Uitwerking ontwerpregels architectuurblauwdruk v1.1

Architectuurgebied security

Inhoudsopgave

Documentbeheer

Revisiegeschiedenis

Versie	Opmerkingen
0.1	Opzet document
0.2	Invulling document
1.0	Vaststelling door gremium Design Office
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.

Azure-gerelateerde onderdelen zijn 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 Zonering

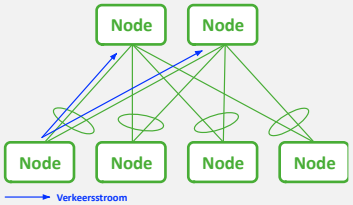
Ontwerpregel 1	Zonering
1.1	De ICT-infrastructuur van het ROC dient te kunnen worden gezoneerd. Dit geldt voor alle modules waarbinnen het ROC diensten aanbiedt.
Uitwerking	*Met referte aan par. 3.2.8.1 Zonering in het HLD. De door de winnaar van de aanbesteding aangeboden apparatuur dient zonering te ondersteunen. Het is van belang, dat binnen elke module isolatie van verschillende typen verkeer mogelijk is. De module SURF wordt ontsloten door het internet. Binnen SURF zelf worden geen netwerk- en/of securitycomponenten ondergebracht die behoren tot de NAAS-dienst-verlening. Derhalve is zonering in dit kader niet relevant voor de winnaar van de aanbesteding.*
1.2	Communicatie tussen verschillende zones dient altijd middels PEP-functies te verlopen. PEP-functies zijn de gedefinieerde koppelvlakken tussen zones. Deze koppelvlakken kunnen worden ingevuld door firewalls, packetfilters, IPS-systemen, IDS-systemen e.d. Per dienst/communicatiestroom dient in een afgeleid HLD en in overleg met de markt worden vastgesteld welke PEP-functies waar moeten worden toegepast.
Uitwerking	*Met referte aan par. 3.2.8.1 Zonering en 3.2.8.2 Segmentatie in het HLD. Zoals in het HLD is gesteld, wordt het netwerk van ROC FP verder onderverdeeld in segmenten om het beveiligingsniveau te verhogen. Afhankelijk van het communicatiemodel worden PEP-functies toegepast. In par. 3.2.10 PEP-functies zijn de verschillende PEP-functies beschreven. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat er hierbij van uit, dat de winnaar van de aanbesteding ruimte ervaring heeft in zonerings- en segmentatievraagstukken binnen gelijksoortige omgevingen als het ROC FP. Het ROC FP wil hierbij ontzorgt worden en verwacht derhalve een advies over welke PEP-functies de winnaar wel/niet inzet.*
1.3	PEP-functies dienen worden aangebracht in de module Backbone: • Voor de module Locatie (inter-zonering en directe uitbraak naar het internet), • Voor de module SURF en Cloud vanwege de beheerverantwoordelijkheid van de ICT-infrastructuur binnen deze modules door een andere partij dan het ROC. • Eventueel voor de module Datacenter (onprem) indien dit in de praktijk opportuun is (e.g. kostentechnisch neutraal, geen additionele complexe beheerlasten, standaardisatie). PEP-functies dienen te worden aangebracht in de modules: • Datacenter (onprem) voor inter-zoneringsverkeer en verkeersafhandeling vanaf het internet en de module Backbone. De PEP-functie in dit kader betreft derhalve de 'toegangspoort' naar diensten van het ROC die (nog) onprem worden aangeboden. Tevens dienen deze PEP-functies te worden gebruikt voor systemen die updates vanaf het internet ophalen.

	• SURF en Cloud voor inter-zoneringsverkeer en verkeersafhandeling afkomstig vanaf het internet en de module Backbone.
Uitwerking	*Met referte aan par. 3.2.10 PEP-functies en de securitybouwblokkenbeschrijvingen in par. 4.3 Security-bouwblokken. PEP-functies zijn integraal aangebracht op het niveau van het SD-WAN. Daarnaast is een minimale set aan PEP-functies aangebracht in de on-premises-firewall in de on-premises-datacenters. Op verkeersstromen tussen verschillende zones en die passen binnen de communicatiemodellen 2 en 3 zullen derhalve PEP-functies worden toegepast. Indien de winnaar van de aanbesteding PEP-functies wil 'uitruilen' tussen het SD-WAN-netwerk en de centrale on-premises-firewall, dan is dat toegestaan. Het blijft hierbij van belang dat geen afbreuk wordt gedaan c.q. informatiebeveiligingsrisico's ontstaan waar het de lokale internet-uitbraak (Direct Internet Access) betreft en de integraliteit van de oplossing (i.e. één managementplatform).*
1.4	PEP-functies mogen: • Als managed dienst worden afgenomen, • Geïntegreerd zijn binnen één platform, waarbij het platform gevirtualiseerd mag worden voor ondersteuning van zonerings-principes.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat derhalve uit van een managed concept. Voor het ROC FP is het van belang, dat integraliteit van de oplossing voorop staat. Met andere woorden: Het ROC FP wil toegang krijgen (i.e. een leesrechten-account) tot één cloudportal (op grond van de 'cloud, tenzij strategie') via welke het gehele security-ecosysteem kan worden geraadpleegd. Met referte aan par. 3.2.10.3 Centraal Management PEP-voorzieningen. Een platform als de centrale on-premises-firewalls voorziet hierbij in virtualisatiemogelijkheden. Met referte aan par. 3.2.10.1 Centrale on-premises firewall. Hierbij is het mogelijk om op virtueel firewall-niveau onderscheid in de toepassing van PEP-functies te kunnen aanbrengen*

2 Module Backbone – security

Ontwerpregel 2	Versleuteling van data
2.1	De module Backbone dient versleuteling van data-overdracht te ondersteunen middels encryptie-algoritmen die in de hedendaagse informatiebeveiligings-praktijk als ‘proven’ en ‘sterk’ worden beschouwd. De leverancier van de backbone dient hierbij voldoende te waarborgen, dat alleen het ROC verkeer kan ‘decrypten’.
Uitwerking	*Met referte aan par. 4.3.2 SB02 Encryptie SD-WAN in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur de functionaliteit ondersteunt.*
2.2	Versleuteling van data mag geen nadelige impact hebben op de diensten die door de module Backbone worden getransporteerd.
Uitwerking	*Met referte aan par. 4.3.2 SB02 Encryptie SD-WAN in het HLD. Het ROC FP neemt de NAAS-dienst-verlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze vereisten ondersteunt.*

3 Module Locatie - security

Ontwerpregel 3	LAN-security module Locatie
3.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
Uitwerking	*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.*  *Met andere woorden: LAG (Link Aggregation) en active/active paden worden door de apparatuur van de leverancier ondersteund.*
3.2	Overbodige services dienen te worden gedeactiveerd op de LAN-nodes.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de winnaar van de aanbesteding de overbodige services deactiveert conform de gangbare informatiebeveiligingspraktijk. Tijdens de concretiseringsfase kan/zal dit aspect waar nodig worden uitgediept en aangescherpt.*
3.3	In het kader van management mogen alleen protocollen worden gebruikt met ingebouwde beveiligingsmaatregelen. Dit wil zeggen dat het niet is toegestaan U2M en M2M verkeer naar en vanaf een node in ‘clear text’ te versturen.
Uitwerking	*Het ROC FP neemt de NAAS-dienst-verlening managed af en gaat in dit kader ervan uit, dat de winnaar van de aanbesteding het management op deze wijze inricht. Indien de winnaar van de aanbesteding gebruikmaakt van PKI-certificaten gaat het ROC FP ervan uit, dat deze tot de managed dienstverlening behoren.*
3.4	Het gebruik van een PKI-infrastructuur is de norm. De nodes dienen in dit kader het SCEP-protocol te ondersteunen, waarbij automatisch een PKI-certificaat kan worden aangebracht in de betreffende node.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur het SCEP-protocol ondersteunt. Echter, het betreft een managed dienstverlening zodat dit aspect transparant voor het ROC FP plaatsheeft zolang de certificaten maar valide zijn.*
3.5	Nodes die deel uitmaken van het LAN dienen zonering te ondersteunen waarbij op grond van gebruikers- en/of device-kenmerken gebruikers en systemen in een aparte zone kunnen worden ondergebracht. Dit op grond van de principes van IEEE 802.1x en MAB.
Uitwerking	*Met referte aan de paragrafen 3.2.8 Zonering en 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Eveneens is het van belang, dat de*

	RADIUS-server/Policy server over functionaliteiten beschikt waarmee het mogelijk is de combinatie van MAC-adres (MAB) en device-specifieke kenmerken als zodanig in beleidsregels te verwerken, opdat middels deze combinatie toegang kan worden verkregen tot het netwerk.
3.6	Om een potentiële overload van de CPU door bugs en aanvallen tegen te gaan dienen alleen de voor management noodzakelijke protocollen toegestaan te worden met gelimiteerde doorvoersnelheden.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
3.7	De nodes dienen DHCP snooping te ondersteunen. IP-adresuitgifte mag alleen worden gedaan over vertrouwde poorten. Op deze poorten worden de DHCP-servers aangesloten of switches die leiden naar de DHCP-servers. Alle overige poorten worden als onbetrouwbaar bestempeld en hierop aangesloten apparaten mogen uitsluitend DHCP-aanvragen doen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
3.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
3.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
3.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
Uitwerking	*Met referte aan de par. 3.2.8 Zonering/segmentatie in het HLD. Logische scheiding van verkeersstromen dient te worden ondersteund door de door de winnaar van de aanbesteding aangeboden apparatuur. Fysieke scheiding is hierbij niet noodzakelijk.*
3.11	De nodes dienen het RADIUS-protocol te ondersteunen in het kader van toegangsbeveiliging middels de principes van IEEE 802.1x en MAB.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
3.12	De nodes dienen IEEE 802.1x en MAB te ondersteunen.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
3.13	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.

Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Indien de centrale mgmt.- en controle-omgeving niet meer functioneert kan alsnog worden teruggevallen op het direct inloggen in netwerknodes. Hierbij moet worden aangetekend, dat device administration (e.g. troubleshooten) door de winnaar van de aanbesteding wordt gedaan. Het ROC FP verwacht hierbij middels een leesrechten-account toegang te kunnen krijgen tot de netwerknodes.*
3.14	Verkeer naar/vanaf de module Backbone en het internet dient middels PEP-functies te verlopen. Aan de markt wordt om advies gevraagd welke PEP-functies exact moeten worden geïmplementeerd op grond van best practices en het marksegment van het ROC (onderwijs/vergelijkbare omgevingen).
Uitwerking	*Met referte aan par. 3.2 SD-WAN in het HLD. Het SD-WAN-netwerk is de representatie van de module Backbone en is qua underlay-netwerk samengesteld uit internetdragers. Het SD-WAN-netwerk voorziet hierbij in een lokale internetuitbraak (Direct Internet Access) waarbij PEP-functies noodzakelijk zijn. Met referte aan par.3.2.10 PEP-functies in het HLD. Aan de markt wordt gevraagd naar de best practices voor de aantallen, typen, posities en toepassingen van PEP-functies op grond van vergelijkbare omgevingen en conform de gangbare informatiebeveiligingspraktijk.*
3.15	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*

4 WLAN-security

Ontwerpregel 4	WLAN-security
4.1	Het draadloze netwerk dient te zijn gebaseerd op WPA2/Enterprise. Voor authenticatie dient gebruikgemaakt te worden van IEEE802.1x en MAB.
Uitwerking	*Met referte aan paragrafen. 3.2.9. Network Access Control (IEEE 802.1x/MAB) en 4.3.14 Encryptie WLAN in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Het ROC FP verwacht in dit kader ook een advies t.a.v. WPA3 (nut/noodzaak o.b.v. vergelijkbare omgevingen).*
4.2	Om versleuteling (privacy) van berichtgevingen tussen de Access Points en wireless clients te borgen, dient gebruikgemaakt te worden van AES als cryptografisch algoritme. CCMP dient te worden gebruikt voor het bewaken van de integriteit van deze berichtgevingen.
Uitwerking	*Met referte aan par. 4.3.13 SB14 Encryptie WLAN in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
4.3	Access points dienen dermate te zijn opgesteld/gepositioneerd, dat deze niet binnen handbereik zijn of eigenmachtig gemaakt kunnen worden.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze de access points strategisch onderbrengt in de omgeving van het ROC FP. Tijdens de concreti-seringsfase zal dit onderdeel verder worden geduid met de winnaar van de aanbesteding.*
4.4	De WLC of gelijksoortige centrale draadloze functionaliteit dient verkeersscheiding te ondersteunen in het Distribution Systeem/ ICT-infrastructuur van het ROC.
Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
4.5	Bij het inloggen in een access point of WLC middels de console dient een warning banner tevoorschijn te komen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
4.6	De WLC of gelijksoortige centrale draadloze functionaliteit dient te voorzien in functies waarmee point-to-point verbindingen tussen wireless clients kunnen worden geblokkeerd.
Uitwerking	*Met referte aan par. 4.3.11 SB01 Zonering/segmentatie in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*

4.7	Het draadloze netwerk dient zonering te ondersteunen, waarbij op grond van gebruikers- en/of device-kenmerken gebruikers en systemen in een aparte zone kunnen worden ondergebracht. Dit op grond van de principes van IEEE 802.1x en MAB.
Uitwerking	*Met referte aan paragrafen 3.2.8 Zonering/segmentatie en 3.2.9. Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Het is van belang, dat de RADIUS-server/Policy server over functionaliteiten beschikt waarmee het mogelijk is de combinatie van MAC-adres (MAB) en device-specifieke kenmerken als zodanig in beleidsregels te verwerken opdat middels deze combinatie toegang kan worden verkregen tot het netwerk.*
4.8	Het draadloze netwerk dient het RADIUS-protocol te ondersteunen in het kader van toegangsbeveiliging middels de principes van IEEE 802.1x en MAB.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
4.9	Het draadloze netwerk dient het TACACS-protocol te ondersteunen in het kader van device administration van de access points en, indien van toepassing, de centrale draadloze functionaliteiten.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Indien de centrale mgmt.- en controle-omgeving niet meer functioneert kan alsnog worden teruggevallen op het direct inloggen in netwerknodes. Hierbij moet worden aangetekend, dat device administration (e.g. troubleshooten) door de winnaar van de aanbesteding wordt gedaan. Het ROC FP verwacht hierbij middels een leesrechten-account toegang te kunnen krijgen tot de netwerknodes.*
4.10	Het productieverkeer dient te zijn gescheiden van het managementverkeer.
Uitwerking	*Met referte aan de par. 3.2.8 Zonering/segmentatie in het HLD. Logische scheiding van verkeersstromen dient te worden ondersteund door de door de winnaar van de aanbesteding aangeboden apparatuur. Fysieke scheiding is hierbij niet noodzakelijk.*
4.11	Indien de centrale draadloze faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
4.12	Het dient mogelijk te zijn rogue access points te detecteren en daarop (automatisch) te kunnen acteren. Hetzelfde geldt t.a.v. bijvoorbeeld WiFi Pineapple.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*

5 Toegangsbeveiliging

Ontwerpregel 5	Toegangsverleningsdienst
5.1	Toegang tot het bedrade en draadloze netwerk van het ROC dient middels een toegangsverleningsdienst te worden gereguleerd.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Zowel draadloze als bedrade toegang tot het netwerk wordt in eerste instantie gereguleerd middels IEEE 802.1x en/of MAB. Het is van belang, dat de RADIUS-server/Policy server over functionaliteiten beschikt waarmee het mogelijk is de combinatie van MAC-adres (MAB) en device-specifieke kenmerken als zodanig in beleidsregels te verwerken opdat middels deze combinatie toegang kan worden verkregen tot het netwerk. Tevens is het noodzakelijk om BYOD-devices te kunnen 'onboarden' via portals in de RADIUS-server/Policy server op grond waarvan de status van het device kan worden achterhaald, rekeninghoudende met voorschriften vanuit de AVG. De toegangsverleningsdienst is een combinatie van Active Directory, Azure Active Directory en Intune.*
5.2	Centrale onderdelen van de toegangsverleningsdienst (i.e. de RADIUS-omgeving) wordt bij voorkeur in als clouddienst afgenomen, tenzij er goede redenen zijn deze faciliteiten in het eigen onprem datacenter aan te brengen. Indien deze als clouddienst worden afgenomen, dient de IDP van het ROC te worden gebruikt.
Uitwerking	*In het HLD is het ROC uitgegaan van het aanbrengen van de RADIUS-server/Policy server in Azure. Dit op grond van de strategie 'cloud, tenzij'. Azure is echter out-of-scope. Indien de winnaar van de aanbesteding een andere systematiek erop nahoudt, staat het ROC daarvoor open mits de uitgevraagde functionaliteiten geleverd kunnen worden en bijvoorbeeld een on-premises-installatie kostenloos en zonder (noemenswaardige) onderbrekingen alsnog naar bijvoorbeeld een Azure kan worden gemigreerd in de toekomst. Het ROC neemt hierbij de dienstverlening managed af.*
5.3	Managed gebruikers van het ROC dienen middels user credentials te kunnen inloggen op het netwerk. Dit op basis van het IEEE 802.1x protocol.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Credentials kunnen zich ook in Azure Active Directory bevinden. Tijdens de concretiseringsfase zal dit aspect nader worden geduid.*
5.4	Managed computers (CYOD) zijn niet meer AD-joined, maar AAD-joined. Aan de markt wordt een advies gevraagd hoe deze computers op een gestandaardiseerde en veilige wijze toegang te verlenen tot het netwerk van het ROC.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB). In het HLD gaat het ROC ervan uit, dat de 'store' voor CYOD wordt ingevuld middels Intune. Dit om middels IEEE802.1x de status van een CYOD-device te kunnen raadplegen en verifiëren op compliancy. Tijdens de concretiseringsfase zal dit aspect nader worden geduid.*
5.5	Het is toegestaan managed systemen te laten inloggen op het netwerk middels het MAC-adres. Dit op basis van MAB (MAC Address Bypass) met dien verstande, dat

	aanvullende systeemspecifieke kenmerken worden meegestuurd bij het authenticatieverzoek.
Uitwerking	*Met referte aan de par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het is van belang, dat de RADIUS-server/Policy server over functionaliteiten beschikt waarmee het mogelijk is de combinatie van MAC-adres (MAB) en device-specifieke kenmerken als zodanig in beleidsregels te verwerken opdat middels deze combinatie toegang kan worden verkregen tot het netwerk*
5.6	Na authenticatie dienen managed gebruikers/computers automatisch te worden ondergebracht in een zone.
Uitwerking	*Met referte aan paragrafen. 3.2.8 Zonering/segmentatie en 3.2.9. Network Access Control (IEEE 802.1x/MAB) in het HLD. Op grond van aangebrachte beleidsregels in de RADIUS-server/Policy server krijgt een device/gebruiker een autorisatieniveau toegewezen, waarbij gebruikgemaakt kan worden van bijvoorbeeld VLAN-toewijzing of tag waarmee verdere 'beleidsbeslissingen' in het netwerk gemaakt kunnen worden. Het ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
5.7	Na authenticatie dienen managed systemen te worden ondergebracht in een zone die voor hen bestemd is. Dit kunnen verschillende zones zijn afhankelijk van het type systeem.
Uitwerking	*Met referte aan paragrafen. 3.2.8 Zonering/segmentatie en 3.2.9. Network Access Control (IEEE 802.1x/MAB) in het HLD. Op grond van aangebrachte beleidsregels in de RADIUS-server/Policy server krijgt een device/gebruiker een autorisatieniveau toegewezen, waarbij gebruikgemaakt kan worden van bijvoorbeeld VLAN-toewijzing of tag waarmee verdere 'beleidsbeslissingen' in het netwerk gemaakt kunnen worden. Het ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
5.8	Foutief inloggen leidt ertoe, dat geen gebruikgemaakt kan worden van het netwerk van het ROC (zowel bedraad als draadloos).
Uitwerking	*ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Dit conform de functionaliteiten zoals beschreven in par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het is hierbij van belang, dat foutieve inlogpogingen worden vastgelegd/gelogd in de centrale RADIUS-server/Policy server.*
5.9	Indien de centrale RADIUS-faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
Uitwerking	*ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Dit conform de functionaliteiten zoals beschreven in par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD.*
5.10	Het dient (bij voorkeur) mogelijk te zijn alle typen devices die worden ontsloten aan het ROC-netwerk te valideren op de juiste systeem updates, virusupdates, patchupdates

	e.d. Indien deze niet up-to-date zijn, dienen deze devices automatisch te worden ondergebracht in een aparte quarantaine zone van waaruit de benodigde remediation servers (op het internet) kunnen worden bereikt. De oplossing dient hierbij de gebruikers van dergelijke systemen te informeren over de status van het device. Na 'remediation' dienen de managed computers/systemen zich opnieuw aan te melden op het netwerk.
Uitwerking	*ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Dit conform de functionaliteiten zoals beschreven in par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Dit geldt derhalve niet alleen voor BYOD-gebruik maar ook voor bijvoorbeeld CYOD-gebruik, waarbij de status van het device (i.e. wel/niet compliant) de basis vormt voor netwerktoegang. Met andere woorden: posture assessment is van belang om te kunnen toepassen waarbij systeemvalidaties kunnen worden uitgevoerd.*
5.11	Gasten van het ROC dienen in een zone te worden opgenomen waarmee alleen internet als dienst kan worden benaderd.
Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Zonering en segmentatie voorzien in de logische scheiding tussen onderdelen van het fysieke netwerk. Op grond van beleidsregels in de RADIUS-server/Policy server wordt een apparaat, systeem of gebruiker ondergebracht in vooraf gedefinieerde netwerkzones en onderhavige segmenten. Eén van deze zones betreft derhalve een gastennetwerk.*
5.12	Studenten aan andere onderwijsinstellingen worden geauthentiseerd middels de RADIUS-proxy van SURF. Het ROC-netwerk dient te worden ontworpen om dit gebruik te faciliteren. Na authenticatie worden studenten aan andere onderwijsinstellingen in een zone opgenomen waarmee alleen internet als dienst kan worden benaderd.
Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Zonering en segmentatie voorzien in de logische scheiding tussen onderdelen van het fysieke netwerk. Op grond van beleidsregels in de RADIUS-server/Policy server wordt een apparaat, systeem of gebruiker ondergebracht in vooraf gedefinieerde netwerkzones en onderhavige segmenten. Eén van deze zones betreft derhalve een netwerkzone waarvanuit alleen het internet kan worden benaderd. Deze zone kan derhalve hetzelfde zijn als de zone voor het gastgebruik.*
5.13	De centrale RADIUS-faciliteiten kunnen beschikken over een eigen Identity database voor authenticatiedoeleinden in het kader van MAB. Hierbij wordt een advies van de markt gevraagd -> i.e. MAB binnen de eigen Identity database versus MAB binnen de (A)AD-omgeving van het ROC.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. De toename in het gebruik van bijvoorbeeld systemen als IoT leidt er mogelijk toe, dat meer en meer devices alleen middels MAB + devicekenmerken kunnen worden geauthentiseerd. Tijdens de concretiseringsfase zal hierover nader worden gedelibereerd. Het ROC FP gaat hierbij uit van een door de winnaar van de aanbesteding geformuleerd advies op grond van vergelijkbare systemen en omgevingen.*

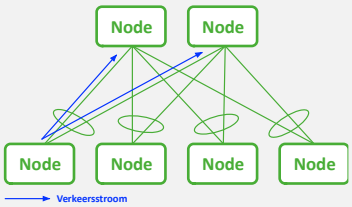
5.14	De oplossing dient te kunnen communiceren met een IDP-omgeving van het ROC voor authenticatiedoeleinden voor studenten/medewerkers van het ROC.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Tijdens de concretiseringsfase zal hierover nadere afstemming plaatsvinden. IDP-omgevingen zijn in ieder geval Active Directory, Azure Active Directory en Intune. Het ROC gaat hierbij uit van een door de winnaar van de aanbesteding geformuleerd advies op grond van vergelijkbare omgevingen.*
5.15	De authenticatie voor studenten/medewerkers is gebaseerd op TEAP, waarbij van de markt wordt verwacht een certificaat hiertoe te implementeren. Van de markt wordt ook verwacht een voorstel te doen voor de gebruikte versleuteling die in gelijksoortige onderwijsomgevingen wordt gebruikt of als sterk wordt beschouwd in de gangbare informatiebeveiligingspraktijk.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Tijdens de concretiseringsfase zal hierover nadere afstemming plaatsvinden. IDP-omgevingen zijn in ieder geval Active Directory, Azure Active Directory en Intune. Het ROC FP gaat hierbij uit van een door de winnaar van de aanbesteding geformuleerd advies op grond van vergelijkbare omgevingen. Hierbij kan worden afgeweken van TEAP, zodra dit bijvoorbeeld technologisch noodzakelijk is in cloudomgevingen met dien verstande dat recht blijft worden gedaan aan de gangbare informatiebeveiligingsprak-tijk.*
5.16	Van de markt wordt een oplossing verwacht voor profiling, temeer steeds meer apparatuur als IoT-devices (e.g. sensoren) aan het netwerk worden verbonden. Middels deze functie dienen alle MAC-adressen te worden vastgelegd in een centrale identity store (zie ontwerpregel 5.13).
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat dit aspect tot de dienstverlening behoort. Het ROC FP gaat hierbij uit van een door de winnaar van de aanbesteding geformuleerd advies op grond van vergelijkbare omgevingen. Tijdens de concretiseringsfase zal hierover nadere afstemming plaatsvinden.*
5.17	MAC-adres registratie moet worden meegenomen in de CMDB, waarbij gezien de hoeveelheid aan (toekomstige) MAC-adressen en de foutgevoeligheid van handmatige verwerking een automatisch proces van opname moet kunnen worden afgedwongen.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat dit aspect tot de dienstverlening behoort. Het ROC FP gaat hierbij uit van een door de winnaar van de aanbesteding geformuleerd advies op grond van vergelijkbare omgevingen waar bijvoorbeeld middels profilingfuncties MAC-adressen automatisch centraal worden vastgelegd en inzichtelijk worden gemaakt. Tijdens de concretiseringsfase zal hierover nadere afstemming plaatsvinden.*
5.18	Het dient mogelijk te zijn configuratiegegevens en operationele data op een extern medium op te slaan (backup), zodat bij issues deze data kan worden teruggezet op de centrale toegangsfaciliteiten.
Uitwerking	*Het ROC FP neemt de dienstverlening managed af en gaat hierbij ervan uit, dat dit aspect tot de dienstverlening behoort. Het ROC FP gaat hierbij ervan uit, dat logging*

	ook kan worden verkregen en worden opgeslagen in een door het ROC FP opgegeven bestemming.
5.19	Het is aan de markt te adviseren of de centrale oplossing als appliance, virtual machine of als SaaS-dienst wordt ingezet.
Uitwerking	*Met referte aan par. 3.2.9 Network Access Control (IEEE 802.1x/MAB) in het HLD. Het ROC FP gaat in het HLD uit van centrale RADIUS/Policy-functionaliteiten in Azure. Dit op grond van de 'cloud, tenzij' strategie die het ROC FP voert. Echter, Azure is out-of-scope. Derhalve wordt van de markt een advies verwacht hoe en waar de functionaliteit in te richten.*

6 Module Datacenter (onprem) - security

Ontwerpregel 6	Functionele onderdelen Datacenter (onprem)
6.1	Tussen de functionele onderdelen: • Publieke DMZ voor applicaties die publiekelijk geraadpleegd kunnen worden. • Beheer DMZ voor systemen, applicaties, tooling waarmee beheerders van het ROC of beheerders van externe partijen hun beheerwerkzaamheden kunnen uitvoeren. Dit geldt ook voor managementsystemen van bijvoorbeeld draadloze faciliteiten, authenticatieservers e.d. • Front-end en Back-end systemen die diensten leveren in de productieomgeving van het ROC. • Front-end en Back-end systemen die gebruikt worden in het kader van OTA-doeleinden. dient een scheiding te zijn aangebracht middels PEP-functies.
Uitwerking	*Met referte aan paragrafen 3.2.8 Zonering/segmentatie in het HLD. Deze omgevingen zijn ondergebracht in aparte zones. Op verkeer tussen zones en in relatie tot communicatiemodellen 2 en 3 worden PEP-functies toegepast die zich op het niveau van de centrale on-premises-firewall bevinden.*
6.2	De randen van het Datacenter (onprem) dienen te zijn afgeschermd van de modules Internet en Backbone middels PEP-functies.
Uitwerking	*Met referte aan de paragrafen 3.2.3 SD-WAN en 3.2.10 PEP-functies in het HLD. Op het niveau van het SD-WAN-netwerk worden PEP-functies aangebracht die de randen van het on-premises-datacenter afschermen. Zie tevens de security-paragraaf 4.3 Security-bouwblokken voor meer duiding van PEP-functies.*
6.3	Het is toegestaan het platform dat PEP-functies biedt middels virtualisatie-technieken voor meerdere doeleinden te gebruiken. Dit wil zeggen, dat het is toegestaan om alle PEP-functies in relatie tot alle functionele onderdelen (en zones daarbinnen) onder te brengen in één fysiek platform dat virtualisatiemogelijkheden biedt voor scheiding van domeinen. Het platform dient hierbij een beschikbaarheid van 99,99% in de keten te ondersteunen (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid). Hierbij wordt een advies van de markt verwacht t.a.v. deze centrale PEP-functies in de module Datacenter (onprem).
Uitwerking	*Met referte aan par. 3.2.10 PEP-functies in het HLD. Het on-premises-firewallcluster wordt opgedeeld in verschillende virtuele firewalls ter ondersteuning van het zonerings-concept/functionele scheiding van omgevingen. Van de markt wordt een end-to-end-ke-tenbeschikbaarheidsberekening verwacht. Voor wat betaalbaarheid wordt verwezen naar par. 2.10 Risico's als mogelijke risico-mitigatiemaatregel.*

Ontwerpregel 7	LAN-security Datacenter (onprem)
7.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
Uitwerking	*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.  *Met andere woorden: LAG (Link Aggregation) en active/active paden worden door de apparatuur van de leverancier ondersteund.*
7.2	Overbodige services dienen te worden gedeactiveerd.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de winnaar van de aanbesteding de overbodige services deactiveert conform de gangbare informatiebeveiligingspraktijk. Tijdens de concretiseringsfase kan/zal dit aspect waar nodig worden uitgediept.*
7.3	In het kader van management mogen alleen protocollen worden gebruikt met ingebouwde beveiligingsmaatregelen. Dit wil zeggen dat het niet is toegestaan U2M- en M2M-verkeer naar en vanaf een node in 'clear text' te versturen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de winnaar van de aanbesteding het management op deze wijze inricht. Indien de winnaar van de aanbesteding gebruikmaakt van PKI-certificaten gaat het ROC FP ervan uit, dat deze tot de managed dienstverlening behoren.*
7.4	Het gebruik van een PKI-infrastructuur is de norm. De nodes dienen in dit kader het SCEP-protocol te ondersteunen, waarbij automatisch een PKI-certificaat kan worden aangebracht in de betreffende node.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur het SCEP-protocol ondersteunt. Echter, het betreft een managed dienstverlening zodat dit aspect transparant voor het ROC FP plaatsheeft zolang de certificaten maar valide zijn.*
7.5	Nodes die deel uitmaken van het DC-LAN dienen zonering te ondersteunen. Hierbij dienen de nodes verkeersscheiding op logisch niveau te ondersteunen.
Uitwerking	*Met referte aan de par. 3.2.8 in het HLD. Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*
7.6	Om een potentiële overload van de CPU door bugs en aanvallen tegen te gaan dienen alleen de voor management noodzakelijke protocollen toegestaan te worden met gelimiteerde doorvoersnelheden.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
7.7	De nodes dienen DHCP snooping te ondersteunen. IP-adresuitgifte mag alleen worden gedaan over vertrouwde poorten. Op deze poorten worden de DHCP-servers aangesloten of switches die leiden naar de DHCP-servers. Alle overige poorten worden

	als onbetrouwbaar bestempeld en hierop aangesloten apparaten mogen uitsluitend DHCP-aanvragen doen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
7.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
7.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteit ondersteunt.*
7.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
Uitwerking	*Met referte aan de par. 3.2.8 Zonering/segmentatie in het HLD. Logische scheiding van verkeersstromen dient te worden ondersteund door de door de winnaar van de aanbesteding aangeboden apparatuur. Fysieke scheiding is hierbij niet noodzakelijk.*
7.11	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt. Indien de centrale mgmt.- en controle-omgeving niet meer functioneert kan alsnog worden teruggevallen op het direct inloggen in netwerknodes. Hierbij moet worden aangetekend, dat device administration (e.g. troubleshooten) door de winnaar van de aanbesteding wordt gedaan. Het ROC FP verwacht hierbij te kunnen beschikken over een leesrechten-account.*
7.12	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur deze functionaliteiten ondersteunt.*

7 Azure- security

Ontwerpregel 8	Azure security hub-and-spoke topologie
8.1	Directe communicatie tussen spokes is niet toegestaan. Indien communicatie noodzakelijk is, dient deze te verlopen via de hub.
Uitwerking	*Met referte aan par. 3.2.6 Azure in het HLD. Communicatie tussen spokes wordt omgeleid via het hubnetwerk, waarin de SD-WAN-node is ondergebracht. Deze node verricht in dit kader de PEP-functies. Let op: ook al behoren systemen in verschillende spokes tot dezelfde zone (of mate van vertrouwdheid in dezen), directe communicatie is niet toegestaan op grond van het niet te hoeven aanleggen van spoke-to-spoke-vnet-connecties. M.a.w.: er wordt geopteerd voor eenduidigheid en eenvoud van beheer.*
8.2	Verkeer van/naar het internet, dat direct via Azure wordt aangeboden, dient middels een PEP-functie te zijn afgeschermd. Deze PEP-functie dient aanwezig te zijn in de hub.
Uitwerking	*Met referte aan par. 3.2.6 Azure in het HLD. In het hubVnet zijn de PEP-functies ondergebracht en wel op het niveau vvan de SD-WAN-node.*
8.3	Verkeer van/naar de module Backbone dient middels een PEP-functie te zijn afgeschermd. Deze PEP-functie dient aanwezig te zijn in de hub.
Uitwerking	*Met referte aan par. 3.2.6 Azure in het HLD. In het hubVnet zijn de PEP-functies ondergebracht en wel op het niveau van de SD-WAN-node. Via de SD-WAN-node is verkeer naar en vanaf de module Backbone, zijnde het SD-WAN-netwerk en de lokale internetuitbraak (Direct Internet Access), middels PEP-functies afgeschermd.*
8.4	Het is toegestaan zowel cloud native (Azure) als vendorspecifieke platformen in te zetten voor het realiseren van de PEP-functies. Hier dient een goede afweging aan ten grondslag liggen, waarbij performance en kosten belangrijke factoren zijn.
Uitwerking	*Het ROC FP neemt de dienstverlening managed af. In het HLD is uitgegaan van PEP-functies op het niveau van het SD-WAN, temeer op deze manier integraliteit van de oplossingen wordt gerealiseerd in plaats van puntoplossingen (e.g. geen DDOS-protectie via de SD-WAN-node, maar via Azure). Tijdens de conretiseringsfase kan dit aspect nader worden afgestemd.*
8.5	In het kader van management mogen alleen protocollen worden gebruikt met ingebouwde beveiligingsmaatregelen. Dit wil zeggen dat het niet is toegestaan U2M en M2M verkeer naar en vanaf een node in ‘clear text’ te versturen.
Uitwerking	*Het ROC FP neemt de NAAS-dienst-verlening managed af en gaat in dit kader ervan uit, dat de winnaar van de aanbesteding het management op deze wijze inricht. Indien de winnaar van de aanbesteding gebruikmaakt van PKI-certificaten gaat het ROC FP ervan uit, dat deze tot de managed dienstverlening behoren.*
8.6	Het gebruik van een PKI-infrastructuur is de norm. De nodes dienen in dit kader het SCEP-protocol te ondersteunen, waarbij automatisch een PKI-certificaat kan worden aangebracht in de betreffende node.
Uitwerking	*Het ROC FP neemt de NAAS-dienstverlening managed af en gaat in dit kader ervan uit, dat de door de winnaar van de aanbesteding aangeboden apparatuur het SCEP-protocol ondersteunt. Echter, het betreft een managed dienstverlening zodat dit aspect transparant voor het ROC FP plaatsheeft zolang de certificaten maar valide zijn.*

8 Internet of Things

Ontwerpregel 9	IoT-lagen
9.1	Het IoT-ecosysteem van het ROC is gebaseerd op vier lagen: 1. IoT-devices (de IoT-componenten/objecten zelf), 2. Netwerk & Connectiviteit (de netwerkfuncties in de modules Locatie, Backbone, Datacenter (onprem), SURF, Cloud), 3. Platformen voor verschillende processen en dataopslag, 4. Applicaties die 'iets met de processen en data' doen.
Uitwerking	*Het HLD beschrijft in dit kader de zonering/segmentatie, netwerkconnectiviteit en toegang tot het netwerk middels IEEE802.1x/MAB. Met referte aan het integrale HLD.*
9.2	Bij voorkeur worden platformen en applicaties benut vanuit de modules Cloud en SURF, temeer de strategie van het ROC gebaseerd is op het 'cloud, tenzij' principe.
Uitwerking	*Met referte aan paragrafen 3.2.3 SD-WAN, 3.2.4 SD-LAN, 3.2.5 Wireless, 3.2.10.3 Centraal management PEP-voorzieningen in het HLD. In het HLD is uitgegaan van integraliteit van centrale mgmt.- en controlesystemen die als SaaS-dienst worden afgenomen. Dit derhalve vanuit de module Cloud, tenzij de winnaar van de aanbesteding een andersoortige cloudoplossing heeft of wegens goed onderbouwde motieven on-premises-componenten wil aanbrengen die in de toekomst kosteloos en zonder (noemenswaardige) service-onderbrekingen alsnog naar een cloud-omgeving kunnen worden gemigreerd).*
9.3	Ontsluiting van IoT-devices dient te zijn gebaseerd op het IP-protocol, waarbij zowel IPv4 als IPv6 ondersteund dienen te worden
Uitwerking	*De 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.*
9.4	Ontsluiting van IoT-devices dient zowel bedraad als draadloos te kunnen worden uitgevoerd.
Uitwerking	*Het access-netwerk op de verschillende locatietypen voorziet zowel in draadloze als bedrade netwerktoegang. Tijdens de concretiseringsfase zullen verdiepingsslagen worden gemaakt met de winnaar van de aanbesteding. Dit betreft bijvoorbeeld sizing en poortbezettingen, waarbij het ROC FP ervan uitgaat dat het netwerk voorziet in zowel horizontale als verticale schaalbaarheid.*

Ontwerpregel 10	Scheiding IT/OT
10.1	Zowel IT- als OT-zones dienen te worden aangebracht binnen hetzelfde fysieke netwerk, waarmee consolidatie van dit netwerk wordt gerealiseerd (i.e. geen separate fysieke netwerken). Scheiding is derhalve op logisch niveau en niet op fysiek niveau.
Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Zonering en segmentatie voorzien in de logische scheiding tussen onderdelen van het fysieke netwerk. Op grond van beleidsregels in de RADIUS-server/Policy server wordt een apparaat, systeem of*

	gebruiker ondergebracht in vooraf gedefinieerde netwerkzones en onderhavig segmenten.
10.2	Tussen IT- en OT-devices dient een scheiding te zijn aangebracht op het niveau van het geconsolideerd netwerk. Hiertoe dienen IT-systemen in IT-zones te worden ondergebracht en OT (IoT)-systemen in OT-zones, tenzij IoT-systemen en IT-systemen in hetzelfde broadcastdomein aanwezig moeten zijn. Het ROC vraagt hierbij advies van de markt om voldoende beveiligingswaarborgen te kunnen afdwingen voor deze uses cases. Bijv: Hoe is het mogelijk te maken dat BYOD-devices van studenten dit type IoT- devices 'rechtstreeks' kunnen benaderen. Soms hebben IoT-devices als eis, dat beide devices in hetzelfde broadcast domain zitten en bijvoorbeeld MDNS nodig hebben. Deze wens gaat tegen de zoneringseis in. Immers, men wil het IoT-device niet in dezelfde zone hebben als het BYOD-device van de student, maar veel IoT en home-domotica vereisen dit echter wel. Hetzelfde geldt voor bijvoorbeeld een hue lamp (bedraad IoT-device) dat in dezelfde zone aanwezig moet zijn als een onbedraad BYOD-device.
Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Zonering en segmentatie voorzien in de logische scheiding tussen onderdelen van het fysieke netwerk. Op grond van beleidsregels in de RADIUS-server/Policy server wordt een apparaat, systeem of gebruiker ondergebracht in vooraf gedefinieerde netwerkzones en onderhavig segmenten. Dit geldt derhalve ook voor scheiding tussen IT- en OT-devices (i.e. IoT-devices).* *Met referte aan par. 3.2.8.2 segmentatie in het HLD. Binnen zones worden verschillende typen segmenten aangemaakt in het kader waarvan verkeersstromen worden gefaciliteerd conform de betreffende communicatiemodellen. Indien communicatie noodzakelijk is binnen een zone (en normaliter tussen zones plaatsheeft) en binnen hetzelfde broadcastdomein communicatie noodzakelijk is, wordt communicatiemodel 3 toegepast waarbij verkeersstromen via de PEP-functies in de SD-WAN-node worden omgeleid om te worden 'gecontroleerd'. Alle communicerende entiteiten bevinden zich in hetzelfde segment en broadcastdomein, maar communicatie tussen deze entiteiten is zonder PEP-functies niet toegestaan. De facto wordt hierbij uitgegaan van het zero-trust-model om betreffende communicatie zo veilig mogelijk te laten verlopen. BYOD-devices wordt in dit kader toegang verleend tot het netwerk, nadat deze zijn 'geonboard' in de portal van de RADIUS-server/Policy server. Met referte aan par. 3.2.9 Network Access Control (IEEE802.1x/MAB) in het HLD.*

Ontwerpregel 11	**Communicatie IT/OT**
11.1	Indien tussen IT- en OT-devices (IoT) communicatie nodig is, geschiedt dit middels PEP-functies zoals deze aangebracht dienen te zijn voor inter-zoneringsverkeer. Van de markt wordt verwacht een voorstel te doen hoe en op welke manier scheiding aan te brengen, waarbij eveneens communicatie tussen IT/OT-systemen mogelijk kan zijn. Dit op grond van best practices zoals deze gelden voor een onderwijsinstelling als het ROC.

Uitwerking	*Met referte aan par. 3.2.8 Zonering/segmentatie in het HLD. Zonering en segmentatie voorzien in de logische scheiding tussen onderdelen van het fysieke netwerk. Op grond van beleidsregels in de RADIUS-server/Policy server wordt een apparaat, systeem of gebruiker ondergebracht in vooraf gedefinieerde netwerkzones en onderhavig segmenten. Interzoneringsverkeer verloopt via centrale PEP-functies die op het niveau van het SD-WAN zijn aangebracht. Indien communicatie tussen IT- en OT-systemen op het niveau van het datacenter noodzakelijk is, verlopen de verkeersstromen via de centrale on-premises-firewall alwaar PEP-functies worden uitgeoefend.*