

Uitwerking ontwerpregels architectuurblauwdruk V1.1

Architectuurgebied netwerk

Datum	28-03-2022
Auteur(s)	Design Office ROC FP
Versie	1.2
Status	Definitief

Inhoudsopgave

DOCUMENTBEHEER	3
1 MODULE BACKBONE	5
2 MODULE LOCATIE	10
2.1 SDN	10
2.1.1 <i>Positie module Backbone binnen het SDN-model</i>	10
2.1.2 <i>Locatietype flexibel</i>	11
2.1.3 <i>Locatietype vast</i>	13
2.1.4 <i>Generieke kenmerken SDN-edge-nodes en SDN-border-nodes</i>	17
3 MODULE DATACENTER (ON-PREMISES).....	22
3.1.1 <i>Communicatie SDN en traditioneel:</i>	22
3.2 SDN	22
3.2.1 <i>Generieke kenmerken leaf en spine nodes:</i>	24
4 MODULE CLOUD	28
4.1 BENADERING CLOUDDIENSTEN	28
4.2 GENERIEKE ONTWERPREGELS CLOUDDATACENTER (OUT-OF-SCOPE)	28
5 WLAN	30
5.1 GENERIEK.....	30

Documentbeheer

Revisiegeschiedenis

Versie	Opmerkingen
0.1	Opzet document
0.2	Invulling document
1.0	Vaststelling door gremium Design Office ROC FP
1.1	Definitieve versie

Distributielijst

Marktpartijen aanbesteding.

Contactpersonenlijst

Zie aanbestedingsdocumentatie.

Relatie met andere documenten/brondocumentatie

Document/bronbestand	Status	Auteur
Techniek Architectuurblauwdruk domein security v1.0	Definitief	Design Office ROC FP
Techniek Architectuurblauwdruk domein netwerk v1.0	Definitief	Design Office ROC FP

Classificatie

	Categorie	Toelichting
	Laag	Informatie geschikt voor algemene publicatie en externe distributie.
✓	Midden	Informatie die gevoelig is en enkel bestemd voor een beperkte groep.
	Hoog	Informatie die zeer gevoelig is en enkel bestemd voor specifiek benoemde personen.

In het *HLD netwerk en beveiliging ROC FP* is uitgegaan van software-defined technologie voor het WAN, het LAN op de verschillende locatietypen en in de on-premises-datacenters, zodat ontwerpregels in de *architectuurblauwdruk architectuurdomein netwerk* die betrekking hebben op het traditionele model verder niet zijn uitgewerkt in deze bijlage. Tevens zijn Azure-gerelateerde onderdelen out-of-scope, maar voor duidingen/zienswijze van het ROC FP verwerkt in dit document.

Functionaliteiten in dit document zijn generiek beschreven. Eventuele terminologie die (mogelijk vaker) gebezigd wordt door een bepaalde vendor of eventueel aan een bepaalde vendor kan worden toegeschreven, is louter gebaseerd op toeval. Het ROC FP is van mening, dat uitgewerkte functionaliteiten door verschillende vendors technisch kunnen worden ingevuld.

1 Module backbone

Ontwerpregel 1	Communicatie modules
1.1	Communicatie tussen: • locaties onderling, • datacenters (onprem) onderling, • locaties en het onprem datacenter, • locaties en het publieke clouddatacenter (onderdeel module Cloud), • locaties en de onderwijsdienstenleverancier SURF, • locaties en PaaS/SaaS-diensten (onderdeel module Cloud) die direct op de Backbone gekoppeld kunnen worden, dient te verlopen via de module Backbone.
<i>Uitwerking</i>	<i>Met referentie aan de verschillende figuren met verkeersstromen in het HLD.</i> <i>Het SD-WAN representeert de module Backbone en voorziet in communicatiestromen tussen locatietypes onderling, de on-premises-datacenters onderling, locatietypes en de on-premises-datacenters voor 'private communicatie' hetgeen inhoudt: Interne communicatie binnen het netwerk van ROC FP middels private IP-subnetten. Op het niveau van het SD-WAN is een lokale internetuitbraak (Direct Internet Access) aangebracht, zodat diensten die via het internet worden ontsloten ook direct via het internet bereikbaar zijn. Dit betreft SaaS- en PaaS-diensten en regulier internet browsen.</i>
1.2	Het is toegestaan de modules Datacenter (onprem) direct aan elkaar te verbinden zonder tussenkomst van de module Backbone. In dit laatste scenario is sprake van een DCI (Datacenter Interconnect).
<i>Uitwerking</i>	<i>In de huidige configuratie van het ROC FP-netwerk is een DCI-netwerk beschikbaar. Met referentie aan specifiek de figuren 3-30 en 3-31 in het HLD (tevens is de DCI-connectie in alle illustraties verwerkt).</i>
1.3	De module Backbone dient als fallbackscenario te kunnen worden gebruikt, zodra de DCI-interconnect niet meer functioneert.
<i>Uitwerking</i>	<i>Met referentie aan specifiek de figuren 3-30 en 3-31 in het HLD. Het SD-WAN-netwerk representeert de module Backbone. Het SD-WAN-netwerk wordt ingezet als fallbacknetwerk voor communicatiestromen die primair gebruik maken van het DCI-netwerk. Dit betreft onder meer heart beats van de on-premises-firewalls en de SD-WAN-nodes op datacenterniveau. Tevens worden verkeersstromen, geïnitieerd/ontvangen door serversystemen/storagesystemen in het on-premises-datacenter, omgeleid via het SD-WAN-netwerk indien het DCI-netwerk niet meer beschikbaar is.</i>
1.4	Communicatie tussen publieke clouddatacenters die deel uitmaken van de module Cloud verloopt via de Backbone van de provider van het publieke clouddatacenter.
<i>Uitwerking</i>	<i>Op het moment van schrijven maakt het ROC FP gebruik van één availability zone (i.e. één cloud-datacenter) binnen de regio West-Europa (i.e. Azure), zodat deze ontwerpregel in de huidige setting niet relevant is. Zodra het wel relevant wordt zal per service moeten worden bekeken of</i>

	<i>deze middels de backbone van de publieke cloudprovider wordt afgehandeld of via het betreffende hubVnet om vanuit informatiebeveiligingsoogpunt recht te blijven doen aan de hub-and-spoke-topologie van het netwerk.</i>
1.5	Voor zover mogelijk en opportuun dient dataoverdracht tussen modules direct middels de module Backbone te verlopen, waarmee <i>hairpinning</i> in het onprem datacenter wordt voorkomen. Dit op grond van trends in het onderwijs, waarbij steeds vaker gebruikgemaakt zal worden van diensten die niet meer geleverd worden vanuit het onprem datacenter.
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk representeert de module Backbone. Het SD-WAN-netwerk heeft het internet als underlay medium en voorziet hierdoor in een lokale internetuitbraak (Direct Internet Access). Op deze manier wordt ervoor gezorgd, dat verkeer dat een bestemming heeft op het internet direct via de decentrale/lokale internetopgang wordt afgehandeld en niet via de centrale internet-opgang in de on-premises-datacenters.</i>

Ontwerpregel 2	Backbone As A Service
2.1	De Backbone dient als een Service te kunnen worden afgenomen bij een Backbone-provider die connectiviteitsafspraken heeft met leveranciers van clouddatacenters en andere clouddiensten-leveranciers.
<i>Uitwerking</i>	<i>Dit valt binnen de NAAS-dienst. Hierbij moet worden aangetekend dat op grond van voortschrijdend inzicht het ROC FP opteert om geen gebruik te maken van (dure) express routes en cloudconnects. Het Azure-clouddatacenter wordt direct op het SD-WAN-netwerk aangesloten en wel middels een SD-WAN-node, gebruikmakend van het internet als underlay-netwerk. Hierdoor ontstaat integraliteit van de SD-WAN-oplossing met de mogelijkheid tot een decentrale internet-uitbraak op het niveau van Azure.</i>
2.2	De aansturing, monitoring, provisioning van de Backbone As A Service dient bij voorkeur te worden gereguleerd middels een SaaS-dienst, waarbij het ROC via een portal inzicht heeft in minimaal: • De status van diensten, • De status van de overall Backbone, • Trends in de Backbone, waarmee voorspelbaarheid en daardoor beheerbaarheid van de omgeving optimaal kan worden nagestreefd (e.g. O.b.v. ML/AI voorspellende karakteristieken voor bijvoorbeeld capaciteitsmanagement). Hierbij dient het mogelijk te zijn: • Business rules (intelligence) op te nemen via de portal voor alle diensten, waarmee de Backbone op een intelligente en automatische manier invulling kan geven aan de technische vereisten voor de diensten (e.g. thresholds voor metrics als delay, jitter waarbij andere netwerkpaden gebruikt kunnen worden indien thresholds worden overschreden. E.g. gebruik maken van de meest kostenefficiënte onderliggende fysieke dragers, waarbij in geval van overschrijding van bepaalde thresholds (simultaan) een duurdere backup-verbinding kan worden benut). • De Portal locatie-onafhankelijk te kunnen benaderen.

	De Backbone te laten doorwerken, indien de onderliggende NMS-systemen (tijdelijk) geen verbinding meer hebben met de module Backbone.
<i>Uitwerking</i>	<i>Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN in het HLD. Het ROC gaat hierbij uit van conformiteit van de aangeboden NAAS-dienstverlening. Op grond van de 'cloud, tenzij strategie' die het ROC FP nastreeft wordt in het HLD uitgegaan van een cloudplatform/portal waar vanuit de aansturing van het SD-WAN-netwerk plaatsheeft. Hiervan kan worden afgeweken indien technologie en/of kosten een andere oplossing 'rechtvaardigen'.</i>
2.3	De backbone dient in een beschikbaarheid te voorzien van 99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
<i>Uitwerking</i>	<i>Het ROC FP laat dit aspect over aan de winnaar van de aanbesteding. Op grond van de aangeboden SD-WAN-nodes en de configuratie van het SD-WAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheidsberekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>
2.4	De geboden service dient de access-nodes of aggregatie-nodes op locaties te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 3.3 (van de architectuurblauwdruk architectuurgebied netwerk). Hierbij dient het mogelijk te zijn de service te laten 'meegroeien' of 'inkrimpen' met het type en/of subtype locatie.
<i>Uitwerking</i>	<i>Het ROC FP gaat uit van de mogelijkheid de SD-WAN-omgeving (i.e. de representatie van de module Backbone) te ontsluiten en op- of af te schalen conform de ontwerpregels in de blauwdruk en op grond van de beschrijvingen in het HLD. Dit geldt eveneens voor de aanpalende netwerken die functioneel zijn beschreven in het HLD (met referentie aan de paragrafen 3.2.4 SD-LAN, 3.2.5 Wireless, 3.2.6 Azure, 4.1.2 NB02 Access bedraad, 4.1.3 NB03 Access/distributie bedraad, 4.1.6 NB06 Distributie datacenter). Het ROC FP laat de verdere technisch inhoudelijke aspecten over aan de winnaar van de aanbesteding. De NAAS-dienstverlening dient i.i.g. te voorzien in deze mogelijkheden.</i>
2.5	De geboden service dient de aggregatie-nodes in onprem datacenters te ontsluiten conform de ontwerpregels zoals opgesteld in paragraaf 4.3 (van de architectuurblauwdruk architectuurgebied netwerk).
<i>Uitwerking</i>	<i>Het ROC FP gaat uit van de mogelijkheid de SD-WAN-omgeving (i.e. de representatie van de module Backbone) te ontsluiten en op- of af te schalen conform de ontwerpregels in de blauwdruk en op grond van beschrijvingen in het HLD. Dit geldt eveneens voor de aanpalende netwerken die functioneel zijn beschreven in het HLD (met referentie aan de paragrafen 3.2.4 SD-LAN, 3.2.5 Wireless, 3.2.6 Azure, 4.1.2 NB02 Access bedraad, 4.1.3 NB03 Access/distributie bedraad, 4.1.6 NB06 Distributie datacenter). Het ROC FP laat de verdere technisch inhoudelijke aspecten over aan de winnaar van de aanbesteding. De NAAS-dienstverlening dient i.i.g. te voorzien in deze mogelijkheden.</i>
2.6	De service dient te voorzien in koppelingen met clouddatacenters en andere clouddiensten die direct op de backbone kunnen worden aangesloten.
<i>Uitwerking</i>	<i>Met referentie aan par. 3.2.6. Het Azure-clouddatacenter wordt direct op het SD-WAN-netwerk aangesloten. Overige clouddiensten worden waar mogelijk direct op de module Backbone (i.e. het SD-WAN-netwerk als representatie van het SD-WAN-netwerk) aangesloten. Indien dit niet mogelijk is worden deze diensten direct beschikbaar gesteld via de lokale internetuitbraak (Direct Internet Access t.b.v. SaaS-diensten/PaaS-diensten).</i>
2.7	Het ROC dient controle te kunnen uitoefenen op het backbone-netwerk. Toegang is nodig voor:

	• Het toepassen van security-polices op basis van het vigerende informatiebeveiligingsbeleid van het ROC, • Inzage in de verkeersstromen (Application Visibility & Control) opdat tijdig kan worden bijgestuurd conform de policies van het ROC (e.g. QoS-toepassing/wijziging, bandbreedte wijzigingen et cetera).
<i>Uitwerking</i>	<i>Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN in het HLD, waarin deze functionaliteiten zijn beschreven. Het backbone-netwerk in dezen is het SD-WAN-netwerk.</i>

Ontwerpregel 3	Technologie
De Backbone dient te kunnen worden vormgegeven middels verschillende technologische dragers, waarbij verandering van leverancier en technologie geen of nauwelijks impact mag hebben op het overlay-netwerk van het ROC. Dit overlay-netwerk wordt gevormd door actieve Backbone-nodes die integraal deel uitmaken van de Backbone As A Service.	
<i>Uitwerking</i>	Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN. Het SD-WAN-netwerk is de representatie van de module Backbone. SD-WAN-technologie voorziet bij uitstek in de mogelijkheid om verschillende underlay-technologieën te gebruiken als drager voor het overlay netwerk.

Ontwerpregel 4	Functies
4.1	De Backbone dient te voorzien in data-overdracht waarbij het mogelijk is op grond van specifieke business rules/intelligence de Backbone automatisch aan te passen aan de eisen van de applicatie. Indien bijvoorbeeld een normaliter geprefereerd overlay-pad niet optimaal functioneert, dient een ander overlay-pad automatisch te kunnen worden geactiveerd c.q. opgeschaald.
<i>Uitwerking</i>	<i>Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN in het HLD. Het SD-WAN-netwerk is de representatie van de module Backbone. SD-WAN-technologie voorziet bij uitstek in de mogelijkheid om overlay-paden automatisch te kunnen genereren, op te schalen, af te schalen, te deactiveren en te activeren. Ook voorziet de technologie in uitstekende mogelijkheden SLA's/policies centraal toe te passen op het applicatielandschap dat wordt getransporteerd door het SD-WAN-netwerk. Indien een applicatie niet voldoet aan de SLA/policy is het mogelijk het SD-WAN automatisch aanpassingen te laten uitvoeren om alsnog compliant te zijn (waar mogelijk).</i>
4.2	De Backbone dient te voorzien in foutendetectie en automatisch herstel.
<i>Uitwerking</i>	<i>Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN in het HLD. Het SD-WAN-netwerk is de representatie van de module Backbone. SD-WAN-technologie voorziet bij uitstek in deze voorzieningen middels de centrale cloudcontroller. De hardware van de leverancier dient hieraan te voldoen.</i>
4.3	De Backbone dient te voorzien in Quality of Service.
<i>Uitwerking</i>	<i>Met referentie aan de paragrafen 3.2.3 SD-WAN en 4.1.4 NB04 SD-WAN in het HLD. Het SD-WAN-netwerk is de representatie van de module Backbone. SD-WAN-technologie voorziet in Quality of Service. De SD-WAN-apparatuur van de leverancier dient hieraan te voldoen.</i>
4.4	De Backbone dient te voorzien in IPv4- en IPv6-functies.
<i>Uitwerking</i>	<i>De SD-WAN-apparatuur van de leverancier dient hieraan te voldoen. Let op: het is de bedoeling het netwerk van ROC FP op basis van IPv4 in te richten, maar naar de toekomst toe mag het gebruik van IPv6 niet worden uitgesloten indien use cases c.q. de noodzaak hiertoe bestaat.</i>

4.5	Redundante uplink/downlinkverbindingen dienen middels linkbundelingstechnologie te kunnen worden vormgegeven.
<i>Uitwerking</i>	<i>De SD-WAN-apparatuur van de leverancier dient hieraan te voldoen. Op de locatietypen: vast middel, vast groot en in de on-premises-datacenters is sprake van substantiële verkeersafhandeling.</i>
4.6	De Backbone dient automatisch de door de applicatie/dienst gevraagde netwerktopologie te ondersteunen, zijnde: • Any-to-any topologie, • Hub-and-spoke topologie, • Full-mesh topologie, • Point-to-point topologie.
<i>Uitwerking</i>	<i>De SD-WAN-apparatuur van de leverancier dient hieraan te voldoen. Dit is een standaard functionaliteit van een SD-WAN-netwerk.</i>
4.7	De Backbone dient te voorzien in traffic-steering-mogelijkheden, waarbij het onprem datacenter als <i>hub</i> zoveel als mogelijk wordt ontlast van verkeer dat niet bestemd is voor services die vanuit dit type datacenter worden aangeboden.
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk is de representatie van de module Backbone. Het underlay-netwerk wordt gevormd door internetdragers, zodat het SD-WAN-netwerk voorziet in decentrale internetuitbraakmogelijkheden (Direct Internet Access). Verkeer dat derhalve niet bestemd is voor het on-premises-datacenter wordt hiermee direct naar de decentrale/lokale internetopstap geleid.</i>
4.8	Backbone-nodes dienen te kunnen worden geclusterd, waarbij de beide nodes simultaan verkeer kunnen verwerken afhankelijk van de business rules/intelligentie die worden toegekend aan de betreffende diensten/ applicaties.
<i>Uitwerking</i>	<i>Met referentie aan figuur 4-1 in het HLD. Het SD-WAN-netwerk is de representatie van de module Backbone. Op het niveau van het locatietype: vast groot en de beide on-premises-datacenters zijn de SD-WAN-nodes geclusterd afgebeeld. De SD-WAN-apparatuur van de leverancier dient hieraan te kunnen voldoen. Middels policies die worden aangebracht in de centrale controller (als SaaS-dienst) is het mogelijk om het cluster simultaan het netwerkverkeer te laten afhandelen. Tevens is het hierbij mogelijk om verkeersafhandeling door primair één van de twee SD-WAN-nodes te laten uitvoeren.</i>
4.9	De Backbone dient flexibel te zijn. Met flexibiliteit wordt bedoeld: • Eenvoudig en snel opschaalbaar, • Eenvoudig en snel afschaalbaar, • Eenvoudig en snel leverbaar op locaties waar bijvoorbeeld vaste/bedrade verbindingen niet/nauwelijks en/of niet snel genoeg kunnen worden geleverd. • De implementatie van nieuwe diensten dient snel en zonder tussenkomst van de leverancier te kunnen worden uitgevoerd (snelle <i>time-to-market</i>).
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk is de representatie van de module Backbone. De SD-WAN-apparatuur van de leverancier dient hieraan te voldoen. Ieder type fysieke drager (i.e. het underlay-netwerk) dient te kunnen worden ondersteund, zodat de uitrol van een nieuwe locatie eenvoudig en snel (zero-touch) middels SD-WAN-technologie kan worden doorgevoerd. De NAAS-dienstverlening voorziet hierbij ook in horizontale schaalbaarheid (i.e. het toevoegen van extra node waar noodzakelijk) en het verhogen van de ontsluitingssnelheden (i.e. het verhogen van de bandbreedte waar noodzakelijk).</i>

2 Module Locatie

2.1 SDN

2.1.1 Positie module Backbone binnen het SDN-model

Ontwerpregel 8	Positie module Backbone binnen het SDN-model
Ontwerpregel 8.1	De module Backbone dient separaat en (technologisch) flexibel te zijn in relatie tot het SDN-model op LAN/WLAN-niveau. Dit in verband met de mogelijkheid de module Backbone sourceable te houden door een duidelijk demarcatiepunt tussen de module Backbone en de module Locatie te creëren (dus ook qua technologie indien dit de flexibiliteit en sourceability van de module Backbone ten goede komt).
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk is de representatie van de module Backbone. Het ROC FP gaat er hierbij vanuit, dat de winnaar van de aanbesteding deze ontwerpregel meeneemt in de aanbidding en daarmee in de NAAS-dienstverlening. Indien uit bijvoorbeeld kosten-overwegingen het verstandiger is om onderdelen van het SD-WAN-netwerk te combineren met bijvoorbeeld de distributielagen van het ROC-FP-netwerk (i.e. SD-LAN) staat het ROC FP daarvoor open. Echter, naar de toekomst toe dient het wel mogelijk te zijn de Backbone (i.e. het SD-WAN-netwerk) alsnog flexibel te kunnen outsourcen naar een andere partij. Het ROC FP gaat er hierbij vanuit, dat dit kosteloos geschiedt binnen de NAAS-dienstverlening indien de winnaar van de aanbesteding bijvoorbeeld nog steeds de aanpalende netwerken beheert maar een andere partij het SD-WAN wordt gegund.</i>
Ontwerpregel 8.2	Locaties waar SDN-functies worden aangebracht dienen te worden ondergebracht conform het SDN-model type 'multi-site'.
<i>Uitwerking</i>	<i>Met referte aan de paragrafen 3.2.4 SD-LAN, 4.1.2 NB02 Access bedraad, 4.1.3 NB03 Access/distributie bedraad, 4.1.6 NB06 Distributie datacenter in het HLD. Het ROC FP gaat er hierbij vanuit, dat de winnaar van de aanbesteding deze ontwerpregel meeneemt in de aanbidding.</i>
Ontwerpregel 8.3	Communicatie tussen SDN-fabric-sites onderling en communicatie tussen SDN-nodes en de centraal in het datacenter opgestelde SDN-controllers (of SDN-controllers die als SaaS-dienst worden afgenomen) wordt gefaciliteerd door de module Backbone, waarbij het flexibele IP-protocol gebruikt moet kunnen worden.
<i>Uitwerking</i>	<i>Met referte aan par. 3.2.4 SD-LAN in het HLD. Het ROC FP volgt een 'cloud, tenzij strategie', waarbij de centrale mgmt.- en controle-omgeving van het SD-LAN-netwerk vanuit de cloud wordt afgenomen. Het SD-WAN-netwerk is de representatie van de module Backbone. Het underlay-netwerk wordt hierbij gevormd door internetdragers als het fysieke medium. Dit verschaft de mogelijkheid om lokale internetuitbraak (Direct Internet Access) te bouwen, zodat het mgmt.- en controleverkeer direct via deze decentrale/lokale internetopgang wordt gerouteerd richting de SaaS-dienst.</i>

2.1.2 Locatietype flexibel

Ontwerpregel 9	SDN-model: Eigenschappen locatie-type: Flexibel	
Ontwerpregel 9.1	Aantal personen & systemen	Max. 100
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. Voor sizing en dimensionering wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 9.2	Afname onderwijskritieke ICT-services	Ja
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. Gezien de afname van onderwijskritieke ICT-services is het van belang te kunnen prioriteren tussen verschillende verkeersklassen (e.g. regulier internet browsen, VoIP et cetera). De aangeboden apparatuur van de leverancier dient derhalve QoS te ondersteunen. Tijdens de concretiseringsfase zal in overleg worden vastgesteld welke prioritering tussen verkeersklassen moet worden aangebracht. Het ROC FP wil ontzorgt worden en gaat er derhalve vanuit, dat de winnaar van de aanbesteding een voorstel doet op grond van vergelijkbare omgevingen.</i>	
Ontwerpregel 9.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Zie voor de gestelde eisen per locatie de bijlage 13 ^F ROC FP poortbezettingen,
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 9.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Aangezien dit binnen SDN, in het SDWAN device zit is dit in de huidige aanbidding niet van toepassing
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 9.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd.
<i>Uitwerking</i>	<i>Met referte aan figuur 4-1 in het HLD en de paragrafen 4.1.3 NB03 Access/distributie bedraad, 4.1.5 NB05 Access datacenter, 4.1.6 NB06 Distributie datacenter in het HLD. De aangeboden apparatuur van de leverancier dient dit te ondersteunen.</i>	
Ontwerpregel 9.6	Ontsluiting nodes module Backbone	Zie voor de gestelde eisen per locatie de bijlage 13 ^F ROC FP poortbezettingen, WAN ontsluiting.
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk is de representatie van de module Backbone. Er wordt hierbij uitgegaan van het internet als underlay-netwerk (i.e. de mogelijkheid tot Direct Internet</i>	

	Access). Tevens dient het mogelijk te zijn een SD-WAN-node op te nemen in de SD-WAN-cloud op locaties waar het ROC FP geen pandeigenaar is. Dit om ervoor te zorgen, dat integraliteit van de oplossing behouden blijft zonder puntoplossingen. Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'.	
Ontwerpregel 9.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
<i>Uitwerking</i>	Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken - > i.e. een ketenbeschikbaarheidsberekening).	
Ontwerpregel 9.8	SLA backbone-ontsluiting	Zie hiervoor in bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).	
Ontwerpregel 9.9	SLA SDN-border-node	Zie hiervoor in bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).	
Ontwerpregel 9.10	SLA SDN-edge-node	Zie hiervoor bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.

<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aansluitende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 9.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe van de leaf-spine-architectuur te worden toegepast waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
<i>Uitwerking</i>	<i>Het ROC FP laat de technische configuratie en onderbouwing over aan de winnaar van de aanbesteding. Immers, het kan zo zijn dat niet de leaf-spine-leaf-topologie wordt aangebracht maar een gelijksoortige of andere opzet die alsnog voldoet aan de principes van SD-LAN. Ongeacht de netwerktopologie is het van belang, dat de apparatuur van de leverancier voorziet in horizontale schaalbaarheid (i.e. aantallen poorten) als verticale schaalbaarheid (i.e. interface-snelheden/bandbreedtetoe wijzingen). Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort.</i>	
Ontwerpregel 9.12	Toekomstige groei	Bij toekomstige groei dient het type locatie te kunnen doorgroeien naar het locatietype vast. Per geval / situatie dienen hiertoe de mogelijkheden te worden bekeken.
<i>Uitwerking</i>	<i>Vast in de zin van bijvoorbeeld een groei naar het locatietype vast: middel. In dit kader is de bij ontwerpregel 9.11 voornoemde schaalbaarheid van belang. Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort.</i>	

2.1.3 Locatietype vast

Ontwerpregel 10	SDN-model: Eigenschappen locatie-type: Vast	
Ontwerpregel 10.1	Aantal personen & systemen	> 5
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. Voor sizing en dimensionering wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 10.2	Afname onderwijskritieke ICT-services	Ja
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. Gezien de afname van onderwijskritieke ICT-services is het van belang te kunnen prioriteren tussen verschillende verkeersklassen (e.g. regulier internet browsen, VoIP et cetera). De aangeboden apparatuur van de leverancier dient derhalve QoS te ondersteunen. Tijdens de concretiseringsfase zal in overleg worden vastgesteld welke prioritering tussen verkeersklassen moet worden aangebracht. Het ROC FP wil ontzorgt</i>	

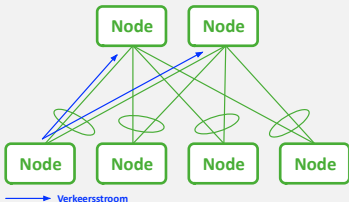
	worden en gaat er derhalve vanuit, dat de winnaar van de aanbesteding een voorstel doet op grond van vergelijkbare omgevingen.	
Ontwerpregel 10.3	Medium tussen nodes SDN-edge-laag en nodes SDN-border-laag	Zie voor de bijlage 13 ^E ROC FP poortbezettingen, WAN ontsluiting.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 10.4	Medium tussen nodes SDN-border-laag en nodes module Backbone	Aangezien dit binnen SDN, in het SDWAN device zit is dit in de huidige aanbidding niet van toepassing
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 10.5	Clustering/stacking	De nodes die deel uitmaken van de fabric-site dienen als één logische SDN-wolk te kunnen worden aangestuurd. Border nodes dienen geclusterd te kunnen worden.
<i>Uitwerking</i>	<i>Met referte aan figuur 4-1 en de paragrafen 4.1.3 NB03 Access/distributie bedraad, 4.1.5 NB05 Access datacenter, 4.1.6 NB06 Distributie datacenter in het HLD. De aangeboden apparatuur van de leverancier dient dit te ondersteunen. Het ROC hanteert een 'cloud, tenzij strategie, zodat de aansturing vanuit 'de cloud' geschiedt. Zie hiervoor de verschillende figuren, beschrijvingen en duiding in het HLD.</i>	
Ontwerpregel 10.6	Ontsluiting nodes module Backbone	Zie voor de gestelde eisen per locatie de Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" : WAN ontsluiting
<i>Uitwerking</i>	<i>Het SD-WAN-netwerk is de representatie van de module Backbone. Er wordt hierbij uitgegaan van het internet als underlay-netwerk (i.e. de mogelijkheid tot Direct Internet Access). Tevens dient het mogelijk te zijn een SD-WAN-node op te nemen in de SD-WAN-cloud op locaties waar het ROC FP geen pandeigenaar is. Dit om ervoor te zorgen, dat integraliteit van de oplossing behouden blijft zonder puntoplossingen. Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'.</i>	
Ontwerpregel 10.7	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-</i>	

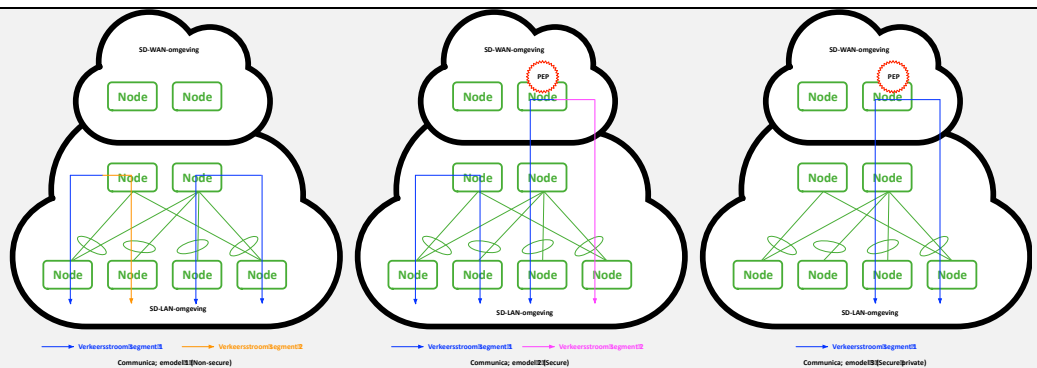
	<i>berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 10.8	SLA backbone-ontsluiting	Zie hiervoor Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheidsberekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 10.9	SLA SDN-edge-node	Zie hiervoor Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheidsberekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 10.10	SLA SDN-border-node	Zie hiervoor Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheidsberekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 10.11	Schaalbaarheid	De locatie dient te voorzien in schaalbaarheid, zowel horizontaal als verticaal. Zodra meer dan één SDN-border-node wordt ondergebracht, dient het principe van de leaf-spine-architectuur te worden toegepast

		waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes.
<i>Uitwerking</i>	<i>Het ROC FP laat de technische configuratie en onderbouwing over aan de winnaar van de aanbesteding. Immers, het kan zo zijn dat niet de leaf-spine-leaf-topologie wordt aangebracht maar een gelijksoortige of andere opzet die alsnog voldoet aan de principes van SD-LAN. Ongeacht de netwerktopologie is het van belang, dat de apparatuur voorziet in horizontale schaalbaarheid (i.e. aantallen poorten) als verticale schaalbaarheid (i.e. interface-snelheden). Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort.</i>	
Ontwerpregel 10.12	Toekomstige groei/krimp	Bij toekomstige groei dient het type locatie deze groei flexibel te kunnen accommoderen zonder wijzigingen te hoeven aanbrengen in de SDN-topologie. Bij toekomstige krimp dient het type locatie te kunnen afschalen naar het locatietype flexibel.
<i>Uitwerking</i>	<i>Flexibel in de zin van bijvoorbeeld een groei naar een kleiner type locatie. Dit kan een krimp zijn naar het locatietype vast: klein (vanaf bijvoorbeeld een locatietype vast: middel). In dit kader is de bij ontwerpregel 10.11 voornoemde schaalbaarheid van belang. Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort.</i>	

2.1.4 Generieke kenmerken SDN-edge-nodes en SDN-border-nodes

Ontwerpregel 11	SDN-model: Generieke kenmerken SDN-edge-nodes en SDN-border-nodes
Ontwerpregel 11.1	De functies van de SDN-edge-lagen en SDN-border-lagen mogen in één SDN-node zijn ondergebracht indien dit technologisch kan worden doorgevoerd. Deze SDN-node dient dan direct verbonden te worden aan de module Backbone. Indien de functies van SDN-edge- en SDN-border-lagen niet in één SDN-node kunnen worden ondergebracht, geldt het volgende: SDN-edge-nodes zijn redundant aangesloten op één SDN-border-node, tenzij de onderhavige SDN-technologie/systematiek een dergelijke ontsluiting niet toestaat. Indien deze redundante ontsluiting technologisch niet kan worden verwezenlijkt, dient te worden teruggevallen op de leaf-spine-architectuur, waarbij een SDN-edge-node is verbonden aan twee verschillende SDN-border-nodes. Deze SDN-border-nodes dienen als cluster te kunnen worden aangebracht.
<i>Uitwerking</i>	<i>Het ROC FP laat de netwerktopologie over aan de winnaar van de aanbesteding. Het kan zo zijn, dat per vendor/aangeboden oplossing een andersoortige netwerktopologie wordt aangebracht. Het is van belang, dat in ieder geval wordt voldaan aan beschikbaarheidseisen (i.e. ketenbeschikbaarheid) waar het ROC FP om vraagt binnen en tussen alle modules.</i>
Ontwerpregel 11.2	De access-poorten van een SDN-edge-node zijn van het type koper 10/100/1000 Mbit/s. Voor de te aansluiten AP's is het een pre dat er gebruik gemaakt kan worden van Multigig poorten
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Hierbij dient ook gelet te worden op het gebruik van de standaard WiFi-6 (i.e. doorvoersnelheden). De aangeboden AP's op de locaties moeten voor de locaties Middel en Groot op de access-laag aangesloten te worden op Multi-Gig poorten. De overige poorten moeten minimaal 10/100/1000 Base-T zijn</i>
Ontwerpregel 11.3	Access-nodes dienen te voorzien in Power-over-Ethernet-mogelijkheden om Access Points en IP-telefoons van stroom te kunnen voorzien. Hierbij dient per locatie/gebruikssituatie bekeken te worden welk type POE (type 15W, 30W, 60W).
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Voor de aangeboden AP's op de locaties moeten op de access-laag voldoende POE poorten en POE-capaciteit beschikbaar te zijn, om de volledige radiocapaciteit van de radio's te kunnen benutten. De overige poorten moeten minimaal POE+ ondersteunen</i>
Ontwerpregel 11.4	SDN-edge-nodes dienen het gebruik van Wake-on-LAN te ondersteunen.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen.</i>
Ontwerpregel 11.5	SDN-border-nodes dienen te zijn voorzien van de control plane functies die noodzakelijk zijn binnen het SDN-ecosysteem.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Let op: controle plane functie is het niet hetzelfde als de centrale controller in de cloud. De aan te brengen netwerktopologie laat het ROC FP over aan de winnaar van de aanbesteding.</i>
Ontwerpregel 11.6	SDN-border-nodes dienen de SDN-fabric-site richting de module Backbone te kunnen ontsluiten op basis van het IP-protocol, waarbij gebruikgemaakt kan worden van open standaarden routeringsprotocollen.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen.</i>
Ontwerpregel 11.7	SDN-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Let op: het is de bedoeling het netwerk van ROC FP op basis van IPv4 in te richten, maar naar de toekomst toe mag het gebruik van IPv6 niet worden uitgesloten indien use cases c.q. de noodzaak hiertoe bestaat.</i>

Ontwerpregel 11.8	SDN-nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen.</i>
Ontwerpregel 11.9	De SDN-edge-nodes zijn niet voorzien van redundante voedingen. De SDN-border-nodes zijn wel voorzien van redundante voedingen.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Het ROC FP gaat hierbij echter uit van door de winnaar te maken ketenbeschikbaarheidsberekeningen op grond van de aangeboden apparatuur en netwerktopologie. Indien uit deze berekeningen geen noodzaak blijkt tot redundantie, neemt het ROC FP dit advies over.</i>
Ontwerpregel 11.10	SDN-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
<i>Uitwerking</i>	<i>Dit concept is high-level afgebeeld in de onderstaande figuur. Vanaf een node kunnen simultaan verkeersstromen worden afgehandeld. Op grond van instellingen in de cloud-controller kunnen alle beschikbare paden worden gebruikt. De netwerktopologie en te gebruiken netwerkprotocollen voorzien hierbij in een loopvrije omgeving.</i>  <i>Met andere woorden: LAG (Link Aggregation) en active/active paden worden door de apparatuur van de leverancier ondersteund.</i>
Ontwerpregel 11.11	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
<i>Uitwerking</i>	<i>Het ROC FP gaat ervan uit, dat dit binnen de dienstverlening is opgenomen. Licenties kunnen bijvoorbeeld op grond van consumptie worden afgenomen naar gelang de behoeften van het ROC FP (e.g. opschalen/afschalen van de dienstverlening, aantallen gebruikers e.d.).</i>
Ontwerpregel 11.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de backbone-node, maar in ieder geval binnen de module Locatie. Hiervan kan worden afgeweken, indien bijvoorbeeld: • voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een locatie-overschrijdend OSI Laag 2 pad aan te brengen, • de gekozen technologie in de praktijk dermate anders is c.q. andere inzichten met zich meebrengt dat niet aan dit principe voldaan kan worden.
<i>Uitwerking</i>	<i>In de onderstaande figuur zijn de drie communicatiemodellen afgebeeld zoals beschreven in paragraaf 3.2.8.2 Segmentatie.</i>



In communicatiemodel 1 ligt het OSI Laag 3 terminatiepunt in het SD-LAN-netwerk zelf. Directe communicatie tussen gebruikers/systemen is hierbij toegestaan. In de concretiseringsfase zal situationeel moeten worden vastgesteld of dit model kan worden doorgevoerd. Indien de door de winnaar van de aanbesteding aangeboden apparatuur en/of netwerktopologie het OSI Laag 3 terminatiepunt te allen tijde aanbrengt op SD-WAN niveau is dit toegestaan, waarbij de SD-WAN-nodes wel dienen te worden gedimensioneerd op het af te handelen netwerkverkeer. De PEP-functies zijn op het niveau van het SD-WAN aangebracht. Op de onderhavige verkeersstromen dienen geen PEP-functies te worden toegepast.

In communicatiemodel 2 ligt het OSI Laag 3 terminatiepunt zowel op het niveau van het SD-LAN (zie beschrijving hierboven) als op het niveau van het SD-WAN. Dit laatste voor verkeersstromen die tussen verschillende segmenten kunnen plaatshebben. Met andere woorden: op deze verkeersstromen dienen derhalve PEP-functies te kunnen worden toegepast die zich op het niveau van de SD-WAN-node bevinden. Ook hier de notie, dat situationeel en netwerktopologisch bepaald moet worden waar de exacte OSI Laag 3 terminatiepunten zich bevinden in het netwerk.

In communicatiemodel 3 ligt het OSI Laag 3 terminatiepunt op het niveau van het SD-WAN alwaar de PEP-functies zich bevinden. Communicatie binnen dit model dient immers altijd plaats te vinden met PEP-functies. Ook hier de notie: situationele duiding en netwerktopologische vaststelling tijdens de concretiseringsfase en op grond van de hardware die de winnaar van de aanbesteding levert.

Indien de situatie zich voordoet dient de aangeboden apparatuur van de winnaar van de aanbesteding te voorzien in de mogelijkheid een communicatiepad op het niveau van OSI Laag 2 te aan te leggen. Dit is in de onderstaande figuur geduid. Het betreft een end-to-end communicatiestroom die zich kan voordoen tussen verschillende locatietypen, tussen de on-premises-datacenters en tussen verschillende locatietypen en on-premises datacenters. De door de winnaar van de aanbesteding aangeboden apparatuur dient op zowel SD-LAN- als SD-WAN-niveau hierin te voorzien

Ontwerpregel 11.13	• SDN-nodes worden bij voorkeur afgenomen van één vendor i.v.m.:eenvoudig beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
<i>Uitwerking</i>	<i>Het ROC FP neemt de dienstverlening als managed NAAS af en laat dit aspect derhalve over aan de winnaar van de aanbesteding, ervan uitgaande dat de aangeboden apparatuur van een vendor is met goede reputatie. Goede reputatie in dezen is (bijvoorbeeld): 'leader' in de magic quadrants van Gartner.</i>
Ontwerpregel 11.14	SDN-nodes communiceren bij voorkeur met hun omgeving op basis van open standaarden, tenzij de voor het ROC gekozen SDN-oplossing alleen middels proprietary protocollen kan worden opgebouwd. Hierbij is het van belang, dat communicatie naar de module Backbone middels open standaarden kan worden gefaciliteerd.
<i>Uitwerking</i>	<i>Het ROC FP neemt de dienstverlening NAAS managed af en gaat er hierbij vanuit, dat het gebruik van open standaarden mogelijk is. Denk hierbij aan protocollen als VXLAN, GRE, IP sec e.d.</i>
Ontwerpregel 11.15	De node(s) van de module Backbone mogen geen deel uitmaken van de laag SDN-border in verband met: • Het kunnen scheiden van de modules Locatie en Backbone ('behoud van functionele modulariteit'), • Het kunnen scheiden van beheerverantwoordelijkheden, • Het (eenvoudig) kunnen uitbesteden van de module Backbone.
<i>Uitwerking</i>	<i>Het ROC FP neemt de dienstverlening NAAS managed af en gaat er hierbij vanuit, dat dit mogelijk is of op z'n minst mogelijk wordt indien de module Backbone (i.e. het SD-WAN-netwerk) aan een andere partij zou worden gegund in de toekomst. Het is hierbij toegestaan functies van het SD-LAN-netwerk te integreren met functies van het SD-WAN-netwerk, zolang de functies kunnen worden gesepareerd bij een uitbesteding van de Backbone aan een andere partij. Dit dient binnen de NAAS-dienstverlening te vallen waarbij het ROC FP ervan uitgaat, dat een latere functie-scheiding technisch mogelijk is en kosteloos kan plaatshebben.</i>

3 Module Datacenter (on-premises)

3.1.1 Communicatie SDN en traditioneel:

Ontwerpregel 14	Communicatie tussen SDN en traditioneel model
Communicatie tussen onderdelen die deel uitmaken van het SDN-model en onderdelen die deel uitmaken van de module Backbone of deel uitmaken van services als storage, security verlopen middels border leafs. Communicatie dient te kunnen worden gestandaardiseerd op protocollen die opereren op de niveaus van OSI laag 2 en OSI laag 3.	
<i>Uitwerking</i>	<i>Het ROC FP neemt NAAS als managed dienst af en gaat hierbij ervan uit, dat de door de winnaar aangeboden apparatuur open protocollen ondersteunt voor connectiviteit met aanpalende traditionele omgevingen. Traditioneel impliceert geen SDN in dezen.</i>

3.2 SDN

De onderstaande kenmerken gelden voor dit model:

Ontwerpregel 15	SDN-model-Eigenschappen datacenter onprem	
Ontwerpregel 15.1	Aanwezigheid onderwijskritieke ICT-services	Ja
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. Gezien de afname van onderwijskritieke ICT-services is het van belang te kunnen prioriteren tussen verschillende verkeersklassen (e.g. regulier internet browsen, VoIP et cetera). De aangeboden apparatuur van de leverancier dient derhalve QoS te ondersteunen. Tijdens de concretiseringsfase zal in overleg worden vastgesteld welke prioritering tussen verkeersklassen moet worden aangebracht. Het ROC FP wil ontzorgt worden en gaat er derhalve vanuit, dat de winnaar van de aanbesteding een voorstel doet op grond van vergelijkbare omgevingen.</i>	
Ontwerpregel 15.2	Medium tussen nodes lagen 'leaf' en collapsed-core	Glas, minimaal 10 Gbit/s
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA".</i>	
Ontwerpregel 15.3	Medium tussen nodes lagen 'leaf' en 'spine'	Glas, minimaal 10 Gbit/s
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De aangeboden apparatuur van de leverancier dient dit te ondersteunen waarbij situationeel moet worden vastgesteld welk type gebouwbekabeling gebruikt moet worden. Voor meer informatie wordt verwezen naar het document Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA".</i>	
Ontwerpregel 15.4	Beschikbaarheid	99,99% (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).

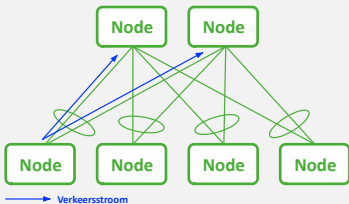
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 15.5	SLA leaf-node	Zie hiervoor in Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" (tabblad datacenter) naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 15.6	SLA aggregatie-node	Zie hiervoor in Bijlage 13 E "ROC FP Poortbezettingen dimensionering en SLA" (tabblad datacenter) naar de toegekende prioriteit. In de bijlage 7 Kwaliteit worden de gewenste respons- en hersteltijden behorende bij de toegekende prioriteit gevraagd.
<i>Uitwerking</i>	<i>Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'. Op grond van de aangeboden SD-LAN-nodes en de configuratie van het SD-LAN-netwerk dient de winnaar van de aanbesteding een beschikbaarheids-berekening op te leveren (ook in combinatie met aanpalende netwerken -> i.e. een ketenbeschikbaarheidsberekening).</i>	
Ontwerpregel 15.7	Schaalbaarheid	'Leaf-laag': horizontale en verticale schaalbaarheid 'Spine-laag': verticale schaalbaarheid
<i>Uitwerking</i>	<i>Het ROC FP laat de technische configuratie en onderbouwing over aan de winnaar van de aanbesteding. Immers, het kan zo zijn dat niet de leaf-spine-leaf-topologie wordt aangebracht maar een gelijksoortige of andere opzet die alsnog voldoet aan de principes van SD-LAN. Ongeacht de netwerktopologie is het van belang, dat de apparatuur voorziet in horizontale schaalbaarheid (i.e. aantallen poorten) als verticale schaalbaarheid (i.e. interface-snelheden). Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort.</i>	
Ontwerpregel 15.8	Toekomstige groei	In principe geen i.v.m. cloud, tenzij...principe. Eventuele groei

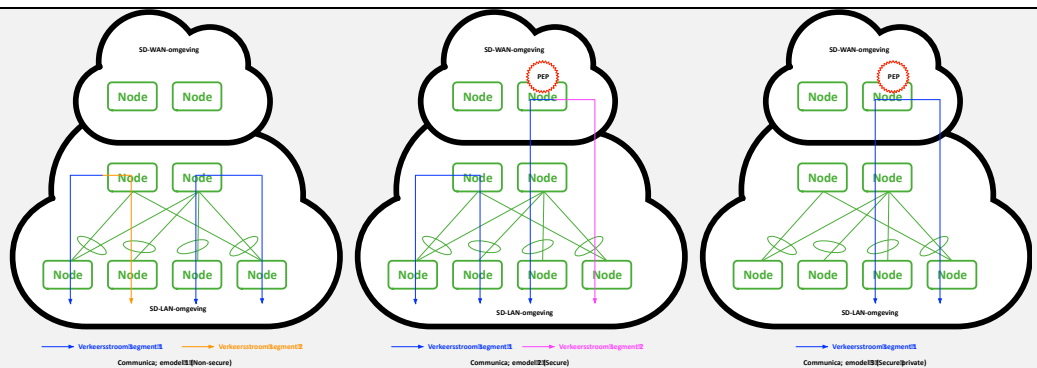
		dient wel te kunnen worden geaccommodeerd in de 'leaf' en 'spine' laag.
<i>Uitwerking</i>	<i>Het ROC FP gaat ervan uit, dat schaalbaarheid tot de standaard dienstverlening behoort. Echter, het ROC FP verwacht geen of in ieder geval geen noemenswaardige groei op het niveau van het on-premises-datacenter. Immers, het ROC FP volgt een 'cloud, tenzij strategie'. Tevens worden toepassingen in de onderwijssector steeds vaker in de hoedanigheid van SaaS-dienst geconsumeerd.</i>	

3.2.1 Generieke kenmerken leaf en spine nodes:

Het model bevat nodes van het type leaf en spine die generieke kenmerken hebben of kenmerken die dermate overeenkomen dat deze hieronder gegroepeerd zijn opgenomen.

Ontwerpregel 16	SDN-model: Generieke kenmerken leaf en spine nodes
Ontwerpregel 16.1	Leaf-nodes zijn verbonden met iedere spine-node in de topologie, zodat uitval van een uplinkverbinding of een spine-node niet leidt tot een algeheel verlies van connectiviteit vanaf een leaf-node. Leaf nodes dienen geclusterd te kunnen worden.
<i>Uitwerking</i>	<i>Het ROC FP neemt de NAAS-dienstverlening als managed dienst af en gaat hierbij af op de door de winnaar van de aanbesteding aangeboden apparatuur. Dit zowel op grond van de aan te brengen netwerktopologie alsmede de ketenbeschikbaarheidsberekeningen (end-to-end).</i>
Ontwerpregel 16.2	De access-poorten van een leaf-node zijn deels van het type koper of glas met ondersteuning van de interfacesnelheden 1Gbit/s, 10Gbit/s UTP en , en deels SFP+ Twinax, waarbij een groei naar 25Gbit/s of hoger mogelijk is
<i>Uitwerking</i>	<i>De door de winnaar van de aanbesteding aangeboden apparatuur dient hieraan te voldoen. Voor meer informatie wordt verwezen naar het document 'Bijlage 13 E ROC FP Poortbezettingen, dimensionering en SLA'.</i>
Ontwerpregel 16.3	Leaf-nodes ontsluiten het SDN-model naar de module Backbone, waarbij: • Gebruik gemaakt kan worden van linkbundelingstechnieken, • De ontsluiting gebaseerd is op minimaal 20Gbit/s (modulariteit moet kunnen voorzien in 10 Gbit/s UTP, 10 Gbit/s Twinax en combinaties MMF, SMF). • Meerdere leaf-nodes gebruikt kunnen worden voor de ontsluiting naar de module Backbone ter voorkoming van SPOFs, • Connectiviteit kan worden gerealiseerd op basis van zowel OSI laag 2 als OSI laag 3.
<i>Uitwerking</i>	<i>Het ROC FP neemt de NAAS-dienstverlening als managed dienst af en gaat hierbij af op de door de winnaar van de aanbesteding aangeboden apparatuur. Dit zowel op grond van de betreffende aan te brengen netwerktopologie alsmede de ketenbeschikbaarheidsberekeningen (end-to-end). De gevraagde doorvoersnelheden zijn hierbij wel van belang.</i>
Ontwerpregel 16.4	Nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Let op: het is de bedoeling het netwerk van ROC FP op basis van IPv4 in te richten, maar naar de toekomst toe mag het gebruik van IPv6 niet worden uitgesloten indien use cases c.q. de noodzaak hiertoe bestaat.</i>

Ontwerpregel 16.5	Nodes dienen Quality of Service te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen.</i>
Ontwerpregel 16.6	Spinde-nodes zijn voorzien van redundante power supplies, leaf-nodes niet.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen. Het ROC FP gaat hierbij echter uit van door de winnaar te maken ketenbeschikbaarheidsberekeningen op grond van de aangeboden apparatuur en netwerktopologie. Indien uit deze berekeningen geen noodzaak blijkt tot redundantie, neemt het ROC FP dit advies over.</i>
Ontwerpregel 16.7	Nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
<i>Uitwerking</i>	<i>Dit concept is high-level afgebeeld in de onderstaande figuur. Vanaf een node kunnen parallel verkeersstromen worden afgehandeld. Op grond van instellingen in de cloud-controller kunnen alle beschikbare paden worden gebruikt. De netwerktopologie en te gebruiken netwerkprotocollen voorzien hierbij in een loopvrije omgeving.</i>  <i>Met andere woorden: LAG (Link Aggregation) en active/active paden worden door de apparatuur van de leverancier ondersteund.</i>
Ontwerpregel 16.8	Ontsluiting tussen leaf-nodes en spine-nodes zijn gebaseerd op minimaal 10Gbit/s, waarbij een groei naar 40 Gbit/s of hoger mogelijk dient te zijn.
<i>Uitwerking</i>	<i>Het ROC FRP neemt de NAAS-dienstverlening als managed dienst af en gaat hierbij af op de door de winnaar van de aanbesteding aangeboden apparatuur. Dit zowel op grond van de betreffende aan te brengen netwerktopologie alsmede de ketenbeschikbaarheidsberekeningen (end-to-end). De gevraagde doorvoersnelheden zijn hierbij wel van belang.</i>
Ontwerpregel 16.9	De software-architectuur is modulair opgebouwd, zodat toekomstige/nieuwe features conform het stramien 'pay as you grow' kunnen worden ingevuld.
<i>Uitwerking</i>	<i>Het ROC FP gaat ervan uit, dat dit binnen de dienstverlening is opgenomen. Licenties kunnen bijvoorbeeld op grond van consumptie worden afgenomen naar gelang de behoeften van het ROC FP (e.g. opschalen/afschalen van de dienstverlening, aantallen gebruikers e.d.).</i>
Ontwerpregel 16.10	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de module Backbone, maar in ieder geval binnen de module Datacenter. Hiervan kan worden afgeweken, indien bijvoorbeeld voor een optimale werking van ICT-services of connectiviteit tussen entiteiten in het algemeen het noodzakelijk is een datacenter-overschrijdend OSI Laag 2 pad aan te brengen.
<i>Uitwerking</i>	<i>In de onderstaande figuur zijn de drie communicatiemodellen afgebeeld zoals beschreven in paragraaf 3.2.8.2 Segmentatie.</i>



In communicatiemodel 1 ligt het OSI Laag 3 terminatiepunt in het SD-LAN-netwerk zelf. Directe communicatie tussen gebruikers/systemen is hierbij toegestaan. In de concretiseringsfase zal situationeel moeten worden vastgesteld of dit model kan worden doorgevoerd. Indien de door de winnaar van de aanbesteding aangeboden apparatuur en/of netwerktopologie het OSI Laag 3 terminatiepunt te allen tijde aanbrengt op SD-WAN niveau is dit toegestaan, waarbij de SD-WAN-nodes wel dienen te worden gedimensioneerd op het af te handelen netwerkverkeer. De PEP-functies zijn op het niveau van het SD-WAN aangebracht. Op de onderhavige verkeersstromen dienen geen PEP-functies te worden toegepast.

In communicatiemodel 2 ligt het OSI Laag 3 terminatiepunt zowel op het niveau van het SD-LAN (zie beschrijving hierboven) als op het niveau van het SD-WAN. Dit laatste voor verkeersstromen die tussen verschillende segmenten kunnen plaatshebben. Met andere woorden: op deze verkeersstromen dienen derhalve PEP-functies te kunnen worden toegepast die zich op het niveau van de SD-WAN-node bevinden. Ook hier de notie: situationeel en netwerktopologisch bepaald moet worden waar de exacte OSI Laag 3 terminatiepunten zich bevinden in het netwerk.

In communicatiemodel 3 ligt het OSI Laag 3 terminatiepunt op het niveau van het SD-WAN alwaar de PEP-functies zich bevinden. Communicatie binnen dit model dient immers altijd plaats te vinden met PEP-functies. Ook hier de notie: situationele duiding en netwerktopologische vaststelling tijdens de concretiseringsfase en op grond van de hardware die de winnaar van de aanbesteding levert.

Indien de situatie zich voordoet dient de aangeboden apparatuur van de winnaar van de aanbesteding te voorzien in de mogelijkheid een communicatiepad op het niveau van OSI Laag 2 te aan te brengen. Dit is in de onderstaande figuur geduid. Het betreft een end-to-end communicatiestroom die zich kan voordoen tussen verschillende locatietypen, tussen de on-premises-datacenters en tussen verschillende locatietypen en on-premises datacenters. De door de winnaar van de aanbesteding aangeboden apparatuur dient op zowel SD-LAN- als SD-WAN-niveau hierin te voorzien

Ontwerpregel 16.11	Nodes worden bij voorkeur afgenomen van één vendor i.v.m.: • eenvoud van beheer, • gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), • ter voorkoming van compatibiliteitsissues.
<i>Uitwerking</i>	<i>Het ROC FP neemt de dienstverlening als managed NAAS af en laat dit aspect derhalve over aan de winnaar van de aanbesteding, ervan uitgaande dat de aangeboden apparatuur van een vendor is met goede reputatie. Goede reputatie in dezen is (bijvoorbeeld): 'leader' in de magic quadrants van Gartner.</i>
Ontwerpregel 16.12	Nodes die deel uitmaken van de SDN-topologie communiceren met nodes buiten deze topologie op basis van open standaarden.
<i>Uitwerking</i>	<i>De SD-LAN-apparatuur van de leverancier dient hieraan te voldoen.</i>

4 Module Cloud

4.1 Benadering clouddiensten

Ontwerpregel 17	Benadering van clouddiensten
Ontwerpregel 17.1	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone waaraan de module Cloud direct is verbonden. Dit indien bepaalde ROC-diensten alleen vanaf de module Locatie via de module Backbone benaderd mogen worden.
<i>Uitwerking</i>	<i>Met referte aan de figuren 3-4 en 3-5 in het HLD. Indien mogelijk en noodzakelijk voor workloads die als IaaS-dienst zijn aangebracht, wordt een cloudomgeving zoals Azure direct op module Backbone (i.e. zijnde het SD-WAN-netwerk) aangesloten. Op deze manier kunnen deze services 'privaat worden benaderd' middels private adressenschema's. Indien dit niet mogelijk blijkt temeer gebruik wordt gemaakt van via het internet te benaderen SaaS-/PaaS-diensten zal de lokale internetuitbraak (Direct Internet Access) worden ingezet voor verkeersafhandeling.</i>
Ontwerpregel 17.2	Het dient mogelijk te zijn clouddiensten alleen te ontsluiten via de module Backbone, waarbij gebruikgemaakt wordt van een local-internetbreakout. Tevens kunnen gebruikers die op afstand werken (e.g. mobiel/vanaf huis) de betreffende clouddiensten benaderen.
<i>Uitwerking</i>	<i>Met referte aan de figuren 3-4 en 3-5 in het HLD. Het SD-WAN-netwerk wordt gebouwd met het internet als underlay-netwerk op grond waarvan directe/lokale internetuitbraak (Direct Internet Access) mogelijk is.</i>

4.2 Generieke ontwerpregels clouddatacenter (out-of-scope)

De onderstaande ontwerpregels gelden voor het gebruik van clouddatacenters (e.g. Azure, AWS, GCP).

Ontwerpregel 18	Generieke ontwerpregels clouddatacenter
Ontwerpregel 18.1	ROC-diensten dienen in verschillende availability zones te kunnen worden ondergebracht.
<i>Uitwerking</i>	<i>In het HLD is voorlopig uitgegaan van één availability zone, waarin diensten worden ondergebracht. Binnen deze availability zone kunnen meerdere availability sets met componenten worden aangebracht, zodat een hoge beschikbaarheid van de dienstverlening ontstaat. Tevens wordt gebruikgemaakt van een load balancer die een verhoging van beschikbaarheid van 'achterliggende' services (VM's) mogelijk maakt.</i>
Ontwerpregel 18.2	ROC-diensten dienen in verschillende availability sets te kunnen worden ondergebracht.
<i>Uitwerking</i>	<i>Dit is een standaard dienstverlening van Azure. Het ROC FP gaat voorlopig uit van één SD-WAN-node in het clouddatacenter van Azure, tenzij uit ketenbeschikbaarheids-berekeningen de noodzaak blijkt twee nodes aan te brengen. SD-WAN-componenten dienen in availability sets te kunnen worden ondergebracht of op z'n minst als cluster te worden ingericht conform de nodes op het locatietype: vast groot en in de on-premises-datacenters. Het ROC FP laat zich hierbij informeren of het noodzakelijk is c.q. verstandig is SD-WAN-nodes onder te brengen in twee verschillende availability zones indien de noodzaak hiertoe bestaat.</i>
Ontwerpregel 18.3	Binnen een clouddatacenter wordt gebruikgemaakt van de door de provider aangeboden default route naar het internet.

<i>Uitwerking</i>	<i>Dit is een standaard dienstverlening van Azure. Deze internetopgang wordt gebruikt als lokale internetuitbraak op SD-WAN-niveau (Direct Internet Access). De SD-WAN-node bevindt zich in het hubVnet. Met referentie aan par. 3.2.6. Azure in het HLD.</i>
Ontwerpregel 18.4	ROC-diensten worden ondergebracht in de regio EER met uitsluiting van de UK.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding.</i>
Ontwerpregel 18.5	Koppeling tussen een clouddatacenter en de module Backbone wordt verzorgd door de leverancier van de module Backbone, waarbij de koppeling met een beschikbaarheid 99,99% wordt aangebracht (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).
<i>Uitwerking</i>	<i>Het internet wordt gebruikt als underlay-netwerk voor het SD-WAN-overlay-netwerk. Het SD-WAN-netwerk vormt hierbij de representatie van de module Backbone. Hierbij onderkent het ROC FP de beschikbaarheid/SLA van de door Azure aangeboden internetopgang als afhankelijkheid). Met referentie aan par. 3.2.6. Azure in het HLD.</i>
Ontwerpregel 18.6	Koppeling tussen een clouddatacenter en de module Backbone ondersteunt Quality of Service.
<i>Uitwerking</i>	<i>Op het internet is geen Quality of Service mogelijk. Echter, het SD-WAN-netwerk maakt gebruik van IPsec-tunnels (VPNs) voor verkeersstromen. In dit kader worden QoS-markeringen behouden en overgebracht c.q. 'gemapped' in aanpalende netwerken. Tijdens de concretiseringsfase moet worden bekeken in hoeverre QoS-markeringen binnen Azure mogelijk/noodzakelijk zijn. In ieder geval dient op het niveau van het SD-WAN QoS te worden ondersteund.</i>
Ontwerpregel 18.7	Koppeling tussen een clouddatacenter en de module Backbone is gebaseerd op minimaal 10Gbit/s, waarbij de afgenomen bandbreedte kan worden afgestemd op het gebruik.
<i>Uitwerking</i>	<i>Hierbij moet worden uitgegaan van de standaard Azure-dienstverlening in het kader van internetontsluitingen geleverd door Azure. Derhalve is dit aspect niet 'tweakable' en beschouwt het ROC FP dit aspect als afhankelijkheid van de Azure-dienstverlening.</i>
Ontwerpregel 18.8	Zowel IPv4 als IPv6 dienen te worden ondersteund.
<i>Uitwerking</i>	<i>Het is de bedoeling het netwerk van ROC FP op basis van IPv4 in te richten, maar naar de toekomst toe mag het gebruik van IPv6 niet worden uitgesloten indien use cases c.q. de noodzaak hiertoe bestaat. Hierbij moet worden aangetekend, dat per use case de mogelijkheid tot het gebruik IPv6 binnen Azure moet worden vastgesteld. Dit betreft derhalve een afhankelijk van de Azure-dienstverlening, hetgeen het ROC FP dan ook als zodanig onderkent.</i>

5 WLAN

5.1 Generiek

Ontwerpregel 19	WiFi generiek
Ontwerpregel 19.1	Bij voorkeur wordt WiFi aangeboden vanuit de module Cloud op grond van het beleidsuitgangspunt van het ROC: <i>cloud, tenzij</i>...Dit houdt in dat: - Centrale functies als controller/management vanuit 'de cloud' worden afgenomen, - Management-, provisioning- en beheerportals vanuit 'de cloud' worden afgenomen. Indien de leverancier van de module Backbone geen directe connectiviteitsmogelijkheden heeft met de leverancier van WiFi is het toegestaan connectiviteit aan te brengen vanaf de module Locatie naar de betreffende SaaS-oplossing middels een decentrale internet breakout. Hierbij dient de communicatiestroom echter wel te worden beschermd door protocollen met ingebouwde beveiligingsfuncties (e.g.: IPsec, HTTPS e.d.).
<i>Uitwerking</i>	<i>Met referentie aan paragrafen 3.2.5 Wireless en 4.1.1. NB-1 Access draadloos in het HLD. Het ROC FP gaat uit van een 'cloud, tenzij strategie' waarbij zo min mogelijk on-premises componenten en systemen worden aangebracht in de on-premises-datacenters. Aangezien vandaag de dag veel LAN/WiFi-oplossingen als managed SaaS-dienst (kunnen) worden aangeboden, gaat het ROC FP in het HLD dan ook uit van een clouddienst waar functies voor het mgmt.- en controleverkeer zich bevinden. Clouddiensten worden in dit kader direct via de lokale internetuitbraak (Direct Internet Access) benaderd. Het ROC FP staat er wel voor open een andere oplossing (e.g. on-premises) te accepteren, indien dit technologisch en/of kostentechnisch voordelen heeft.</i>
Ontwerpregel 19.2	Access points dienen de standaard IEEE 802.11ax te ondersteunen met extra functionaliteiten voor Bluetooth en Zigbee.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden hardware dient WiFi 6 te ondersteunen. Dit gezien de toename van het draadloze netwerkverkeer, onder meer door de toename in het toepassen van IoT-devices en de aantallen ontsluitende draadloze BYOD-devices. Tevens is ondersteuning van de protocollen Bluetooth en Zigbee noodzakelijk ter voorbereiding op het IoT-ecosysteem.</i>
Ontwerpregel 19.3	Access points dienen te voorzien in 4x4 MU-MIMO (Multi-User MIMO) met minimaal 4 spatial streams.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen.</i>
Ontwerpregel 19.4	Access points dienen te voorzien in flexibele radio-instellingen op grond van de RF-omgeving, waarbij deze dual band frequenties (2.4 en 5Ghz) ondersteunt.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen.</i>

Ontwerpregel 19.5	Access points dienen middels PoE van stroom te worden voorzien.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen.</i>
Ontwerpregel 19.6	Access points dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
<i>Uitwerking</i>	<i>Het is de bedoeling het netwerk van ROC FP op basis van IPv4 in te richten, maar naar de toekomst toe mag het gebruik van IPv6 niet worden uitgesloten indien use cases c.q. de noodzaak hiertoe bestaat.</i>
Ontwerpregel 19.7	Quality of Service dient te worden ondersteund in de draadloze netwerk-faciliteiten.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen. Verschillende typen verkeersstromen dienen end-to-end te kunnen worden onderscheiden en geprioriteerd (e.g. VoIP-verkeer wordt anders geprioriteerd dan regulier internetbrowsen).</i>
Ontwerpregel 19.8	Het draadloze netwerk dient multicast te ondersteunen. Het draadloze netwerk dient ook mDNS te ondersteunen in verband met te gebruiken digiborden.
<i>Uitwerking</i>	<i>Dit aspect dient te worden beschouwd als uitgangspunt voor de aanbidding door de winnaar van de aanbesteding. De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen.</i>
Ontwerpregel 19.9	Het draadloze netwerk dient goede ondersteuning/support te leveren voor 'home oplossingen' als 'hue lampen'. Hierbij dient rekening te worden gehouden met de samenhang tussen het bedrade en draadloze netwerk. Deze lampen vereisen namelijk, dat 'gewerkt' wordt binnen in hetzelfde broadcastnetwerk.
<i>Uitwerking</i>	<i>De door de winnaar van de aanbesteding aangeboden apparatuur dient dit te ondersteunen. Hierbij dient te worden opgemerkt, dat gebruikers en systemen als 'hue lampen' in principe in verschillende zones worden ondergebracht. Echter, gezien het uitgangspunt van 'werken binnen hetzelfde broadcastnetwerk' zullen gebruikers (e.g. studenten) ook binnen de zone waarin de 'hue lampen' zich bevinden moeten kunnen acteren. Dit impliceert een risico, zodat gekozen moet worden om communicatiestromen tussen gebruikers/'hue lampen' conform model 2 of 3 te laten verlopen om PEP-functies te kunnen toepassen. Dit zal situationeel moeten worden bepaald tijdens de concretiserings-fase. Tevens dient het ICT-middel van de gebruiker middels IEEE 802.1x te worden geauthentiseerd op het netwerk. Indien dit een BYOD-device betreft (en dus niet door het ROC FP wordt gemanaged) wordt het betreffende device eerst 'ge-onboard' in de RADIUS-server/Policy server om vervolgens posture assesement toe te kunnen passen. Op deze wijze worden integraal de risico's van bijvoorbeeld besmettingen gemitigeerd. Een alternatief is het alsnog toestaan van point-to-point-verbindingen op wireless niveau, maar IEEE 802.1x/BYOD-onboarding zijn hierbij wel noodzakelijk om risico's van besmettingen te mitigeren. Het ROC FP neemt NAAS als managed dienstverlening af en gaat hierbij uit van de mogelijkheid om op een veilige manier de betreffende communicatie te accommoderen. Een advies in dezen door de winnaar van de aanbesteding is derhalve relevant voor het ROC FP.</i>
Ontwerpregel 19.10	De managementomgeving/portal van het draadloze netwerk dient goede inzage te geven in 'client-gebruik', 'client-dichtheid', 'client failures', 'AP-failures'. Tevens dient de

	managementomgeving/portal te beschikken over goede monitoring & troubleshootfuncties.
<i>Uitwerking</i>	<i>Met referte aan de paragrafen 3.2.5 Wireless en 4.1.1 NB01 Access draadloos in het HLD. Het ROC FP neemt NAAS als managed dienstverlening af en gaat hierbij ervan uit, dat de centrale portal-functionaliteiten hierin voorzien. Het ROC FP gaat er hierbij vanuit, dat medewerkers van het ROC FP een leesrechten-account kunnen ontvangen voor inzage in verschillende topics.</i>
Ontwerpregel 19.11	'Local breakout' en 'central breakout' moet mogelijk zijn (al dan niet als elkaars fallbackoplossing bij storingen), waarbij authenticatie in alle omstandigheden mogelijk moet blijven.
<i>Uitwerking</i>	<i>Met referte aan par. 3.2.5 Wireless in het HLD. Op grond van de 'cloud, tenzij strategie' van het ROC geschiedt de aansturing van het draadloze netwerk vanuit de cloud (tenzij uit kostenoverwegingen/technologische overwegingen alternatieven beter passen). In dit kader is een 'klassieke central breakout' via on-premises wireless controllers in principe niet meer mogelijk of gangbaar. Indien de winnaar van de aanbesteding dit anders ziet c.q. inzet, verneemt het ROC FP dit graag in de vorm van een gefundeerd advies.</i>
Ontwerpregel 19.12	Het draadloze netwerk dient dezelfde functionaliteit te bieden als het bedrade netwerk voor dezelfde categorieën devices.
<i>Uitwerking</i>	<i>Netwerkfunctionaliteiten zijn 'een commodity' voor de gebruikers van het netwerk van het ROC FP. Met andere woorden: ongeacht de wijze van connectiviteit (draadloos of bedraad) worden alle services geleverd aan gebruikers, waarbij de netwerkomgeving transparant is voor deze gebruikers. Alle door het ROC FP aangeboden diensten worden zowel door het bedrade als het draadloze netwerk gefaciliteerd. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader dan ook uit van een uniforme infrastructuur.</i>