

Netwerkdiensten

1	NETWERKDIENTEN	4
1.1	OMSCHRIJVING VAN DE NETWERKDIENTEN	4
1.1.1	<i>WAN netwerkindegratie en Cloud/Internet connectiviteit</i>	4
1.1.2	<i>LAN/WLAN connectiviteit</i>	5
1.1.3	<i>VO brede netwerkfunctionaliteiten en monitoring</i>	5
1.1.4	<i>Netwerkbeveiligingsfunctionaliteiten voor de rechtstreeks op de netwerken van de Vlaamse overheid aangesloten systemen.</i>	6
1.2	MEERWAARDEN VOOR DE KLANTEN.....	7
1.3	OMSCHRIJVING VAN DE VERDERE CONCRETISERING VAN DE ONDERSTEUNENDE PROCESSEN EN SYSTEMEN VOOR DIT DIENSTENPAKKET.....	8
1.4	OVERZICHT VAN DE NETWERKDIENTEN	13
1.4.1	<i>Uitbating van de netwerkomgeving</i>	13
1.4.1.1	Scope en doel.....	13
1.4.1.1.1	Exploitatie van de VO-WAN backbone omgeving	13
1.4.1.1.2	Exploitatie van de bestaande VO-WAN aansluitingen	13
1.4.1.1.3	Exploitatie van de beveiligde aansluitingen van partner netwerken op het VO-netwerk	15
1.4.1.1.4	Exploitatie van de connecties tussen VO-WAN en het internet.....	16
1.4.1.1.5	Exploitatie van de centrale netwerk- en beveiligingsdiensten.....	17
1.4.1.1.6	Exploitatie van de LAN/WLAN omgeving.....	19
1.4.1.2	Geconcretiseerd door.....	21
1.4.1.3	SLA	22
1.4.1.3.1	Beschikbaarheid van de VO-WAN backbone omgeving	22
1.4.1.3.2	Round trip delay van de VO-WAN backbone omgeving	23
1.4.1.3.3	Pakketverlies binnen de VO-WAN backbone omgeving	24
1.4.1.3.4	Jitter van de VO-WAN backbone	24
1.4.1.3.5	Beschikbaarheid van de WAN-aansluiting per Site	25
1.4.1.3.6	Round trip delay van de WAN-aansluiting per Site	26
1.4.1.3.7	Pakketverlies van de WAN-aansluiting per Site	27
1.4.1.3.8	Jitter van de WAN-aansluiting per Site	28
1.4.1.3.9	Beschikbaarheid van de beveiligde aansluitingen van partner netwerken op het VO-netwerk	29
1.4.1.3.10	Beschikbaarheid van de Internet connectiviteit.....	30
1.4.1.3.11	Beschikbaarheid van de centrale netwerk- en beveiligingsdiensten.....	31
1.4.1.3.12	Hersteltijd LAN/WLAN componenten	32
1.4.1.4	Prijsmechanisme.....	34
1.4.1.5	Facturatie	36
1.4.1.6	Rapportering.....	36
1.4.2	<i>Werkaanvragen m.b.t. de netwerkomgeving</i>	38
1.4.2.1	Scope en doel.....	38
1.4.2.1.1	Werkaanvragen m.b.t. het aanmaken, wijzigen of verwijderen van filtering van internetverkeer.....	38
1.4.2.1.2	Werkaanvragen m.b.t. het controleren van het internetgebruik binnen de ICT-code	38
1.4.2.1.3	Werkaanvraag voor het aanmaken/verwijderen van een draadloos internetaccount (VO-Werknemer).....	39
1.4.2.1.4	Werkaanvraag voor het aanmaken/wijzigen of verwijderen van een DNS record	40
1.4.2.1.5	Werkaanvraag voor het aanpassen van datastromen op een klantelijke firewall	40
1.4.2.1.6	Werkaanvragen voor het patchen van netwerkaansluitingen (1 tot 5) op éénzelfde verdieping	40
1.4.2.1.7	Werkaanvraag voor het aanpassen van de configuratie van een switchpoort.....	41
1.4.2.2	Geconcretiseerd door.....	41
1.4.2.3	SLA	41
1.4.2.3.1	Tijdige uitvoering van éénmalige Diensten.....	41
1.4.2.4	Prijsmechanisme.....	43
1.4.2.5	Facturatie	43
1.4.2.6	Rapportering.....	43
1.4.3	<i>Ondersteuning in regie m.b.t. de netwerkomgeving</i>	44
1.4.3.1	Scope en doel.....	44
1.4.3.2	Geconcretiseerd door.....	45
1.4.3.3	SLA	45
1.4.3.4	Prijsmechanisme.....	45
1.4.3.5	Facturatie.....	45
1.4.3.6	Rapportering.....	45
1.4.4	<i>Infrastructuurprojecten m.b.t. de netwerkomgeving</i>	45
1.4.4.1	Scope en doel.....	45
1.4.4.2	Geconcretiseerd door.....	47

1.4.4.3	Uitvoering.....	49
1.4.4.3.1	Werkaanvraag voor opmaken van een Projectvoorstel	49
1.4.4.3.2	Werkaanvraag voor uitvoering van een Project of projectfase	50
1.4.4.3.3	Werkaanvraag voor de bestelling van een projectwijziging	51
1.4.4.4	SLA	52
1.4.4.4.1	Tijdige uitvoering van Projecten	52
1.4.4.5	Prijsmechanisme	52
1.4.4.6	Prijscorrectie.....	55
1.4.4.7	Facturatie	55
1.4.4.8	Rapportering	55
1.5	TRANSITIE.....	56
1.5.1	<i>Initiële Transitie</i>	<i>56</i>
1.5.2	<i>Deeltransitie tijdens de duur van de Overeenkomst.....</i>	<i>59</i>
1.6	EXIT.....	59
1.6.1	<i>Maatregelen bij het beëindigen van de overeenkomst.....</i>	<i>59</i>
1.6.2	<i>Deelexit tijdens de duur van de Overeenkomst</i>	<i>60</i>

1 Netwerkdiensten

1.1 Omschrijving van de netwerkdiensten

Het Dienstenpakket netwerken bestaat uit verschillende Dienstenpakketten die de connectiviteit tussen verschillende locaties van de Vlaamse overheid en het transport van data mogelijk maken op een beveiligde, performante manier volgens de afgesproken beschikbaarheidspercentages.

Een aantal grote principes zijn van toepassing op alle netwerkdiensten en alle Projecten die in het kader van de netwerkdiensten worden uitgevoerd:

- Own-Fiber First: Waar mogelijk wordt geopteerd voor Vlaams glas boven commerciële bandbreedtes;
- Fysiek gedeeld, logisch gescheiden voor wat betreft netwerken in VO gebouwen (in beheer van het Bestuur);
- Ondersteunen van Cloud First strategie;
- Inzet op innovatie (evolutie naar Software Defined, innovatieve technologie, ondersteunen IOT, enz...);
- meer autonomie, een modulariteit van netwerkdiensten voor Entiteiten.
- Inzet op duurzaamheid.

Dit Dienstenpakket wordt aangeboden aan alle Klanten zoals opgenomen in de definitie van Klantenbereik in het Basiscontract. Er is geen verplichte afname met betrekking tot de Dienstenpakketten in deze Service Portfolio.

Het 'hoog' beschikbaar houden van de centrale netwerk- en beveiligingsdiensten is ook één van de belangrijke pijlers en vergt een centrale netwerk twin-DC setup voor netwerk- en beveiligingsapparatuur die van A tot Z volledig redundant is uitgebouwd.

Een belangrijke uitvoeringsmodaliteit van de in deze Service Portfolio voorziene Dienstenpakketten betreft de toepassing, bij de verwerking van Persoonsgegevens door de ICT-Dienstverlener als verwerker (zoals bedoeld in de AVG), van passende technische en organisatorische maatregelen (zie Basiscontract rubriek 6.8.3.) die voldoende garanties bieden dat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkenen is gewaarborgd. Minstens zullen daarbij de adviezen van de Commissie voor de Bescherming van de persoonlijke Levenssfeer/Gegevensbeschermingsautoriteit als leidraad worden genomen.

De Vlaamse overheid beschikt over haar eigen op Vlaams glas gebaseerde backbone, die de meest relevante gebouwen bestrijkt. Onder het motto fysiek gedeeld, logisch gescheiden wordt voor de decentrale VO locaties gestreefd naar een architectuur die meer aansluit bij de snelle evolutie in gebruikerstoestellen (van verschillende types) en hun gebruikservaring (rekening houdend met geografische plaats van de Gebruiker op het moment, multi device, mobile first,...). De netwerkdiensten en beveiligingsdiensten moeten toelaten om op elk ogenblik en via diverse toegangskanalen (vaste verbindingen, draadloze verbindingen (publieke en private Wifi), mobiele dataverbindingen, internet, ...) en vanaf meerdere types toestellen (smartphones, tablets, laptops, desktop, werkstations..., eigendom van de werkgever of van de werknemer; al dan niet in eigen beheer, IOT assets, ...) een veilige toegang te krijgen tot de bedrijfstoepassingen en bedrijfsdata of andere toepassingen toegankelijk via het private netwerk en/of het Internet, kortom anytime, anywhere, anydevice.

De netwerkdienstverlening is gebaseerd op vier domeinen die hier kort besproken worden.

1.1.1 WAN netwerkintegratie en Cloud/Internet connectiviteit

Dit domein betreft het mogelijk maken van IP connectiviteit van het Wide Area Netwerk van de Vlaamse overheid (VO WAN) en het intelligent transport van data op IP niveau op een efficiënte en performante manier :

- tussen de verschillende locaties van de Vlaamse overheid (VO) en de door de VO gebruikte traditionele datacenters onderling middels een privaat IP backbone - op Vlaamse bodem - waarbij onderliggende glasvezels en belichtingen (xWDM) door het Agentschap Wegen en Verkeer zullen worden aangeleverd en uitgebaat. Voor VO locaties waar geen eigen glasvezel mogelijk of wenselijk is, wordt beroep gedaan op gehuurde lijnen via een commercieel beschikbare WAN operator;
- naar het Internet (High Capacity Internet connectiviteit);
- naar diverse Cloud platformen;

Het 'hoog' beschikbaar houden van de backbone infrastructuur en de centrale netwerk- en beveiligingsdiensten is één van de belangrijke pijlers en vergt een design die volledig redundant is uitgebouwd, zowel on-prem als in de cloud. Voor de backbone en centrale infrastructuur wordt derhalve een hoge beschikbaarheid (24/24 7/7 en voorzien van de nodige ontdubbelde infrastructuur) en capaciteit voorzien. Daarnaast wordt per Site het gepaste niveau van beschikbaarheid en capaciteit aangeboden via verschillende types van aansluitingen.

Verder wordt er een disaster recovery (DR) oplossing voorzien ingeval totale onbeschikbaarheid van het primaire knooppunt (thans in Nossegem) door een (zware) calamiteit. De site redundantie wordt opgezet op een tweede locatie namelijk in Antwerpen, met name het datacenter van het Vlaams verkeerscentrum. Deze oplossing wordt beschreven in de Disaster recovery procedure die maandelijks up to date gehouden wordt. Het herstellen van volgende basisfuncties is voorzien binnen de 4 uren:

- Netwerk authenticatie
- Internet toegang (DNS / DHCP)
- De WLAN controller
- Security functies voor alle netwerk trafiek (F5, Palo Alto inclusief telewerkkfunctie)
- Belangrijke partner koppelingen (ontdubbeld op DR-site bv. Proximus, Muisen-VPC).

Deze oplossing zal geleidelijk aan evolueren naar een meer actief-actief setup voor de meeste netwerk en beveiligingsdiensten. Voor deze diensten zal dan geen DR procedure meer van toepassing zijn.

De netwerkdiensten worden geleverd conform afgesproken dienstverleningsniveaus.

1.1.2 LAN/WLAN connectiviteit

Dit domein omvat de onderdelen van een intelligent en geautomatiseerd VO breed campus LAN & WLAN netwerk voor alle gebouwen van de Vlaamse overheid:

- Dynamisch opzetten van segmentatie tussen verschillende Gebruikers en toestellen (concept van één fysiek gedeeld, logisch gescheiden netwerk);
- Netwerk Access Controle (NAC) op basis van 802.1x (alsook waar nodig MAC authentication bypass) en gecentraliseerde RADIUS;
- Laagdrempelige oplossing voor bezoekers in de gebouwen van de VO, met authenticatie, logging en afdoende beveiliging tegen misbruik.

De DC LAN netwerk technologie voor de on-prem Netwerk-DC's (verder gerefereerd als netwerk knooppunten) is gebaseerd op Software Defined Networking (SDN).

1.1.3 VO brede netwerkfunctionaliteiten en monitoring

Dit domein omvat volgende onderdelen:

- Het verzekeren van basis VO brede netwerkfunctionaliteiten met actieve apparatuur zoals Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), IP adres Management (IPAM) en Network Time Protocol (NTP). Deze services worden door VO als uiterst kritisch ervaren, de opzet ervan dient derhalve volledig hardwarematig en softwarematig redundant en hardware 'appliance' based te zijn.
- Het voorzien van een Netwerk Performance monitoring met volgende vereisten:
 - een permanent en globaal (in)zicht op de communicatiestromen van en naar verschillende omgevingen en zones;
 - het kunnen positioneren van metingen ten aanzien van een zelf aangeleerde baseline waarde (die weergeeft wat de waarde is onder "normale omstandigheden") en dus afwijkingen en trends hierop kan rapporteren;
 - een instrument voor 'ad hoc troubleshooting' en onweerlegbare afbakening van het probleemdomein;
 - een mogelijkheid om concrete realtime en historische detail-analyses te kunnen maken op vlak van specifiek te onderzoeken toepassingen, servers of gebruikers;
 - virtuele probes binnen een cloud context.

1.1.4 Netwerkbeveiligingsfunctionaliteiten voor de rechtstreeks op de netwerken van de Vlaamse overheid aangesloten systemen.

De aan de netwerkdiensten gekoppelde netwerkbeveiligingsfunctionaliteiten om een veilige toegang en afscherming te verzekeren zijn mee opgenomen in de scope van dit Dienstenpakket.

Dit omvat:

- Next-generation firewall functionaliteit binnen on-prem VO omgevingen om netwerken in zones op te kunnen delen en van elkaar te scheiden. Deze bescherming omvat zowel 'stateful firewalling' als Intrusion Prevention System (IPS) en advanced anti-malware beveiliging (Advanced Threat Protection (ATP)/Sandboxing), en dient zowel user als application aware te zijn (waarbij VO de mogelijkheid wenst te hanteren om security policy's op te bouwen op basis van applicaties);
- De ICT-Dienstverlener dient in het kader van technologische evolutie de mogelijkheid te voorzien dat Forward proxy diensten voor outbound verkeer met inbegrip van Secure Socket Layer (SSL) inspectie in de toekomst zullen uitgerold worden, thans binnen de on-prem netwerk knooppunten, op termijn in de cloud.
- Loadbalancing & Web Application Firewall (WAF) functionaliteit, voor wat betreft toepassingen in VPC overgangszone (in afbouw) of gerelateerd aan netwerk en beveiligingsbeheer binnen de on-prem netwerk knooppunten. Naargelang het geval, toegang tot interne applicaties en resources kunnen bieden en tegelijk de werklust te verdelen en de beschikbaarheid ervan te waarborgen en, naargelang het geval, de applicatie-inhoud te filteren tegen frauduleuze aanvragen;
- Transparante en portaal gebaseerde SSL VPN diensten met authenticatie afwikkeling;
- Distributed Denial Of Service (DDOS) functionaliteit ter bescherming van de eigen public IP ranges, voornamelijk in gebruik binnen de netwerk knooppunten, dewelke gedrags-sensitief is en bescherming biedt ten aanzien van (zelf aangeleerde) baseline waarden met voldoende garanties om het aantal "false positives" te minimaliseren.

1.2 Meerwaarden voor de Klanten

Met de netwerkdiensten worden ten behoeve van de Klanten de volgende meerwaarden nagestreefd:

- Hoge beschikbaarheid van de WAN netwerk dienstverlening 24/24 7/7 voorzien van de nodige redundantie en failover-systemen;
- Een performante en technologisch up-to-date WAN en LAN/WLAN (met voldoende bandbreedte en capaciteit) ter ondersteuning van het uitwisselen van digitale informatie tussen de Entiteiten onderling en tussen de Entiteiten en hun klanten. Dit performant netwerk moet toelaten om antwoorden te formuleren op toekomstige uitdagingen;
- Hoge beschikbaarheid van de LAN/WLAN netwerk dienstverlening tijdens Uitgebreide Kantooruren voorzien van de nodige redundantie en failover-systemen met verschillende beschikbaarheidsopties afhankelijk van de grootte van de locatie;
- Een goede beveiliging en afscherming van het internet; bescherming tegen cybersecurity aanvallen van de volgende generatie (mogelijkheden tot ATP/Sandboxing, SSL decryptie, aDDOS..) Een intelligente en geautomatiseerde VO netwerk omgeving op basis van het software defined principe, die een effectievere en flexibelere manier van werken kan mogelijk maken en die nieuwe Projecten (vb in de context van IOT) op een productievere/snellere wijze weet op te leveren en eventuele problemen snel kan tackelen, dus kortere implementatie door hogere operationele efficiëntie;
- Maximaal gebruik van gemeenschappelijke omgevingen (o.a. gebruik van Vlaamse glasvezelbekabeling) om de kostprijs voor de Klanten zo laag mogelijk te houden;
- De Vlaamse overheid wenst in het kader van deze Raamovereenkomst bij te dragen aan duurzaamheid en verwacht van de ICT-Dienstverlener dat hij een beleid inzake Maatschappelijk Verantwoord Ondernemen (MVO) ontwikkelt en uitvoert. De ICT-Dienstverlener geeft daarom in zijn Serviceorganisatie aan welke MVO-maatregelen hij neemt en hoe die bijdragen tot de duurzame uitvoering van de Diensten beschreven in deze Service Portfolio. De ICT-Dienstverlener is als professionele onderneming het best geplaatst om te identificeren welke MVO-elementen voor de aangeboden Diensten het meest relevant zijn en de grootste duurzaamheidswinsten en maatschappelijke meerwaarde kunnen genereren;
- Een performante monitoring van de beheerde netwerkomgeving en een efficiënte behandeling van eventuele Incidenten en Problemen;
- De netwerkdiensten en de erin opgenomen beveiligingsdiensten moeten toelaten om op elk ogenblik en via diverse toegangskanalen (vaste verbindingen, draadloze verbindingen (publieke en private Wifi), mobiele dataverbindingen, internet (VPN), ...) en vanaf meerdere types toestellen (smartphones, tablets, laptops, ..., eigendom van de werkgever of van de werknemer; al dan niet in eigen beheer, ...) een veilige toegang te krijgen tot de bedrijfstoepassingen en bedrijfsdata, kortom anytime, anywhere, anydevice;
- Segmentatie, mogelijkheid voor de Entiteiten om een apart virtueel netwerk af te nemen binnen het gemeenschappelijke fysieke netwerk;
- Transparante prijszetting met duidelijke opgaven van de kostencomponenten;
- Optimalisatie van exploitatie kosten door gebruik te maken van SDN technologie;
- Snelle evolutie mogelijk op vlak van IOT en de groei aan diversiteit binnen de gebruikers omgevingen;
- Maximale integratie met andere VO-Entiteiten;
- Verlaging van de administratieve lasten voor het uitvoeren van Projecten;
- Schaalvoordelen op het vlak van prijs en kwaliteit en gebruik van beste praktijken m.b.t. het realiseren van een Project;
- Professionele dienstverlening, via de inzet van getraind en bekwaam technisch personeel ook voor aan de exploitatieomgeving gerelateerde Projecten, en specifiek voor Projecten

het samenwerken met bekwame projectmanagers die op een methodologisch verantwoorde manier de beoogde projectresultaten behalen.

- Geïntegreerde processen, rapporten, bestellingen en facturatie;
- Uitvoeren van Projecten in overeenstemming met algemeen geldende beste praktijken (bv. PRINCE2).

1.3 Omschrijving van de verdere concretisering van de Ondersteunende processen en systemen voor dit dienstenpakket

De algemene procesvereisten en vereisten voor de Gemeenschappelijk Ondersteunende Systemen zijn opgenomen in het contractuele document "Vereisten Ondersteunende processen en overlegfora". Hieronder zijn meer gedetailleerde vereisten opgenomen specifiek voor het Dienstenpakket "Netwerken".

De Vlaamse overheid (VO) heeft de jongste jaren haar netwerk op een niet aflatende wijze dienen aangepast aan de steeds veranderende behoeften in diverse contexten zoals meer digitalisering, toename van IAAS / SAAS gebaseerde toepassingen, de introductie van het nieuwe werken, mobiel werken, cloud diensten, bescherming tegen een hogere graad van (cyber)bedreigingen, Om aan al deze veranderingen tegemoet te komen is het noodzakelijk dat er een nauwe samenwerking is van het Bestuur met alle ICT-Dienstverleners en dat er ook tussen de ICT-Dienstverleners onderling een goede samenwerking en communicatie wordt opgezet.

Het Bestuur is voor de meeste bouwstenen de design authority en bijgevolg verantwoordelijk voor het architectuurbeheer. Van de ICT-Dienstverlener wordt verwacht dat hij het proces architectuurbeheer ondersteunt door advies en ondersteuning bij het opstellen van nieuwe architectuur. Verder wordt verwacht dat hij zorgt voor de verwerking tot een TO-BE design en de realisatie van de operationele uitvoering via Projecten.

Naast de netwerkdienstverlening zal de ICT-Dienstverlener moeten afstemmen met de ICT-Dienstverlener die de integratiediensten levert in het kader van deze Overeenkomst. De ICT-Dienstverlener voor de netwerkdiensten zorgt samen met de ICT-Dienstverlener voor de Integratiediensten voor een vlotte samenwerking m.b.t. processen, procedures en tools (bv. Interfacing tussen de tools voor afhandelen van Incidenten en Problemen, het Klachtenbeheer, Communicatiebeheer, SLA rapportering, ...). De kost voor de eventueel vereiste aanpassingen langs de kant van de ICT-Dienstverlener voor netwerken ten gevolge van wijzigingen in de ITSM-tool van de ICT-Dienstverlener voor de integratiediensten moet mee inbegrepen zijn in de forfaitaire prijzen. Enkel grotere wijzigingen zouden een apart te betalen Project mogen vereisen.

Daarnaast zal de ICT-Dienstverlener waar nodig ook samenwerken met de ICT-Dienstverleners voor andere Dienstenpakketten.

De nodige processen en procedures voor de nodige samenwerking en interactie met de integratiediensten, inclusief Servicedesk & overkoepelende security Diensten moeten opgenomen worden in de Serviceorganisatie. Zo moeten vanuit dit Dienstenpakket de nodige kennisartikelen en scripts aangeleverd worden aan de overkoepelende eerstelijns Servicedesk zodat Incidenten zo goed mogelijk in eerste lijn kunnen opgelost worden en indien dit niet mogelijk is, correct kunnen toegewezen worden aan de juiste tweede lijn.

De Vlaamse overheid zet in op duurzaamheid. De ICT-Dienstverlener beschrijft in de Serviceorganisatie hoe hij invulling geeft in de processen om een ICT-Dienstverlening te realiseren die rekening houdt met maatschappelijk en ethisch verantwoord en/of duurzaam ondernemen.

Vanuit dit Dienstenpakket moeten afstemming gebeuren i.v.m. de nodige datastromen naar een overkoepelende Security Information and Event Management (SIEM) die deel uitmaakt van de

Integratiediensten.

De ICT-Dienstverlener consolideert security logs van eigen bouwstenen (met focus op 'threat' gebaseerde correlatie op eigen bouwstenen) en stuurt gefilterde/relevante logs sturen naar SIEM van de Service Integrator (incl. definiëren van usecases). Ook voor Events stuurt de ICT-Dienstverlener zelf gegenereerde events – dei van toepassing zijn op zijn eigen omgeving, voor eigen operationele verantwoordelijkheid - door naar Service Integrator (middels principe van soort van subscr. op 'service event bus'). De Service Integrator verzamelt, interpreteert en correleert deze logs en events over de diverse ICT-Dienstverleners heen en zal op adequate en overkoepelende wijze reageren en rapporteren (globale views/dashboards).

De Service Integrator zal tevens verantwoordelijk zijn voor cross-domain architecturale (security) Governance Coördinatie en cross-domain settings (bijvoorbeeld in de context van zerotrust).

Wat 'cloud' betreft zal de (Netwerk) ICT-Dienstverlener alles wat beveiligde communicatie en routing betreft tot in en binnen de cloud 'Transit zone' voor zijn rekening nemen (Direct Connect, ExpressRoute, routing naar VONET, naar Forward proxy etc.) inclusief inter-cloud WAN verbindingen en IPSEC. Dit omvat eveneens het invullen van requests van klanten om flows/NAT tussen applicaties van diverse Entiteiten mogelijk te maken.

Vanuit de Transit zones worden verbindingen opgezet naar de diverse IAAS/PAAS cloud zones. De routing en beveiliging van toepassingen binnen deze (Applicatie) zones valt niet onder de verantwoordelijkheid van de (Netwerk) ICT-Dienstverlener.

Volgende aspecten behoren tot de scope van de netwerkdiensten:

- De tweede lijn Service Desk voor het oplossen van Incidenten en Problemen m.b.t. de netwerkdiensten en de aan het netwerk gekoppelde beveiligingsdiensten (Incident management). De eerste lijn Service Desk zit bij de ICT-Dienstverlener voor de Intergratiediensten. De ICT-Dienstverlener geeft de gepaste prioriteit aan de Incidenten die via de eerste lijn doorgegeven worden of die automatisch gegenereerd worden via alarmen uit de monitoring tools, om voor de in deze Service Portfolio beschreven Diensten de SLA's te garanderen. Dit omvat eveneens het voorzien van een wachtdienst voor het garanderen van de overeengekomen dienstverleningsniveaus met betrekking tot de netwerkdienstverlening.
- Het oplossen van Problemen in het kader van de netwerkdiensten en de aan het netwerk gekoppelde beveiligingsdiensten d.m.v. "proactief probleembeheer" o.b.v. monitoring. Verder voert de ICT-Dienstverlener een root cause analyse uit, voert de nodige Correctieve acties uit en legt Proactieve Verbetervoorstellen voor aan de Klant. (Problem management).
- Voorstellen doen en adviezen geven in het kader van het opstellen van een roadmap voor het Dienstenpakket netwerken in het kader van Service Portfolio Management. De visie en architectuur wordt bepaald door het Bestuur maar van de ICT-Dienstverlener wordt verwacht dat hij voorstellen doet voor Projecten (grotere wijzigingen) of aanpassingen in regie (kleinere wijzigingen) om op basis van een roadmap de netwerkdienstverlening te laten evolueren in lijn met de vooropgestelde visie en architectuur.
- De monitoring van de voor de netwerkdiensten onderliggende infrastructuurcomponenten (zowel reactief als proactief) (o.a. appliances/routers/lijnen, ...). Dit zodat abnormaal hoog gebruik of inbreuken op de veiligheid snel gedetecteerd worden. Vanuit een centraal monitoring systeem worden alarmberichten uitgestuurd die automatisch Incidenten en Problemen melden als bepaalde alarmdrempels worden overschreden. (Eventmanagement).
 - Specifiek betreft het de monitoring (zowel performantie als beschikbaarheid) van o.a.
 - de datalijnen tussen VO-WAN en het internet;

- de betrokken netwerkcomponenten (routers, ..);
- de on-prem firewalls (externe Internet facing en internet);
- de infrastructuur die nodig is voor het beheer en de ondersteuning met betrekking tot centrale VPN infrastructuur voor de thuiswerkers;
- de infrastructuur die nodig is om vanuit het internet toegang te krijgen tot applicaties van Klanten op de VO-WAN om bepaalde beheerstaken (met admin bevoegdheid) uit te voeren;
- andere beveiligingsinfrastructuur die de ICT-Dienstverlener nodig acht om een beveiligde connectie tussen VO-WAN en internet te realiseren.
 - Het starten, stoppen en herstarten van de onderliggende infrastructuur indien nodig;
 - Het regelmatig nakijken en tunen van de onderliggende infrastructuur;
- Het up-to-date houden van de omgeving. Dit omvat het up-to-date houden van de software (patches). Dit conform de geldende normen i.v.m. Change Controle.
- Het vervangen van infrastructuur als onderdeel van Incidentmanagement in het kader van defecten. Het aankopen, leveren en installeren van nieuwe componenten (uitbreiding o.b.v. "Capacity en performance management" en vervanging van verouderde componenten) gebeurt op basis van afzonderlijke Projecten.
- De wijzigingen aan de interface ten gevolge van een major release van de Gemeenschappelijke Ondersteunende Systemen zijn inbegrepen in de Eenheidsprijzen.
- Het correct houden van de Configuratiebank m.b.t. de netwerkdiensten en de aan netwerk gekoppelde beveiligingsdiensten (Configuratiebeheer). De Inventaris (inclusief topologietekeningen) van de te beheren omgevingen, is opgenomen in de Inventaris en dient door de ICT-Dienstverlener te worden geactualiseerd in het kader van wijzigingen aan de ICT-dienstverlening.
- Het efficiënt en gecontroleerd uitvoeren van wijzigingen aan de netwerkomgeving die niet projectmatig moeten uitgevoerd worden (Change controle). De planning voor deze changes moet duidelijk zijn voor alle geïmpacteerde Klanten. Zo moeten Entiteiten met continudiensten de impact kunnen aflezen uit de communicatie en de planning van deze changes. Verder moet er ook een afstemming zijn m.b.t. deze changes met de ICT-Dienstverlener van de Integratiediensten zodat er een overzicht gehouden wordt over de verschillende raamcontracten heen m.b.t. het uitvoeren van wijzigingen. De ICT-Dienstverlener neemt ook deel aan de "Gemeenschappelijke Ondersteunende Systemen CAB" om de impact van wijzigingen aan de Gemeenschappelijke Ondersteunende Systemen of de eigen systemen en de interface ertussen tussen te bespreken.
- Het proactief voorstellen te doen om deze bestaande omgeving voldoende performant te houden (Capacity en performance management).
- Het proactief voorstellen doen om de bestaande omgeving te verbeteren (Continu verbeteren en innovatie). Aan de ICT-Dienstverlener wordt gevraagd om in zijn Serviceorganisatie concreet zijn visie op te nemen voor volgende toekomstige mogelijke ontwikkelpistes:
 - Het mogelijks (toekomstig) gebruik van Edge computing gedurende de looptijd van het contract. De volgende elementen dienen minimaal toegelicht te worden: summieri beschrijving van de oplossing, beveiliging, bandbreedte, dekking, tijdslijn / roadmap, ondersteunde sensoren, limitaties en kostindicaties.

- Het mogelijks (toekomstig) gebruik van LP-WAN gedurende de looptijd van het contract. De volgende elementen dienen aan bod te komen: summier beschrijving van de oplossing, beveiliging, bandbreedte, dekking, tijdslijn / roadmap, toevoegen business logica, lijst ondersteunde sensoren, beperkingen en kostindicaties.
- Tot op heden werd nog niet beslist wie de IOT sensoren zal leveren en beheren. Er zal eventueel fieldservice nodig zijn. De ICT-Dienstverlener zal hierover potentieel voor bevraagd worden.
- Het uitvoeren van capacity monitoring door de operationele performantie en verbruik van de resources van alle netwerk- en beveiligingcomponenten inclusief naar de Cloud omgevingen te meten en te monitoren. Capaciteitsuitbreidingsvoorstellen worden opgemaakt en voorgelegd aan de Klant.
- Het voldoende beschikbaar houden van de netwerkdiensten en de aan netwerk gekoppelde beveiligingsdiensten (Availability management). De ICT-Dienstverlener zorgt voor de nodige redundancy- en failover mogelijkheden om de gevraagde beschikbaarheid niveaus per Dienst te garanderen en single points of failure te vermijden;
- M.b.t. het proces “Beheer van sub-contracten en aankoop” wordt van de ICT-Dienstverlener verwacht dat hij minstens volgende activiteiten voorziet:
 - Het afsluiten (en tijdig verlengen/actualiseren) van de nodige (onderhouds)contracten om de netwerkdiensten en de aan netwerk gekoppelde beveiligingsdiensten te realiseren. Voor de voor deze Dienst nodige onderhoudscontracten en licenties zal de ICT-Dienstverlener aan de Klanten minstens 3-maandelijks een geactualiseerde lijst voorleggen met alle aan deze Diensten onderliggende contracten en licentieovereenkomsten met hun vervaldatum. Minstens 1 maand voor de vervaldag, of de dag waarop voor het bestaande contract de opzeg moet worden gegeven, wordt de Klant via mail op de hoogte gesteld dat een vernieuwing van een lopend contract in aantocht is. Deze mail bevat alle kostprijsinformatie zodat de Klant kan beslissen al dan niet te verlengen.
 - Het organiseren van marktbevragingen voor de huur van nieuwe datalijnen of infrastructuurcomponenten die projectmatig worden besteld met het oog op het bekomen van de voor de gevraagde datacapaciteit beste prijs/kwaliteit. De ICT-Dienstverlener dient voor nieuwe datalijnen en infrastructuur aan te tonen in het Projectvoorstel dat de op dat ogenblik voordeligste keuze wordt gemaakt. Dit kan gerealiseerd worden door een op dat ogenblik geldige marktbevraging.
- Het Beveiligingsbeheer m.b.t. de netwerkdiensten en de aan netwerk gekoppelde beveiligingsdiensten in lijn met de wettelijke en algemene ICT-veiligheidsrichtlijnen van de Vlaamse overheid. Dit kan o.m. bestaan uit volgende Diensten:
 - Bescherming tegen cybercriminaliteit via de uitbating en controle van de in scope zijnde veiligheidsbouwstenen (beschermen tegen externe aanvallen, misconfiguraties, PEN testing, alerting/response etc.).
 - De inrichting van bouwstenen zoals LOG-Management, Event management, Threat Intelligence en Threat hunting om de veiligheid van de ‘eigen’ in-scope zijnde bouwstenen te bewaken en te beheren; de ICT-Dienstverlener consolideert security logs van eigen bouwstenen met focus op 'threat' gebaseerde correlatie. Gefilterde/relevante logs dienen doorgestuurd te worden naar de SIEM van SI (incl. definiëren van usecases).
 - De nauwe samenwerking met het Bestuur en de externe ICT-Dienstverlener van de integratiediensten op het vlak van risicomangement & incident response;

- In de logs worden enkel Persoonsgegevens opgeslagen wanneer dit echt nodig is. De bepalingen hierover zijn opgenomen in het Basiscontract (hoofdstuk 3);
- Toegangscontroles en –restricties d.m.v. next generation firewalls;
- Preventieve en schadebeperkende maatregelen nemen tegen algemeen voorkomende bedreigingen die een gevaar vormen voor de integriteit van de informatie, zoals computervirussen, hacking-activiteiten, etc....;
- Schadelijke activiteiten voorkomen: niet geautoriseerde toegang voorkomen zoals hacking, evenals het onderscheppen van wachtwoorden, encryptiesleutels, of het aanwenden van om het even welk mechanisme dat niet geautoriseerde toegang mogelijk maakt;
- Een beveiligde interoperabiliteit tussen de Klanten andere overheden, de burger en de bedrijven;
- Een intrusiedetectie (IDS) en intrusie preventie (IPS) en Advanced Threat Protection functionaliteit incl. SSL decryptie en sandboxing technologie op alle verkeer van en naar het Internet;
- de restrictieregels (policy's) van de firewall actualiseren, onderhouden en controleren;
- de content- en URL-filtering op te volgen en te controleren met o.a. lijsten van de gebruikers en de zwarte en witte lijsten ('black & white-lists'), enz.;
- Een veilige toegang voor thuiswerkers (VPN);
- In lijn met de algemene ICT-veiligheidsrichtlijnen van de ICT-Dienstverlener wordt de (beheers)toegang tot de netwerkcomponenten sterk beveiligd en geregistreerd;
- Ongeoorloofde toegang tot de informatie in de netwerkcomponenten of tot de logs worden als Incident m.b.t. de ICT-beveiliging geregistreerd en behandeld.
- De disaster recovery (niet van toepassing voor de actief-actief diensten):
 - Maandelijks up-to-date houden van de Disaster recovery procedure inclusief alle kleine changes en personeelsveranderingen.
 - Opnemen van de nodige taken binnen netwerk en security projectvoorstellen om de Disaster Recovery procedure en het architectuur referentiedocument up to date te houden.
 - Meewerken aan de jaarlijkse Disaster recovery procedure test wanneer die via een project door de Klant wordt besteld.
- Het leveren van dashboards en rapporten voor het management, peergroepen en de technische teams met de status van de verschillende componenten. Via het dashboard kan men afhankelijk van de rol, detail rapporten raadplegen en steeds met de mogelijkheid om te groeperen per Entiteit.
- Het bewaken van de tevredenheid over de door de ICT-Dienstverlener geleverde Diensten conform het proces beschreven in het document "Vereisten Ondersteunende processen en overlegfora".
- Het opnemen in de operationele omgeving van bijkomende netwerkinfrastructuur nadat deze infrastructuur werd overgedragen vanuit projectwerking naar Exploitatie.
- Het voorzien van een meekijkfunctionaliteit (read only access) met volledige diepgang voor het Bestuur op alle voor netwerken beveiliging gebruikte monitoring-, opvolg- en beheersystemen (inclusief SDN beheerscomponenten).
- Het bijwonen van operationele overlegfora met het Bestuur om de processen, procedures en ICT-dienstverlening m.b.t. de netwerkdiensten continu te optimaliseren.

1.4 Overzicht van de netwerkdiensten

1.4.1 Uitbating van de netwerkgeving

1.4.1.1 Scope en doel

Voor de Exploitatie van de netwerkgeving zal de ICT-Dienstverlener de verschillende operationele betrokkenen (de medewerkers van de ICT-Dienstverlener, zijn Oderaannemers/Leveranciers en indien van toepassing de Entiteiten van de Vlaamse overheid die instaan voor de investering in de nodige infrastructuur. (glasvezelbekabeling, Lan bekabeling, ...)) aansturen om een kwalitatieve uitvoering te realiseren.

1.4.1.1.1 Exploitatie van de VO-WAN backbone omgeving

Deze dienstverlening omvat alle Diensten die nodig zijn om steeds over een veilig, performant en up-to-date gemeenschappelijk Wide Area Network voor de Vlaamse overheid (VO-WAN) te kunnen beschikken (exclusief de datalijnen naar de Sites).

De VO-WAN backbone staat in voor het transport van IP data – voornamelijk op Vlaamse bodem - tussen de verschillende VO locaties. Dit ter ondersteuning van het uitwisselen van digitale informatie tussen de Entiteiten onderling en tussen de Entiteiten en hun klanten, partners, burgers enz....

De VO-WAN backbone is het gemeenschappelijk Wide area netwerk (WAN) van de Vlaamse Overheid (VO). Deze VO-WAN bestaat uit een op MPLS technologie gebaseerde backbone infrastructuur. Deze heeft een capaciteit van 100Gbit/s. De huidige omgeving (P ("Provider") en PE ("Provider edge") routers) bestaat vooral uit CISCO-apparatuur. Voor de verbindingen wordt enerzijds gebruik gemaakt van een glasvezel bekabeling die eigendom is van de Vlaamse overheid, en anderzijds van gehuurde lijnen. Daar waar technisch mogelijk is kan gekozen worden voor de implementatie van QoS.

De VO-WAN backbone kan beschouwd worden als hoogperformante en hoogbeschikbare ruggengraat en dient te worden uitgebaut door de ICT-Dienstverlener (24/24 7/7).

Het kunnen (netwerkmatic) encrypteren van data op private WAN verbindingen is geen vereiste.

De ICT-Dienstverlener dient de VO-WAN backbone zoals hij deze heeft opgezet of overgenomen tijdens de Initiële Transitie te exploiteren en moet ook de nodige processen voorzien om uitbreidingen die projectmatig worden opgezet bij op te nemen in de exploitatieomgeving.

De dienstverlening omvat o.m. de inrichting van de onder 1.3 beschreven processen en activiteiten.

De Inventaris van de te beheren netwerkcomponenten is opgenomen in de Referentiebibliotheek. De VO-WAN Diensten worden geleverd conform de hierna beschreven dienstverleningsniveaus (zie paragrafen 1.4.1.3.1, 1.4.1.3.2, 1.4.1.3.3, 1.4.1.3.4).

Teneinde de VO-WAN up-to-date te houden zullen in overleg met het Bestuur in een meerjarenperspectief tijdig de nodige Projecten opgestart worden voor vernieuwing of uitbreiding. De Projecten worden uitgevoerd overeenkomstig de modaliteiten van het Dienstenpakket Projecten (zie 1.4.4).

1.4.1.1.2 Exploitatie van de bestaande VO-WAN aansluitingen

De scope van dit Dienstenpakket beperkt zich niet tot de verbindingen naar de VO-WAN maar omvat ook rechtstreekse verbindingen tussen Sites van Klanten en de datacenters van de ICT-Dienstverlener of zijn Oderaannemer (met uitzondering van het managed datacenter waarbij de ICT-Dienstverlener van het raamcontract van de datacenter Diensten instaat voor de connectiviteit naar het datacenter en de mainframe waar de ICT-Dienstverlener van het raamcontract voor de mainframediensten instaat voor de connectiviteit naar de VO-WAN).

De hoofdgebouwen van de Vlaamse overheid in de provincies (VAC's) zijn eveneens aangesloten op

het VO-WAN.

Voor wat betreft de gebouwen van de Vlaamse overheid wordt een onderscheid gemaakt afhankelijk van de grote van de Site:

- De grote Sites met twee gegarandeerde vaste lijnen naar twee verschillende IP POPs van de backbone (Type S1);
- De standaard Sites op basis van een gegarandeerde vaste lijn in combinatie met IPSEC over Internet broadband (Type S2);
- Kleine Sites op basis van één gegarandeerde vaste lijn (Type S3);
- Kleine Sites op basis van IPSEC over Internet broadband, inclusief 5G in de toekomst (Type S4);

Elk type Site heeft een het gepaste niveau van beschikbaarheid en capaciteit via verschillende types van aansluitingen, voorzien van de nodige redundantie en failover-systemen.

Voor de Sites S1 tot en met S3 dient het 'own fiber first' principe gerespecteerd te blijven. Voor de aansluiting van de (veelal iets grotere) gebouwen op het netwerk van de VO zullen de administratie Wegen en Verkeer van de Vlaamse overheid (AWV) en de ICT-Dienstverlener waar mogelijk blijven optreden als gezamenlijke uitbater van onderliggende access connectiviteit. Hierbij behoudt AWV de focus op de fysieke infrastructuur, voornamelijk glasvezel met inbegrip van de optische belichting op basis van WDM technologie (dus op Laag 2), en zal de ICT-Dienstverlener zich blijven toespitsen op het aanbieden van netwerkdiensten op IP niveau (Laag 3). Voor deze gebouwen blijft de doelstelling om gebruik te blijven maken van het Vlaamse glas gedurende de looptijd van de Overeenkomst zolang de kost lager blijft dan het commerciële aanbod voor dezelfde capaciteit. De topologie blijft steeds van het type 'dual star', m.a.w. deze locaties zullen op een redundante wijze middels punt-tot-punt L2 verbindingen worden gekoppeld aan twee (geografisch) verschillende IP POPs van de backbone.

Voor de gebouwen waar het niet opportuun of rendabel is om het Vlaamse glas binnen te trekken of uit te baten, zal de ICT-Dienstverlener een punt-tot-punt Laag 2 bandbreedte aanbieden (100 Mbit/s, 1Gbit/s, nx 1Gbit/s of 10 Gbit/s). De ICT-Dienstverlener kan hiertoe beroep doen op één of meerdere WAN operators als Onderaannemer. Er wordt hier specifiek Laag-2 gevraagd omdat een overlay campus-alike netwerk beoogd wordt die onderliggend zo transparant mogelijk dient te zijn (ondersteunen van jumbo frames). Voor bijkomende lijnen die via een Project worden gerealiseerd zal aan de ICT-Dienstverlener gevraagd worden de markt te laten spelen door meerdere alternatieve Onderaannemers een offerte te laten indienen.

Voor de kleine gebouwen tot één persoonslocaties (S4) kan beroep gedaan worden op de gangbare Internet broadband connectiviteit (Eurodocsis, xDSL, FTTH) of 5G op termijn. Momenteel is een verschuiving aan de gang van ADSL2+ en VDSL broadband naar GPON (Gigabit Passive Optical network). Van de ICT-Dienstverlener wordt verwacht dat hij deze evolutie mee opvolgt en tijdig Verbeterprojecten voorstelt om deze technologieën te introduceren in het netwerklandschap van de Vlaamse overheid.

Eenzijds worden binnen dit Dienstenpakket VO-WAN aansluitingen aangeboden via de Exploitatie van de infrastructuur van het Bestuur of van de betrokken Klanten.

Anderzijds moet het via dit Dienstenpakket ook mogelijk zijn om VO-WAN aansluitingen aan te bieden as a Service. Dit impliceert dat alle activiteiten, inclusief de nodige infrastructuur, inbegrepen zijn in deze Dienst. Dit met als doel om in de toekomst projectmatig VO-WAN aansluitingen te kunnen leveren aan Klanten waarbij de betrokken Klant niet zelf wenst te investeren in infrastructuur.

Dit Dienstenpakket betreft o.a.:

- Indien het infrastructuur van de Klant betreft: het beschikbaar houden en eventueel vervangen van de "Customer Edge" (CE) netwerkcomponenten (routers en firewalls) en de verbindingen binnen dit Dienstenpakket (o.a. glasvezelbekabeling van de Vlaamse overheid en door de ICT-Dienstverlener gehuurde lijnen) als onderdeel van Incidentmanagement in het kader van defecten. Andere vervangingen gebeuren via Projecten.
- Indien het infrastructuur van de ICT-Dienstverlener betreft (as a Service) : het aankopen, leveren, installeren, uit dienst nemen, upgraden naar hogere bandbreedte, beheren,

beschikbaar en up to date houden, alsook het verder laten evolueren (capaciteit en technologie) van de as a Service aansluitingen van de Sites van de Vlaamse overheid op het VO-WAN.

- De ICT-Dienstverlener zorgt voor voldoende redundantie om de afgesproken beschikbaarheidsniveaus (zie paragrafen 1.4.1.3.5, 1.4.1.3.6, 1.4.1.3.7, 1.4.1.3.8) te kunnen garanderen aan de Klanten van de VO-WAN-aansluiting.
- Via deze Dienst wordt ook de mogelijkheid aangeboden aan de Klant om te opteren voor een eigen Virtueel Privaat Netwerk (IP-VPN technologie), waardoor het netwerkverkeer op het gedeelde fysieke medium op een veilige manier gescheiden wordt.

Het procesmatig uitvoeren van alle taken in het kader van de Ondersteunende processen zoals in paragraaf 1.3 beschreven.

In principe bestaat de geografische scope van dit Dienstenpakket uit de gebouwen van de Klanten in het Vlaamse en het Brusselse gewest. In uitzonderlijke gevallen kan het zijn dat er aansluitingen in gebouwen van de Vlaamse overheid in het buitenland (bv Vlissingen) worden geleverd maar hiervoor zullen dan ook afzonderlijke afspraken gedocumenteerd worden.

1.4.1.1.3 Exploitatie van de beveiligde aansluitingen van partner netwerken op het VO-netwerk

Dit Dienstenpakket betreft de Exploitatie van de connectiviteit tussen Vlaamse overheid en de partners van de Vlaamse overheid. Deze connectiviteit dient tot stand gebracht te worden op een beveiligde manier waarbij de datastromen tussen de verschillende partijen duidelijk in kaart gebracht zijn, geautoriseerd en de impact binnen beide partijen kan geminimaliseerd worden.

Dit Dienstenpakket bevat ook de directe private Cloud connectiviteit tussen de Vlaamse overheid en de publieke cloud providers. Doestelling is om in de meest gangbare hyperscale cloud spelers (AWS, MS Azure, ...) een VO Point of Presence (POP) te hebben met performante, gegarandeerde en redundante connectiviteit naar de twee netwerk-knooppunten als netwerk aggregatie naar andere datacenters en gebouwen van de Vlaamse overheid.

Externe partners zijn op het VO-netwerk aangesloten via de partnerzone.

Primaire partners van de Vlaamse overheid worden opgenomen in een "closed user group netwerk" VONET. Hierop konden enkel primaire partners van de Vlaamse overheid aangesloten worden. Een primaire partner behoort tot een beleidsdomein van de Vlaamse overheid en is gebonden door het ICT-veiligheidsbeleid voor de beleidsdomeinen van de Vlaamse overheid. VONET zal om continuïteitsredenen de komende jaren actief blijven maar zal worden afgebouwd. Het huidige VONET netwerk biedt vandaag geen enkele meerwaarde meer, ook niet qua beveiliging en heeft derhalve geen bestaansredenen meer, behalve dan het (tijdelijk) onderhouden van continuïteit. 'Shared services' voor toepassingen kunnen ingevuld worden via het publieke Internet (dewelke de voorkeur geniet), private koppelingen binnen cloud diensten zelf of (om legacy redenen) via het door het Bestuur beheerde private (niet-overlappende) IP netwerk.

Voor de toegang tot het VO-netwerk zal er altijd een outer-firewall moeten gepasseerd worden. De ipsec verbinding waarop de partnerkoppelingen (langs VO kant) termineren vormt die outer-firewall. Vertrouwde partners hebben geen rechtstreekse toegang op het VO-netwerk. Zij zullen gebruik kunnen maken van een specifiek voor hen via dit Dienstenpakket gerealiseerde toegang.

Ook het beheer van de verbindingen tussen de VO-WAN en de voor de ICT-Dienstverlening gebruikte datacenters, inclusief alle onderliggende beveiligingscomponenten maken deel uit van dit Dienstenpakket. Uitzondering hierop is de connectie tussen het datacenter van de ICT-Dienstverlener van de Datacenterdiensten (managed DC) in het kader van deze Overeenkomst en de MPLS backbone en de connectie tussen de mainframe en de MPLS backbone. Dit behoort tot de respectievelijke scope van de Datacenterdiensten en de mainframediensten.

Deze dienstverlening betreft :

- het beheren van aansluitingen van externe partners van de Vlaamse overheid op het VO-netwerk;

- het beschikbaar en up to date houden van de betrokken componenten of lijnen en het vervangen ervan als onderdeel van Incidentmanagement in het kader van defecten;
- De ICT-Dienstverlener zorgt voor voldoende redundantie om de afgesproken beschikbaarheidsniveaus (zie paragraaf 1.4.1.3.9) te kunnen garanderen.

1.4.1.1.4 Exploitatie van de connecties tussen VO-WAN en het internet

De Vlaamse overheid heeft voor tal van functionele behoeften via het internet contact met de buitenwereld enerzijds en vanuit de buitenwereld moet het mogelijk zijn op een veilige manier gegevens die zich op het netwerk van de Vlaamse overheid bevinden te kunnen raadplegen anderzijds.

Voorbeelden van deze functionele behoeften zijn:

- Een thuiswerker moet vanop zijn thuisadres alle toegang hebben tot zijn gegevens die zich op het netwerk van de Vlaamse overheid bevinden;
- Gebruikers moeten de mogelijkheid hebben om ook van in het buitenland toepassingen en documenten te raadplegen;
- Een burger moet vanuit het internet toepassingen van de Vlaamse overheid kunnen gebruiken en veilig gegevens uitwisselen;
- In het kader van Bring Your Own Device moet het mogelijk zijn dat Gebruikers met eigen Gebruikersinfrastructuur (die niet noodzakelijk afgenomen is van de Raamovereenkomst voor de Werkplekdiensten) beveiligd toegang kunnen hebben vanuit het internet tot hun gegevens;
- Via mobiele netwerken en vanop publieke Wifi hotspots moet het mogelijk zijn het interne netwerk op een veilige manier te benaderen.

De algemene trend m.b.t. de vraag naar Internet bandbreedte (voornamelijk m.b.t. Internet access voor buretica) vanuit het Internet of de cloud zal alleen maar toenemen en dit exponentieel de komende jaren. Om hieraan tegemoet te komen moet de ICT-Dienstverlener tijdig Verbetervoorstellen voorleggen aan het Bestuur.

Gezien alle gebouwen (en Datacenters) van de Vlaamse overheid op VO WAN backbone gekoppeld zijn, zal het Internet op een gecentraliseerde wijze kunnen worden aangeboden vanuit de netwerk knooppunten. Hiermee wordt voldaan aan de doelstelling om maximaal gebruik van gemeenschappelijke platformen/lijnen en om zodoende de kostprijs zo laag mogelijk te houden. Toch is het de wens van Klanten om meer autonomie te bekomen op deze door het Bestuur beheerde gedeelde infrastructuur. Zo zal elke Klant de optie moeten hebben tot het bekomen van een logisch gescheiden beveiligde Internet toegang waarbij het veiligheidsbeleid door de Klant zelf kan worden ingevuld, bijv. middels afgescheiden URL filtering, firewall policies in beheer van de Entiteit zelf.

Er is met de komst van SDN/DNA overlay(s) geen noodzaak om specifiek Laag-2 te gaan. De wens gaat uit naar standaard Laag-3 MPLS, incl. managed CE met ondersteuning van frames > 1800 bytes (MTU). Deze CE zal een beperkte set van specifieke configuratie dienen te bevatten ten behoeve van zero-touch DNA deployments zoals DHCP relay, het gebruik van interne IP pools aan L etc. En dus geen noodzaak meer voor VPLS. De Internet connectiviteit nodig voor de Diensten beschreven in de Service Portfolio Applicatiediensten valt buiten de scope van de netwerkdiensten. De Internet connectiviteit nodig voor de Diensten beschreven in deze Service Portfolio en in de gebouwen in beheer van het Bestuur (o.a. Portfolio voor de Werkplekdiensten, technische faciliteiten IOT, ...) behoort tot de scope van deze Dienst.

De huidige opzet is verspreid over 2 verschillende ISP's (Colt & Cogent) op een drager van telkens 10Gbit/s. Er wordt ontsloten op zowel IPv4 als IPv6 en de VO beschikt over een eigen public RIPE assigend PI space (/22). (zie Referentiebibliotheek)

Het beschikbaar en up to date houden van de betrokken componenten of lijnen en het vervangen ervan als onderdeel van Incidentmanagement in het kader van defecten is onderdeel van deze Dienst.

De ICT-Dienstverlener zorgt ervoor dat hij de nodige maatregelen neemt om de afgesproken beschikbaarheidsniveaus (zie paragraaf 1.4.1.3.10) te kunnen garanderen.

Het Internet wordt zoals hierboven beschreven op een gecentraliseerde wijze aangeboden. Voor Klanten die gebruik willen maken van deze gecentraliseerde internetfunctionaliteit naar hun eigen datacenteromgeving/firewall wordt een gedeelde Managed netwerkdienst (VO-ISP) voorzien. Dit wil zeggen dat de ICT-Dienstverlener de door de Klant gevraagde capaciteit als onderdeel van de centrale internetconnectie ter beschikking stelt en het gebruik ervan door de ICT-Dienstverlener aan de betrokken Klant wordt gefactureerd onder de vorm van een gebruikskost. Deze gebruikskost zal in mindering gebracht worden van de forfaitaire maandelijkse kost voor niet direct aan één dienst toe te wijzen activiteiten die aan Agentschap Digitaal Vlaanderen wordt gefactureerd. De aangeboden VO-ISP oplossing omvat oa. anti-ddos voorziening, basis beveiliging, terbeschikkingstelling vast IP adres/blok.

1.4.1.1.5 Exploitatie van de centrale netwerk- en beveiligingsdiensten

Het internet is echter geen veilige omgeving op zich, zodat er tal van maatregelen genomen moeten worden niet alleen om de interne gegevens te beveiligen maar ook om de communicatie met de buitenwereld vlot en veilig te laten verlopen.

M.b.t. Managed Datacenters en de Applicatieve zones binnen de hyperscale cloud Datacenters zal de DC/Cloud ICT-Dienstverlener verantwoordelijk zijn voor de Datacenter eigen netwerk en beveiligings diensten zoals DC/Cloud border protection (beveiligd toegang naar Internet, aDDoS, ..), Advanced WAF, maatregelen voor ontsluiting toepassing ivf dataclassificatie vereisten zoals ATP, URL filtering etc.

De centrale netwerk- en beveiligingsdiensten onder verantwoordelijkheid van de ICT-Dienstverlener voor de netwerkdiensten dienen zo te worden opgezet dat het mogelijk is voor Entiteiten die dit wensen om projectmatig een logisch gescheiden beveiligd Internet toegang te bestellen waarbij het veiligheidsbeleid door de te Entiteit zelf kan worden ingevuld, bijv. middels afgescheiden URL filtering, firewall policies in beheer van de Entiteit zelf.

Voor wat betreft de site-to-site connectiviteit (datatransport) over Internet (Broadband) dient IPSEC encryptie te worden toegepast.

Via een door de ICT-Dienstverlener beheerde centrale beveiligingsomgeving wordt aan de op het VO-WAN aangesloten systemen een beveiligde en beheerde internettoegang geboden enerzijds en wordt anderzijds vanuit het internet op een beveiligde en beheerde manier toegang gegeven tot systemen en toepassingen die aangesloten zijn op de VO-WAN.

Het beschikbaar en up to date houden van de betrokken beveiligingscomponenten en het vervangen ervan als onderdeel van Incidentmanagement in het kader van defecten is onderdeel van deze Dienst.

De centrale beveiligingsomgeving maakt deel uit van de scope van dit Dienstenpakket en biedt het hoofd aan veiligheidsincidenten zoals onder andere:

- aanvallen door kwaadaardige software;
- aanvallen afkomstig van onveilige ('untrusted') netwerken;
- fraude en/of sabotage;
- schending van vertrouwelijkheid zoals hacking;
- fouten die voortvloeien uit onvolledige of onjuiste informatie, en inbreuken op het 'need to have' en 'need to know' principe, rekening houdend met de bestaande wet-en regelgeving;
- niet geautoriseerd gebruik van netwerktoepassingen om het netwerkverkeer te monitoren en/of aan te passen;
- distributed Denial of Service (DDoS);
- andere ongekende bedreigingen (zero day).

De doelstelling blijft om VO brede netwerkdiensten met actieve apparatuur voor diensten zoals DNS, DHCP, IPAM en NTP aan te blijven bieden vanuit de netwerk knooppunten ten dienste van alle VO gebouwen en legacy Datacenters. Mbt managed Datacenters en hyperscale cloud Datacenters zal de DC/Cloud ICT-Dienstverlener verantwoordelijk zijn voor dit soort van netwerkdiensten (rekening houdend met het feit de de Netwerk Dienstverlener het VO private IP plan zal beheren).

Een aantal centrale netwerddiensten worden als kritisch ervaren en de opzet ervan dient derhalve volledig redundant en 'appliance' based te blijven teneinde geen afhankelijkheden te hebben met de operationele compute/hypervisor omgeving. In de on-prem knooppunten wordt Infoblox technologie gebruikt.

Deze Diensten maken deel uit van de scope van dit Dienstenpakket:

- Beheren van Reverse Proxy (RP) en Forward Proxy (FP)
- Beheren van het IP address management systeem voor alle IP adressen (IPv4/IPv6)
- Beheren van de SMTP mail relay om Vo toepassingen, die zich op het interne netwerk van de Vlaamse overheid bevinden, te voorzien van de mogelijkheid om mails te versturen en te ontvangen zowel intern als extern (internet). De Mailrelay dienst fungeert dus als intern centraal distributiepunt en mitigatiecomponent voor alle mailverkeer van en naar de betrokken toepassingen. De dienst wordt aangeboden naar de Vo toepassingen die bij de start van de Overeenkomst deze dienst gebruiken. De nodige veiligheidsvoorzieningen moeten genomen worden om de communicatie veilig te laten verlopen. Zo moet het platform de meest recentste versies voor transport veiligheid (TLS) ondersteunen, het gebruik van DKIM ondersteunen, authenticated SMTP ondersteunen. Beheren van firewall diensten om een veilige afscherming te garanderen:
 - Next-generation Firewall diensten (on-prem) om netwerken in zones op te kunnen delen en van elkaar te scheiden. Deze bescherming omvat zowel 'stateful firewalling' als IPS en advanced anti-threat/malware beveiliging (ATP/Sandboxing), en dient zowel user als application aware te zijn (waarbij VO de mogelijkheid wenst te hanteren om security policy's op te bouwen op basis van applicaties);
 - Forward proxy diensten voor uitgaand verkeer met inbegrip van SSL inspectie, advanced anti-malware beveiliging (ATP/Sandboxing) en URL filtering zowel on-prem als in een cloud context. De ICT-Dienstverlener zal tevens verantwoordelijk zijn voor alle huidige proxy apparatuur thans opgesteld binnen de netwerk knooppunten, en op termijn in de cloud (Cloud PEP/SWG met optioneel inline CASB & DLP mogelijkheden);
 - Loadbalancing (& eventueel WAF) diensten, voornamelijk on-prem. Naargelang het geval, toegang tot interne applicaties en resources kunnen bieden en tegelijk de werklast te verdelen en de beschikbaarheid ervan te waarborgen en, naargelang het geval, de applicatie-inhoud te filteren tegen frauduleuze aanvragen;
 - Transparante en portaal gebaseerde SSL VPN diensten met authenticatie afwikkeling (medewerkers, partners) als onderdeel binnen de huidige Firewalls en proxies. Deze zullen vermoedelijk worden uitgefaseerd. De SSL/VPN service zoals die vandaag is ingeregeld als een aparte dienst heeft geen bestaansreden meer. De 'transparante' SSL/VPN is momenteel onderdeel van de Firewall service maar zal later als functie worden ondergebracht in de Cloud PEP/SWG dienst. De 'portaal' gebaseerde SSL/VPN voor beheerstoegang is momenteel in afbouw gezien de standaardisatie naar PAM;
 - Voor Specifieke use cases rond Application Delivery (al dan niet portaal gebaseerd) zal nog steeds beroep kunnen gedaan worden op een gecustomiseerde Reverse Proxy opzet (url redirect/rewriting, specifieke authenticatie, ssl offloading, App emulatie/tunneling, etc);
 - Cloud gebaseerde aDDOS dienst, dewelke gedrags-sensitief is en bescherming biedt ten aanzien van (zelf aangeleerde) baseline waarden met voldoende garanties om het aantal "false positives" te minimaliseren.
- Beheren van security servers voor de beveiligde toegang naar het internet (o.a. centrale VPN infrastructuur, ...).
- Het beheren van een stabiele High Available NTP service die meerdere externe clock-sources aan kan.
- DNS (Domain Name System)-diensten: Dit is het systeem en protocol dat gebruikt wordt om domeinnamen naar IP-adressen te vertalen en omgekeerd:
 - Cache DNS service voor alle interne endpoints en servers die gebruik maken van de forwards in de Internet Access POD;

- DHCP/DNS integraties voor dynamic DNS (Microsoft AD integratie), ... De service zal in staat zijn om op een beveiligde manier DNS Updates te ontvangen (authenticated);
- Authoritative DNS services voor vlaanderen.be en tal van andere domeinen al dan niet op basis van API. In geval van API wordt het Change controle proces volledig geautomatiseerd, behoeft dan geen Werkaanvraag, tenzij voor initieel gebruik van de API (onboarding)..;
- Het beheer van de centrale infrastructuur die toelaat om vanaf mobiele toestellen een beveiligde toegang te bekomen tot de datacenterdiensten voor werkplek;

Momenteel wordt voor datacenter firewalling beroep gedaan op Fortinet en Palo Alto. Met betrekking tot forward proxy, loadbalancing/L7-reverse proxy (ADC) en portaal gebaseerde SSL VPN wordt momenteel gestandaardiseerd op F5 technologie. Voor transparante VPN (RAS) wordt gebruik gemaakt van Palo Alto global protect.

De specifieke beveiligingscomponenten verbonden aan de Gebruikersinfrastructuur maken geen deel uit van de scope van dit Dienstenpakket.

De ICT-Dienstverlener zorgt ervoor dat hij de nodige maatregelen neemt om de afgesproken beschikbaarheidsniveaus (zie paragraaf 1.4.1.3.11) te kunnen garanderen.

De centrale netwerk- en beveiligingsdiensten zoals hierboven beschreven worden op een gecentraliseerde wijze aangeboden. Voor Klanten die gebruik willen maken van deze gecentraliseerde beveiligingsdiensten wordt een gedeelde Managed netwerkdienst voorzien. Dit wil zeggen dat de ICT-Dienstverlener de door de Klant gevraagde beveiligingsfunctionaliteit als logisch gescheiden onderdeel van de centrale beveiligingsomgeving ter beschikking stelt en het gebruik ervan door de ICT-Dienstverlener aan de betrokken Klant wordt gefactureerd onder de vorm van een gebruikskost. Deze gebruikskost zal in mindering gebracht worden van de forfaitaire maandelijkse kost voor niet direct aan één dienst toe te wijzen activiteiten die aan Agentschap Digitaal Vlaanderen wordt gefactureerd.

1.4.1.1.6 Exploitatie van de LAN/WLAN omgeving

Deze dienstverlening omvat alle Diensten die nodig zijn om steeds over een veilig, performant en up-to-date gemeenschappelijk Local Area Network (LAN) en draadloos Local Area Network (WLAN) voor de Vlaamse overheid te kunnen beschikken.

Deze dienstverlening omvat ook het beheer van een centrale infrastructuur die de toegang voor toestellen en/of Gebruikers tot de LAN diensten moet inregelen en beveiligen zodat een toestel en/of Gebruiker die zich aanmeldt op het netwerk geauthentiseerd en geautoriseerd kan worden op het netwerk.

Dit moet mogelijk zijn voor Gebruikersinfrastructuur die in Exploitatie is bij de ICT-Dienstverlener voor de Werkplekdiensten maar ook voor gebruikersinfrastructuur die niet in beheer is bij de ICT-Dienstverlener voor de Werkplekdiensten, onafhankelijk of deze infrastructuur eigendom is van de Vlaamse overheid of van de betrokken Gebruiker (BYOD).

De aansluitingen van IoT devices (camera's, slagbomen, kassa's, sleutelkasten, toegangscontrole, enz.) vallen ook onder deze Dienst en dienen ten alle tijden ondersteund te worden.

Het Bestuur voorziet alle structurele bekabeling in de gebouwen (koper en/of fiber) geplaatst en afgemonteerd volgens de gangbare industrie normen. Dit valt buiten bereik van deze Dienst.

Wireless dekking in de gebouwen is gedimensioneerd op VoIP.

Momenteel is QoS geconfigureerd op zowel op LAN als WLAN (WMM) niveau ter prioriterisering van kritieke flows zoals bijv. audio flows (Skype/Teams/IP telefoons). Alle netwerken dienen steeds 'UC ready' t.t.z., voldoende dekking en densiteit m.b.t. de Access Points, voldoende kwalitatief en ondersteuning van QoS.

Dit Dienstenpakket omvat de onderdelen van een intelligent en geautomatiseerd VO breed campus LAN & WLAN netwerk voor alle gebouwen van de Vlaamse Overheid:

- Het ter beschikking houden van een operationele LAN/WLAN omgeving inclusief het oplossen van Incidenten, het gezond houden van de technische omgeving (patches), de monitoring, het beveiligen van de LAN/WLAN, het correct houden van de Configuratie-databank m.b.t. de LAN/WLAN omgeving;
- Het beheer van de beveiliging van de gemeenschappelijke LAN/WLAN omgeving tegen externe en laterale aanvallen, virussen,...;
- het beheer van poortgebaseerde toegangscontrole op de LAN (IEEE 802.1x);
- DHCP-diensten: het doel van DHCP (Dynamic Host Configuration Protocol) is het vereenvoudigen van de netwerkconfiguratie; DHCP maakt het mogelijk om Pc's en andere apparatuur die in het netwerk van de Vlaamse overheid zitten dynamisch de juiste configuratiegegevens mee te geven;
- Dynamisch opzetten van segmentatie tussen verschillende Gebruikers en toestellen (concept van fysiek gedeeld, logisch gescheiden)
- Netwerk Access Controle (NAC) op basis van 802.1x (alsook waar nodig MAC authentication bypass) zonder nood aan inspectie van de host. Momenteel is het netwerk van de VO NAC-gestandaardiseerd op basis van machine certificate gebaseerde authenticatie (EAP-TLS) met dynamic LAN assignment.
- 'near-zero-touch-deployments' gecentraliseerde beheersconsole, gecentraliseerde authenticatie voor NAC (RADIUS) voor alle gebruikers in de gebouwen.
- Laagdrempelige oplossing voor bezoekers met authenticatie, logging en afdoende beveiliging tegen misbruik.
- Het ter beschikking stellen van een laagdrempelige draadloze toegang tot het internet via de WLAN toegangspunten voor bezoekers met authenticatie, logging en afdoende beveiliging tegen misbruik.
- Indien het infrastructuur van de Klant betreft: het vervangen van de LAN/WLAN-componenten als onderdeel van Incidentmanagement in het kader van defecten (met uitzondering van WIFI access points). Het aankopen, leveren en installeren van nieuwe componenten in eigendom van de Klant (uitbreiding o.b.v. "Capacity en performance management" en vervanging van verouderde componenten) gebeurt op basis van afzonderlijke Projecten.
- Indien het infrastructuur van de ICT-Dienstverlener betreft (as a Service): het marktconform aankopen, leveren, installeren, uit dienst nemen, upgraden naar hogere bandbreedte, beheren, beschikbaar en up to date houden, alsook het verder laten evolueren (capaciteit en technologie) van de as a Service LAN/WLAN functionaliteit.
- Het efficiënt en gecontroleerd uitvoeren van kleine wijzigingen. Deze wijzigingen kunnen zowel op initiatief van de ICT-Dienstverlener als op vraag van de Klant of Gebruiker uitgevoerd worden;
- Het ter beschikking stellen van een draadloze verbinding via WLAN toegangspunten met het netwerk van de Vlaamse overheid waardoor het voor medewerkers van de Vlaamse overheid mogelijk wordt om eenvoudig te switchen tussen werkruimtes en vergaderzalen. Via het draadloze netwerk van de Vlaamse overheid wordt een veilige toegang geboden tot dezelfde websites en toepassingen als het bedrade netwerk van de Vlaamse overheid, en dit vanuit alle aangesloten gebouwen;
- Het beheer van een netwerkmonitoringomgeving;
- Het actualiseren van de Configuratie-databank (CMDDB) met betrekking tot de ICT-componenten die binnen dit Dienstenpakket vallen in het kader van wijzigingen aan de exploitatieomgeving maakt deel uit van de scope.
- Het 24/24 7/7 beheer van de Mac Authenticatie Bypass functionaliteit op de LAN/WLAN omgeving; Voor de MAB portaal functionaliteit geldt enkel tijdens de Uitgebreide Kantooruren.
- M.b.t. de LAN dienstverlening is de Vlaamse overheid bezig met de uitrol van een volledig geautomatiseerd Software Defined Access (SDA) gebaseerd VO-campus LAN/WLAN netwerk omgeving die een effectievere en flexibelere manier van werken kan mogelijk maken, nieuwe Projecten (vb. in de context van IOT) op een productievere/snellere wijze weet op te leveren en eventuele problemen snel kan tackelen, dus kortere implementatie door hogere operationele efficiëntie. De operationele efficiëntie winst wordt geraamd op zo'n 60 tot 80%. Door de steeds snellere evolutie en nood op vlak van IOT en de groei aan diversiteit binnen de gebruikers

omgevingen in de gebouwen van de Vlaamse Overheid is er nood aan een meer intelligent geautomatiseerd Campus netwerk. Dit geautomatiseerd, programmeerbaar netwerk is wendbaar en vertaalt bedrijfsnaden onmiddellijk naar netwerk configuraties. Doorlooptijden voor nieuwe realisaties worden korter en de operationele kost wordt verlaagd.

- De centraal beheerde policy voor netwerkcomponenten, de op het netwerk aangesloten toestellen en gebruikers zorgt voor standaardisatie binnen de campus en datacenter ongeacht de fysieke locatie, maw iedere configuratie is gestandaardiseerd en wordt beheerd vanuit een centraal controle punt de “network controller” genoemd. Voor het netwerk in het centrale knooppunt is er ook een controller. De controller zorgt ook voor een veiligere omgeving waar segmentatie tussen verschillende gebruikers / toestellen dynamisch kan worden opgezet. Niet enkel en alleen zal de netwerk controller gebruikers / toestellen via een verscheidenheid aan metrieken kunnen herkennen en dynamisch een vooraf gedefinieerde policy aan kunnen toewijzen, maar de aan de gebruiker/toestel toegewezen policy zal automatisch toepasbaar zijn binnen de hele campus.
- Ook hier zullen Entiteiten die op vlak van veiligheidsbeleid autonoom wensen te blijven, de optie hebben om binnen SD-Access logisch gescheiden te worden ingericht ten aanzien van andere Entiteiten en in te staan voor entiteitspecifieke netwerk policies.

Eenzijds worden binnen dit Dienstenpakket LAN/WLAN-diensten aangeboden via de Exploitatie van de netwerkcomponenten van het Bestuur of van de betrokken Klanten.

Anderzijds moet het via dit Dienstenpakket ook mogelijk zijn om LAN/WLAN-diensten aan te bieden as a Service. Dit impliceert dat alle beheersactiviteiten en ook de nodige onderliggende infrastructuur inbegrepen zijn in deze Dienst. Dit met als doel om in de toekomst projectmatig bijkomende Sites of toekomstige Klanten aan te sluiten zonder zelf in infrastructuur te moeten investeren. De ICT-Dienstverlener voorziet hiervoor een Dienst LAN/WLAN as a Service (LAN aaS/WLAN aaS) .

Voor de Exploitatie van de LAN/WLAN omgeving zal de ICT-Dienstverlener samenwerken met de verschillende operationele betrokkenen (de medewerkers van de ICT-Dienstverlener, zijn Onderaannemers/Leveranciers en indien van toepassing de Entiteiten van de Vlaamse overheid die instaan voor de investering in de nodige infrastructuur. (glasvezelbekabeling , Lan bekabeling, ...)) om een kwalitatieve uitvoering te realiseren.

De ICT-Dienstverlener zorgt ervoor dat hij de nodige maatregelen neemt om de afgesproken beschikbaarheidsniveaus (zie paragraaf 1.4.1.3.12) te kunnen garanderen.

1.4.1.2 Geconcretiseerd door

Deze Diensten wordt verder geconcretiseerd door:

- De identificatiegegevens van de betrokken Klant (voor alle Diensten);
- De Inventaris van te beheren componenten:
 - Voor VO-WAN backbone:
 - Aantal en type van de routers (provider (P) en provider edge (PE) routers);
 - Voor de VO-WAN aansluitingen:
 - Het aantal en het type (bandbreedte en technologie en QoS optie) van de connecties;
 - Het type Site (S1->S4)
 - Voor de beveiligde aansluitingen van partner netwerken op het VO-netwerk
 - De lijnen en beveiligingscomponenten van de verbindingen tussen de VO_WAN en de voor de ICT-Dienstverlening gebruikte datacenters;

- Voor de connecties tussen VO-WAN en het internet:
 - Het aantal en het type van de voor deze omgeving te beheren connecties
 - Voor de klanten die afnemen van de gedeelde managed netwerkdienst VO-ISP
 - Identificatie van de klant
 - Afgenomen capaciteit
 - Type lijn of lijnen wanneer een redundante aansluiting gevraagd wordt
- Voor de centrale netwerk- en beveiligingsomgeving:
 - Het aantal en het type van de voor deze omgeving te beheren beveiligingscomponenten (o.a. firewalls, ...)
 - Voor de klanten die afnemen van de gedeelde managed netwerkdienst
 - Identificatie van de klant
 - Gevraagde staffel mbt het aantal gebruikers van de klant
- Voor de VO-LAN/WLAN omgeving:
 - De Inventaris van de te beheren LAN/WLAN componenten
 - Het gewenste beschikbaarheidsvenster

1.4.1.3 SLA

1.4.1.3.1 Beschikbaarheid van de VO-WAN backbone omgeving

Beschrijving en definitie

De beschikbaarheid op maandbasis van VO-WAN backbone omgeving exclusief de Site connectiviteit.

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau
Beschikbaarheid VO-WAN backbone	99,95 %

Geplande onbeschikbaarheden voor o.a. netwerkupgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per Dienstenpakket) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn, worden de Klanten en Gebruikers geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Inbreuken op beschikbaarheid ten gevolge van een hoge bezettingsgraad, worden niet in rekening gebracht indien de ICT-Dienstverlener hiervoor een verbetervoorstel voor capaciteitsuitbreiding aan de Klant heeft voorgelegd;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.

Meetelementen en –methode

De beschikbaarheidsgegevens worden continu gemeten via netwerkmonitoringsystemen van de ICT-Dienstverlener. De meting betreft de beschikbaarheid tussen de eindpunten van de VO-WAN backbone en niet de beschikbaarheid van de individuele lijnen. Er mag maximaal 5 minuten zitten tussen 2 verschillende meetpunten. Het beschikbaarheidspercentage wordt per maand bepaald.

1.4.1.3.2 Round trip delay van de VO-WAN backbone omgeving

Beschrijving en definitie

De round trip delay tussen provider edge routers is de tijd nodig voor een datapakket om van de zender naar de ontvanger te gaan en terug.

Service Level

De round trip delay wordt bepaald voor de connecties tussen provider edge routers en mag maximaal 10 ms bedragen. Op maandbasis mag slechts 1 % van de metingen hiervan afwijken.

Randvoorwaarden, assumpties en uitzonderingen

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

De round trip delay wordt maandelijks gemeten voor de connecties tussen provider edge routers via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van test pakketten (ping, ip-sla, ...). Zender en ontvanger betreffen de monitoring routers die rechtstreeks aangesloten zijn op de PE routers. De meetmethode mag de normale werking van de Site niet hinderen. De round-trip delay wordt gemeten tussen de eindpunten van de verbinding (niet tot op de firewall). Er mag maximaal 5 minuten zitten tussen 2 verschillende meetpunten. Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.3 Pakketverlies binnen de VO-WAN backbone omgeving**Beschrijving en definitie**

Het pakketverlies tussen provider edge routers is het aantal datapakketten dat verloren gaat tussen de zender en de ontvanger.

Service Level

Het pakketverlies wordt bepaald op de connecties tussen provider edge routers en mag maximaal 0,1 % bedragen op maandbasis. Op maandbasis mag slechts 1% van de metingen hiervan afwijken.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstampt in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties.
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

Het pakketverlies wordt maandelijks gemeten voor de verschillende connecties tussen provider edge routers via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van test pakketten (ping, ip-sla, ...). Zender en ontvanger betreffen de monitoring routers die rechtstreeks aangesloten zijn op de PE routers. De meetmethode mag de normale werking van de Site niet hinderen. Het pakketverlies wordt gemeten tussen de eindpunten van de verbinding.

Er mag maximaal 5 minuten zitten tussen 2 verschillende meetpunten. Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.4 Jitter van de VO-WAN backbone**Beschrijving en definitie**

De jitter gemeten tussen provider edge routers is de variërende vertraging in het afleveren van datapakketten tussen de zender en de ontvanger.

Service Level

De jitter wordt bepaald op de connectie tussen provider edge routers en mag maximaal 5 ms bedragen. Op maandbasis mag slechts 1% van de metingen hiervan afwijken.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebraat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

De Jitter wordt maandelijks gemeten voor de verschillende connecties tussen provider edge routers routers via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van test pakketten (ping, ip-sla, ...). Zender en ontvanger betreffen de monitoring routers die rechtstreeks aangesloten zijn op de PE routers. De meetmethode mag de normale werking van de Site niet hinderen. De jitter wordt gemeten tussen de eindpunten van de verbinding.

Er mag maximaal 5 minuten zitten tussen 2 verschillende meetpunten. Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.5 Beschikbaarheid van de WAN-aansluiting per Site

Beschrijving en definitie

De beschikbaarheid op maandbasis van de WAN-aansluiting per Site. Dit omvat de betrokken Customer edge routers en firewalls (indien aanwezig) en de dataverbindingen tussen de Site en de VO-WAN.

Service Level

De SLA per Site is afhankelijk van het type van aansluiting.

Met betrekking tot het beschikbaarheidsvenster wordt een onderscheid gemaakt tussen Uitgebreide Kantooruren en 24/24 7d/7d.

Periodes voor gepland en vooraf met de Klant overeengekomen onderhoud worden niet aanzien als onbeschikbaarheid.

Indicator	Dienstverleningniveau
S1: Beschikbaarheid grote Sites met twee gegarandeerde vaste lijnen naar twee verschillende IP POPs van de backbone 24/24 7/7	99,95 %

S2: Beschikbaarheid standaard Sites op basis van een gegarandeerde vaste lijn in combinatie met IPSEC over Internet broadband 24/24 7/7	99,50 %
S3: Beschikbaarheid kleine Sites op basis van een gegarandeerde vaste lijn Uitgebreide Kantooruren	99,50 %
S4: Beschikbaarheid kleine Sites op basis van IPSEC over Internet broadband, incl.5G in de toekomst (Uitgebreide Kantooruren)	99,00 %

De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per Dienstenpakket) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Inbreuken op beschikbaarheid ten gevolge van een hoge bezettingsgraad, worden niet in rekening gebracht indien de ICT-Dienstverlener hiervoor een verbetervoorstel voor capaciteitsuitbreiding aan de Klant heeft voorgelegd;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.
- Indien de onbeschikbaarheid te wijten is aan een onderliggende datalijn met minimale dienstverlening (zie Prijslijst huurlijnen) (vb S4)

Meetelementen en –methode

De beschikbaarheidsgegevens worden continu gemeten via netwerkmonitoringsystemen van de ICT-Dienstverlener en dit per Site. De meting betreft de beschikbaarheid van de connectiviteit van de Site en niet van elke individuele lijn.

Voor S3 en S4 sites worden in de berekening van de SLA enkel onderbrekingen tijdens Uitgebreide Kantooruren (UKU) in rekening gebracht.

1.4.1.3.6 Round trip delay van de WAN-aansluiting per Site

Beschrijving en definitie

De round trip delay tussen customer edge routers en firewalls is de tijd nodig voor een datapakket om van de zender naar de ontvanger te gaan en terug. De round-trip delay wordt gemeten tussen de eindpunten van de verbinding en niet tot op de firewall.

Service Level

De round trip delay wordt bepaald per WAN-aansluiting op een Site en mag maximaal 50 ms bedragen. Geen gemiddelde waarden toegelaten. Op maandbasis mag slechts 1% van de metingen hiervan afwijken

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren zoals beschreven in 'Beschikbaarheid van de WAN-aansluiting per Site' vallen buiten de verantwoordelijkheid van de Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA.

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend;
- Indien de onbeschikbaarheid te wijten is aan een onderliggende datalijn met minimale dienstverlening (zie Prijslijst huurlijnen) (vb S4) ;
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

De round trip delay wordt gemeten per VO-WAN aansluiting op een Site via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van testpakketten (ping, ip-sla, ...) . De meetmethode mag de normale werking van de Site niet hinderen. De meetperiode bedraagt telkens één maand. Er mag maximaal 5 minuten zitten tussen 2 metingen.

Voor S3 en S4 sites worden in de berekening van de SLA enkel onderbrekingen tijdens Uitgebreide Kantooruren (UKU) in rekening gebracht.

Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.7 Pakketverlies van de WAN-aansluiting per Site**Beschrijving en definitie**

Het pakketverlies tussen customer edge routers is het aantal datapakketten dat verloren gaat tussen de zender en de ontvanger.

Service Level

Het pakketverlies wordt bepaald per WAN-aansluiting op een Site en mag maximaal 0,5% bedragen. Op maandbasis mag slechts 1% van de metingen hiervan afwijken.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren zoals beschreven in 'Beschikbaarheid van de WAN-aansluiting per Site' vallen buiten de verantwoordelijkheid van de Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA.

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.
- Indien de onbeschikbaarheid te wijten is aan een onderliggende datalijn met minimale dienstverlening (zie Prijslijst huurlijnen) (vb S4)
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

Het pakketverlies wordt gemeten per VO-WAN aansluiting op een Site via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van testpakketten (ping, ip-sla, ...) . De meetmethode mag de normale werking van de Site niet hinderen. De meetperiode bedraagt telkens één maand. Er mag maximaal 5 minuten zitten tussen 2 metingen.

Voor S3 en S4 sites worden in de berekening van de SLA enkel onderbrekingen tijdens Uitgebreide Kantooruren (UKU) in rekening gebracht.

Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.8 Jitter van de WAN-aansluiting per Site

Beschrijving en definitie

De jitter tussen customer edge routers en firewalls is de variërende vertraging in het afleveren van datapakketten tussen de zender en de ontvanger.

Service Level

De jitter wordt bepaald per WAN-aansluiting op een Site mag maximaal 10 ms bedragen. Op maandbasis mag slechts 1% van de metingen hiervan afwijken.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren zoals beschreven in 'Beschikbaarheid van de WAN-aansluiting per Site' vallen buiten de verantwoordelijkheid van de Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA.

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Vastgestelde inbreuken op het ogenblik dat de bezettingsgraad 60% overschrijdt, worden niet in rekening gebracht voor de berekening van de prijscorrecties;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.

- Indien de onbeschikbaarheid te wijten is aan een onderliggende datalijn met minimale dienstverlening (zie Prijslijst huurlijnen) (vb S4)
- De meettoestellen (routers) van het Bestuur zijn in staat om IPSLA te beantwoorden;

Meetelementen en –methode

De jitter wordt gemeten per VO-WAN aansluiting op een Site via netwerkmonitoringsystemen van de ICT-Dienstverlener via het periodisch zenden van testpakketten (ping, ip-sla, ...) . De meetmethode mag de normale werking van de Site niet hinderen. De meetperiode bedraagt telkens één maand. Er mag maximaal 5 minuten zitten tussen 2 metingen.

Voor S3 en S4 sites worden in de berekening van de SLA enkel onderbrekingen tijdens Uitgebreide Kantooruren (UKU) in rekening gebracht.

Geen berekening op basis van gemiddelde waarden over de verschillende meetpunten heen toegelaten.

1.4.1.3.9 Beschikbaarheid van de beveiligde aansluitingen van partner netwerken op het VO-netwerk

Beschrijving en definitie

De beschikbaarheid van de beveiligde aansluitingen van partner netwerken (inclusief aansluitingen van een publieke cloudaanbieder) op maandbasis op het VO-netwerk wordt bepaald per partner. Dit omvat alle aan de aansluiting onderliggende componenten.

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau
Beschikbaarheid (Enkelvoudige CPE/ Datalijn)	99,50 %
Beschikbaarheid (Dubbele CPE/ Datalijn)	99,95%
Beschikbaarheid zonder CPE over internet	Geen afzonderlijke SLA*

* De SLA voor de beschikbaarheid van de firewall langs VO zijde zit reeds vervat in de SLA van de Beschikbaarheid van de centrale netwerk- en beveiligingsdiensten en beschikbaarheid van de internet connectiviteit (paragraaf 1.4.1.3.11 en 1.4.1.3.10).

Geplande onbeschikbaarheden voor o.a. Upgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per Dienstenpakket) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende WAN connectiviteit door een externe partij aangeleverd en uitgebaat. Voorwaarde voor het niet in rekening brengen is:
 - En dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);
- Inbreuken op beschikbaarheid ten gevolge van een hoge bezettingsgraad, worden niet in rekening gebracht indien de ICT-Dienstverlener hiervoor een verbetervoorstel voor capaciteitsuitbreiding aan de Klant heeft voorgelegd;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.
- Indien het Incident te wijten is aan een publieke cloud-aanbieder: Voorwaarde voor het niet in rekening brengen:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);

Meetelementen en –methode

De beschikbaarheidsgegevens worden maandelijks gemeten via netwerkmonitoringsystemen van de ICT-Dienstverlener en dit per component. De meting betreft de beschikbaarheid van de connectiviteit met de Partner en niet van elke individuele lijn. Er mag maximaal 5 minuten zitten tussen 2 metingen.

1.4.1.3.10 Beschikbaarheid van de Internet connectiviteit

Beschrijving en definitie

De beschikbaarheid van de connecties naar de Internet Service Provider (ISP) op maandbasis. Het Internet is beschikbaar als de 'next hop' (dit is de eerste router van de Internet provider) bereikbaar is via PING.

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau
Beschikbaarheid Internet connectie (redundant),	99,95 %

Geplande onbeschikbaarheden voor o.a. upgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar Dienstenpakket) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de

uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Indien het Incident te wijten is aan de onderliggende internetverbinding die door een externe partij wordt aangeleverd en uitgebaat.
- Inbreuken op beschikbaarheid ten gevolge van een hoge bezettingsgraad, worden niet in rekening gebracht indien de ICT-Dienstverlener hiervoor een verbetervoorstel voor capaciteitsuitbreiding aan de Klant heeft voorgelegd;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.
- Het Internet wordt beschouwd beschikbaar te zijn, indien de 'next hop' (dit is de eerste router van de Internet provider) bereikbaar is via ICMP (ping);
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.

Meetelementen en –methode

De end tot end beschikbaarheidsgegevens worden maandelijks gemeten via monitoringsystemen van de ICT-Dienstverlener. De meting betreft de beschikbaarheid van de connectiviteit met de internet provider en niet internet lijn.

Er mag maximaal 5 minuten zitten tussen 2 metingen.

1.4.1.3.11 Beschikbaarheid van de centrale netwerk- en beveiligingsdiensten

Beschrijving en definitie

De beschikbaarheid van de centrale netwerk- en beveiligingsdiensten per afzonderlijke Dienst op maandbasis. Dit omvat firewall service, load balancing/proxy/VPN services, DDIN (DNS, DHCP, IPAM en NTP) en de centrale SDN/NAC componenten.

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau
Beschikbaarheid firewall services (high availability)	99,95 %
Beschikbaarheid load balancing/proxy/VPN services (high availability)	99,95 %
Beschikbaarheid DDIN (DNS, DHCP, IPAM en NTP) (high availability)	99,95 %
Beschikbaarheid SDN/NAC componenten (high availability)	99,95 %

Geplande onbeschikbaarheden voor o.a. upgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per afzonderlijke Diensten) en

nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Indien de ICT-Dienstverlener bij een Incident dat een interventie ter plaatse vergt, geen toegang krijgt tot de lokalen waar de betrokken netwerkcomponenten staan;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.
- Indien het Incident te wijten is aan een publieke cloud-aanbieder: Voorwaarde voor het niet in rekening brengen:
 - dat de ICT-Dienstverlener aantoont dat hij binnen het uur na de vaststelling dat het incident een onderliggend lijnprobleem betreft de externe partij op de hoogte heeft gesteld. (aan te tonen op basis van een ticketnummer of e-mailstamp in de documentatie van het Incident);

Meetelementen en –methode

De end tot end beschikbaarheidsgegevens worden maandelijks gemeten via monitoringsystemen van de ICT-Dienstverlener. Er mag maximaal 5 minuten zitten tussen 2 metingen.

1.4.1.3.12 Beschikbaarheid van de LAN/WLAN componenten

Beschrijving en definitie

De beschikbaarheid van LAN/WLAN omgeving per Site houdt in dat alle componenten (met uitzondering van de UPS'en) beschikbaar moeten zijn.

Voor de WLAN componenten en UPS-en zullen hardware vervangingen en batterijwissels via afzonderlijke door de Klant te geven opdrachten voor Ondersteuning in regie m.b.t. de netwerkomgeving.

Service Level

Er is een keuzemogelijkheid per site tussen een beschikbaarheidsvenster Uitgebreide Kantooruren (default) of een beschikbaarheidsvenster 24/24 uur 7/7 dagen. Uiteraard is de keuze van 24/24 uur enkel van toepassing als de WAN-aansluiting van de betrokken site ook 24/24 u SLA heeft. Bij Uitgebreide Kantooruren loopt de klok enkel tussen 7:30 en 19 uur op Werkdagen.

Indicator	Dienstverleningniveau binnen Uitgebreide kantooruren	Dienstverleningniveau 24/24 7/7
Beschikbaarheid LAN omgeving Uitgebreide Kantooruren	99,00 %	N.V.T
Beschikbaarheid LAN omgeving 24/24 7/7	99,50 %	99,50 %

Beschikbaarheid WLAN omgeving Uitgebreide Kantooruren	99,00 %	N.V.T
Beschikbaarheid WLAN omgeving 24/24 7/7	99,50 %	99,50 %

De geplande onbeschikbaarheden in het kader van de exploitatie LAN/WLAN voor o.a. netwerkupgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per Dienstenpakket) en nemen maximum 4u per maand in beslag, met uitzondering van dringende patches/updates om security kwetsbaarheden te herstellen. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Geen toegang tot de lokalen waar de netwerkcomponenten staan;
- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend;
- Binnen de Mac Authenticatie Bypass functionaliteit geldt een "Uitgebreide Kantooruren" SLA voor MAB-portaal toepassing die ervoor zorgt dat een geautoriseerde VO-medewerker in selfservice een niet 802.1x toestel kan activeren of deactiveren in de MAB LDAP database;
- Wanneer in het geval van een onbeschikbaarheid van een WLAN access point of een UPS blijkt dat er een hardware defect is of er een batterijwissel nodig is, dan mag de tijd, tussen de melding van deze vaststelling door de ICT-Dienstverlener aan de betrokken Klant en het einde van de uitvoering van de door de Klant gegeven opdracht voor Ondersteuning in regie m.b.t. de netwerkomgeving worden afgetrokken van de onbeschikbaarheid.

Meetelementen en –methode

De beschikbaarheidsgegevens worden continu gemeten via netwerkmonitoringsystemen van de ICT-Dienstverlener. De beschikbaarheid per Site wordt op maandbasis berekend. Alle componenten worden gemeten met een interval van 5 seconde met uitzondering van de WLAN componenten waar een interval van 15 seconde wordt gehanteerd.

1.4.1.4 Prijsmechanisme

Gemeenschappelijk voor alle exploitatiediensten wordt er een maandelijkse Eenheidsprijs opgegeven voor de niet direct aan één exploitatiedienst toewijsbare kosten. Het betreft o.a. sleutelpersoneel en overlegfora, administratieve ondersteuningtaken, recurrente tooling kosten, De samenstelling van deze Eenheidsprijs dient via een transparant kostenmodel geduid te worden in het voorstel van de ICT-Dienstverlener.

De prijzen voor de Exploitatie van de VO-WAN backbone omgeving worden als volgt bepaald:

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten exclusief de eventuele VO-specifieke contracten en de huur van datalijnen) (zie Eenheidsprijzen netwerken Exploitatie);
- Het aantal en het type van de in voorbije maand gehuurde datalijnen (zie Eenheidsprijzen netwerken huurlijnen).
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).

De prijzen voor de Exploitatie van de VO-WAN aansluitingen op componenten die van de Klanten zijn omgeving worden als volgt bepaald:

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten (exclusief de eventuele VO-specifieke contracten en de huur van de datalijnen) (zie Eenheidsprijzen netwerken Exploitatie);
- De in de voorbije maand beschikbaar gehouden specifieke VPN netwerken i.k.v. een VO-WAN aansluiting router (exclusief de eventuele onderhoudscontracten hierop enerzijds (zie Eenheidsprijzen netwerken exploitaite);
- Het aantal en het type van de in voorbije maand gehuurde datalijnen (zie Eenheidsprijzen netwerken huurlijnen)..
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).

De prijzen voor de Exploitatie van de beveiligde aansluitingen van partner netwerken op het VO-netwerk worden als volgt bepaald :

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten (exclusief de eventuele VO-specifieke contracten en de huur van de datalijnen) (zie Eenheidsprijzen netwerken Exploitatie).
- Het aantal en het type van de in voorbije maand gehuurde datalijnen, waaronder ook de datalijnen voor de beveiligde verbindingen tussen de VO-WAN en de voor de ICT-Dienstverlening gebruikte datacenters. (zie Eenheidsprijzen netwerken huurlijnen).
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).

De prijzen voor Exploitatie van de connecties tussen VO-WAN en het internet worden als volgt bepaald:

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten (exclusief de eventuele VO-specifieke contracten en de huur van de datalijnen) (zie Eenheidsprijzen netwerken Exploitatie) .
- Het aantal en het type van de in voorbije maand gehuurde datalijnen en internetprovider (ISP) abonnementen. De Eenheidsprijs per type datalijn en per ISP abonnement is bepaald in de Eenheidsprijzen netwerken huurlijnen.
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).
- Voor de gedeelde managed netwerkdiensten die mogelijks worden ingeregeld voor het verlenen van dienstverlening aan gebruikende afnemers:
 - De gebruikskosten, zijnde het gedeelte van de centrale exploitatiekosten voor deze specifieke diensten op basis van de eenheidsprijzen in de Prijslijst exploitatie Netwerkdiensten. Deze kost kan forfaitair zijn, en/of volume gebaseerd (eindgebruik, afname door afnemers), of een combinatie van beide. Het betreft een kost die per maand wordt aangerekend aan de gebruikende afnemers.
 - De kosten voor het gebruik van de gedeelde managed netwerkdiensten zelf, die in opdracht van de Klant (Agentschap Digitaal Vlaanderen) periodiek worden gefactureerd via de ICT-Dienstverlener aan de gebruikende afnemers, worden integraal in mindering gebracht op de forfaitaire maandelijkse kost voor niet direct aan één dienst toe te wijzen activiteiten van het Agentschap Digitaal Vlaanderen. In dit concept kan een kostenmodel worden gebruikt voor de aanrekening van kosten aan de afnemers, dat bijv. kan gebaseerd zijn op reëel gebruik, verbruik of aantallen, frequentie, intensiteit of volumes, ed.

De prijzen voor Exploitatie van de centrale netwerk- en beveiligingsdiensten worden als volgt bepaald:

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten (exclusief de eventuele VO-specifieke contracten hierop) (zie Eenheidsprijzen netwerken Exploitatie) .
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).
- Voor de gedeelde managed netwerkdiensten die mogelijks worden ingeregeld voor het verlenen van dienstverlening aan gebruikende afnemers:
 - De gebruikskosten, zijnde het gedeelte van de centrale exploitatiekosten voor deze specifieke diensten op basis van de eenheidsprijzen in de Prijslijst exploitatie Netwerkdiensten. Deze kost kan forfaitair zijn, en/of volume gebaseerd (eindgebruik, afname door afnemers), of een combinatie van beide. Het betreft een kost die per maand wordt aangerekend aan de gebruikende afnemers.
 - De kosten voor het gebruik van de gedeelde managed netwerkdiensten zelf, die in opdracht van de Klant (Agentschap Digitaal Vlaanderen) periodiek worden gefactureerd via de ICT-Dienstverlener aan de gebruikende afnemers, worden integraal in mindering gebracht op de forfaitaire maandelijkse kost voor niet direct aan één dienst toe te wijzen activiteiten van het Agentschap Digitaal Vlaanderen.
 - In dit concept kan een kostenmodel worden gebruikt voor de aanrekening van kosten aan de afnemers, dat bijv. kan gebaseerd zijn op reëel gebruik, verbruik of aantallen, frequentie, intensiteit of volumes, ed.

De prijzen voor de Exploitatie van de LAN/WLAN omgeving worden als volgt bepaald:

- Het aantal en type van de in de voorbije maand beschikbaar gehouden componenten rekening houdend met het gegeven of het een 24/24 7/7 dagen Site is of een Site Uitgebreide Kantooruren (exclusief de eventuele VO-specifieke contracten hierop) (zie Eenheidsprijzen netwerken Exploitatie) ;
- De prijs voor de VO-specifieke contracten die nodig zijn voor deze Dienst. Deze contracten worden aangerekend volgens de modaliteiten bepaald in het VO-specifiek contract (regime van facturatie (maandelijks, jaarlijks) en wijze van facturatie (variabel of vast)).

1.4.1.5 Facturatie

Voor de exploitatiediensten is er een maandelijkse facturatie per Klant. De factuur bevat een overzicht van de forfaitaire maandelijkse kost voor niet direct aan één dienst toe te wijzen activiteiten, de beschikbaar gehouden componenten met hun Eenheidsprijzen en de gehuurde datalijnen met hun Eenheidsprijzen.

Voor de gedeelde managed netwerkdiensten:

- Wordt de maandelijkse factuur gestuurd aan de afnemers van deze diensten. Ze bevat een overzicht van de forfaitaire maandelijkse gebruikskosten en indien van toepassing de volume gedreven gebruikskosten, gestaafd met de volume -gerelateerde gegevens;

Wordt het totaal van de afgenomen diensten door de verschillende afnemers van deze diensten in mindering gebracht op de factuur van het Agentschap Digitaal Vlaanderen.

Voor de VO-specifieke contracten wordt de kost aangerekend volgens de periodiciteit afgesproken in het contract, voor zover ze nog niet verrekend werden als onderdeel van een Werkaanvraag. Deze worden onderbouwd door de geldende contractuele documenten van die VO-specifieke contracten in DDC-DMS en registratie in de Configuratiebank. Indien de contractkost volume-gedreven is, dient naast de onderbouwing van de gebruikte Eenheidsprijzen ook een rapportering meegegeven te worden waaruit de reële volumes blijken (bv een contract voor pay-as-you-use-diensten van een publieke cloud).

Indien de SLA m.b.t. de beschikbaarheid van de Dienst niet gehaald wordt dan is de Prijscorrectie zoals voorzien in het Basiscontract van toepassing. Deze Prijscorrectie wordt toegepast op het bedrag van de voor de Klant beschikbaar gehouden componenten. Daar waar de SLA expliciet vermeldt dat het per Site is wordt de Prijscorrectie toegepast op het bedrag per Site. De Prijscorrectie wordt niet toegepast op het bedrag dat betrekking heeft op de VO-specifieke contracten (o.a. de kosten van een publieke Cloud aanbieder). Daarnaast zijn ook de in het kader van de VO-specifieke contracten bepalingen m.b.t. eventuele prijsverminderingen bij het niet halen van de afspraken in dat contract ook van toepassing.

1.4.1.6 Rapportering

Maandelijkse rapportering:

- De SLA-metrieken
 - Rapportering van de beschikbaarheid van de VO-WAN omgeving met een detail per component/lijn tijdens de voorbije maand;
 - Rapportering van de round trip delay van de VO-WAN omgeving met een detail per connectie tussen provider edge routers in de voorbij maand;
 - Rapportering van het pakketverlies van de VO-WAN omgeving met een detail per connectie tussen provider edge routers in de voorbij maand;

- Rapportering van de jitter van de VO-WAN omgeving met een detail per connectie tussen provider edge routers in de voorbij maand;
- Rapportering van de beschikbaarheid van de VO-WAN aansluitingen tijdens de voorbije maand;
- Een overzicht van de VO-WAN aansluitingen van de betrokken Klant inclusief de bandbreedte en het werkaanvraagnummer waarmee deze WAN-aansluiting door de ICT-Dienstverlener werd gerealiseerd;
- Rapportering van de round trip delay per VO-WAN aansluiting in de voorbij maand;
- Rapportering van het pakketverlies per VO-WAN aansluiting in de voorbij maand;
- Rapportering van de jitter per VO-WAN aansluiting in de voorbij maand;
- Rapportering van de beschikbaarheid van de LAN/WLAN omgeving met een detail per component/lijn rekening houden met toepasbare beschikbaarheidsvenster tijdens de voorbije maand;
- De beschikbaar gehouden VO-WAN backbone componenten met hun technische kenmerken zoals opgenomen in de Configuratie-databank;
- De beschikbaar gehouden VO-WAN aansluitingen en datalijnen met hun technische kenmerken zoals opgenomen in de Configuratie-databank;
- De beschikbaar gehouden beveiligde aansluitingen van partner netwerken op het VO-netwerk met hun technische kenmerken zoals opgenomen in de Configuratie-databank.
- Een overzicht van de veiligheidsovertredingen, Incidenten en cruciale activiteiten geregistreerd en geanalyseerd voor managementdoeleinden;
- De ICT-Dienstverlener levert periodiek rapporten over security Incidenten zoals onder andere, maar niet beperkt tot:
 - Intrusies;
 - Hacking pogingen;
 - DoS pogingen;
 - Verkeerde toegangsrechten met potentiële impact;
 - Firewall statistieken: dropped ports, port scans, most used ports, etc...;

De ICT-Dienstverlener werkt hiervoor een standaardrapportering uit en houdt ermee rekening dat deze rapportering een dynamisch gegeven is. De Klant kan naargelang de gewijzigde kwetsbaarheden nieuwe standaardrapporten wensen, standaardrapporten laten wijzigen, of specifieke rapporten vereisen i.g.v. een Incident met hoge impact en/of visibiliteit.

- Rapportering van maximale gebruik van de WAN bandbreedte naar de verschillende netwerklocaties.
- De beschikbaar gehouden LAN/WLAN componenten en datalijnen met hun technische kenmerken zoals opgenomen in de Configuratie-databank;
- Voor de Mac Authenticatie Bypass functionaliteit zal er een controlerapport worden gemaakt waarin gecheckt wordt of alle CI's die in de MAB database zitten opgenomen zijn in Configuratie-databank.
- Op het einde van het jaar of op een met de Klant afgesproken tijdstip moet aan de Klant een overzicht worden voorgelegd m.b.t alle onderhoudscontracten nodig voor de uitbating van de netwerkdiensten met hun respectievelijke vervaldag teneinde de Klant in staat te stellen zijn budgetplanning op te stellen.

Deze rapporteringen kunnen (deels) in overleg met de Klant tijdens de Initiële Transitie ook gerealiseerd worden op basis van meekijkfunctionaliteit in de systemen of op basis van het beschikbaar stellen van de data in het DDC-DWH.

1.4.2 Werkaanvragen m.b.t. de netwerkomgeving

1.4.2.1 Scope en doel

Voor de éénmalige Diensten is het bestelproces (opmaken van een offerte – uitvoering – facturatie) snel, flexibel en transparant voor de Klant. De bestellingen zullen net zoals andere bestellingen m.b.t. ICT-Diensten via één bestelkanaal kunnen ingediend worden. Voor de realisatie hiervan zal moeten samengewerkt worden met de ICT-Dienstverlener van de Integratiediensten. De ICT-Dienstverlener zorgt ervoor dat hij een interface heeft met dit bestel kanaal waardoor hij bestellingen kan oppikken en correct uitvoeren.

Daarnaast kunnen ook, voor bepaalde éénmalige Diensten waar meer automatisatie mogelijk is en het proces 100% kan geautomatiseerd worden, de nodige interfaces worden opgezet om de dienstverlening sneller en kwalitatief te realiseren. (bv aanvragen bezoekersaccount, aanvragen DNS entries, ...)

De Klanten dienen de Werkaanvraag in via de bestelportaal. De ICT-Dienstverlener voor de integratiediensten zorgt voor de autorisatie en wijst de Werkaanvraag toe aan de juiste Service-provider in het Ecosysteem. De ICT-Dienstverlener voor de netwerkdiensten is verantwoordelijk voor de correcte uitvoering van de Werkaanvraag conform het proces “Behandelen van Werkaanvragen” in het document Vereisten Ondersteunende Processen.

1.4.2.1.1 Werkaanvragen m.b.t. het aanmaken, wijzigen of verwijderen van filtering van internetverkeer

In het kader van Werkaanvragen voor het aanmaken, het wijzigen of het verwijderen van een filtering van het internetverkeer worden volgende activiteiten uitgevoerd afhankelijk van de in de Werkaanvraag bestelde opties:

- Het toesturen aan de Klant van de policy die van kracht is;
 - Opstellen van het rapport;
 - Doorsturen van de huidige policy;
- Voor de optie blokkering/deblokkering van categorieën:
 - Aanmaken van de url filter;
 - Aanmaken van de policy;
 - Pushen van de policy naar achterliggende infrastructuur en rapportering;
 - Checken van de werking van de firewall;
 - Aanpassen van de rapportering;
- Voor de optie url of web-applicatie blokkering/deblokkering;
 - Definiëren van de applicatie (per url);
 - Aanmaken van de policy;
 - Pushen van de policy naar achterliggende infrastructuur en rapportering;
 - Checken van de werking van de firewall;
- Voor de optie verlenen van additioneel advies m.b.t. specifieke aanvragen (sessie van 2uur);
 - Uitvoeren van een impactanalyse;
 - Formuleren advies;
 - Toelichten van categorieën en technologie gebruikt voor filtering (vandaag product Palo Alto);
 - Beantwoorden van vragen van de Klant;

1.4.2.1.2 Werkaanvragen m.b.t. het controleren van het internetgebruik

binnen de ICT-code

In het kader van Werkaanvragen voor het controleren van het internetgebruik binnen de ICT-code worden volgende activiteiten uitgevoerd afhankelijk van de in de Werkaanvraag gestelde opties:

- Ingeval van een individuele controle, na ontvangst van de Werkaanvraag wordt zo snel mogelijk door de ICT-Dienstverlener contact opgenomen met het opgegeven telefoonnummer, om de privacy gevoelige informatie (persoon/personen/ waarover gerapporteerd dient te worden) op te vragen;
- Er wordt nagegaan of de aanvraag kadert in één van de vastgelegde doelen voor het uitvoeren van een controle via ICT-code.
- Alle informatie wordt vervolgens samengebracht en per e-mail, voorgelegd aan Audit Vlaanderen.
- De medewerkers van Audit Vlaanderen zullen voor elke aanvraag nagaan via het Vlimperssysteem of de aanvrager effectief een lijnmanager – een afdelingshoofd of hoger – is en of hij/zij de hiërarchische meerdere van betrokken personeelslid of Entiteit is.
- Zodra de validatie positief is wordt met de uitvoering van de Werkaanvraag gestart.
- De optie “Opvragen van een permanente algemene controle onder de vorm van een maandelijks rapport door de lijnmanager over het internetgebruik door personeelsleden van zijn Entiteit (binnen de grenzen van de ICT-code)” betreft niet-geïndividualiseerde gegevens, dus gegevens die niet gelinkt kunnen worden aan een persoon.
 - Het maandelijks rapport met de in de Werkaanvraag gespecificeerde gegevens (zoals totaal internet verbruik, top URL categorieën, ...) wordt opgesteld;
 - Elke maand wordt het rapport opgeleverd via e-mail aan het in de Werkaanvraag opgegeven adres. De Werkaanvraag wordt beschouwd als uitgevoerd nadat het maandelijks rapport voor de eerste keer via push werd bezorgd;
 - Een wijziging aan een reeds opgeleverd rapport dient aangevraagd te worden door het indienen van een nieuwe Werkaanvraag van dit type;
- De optie “Opvragen van een occasionele algemene controle onder de vorm van een éénmalig rapport door de lijnmanager over het internetgebruik van de personeelsleden van zijn een Entiteit (binnen de grenzen van de gedragscode ICT)” betreft het verzamelen en de inzage van globale on-line communicatiegegevens die tijdens een beperkte periode werden gegenereerd.
 - Het éénmalig rapport met de in de Werkaanvraag gespecificeerde gegevens (zoals lijst bezochte websites, frequentie en volume doorgestuurde informatie, startdatum en einddatum van het gewenste rapport, ...) wordt opgesteld;
 - Het gaat hier over een algemene eenmalige controle van een groep personen op basis waarvan geen gegevens over het internetgebruik van een individu kunnen worden afgeleid;
- De optie “Opvragen van een individuele controle onder de vorm van een éénmalig rapport door lijnmanager over het internetgebruik van een individu (binnen de grenzen van de gedragscode ICT)” betreft het verzamelen en de inzage van globale on-line communicatiegegevens die tijdens een beperkte periode werden gegenereerd en betrekking hebben op een individu.
 - De aanvrager specificeert welke informatie gerapporteerd moet worden, zoals lijst bezochte websites, frequentie en volume doorgestuurde informatie, uur en tijdperk van internet surfen, startdatum en einddatum van het gewenste rapport, ...;
 - Het gaat hier over een individuele controle binnen een Entiteit;

1.4.2.1.3 Werkaanvraag voor het aanmaken/verwijderen van een draadloos internetaccount (VO-Werknemer)

Deze Dienst geeft de mogelijkheid aan ambtenaren om op eenvoudige manier een internettoegang te

bekomen. De doelgroep voor deze Dienst zijn Gebruikers die via de WLAN in de gebouwen van de Vlaamse overheid willen connecteren met het internet van op mobiel toestel dat niet in beheer is bij één van de ICT-Dienstverleners in het Ecosysteem.

Het via deze Werkaanvraag besteld draadloos internetaccount heeft geen vervaltijd maar indien het account 1 jaar op non actief staat wordt het automatisch verwijderd en dient het opnieuw aangevraagd te worden. Deze Dienst is enkel mogelijk voor “bestaande gebruikers”. Met “bestaande gebruikers” worden gebruikers bedoeld die reeds beschikken over een GebruikersID. Indien er nog geen GebruikersID geactiveerd is kan die aangevraagd worden bij de ICT-Dienstverlener van de Werkplekdiensten of bij de lokale beheerder in de eigen organisatie die dit zelf kan uitvoeren via WebIDM.

Nadat de Werkaanvraag is besteld ontvangt de Gebruiker 2 e-mails:

- In de eerste e-mail wordt de gebruikeraccount vermeld
- De tweede e-mail bevat het paswoord van de SSID account.

1.4.2.1.4 Werkaanvraag voor het aanmaken/wijzigen of verwijderen van een DNS record

Deze Dienst richt zich op Klanten die gebruik maken van de centrale DNS services voor hun toepassingen die niet in beheer zijn van de ICT-Dienstverlener en die ergens op het internet gehost zijn. DNS aanpassingen kunnen veel doestellingen hebben (bv. link instellen tussen verschillende domeinnamen, name servers wijzigen, ...).

De uitvoering zal in 2 stappen gebeuren. In eerste instantie wordt er een impactanalyse van de aanvraag uitgevoerd om na te gaan of de wijziging geen consequenties heeft op andere Diensten die gebruik maken van DNS records. Zodra er duidelijkheid is wordt de aanvraag uitgevoerd.

Indien uit de impactanalyse blijkt dat er ook een aanpassing van de proxy.pac file nodig is dan wordt deze Werkaanvraag automatisch op afgesproken datum uitgevoerd.

1.4.2.1.5 Werkaanvraag voor het aanpassen van datastromen op een klanteigen firewall

Via deze Dienst kan de Klant aan de ICT-Dienstverlener een aanvraag doen voor het aanpassen van datastromen op een klanteigen firewall.

Deze firewalls worden door de ICT-Dienstverlener beschikbaar gehouden maar op vraag van de Klant is het mogelijk om via deze Dienst bijkomende datastromen open te zetten.

Het aanvragen van aanpassingen op een gemeenschappelijke firewall zal op basis van ondersteuning in regie of als onderdeel van een Project uitgevoerd worden.

1.4.2.1.6 Werkaanvragen voor het patchen van netwerkaansluitingen (1 tot 5) op éénzelfde verdieping

Deze Werkaanvraag betreft het patchen van één tot vijf netwerkaansluitingen op éénzelfde verdieping. In de verschillende gebouwen van de Vlaamse overheid zijn er per zone datalokaaltjes aanwezig waarin de centrale netwerkcomponenten voor die zone gecentraliseerd worden. Het patchen betreft het fysiek connecteren van de netwerkkabels die vanuit de diverse werkplekken toekomen in deze datalokalen met deze centrale netwerkcomponenten.

Deze Dienst capteert het aansluiten van beheerde of niet beheerde toestellen (o.a. desktop, dockingstations, printers, frankeermachines, badgelezers, pelletkachels, ...).

Om dit te realiseren dient een techniker ter plaatse te gaan.

Afhankelijk van de beschikbare infrastructuur en de wensen van de aanvrager wordt er “gepatcht” naar de juiste werkplekken.

1.4.2.1.7 Werkaanvraag voor het aanpassen van de configuratie van een switchpoort

Deze Dienst laat toe dat Klanten een aanvraag doen bij de ICT-Dienstverlener om de configuratie van een individuele switch poort te wijzigen. Het betreft wijzigingen m.b.t. snelheid, al dan niet duplex, VLAN.

1.4.2.2 Geconcretiseerd door:

De éénmalige aan te vragen Diensten (Eenvoudige Werkaanvragen) in het kader van de netwerkomgeving worden geconcretiseerd door :

- Identificatiegegevens van de Klant (naam, Entiteit, telefoonnummer)
- In geval van “Aanmaken, wijzigen of verwijderen van filtering van internetverkeer”:
 - Lijst van de te blokkeren/deblokkeren categorieën;
 - Lijst van de te blokkeren/deblokkeren url's of web-applicaties;
 - Permanente blokkering of blokkering op voorgedefinieerde tijdstippen;
 - Gevraagd advies rond categorieën inclusief uitleg rond mogelijke impact van blokkering van specifieke categorieën.
- In het geval van “Controleren van het internetgebruik door de lijnmanager”:
 - E-mail adres waarheen het rapport dient te worden verstuurd;
 - In geval van (permanente of occasionele) algemene controle, de Entiteit waarvoor de controle moet opgezet worden;
 - In geval van een occasionele algemene controle of een individuele controle, de start- en einddatum van het gewenste rapport;
 - Welke informatie gerapporteerd moet worden, zoals totaal internet verbruik, top URL categorieën, lijst bezochte websites , tijdstip, duur, ...
- In het geval van “aanmaken/verlengen/verwijderen van een draadloos internetaccount (VO-Werknemer) voor 1 jaar”
 - Identificatiegegevens van de betrokken Gebruiker inclusief GebruikersID;
- In het geval van “Aanmaken/wijzigen of verwijderen van een DNS record” - Identificatie van het type DNS record
 - Identificatie DNS record
 - Eventueel aanduiding of proxy.pac moet aangepast worden
- In het geval van “aanpassen van datastromen op een klanteigen firewall”
 - Identificatie van de betrokken firewall infrastructuur;
 - Aan te passen of toe te voegen firewall policy
- In het geval van “patchen van netwerkaansluitingen (1 tot 5) op éénzelfde verdieping”
 - Identificatie van de locatie;
- In het geval van “Wijzigen van de configuratie van een switchpoort”:
 - Identificatie van de betrokken switchpoort;
 - Omschrijving en motivatie van de gewenst wijziging;

1.4.2.3 SLA

1.4.2.3.1 Tijdige uitvoering van éénmalige Diensten

Beschrijving en definitie

Met betrekking tot tijdige uitvoering wordt een onderscheid gemaakt tussen Werkaanvragen met een hieronder vastgelegde uitvoeringstermijn en een uitvoeringstermijn die met de Klant wordt afgesproken voor het realiseren van de Dienst .

De Klant moet zijn keuze kunnen opgeven bij het bestellen van de Werkaanvraag.

Indien de Klant in zijn Werkaanvraag expliciet melding maakt van een uitvoeringstermijn of via mail met de ICT-Dienstverlener een uitvoeringstermijn (in Werkdagen) afspreekt dan is deze uitvoeringstermijn de Contractuele Service Level. De reële uitvoeringstermijn moet aldus kleiner of gelijk zijn aan de

afgesproken uitvoeringstermijn. De Klant(en) wordt steeds op voorhand verwittigd indien de tijdslijm niet kan gerespecteerd worden.

	Service Level(uitvoeringstermijn)
Aanmaken, wijzigen of verwijderen van filtering van internetverkeer	1 uur (urgent change)
Aanmaken, wijzigen of verwijderen van filtering van internetverkeer	Einde volgende Werkdag
Aanmaken, wijzigen of verwijderen van filtering van internetverkeer	Afgesproken termijn (minimaal 5 Werkdagen)
Controleren van het internetgebruik binnen de ICT-gedragcode	Afgesproken termijn (minimaal 10 Werkdagen)
Aanmaken/verwijderen draadloos internetaccount (VO-Werknemer)	Einde volgende Werkdag
Aanvragen voor het aanmaken/wijzigen of verwijderen van een DNS record zonder aanpassing proxy	1 uur
Aanvragen voor het aanmaken/wijzigen of verwijderen van een DNS record zonder aanpassing proxy	Einde volgende Werkdag
Aanvragen voor het aanmaken/wijzigen of verwijderen van een DNS record zonder aanpassing proxy	Afgesproken termijn (minimaal 5 Werkdagen)
<i>Aanpassing datastromen op een klanteigen Firewall op basis van door de Klant ingevuld elektronisch formulier</i>	Einde volgende werkdag
<i>Aanpassing datastromen op een klanteigen Firewall op basis van door de Klant ingevuld elektronisch formulier</i>	Afgesproken termijn (minimaal 5 Werkdagen)
Patchen van één tot vijf netwerkaansluitingen op éénzelfde verdieping	Einde volgende werkdag
Aanvraag aanpassing switchpoortconfiguratie	Einde volgende werkdag

Service Level

De met de Klant afgesproken uitvoeringstermijn moet in 100 % van de transacties die door een Kant in de betrokken maand werden aangevraagd gehaald worden.

Randvoorwaarden, assumpties en uitzonderingen

Voor de uitvoering van deze Diensten stopt de SLA klok vanaf het moment dat de juiste uitvoering van de Werkaanvraag extra input of bevestiging van de aanvrager eist tot op het moment dat deze informatie teruggekoppeld wordt aan de ICT-Dienstverlener.

Meetelementen en –methode

Voor elke Werkaanvraag wordt op de Service desk het tijdstip van indiening van de Werkaanvraag en het tijdstip van afsluiten geregistreerd. Indien de Werkaanvraag uit verschillende Diensten bestaat worden dezelfde gegevens per Dienst geregistreerd.

De registratie bestaat uit:

- Datum en uur van indiening de Werkaanvraag;

- Datum en uur waarop de uitvoering van de Dienst kan starten indien binnen dezelfde Werkaanvraag een afhankelijke Dienst besteld werd waarop de uitvoering van deze Dienst moet wachten;
- Datum en uur van het einde van de uitvoering van alle activiteiten m.b.t. de Dienst;
- Datum en uur goedkeuring door de Klant van de Dienst/Werkaanvraag;

Mislukt een eerste poging om de Dienst succesvol uit te voeren, dan volgt hiervoor niet de goedkeuring door de Klant, maar een terugmelding door de Klant naar de Service desk zodat dit geregistreerd en opgevolgd kan worden. De uitvoering van de Dienst wordt pas afgesloten na succesvolle afwerking ervan en na expliciete goedkeuring door de Klant en na aanpassing van de gegevens in de Configuratiebank. Ingeval een terugmelding gebeurt, omdat de Klant niet tevreden is over de uitvoering (zowel op niveau van de Werkaanvraag als op het niveau van de Dienst), wordt de registratie als volgt aangevuld:

- Datum en uur van deze terugmelding;
- Datum en uur van het einde van de nieuwe acties;
- Datum en uur goedkeuring door de Klant;

De registratie herhaalt zich tot het moment dat de Klant zijn goedkeuring geeft.

Na goedkeuring door de Klant van de Dienst:

- Datum en uur afsluiten van Dienst/Werkaanvraag;

De volledige uitvoeringstermijn voor een Dienst wordt berekend als volgt:

- De looptijd tussen het tijdstip waarop de Dienst toekomt bij de Service desk (=datum van indiening) of het tijdstip dat de uitvoering kan starten (in het geval een afhankelijke Dienst besteld binnen dezelfde Werkaanvraag is uitgevoerd) en het tijdstip van het einde van de uitvoering van alle activiteiten van de Dienst volgens de ICT-Dienstverlener;
- Indien de interventie niet wordt goedgekeurd door de Klant en er bijgevolg een terugmelding gebeurt, wordt de uitvoeringstermijn vermeerderd met de tijd tussen begin- en eindtijd van elke bijkomende activiteit, totdat de Klant de Dienst heeft goedgekeurd.

Dit betekent dat de uitvoeringstermijn, die zal getoetst worden aan de Service Level, enkel de effectieve uitvoeringstermijn berekent tot de Dienst is afgesloten, en niet de tijd nodig voor goedkeuring door de Klant.

Voor de éénmalige Diensten waar de Service Level 1 uur (urgent change) is loopt de SLA-klok enkel door tijdens de Kantooruren.

1.4.2.4 Prijsmechanisme

De prijzen voor de éénmalige Diensten i.k.v. de netwerkomgeving wordt bepaald op basis van de Eenheidsprijzen door de Diensten die in de voorbije maand werden goedgekeurd voor afsluiten (zie Eenheidsprijzen netwerken Werkaanvragen);

1.4.2.5 Facturatie

De factuur bevat de in de afgelopen maand afgesloten en door de Klant geaccepteerde Werkaanvragen.

1.4.2.6 Rapportering

De rapportering van de éénmalige Diensten bestaat uit:

- een maandelijks rapport per Klant met een overzicht van alle openstaande Werkaanvragen;
- een maandelijks rapport per Klant met de in de betrokken maand afgesloten Werkaanvragen, de reële uitvoeringstermijn en de Contractuele Service Level.

1.4.3 Ondersteuning in regie m.b.t. de netwerkomgeving

1.4.3.1 Scope en doel

Naast de recurrente taken die reeds inbegrepen zijn in de Diensten voor de uitbating van de netwerkomgeving (zie paragraaf 1.4.1) kan, in functie van de met de Klant gemaakte afspraken, ook het uitvoeren van ad hoc taken via deze Dienst besteld worden. De aard van de ad hoc taken kan velerlei zijn doch is altijd gekoppeld aan bestaande Exploitatiediensten. Via deze Dienst is het dus niet mogelijk om in regie de volledige exploitatie van een netwerkomgeving te laten uitvoeren. Op vraag van de Klant kan samen met de Service Delivery Manager een prognose opgesteld worden van het aantal en de aard van dergelijke kleine aanpassingen die verwacht worden in het komende jaar. Op basis van deze prognose kunnen in de loop van het jaar opdrachten gegeven worden door de bij de Klant hiertoe aangewezen personen, om kleine aanpassingen in middelenverbintenis uit te voeren.

De ICT-Dienstverlener richt de nodige processen, procedures in om dit soort aanvragen snel en vlot te laten verlopen. Liefst wordt hiervoor een web-based project management and issue tracking tool (bv redmine) ingezet die de ICT-Dienstverlener ter beschikking stelt. M.b.t. de opvolging van deze opdrachten en de eraan gekoppelde taken is er een volledige transparantie voor de Klant op basis van een toegang voor de Klant in de Ondersteunende tool.

Het kan over alle wijzigingen gaan waarvoor het niet mogelijk of niet efficiënt zou zijn om dit te realiseren via het Dienstenpakket “Infrastructuurprojecten m.b.t. de netwerkomgeving” of via “Werkaanvragen m.b.t. de netwerkomgeving”.

Voorbeelden van dergelijke kleine wijzigingen zijn:

- Vervangingen van WLAN access point in het kader van incident management;
- Kleine aanpassingen aan de firewall configuraties;
- Kleine aanpassingen aan een bestaand netwerk in een gebouw (extra switch, extra lijn,...);
- Inrichting tijdelijke netwerken (pop-up lokaties);
- Netwerkondersteuning bij events;
- Wifi site survey
- Allerlei kleine operationele ingrepen
-

De raming van het aantal te voorziene VTE's per Profiel voor het uitvoeren van deze ad hoc taken en de afspraken m.b.t. de wijze waarop dergelijke opdrachten worden gegeven, worden door de ICT-Dienstverlener gedocumenteerd in de processen.

M.b.t. ondersteuning in regie aangaande de connectiviteit zal vanuit dit Dienstenpakket moeten samengewerkt worden met andere dienstverleners:

- MOW voor wat betreft Vlaamse glasvezel ;
- Mogelijks andere operatoren voor WAN bandbreedte voor locaties waar geen Vlaams glas mogelijk/wenselijk is
- De fysieke bekabeling in de gebouwen die door een andere dienstverlener geleverd worden

1.4.3.2 Geconcretiseerd door

De opdrachten voor “Ondersteuning in regie” in het kader van de netwerkgeving worden geconcretiseerd door :

- Identificatiegegevens van de Klant (naam, Entiteit, telefoonnummer);
- Een duidelijke omschrijving van de opdracht en uit te voeren taken;
- Een jaarlijkse prognose van het aantal en de aard van de uit te voeren taken.

1.4.3.3 SLA

Deze ad hoc taken worden in onderling overleg met de Klant uitgevoerd. De uitvoeringstermijn dient steeds in overleg met Klant te worden afgesproken.

1.4.3.4 Prijsmechanisme

De prijzen voor de prestaties voor kleine aanpassingen via “Ondersteuning in regie m.b.t. de netwerkgeving” worden bepaald op basis van de geldende Eenheidsprijzen van de betrokken Profielen die ingezet worden voor het uitvoeren ervan. Deze Eenheidsprijzen zijn opgenomen in de Eenheidsprijzen netwerken Profielen.

1.4.3.5 Facturatie

De facturatie gebeurt maandelijks en de factuur bevat:

- het totaal van de prestaties m.b.t. de kleine aanpassingen op basis van de door de Klant goedgekeurde prestatieregisters.

1.4.3.6 Rapportering

Maandelijks rapport of meekijk in de tool m.b.t. de prestaties uitgevoerd in de betrokken maand gekoppeld aan de unieke identificatie van de opdracht waarin de prestaties kaderen.

1.4.4 Infrastructuurprojecten m.b.t. de netwerkgeving

1.4.4.1 Scope en doel

Grotere wijzigingen aan de dienstverlening m.b.t. de netwerkdiensten dienen projectmatig aangepakt te worden. Het kan gaan om alle wijzigingen in de netwerkgeving, studies, aanvullingen die niet via een Werkaanvraag of via een ondersteuning in regie kunnen uitgevoerd worden. De Projecten kunnen betrekking hebben op netwerk- en beveiligingsinfrastructuur of kunnen onderdeel zijn van een globaal Project dat ruimer kadert dan de dienstverlening in deze Service Portfolio. In dit laatste geval zal de ICT-Dienstverlener moeten samenwerken met andere ICT-Dienstverleners o.b.v. de afspraken die opgenomen worden in het Projectvoorstel.

Het doel van dit Dienstenpakket is het uitvoeren van alle nodige activiteiten om een Project te realiseren. Het rapporteren, het geven van feedback aan de projectleider van de Klant aangaande de voortgang van het Project en alle niet nader opgesomde maar normaal geachte projectactiviteiten maken eveneens deel uit van de scope van dit Dienstenpakket.

De Diensten kunnen afgenomen en uitgevoerd worden in projectvorm met bijhorend

projectmanagement. Ingeval van Projecten wordt naargelang het geval geopteerd voor een realisatie in resultaatsverbintenis of in middelenverbintenis, of de variant Target cost (zie verder).

Alle Projecten moeten uitgevoerd worden conform de beschrijving van het proces Projectmanagement in het document “Vereisten Ondersteunende Processen en Overlegfora”.

Er kunnen een aantal veel voorkomende types van Projecten onderkend worden waarvoor de te doorlopen fasen en de op te leveren specifieke Werkproducten vooraf kunnen bepaald worden.

Hierna volgt een mogelijke niet limitatieve lijst van dergelijke projecttypes:

- Het realiseren van een nieuwe infrastructuuromgeving: Het einddoel is het beschikbaar stellen van een nieuwe infrastructuuromgeving die operationeel is en aan de noden van de Klant voldoet;
- Het aanpassen van een bestaande infrastructuuromgeving: Het einddoel is een gewijzigde infrastructuur die operationeel is en aan de gewijzigde behoeften van de Klant voldoet. Hiertoe behoort eveneens het aanpassen van de actuele infrastructuur naar aanleiding van structurele veranderingen als gevolg van onvoorzienbare omstandigheden of als gevolg van veranderingen in de technologie markt. Deze Projecten kunnen ook betrekking hebben op optimalisatie en automatisatie van de infrastructuuromgeving;
- Het overnemen en/of integreren en of overdragen/isoleren van een bestaande infrastructuuromgeving. Dit betreft bijvoorbeeld de onboarding van nieuwe Klanten;
- Het realiseren van bijkomende aansluitingen op het VO-WAN. Hierbij moet het mogelijk zijn een keuze te maken uit een aantal opties m.b.t. o.a. de bandbreedte, de redundantie en met een QoS optie waar technisch mogelijk. Dit dient specifiek per aanvraag te worden geconcretiseerd.
- Het realiseren van bijkomende beveiligde aansluitingen van partner netwerken op het VO-netwerk.
- Het realiseren van een zekere autonomie op de shared Internet infrastructuur voor de Entiteiten die dit wensen d.m.v. het opzetten van een logisch gescheiden beveiligde Internet toegang waarbij het veiligheidsbeleid door de te Entiteit zelf kan worden ingevuld, bijv. middels afgescheiden URL filtering, firewall policies in beheer van de Entiteit zelf.
- Het projectmatig stopzetten van Exploitatiediensten waarvoor er geen expliciete Werkaanvraag is opgenomen in de Service Portfolio.
- Het initiëren of verlengen van VO-specifieke contracten. Voor wat het verlengen betreft gaat het om verlengingen waarbij er significante wijzigingen zijn van het voorwerp of verhoging van de prijs. Andere verlengingen gebeuren conform de bepalingen in het hoofdstuk “Beheer van subcontracten en aankoop” in het document Vereisten Ondersteunende Processen en Overlegfora.
- Het inkantelen van een Klant voor afname van een gedeelde managed netwerkdienst of het uitstappen van een Klant uit een gedeelde managed netwerkdienst. Hierbij moet het afhankelijk van welke gedeelde managed netwerkomgeving het betreft mogelijk zijn een keuze te maken uit een aantal opties m.b.t. o.a. type dienst, wijze van afname volume, verwacht gebruik, Voor dit type van Project wordt ook een voorafgaand advies gevraagd aan de productmanager voor netwerken bij Digitaal Vlaanderen.

M.b.t. Projecten aangaande de connectiviteit zal vanuit dit Dienstenpakket moeten samengewerkt worden met andere dienstverleners:

- MOW voor wat betreft Vlaamse glasvezel ;
- Mogelijks andere operatoren voor WAN bandbreedte voor locaties waar geen Vlaams glas mogelijk/wenselijk is
- De dienstverlener(s) die instaan voor de fysieke bekabeling in de gebouwen van de Klant.

1.4.4.2 Geconcretiseerd door

Een Project zal in principe steeds starten met een Werkaanvraag voor het opmaken van een Projectvoorstel. Nadien volgen dan een of meerdere Werkaanvragen voor de bestelling van opeenvolgende fasen (overeenkomstig de offerte) of desgevallend voor het bestellen van wijzigingen aan de oorspronkelijk vooropgestelde uitvoering.

De Klant dient in zijn Werkaanvraag voor de opmaak van een Projectvoorstel steeds de volgende elementen op te nemen:

- De identificatiegegevens van de Klant: de organisatorische eenheid en de naam van de persoon die voor dit Project bevoegd is om beslissingen te nemen voor de Klant (projectleider van de Klant) en die dus o.a. de PV van Oplevering zal tekenen;
- De omschrijving van de huidige situatie, duiden van de huidige problematiek;
- De omschrijving van de gewenste situatie: geven van een visie van waar men naartoe wil en omschrijving van wat men wil bereiken (doelstellingen);
- De precisering van de gewenste Werkproducten;
- De functionele vereisten: beschrijving van de functionaliteiten die verwacht worden van de te realiseren omgeving;
- De niet-functionele vereisten: Beschrijving van niet-functionele eisen waaraan de voorgestelde oplossing moet voldoen (bijvoorbeeld flexibiliteit, documentatie, uitbreidbaarheid, capaciteit, interfaces, performantie, aanduiding van specifieke SLA, beschikbaarheid, , veiligheidsvereisten (o.a. m.b.t. Persoonsgegevens), ...);
- Eventuele locatie-vereisten. In het bijzonder indien de Klant eist dat alle of bepaalde activiteiten op een locatie bij de Klant moeten worden uitgevoerd.
- De aard van de verbintenis: resultaatsverbintenis of middelenverbintenis of target based cost;
- De bijlagen: een lijst van documenten, die als bijlage (of via een referentie (link) naar een elektronische versie in een daarvoor geëigend systeem dat voor alle voor alle partijen toegankelijk is) zijn opgenomen (bijvoorbeeld bestaande installatiedossier, exploitatiedossier, broncodes,...).

Afhankelijke van het type Project komen hierbij nog volgende gegevens bij:

- Voor bestellingen m.b.t. VO-WAN aansluitingen:
 - De identificatie van de betrokken Site(s);
 - De gewenste dienstverlening: nieuwe aansluiting, uit dienst nemen aansluiting, wijzigen van de specificaties van de aansluiting (bv bandbreedte , technologie, ...)
 - Het gewenste beschikbaarheidsniveau (mogelijkheid van redundantie) – al dan niet ontdubbelde aansluiting op de backbone;
 - De optie om een Klant specifiek VPN netwerk op te zetten;
- Voor bestellingen m.b.t. het opzetten van partnerkoppeling betreft het o.a. volgende stappen:
 - Identificatie van de partner en zijn relatie met Vlaamse overheid.
 - Classificatie van de partner (bijv. extern)

- Autorisatie tot opzetten van partnerconnectie met de Vlaamse overheid
- Technische gegevens: gewenste fysieke aansluiting, bandbreedte, type lijn, etc.
- Het autoriseren van datastromen tussen de functionele componenten
- Het opzetten van een datastroom
- Logging van gegevens (onder bepaalde voorwaarden)
- Bijhouden en onderhouden documentatie over de opgezette verbinding
- Voor bestellingen m.b.t. het opzetten van beveiligd VO-ISP betreft het o.a. volgende stappen:
 - Identificatie van de partner.
 - Autorisatie tot opzetten van VO-ISP met de Vlaamse overheid
 - Technische gegevens: gewenste fysieke aansluiting, bandbreedte, type lijn, etc.
 - Logging van gegevens (onder bepaalde voorwaarden)
 - Bijhouden en onderhouden documentatie over de opgezette verbinding

De volledigheid en de mate van detail waarin bovenstaande elementen beschreven dienen te worden, is afhankelijk van het type Project en van het feit of het om een nieuwe infrastructuur gaat dan wel om een aanpassing aan de bestaande ICT-infrastructuur.

In de Werkaanvragen voor de bestelling van de uitvoering van de Project of projectfase zal de Klant verwijzen naar het betrokken Projectvoorstel.

In een Werkaanvraag voor de bestelling van een projectwijziging, verwijst de Klant naar

- het bestelde Project waarop de wijziging betrekking heeft
- een vooraf opgesteld wijzigingsvoorstel, dat werd opgesteld als onderdeel van wijzigingsbeheer in de projectuitvoering, en dat het doel, het bereik en de impact van de wijziging op alle projectaspecten (planning, scope, kosten, ...) helder beschrijft.

1.4.4.3 Uitvoering

1.4.4.3.1 Werkaanvraag voor opmaken van een Projectvoorstel

Deze Dienst wordt geïnitieerd via het indienen van een Werkaanvraag voor het opmaken van een Projectvoorstel en eindigt bij de Oplevering (via een PV van Oplevering), facturatie en betaling door de Klant van de laatste projectfase.

Inhoud

Een Projectvoorstel geeft o.a. aan tegen welke prijs en met welke doorlooptijd de ICT-Dienstverlener een Project of specifieke projectdelen van een Project dient uit te voeren. Het Projectvoorstel omvat minstens een projectplan met o.a. een duidelijke omschrijving van het bereik, de te bekomen projectresultaten of op te leveren producten (in de zin van Prince-2), de planning (bijv. GANTT) en de prijs.

De aspecten scope, tijd en kost komen expliciet aan bod, en worden in een consistente verhouding tot elkaar opgenomen in het Projectvoorstel, conform aan de vooropgestelde projectmethodiek.

Aanpak van de offerteopmaak

De ICT-Dienstverlener bereidt een professionele offerte voor die een geschikt antwoord biedt op de geformuleerde Werkaanvraag. Waar nodig of waar expliciet als werkwijze voorzien en gevraagd, wordt er afgestemd met de Klant:

- Meestal zal in de opmaakfase een afstemmingsgesprek met de Klant gebeuren, om de verwachtingen en vereisten scherp te stellen en toe te laten een correct Projectvoorstel neer te leggen dat daarmee maximaal overeenstemt.
- Eventueel wordt afgesproken om tijdens offerteopmaak een preliminaire voorstelling te doen van de oplossing die zou worden voorgesteld, t.t.z.. 'pitching' van een oplossingsalternatief en -aanpak, waarbij in beperkte sessie de oplossingspiste wordt gepresenteerd en afgetoetst met de Klant, of een essentieel element van oplossing wordt getoetst aan de klantverwachting.

Termijn

De termijn voor het opmaken van een Projectvoorstel wordt gemeten d.m.v. metrieken beschreven onder Projectmanagement in het document "Vereisten Ondersteunende Processen en Overlegfora".

De offerteopmaak moet in elk geval zo spoedig mogelijk na de aanvraag effectief opgenomen en aangevat worden, en moet een beperkte doorlooptijd kennen. Een verwachte antwoorddatum (NDD) kan worden afgesproken of bijgesteld tijdens de offerteopmaak, met akkoord van de Klant, indien voortschrijdend inzicht leidt tot een aangepaste opdrachtformulering of er belangrijke aangepaste verwachtingen inzake de oplossing zijn, die nopen tot (gedeeltelijke) herwerking van een gevorderd ontwerp van Projectvoorstel.

Indien de ICT-Dienstverlener meent dat er geen professioneel antwoord kan geleverd worden binnen een voor een dergelijke offerteopmaak redelijke termijn, omdat er in aanzienlijk meer of langer durende voorbereidingen nodig zijn om zover te geraken als in de aanvraag werd gesteld, dan is het wenselijk om dit als dusdanig met de aanvrager te bespreken en een preliminair voorbereidingstraject als bestelbaar Projectvoorstel voor te stellen. De uitvoering en het resultaat daarvan zal vervolgens toelaten om een professioneel en geschikt antwoord te bieden op de oorspronkelijke vraagstelling, en dit bestelbaar voor te leggen als Projectvoorstel.

Voor alle Projectvoorstellen wordt een geldigheidstermijn van minstens 3 maanden gerespecteerd, of een andersluidende geldigheidsperiode en dus uiterste besteldatum mits de nodige valabele verantwoording op basis van objectieve elementen van het Projectvoorstel.

Product-focus

Bij een Project heeft de Klant steeds een bepaald resultaat voor ogen. In functie van het gewenste resultaat en van de vertreksituatie zullen meer of minder activiteiten moeten uitgevoerd worden.

Naast de generieke Werkproducten die bij ieder Project noodzakelijk zijn in het kader van het projectbeheer (onder andere het projectplan) zijn er ook een reeks specifieke Werkproducten die in het kader van het Project zullen moeten geleverd worden. Deze specifieke Werkproducten kunnen voor elk Project verschillend zijn en worden gepreciseerd in het Projectvoorstel. In elk geval moet de projectaanpak methodisch zijn, en in lijn met de betreffende methodiek worden ook de planning, fasering, beheerwijze en uitvoeringsmethode opgenomen, die gericht zijn op en zo effectief mogelijk zullen leiden tot een gewenst en afdoend resultaat.

Passend projectbeheer

De uitvoering van een Project gebeurt, afhankelijk van het type Project, in één of meerdere fasen en resultaatgericht, waarbij het aandeel van de projectmanagement activiteiten (planning, budgettering, opvolging van globale voortgang en oplevering, escalaties en beheer van de klant-relaties i.v.m. het project, projectrapportering, ...) steeds in verhouding zal staan tot het uit te voeren werk. Het voor projectmanagement voorziene bedrag mag maximaal 15% bedragen van het totale bedrag voor prestaties voor het Project. Het aandeel projectmanagement kan per fase in een Project hoger of lager liggen, maar voor het totale Project dient het maximaal percentage gerespecteerd te worden. Enkel in uitzonderlijke gevallen en op basis van concrete argumenten kan hier in het Projectvoorstel van afgeweken worden.

Sjablonen

Als onderdeel van de beschrijving van de Serviceorganisatie dient ook een sjabloon opgesteld en beheerd te worden voor Projectvoorstellen. Hierin bepaalt de ICT-Dienstverlener welke elementen minstens dienen opgenomen te worden in een Projectvoorstel. Meerdere sjablonen zijn mogelijk per onderscheiden projecttype of methodiek. In functie van een vormelijke en inhoudelijke consistentie van de projectvoorstellen over de dienstverleners heen, wordt dit maximaal afgestemd met de andere ICT-Dienstverleners, en met de ICT-Dienstverlener voor de integratiediensten en het Bestuur.

Algemeen

De output van alle voorgaande fasen vormen de input voor de fase uit de projectlevenscyclus waarop het Projectvoorstel betrekking heeft.

De Klant staat centraal m.b.t. de specificatie van de verwachtingen en de vereisten, en zal ook alle Werkproducten accepteren; voor beide zal hij een gedegen begeleiding krijgen vanwege de ICT-Dienstverlener.

1.4.4.3.2 Werkaanvraag voor uitvoering van een Project of projectfase

Op basis van het ontvangen Projectvoorstel kan de Klant beslissen om de uitvoering van het Project (of van een of meerdere projectfasen) te bestellen.

Minstens op het einde van het Project, maar voor zover afgesproken bij de bestelling ook op het einde van een fase van het Project, wordt een Oplevering gevraagd van de betrokken Werkproducten.

Om een Project te realiseren zal de ICT-Dienstverlener gebruik maken van een erkende projectmethodologie (PRINCE2 of gelijkwaardig)..

Voor elk Project wordt afgesproken welke specifieke overlegstructuren er voorzien worden en wat hun respectievelijke bevoegdheden zijn.

Voor elk Project zal er minstens een Project stuurgroep voorzien worden die formele beslissingen kan nemen met betrekking tot het Project. In die Project stuurgroep zal minstens de projectleider van de Klant en de projectleider van de ICT-Dienstverlener zetelen. Minstens bij mijlpalen, dient een Project stuurgroep samengeroepen te worden om het afsluiten van de vorige fase en de start van de volgende fase goed te keuren.

Daarnaast moet er regelmatig ad hoc contact zijn tussen de beide projectleiders.

Bij de start van het Project wordt de “base line” voor uitvoering vastgelegd, conform aan het goedgekeurde Projectvoorstel. Deze kan nadien enkel gewijzigd worden bij formeel goedgekeurde wijzigingen aan het projectplan. Tijdens de realisatie van het Project zal de ICT-Dienstverlener aan de Klant rapporteren conform de afspraken die gemaakt zijn in het Projectvoorstel. Minimaal zal de projectleider van de Klant regelmatig een voortgangsrapportering t.o.v. van het oorspronkelijk projectplan ontvangen. De voortgangsrapportering moet de actuele situatie vergelijken met de “base line”. Hierbij kan gebruik gemaakt worden van “earned value” –berekningen. Bijkomende rapporteringseisen kunnen per Project worden afgesproken.

Na afwerking van de verschillende in het Projectvoorstel vermelde Werkproducten (inclusief Project-documenten) kan de ICT-Dienstverlener aan de Klant vragen om de Oplevering te laten plaatsvinden op basis van de in het Projectvoorstel opgenomen acceptatiecriteria. Voorafgaand zullen (gedeeltelijke) acceptatietesten plaats vinden. Vanaf het moment dat de ICT-Dienstverlener formeel de afwerking van de in het Projectvoorstel opgenomen Werkproducten meldt en de Oplevering vraagt beschikt de Klant over een termijn van één kalendermaand binnen dewelke hij de Oplevering moet uitvoeren, tenzij er in het Projectvoorstel een andere regeling is afgesproken.

De ICT-Dienstverlener dient voor de uitvoering van deze Dienst Profielen in te zetten met de juiste competenties.

1.4.4.3.3 Werkaanvraag voor de bestelling van een projectwijziging

In de loop van de uitvoering van een Project, kan het nodig blijken dat belangrijke wijzigingen aan een Project nodig zijn die formeel dienen te worden besteld en doorgevoerd.

Projectwijzigingen die een wezenlijke impact hebben op de projectuitvoering, worden conform methodologisch bepaalde processen van wijzigingsbeheer (zie bijv. PRINCE-2) voorbereid. Deze voorbereiding resulteert in het opstellen van een onderbouwd en helder wijzigingsvoorstel vanwege de ICT-Dienstverlener, dat aan de Klant wordt voorgelegd voor goedkeuring en bestelling.

De uitvoering van zulke projectwijziging kan besteld worden door de Klant, door het indienen van een Werkaanvraag voor projectwijziging.

De wijziging wordt vervolgens in het Project doorgevoerd, conform het goedgekeurde en bestelde wijzigingsvoorstel. De wijziging zelf wordt volledig geïntegreerd in de (aangepaste) uitvoering van het Project. Een Werkaanvraag voor projectwijziging wordt op zich niet apart opgeleverd.

Ook een opdracht vanwege de Klant om het Project voortijdig te beëindigen, wordt als een dergelijke formeel te bestellen wijziging beschouwd.

1.4.4.4 SLA

1.4.4.4.1 Tijdige uitvoering van Projecten

Beschrijving en definitie

Deze indicator meet de verhouding tussen de effectieve projectduur en de afgesproken projectduur. Indien een Project bestaat uit verschillende afzonderlijk op te leveren fasen dan geldt deze indicator voor elke op te leveren fase. De projectduur start op het ogenblik van de bestelling van het Project (of de betrokken fase) en loopt tot op het ogenblik van de Oplevering van het Project (of de betrokken fase).

Service Level

De effectieve duur (in Werkdagen) voor het Project (of de betrokken fase) mag de afgesproken duur voor het Project (of betrokken fase) met niet meer dan 10% overschrijden. Die toegelaten overschrijding bedraagt 5 Werkdagen voor Projecten met een afgesproken duur van minder dan 50 Werkdagen.

Wanneer een Project uit verschillende afzonderlijk op te leveren fasen bestaat, dan zal bij het niet halen van de vooropgestelde duur voor een bepaalde fase, de einddatum van de daaropvolgende fasen aangepast worden. Echter de duurtijd (aantal Werkdagen) van de daaropvolgende fasen blijft ongewijzigd.

Randvoorwaarden, assumpties en uitzonderingen

In het Projectvoorstel wordt de baseline-planning opgenomen. De planning dient alle activiteiten te omvatten vanaf de bestelling tot de Oplevering. De baseline van een Project kan enkel herzien worden via een beslissing van de Project stuurgroep. Hierbij kunnen eventuele vertragingen te wijten aan de Klant, alsook de gevolgen van eventuele belangrijke wijzigingen in rekening gebracht worden.

Meetelementen en –methode

Op het ogenblik van de bestelling van een Project (of een fase) wordt de besteldatum geregistreerd als aanvangsdatum van het Project (of van de fase). Op basis van deze aanvangsdatum en de in het Projectvoorstel opgenomen planning worden de geplande data geregistreerd voor elke voorziene mijlpaal, waaronder de geplande datum van Oplevering van het Project (of de fase). Naarmate het Project (of de fase) uitgevoerd wordt, worden de effectieve data voor elk van de mijlpalen geregistreerd. Op het ogenblik van Oplevering van het Project (of de fase) wordt dan de effectieve doorlooptijd in Werkdagen, tussen besteldatum of de startdatum van de fase uit de baseline en datum van Oplevering, vergeleken met de geplande doorlooptijd in Werkdagen voor dezelfde periode.

De start- en einddata van Projecten en de eventuele fasen binnen het Project dienen ook geregistreerd te worden in de Gemeenschappelijke Ondersteunende Systemen.

1.4.4.5 Prijsmechanisme

Voor een Project wordt steeds afgerekend op basis van de kosten opgenomen in het Projectvoorstel. De kosten voor het opmaken van het Projectvoorstel zelf, worden verondersteld verrekend te zijn in de algemene Overhead.

De prijs voor deze Dienst bestaat uit de volgende delen :

- De prijs voor de te leveren prestaties;

- De prijs voor de te leveren Producten (Hardware/Software);
- De prijs voor de door Onderaannemers te leveren prestaties (o.a. indien er specifieke competenties vereist zijn waarover de ICT-Dienstverlener niet beschikt)

Voor wat betreft de prijs van de prestaties, zijn er per fase drie opties : in resultaatsverbintenis (RV) tegen vaste prijs, in middelenverbintenis (MV) of volgens Target cost (TC).

Voor de Projecten of projectfasen die in “resultaatsverbintenis” uitgevoerd worden, wordt de uiteindelijk te betalen prijs bepaald door de forfaitaire prijs die bepaald werd in het Projectvoorstel.

Voor de Projecten of projectfasen die in “middelenverbintenis” uitgevoerd worden, wordt de uiteindelijk te betalen prijs bepaald door het reëel gepresteerde aantal uren per Profiel en hun Eenheidsprijs en de werkelijk geleverde Producten met hun Eenheidsprijs. Dit wordt gestaafd op basis van timesheets die wekelijks aan de projectleider van de Klant ter goedkeuring dienen voorgelegd. Bij projectfasen in middelenverbintenis kunnen eventueel wel bepaalde delen in resultaatsverbintenis aangeboden worden.

Target cost zoals in deze Overeenkomst toegepast, betekent:

- Een Target kostprijs wordt vooraf in offerte vastgesteld, voor een geheel van te leveren prestaties. Dit geeft een totaalprijs aan waartegen de fase normaliter gerealiseerd kan worden, en die aldus ook het bedrag aangeeft voor de kostprijs van betreffende fase of project.
- De Target kost komt tot stand door een professionele raming met kennis van zaken, op basis van een zo concrete mogelijke vooropgestelde opdrachtbeschrijving (bijv. user stories), en eventueel na een vorm van onderhandeling. De Target kost is een zo goed als mogelijk ingeschatte kostprijs, die in overeenstemming is met en akkoord kan krijgen van de Klant. Voor opdrachten waar een redelijke inschatting onmogelijk vooraf te maken is, is Target cost niet aangewezen.
- Er wordt ook een “Cap” bedrag vooraf vastgesteld, dat de absolute bovengrens aangeeft. Het kostendeel bovenop een bereikte Cap-kostprijs, wordt niet aangerekend aan de Klant. Per default wordt de Cap vastgesteld op: Target kost + 40%.
- Prestatiekosten waarmee de Target wordt overschreden, tot aan de Cap, worden aan 50% van dit kostendeel aangerekend. Aldus wordt de overschrijding van de Target kostprijs ontmoedigd.
- Indien een fase of project kan worden gerealiseerd met minder dan de geplande prestatieskost van de Target kost, dan wordt het verschil tussen de aangerekende feitelijk geleverde prestaties en de voor dezelfde opdracht geldende Target kost, aan 50% gefactureerd aan de Klant.

Formule:

Factuurprijs voor prestaties = 50% van Target kostprijs + 50% van kostprijs van feitelijke prestaties, en dit tot aan het Cap bedrag.

Voorbeeld ter illustratie: Target = 100K, Cap = 140K. Er zijn daarenboven 20K aan investeringen.

Indien bijv. reëel gepresteerd twv 80K + 20K investeringen

Factuur: 50K (50% target) + 40K (50% van 80K) = 90K + 20K investering = 110K

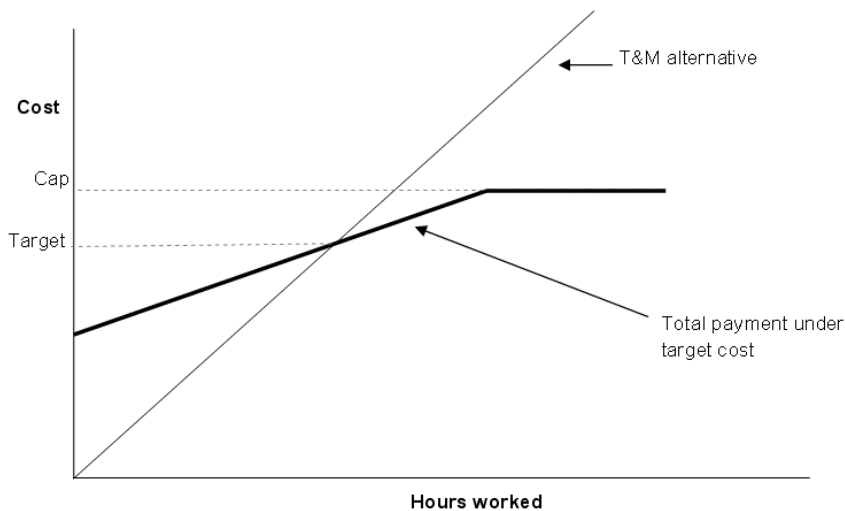
Indien bijv. reëel gepresteerd twv 120K + 20K investeringen

Factuur: 50K + 60K (50% van 120K) = 110K + 20K investering = 130K

Indien bijv. reëel gepresteerd boven Cap, bv. twv 200K prestaties + 20K investeringen

Factuur: CAPPED (50K + 50% x 200K = 150K >140K) = 140K + 20K investering = 160K

Grafisch geschetst (illustratie):



Deze TC-aanpak is bedoeld om het risico bij uitvoering te delen tussen Klant en ICT-Dienstverlener. Een Target kostprijs laat toe om minder risicopremie te verrekenen in de te bestellen totaalprijs, dan wat ingeval van een RV het geval zou zijn. Tegelijk stelt de Target cost een te verwachten totaalprijs, en bovendien nog eens een Cap, in tegenstelling tot een eventueel mogelijke belangrijke prestatie- en kostenverhoging indien een MV opdracht in de uitvoering zou uitlopen ten opzichte van de bij bestelling aangenomen verwachting; in een MV worden alle nodige effectieve prestaties aangerekend.

Een TC aanpak en kostprijs is aangewezen indien er in voldoende mate een normale verwachting ten aanzien van de werklust in de opdracht geraamd of berekend kan worden (de Target), wat bijvoorbeeld het geval is indien er op basis van een voldoende heldere behoeftenformulering een voorafgaande plannings- en ramingsoefening is kunnen gebeuren, waarmee het Target niveau voor betreffende bereik van de opdracht met voldoende vertrouwen vastgesteld is kunnen worden.

Ingeval van Target cost worden eventuele gedeelten tegen een forfaitaire vaste kost zoals investeringen, afzonderlijk behandeld en afgerekend, en deze worden niet in rekening gebracht in bovenvermelde verrekening van prestaties.

Voor wat betreft de door Onderaannemers te leveren prestaties, kunnen de prijzen van Onderaannemers in de offertes opgenomen worden. Deze prijzen dienen overeenkomstig de in rubriek 8.2.3 van het Basiscontract beschreven basisprincipes tot stand te komen. .

1.4.4.6 Prijscorrectie

Er wordt een Prijscorrectie toegepast indien de effectieve duur (in Werkdagen) voor het Project (of de betrokken fase), de afgesproken duur voor het Project (of betrokken fase) met meer dan 10% overschrijdt. Deze Prijscorrectie bedraagt 10% van de prijs (excl. de prijs van de Producten) voor het Project (of de betrokken fase).

De ICT-Dienstverlener kan 50% van de toegepast Prijscorrectie recupereren indien de ICT-Dienstverlener er in slaagt om het volledige Project toch op te leveren voor de vooraf formeel goedgekeurde afgesproken einddatum ('deadline') van het volledige Project, zijnde de uiterste uitvoeringsdatum conform de (baseline planning van) de bestelde offerte.

Indien de effectieve duur (in Werkdagen) voor het Project (of de betrokken fase), de afgesproken duur voor het Project (of betrokken fase) met meer dan 20% overschrijdt heeft de Klant de optie om het Project stop te zetten zonder enige vergoeding aan de ICT-Dienstverlener.

Deze bepaling aangaande Prijscorrectie affecteert geenszins de bepalingen aangaande schadevergoeding die opgenomen zijn in het Basiscontract.

1.4.4.7 Facturatie

Voor Projecten zal de Oplevering per Project of per op te leveren fase van het Project, indien er fasen met afzonderlijke facturatie voorzien zijn, plaatsvinden door de Klant die de bestelling heeft geplaatst. De facturatie gebeurt op basis van een Proces Verbaal van Oplevering.

1.4.4.8 Rapportering

Tijdens de uitvoering van een Project dient in een gemeenschappelijk met de Klant gedeeld documentatiesysteem een projectfolder up-to-date gehouden te worden met minstens de volgende elementen:

- Het goedgekeurde Projectvoorstel
- De eventueel goedgekeurde wijzigingen
- De actuele planning (GANTT)
- Het verslag van o.a. stuurgroep vergaderingen
- Voortgangsrapporteringen
- De documentaire Werkproducten
- De PV's van Oplevering

De Klant (voor de door hem aangevraagde Projecten) en het Bestuur (voor het geheel van de aangevraagde Projecten) dienen op ieder ogenblik via intranet toegang te krijgen tot de informatiesystemen. Dit moet toelaten om een rapport te genereren met minstens de volgende elementen :

- Identificatie van het Programma waartoe het Project behoort (optioneel en in te geven door de Klant);
- Identificatienummer van het Project (Werkaanvraagnummer);
- Korte omschrijving van het Project;
- Identificatie van de Klant;
- Datum indiening Werkaanvraag;

- Datum beschikbaarheid bestelbaar Projectvoorstel;
- Datum vastlegging (door Klant in te geven datum);
- Identificatie van de fase;
- Korte omschrijving van de fase;
- Datum bestelling (van de uitvoering van het Project als geheel of van de betrokken fase);
- Datum Oplevering (van de fase of van het Project);

1.5 Transitie

1.5.1 Initiële Transitie

De algemene bepalingen van de Initiële Transitie zijn opgenomen in het Basiscontract (Hoofdstuk 9).

De Transitie van de netwerkdienstverlening is onderdeel van de Initiële Transitie van het totale Ecosysteem van de ICT-Dienstverlening. De Service Integrator staat in voor het overkoepelend programma-management voor de transitie van het Ecosysteem. Elke ICT-Dienstverlener staat weliswaar in voor het eigen Transitieproject, maar het overkoepelend programma-management wordt opgenomen door de Service Integrator en alle ICT-Dienstverleners moeten hun medewerking hieraan verlenen.

Alle kosten voor het Transitieproject, dus zowel de kosten voor het overnemen van het beheer van de bestaande omgevingen en voor het inrichten van de dienstverlening tegen 1/2/2022 als de kosten voor de verdere optimalisatie na 1/2/2022 moeten verrekend worden in de Eenheidsprijzen voor de dienstverlening tijdens de uitvoering van de Overeenkomst o.b.v. van een transparante versleuteling in de kostenmodellen. Dit betekent dat in de Financiële bijlage de totaalprijs voor de uitvoering van het Transitieproject voor de netwerkdiensten op 0 Euro wordt vastgezet.

Alle functies die deel uitmaken van de huidige netwerk omgeving en dus actief draaien op de huidige infrastructuur zoals beschreven de Referentiebibliotheek, dienen minimaal overgenomen te worden in de nieuwe gevraagde oplossingen en Diensten. De ICT-Dienstverlener staat in voor een vlekkeloze migratie door proactief alle vereiste maatregelen te nemen teneinde onderbrekingen van de Diensten tot het strikte minimum te beperken en aldus de continuïteit maximaal te garanderen. Voorts dient de veiligheid van de informatiestromen op elk gegeven moment tijdens de verschillende migraties gewaarborgd te blijven.

De migratie van de netwerkdienstverlening dient uitgevoerd te worden als een Project in Resultaatsverbintenis.

Er wordt van de ICT-Dienstverlener verwacht dat hij volgende projectondersteuning voorziet:

- Een projectorganisatie met een projectleider en team dat verantwoordelijk is voor de opvolging, de coördinatie en de bijsturing van het Transitieproject voor de netwerkdienstverlening;
- Een vertegenwoordiging in de Stuurgroep Transitieproject van het Ecosysteem van ICT-Diensten dat de Initiële Transitie voor het geheel van ICT-Diensten opvolgt;
- De ICT-Dienstverlener geeft een duidelijke omschrijving van het aantal VTE's, de functies en rollen met bijhorende competentieprofielen die door de ICT-Dienstverlener zullen ingezet worden tijdens de uitvoering van het transitieplan;
- De ICT-Dienstverlener geeft een duidelijke planning op voor het Transitieproject van de netwerkdiensten met minimaal een Gantt chart, een overzicht van de mijlpalen met per mijlpaal de op te leveren werkproducten, een lijst van risico's en bijbehorende mitigerende maatregelen, ...

Onvermijdelijke dienstonderbrekingen dienen gepland te worden in de periodes dat de activiteit het laagst is. Er dient steeds een rollback procedure te worden voorzien teneinde adhoc de stabiliteit te kunnen herstellen bij onvoorziene problemen. Deze onderbrekingen moeten steeds in overleg met de Klant worden afgesproken. (Zie proces Change controle).

Voor de Netwerkdiensten wordt verwacht dat tijdens de het Transitieproject minimaal volgende activiteiten voorzien worden:

- Overnemen van de bestaande ICT-Dienstverlening m.b.t. alle hierboven beschreven netwerkdiensten in het kader van de continuïteit. Alle processen/procedures/hulpmiddelen om deze bestaande Diensten te kunnen leveren conform de vereisten in deze Service Portfolio moeten opgezet worden. Het betreft minimaal volgende onderdelen:
 - Overnemen Exploitatie van bestaande VO IP backbone (PE, CE routers), indien van toepassing migratie WAN bandbreedte van Vlaams glas operator en/of koppeling met andere operatoren;
 - Overnemen en/of migreren van bestaande Internet & Cloud Access bandbreedte. De ICT-Dienstverlener zal verder de rol opnemen van Cloud Broker met betrekking tot alle gevraagde Cloud connectiviteit;
 - Overnemen Exploitatie van huidige LAN/WLAN netwerken;
 - Overnemen Exploitatie van alle in gebruik zijnde gecentraliseerde netwerk- en beveiligingsbouwstenen zoals routers/switches, firewalls, netwerk controle/mgt apparatuur, loadbalancers, proxies, etc. Dit is van toepassing zowel op on-prem knooppunten als Cloud omgevingen. De netwerk knooppunten benodigd voor het aggregeren van Vlaams glas en hosting van netwerk apparatuur zijn opgenomen in de Referentiebibliotheek.
 - Migratie en optimalisatie van diverse policies (netwerk, firewall, loadbalancing, URL, IPS/ATP, WAF, SSL decryptie, SSL VPN, etc.);
 - Migratie van de bestaande Out Of Band connecties naar beheersapparatuur van ICT-Dienstverlener. De monitoring en het onderhoud van op afstand dient uitgevoerd te worden door de ICT-Dienstverlener. De continuïteit van de Management service dient te worden gegarandeerd tijdens Transitie;
 - Het overnemen van alle RIPE, DNS & public certificate administratie;
 - Het overnemen van de bestaande lijnen en connecties;
- Inrichten van alle processen/procedures/hulpmiddelen m.b.t. de nieuwe dienstverlening “beveiligde aansluitingen van partner netwerken op het VO-netwerk” zoals beschreven in de verschillende Service Portfolio’s voor de ICT-Dienstverlening. Het betreft hier in het bijzonder:
 - Het opzetten van de verbindingen naar de voor de ICT-Dienstverlening gebruikte datacenters, inclusief eraan gekoppelde beveiligingscomponenten;
- Inrichten van alle processen/procedures/hulpmiddelen m.b.t. opzetten van de mogelijkheid tot het capteren van de Incidenten en Problemen vanuit een overkoepelend Gemeenschappelijk Ondersteunend Systeem voor opvolgen van Incidenten. De effectieve afhandeling Incidenten door de ICT-Dienstverlener kan gebeuren in een eigen systeem, op voorwaarde dat de ICT-Dienstverlener de nodige interface met het Gemeenschappelijk Ondersteunend systeem opzet, of kan eventueel rechtstreeks gebeuren in het Gemeenschappelijk Ondersteunend Systeem aangeboden door de Service Integrator indien de ICT-Dienstverlener hiervoor kiest. Alle kosten inclusief de eventuele kost van de licenties die hiervoor nodig zijn moeten mee opgenomen zijn in de eenheidsprijzen. Verder is het vanuit Klanten-perspectief belangrijk dat de status van de Incidenten en Problemen steeds kan geraadpleegd worden via het overkoepelende portaal;
- Inrichten van alle processen/procedures/hulpmiddelen m.b.t. opzetten van de mogelijkheid tot het capteren van de bestellingen van Werkaanvragen vanuit een overkoepelende bestelinterface die deel uitmaakt van de Integratiediensten.. De bestelportaal wordt ingericht door de Service Integrator en wordt gebruikt voor de (initiële) registratie van en opvolging door Klanten van:
 - Alle Eenvoudige Werkaanvragen uit de Service Catalogus
 - Projecten
 - Ondersteuningsopdrachten in-regie

Vanuit Klanten-perspectief is het belangrijk dat de status steeds kan geraadpleegd worden via het overkoepelende portaal. De effectieve afhandeling en uitvoering van de Werkaanvragen door de ICT-Dienstverlener kan gebeuren in een eigen systeem, op voorwaarde dat de ICT-Dienstverlener de nodige interface met de Gemeenschappelijke Ondersteunende systemen opzet, of kan eventueel rechtstreeks gebeuren in de Gemeenschappelijke Ondersteunende Systemen aangeboden door de Service Integrator indien de ICT-Dienstverlener hiervoor kiest. Alle kosten inclusief de eventuele kost van de licenties die hiervoor nodig zijn moeten mee opgenomen zijn in

de eenheidsprijzen; Verder is het vanuit Klanten-perspectief belangrijk dat de status van de Werkaanvragen steeds kan geraadpleegd worden via het overkoepelende portaal.

- Inrichten van de nieuwe dienstverlening zoals voorzien in deze Service Portfolio voor het uitvoeren van Ondersteuning m.b.t. de netwerkomgeving in regie. Dit omvat eveneens de inrichting en operationalisering van een aantal Ondersteunende Systemen in functie van deze dienstverlening. Dit met het oog op het bestelbaar en opvolgbaar maken van het Dienstenpakket Ondersteunen van de netwerkomgeving in regie.
- Inrichten van de nieuwe dienstverlening zoals voorzien in deze Service Portfolio voor het uitvoeren van Infrastructuurprojecten m.b.t. de netwerkomgeving. Dit omvat eveneens de inrichting en operationalisering van een aantal Ondersteunende Systemen in functie van deze dienstverlening. Dit met het oog op het bestelbaar maken van het Dienstenpakket Netwerkprojecten, opdat Klanten projectmatige wijzigingen en toevoegingen kunnen aanvragen en bestellen voor uitvoering. Mogelijke voorbeelden van projectmatige wijzigingen zijn:
 - infrastructuurprojecten voor de nodige uitbreiding van de bestaande capaciteit;
 - infrastructuurprojecten voor het vernieuwen van verouderde systemen die vervangen moeten worden;
 - ...

Volgende kostenelementen moeten deel uitmaken van de eenheidsprijzen :

- Kosten voor het opzetten van eigen systemen
- Kosten voor het opzetten van de integratie met de Gemeenschappelijk Ondersteunende Systemen
- Kosten voor het rechtstreeks gebruik van de Gemeenschappelijk Ondersteunende Systemen (indien dit het geval zou zijn).

Voor Transitie kan de ICT-Dienstverlener volgende assumptie nemen: de kosten van het eigen systeem dat geïntegreerd wordt met de GOS (m.u.z. bestelportaal, service desk en DML) worden volledig ingecalculereerd en als dan na de gunning blijkt dat het goedkoper is om toch rechtstreeks te werken met de GOS, dan kan men dit nog realiseren via een Verbetervoorstel (m.a.w. het voorstel van de Service Provider wordt aangepast en de prijs wordt verlaagd).

De verschillende ICT-Dienstverleners zullen voor bepaalde beheers- of monitoringsystemen gebruik moeten maken van infrastructuur (o.a. servers) die beheerd wordt door de ICT-Dienstverlener van de Cloud- en datacenterdiensten. Vermits de prijs hiervan nu nog niet gekend is, zullen de verschillende dienstverleners dat in hun BAFO zelf moeten inschatten o.b.v. een scenario waarbij ze hier zelf zullen voor instaan. Dit moet transparant meegegeven worden in de BAFO zodat de impact eenduidig bepaalbaar is indien dit nadien zou vervangen worden door de diensten van de ICT-Dienstverlener van de cloud- en datacenterdiensten.

Ter informatie worden de uiterste data meegegeven wanneer de integratiecatalogus door de Service Integrator ter beschikking zal worden gesteld alsook de uiterste datum vanaf wanneer voorstellen voor ondersteuning in-regie of projecten kunnen worden aangevraagd. Deze data zijn momenteel:

<i>Mijlpaal</i>	<i>Uiterste datum (*)</i>
<i>De Service Integrator stelt de specificaties van de integratiecatalogus ter beschikking aan de verschillende ICT-Dienstverleners van het Ecosysteem (en het Bestuur) zodat ICT-Dienstverleners integraties met eigen Ondersteunende Systemen kunnen opzetten.</i>	<i>1-sept-2021</i>
<i>De Service Integrator stelt een test-omgeving van de Gemeenschappelijke Ondersteunende Systemen, met bijhorende integratiecatalogus, ter beschikking aan de andere ICT-Dienstverleners in het Ecosysteem.</i>	<i>1-sept-2021</i>

<p><i>De Service Integrator stelt de productieomgeving van de Gemeenschappelijke Ondersteunende Systemen, met bijhorende integratiecatalogus, ter beschikking aan de ICT-Dienstverleners in het Ecosysteem. Vanaf dit moment kunnen ICT-Dienstverleners de integratie met hun eigen productie Ondersteunende Systemen operationaliseren.</i></p>	<p>1-nov-2021</p>
<p><i>Klanten hebben de mogelijkheid om via de GOS projectvoorstellen en voorstellen m.b.t. ondersteuning in-regie aan te vragen. Dit houdt in dat systemen ter beschikking moeten zijn en dat processen moeten beschikbaar zijn om dit te realiseren. De systemen en processen kunnen weliswaar nog verder verfijnd worden tijdens de duurtijd van de initiële transitie.</i></p> <p><i>Merk op dat de de aanvraag van Projecten reeds vroeger moet kunnen starten (streefdatum: uiterlijk 1-sept-2021). Mogelijks moet hiervoor (door de Service Integrator) een administratieve interim-oplossing worden voorzien. Ook de uitvoering zelf van deze Projecten kan waar nodig aanvragen voorafgaand aan 1-feb-2022.</i></p> <p>De effectieve exploitatie kan in principe enkel vanaf 1-feb-2022</p>	<p>1-nov-2021</p>

() Uiterste datum in veronderstelling dat de kennisgeving aan de ICT-Dienstverlener van de gunning ten laatste plaats vindt op 31 mei 2021.*

1.5.2 Deeltransitie tijdens de duur van de Overeenkomst

Naast het uitvoeren van de Initiële Transitie m.b.t. de netwerkdienstverlening moet het ook mogelijk zijn om tijdens de uitvoering van de Overeenkomst nieuwe Klanten te onboarden. Deze onboarding gebeurt via een Project. De ICT-Dienstverlener voorziet de nodige processen/procedures en hulpmiddelen om onboarding van nieuwe Klanten mogelijk te maken en vlot te laten verlopen.

1.6 Exit

1.6.1 Maatregelen bij het beëindigen van de overeenkomst

De verschillende situaties waarin de overeenkomst beëindigt kan worden en de modaliteiten hierrond zijn beschreven in het Basiscontract (zie hoofdstuk 10)

De ICT-Dienstverlener zal er voor zorgen dat tijdens de volledige Duur van deze Overeenkomst elke vroegtijdige beëindiging steeds zonder problemen en tegen een vaststelbare en lage kostprijs kan gebeuren.

Dit betekent onder andere dat Inventarissen en documentatie steeds goed dienen bijgehouden te worden.

De volgende maatregelen zullen door de ICT-Dienstverlener genomen worden:

- alle hardware-, software- en netwerk-investeringen zullen zoveel mogelijk conform zijn met de standaard van de ICT-markt. Daarom zal de ICT-Dienstverlener altijd het gebruik van standaarden, normen en richtlijnen aanbevelen waardoor het Bestuur zo weinig mogelijk zal gebonden zijn aan bedrijfseigen en -specifieke apparatuur of programmatuur die een beperkt marktaandeel bezit;
- Er wordt maximaal gebruik gemaakt van open standaarden en open source om een

- eenvoudige overdraagbaarheid maximaal te garanderen;
- Alle VO-specifieke contracten die afgesloten worden moeten kosteloos overdraagbaar zijn naar zowel het Bestuur als een Toekomstige ICT-Dienstverlener en dit met behoud van de voor het Bestuur of de betrokken Klanten bedongen voorwaarden, tenzij vooraf en expliciet anders afgesproken met het Bestuur of de betrokken Klanten. Verder moet ervoor gezorgd worden dat, tenzij vooraf en expliciet anders afgesproken met de Klant, alle onderliggende VO-specifieke contracten maandelijks of jaarlijks geheel of gedeeltelijk moeten kunnen stopgezet worden;
 - Alle procedures en werkwijzen die door de ICT-Dienstverlener zullen gebruikt worden, zijn conform the “State-of-the-Art” (erkend door de internationale ICT-experten en ICT-consultants). Deze conformiteit is een garantie dat het Bestuur het gepaste personeel zal kunnen vinden zonder grote moeilijkheden;
 - De ICT-Dienstverlener zal minstens één keer per jaar een controle uitvoeren van de betrouwbaarheid van de Configuratiebank (lijst van hardware, software en netwerk componenten, operationele procedures, lopende contracten, gebruikershandleidingen van de toepassingen) Deze controle wordt bijgevoegd aan de periodieke controles. Het doel is na te kijken dat de Inventarissen (hardware, software, configuraties,...) werkelijk op een kwalitatieve wijze bijgehouden worden.
 - Alle kennis m.b.t. de ICT-omgeving van het Bestuur en m.b.t. de aan de Klanten geleverde Diensten (processen, procedures, richtlijnen, helpdeskdossiers, exploitatiedossiers, ...) wordt systematisch opgeslagen en ter beschikking gehouden zodat een kosteloze kennisoverdracht op elk ogenblik mogelijk is.

1.6.2 Deelexit tijdens de duur van de Overeenkomst

Aangezien er voor het geheel van de gevraagde ICT-Dienstverlening binnen deze Overeenkomst geen exclusiviteit wordt verleend aan de ICT-Dienstverlener kunnen de verschillende Klanten ervoor opteren om alle of bepaalde Diensten niet meer af te nemen tijdens de Duur van deze Overeenkomst.

Voor een aantal Diensten is in deze Service Portfolio een specifieke Werkaanvraag opgenomen waarbij de modaliteiten rond het stopzetten van de desbetreffende Dienst expliciet is beschreven.

Voor alle andere exploitatiediensten waarvoor er geen expliciete omschrijving is opgenomen in de Service Portfolio, dient de stopzetting projectmatig gerealiseerd te worden via een Exit Project.

Default omvat het Exit Project alle activiteiten die nodig zijn om de betreffende Dienst te stoppen en zal vanaf datum van stopzetting de facturatie van de maandelijkse Eenheidsprijs stoppen.

Enkel in het geval dat in het Projectvoorstel voor het starten van de Exploitatie dienst expliciet werd opgenomen en bijgevolg met de Klant werd afgesproken dat de onderliggende onderhoudscontracten en/of Licenties voor een langere periode dan 1 jaar worden afgesloten kan deze extra en nog niet verrekende reële kost in rekening gebracht worden naar de Klant toe via het betrokken Exit Project.