Capaciteitsmanagement is onderdeel van de dienst en bestaat uit het monitoren van de belasting van AP's door KPN DO RWS. Indien een radio van een AP gedurende een periode van vijf werkdagen tijdens kantoortijd gemiddeld meer dan 75 clients bedient, wordt een onderzoek gestart. Op basis van dit onderzoek wordt besloten of er aanpassingen doorgevoerd moeten worden in de configuratie van de radiodekking of dat uitbreiding van het aantal AP's op die locatie/ruimte de oplossing biedt. Deze acties worden vanuit de dienst gerealiseerd.

4.4.3.3.2 Randvoorwaarden

De volgende randvoorwaarden zijn van toepassing:

- Voor het leveren van WIFI is een door RWS CIV IRN Infra Netwerken geleverde en door DO RWS beheerde LAN omgeving in het pand vereist, welke is aangesloten op het RWS netwerk via een vaste VPN aansluiting;
- Afhankelijk van de SSID's die nodig zijn op een locatie zal/zullen ook één of meer van de volgende VPN's **aanwezig moeten zijn: RWS:RWS bij RWS-Intern, RWS:GOVROAM bij Govroam en/of WAN-i voor** Rijkskantoorgast.
- Verkregen gebouwplattegronden die gebruikt worden voor site survey's en voor intekening van dekkingsmetingen dienen door alle betrokken partijen vertrouwelijk te worden behandeld;

- Bij toepassing van PoE+ voor WIFI dient de bekabeling te voldoen aan minimaal CAT5E of CAT6 ten behoeve van het aansluiten van Access Points;
- Bij uitbreiding van het aantal Access Points op basis van capacity management dient rekening te worden gehouden met de aanwezigheid van juiste bekabeling (zie boven) en stroomvoorziening. De gebouwenbeheerder is hier verantwoordelijk voor;
- WIFI is afhankelijk van de dienst die de LAN functionaliteit levert. Deze LAN functionaliteit is geen onderdeel van de dienst Wi-Fi. Het aansluiten van een AP vereist een 1Gbps LAN Aansluiting.

4.4.3.3.3 Opties

Voor WIFI gelden de volgende opties:

- **Site Survey en Dekkingsmeting (verplicht bij nieuwe locatie)**
  Voor elke nieuwe levering, op een nieuwe locatie of in een nieuwe ruimte, wordt een site survey en een dekkingsmeting uitgevoerd.
  - De site survey levert gegevens over de fysieke omgeving en benodigde aanpassingen om AP's te kunnen plaatsen (stroomvoorziening, LAN Aansluitingen en bekabeling etc.).

De dekkingsmeting bepaalt het aantal AP's, de te gebruiken radio's (intern/extern) en de plaatsing van de radio's aan de hand van de gewenste capaciteit en gewenste toepassingen. In overleg met de afnemer wordt voor het uitvoeren van de dekkingsmeting besproken wat de gewenste capaciteit (aantal gebruikers) per ruimte/vloer is.

4.4.3.4 *Open WIFI*

Open WIFI Is een optionele dienst onder WIFI die open internet toegang biedt zonder identificatie voor alle gebruikers op de gekozen locatie. Open WIFI kan voor twee doeleinden worden ingezet:

- Voor gastgebruikers zonder een tijdelijk account, die akkoord gaan met de algemene voorwaarden die in de vorm van een disclaimer aan hen wordt voorgelegd. Toegang alleen naar publiek internet op de door RWS aangewezen locaties. Hierbij wordt onderscheid gemaakt tussen Westraven LEF en Open WIFI op andere RWS-locaties;

- Open WIFI maakt het ook mogelijk om apparatuur zonder webbrowser (bv. informatiezuilen) met internet te verbinden. Dit vindt plaats o.b.v. het MAC-adres van deze apparatuur. Activatie van een MAC-adres is niet locatie-gebonden. Als Open WIFI voor een locatie wordt opgeheven, dan moeten de MAC-adressen voor deze locatie apart worden verwijderd.

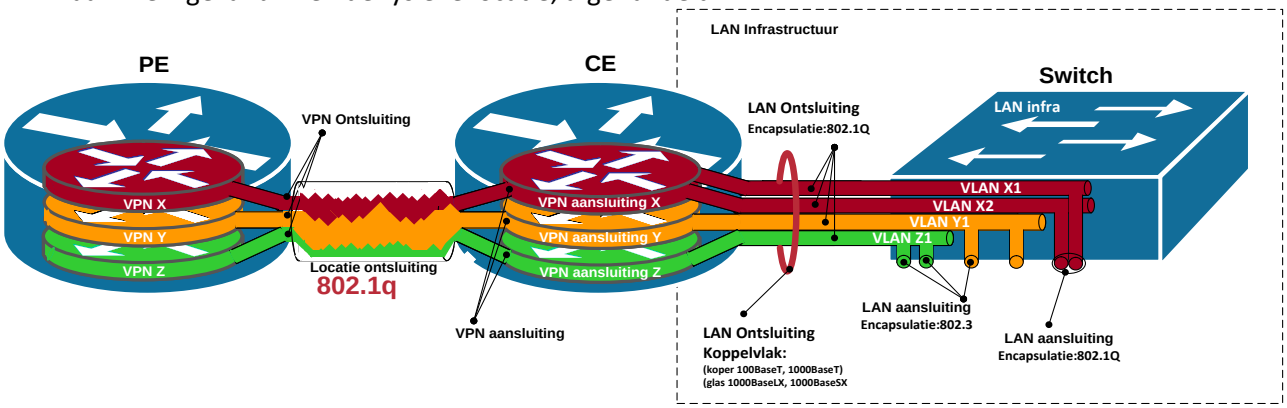
- Open WIFI is alleen mogelijk op locaties met NNV connectiviteit en waar al WIFI dienstverlening aanwezig is. De dienst kan worden aangevraagd voor de hele locatie (default) of een deel ervan (incidenteel). Het is ook mogelijk om de dienst voor een beperkte periode, met een begin- en einddatum, aan te vragen, om bijvoorbeeld een tijdelijke behoefte i.v.m. een event te kunnen invullen. Gerelateerd daaraan is het ook mogelijk om de standaard SSID (WIFI-naam) ''RijkskantoorGast'' locatie specifiek aan te passen zodat de WIFI-naam herkenbaar is voor de gastgebruikers die aan dat event deelnemen.

- De totale Open WIFI-dienstverlening is gedimensioneerd (niet gelimiteerd) op max. 1.000 gelijktijdig operationele devices. Bij overschrijding van dit aantal vervallen de beschikbaarheidsgaranties.

4.4.3.5 *LAN Aansluiting type ODC (Uitsluitend bestelbaar via RWS CIV IRN Infra Netwerken)*

Het type LAN aansluiting ODC, weergegeven in **Figuur 42**, is ontwikkeld ten behoeve van de productieomgeving voor systemen met hoge eisen aan beschikbaarheid en bandbreedte zoals in het Overheid datacenter. Dit type LAN Aansluiting heeft de volgende kenmerken:

- Fysiek koppelvlak 100Base / 1000Base / 10GBase, inclusief bekabeling naar het patchpaneel op locatie;
- Gestandaardiseerd ethernet/IP gebaseerd datatransmissienetwerk voor Unicast & Multicast verkeer (inclusief IGMPv2/ IGMP snooping);
- Scheiding van applicatiedomeinen met behulp van VLAN's;
- Bij LAN ontsluiting is inter-VLAN routering toegestaan voor RWS CIV IRN Infra Netwerken, mits deze tot hetzelfde VPN behoren;
- Als onderdeel van een tactische change is het mogelijk om niet-routeerbare / geïsoleerde VLAN's aan te vragen. Tactische aanvragen zijn aanvragen waarvoor de afnemer contact op dient te nemen met de Relatie Manager van RWS CIV IRN Infra Netwerken. De Relatie Manager bepaalt of de aanvraag al dan niet in behandeling wordt genomen;
- De aansluiting is uitsluitend bedoeld voor eindsystemen. Aan de Edge wordt detectie van Spanning-tree toegepast om een loop-free topologie te waarborgen;
- Trunking (802.1Q) uitsluitend naar servers en Blade servers;
- VLAN's binnen een trunk naar een server of Blade server behoren aan uitsluitend één VPN. Hiervan kan afgeweken worden indien de scheiding tussen de VPN's gewaarborgd kan worden.[9] Koppelingen tussen de VPN's mogen uitsluitend via een firewall policy in de Centrale voorzieningen worden gerealiseerd;
- Bieden van LAN aansluiting redundant door interface bundeling (Etherchannel) via redundante switches t.b.v. servers en Blade servers;
- Alle Virtuele LANs worden gestretched over de ODC locaties AM2 en AM3 (via E-services Hub). Alle IP reeksen van de Virtuele LANs zijn via beide WAN uplinks benaderbaar (primair / back-up). Middels de dienstbouwsteen VPN-aansluiting wordt een primaire locatie aangegeven. De primaire locatie is de locatie waarnaartoe het verkeer gerouteerd zal worden als beide locaties beschikbaar zijn. De andere locatie wordt automatisch als back-up-locatie aangemerkt;
- Inter-VLAN verkeer tussen servers binnen een fysieke ODC locatie wordt zo dicht mogelijk bij de server, maar in elk geval binnen de fysieke locatie, afgehandeld.



Figuur 42: LAN infrastructuur ODC

[9] Dit kan bijvoorbeeld gerealiseerd worden door virtuele switches in de aangesloten hypervisor.

4.4.3.6 *LAN aansluiting type SPAN (uitsluitend te bestellen door RWS SOC)*

Dit type LAN aansluiting maakt het mogelijk dat er een kopie van het lokale netwerkverkeer aan de RWS Cyber Security Logging en Monitoring (CSLM) keten kan worden geleverd. De SPAN poort wordt gerealiseerd op een laag-2 omgeving óf op basis van poort óf op basis van VLAN (max. 50 VLANs per poort). Management poorten en stack poorten komen niet in aanmerking voor de (R)SPAN-functionaliteit. Het gekopieerde verkeer kan worden verstuurd naar een of meerdere (max. 4 indien technisch mogelijk) poort(en) op dezelfde switch (SPAN) of naar een remote VLAN (RSPAN). Poort channels kunnen wel als source maar niet als destination worden ingezet, waarbij tevens de bandbreedte toereikend moet zijn. By default wordt gebruik gemaakt van ingress (inkomend) verkeer spannen. Egress (uitgaand) verkeer spannen kan alleen op speciaal verzoek, met toestemming van een RWS architect. De sensor die door het RWS SOC op de SPAN poort wordt aangesloten is geen onderdeel van de dienstverlening. (R)SPAN mag alleen worden uitgevoerd binnen één locatie. Wanneer het gebruik van (R)SPAN leidt tot een processor load van 70% of hoger op een switch zal deze poort na overleg met de aanvrager van de SPAN-poort (tijdelijk) worden uitgezet. (R)SPAN is niet geschikt voor forensische doeleinden.

4.4.4 *Bestelbare items levertijd*

Voor de LAN Aansluiting gelden de in onderstaande **Figuur 43** weergegeven bestelbare items met bijbehorende standaard levertijden.

LAN aansluiting		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
RWS Netwerk LAN		
Gebouw, VC (Rekencentrum), CVR/VOR		
Aanvragen	leveren 1e LAN aansluiting op apparaat	L60
Opheffen	opheffen laatste LAN aansluiting op apparaat	L10
Activeren	activeren extra LAN aansluiting op afstand	L5
Deactiveren	deactiveren extra LAN aansluiting op afstand	L5
Wijzigen	wijzigen instelling bestaande LAN aansluiting op afstand	L5
Verhuizen	verhuizen diensten/hardware per apparaat	L30
Wegkant/Waterkant		
Aanvragen	leveren 1e LAN aansluiting op apparaat	L60
Aanvragen	leveren 1e LAN aansluiting op apparaat zonder installatie	L60
Opheffen	opheffen laatste LAN aansluiting op apparatuur	L10
Opheffen	opheffen laatste LAN aansluiting op apparatuur zonder installatie	L10
Activeren	activeren extra LAN aansluiting op afstand	L5
Deactiveren	deactiveren extra LAN aansluiting op afstand	L5
Wijzigen	wijzigen instelling bestaande LAN aansluiting op afstand	L5
Verhuizen	verhuizen diensten/hardware per apparaat	L30
Verhuizen	verhuizen diensten/hardware per apparaat zonder installatie	L30
KA LAN		
Aanvragen	leveren switch (abonnement op switch)	L60
Opheffen	opheffen switch (abonnement op switch)	L10
Wijzigen	wijzigen instelling switch op afstand	L1
Verhuizen	verhuizen diensten/hardware per apparaat	L30
Aanvragen Onsite Patching	Leveren patching op locatie	L60
WIFI		
Aanvragen	leveren access point	L50
Opheffen	opheffen access point	L20
Wijzigen	wijzigen instelling access point op afstand	L5
Verhuizen	verhuizen diensten/hardware access point	L30
Aanvragen site survey (per etage)	Leveren site survey op locatie	L15

Open WIFI		
Activeren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID.	L20
Deactiveren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID.	L20
Wijzigen Open WIFI	Registratie MAC adres vaste apparatuur per 10 devices	L1
Aanvragen site survey (per etage)	Leveren site survey Open WIFI op locatie	L15
ODC (Uitsluitend bestelbaar via CIV IRN Infra Netwerken)		
Aanvragen	leveren 1e LAN aansluiting op apparaat	L60
Opheffen	opheffen laatste LAN aansluiting op apparatuur	L60
Activeren	activeren extra LAN aansluiting en patching op locatie	L5
Deactiveren	deactiveren extra LAN aansluiting en patching op locatie	L5
Wijzigen	wijzigen instelling bestaande LAN aansluiting op afstand	L5
Verhuizen	verhuizen diensten/hardware per apparaat	L30
Vervangen	vervangen hardware per apparaat (LCM)	L30
LAN aansluiting type SPAN (Uitsluitend te bestellen door RWS SOC)		
Activeren	activeren extra LAN aansluiting op afstand	L5
Deactiveren	deactiveren extra LAN aansluiting op afstand	L5
Wijzigen	wijzigen instelling bestaande LAN aansluiting op afstand	L5

Figuur 43: Bestelbare items LAN Aansluiting

4.5 Categorie Eindsystemen

De categorie **Eindsystemen** beschrijft verschillende eindsysteemtoepassingen: de Digitale Video aansluiting (Encoder Analoge Camera), MiniFEP, AAA Remote Access Groepsprofiel, PPP, TBMS BUS en Draadloze aansluiting.

4.5.1 *Dienstenmatrix eindsystemen*

De categorie Eindsystemen is opgebouwd uit verschillende diensten ieder met hun specifieke kenmerken voor wat betreft beschikbaarheid en storingshersteltijd. Zie hiervoor **Figuur 44**.
De per dienst afgegeven beschikbaarheid is empirisch bepaald. Dit betekent dat het technisch design zodanig is dat de afgegeven SLA gegarandeerd kan worden.
De weergegeven storingshersteltijd is gebaseerd op incidenten waarbij de dienstverlening onderbroken is (er is business impact). Wanneer er sprake is van verstoorde dienstverlening (geen business impact) geldt het SLA zoals weergegeven in **Bijlage 5**.

Dienstenmatrix Eindsystemen							
	Beschikbaarheid			Storingshersteltijd in 95% van de gevallen			
	99,5%	99,7%	99,95%	Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
	Onbeschikbaarheid per jaar						
Type Eindsysteem	ca. 1d20u	ca. 1d2u	ca. 4u28m	K8	K4	E8	E4
Digitale Video aansluiting		√*					√
MiniFEP	√						√
Remote Access groepsprofiel			√				√
AAA	√				√		
PPP aansluiting	n.v.t.			redelijke effort			
Draadloze aansluiting	n.v.t.			redelijke effort			

** 99,7% is typische karakteristiek (niet pro-actief bewaakt of gemeten)*

Figuur 44: Eindsystemen

4.5.2 *Type eindsysteemtoepassingen*

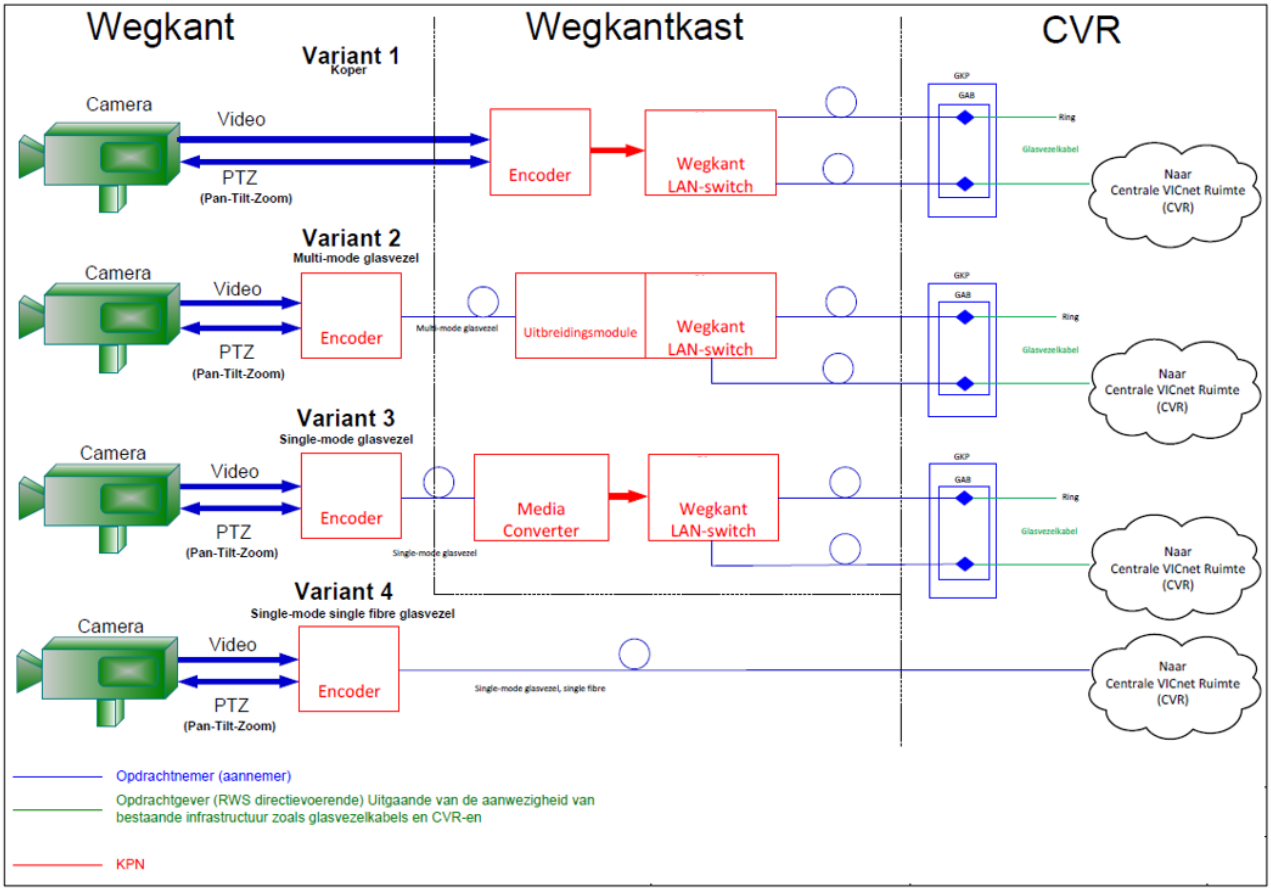
4.5.2.1 *Digitale Video aansluiting (niet meer te bestellen)*

De Digitale Video aansluiting, weergegeven in **Figuur 45**, ten behoeve van Analoge Camera's is bedoeld om analoge Pan Tilt Zoom camera's aan te sluiten op digitale apparatuur. De PTZ camera's worden op afstand bestuurd en kunnen worden gedraaid, in- en uitgezoomd en gekanteld. Als onderdeel van deze dienst worden camerabeelden ge-encodeerd en PTZ-signalen gedecodeerd. Het analoge videosignaal type Phase Alternating Line(PAL) wordt standaard omgezet naar een digitaal MPEG2 over IP signaal en het PTZ signaal wordt omgezet naar een serieel RS-485 signaal. Hierdoor kunnen de videobeelden van deze camera's

worden bekeken in de Verkeerscentrales. De dienst is geschikt voor inzet in ongeconditioneerde ruimtes. Daarnaast wordt Multicasting ondersteund waardoor er met meerdere monitoren tegelijkertijd naar één camera gekeken kan worden. Deze dienst gaat altijd vergezeld van een LAN Aansluiting.

De Digitale Video aansluiting kent vier varianten:

- Variant 1: De Camera is gemonteerd op het portaal en wordt middels koperkabel (COAX) aangesloten op de encoder in de bijbehorende wegkantkast.
- Variant 2: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels multi-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 3: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels single-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 4: De Camera is gemonteerd op een portaal of mast en wordt middels een enkele single mode glasvezelkabel aangesloten op de dichtstbijzijnde CVR.



Figuur 45: Digitale Video aansluiting

Voor het aansluiten van digitale (IP) camera's is een LAN-aansluiting type CVR / VOR of Wegkant/Waterkant bestelbaar (zie resp. paragraaf 4.4.3.1.3 en 4.4.3.1.4). Het demarcatiepunt van deze aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar de camera en eventuele media convertor zijn geen onderdeel van de dienst.

4.5.2.2 *MiniFEP*

Met ingang van december 2021 is de MiniFEP alleen nog bij uitzondering te leveren na akkoord van de Applicatiemanager MiniFEP.

De dienst MiniFEP verzorgt de koppeling tussen een Partyline segment (analoog) tbv Motorway Traffic Management systemen (MTM) en het RWS netwerk (LAN aansluiting). Doormiddel van deze dienst kunnen wegkantsystemen communiceren met de FEP (Front End Processor) concentrator op de verkeerscentrale. Daarbij biedt het een omschakelfunctionaliteit naar de back-up verkeerscentrale in het geval van een calamiteit.

Randvoorwaarden:
- De segmenteringsinformatie wordt bijgehouden door RWS en valt buiten de scope van dienstverlening;
- De segmenteringsinformatie wordt beheerd door RWS en dient aangevuld te worden met netwerkgegevens;
- Segment projectering wordt door de regio dan wel de ON (opdrachtnemer) uitgevoerd terwijl de IP gegevens door KPN DO RWS worden verstrekt.

4.5.2.3 *AAA RAS gebruiker en Remote Access groepsprofiel*

Het doel van de dienst Authenticatie, Autorisatie en Accounting (AAA) is om op gecontroleerde wijze toegang tot het netwerk en/of applicaties van RWS mogelijk te maken. De dienst AAA doet de controle en verificatie aan de hand van de authenticatie/autorisatie gegevens en bestaat uit de volgende onderdelen:
- **Authenticatie:** de verificatie van de aanmeldgegevens, (de identiteitsgegevens van de eindgebruikers die toegang vragen tot het netwerk of applicaties op het netwerk);
- **Autorisatie:** toekennen van toegangsrechten aan de eindgebruiker;
- **Accounting**: consistente administratie en het kunnen verstrekken van aanmeldinformatie over de eindgebruiker en het gebruik.

De dienst AAAbiedt:
- Gecontroleerde toegang voor (netwerk)componenten, applicaties en/of eindgebruikers tot de AAA dienstverlening.
- Gecontroleerde toegang tot het netwerk en/of applicaties van RWS voor een gebruiker voor het gebruik van Token of SMS Authenticatie.
- Gebruikersauthenticatie met een RSA token;
- Gebruikersauthenticatie met SMS One Time Password (OTP);
- User account synchronisatie met RWS Active Directory ldap(s);
- Selfservice voor RSA tokens (HTTPS) .

AAA RAS gebruiker

Deze dienst biedt de mogelijkheid om iemands identiteit met hoge zekerheid, volgens de ‘two-factor authenticatie’ methodiek vast te stellen en aan de hand hiervan toegang te geven tot het RWS netwerk.

Hierbij wordt gebruik gemaakt van:
1. Gebruikersnaam (accountnaam);
2. Iets wat een gebruiker ‘weet’ (kennis);
3. Iets wat een gebruiker ‘bezit’ (token).

Tokens



Er zijn twee soorten tokens beschikbaar:
1. SMS via de eigen telefoon. De verificatie vindt plaats via het versturen van een SMS code naar het voor die gebruiker in de AD van RWS vastgelegde 06-nummer.
2. Een persoonlijke RSA token voorzien van een unieke code die op het scherm van dat token wordt gepresenteerd.

Autorisatie doormiddel van AAA RAS Gebruiker en de dienst RAS Groepsprofiel
Wat een gebruiker of component, na succesvolle authenticatie, mag benaderen op het RWS netwerk wordt bepaald aan de hand van profielen. Deze profielen zijn onderdeel van de dienst Remote Access groepsprofiel. Door het aanvragen van het juiste groepsprofiel is het mogelijk om via het Internet vanaf een willekeurige locatie en willekeurig apparaat veilig met de binnen het profiel vrijgegeven interne systemen en applicaties van RWS te kunnen werken via een versleutelde verbinding. De dienst is niet bedoeld als machine to machine communicatiemedium.

De dienst Remote Access groepsprofiel is randvoorwaardelijk voor het gebruikmaken van de AAA dienst RAS gebruiker. AAA RAS gebruiker voorziet de gebruiker van een token om succesvol te kunnen authentiseren. In het RAS Profiel zijn de toepassingen en systemen waarvan gebruik gemaakt kan worden gespecificeerd.
Om veiligheidsredenen is de set aan toepassingen en systemen beperkt volgens het 'need to access' principe. In combinatie met de dienst AAA, die een koppeling legt tussen een RAS Profiel, een specifieke Active Directory (AD) user-account en een RAS Token, wordt het mogelijk om succesvol via de RAS dienst op het RWS netwerk in te loggen en de in het RAS profiel beschikbaar gestelde applicaties te gebruiken. Na het succesvol inloggen krijgt de gebruiker een specifieke pagina te zien met daarop de snelkoppelingen (hyperlinks) naar de beschikbaar gestelde interne applicaties en systemen. De inhoud van deze pagina komt overeen met hetgeen in het RAS Profiel was gespecificeerd.
In de RAS server worden RAS profielen conform aanvraag vanuit RWS geconfigureerd. De RAS profielen geven zogezegd toegang tot interne RWS applicaties. De autorisatie van een RAS gebruiker tot een RAS profiel vindt plaats via role mapping.

Voor de dienst RAS Groepsprofiel gelden de in **Figuur 46** volgende applicatie en toepassingsvoorwaarden:

Applicatie	Randvoorwaarden gebruiker/randapparaat
Web services (gebaseerd op de http(s) protocollen)	○ Applicaties moeten middels http(s) kunnen werken.
Citrix	○ Citrix ICA Client op Randapparaat
Windows Fileshare/Directories	○ Read-Only (default) of Read-Write. ○ Naar specifieke Share op specifieke Server. ○ Optioneel ook alleen vanaf een specifieke directory (en alle daaronder gelegen directories). ○ Read-Write alleen op basis van een specifieke Risico Analyse. En dit vereist een browser met Java die de Network Connect (*) applicatie kan draaien.
Windows Terminal Services (RDP protocol)	○ Remote Desktop client applicatie (bijvoorbeeld mstsc.exe), ○ user only; hiermee kan men dus niet als admin aanloggen op een remote systeem.
SSH	○ Alleen voor karakter gebaseerde / Virtual Terminal communicatie. ○ Tunneling van andere protocollen is niet toegestaan.
Overige applicaties alleen op basis van transparante netwerktoegang	○ RWS is zeer terughoudend in het toegang verlenen via deze methode, i.v.m. hogere risico's. Deze vorm vereist een specifieke Risico Analyse. ○ Directe communicatie tussen netwerken (Transit verkeer) is expliciet verboden. Hiervoor dient gebruik gemaakt te worden van de dienstbouwsteen Externe Koppeling. ○ Toegang wordt verleend naar specifiek(e) IP adres(sen), Protocol en poort nummer(s). ○ Vereist een browser met Java die de Network Connect applicatie kan draaien.

Figuur 46: Applicatie en toepassingsvoorwaarden RAS Groepsprofiel

De volgende voorschriften gelden voor het definiëren en gebruiken van RAS profielen:

- RAS profielen dienen maximaal van applicatie beveiligingsproxies (bedoeld worden de standaard applicaties zoals rdp, ssh e.d.) gebruik te maken en minimaal van transparante toegang;
- RAS Profielen mogen alleen toegewezen worden aan RAS gebruikers die voor alle applicaties en systemen in het RAS profiel geautoriseerd zijn;

- Het ontsluiten van RWS interne Applicaties en Systemen via de RAS dienst verloopt via een risico afweging en toets ten opzichte van security baseline(s);
- De systeem eigenaar / product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang;
- Indien een RAS profiel gebruikt wordt door gebruikers van derde partijen dan moet deze derde partij voldoen aan de NNV aansluitvoorwaarden;
- Ieder RAS profiel dient een benoemde functioneel beheerder te hebben.

Autorisatie middels AAA SMS authenticatie
Voor AAA SMS authenticatie (OTP) wordt voor de profielen de AD benaderd middels LDAPs en is de autorisatie afhankelijk van de AD groepen waar deze gebruiker of dit component deel van uitmaakt.
De dienst AAA is beschikbaar voor Verkeersmanagement (VM), het Ministerie van Infrastructuur en Waterstaat (IenW), RWS CIV IRN Infra, BOS en Scheepvaartmanagement (SVM).

De dienst AAA heeft de volgende uitgangspunten:
- De dienst maakt gebruik van een aantal interfaces:
  PIN authenticatie
  - Gebruikers moeten een PIN authenticatie uitvoeren in geval van een RSA-token.

  Token authenticatie
  - De RAS server communiceert met token authenticatie systemen via de RADIUS server;
  - De token authenticatie systemen verifiëren op hun beurt of gebruikers bestaan via een eigen koppeling met de RWS Active Directory;
  - https ingang voor eindgebruikers via een self service portal (SSP) om tokenmanagement uit te voeren (bv pin reset of opgeven van een aflever adres);
  - radius ingang voor de component RAS voor authenticatie en autorisatie van de RAS gebruikers. De autorisatie is een RADIUS attribuut dat de RAS component gebruikt bij mapping op een RAS profiel (met bijbehorende permissies);
  - LDAP(s) uitgang naar de RWS AD omgeving voor het authentiseren van gebruikers die op de SSP inloggen, en voor het synchroniseren van de gebruikersdatabase.
- De dienst ondersteunt de volgende protocollen: TACACS+, RADIUS, LDAPs (Light Weight Directory Access Protocol) en gebruik in combinatie met onder ander PPP , PAP, CHAP, EAP, PEAP, TLS en in bredere zin toegangscontrole middels 802.1x.
- Voor andere componenten en diensten zal per stuk bekeken moeten worden welke interfaces geschikt zijn om van AAA gebruik te kunnen maken. Gebruik van RADIUS of koppeling met de AD middels LDAP(s) behoren tot de mogelijkheden.

Voor de dienstcomponenten van AAA gelden de in **Figuur 47** weergegeven voorwaarden:

Dienst component	Voorwaarden
RWS Active Directory	• Gebruiker moet reeds een actief **User-account** hebben in RWS Active Directory. • Bij SMS authenticatie dient het user account ook over een bruikbaar **telefoonnummer** attribuut te beschikken • Bij SMS authenticatie dient het user account ook te zijn opgenomen in een AD groep die correspondeert met een RAS profiel.
Token	• De gebruiker moet een **RSA Token** hebben of krijgen en het serienummer dient daarvan bekend te zijn. Dit is niet van toepassing indien gebruik wordt gemaakt van SMS authenticatie.
Applicaties Autorisatie	• De Gebruiker moet **autorisatie** hebben om de systemen en applicaties te mogen benaderen.
Firewall Rule	• De **Firewalls** dienen de juiste en geautoriseerde toegang mogelijk maken
<ICT-Middelen>	• De Gebruiker moet zelf voorzien in een **internet verbinding**.

	• De Gebruiker moet zelf voorzien in een **ICT-Middel**, zoals een PC, laptop, PDA, smartphone of tablet. De telefoon is essentieel wanneer de gebruiker SMS authenticatie toepast.
	• Het ICT-Middel dient altijd gevrijwaard te zijn van virussen, malware en key loggers; en te voldoen aan het vigerende RWS beveiligingsbeleid.
	• Het ICT-Middel ondersteunt minimaal een standaard **webbrowser** (zoals Internet Explorer of Firefox) met een recente versie (< 3 jaar oud) om de inlogprocedure voor de Remote Access Verbinding te volbrengen.
RAS Gebruiker	• In geval van authenticatie met een 'RSA token', zijn per gebruiker de RWS Active Directory username, het Token-nummer en het RAS Profiel met elkaar gekoppeld. • Wanneer gebruik wordt gemaakt van SMS authenticatie vindt de koppeling plaats via groepslidmaatschap in de RWS active directory en valt de koppeling buiten de dienstbouwsteen

Figuur 47: Voorwaarden dienstcomponenten AAA

Aanvullend geldt het volgende:

- Voor het gebruik van de RSA-Token moet de gebruiker de "Bruikleenovereenkomst ICT-middel" ondertekend hebben. Dit kan middels een notificatie pagina op de Remote Access Service zelf. Dit is niet van toepassing bij het gebruik van SMS tokens;
- RSA tokens en/of telefoons (t.b.v. SMS token codes) mogen niet uit handen gegeven worden;
- RSA tokens dienen niet zichtbaar opgeborgen te worden zodat de gegenereerde tokencodes en het serienummer maximaal afgeschermd zijn voor ongeoorloofde ogen;
- Gebruikers worden geacht geïnformeerd over en bekend te zijn met de fenomenen Social Engineering en Phishing: methoden van afkijken en hoe dit te voorkomen;
- Gebruikers mogen nooit het Token serienummer, PIN-code, tokencode, passcode of wachtwoorden prijsgeven, ook niet aan een helpdesk;
- Gebruikers moeten alert zijn bij het gebruik van sociale media, zodat gevoelige informatie niet indirect prijsgegeven wordt;
- Tokens mogen alleen gebruikt worden op een werkplek met adequate beveiliging tegen malware, keyloggers en screencapture/screenrecorders door middel van anti-malware software;
- Tokens mogen niet gebruikt worden in publieke ruimten zoals cybercafes of op openbare computers;
- Gebruikers moeten bij vermoedens van onrechtmatig gebruik van hun toegang[10], of pogingen daartoe zoals social engineering, dit als security incident melden bij de corporate servicedesk alsmede een directe blokkade aanvragen.

4.5.2.4 *PPP aansluiting (niet meer te bestellen)*

Deze dienst biedt een serieel (RS232) koppelvlak voor de weg- of waterkanttoepassingen naar de Backbone bedoeld voor communicatie met de Verkeerscentrale. Deze dienst werd typisch toegepast bij DRIPs, TDIs, VRIs en GMS2 en is geschikt voor ongeconditioneerde ruimtes.

Deze dienst in niet langer bestelbaar. Er kunnen nog wel wijzigingen aangevraagd worden en de dienst kan opgezegd worden. De opvolgers van deze dienst zijn de Draadloze VPN Aansluiting en de LAN Aansluiting die beiden uitgaan van een LAN koppelvlak.
De Special "PPP met huurlijnverlenging" kan niet worden aangevraagd noch gewijzigd, deze kan alleen worden opgezegd.

4.5.2.5 *TBMS BUS (niet meer te bestellen)*

TBMS staat voor Token Bus Master Slave en is een op 802.4 (Token passing) gebaseerd protocol met een door RWS gemodificeerde TCP/IP stack (VOPP) bedoelt voor de specifieke eisen van de wegkantsystemen ((M)WKS).

[10] Bijvoorbeeld als men een logincode ontvangt via SMS, terwijl men niet aan het telewerken is.

Deze netwerktoegangsdienst maakt het mogelijk dat wegkantstations, die gebruik maken van partylines, voor de applicatie ‘Monica’ via het TBMS protocol gekoppeld kunnen worden aan het generieke op ethernet/IP gebaseerde RWS netwerk.

Deze dienst in niet langer bestelbaar en er kunnen geen wijzigingen meer aangevraagd worden. De dienst kan uitsluitend opgezegd worden. De SLA van de TBMS dienstverlening is op basis van ‘redelijke effort’. Onbeschikbaarheid van spare apparatuur kan ertoe leiden dat een storing niet meer kan worden opgelost en een verstoorde TBMS-dienst daarom niet meer operationeel gekregen kan worden.

4.5.2.6 *Draadloze aansluiting (niet meer te bestellen)*

De Draadloze aansluiting betreft een aansluiting gebaseerd op een serieel koppelvlak en TCP/IP PPP (point to point protocol) en werd toegepast voor het aansluiten van weg- of waterkant toepassingen als DRIPs, TDI’s en Meetnetaansluitingen met een serieel koppelvlak. Omdat er gestreefd wordt naar een all-IP netwerk, wordt dit koppelvlak als ‘legacy’ gecategoriseerd en is niet meer bestelbaar. De Draadloze aansluiting bestaat uit een (ruggedized) draadloos modem + SIM (Wireless 2G/RS232).

Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften. Zie hiervoor de desbetreffende documentatie (beschikbaar op de VPR).

4.5.3 *Bestelbare items en levertijd*

Voor de **Eindsysteem toepassingen** gelden de in **Figuur 48** weergegeven bestelbare items met bijbehorende standaard levertijden.

Eindsystemen		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Digitale Video Aansluiting (Encoder Analoge Camera)		
Opheffen incl. installatie	Opheffen dienst op eindsysteem inclusief installatie	L10
Opheffen	Opheffen dienst op eindsysteem exclusief installatie	L10
Wijzigen	Wijzigen instelling Digitale Video aansluiting	L5
Verhuizen incl. installatie	Verhuizen dienst op eindsysteem inclusief installatie	L30
Verhuizen	Verhuizen dienst op eindsysteem exclusief installatie	L30
MiniFEP		
Opheffen	Opheffen laatste Mini FEP aansluiting op apparaat	L20
Deactiveren	Deactiveren extra Mini FEP aansluiting op locatie	L20
Wijzigen	Wijzigen instelling Mini FEP op afstand	L10
PPP aansluiting		
Opheffen	Opheffen PPP aansluiting	L10
Wijzigen	Wijzigen PPP aansluiting	L10
TBMS BUS		
Opheffen	Opheffen TBMS BUS	L10
Remote Access groepsprofiel		
Aanvragen	Aanvragen RAS profiel	L20
Opheffen	Opheffen RAS profiel	L5
Wijzigen	Wijzigen RAS profiel	L5
AAA Ras gebruiker		
Aanvragen	Aanvragen RSA token	L5
Opheffen	Opheffen RSA token	L5
Wijzigen	Wijzigen RSA token	Direct
Aanvragen	AAA Toegang voor componenten of applicaties	Maatwerk
Opheffen	AAA Toegang voor componenten of applicaties	Maatwerk
Draadloze aansluiting		
Deactiveren	Deactiveren Draadloze aansluiting op afstand	L5
Wijzigen	Wijzigen instelling bestaande Draadloze aansluiting op afstand	L10

Figuur 48: Bestelbare items en levertijd Eindsysteem toepassingen

4.5.4 *Verrekening*

Zie VPR voor prijzen en tarieven.

4.6 Categorie Overig

De categorie **Overig** biedt een overzicht van de diensten gepland werk glas, adviezen, consultancy uren en Rijkskantoorroam.

4.6.1 *Gepland werk Glas*

Indien bij aanleg- of renovatieprojecten mutaties in het glasvezelnetwerk van RWS noodzakelijk zijn, dienen aannemers deze activiteiten uit te voeren op basis van een glasadvies van KPN.

Er wordt onderscheid gemaakt tussen de volgende gradaties gepland werk (**Figuur 49**):

Gepland werk Glas		
Type	Kenmerken	Deliverables
Eenvoudig (zonder additionele kosten aan te vragen als RFI)	Als elk punt van toepassing is: * < 4 uur analyse * < 4 uur begeleiding * Begeleiding tijdens kantooruren * * Max. één overleg met RWS-Opdrachtnemer Verwachte tijdbesteding max 16 uur	* Overzicht van de bezette vezels in de betrokken kabels * Opsomming welke PDC-diensten 'geraakt' worden * Enkelvoudig gerouteerd, zoals camera's * Dubbel gerouteerd, zoals aansluiting via ELDW. * Aansluitingen van derden in beheer bij DO-RWS (LNV, DVM-nat, NNV, e.d.) * Aansluitingen van derden niet in beheer bij DO-RWS (vezels voor bv. Havenbedrijf, politie, e.d.) * Onbekende aansluitingen (bezet zonder bekende PDC-dienst of naam gebruiker) * Analyse of de geraakte dubbel-gerouteerde PDC-diensten niet 'toevallig' ook betrokken zijn bij andere werkzaamheden of lopende incidenten. * Analyse welke andere SI's dan DVM-Droog worden geraakt waardoor ook derden geïnformeerd moeten worden en mogelijk CAB ingeschakeld moet worden. * Review Plan van Aanpak RWS-ON * Begeleiden her-indienststelling switches. * Informeren SI's en afstemmen met CAB.
Standaard	Als één aspect van toepassing is: * > 4 uur analyse * > 4 uur begeleiding * Begeleiding buiten kantooruren * * Meer dan één overleg Verwachte tijdbesteding max 40 uur.	
Projectmatig Small	Als van toepassing is: * Projectmatige begeleiding gewenst en * Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. Eén dagdeel een monteursteam van 2 man. * Werkzaamheden gedurende max. één dag op één tracé. Verwachte tijdbesteding totaal max 80 uur.	* De onder 'eenvoudig' en 'standaard' genoemde deliverables, en tevens: * Projectcoördinator voor voorbereiding en begeleiding van de werkzaamheden * Verificatie vooraf in technische ruimtes (CVR e.d.) of bezetting van de kabels overeenkomst met administratie. Controle met 'lichttang' of vezels daadwerkelijk bezet zijn. * Verificatie vooraf in technische ruimtes (CVR e.d.) of het vrij schakelen van een verbinding het verwachte effect heeft (testen). * Test op redundantie van verbindingen vooraf (op locatie en/of via beheersysteem) * Vooraf omsteken van verbindingen in technische ruimtes (CVR e.d.) indien dit uit oogpunt van handhaven verbinding gewenst is * Vrij schakelen en terugschakelen van verbindingen op de dag van uitvoering. * Tijdens de uitvoering zijn monteurs en de projectcoördinator op locatie aanwezig. * Tijdens de uitvoering zijn een netwerkbeheerder en een back-up beschikbaar voor test en controle via de netwerkmanagementsystemen. Niet inbegrepen is het opgraven, openen en onderzoeken van kabelputten. Dit kan als meerwerk uitgevoerd worden.
Projectmatig Medium	Als van toepassing is: - Projectmatige begeleiding gewenst en - Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. Driedagdelen een monteursteam van 2 man. - Werkzaamheden gedurende max. één dag op één tracé. Verwachte tijdbesteding max 130 uur.	
Projectmatig Large	Indien één van de volgende situaties geldt: - Meer dan drie dagdelen inzet van een monteursteam; - Meerdere tracés, - Werk over meerdere dagen Verwachte tijdbesteding totaal > 130 uur.	

Figuur 49: Gepland werk Glas

4.6.2 *Glasadvies*

Het glasadvies is bedoeld om in een project, voorafgaand aan de bestelling van PDC-diensten, de aanvrager te ondersteunen in het maken van de juiste keuzes. Uitgangspunt is dat er uitgegaan kan worden van bestaande netwerkarchitectuur, technologie en apparatuur.
Daarnaast wordt beoogd:

- Adequate voorbereiding te doen voor de datanetwerken in een RWS-project om latere bestelling en levering van PDC-diensten snel, effectief en efficiënt mogelijk te maken;
- De opdrachtnemer van RWS te ondersteunen in het maken van de juiste keuzes bij het aanleggen van glasvezelinfrastructuur of benutten van bestaande glasvezelinfrastructuur voor datanetwerken, waarmee een goed te beheren en toekomst vast datanetwerk ontstaat.

Er wordt onderscheid gemaakt tussen drie type adviezen zoals weergegeven in **Figuur 50**:

Glasadviess		
Type	Kenmerken	Deliverables
Eenvoudig	* <= 2 overleggen * <= 4 lasseneleiding tijdens kantooruren * * <= 20km netwerk * Bestaande technologie * Bestaande beheeromgeving	* Advies routering nieuwe infra * Advies gebruik bestaande infra * Advies posities glasvezelkabelputten en kasten * Lasschetsen en routeringsschema uit Cocon * Aanwijzing gebruik glasvezellades in CVR e.d. * Advies te bestellen typen PDC-items * Advies en afstemming over eventuele fasering uitvoering * Afstemming met andere lopende projecten * Adviesrapport
Complex	* <= 4 overleggen * <= 10 lasseneleiding tijdens kantooruren * * <= 50km netwerk * Bestaande technologie * Bestaande beheeromgeving	
Maatwerk	* Meer afstemming * Groter netwerk * Afwijkende technologie * Nieuwe beheeromgeving	Als hierboven + * Inventariseren afwijkende bedrijfsmiddelen * Advies posities glasvezelkabelputten en kasten * Advies hoe om te gaan met niet-acceptabele afwijkingenn * Afstemmen en inregelen:. * Incidentbehandeling * Onderhoud * Changemanagemanet * Inventariseren gebruik glas door niet-PDC-diensten * Eventueel opstellen maatwerk-DAP

Figuur 50: Glasadvies

4.6.3 *Netwerkadviezen*

In de RWS Topdesk SelfServicePortal kan via PDC IRN INFRA > NETWERK > NETWERK ADVIES > NETWERKADVIES TYPE EENVOUDIG een Advies aangevraagd worden om te bepalen of een functionele behoefte ingevuld kan worden met PDC leveringen en/of de inzet van KPN DO RW medewerk(st)ers.

Dit resulteert in een Advies van het type ‘eenvoudig’ (zie figuur 3 in paragraaf 2.5).
Indien blijkt dat de functionele behoefte niet ingevuld kan worden met PDC leveringen dan dient het SPM proces gestart te worden om te komen tot een nieuwe of gewijzigde dienst, zoals beschreven in paragraaf 2.5.

4.6.4 *Uurtarieven / Strippenkaart*

Als onderdeel van de dienstverlening biedt KPN DO RWS de inzet van medewerkers aan bij Projecten en Leveringen. De uurtarieven van onderstaande rollen zijn beschikbaar in het Prijzenblad. In het geval van Leveringen wordt gebruik gemaakt van een strippenkaartconstructie. In een ‘Strippenkaart’ wordt een aantal uren per rol aangeboden, welke op basis van werkelijk gemaakte uren worden verrekend. De afnemer wordt tijdig op de hoogte gebracht bij dreigende overschrijding van de geplande uren.

Consultancyrollen	
Rol	**Specificatie**
Assistent Engineer	Junior netwerk engineer
Onsite Engineer	Netwerk engineer die werkzaamheden verricht op locatie
Support medewerker	Netwerkbeheerder die ondersteunt bij het oplossen van complexe verstoringen en het voorbereiden van de uitvoering van wijzigingen
Engineer / Implementatiemanager	Medior netwerk engineer verantwoordelijk voor het uitvoeren van wijzigingen
Engineer +	Senior netwerk engineer
Projectleider	De projectleider coördineert PDC- aanvragen en projecten
Technical Consultant	Ontwerper van technische netwerkoplossingen
Senior Technical Consultant	Senior ontwerper van technische netwerkoplossingen
Beheer Consultant	Ontwerper verantwoordelijk voor het inrichten van de beheerprocessen
DC Manager	De DC Manager is verantwoordelijk voor het huidige aanbod aan standaard diensten en dienstontwikkeling, met als deliverables de Producten en Diensten Catalogus en SPM roadmap. De DC Manager kan in projecten worden ingezet voor het maken van dienstbeschrijvingen, reviewen van documentatie, vaststellen van nieuwe standaard bestelbare items en andere dienstontwikkeling gerelateerde zaken
Project Manager	Project Managers worden ingezet in dienstontwikkelingstrajecten, zowel in de pre-sales als in de projectfase voor het coördineren van dienstontwikkelingsprojecten.
Technical Architect	Architect verantwoordelijk voor het ontwerp en wijzigen van bouwstenen
Business Consultant	De Business Consultant vertaalt de functionele vraag van de aanvrager naar de gewenste oplossing in de vorm van een advies en coördineert het proces om van aanvraag tot project te komen.
Lead Architect	De Lead Architect is het eerste aanspreekpunt voor de Domeinarchitect van RWS CIV IRN Infra en borgt dat de DO RWS organisatie werkt binnen de door RWS CIV IRN Infra gestelde kaders. De Lead Architect is in die hoedanigheid betrokken bij dienstontwikkeling, projecten, innovatie en strategie.
Project Portfolio Manager	De Project Portfolio Manager DO RWS is het eerste aanspreekpunt voor de Project Portfolio en Programma Project Manager van RWS CIV IRN Infra.

Figuur 54: Consultancyrollen

4.6.5 *Rijkskantoorroam*

De dienst Rijkskantoorroam maakt het mogelijk om RWS panden die zijn aangewezen als Rijksverzamelkantoor te voorzien van een Generieke netwerk infrastructuur Connectivity (RijkskantoorRoam). Anderzijds wordt met deze dienst ook de mogelijkheid geboden om RWS medewerkers gebruik te laten maken van de Generieke netwerk infrastructuur Connectivity in Rijksverzamelkantoren van andere overheidsorganisaties.
Rijkskantoorroam is een zogenaamde geïntegreerde dienst; hij wordt samengesteld uit de reeds bestaande diensten VPN aansluiting, WIFI, KA LAN, Virtual Firewall, AAA. Om het de afnemer eenvoudig te maken om Rijkskantoorroam te bestellen hoeft hij alleen in Topdesk de keuze te maken voor een van de twee mogelijkheden en daarna zal KPN DO RWS benodigde diensten/activiteiten aanbieden:

- Aanvraag/opzegging RijkskantoorRoam RWS Kantoor
- Aanvraag/opzegging RijkskantoorRoam RWS koppeling Rijksorganisatie

4.6.6 *Bestelbare items en levertijd*

Voor de diensten in de categorie **Overig** gelden de in **Figuur 55** weergegeven bestelbare items met bijbehorende standaard levertijden.

Overig		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Gepland werk Glas		
Aanvragen	Gepland werk Glas Eenvoudig	in overleg
Aanvragen	Gepland werk Glas Standaard	in overleg
Aanvragen	Gepland werk Glas – Projectmatig Small	in overleg
Aanvragen	Gepland werk Glas – Projectmatig Medium	in overleg
Aanvragen	Gepland werk Glas – Projectmatig Large	in overleg
Glasadvies		

Aanvragen	Glas Advies type Eenvoudig	in overleg
Aanvragen	Glas Advies type Complex	in overleg
Aanvragen	Glas Advies type Maatwerk	in overleg
Dark Fiber advies		
Aanvragen	Dark Fiber Advies type Eenvoudig	*
Aanvragen	Dark Fiber Advies type Complex	*
Dark Fiber levering		
De **dienst Dark Fiber** is uitsluitend bestelbaar op basis van door RWS te accorderen levering en afhankelijk van de bezettingsgraad van een glasvezelkabel. De coördinatie verloopt via de RWS CIV IRN Infra Netwerken Relatie Manager.		
Aanvragen	Dark Fiber RWS levering aanvragen	*
Opheffen	Dark Fiber RWS levering opheffen	*
Activeren	Dark Fiber RWS levering activeren	*
Netwerk adviezen		
Aanvragen	Netwerk Advies Eenvoudig	L15
Aanvragen	Netwerk Advies Normaal	L30
Aanvragen	Netwerk Advies Complex	L60
Aanvragen	Netwerk Advies Maatwerk	in overleg
Uurtarieven		
Aanvragen	Assistent Engineer	in overleg
Aanvragen	Onsite Engineer	in overleg
Aanvragen	Support medewerker	in overleg
Aanvragen	Engineer / Implementatiemanager	in overleg
Aanvragen	Engineer+	in overleg
Aanvragen	Projectleider	in overleg
Aanvragen	Technical Consultant / Beheer Consultant / DC Manager / Project Manager	in overleg
Aanvragen	Technical Architect / Sr Technical Consultant / Business Consultant	in overleg
Aanvragen	Lead Architect / Project Portfolio Manager	in overleg

Figuur 55: Bestelbare items en levertijd Overige Diensten

* De levertijd van een Dark Fiber verbinding is afhankelijk van (1) of en hoe de demarcatie locaties op het RWS glasvezel netwerk zijn aangesloten en (2) van het beschikbaar zijn van de glasvezelverbindingen in het RWS glasvezel netwerk.

4.6.7 *Verrekening*

De eenmalige kosten en abonnementstarieven van de bestelbare items zijn terug te vinden in het Prijzenblad. De actuele versie hiervan is beschikbaar in de RWS Topdesk SelfServicePortal via Startpagina > PDC IRN INFRA > Netwerk

Bijlagen

Bijlage A Contactgegevens

Voor vragen omtrent de standaard dienstverlening en dienstontwikkelingen kan contact opgenomen worden met de Relatie Manager RWS CIV IRN of zijn Service Management collega's.

Een overzicht van de Service Managers is te vinden op
https://corporate.intranet.rws.nl/Organisatie/Organisatieonderdelen/Centrale_Informatievoorziening/Directies_en_afdelingen/IV_RWS_Netwerken/IRN_Loket/IRN_Servicemanagers/

De Service Portfolio Manager is verantwoordelijk voor deze Dienstencatalogus en deze wordt beheerd door de Diensten Portfolio Manager.

De contactgegevens zijn weergegeven in **Figuur 56**.

Organisatie	Functie	Naam	E-mail	Telefoonnummer
Rijkswaterstaat	Relatie Manager	Arjan Hoogenboezem (a.i.)	arjan.hoogenboezem@rws.nl	06 53428730
Rijkswaterstaat	Service Level Manager	Mark Vollebregt	mark.vollebregt@rws.nl	06 50166157
Rijkswaterstaat	Service Portfolio Manager	Bas Brekelmans	bas.brekelmans@rws.nl	06 51120856
Rijkswaterstaat	Supply Manager	Léon van Tiel	leon.van.tiel@rws.nl	06 10492329
KPN DO RWS	Diensten Portfolio Manager	Barbara Koorn	barbara.koorn@kpn.com	06 51080144
KPN DO RWS	Delivery Manager	Marc van der Loo	marc.vanderloo@kpn.com	06 29527023

Figuur 56: Contactgegevens

Bijlage B Afkortingen en Begrippen

Afkortingen

Figuur 57 geeft een overzicht van de in deze catalogus gebruikte afkortingen en hun betekenis.

Afkortingen	
RWS	Rijkswaterstaat
RWS CIV IRN Infra Netwerken	Rijkswaterstaat Centrale Informatie Voorziening Infrastructuur Netwerken
KPN DO RWS	KPN Customer Team Rijkswaterstaat
NNV	Nieuwe Netwerk Voorzieningen
VPN	Virtual Private Network
DDI	De dienst die bestaat uit DHCP DNS en IPAM
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
IPAM	Internet Protocol Adres Management
DMZ en DMZ Client	een Demilitarised Zone (beveiliging laag) en Demilitarised Zone Client (DMZ Aansluiting)
NTP	Network Time Protocol
WoL	Wake on LAN
IPsec	Internet Protocol Security
VO LAN	VPN Ontsluiting LAN
CE	Client Edge
LAN	Local Area Network
KA-LAN	Kantoor Automatisering LAN
CVR	Centrale VicNet Ruimte
VOR	VicNet Object Ruimte
ODC	Overheid Data Center
VC	Verkeerscentrale
VLAN	Virtueel LAN (VLAN)
DRIP	Dynamisch Route Informatie Paneel
DOV	Dynamische Openbare Verlichting
TDI	Toerit Dosering Installatie
VRI	VerkeersRegel Installatie
VAD	Vluchthaven Aanwezigheid Detectie
WIM	Weigh in Motion (ten behoeve van het wegen van vrachtwagens)
CADO	Calamiteiten Doorsteek
MTV	Motorway Traffic Video
UWP	Universeel Wegkant Platform
LEF	Het Future Center van RWS waar innovatie centraal staat. LEF is geen afkorting, maar staat voor lef, durf en moed. Voor het verleggen van grenzen
SSID	Service Set Identifier
AP's	Access Points
QoS	Quality of Service
APN	Access Point Name
Wi-Fi	Wireless Fidelity
AAA	Authenticatie Autorisatie Accounting
WLAN	Wireless Local Area Network
LCM	Lifecycle Management
FEP	Front End Processor
PTZ	Pan Tilt Zoom
PAL	Phase Alternating Line
IP	Internet Protocol
SIM	Subscriber Identity Module
MTM	Motorway Traffic Management
PLCS	Party Line Crossover Switch
ON	Opdracht Nemer
RSA	Merknaam
RAS	Remote Access Services
OTP	One Time Password
AD	Active Directory
RDP	Remote Desktop Protocol
LDAP	Lightweight Directory Access Protocol
VWS	Verkeersmanagement Services
IenW	Infrastructuur en Waterstaat
SVM	Scheepvaart Management

SSP	Self Service Portal
GMS	Gladheidsmeldsystemen
TBMS	Token Bus Master Slave
WKS	Wegkant Systemen
MWKS	Mobiele Wegkant Systemen

Figuur 57: Afkortingen

Begrippen

Figuur 58 geeft een toelichting op de in deze catalogus gebruikte begrippen.

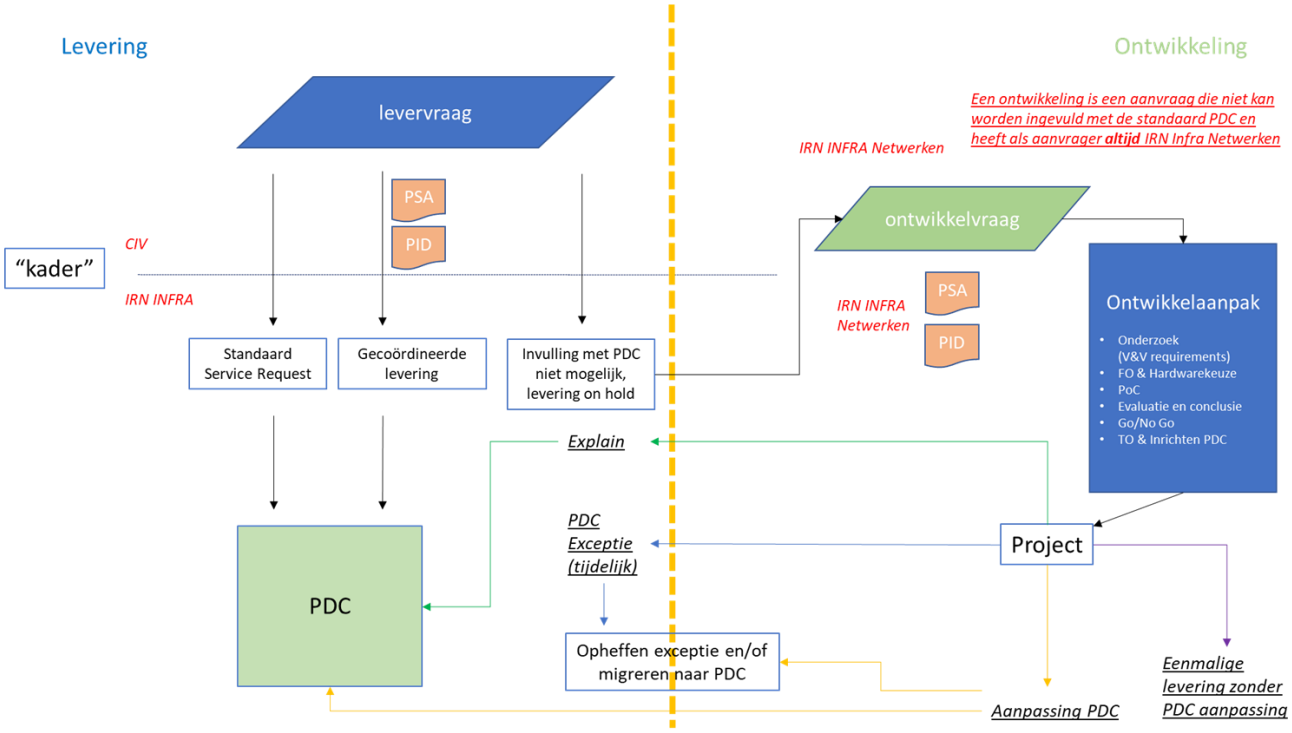
Begrippen	
Prijzenblad	Overzicht van alle bestelbare items inclusief eenmalige kosten en abonnementen
Categorie VPN	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network
Categorie VPN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network Aansluiting
Categorie LAN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Local Area Network
Categorie Eindsysteem	Alle diensten welke onderdeel uitmaken van de categorie Eindsysteem (toepassingen voor eindsystemen)
Categorie Backbone	Alle diensten welke onderdeel uitmaken van de categorie Backbone/Core/CV omdat deze onderdeel uitmaken van het backbone netwerk van Rijkswaterstaat en uitsluitend door RWS CIV te bestellen zijn
Categorie Special	Alle diensten welke geen onderdeel uitmaken van de Categorie VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Backbone en uitsluitend door RWS CIV te bestellen zijn
RWS netwerk	Het netwerk van Rijkswaterstaat voorheen bekend als “Rijkswaterstaat Nieuwe Netwerk Voorzieningen”
Object Access Netwerken	Object LAN
Kunstwerken	Rijkswaterstaat benaming voor objecten als bruggen, sluizen, tunnels
Huurlijnen	Transmissielijnen van andere partijen dan Rijkswaterstaat zelf, waarover verkeer van Rijkswaterstaat loopt
Service Desk	KPN beheert het netwerk van RWS en heeft hiertoe o.a. een Service Desk ingericht.
Aansluitvoorwaarden NNV (CIV)	De voorwaarden waaraan moet worden voldaan om gebruik te maken van het RWS netwerk
Topdesk	De Service Portal van Rijkswaterstaat. Via deze portal kunnen bestelbare
Bulklevering	Levering van een groot aantal bestelbare items in één bestelling
Service Portfolio Management proces	Het proces ingericht om het dienstenportfolio up to date te houden, nieuwe diensten te ontwikkelen, bestaande diensten aan te passen en verouderde diensten uit te faseren
Internet Access	De VPN functie die het mogelijk maakt om toegang tot het internet te verkrijgen
DDI	De dienst die bestaat uit DHCP DNS en IPAM
Mail relay	Configuratie die het mogelijk maakt e-mail berichten te versturen via een SMTP-server
Virtual Firewall	Firewall service in een virtuele omgeving die doormiddel van software communicatie controleert
NTP	Network Time Protocol: maakt het mogelijk om de interne klok van computers met elkaar te kunnen synchroniseren
RWS Backbone	Centrale netwerk-infrastructuur van Rijkswaterstaat
Ruggedized	Verharde apparatuur geschikt voor ongeconditioneerde ruimten
Shaping	Methode om bandbreedte te verdelen zodat data niet verloren gaat en er geen capaciteitstekort ontstaat
Transmissie	Doorlaten van verkeer via verbinding
Wake on LAN	Netwerkstandaard waarmee het mogelijk is een computer op afstand te benaderen
Encrypted Tunnel	Een beveiligde Internet verbinding waarover data versleuteld verzonden wordt
IPsec	Internet Protocol Security
IPsec Gateway	Internet Protocol Security netwerkpunt dat voorziet in toegang tot een netwerk
Externe locatie	Locatie buiten het RWS netwerk
PDC	Standaard dienstverlening uit de Product Diensten Catalogus
NON-PDC	Maatwerk dienstverlening die geen onderdeel is van de Product Diensten Catalogus
CE domein	Een Custom Edge Router domein
VO LAN	VPN Ontsluiting LAN Configuratie op de router om de LAN-aansluiting te ontsluiten naar het VPN
VPR	RWS SharePoint
LAN domein	Gescheiden deel van het Local Area Network
Routering	Het bepalen van de route die door informatie via het netwerk wordt afgelegd
Centrale VicNet Ruimte	voornamelijk kleine gebouwen op knooppunten van snelwegen waarbinnen een geconditioneerde ruimte aanwezig is voor actieve netwerk apparatuur. Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.
VicNet Object Ruimte	dit zijn geconditioneerde ruimtes voor actieve netwerk apparatuur binnen objecten zoals tunnels, sluizen, bruggen, radarposten en dergelijke. Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.

LAN ontsluiting	de logische koppeling naar een specifiek VPN
VLAN	Virtueel LAN in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN Aansluiting	de fysieke poort die toegang biedt naar het virtuele LAN
Ethernet infra	dit is de fysieke infrastructuur (bekabeling en switches)
RWS Netwerk LAN	Alle LAN Aansluitingen in het Rijkswaterstaat netwerk met uitzondering van KA-LAN, ODC LAN en WIFI
Duplex instelling	Het protocol voor verzenden en ontvangen van informatie op de LAN Aansluiting
Trunking	Meerdere VLAN's op één fysieke poort
Port channeling	Combineren van de capaciteit switches
Spanning-tree protocol	Protocol dat er voor zorgt dat er slechts één pad mogelijk is voor het zenden van informatie, waarmee ontvangst gegarandeerd wordt.
loop-free topologie	Netwerk waarin loopvorming niet mogelijk is
PTZ Camera	op afstand bestuurbare camera die kan worden gedraaid, in- en uitgezoomd en gekanteld

Figuur 58: Begrippen

Bijlage C Service Portfolio Management Proces

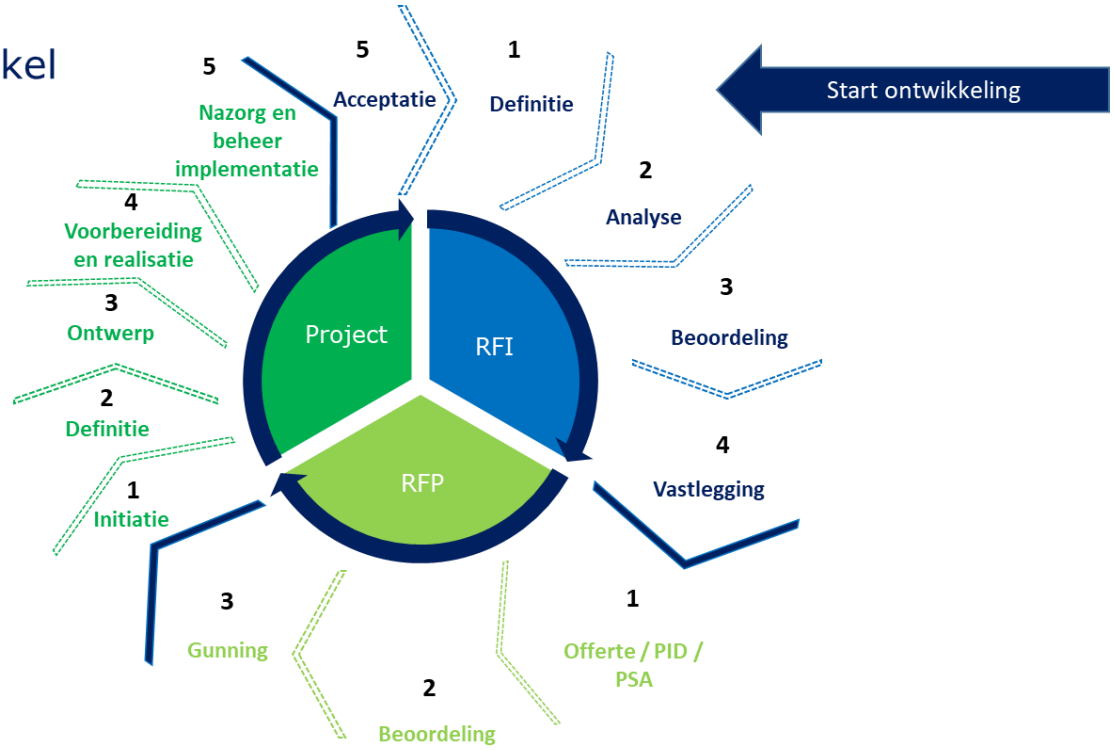
Service Portfolio Management Procesbeschrijving (Versie 2.0).
Voor vragen hieromtrent kan contact worden opgenomen met de Service Portfolio Manager of Relatie Manager van RWS CIV IRN



Generieke uitgangspunten

- Een klantvraag kan ingevuld worden middels:
  - **SSR**: Middels standaard service request geautomatiseerd leveren één of meerdere bestelbare items uit de PDC
  - **Gecoördineerde levering**: Leveren van één of meerdere bestelbare items uit de PDC onder besturing van een PDC projectcoördinator o.b.v. een PDC prijsopgaaf
- Indien de klantvraag niet kan worden ingevuld met de PDC dient RWS CIV IRN Infra Netwerken een ontwikkeltraject te starten
- Het SPM proces wordt gevolgd voor alle **Ontwikkelingen**
- In de **rfi fase** (M-nummer) wordt een advies opgesteld dat beschrijft hoe de klantvraag (uiteindelijk) met standaard dienstverlening kan worden ingevuld en de weg daarnaartoe (requirements, ontwikkeling PDC items, PDC exceptie, PoC)
- Aan het einde van de rfi fase wordt middels het **beslisformulier** bepaald of een Ontwikkeling wordt toegevoegd aan de Project Portfolio Roadmap
- In de **rfp fase** (C-nummer) worden **PID, PSA en offerte** opgesteld
- Een offerte (C-nummer) voor Ontwikkelingen wordt uitsluitend aangevraagd door de **Projecten en Programma Manager**

De SPM cirkel



Bijlage D Technische specificatie

In **Figuur 59 tot en met 61** is een overzicht van technische specificaties van de verschillende netwerkdiensten weergegeven. Deze zijn opgedeeld in Beschikbaarheid, Capaciteit en Prestaties.

Technische specificatie Netwerkdiensten - Beschikbaarheid				
Dienst	Beschikbaarheid	Service Window	Openstellingstijden SD	Storingshersteltijd in 95% van de gevallen
IDS/IPS	99,5 voor IDS, 99,9 voor IPS, 97% voor BAS	E 24 x 7	E 24 x 7	E4
FCoDWDM	99,999%	E 24 x 7	E 24 x 7	E4
Mail relay	99,95%	E 24 x 7	E 24 x 7	E4
Forward webproxy	99,95%	E 24 x 7	E 24 x 7	E4
VPN	99,999%	K8 tot E 24 x 7	E 24 x 7	E4
Virtual firewall	99,95%	E 24 x 7	E 24 x 7	E4
DDI	99,99%	E 24 x 7	E 24 x 7	E4
DMZ en DMZ Client	99,975%	E 24 x 7	E 24 x 7	E4
VPN aansluiting	Standaard 99,5%, Dubbel 99,8% Redundant 99,99%, Missiekritisch 99,999%	K8 tot E 24 x 7	E 24 x 7	K8 – E4
Draadloze VPN aansluiting	>99,7% (geen garantie)	Kantoortijden: 08:00 – 18:00	08:00 – 18:00 werkdagen	K8 – E4
Externe koppeling (beschikbaarheid excl. Internetverbinding)	97% IPSEC Verder gelijk aan VPN aansluiting	K8 tot E 24 x 7	E 24 x 7	K8 – E4 (exclusief Internetverbinding)
LAN aansluiting type Gebouw/ type SPAN	99,5% standaard en 99,95% redundant	K8 tot E 24 x 7	E 24 x 7	K8 – E4
LAN aansluiting type VC / RC	99,5% standaard en 99,95% redundant	K8 tot E 24 x 7	E 24 x 7	K8 – E4
LAN aansluiting type CVR / VOR	99,99% redundant over 2 switches	E 24 x 7	E 24 x 7	E4
LAN aansluiting type Weg- en Waterkant	>99,7% standaard >99,8% redundant	E 24 x 7	E 24 x 7	E4
LAN aansluiting type KA LAN incl. callcenter	99,5% standaard en 99,95% redundant	K8 tot E 24 x 7	E 24 x 7	K8 – E4
WIFI	99,5% (radiodekking)	Kantoortijden: 08:00 – 18:00	E 24 x 7	K8
Open WIFI	99% (centrale omgeving)	Kantoortijden: 08:00 – 18:00	E 24 x 7	K8
LAN aansluiting type ODC	99,5% standaard 99,95% redundant over 2 switches	E 24 x 7	E 24 x 7	E4
Digitale Video aansluiting	99,7%	Kantoortijden: 08:00 – 18:00	E 24 x 7	E8
Draadloze aansluiting	99,5%	E 24 x 7	E 24 x 7	E4
MiniFEP	99,5%	10:00 – 15.00	E 24 x 7	E4
Remote Access groepsprofiel	99,95%	Kantoortijden: 08:00 – 18:00	E 24 x 7	K4 - E4
AAA	99,5%	E 24 x 7	E 24 x 7	E4

Figuur 59: Overzicht Technische specificaties - Beschikbaarheid

Technische specificatie Netwerkdiensten					
Capaciteit					
Dienst	# opdrachten (N) / # gebruikers	# Objecten in Database	Responsetijd	Throughput	
FCoDWDM	X	X	X	<= 8Gbps	X
Mail relay	Max. 10.000 e-mailgebruikers Bericht minimaal 6 uur in queue bij verstoring, na 72 uur hard bounce	X	X	Max. 50.000 e-mails/10GB per uur	X
Forward webproxy	Max. 10.000 gebruikers	X	X	X	X
VPN	X	X	X	<= 10Gbps	X
Virtual firewall	X	X	X	<= 10Gbps	X
DDI (DNS, DHCP, IPAM, Gedelegeerd beheer)	Centrale DNS: max. 25.000 / sec Gedelegeerd beheer: max. 10 gelijktijdige beheerders Centrale DHCP: max. 200 / sec	DNS centraal: max. 440.000 IPAM: max. 3.000.000 DHCP centraal: max. 440.000	DNS: <= 25ms DHCP: <300ms	X	X
DMZ en DMZ Client	X	X	X	<= 10Gbps	X
VPN aansluiting	X	X	X	Afhankelijk van gekozen bandbreedte	X
Externe koppeling	X	X	X	IPsec: Max. Ca. 50Mbps Vaste verbinding: 10Mbps, 100Mbps, 200Mbps, 500Mbps, 1Gbps	X
LAN aansluiting type Gebouw	X	X	X	Afhankelijk van gekozen bandbreedte	X
LAN aansluiting type VC / RC	X	X	X	Afhankelijk van gekozen bandbreedte	X
LAN aansluiting type CVR / VOR	X	X	X	Afhankelijk van gekozen bandbreedte	X
LAN aansluiting type Weg- en Waterkant	X	X	X	<= 1Gbps	X
LAN aansluiting type KA LAN incl. callcenter	X	X	X	Geldend voor aangesloten systemen <= 100 Mbps of <= 1Gbps of	X

				<= 2*1Gbps (Server/ Blade)	
WIFI	X	X	X	Per client minimaal 5Mbps Per AP maximaal 1Gbps	X
Open WIFI	Max. 1.000 gelijktijdige gebruikers over alle betrokken locaties samen	X	X	X	X
LAN aansluiting type ODC	X	X	X	Geldend voor aangesloten systemen <= 100 Mbps of <= 1Gbps standaard of <= 2Gbps (Server/ Blade) redundant <= 4Gbps (Server/ Blade) redundant <= 10Gbps standaard (Server / Blade) <= 20Gbps (Server / Blade) redundant <= 40Gbps (Server / Blade) redundant	X
AAA	X	X	X	<= 1Gbps	X

Figuur 60: Overzicht Technische specificaties - Capaciteit

Technische specificatie Netwerkdiensten						
Prestaties						
Dienst	Convergentiesnelheid	MTU	Packet loss	Delay (RTT) / Latency	Jitter	Multicast
FCoDWDM	X	2148 bytes (2048 bytes payload)	< 1 packet in 100 000 000	Afhankelijk van afstand, typisch <0,1 ms	Delay+jitter < max delay	X
VPN	< 10 sec bij lijnstoringen < 60 sec bij hw storingen < 2 min. Bij draadloze VPN aansluiting	4.470 Bytes (1.500 voor aansluitingen) en 1.260 bij Draadloze VPN	0% bij commerciële transmissie en RWS Glas n.a. bij mobiel	< 10ms	< 10ms	optioneel
Virtual firewall	<= 1 sec	1.500 bytes	0%	< 10ms	X	X
Internet access	<= 180 ms	1.500 bytes en 1.260 bij Draadloze VPN	t/m 1e transit provider <= 0,5%	t/m 1e transit provider: op AMX : <= 10ms Europa: <= 40ms Europa-trans-Atlantisch: <= 95ms		X
DMZ en DMZ Client	X	1.500 bytes	0%	< 10ms	Delay+jitter < max delay	X
VPN aansluiting		1.500 bytes	<= 0,01%	< 10ms bij gebruik RWS glas < 10 ms bij ON2013 en >= 100Mbps < 30 ms bij ON2013 en < 100Mbps	Delay+jitter < max delay	Optioneel
Draadloze VPN aansluiting	< 2 min.	1.260 bytes	X		Delay+jitter < max delay	X
Externe koppeling	< 10s bij redundant	1.500 Bytes 1.436 bij IPsec	0,01% Geen garanties bij verbindingen via Internet	IPsec: Afh. van bandbreedte, ca 100ms Vaste verbinding: < 10ms bij gebruik RWS glas < 10 ms bij ON2013 en >= 100Mbps < 30 ms bij ON2013 en < 100Mbps.	Delay+jitter < max delay	X
LAN aansluiting type CVR / VOR	< 60sec	1.500 Bytes	< 2%	< 2ms	Delay+jitter < max delay	Ja
LAN aansluiting type Weg- en Waterkant	Enkele seconden	1.500 Bytes	0%	< 10ms	Delay+jitter < max delay	Ja
LAN aansluiting type KA LAN incl. callcenter	< 10sec	1.500 Bytes	< 2%	< 10ms	Delay+jitter < max delay	Ja
WIFI	Centraal <30sec	1.500 Bytes	<=1%	<=5msec binnen radiodomein	<=2msec binnen radiodomein	X
LAN aansluiting type ODC	< 10sec	1.500 Bytes	< 2%	< 10ms	Delay+jitter < max delay	Ja

Figuur 61: Overzicht Technische specificaties – Prestaties

Bijlage E SLA Matrix storingshersteltijden verstoord / onderbroken

In **Figuur 62** is een overzicht van de storingshersteltijden van de verschillende netwerkdiensten weergegeven. Hierbij wordt onderscheid gemaakt tussen verstoorde en onderbroken dienstverlening. De dienstverlening is verstoord wanneer de functionaliteit onveranderd beschikbaar is ondanks een gedeeltelijke verstoring van de dienst (bijvoorbeeld het wegvallen van het redundante pad) . Bij onderbroken dienstverlening is er sprake van merkbaar wegvallen van functionaliteit (onbeschikbaarheid).

SLA Matrix storingshersteltijden									
	Storingshersteltijd in 95% van de gevallen								
	verstoord					onderbroken			
	Service Window 'Kantoortijden' in kantooruren			Service Window '24/7' in klokuren		Service Window 'Kantoortijden' in kantooruren		Service Window '24/7' in klokuren	
Diensten	K16	K8	K4	E8	E4	K8	K4	E8	E4
IDS / IPS				√					√
NAC (centrale omgeving)		√					√		
DWDM				√					√
Mailrelay				√					√
Forward webproxy				√					√
VPN		√		√		√			√
Virtual firewall				√					√
DDI - DHCP & DNS*				√					√
DDI - IPAM				√					√
DMZ en DMZ Client				√					√
VPN aansluiting				√			√		√
Draadloze VPN aansluiting				√					√
Externe koppeling	√					√			
LAN aansluiting type Gebouw	√			√			√		√
LAN aansluiting type Rekencentrum	√			√					√
LAN aansluiting type SPAN	√			√			√		√
LAN aansluiting type CVR/VOR				√					√
LAN aansluiting type Callcenter				√					√
LAN aansluiting type Wegkant/Waterkant				√					√
LAN aansluiting type ODC				√					√
KA LAN				√			√		√
WIFI		√				√			
Open WIFI		√				√			
Digitale Video aansluiting				√					√
MiniFEP				√					√
Remote Access groepsprofiel				√					√
AAA		√					√		
PPP aansluiting*									
TBMS BUS*									
Draadloze aansluiting*									
LEG EPL				√					√
CCM aansluiting				√					√

verstoord: de dienstverlening is beschikbaar met beperkte functionaliteit. SLA parameters kunnen afwijken (bijvoorbeeld bij wegvallen redundantie)

onderbroken: de dienstverlening is niet beschikbaar, er is een merkbare verstoring

**: op basis van 'redelijke effort'*

Figuur 62: SLA Matrix storingshersteltijden verstoord/onderbroken