Techniek - Architectuurblauwdruk architectuurgebied Security

Kaders en richtlijnen

Inhoudsopgave

1 Introductie en achtergrond

1.1 Werken onder architectuur

Met het 'werken onder architectuur' wordt ervoor gezorgd, dat losse onderdelen in hun samenhang worden ontworpen, zowel op het niveau van de business, de informatievoorziening als de technische middelen. Een architectuurblauwdruk bevat een samenhangende beschrijving van de door het ROC gebruikte en geleverde ICT-services, informatie-uitwisseling en infrastructurele onderdelen. Het stelt daarmee de kaders voor ontwerp en beheer. Samenwerking en het bereiken van een gezamenlijk doel op het niveau van de business is de voornaamste reden, waarbij de beginselen, grondslagen en richtlijnen op het gebied van architectuur worden gedragen door het senior management.

In deze architectuurblauwdruk wordt het architectuurgebied *Security* beschreven.

1.1.1 Doelstelling architectuurblauwdruk *Techniek - architectuurgebied Security*?

In de blauwdruk worden de volgende onderwerpen beschreven (vanuit het perspectief security):

- De onderlinge uitwerking van de business-, informatie-, en technische architectuurgebieden van het ROC.
- De standaarden (ontwerpregels) die bij het ontwerpen van de technische architectuur gehanteerd dienen te worden. De beschreven/geïllustreerde onderdelen worden door ontwerpregels gevolgd.
- De ontwerpregels geven richtlijnen bij het opstellen van HLDs, LLDs en andere afgeleide technische ontwerpen.
- De architectuurbouwblokken ofwel functionele modules waaruit het te beschrijven architectuurgebied is opgebouwd.
- Eventuele architectuurpatronen die binnen het beschreven architectuurgebied onderkend worden.

1.1.2 Wat zijn ontwerpregels?

Ontwerpregels zijn richtinggevend op het gebied van de (technische) architectuur. Deze zijn gebaseerd op:

- Beleid en business-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de business en vertaald naar de technische eigenschap van de infrastructuur,
- Informatie-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de informatievoorziening en vertaald naar de technische eigenschap van de infrastructuur,

- Technische-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de techniek en vertaald naar de technische eigenschap van de infrastructuur.
- Security-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden op het vlak van informatieveiligheid en vertaald naar de technische eigenschap van de infrastructuur.

Gebruikte ontwerpregels in dit document zijn als volgt vormgegeven:

Ontwerpregel #	**Onderwerp**
[Uitleg van de ontwerpregel]	

Alle ontwerpregels zijn in Bijlage A: Ontwerpregels Technische Architectuur - architectuurgebied Security gegroepeerd opgenomen.

1.1.3 Wat zijn architectuurbouwblokken/ functionele modules[1]?

Architectuurbouwblokken ofwel functionele modules zijn entiteiten binnen een architectuurgebied die services bieden aan hun omgeving. Een bouwblok kan:

- zelfstandig services leveren aan de omgeving,
- interactie hebben met één of meerdere andere bouwblokken om services te realiseren,
- samengesteld zijn uit meerdere (andere) bouwblokken binnen een architectuurdomein,
- onderdeel uitmaken van een groter samengesteld bouwblok,
- (bij voorkeur) herbruikt worden,
- op diverse manieren samengesteld worden zonder de specifieke kenmerken en interfaces van het bouwblok te veranderen.

Een bouwblok wordt onderkend door domeinexperts als een aparte entiteit vanwege:

- de samenhang in, of tussen, de functies die het heeft, en/of,
- de set diensten die het levert.

Een bouwblok heeft:

- expliciet en eenduidig te definiëren grenzen,
- specifieke functies, kenmerken en eigenschappen,
- interfaces via welke interactie met aanpalende bouwblokken plaatsvindt.

Een bouwblok is *loosely coupled* met de architectuur omgeving.

[1] *Met referte aan https://pubs.opengroup.org/architecture/togaf9-doc/arch/ ; Part IV - Architecture Content Framework, 33.Building Blocks*

De opdeling van een architectuurgebied in bouwblokken is specifiek voor een bepaalde organisatie of bedrijf. Echter, een goede opdeling van een architectuur in bouwblokken levert voordelen op bij de integratie van, en interoperabiliteit tussen systemen. Tevens vergroot een goede opdeling flexibiliteit bij de realisatie van systemen en applicaties.

De in dit document onderkende bouwblokken worden in de volgende tabelvorm beschreven of samengevat, waarbij antwoord wordt gegeven op de gestelde vragen en taakstellingen:

TA-bouwblok: <naam>	
(Beknopte) Conceptuele beschrijving van het bouwblok	[Geef een beknopte conceptuele beschrijving van het bouwblok. E.g. waaruit bestaat het bouwblok? Welk doel dient het? Welke interfaces heeft het bouwblok? Op welke wijze vindt interactie met de omgeving plaats?]
Functies van het bouwblok	[Beschrijf de functies die het bouwblok heeft en waardoor het services kan realiseren.]
Services dat het bouwblok biedt (aan de omgeving)	[Beschrijf de services die het bouwblok realiseert en die kunnen worden geconsumeerd door andere architectuur componenten (objecten, bouwblokken, et cetera)]
Kwaliteitskenmerken	[Beschrijf de (kwaliteits)eisen en beperkingen in termen van, schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, et cetera.]

1.1.4 Wat zijn architectuurpatronen[2]?

Architectuurpatronen zijn combinaties van architectuurbouwblokken en/of componenten waarvan de toegevoegde waarde wordt onderkend en is bewezen in de context van de enterprise architectuur. Architectuurpatronen zijn herbruikbaar en bieden een oplossing/ invulling voor een specifiek probleem.

Een architectuurpatroon beschrijft:

- wanneer bepaalde bouwblokken worden toegepast,
- waarom bepaalde bouwblokken worden toegepast en
- in welke gevallen bepaalde bouwblokken worden toegepast.

De in dit document beschreven architectuurpatronen zijn volgens de onderstaande tabelvorm vormgegeven, waarbij antwoord wordt gegeven op de beschreven taakstellingen.

[2] *Met referte aan https://pubs.opengroup.org/architecture/togaf9-doc/arch/ ; Part IV - Architecture Content Framework, 22. Architecture Patterns*

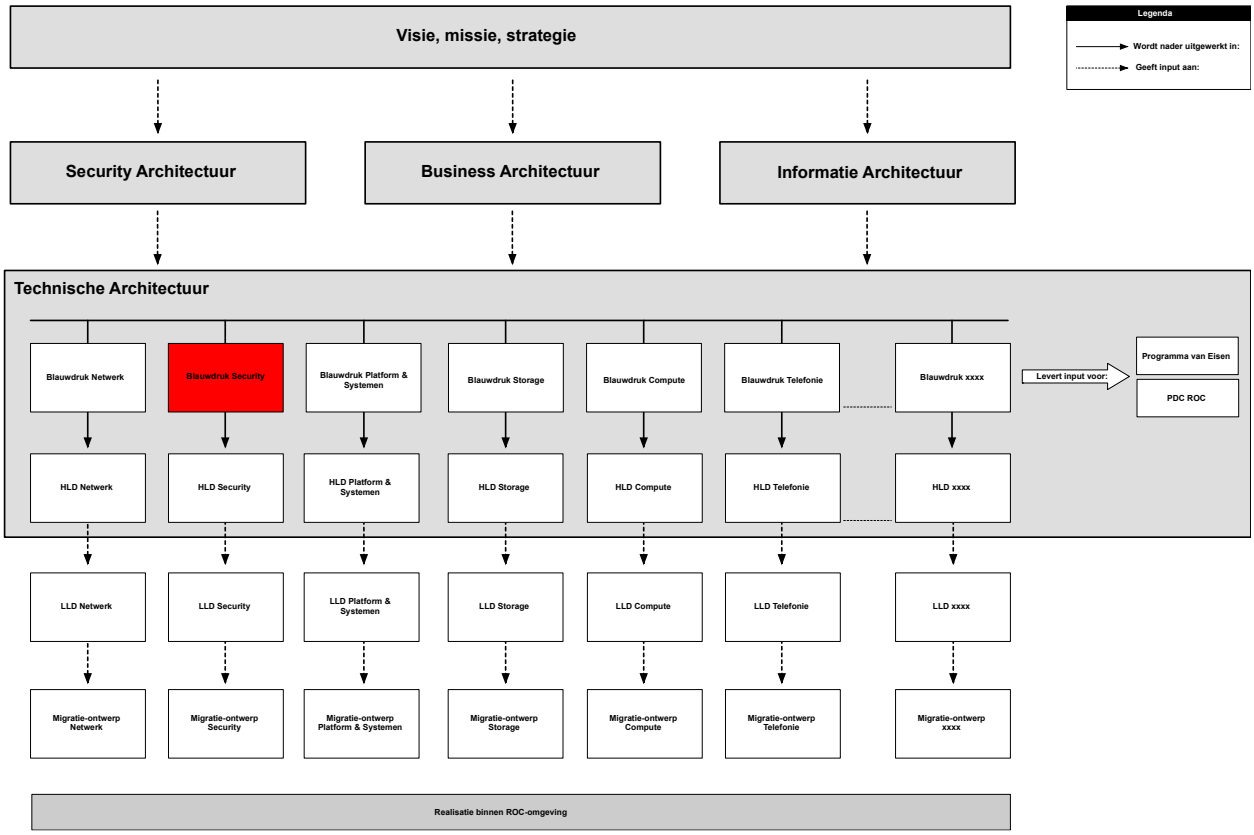
TA-patroon: <naam>	
Toepassing	[Beschrijf het probleem dat het patroon oplost/doel dat bereikt wordt.]
Context	[Beschrijf de condities waaronder het patroon wordt toegepast. Wanneer is het nodig?]
Eisen en beperkingen	[Beschrijf de (kwaliteits)eisen en beperkingen aan het patroon. E.g. op het vlak van schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, et cetera.]
Functionele beschrijving patroon	[<Beschrijf tekstueel op conceptueel niveau wat het doel is van het patroon en hoe dit wordt gerealiseerd. Visualisatie middels platen helpt hierbij.]

1.2 Positie architectuurblauwdruk en scope

In figuur 1-1 op de volgende pagina is de positie van deze architectuurblauwdruk *Techniek – architectuurblauwdruk architectuurgebied Security* (rood) afgebeeld in relatie tot andere documentatie op het gebied van de Enterprise Architectuur. Een architectuurblauwdruk wordt gebruikt als management- en stuurinstrument en vormt de basis voor afgeleide documentatie. Tevens levert het input in het kader van vervolgtrajecten (e.g. RFP-trajecten).

Door in afgeleide technische documentatie als het HLD de ontwerpregels vanuit de architectuur-blauwdruk als leidraad te nemen, zijn alle functioneel en technisch uitgewerkte onderdelen herleidbaar tot aan de betreffende ontwerpregels in deze architectuurblauwdruk. Op deze manier ontstaat een consistent architectuurlandschap, waarbij onderdelen in samenhang worden ontworpen. Dit geldt zowel binnen een architectuurdomein als in relatie tot aanpalende architectuurgebieden.

Deze architectuurblauwdruk beschrijft de diverse services die geleverd worden door de te onderscheiden (architectuur) bouwblokken (ofwel functionele modules) in het architectuurgebied *Security.*



Figuur 1-1: *Positie architectuurblauwdruk Techniek - architectuurgebied Security*

1.3 Belanghebbenden architectuurblauwdruk

Tabel 1-1: *Overzicht belanghebbenden*

Belanghebbenden	Concerns	Invloed (R,A,C,I)[3]	Toelichting
Lead architect Design Office	Conformiteit met technische doelarchitectuur	A	Quality Assurance rol. De technische architectuur zorgt voor het technisch fundament voor de business (en informatie) architectuur. De doelarchitecturen op het vlak van de business en techniek zijn en moeten op elkaar afgestemd blijven, ook bij de doorontwikkeling hiervan.

[3] *RACI = Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Consulted (geraadpleegd), Informed (geïnformeerd).*

Lead architect Netwerk	Conformiteit met technische doelarchitectuur	R	De blauwdruk geeft de technische kaders voor onderliggende architectuur-ontwerpen. Een kwalitatief goede en volledige blauwdruk is essentieel bij het realiseren van de vereiste diverse onderdelen/ diensten/ services binnen de technische doelarchitectuur
Manager Operationeel Beheer	Kwaliteit technische dienstverlening	C	Het daadwerkelijk conform SLA aanbieden van technische automatiseringsdiensten aan klanten van het ROC gebeurt door de operationele afdeling(en) van het ROC. Manager Operationeel Beheer is op dit vlak derhalve operationeel eindverantwoor-delijke.
Service Level Management	Volledigheid PDC/ dienstenportfolio	I	ROC heeft als missie om het primaire en secondaire proces maximaal te ondersteunen bij het halen van haar doelstellingen. Deze ondersteuning bestaat uit automatiseringsdiensten die geleverd worden via (standaard) producten en services uit de PDC.
Security Architect	Conformiteit met security doelarchitectuur	C,I	De Security Architect verifieert of onderdelen van de technische architectuurblauwdruk in overeen-stemming zijn met het vigerende informatiebeveiligingsbeleid van het ROC en in lijn zijn met relevante wet- en regelgeving vanuit de gangbare informatie-beveiligingspraktijk.

1.4 Doelgroep architectuurblauwdruk

- Organisatieonderdelen op het gebied van Beleid en Strategie,
- Organisatieonderdelen op het gebied van Project en Architectuur,
- Organisatieonderdelen op het gebied van Uitvoering en Beheer,
- Business Architecten,
- Informatie Architecten,
- ICT Architecten,
- Security Architecten,
- Technisch Architecten,
- Externe partijen na voorlopige gunning bij aanbestedingen.

1.5 Uitgangspunten

Tijdens het schrijven van dit document zijn de volgende uitgangspunten gehanteerd:

- Het ROC bevindt zich in een transitieperiode. Men is bezig de IT-organisatie te veranderen van een beheerorganisatie in een regie-organisatie. Dit houdt in, dat men:
    - outtasking van standaard ICT-middelen nastreeft,
    - afname van door externe partijen gehoste en beheerde diensten prefereert boven (de eigen ontwikkelde) inhouse-diensten.
- In het kader van dienstverlening in de onderwijssector heeft de SURF-organisatie een speciale rol. Normaliter wordt in een architectuurblauwdruk geen of nauwelijks namen van producten en vendoren opgenomen, gezien de doelstellingen van een architectuurblauwdruk. In concreto -> het (generiek) beschrijven en duiden van architectuureisen waaraan de technische architectuur dient te voldoen. De technische architectuur kan namelijk worden ingevuld door verschillende producten en diensten van verschillende vendoren. Gezien de speciale rol die de SURF-organisatie echter heeft in de onderwijssector in het algemeen en in relatie tot het ROC in het bijzonder, is in deze blauwdruk op verschillende plaatsen bewust de naam SURF opgenomen.
- Architectuurbouwblokken en architectuurpatronen zijn generiek beschreven en voorzien van ontwerpregels. Nadere uitwerking van ontwerpregels dient in afgeleide technische documentatie als HLDs te worden vormgegeven en vastgelegd, waarbij de ontwerpregels vanuit deze blauwdruk als fundament dienen. Dit leidt tot de vraagstelling:

  Wanneer is een nadere uitwerking compleet of volledig en wie bepaalt dat?

  Het antwoord op deze vragen wordt door het gremium Design Office gegeven. Leden[4] van dit gremium stellen onderling vast of functionele uitwerkingen in afgeleide technische documentatie voldoen aan:

[4] *Het gremium Design Office bestaat in hoofdzaak uit de architecten van het ROC. Er zijn in dit kader echter geen beperkingen. Indien noodzakelijk kunnen ook materiedeskundigen (intern/extern) of andere rollen (e.g. engineers (intern/extern), Informatie Management)) worden uitgenodigd zitting te nemen in het gremium (waar nodig)).*

- de generieke ontwerpregels vanuit de architectuurblauwdruk en
- de vigerende wet- en regelgeving waaraan de oplossing(en) dienen te voldoen.

Zodoende kan worden gesteld, dat de architectuurblauwdruk het kader schept voor ontwerp en beheer, maar waarbij ontwerpregels niet per definitie in 'beton zijn gegoten'. Immers, de praktijk is in het algemeen complexer en weerbarstiger waardoor niet 'alles voor 100%' kan worden afgevangen in een architectuurblauwdruk.

- In navolging van de voorgaande bullet dient derhalve te worden uitgegaan van het principe *pas-toe-of-leg-uit*. Ontwerpregels in deze blauwdruk dienen te worden opgevolgd, tenzij met goede redenen kan worden gemotiveerd waarom van de 'baseline' is afgeweken.

1.6 Indeling architectuurblauwdruk

De architectuurblauwdruk bestaat uit de volgende onderdelen:

- **Hoofdstuk 1: Introductie en achtergrond**
  Dit hoofdstuk bevat een inleiding bij de architectuurblauwdruk. De onderbouwing van de blauwdruk en de doelgroepen voor wie het geschreven is, worden kort toegelicht. Tevens worden onderdelen als scope van de architectuurblauwdruk en de belanghebbenden behandeld.

- **Hoofdstuk 2: Dataclassificatie ROC**
  Dit hoofdstuk bevat relevante verwijzingen naar betreffende documenten, waarin data-classificaties en beheersmaatregelen zoals deze voor het ROC gelden zijn toegelicht en uitgewerkt.

- **Hoofdstuk 3: Normenkader Technische Architectuur - architectuurgebied Security**
  In dit hoofdstuk is het normenkader beschreven zoals dat binnen de technische kaders voor het architectuurgebied Security wordt gebruikt.

- **Bijlage 4: Modules Technische Architectuur - architectuurgebied Security**
  In dit hoofdstuk is de technische architectuur voor het architectuurgebied Security nader beschreven.

- **Bijlage A: Ontwerpregels Technische Architectuur - architectuurgebied Security**
  Deze bijlage bevat een gegroepeerd overzicht van alle ontwerpregels die in het document zijn beschreven. Dit voor het overzicht, zodat per topic in één oogopslag de betreffende ontwerpregels kunnen worden achterhaald.

- **Bijlage B: Gebruikte afkortingen**
  Deze bijlage bevat een lijst met afkortingen die gebruikt worden in dit document.

2 Dataclassificatie ROC

2.1 Dataclassificatie ROC

Het classificeren van data is gebaseerd op de impactanalyse van de ‘categorieën’ (B)eschikbaarheid, (I)ntegriteit en (V)ertrouwelijkheid van een bepaalde applicatie of dienst. Per voornoemde categorie onderscheidt het ROC hierbij drie niveau’s:

1. Laag,
2. Midden,
3. Hoog.

Voor meer informatie wordt verwezen naar het document ‘BIV-classificatie ROC’.

2.2 Beheersmaatregelen

Op basis van de vastgestelde classificatie worden beheersmaatregelen toegepast. Voor een algemeen overzicht van diensten, dienstenclassificatie en betreffende beheersmaatregelen wordt verwezen naar de Excelsheet ‘BIV-classificatie en beheersmaatregelen informatievoorziening ROC Friese Poort’.

3 Normenkader Technische Architectuur - architectuurgebied Security

3.1 Normenkader technische architectuur - security

In de onderstaande tabel is het normenkader opgenomen zoals dit gebruikt dient te worden binnen de technische architectuur van het ROC en derhalve betrekking heeft op het architectuurgebied dat wordt beschreven in deze blauwdruk. Het generieke normenkader is bewust op deze plaats opgenomen, vanwege het verdere gebruik in vervolgillustraties en onderdelen van de blauwdruk.

Tabel 2-1: *Normenkader*

Norm	Toelichting
Architectuurbouwblok	Zie par. 1.1.3
Architectuurgebied	Een architectuurgebied beschrijft een afgebakend deel van de technische architectuur. Architectuurgebieden in het kader van de technische architectuur zijn: • Netwerk, • Security, • Unified communications, • Platformen & Systemen (inclusief Cloud) • Enterprise Mobility • Werkplek
Architectuurpatroon	Zie par. 1.1.4
Domein	Een deel van een bepaald architectuurgebied. In het kader van het security -> e.g. domein LAN, domein Datacenter-LAN, domein WAN.
Koppelvlak	Interface tussen twee of meerdere architectuurbouwblokken.
Module	De technische infrastructuur van het ROC is opgedeeld in vaste modules waarbinnen zich architectuurbouwblokken bevinden. Door gebruik te maken van vaststaande modules wordt ervoor gezorgd, dat ieder architectuurgebied hetzelfde stramien volgt c.q. ‘geplot wordt’ binnen de vaststaande modules. Dit zorgt voor samenhang in ontwerp van en een gestructureerd overzicht tussen verschillende architectuurgebieden. De vaststaande modules zijn: • Locatie, • Backbone, • Datacenter (onprem), • Cloud (clouddatacenters, IaaS, PaaS, SaaS), • SURF (gezien de bijzondere positie als dienstenleverancier),

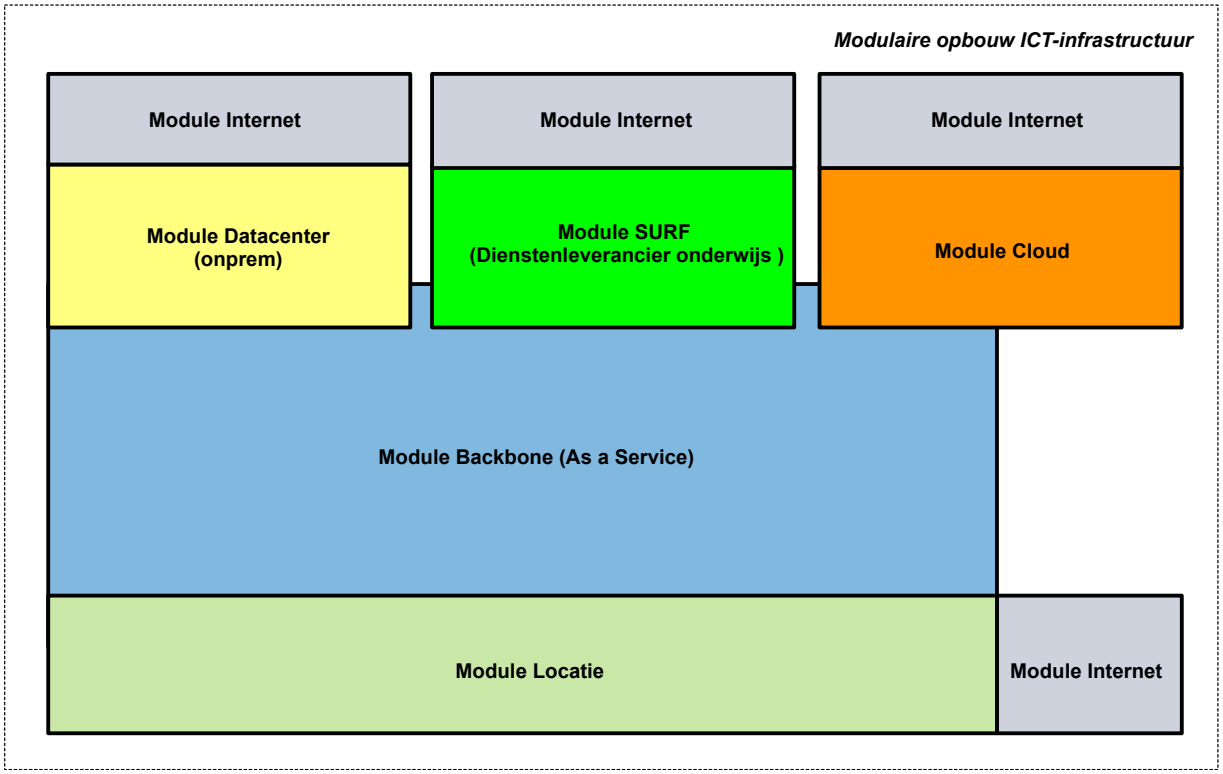
	• Internet.
Node	Een switch, router, firewall, loadbalancer et cetera.
OT	Operational Technologie als ‘tegenhanger’ van Information Technologie. Alle IoT-objecten van het ROC vallen onder de noemer OT.
Zone	Een zone is een geïsoleerd netwerk van ICT-services met gelijkwaardige functionaliteiten, waarin gegevens theoretisch vrijelijk kunnen worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken.

4 Modules Technische Architectuur - architectuurgebied Security

4.1 Generiek overzicht modules

De ROC-infrastructuur is modulair opgebouwd zoals afgebeeld in de onderstaande illustratie. Dit betreft een generiek model dat gebaseerd is op:

- de regio Nederland,
- waarbij de organisatieonderdelen van het ROC gevestigd zijn te:
    - Leeuwarden,
    - Drachten,
    - Emmeloord,
    - Sneek,
    - Dokkum,
    - Urk.



Figuur 4-1: *Overzicht modules ROC*

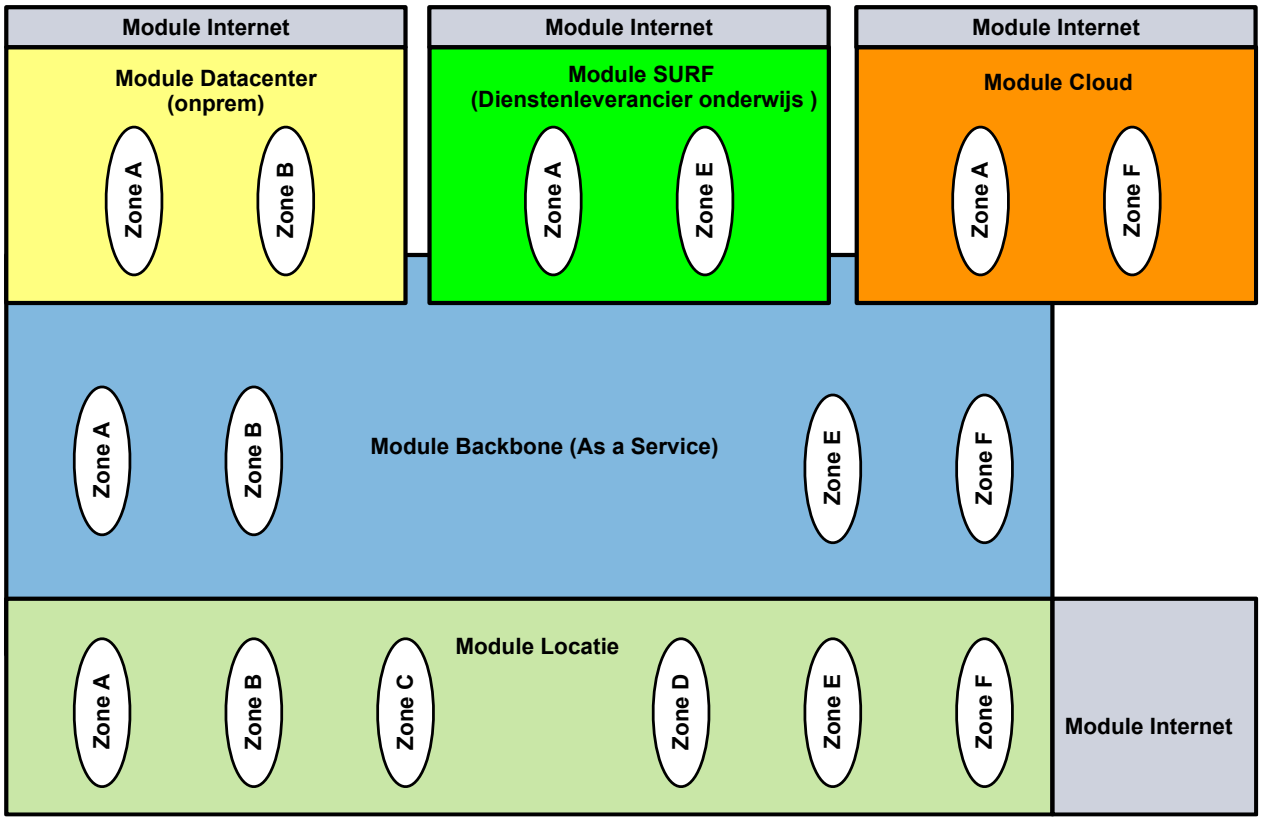
Door de ROC-infrastructuur op te delen in verschillende modules wordt ervoor gezorgd, dat deze infrastructuur:

- Gestandaardiseerd,
- Betrouwbaar,
- Voorspelbaar,
- Beveiligingsfuncties ondersteunt (e.g. segmentatie),
- Sourceable en,
- Schaalbaar is.

Voor uitleg over alle modules en architectuurbouwblokken (ABBs) daarbinnen die netwerkgerelateerd zijn, wordt verwezen naar het document 'Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0'.

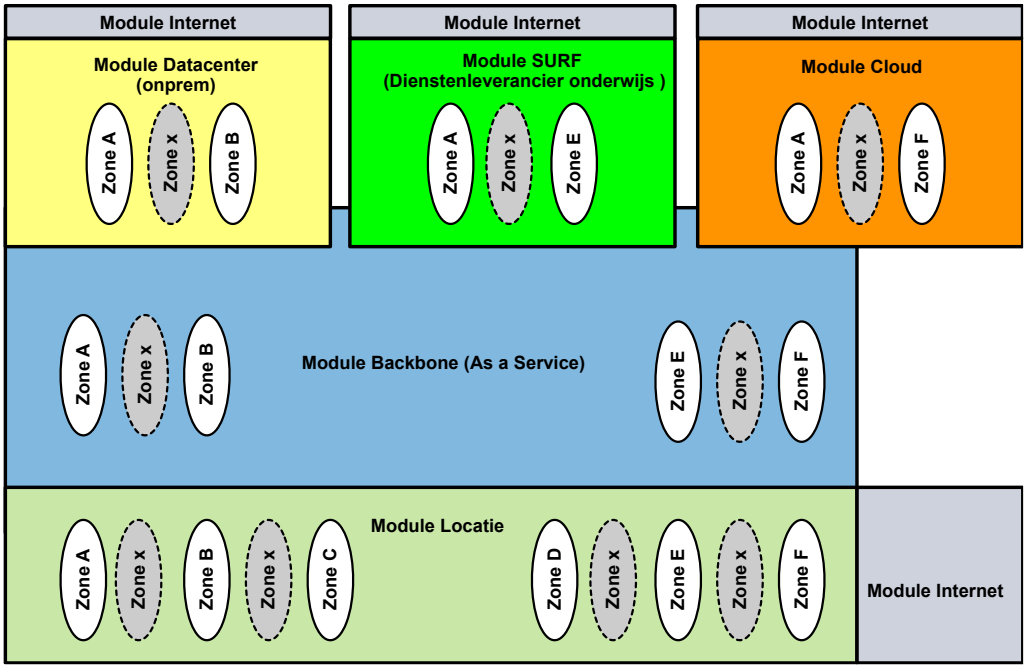
4.2 Zonering

In de onderstaande illustratie zijn zones 'geplot' op de technische infrastructuur van het ROC.

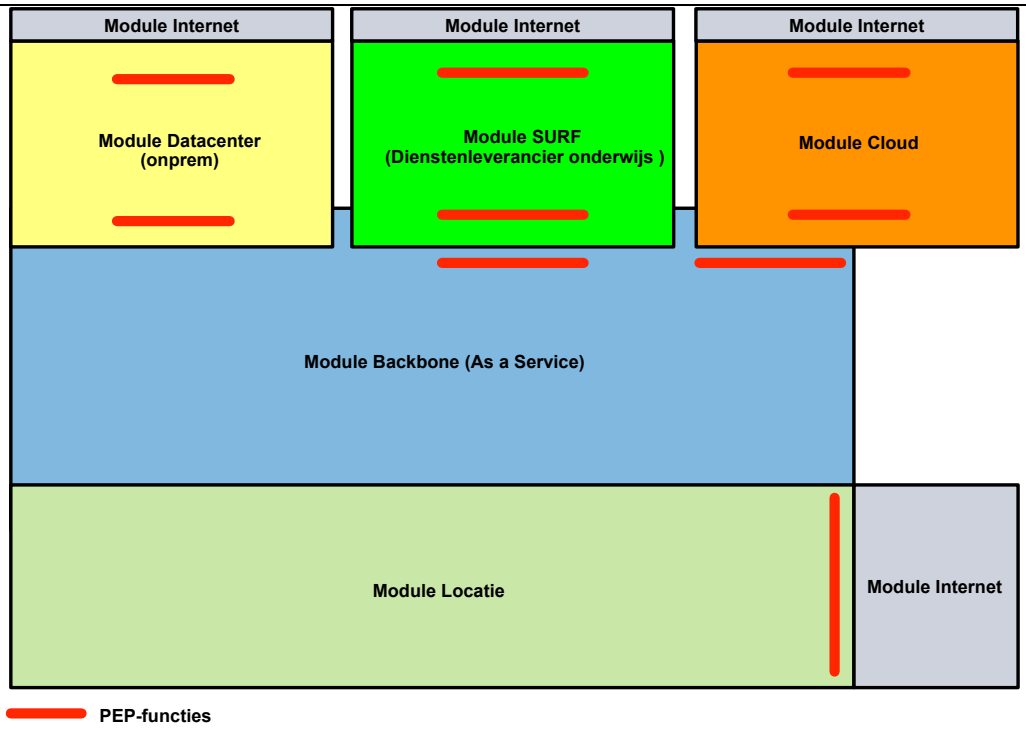


Figuur 4-2: *Overzicht zonering*

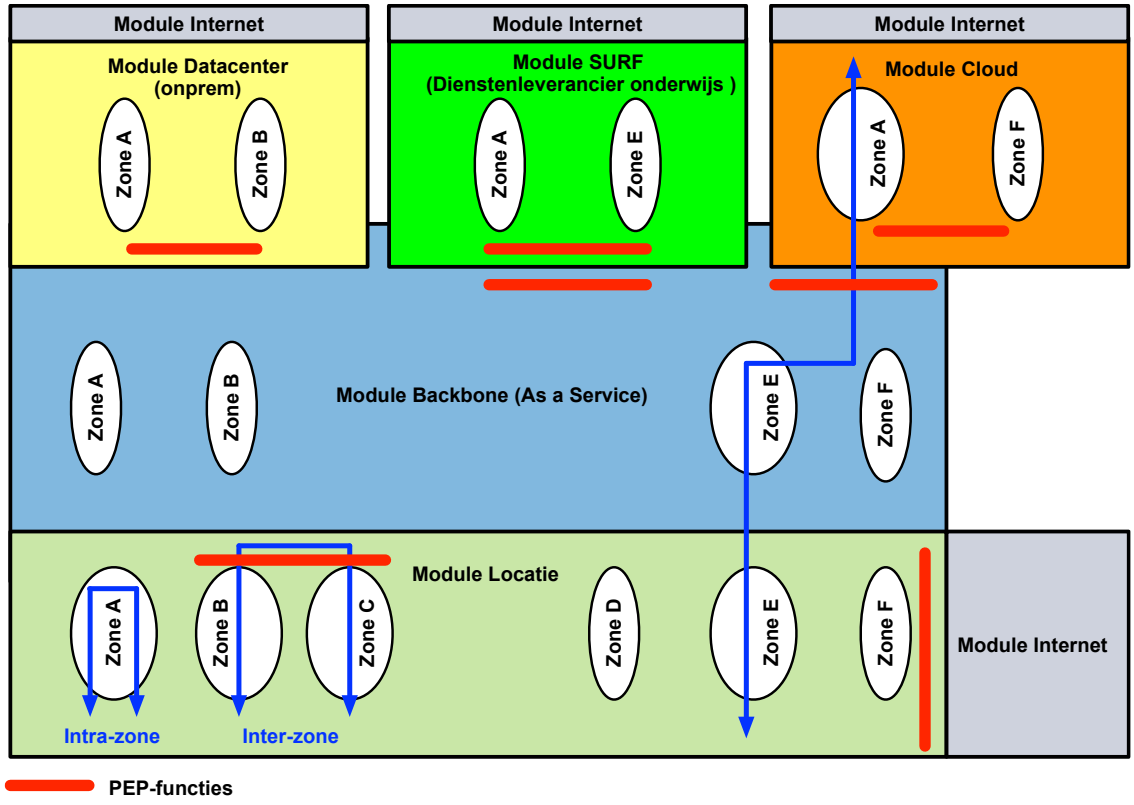
4.2.1 TA-patronen

TA-patroon: Zonering	
Toepassing	Op basis van dataclassificatie kan de beheersmaatregel *zonering* worden toegepast. In de verschillende omgevingen die het ROC gebruikt, kunnen één of meerdere zones worden gedefinieerd. Een zone is een geïsoleerd netwerk van ICT-voorzieningen, waarin gegevens theoretisch vrijelijk kunnen worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken.
Context	Zonering wordt gebruikt voor het scheiden van diensten op het niveau van de technische infrastructuur. Op grond van dataclassificatie kunnen ICT-voorzieningen (waarmee diensten worden aangeboden) in een aparte zone worden ondergebracht. Zones kunnen zowel lokaal zijn aangebracht als over alle modules heen. Te denken valt aan een aparte zone voor management die module-overstijgend is.
Eisen en beperkingen	Zones dienen flexibel te kunnen worden geconfigureerd. Flexibiliteit in dezen houdt in: • Eenvoudig opschaalbaar/afschaalbaar en uitbreidbaar/inkrimpbaar door het ROC, • Centraal aanstuurbaar/configureerbaar (i.e. portalfunctie), • Op het niveau van een SaaS-dienst (en eventuele PaaS-diensten) kan het voorkomen, dat zonering niet kan worden toegepast omdat het ROC geen zeggenschap heeft over de onderliggende ICT-infrastructuur van de dienst.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. De flexibele uitbreiding bestaat uit de grijs gemaakte zone x. 

TA-patroon: Posities PEP-functies	
Toepassing	PEP staat voor Policy Enforcement Point. Het wordt gebruikt om IB-beveiligingsmaatregelen van het ROC toe te passen op communicatiestromen tussen verschillende zones.
Context	Binnen een zone is uitwisseling van gegevens zonder meer mogelijk zonder tussenkomst van een PEP-functie. Communicatie tussen verschillende zones dient te verlopen middels een PEP-functie voor filtermogelijkheden van onderhavige communicatiestromen. PEP-functies dienen strategisch te worden opgesteld binnen de ICT-infrastructuur van het ROC (binnen de vastgestelde modulaire opbouw).
Eisen en beperkingen	• PEP-functies dienen strategisch te worden aangebracht voor filtering van verkeersstromen. • Module Locatie: PEP-functies worden aangebracht voor zowel inter-zone-verkeer als eventuele directe uitbraak naar het internet. • Modules SURF en Cloud: PEP-functies dienen te worden aangebracht op het niveau van de module Backbone en op het niveau van de modules SURF en Cloud. Binnen deze laatste twee modules kan eveneens inter-zone-verkeer plaatsvinden, zodat PEP-functies op dit niveau moeten worden toegepast. Tevens dienen diensten die het ROC afneemt te worden afgeschermd van het internet. Aangezien de onderliggende fysieke infrastructuur van de modules SURF en Cloud niet in beheer is bij het ROC dient op het niveau van de module Backbone richting deze modules ook PEP-functies te zijn aangebracht. De PEP-functies op het niveau van de module Backbone mogen ook gebruikt worden voor verkeer afkomstig van bijvoorbeeld Azure richting de Backbone. Hierdoor hoeft geen ‘dubbele PEP-functie’ te worden aangebracht. M.a.w.: het is toegestaan een separate PEP-functie binnen Azure aan te brengen voor inter-zone-verkeer en verkeer dat vanuit Azure direct het internet opgaat. Verkeer dat naar de Backbone verloopt mag hierbij worden afgehandeld door de PEP-functie die op het niveau van de module Backbone is aangebracht. In illustraties wordt echter deze ‘dubbele PEP-functie’ gehandhaafd. • Module Datacenter (onprem): PEP-functies dienen te worden aangebracht op het niveau van de module zelf voor inter-zone-verkeer en het afschermen van het datacenter t.o.v. de module Backbone en het internet. • Alle platformen die PEP-functies uitoefenen dienen bij voorkeur te kunnen worden gemanaged vanaf één beheertool/platform. Dit geldt in de breedste zin van de modulaire opbouw van de ICT-infrastructuur van het ROC. Aan de markt wordt advies gevraagd over de positionering van de PEP-functies.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld.



TA-patroon: Communicatie zonering	
Toepassing	Binnen een zone is uitwisseling van gegevens zonder meer mogelijk zonder tussenkomst van een PEP-functie. Communicatie tussen zones dient te verlopen middels een PEP-functie voor filtermogelijkheden van onderhavige communicatiestromen.
Context	Op grond van het beveiligingsbeleid van het ROC wordt vastgesteld welke diensten (gefaciliteerd door ICT-voorzieningen) op welke wijze worden gezoneerd. Hierbij dienen ook de betreffende communicatiestromen tussen de gezoneerde diensten te zijn vastgesteld, zodat kan worden bepaald welke communicatiestromen tussen diensten wel en welke niet zijn toegestaan. Op toegestane communicatiestromen kunnen vervolgens verschillende PEP-functies worden toegepast zoals statefull firewalling, IPS/IDS, Anti-virus e.d. In een afgeleid High Level Design en in overleg met de markt dient per zone-overstijgende communicatiestroom te worden vastgesteld welke exacte PEP-functies moeten worden toepast op welke communicatiestroom.
Eisen en beperkingen	• Op inter-zone-verkeer dienen PEP-functies te worden toegepast. Dit geldt voor verschillende zones. Op het niveau van de backbone is geen inter-zone-verkeer. • Intra-zone-verkeer dient zonder tussenkomst van PEP-functies te kunnen worden afgehandeld. • Zonering en verkeer tussen zones is niet mogelijk bij SaaS-diensten (en in het algemeen bij PaaS-diensten met uitzondering van PaaS-diensten die binnen bijvoorbeeld Azure middels Service Endpoints of Private-links worden geaccommodeerd), vanwege het beheer van de onderliggende ICT-infrastructuur door de partij die de SaaS/PaaS-dienst aanbiedt. In dit geval moet middels andere IB-

	maatregelen getracht worden verkeersstromen tussen diensten te reguleren (e.g. middels RBAC).
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. Verkeersstromen binnen een zone worden zonder tussenkomst van een PEP-functie afgehandeld. Verkeersstromen tussen verschillende zones worden middels PEP-functies afgehandeld. Het onderstaande overzicht is een generiek model, zodat alle principes van intra- en inter-zoneringsverkeer gelden voor alle zones (waar deze ook zijn aangemaakt). 

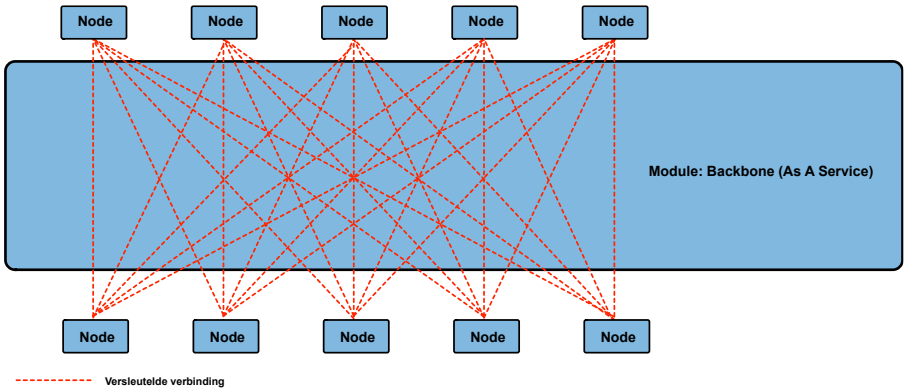
4.2.2 Ontwerpregels

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.
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.

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.
1.4	PEP-functies mogen: • Als managed dienst worden afgenomen, • Geïntegreerd zijn binnen één platform, waarbij het platform gevirtualiseerd mag worden voor ondersteuning van zoneringsprincipes.

4.3 Module Backbone - security

Naast zoneringsaspecten die ook door de module Backbone dienen te worden ondersteund, is het van belang data op een veilige manier binnen de Backbone te transporteren.

TA-patroon: Versleuteling van datatransport	
Toepassing	Veiligheid staat voorop. Dit houdt voor het ROC ook in, dat getransporteerde data binnen de module Backbone versleuteld is (transportversleuteling). Dit zorgt ervoor, dat (vertrouwelijke) data niet kan worden uitgelezen door onbevoegden.
Context	Al het verkeer dat de module Backbone transporteert wordt versleuteld. Hoewel het merendeel van het in de aanpalende modules geïnitieerd en geretourneerd verkeer op applicatief niveau wordt versleuteld (e.g. HTTPS/TLS), kan het voorkomen dat bijvoorbeeld legacy systemen geen of naar hedendaagse maatstaven te zwakke versleutelingsmechanismen ondersteunen. Door versleuteling toe te passen in de module Backbone wordt al het verkeer in de module Backbone versleuteld conform hedendaagse sterke versleutelingsmechanismen.
Eisen en beperkingen	Transportversleuteling moet op line-rate-niveau worden uitgevoerd, zodat geen performance-vermindering van data-overdracht in de module Backbone plaatsvindt. Er dienen encryptie-algoritmen te worden gebruikt die conform de hedendaagse informatiebeveiligingspraktijk als ‘proven’ en ‘sterk’ worden beschouwd. Teves dient de aansturing/monitoring/provisioning van de backbone middels een centrale beheertool/node versleuteld te worden uitgevoerd.
Functionele beschrijving patroon	In de onderstaande figuur is het TA-patroon conceptueel afgebeeld. 

4.3.1 Ontwerpregels

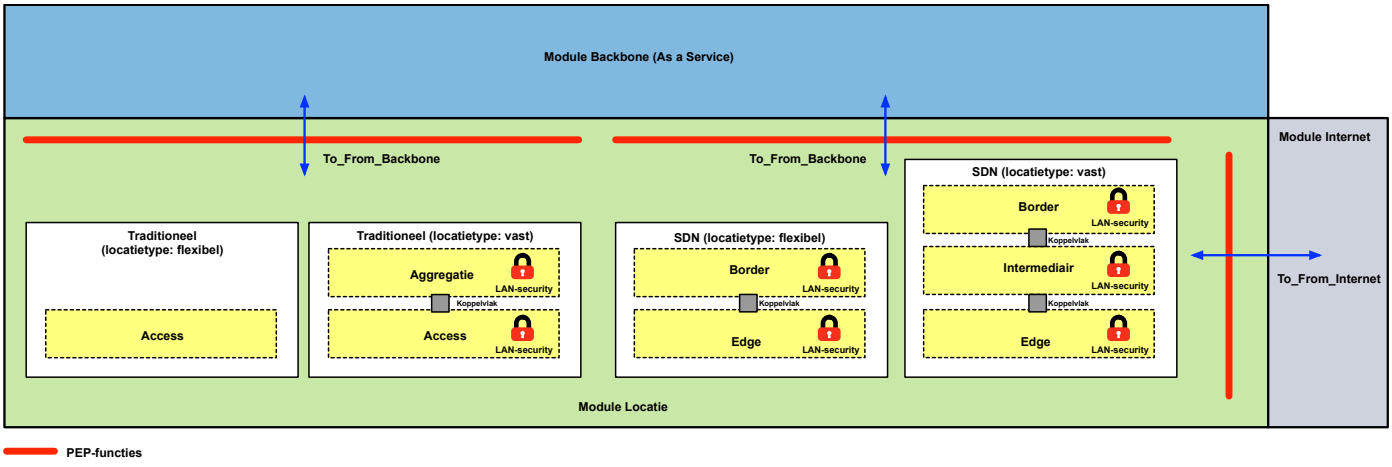
Ontwerpregel 2	**Versleuteling van data**
2.1	De module Backbone dient versleuteling van data-overdracht te ondersteunen middels encryptie-algoritmen die in de hedendaagse informatiebeveiligings-praktijk als ‘proven’ en ‘sterk’ worden beschouwd. De leverancier van de backbone dient hierbij voldoende te waarborgen, dat alleen het ROC netwerkverkeer kan ‘decrypten’.
2.2	Versleuteling van data mag geen nadelige impact hebben op de diensten die door de module Backbone worden getransporteerd.

4.4 Module Locatie - security

4.4.1 LAN-security

In de onderstaande illustratie is conceptueel afgebeeld op welke posities PEP-functies dienen te worden aangebracht in de module Locatie. Zoals in de paragrafen over zonering is aangegeven, dient inter-zoneringsverkeer middels PEP-functies te worden afgehandeld. Dit geldt dus ook voor de module Locatie, zodra verkeer tussen verschillende zones wordt afgehandeld. Voor meer informatie over zonering wordt verwezen naar de vorige paragrafen.

Voor het algehele overzicht is zowel het traditionele als het SDN-model afgebeeld voor de beide locatietypen flexibel en vast. Voor meer informatie over modules en locatietypen wordt verwezen naar het document Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0.



Figuur 4-3: *Overzicht PEP-posities module Locatie*

4.4.1.1 Ontwerpregels

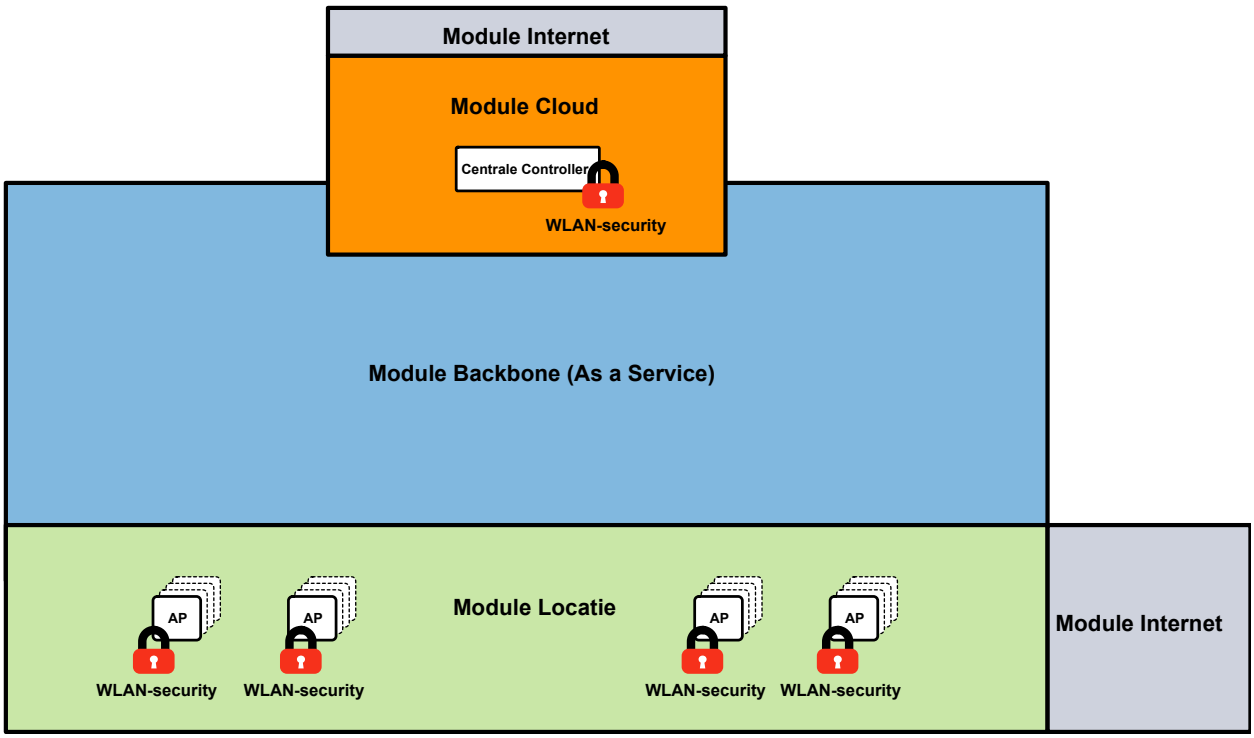
De onderstaande minimalistische set aan maatregelen dient te worden genomen in het kader van LAN-security. Van de markt wordt een advies verwacht welke (aanvullende) maatregelen genomen dienen te worden op grond van best practices en het marktsegment van het ROC (onderwijs/vergelijkbare omgevingen).

Ontwerpregel 3	LAN-security module Locatie
3.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
3.2	Overbodige services dienen te worden gedeactiveerd op de LAN-nodes.
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.

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.
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.
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.
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.
3.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
3.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
3.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
3.11	De nodes dienen het RADIUS-protocol te ondersteunen in het kader van toegangsbeveiliging middels de principes van IEEE 802.1x en MAB.
3.12	De nodes dienen IEEE 802.1x en MAB te ondersteunen.
3.13	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.
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).
3.15	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.

4.4.2 WLAN-security

Ook op het niveau van het WLAN dienen beveiligingsmaatregelen te worden genomen.



Figuur 4-4: *Overzicht posities WLAN-security*

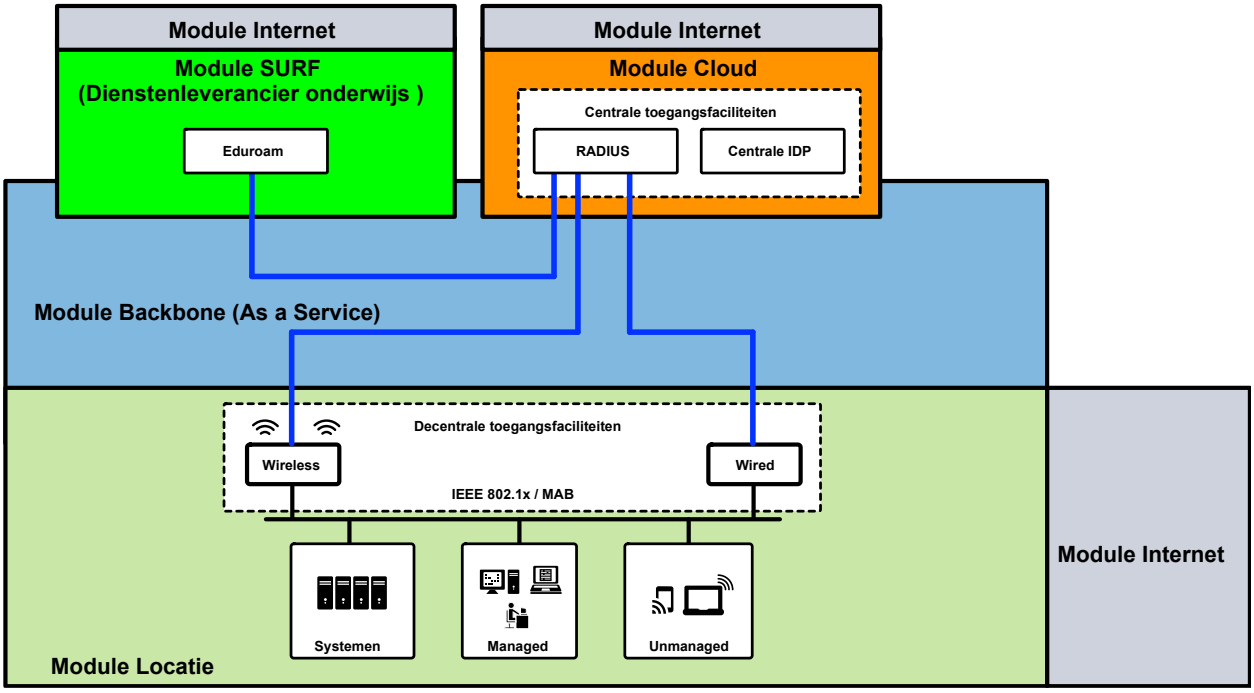
De exacte posities van PEP-functies zijn mede afhankelijk van de keuze van WLAN-architectuur (e.g. decentraal model, centraal model, SaaS-model et cetera). Het ROC vraagt de markt om advies op grond van de eisen die zijn gesteld in zowel deze blauwdruk als in het document 'Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0'. Derhalve zijn hieronder minimalistische ontwerpregels opgenomen waaraan de security van het WLAN dient te voldoen.

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.
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.
4.3	Access points dienen dermate te zijn opgesteld/gepositioneerd, dat deze niet binnen handbereik zijn of eigenmachtig gemaakt kunnen worden.

4.4	De WLC of gelijksoortige centrale draadloze functionaliteit dient verkeersscheiding te ondersteunen in het Distribution Systeem/ ICT-infrastructuur van het ROC.
4.5	Bij het inloggen in een access point of WLC middels de console dient een warning banner tevoorschijn te komen.
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.
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.
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.
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.
4.10	Het productieverkeer dient te zijn gescheiden van het managementverkeer.
4.11	Indien de centrale draadloze faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
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.

4.4.3 Toegangsbeveiliging LAN/WLAN

Het is voor het ROC van belang de gebruikers en systemen op een gecontroleerde en traceerbare wijze toegang te verlenen tot het draadloze & bedrade netwerk en daarmee tot de services/diensten die het ROC biedt. In de onderstaande illustratie zijn de principes van toegangscontrole conceptueel afgebeeld.



Figuur 4-5: *Overzicht toegangsverleningsdienst*

De toegangsverleningsdienst bestaat uit twee delen:

1. Centrale toegangsfaciliteiten (centrale RADIUS-omgeving + centrale IDP)
2. Decentrale toegangsfaciliteiten (bedrade en draadloze netwerk in de module Locatie).

Ad 1. Centrale toegangsfaciliteiten (centrale RADIUS-omgeving + centrale IDP)
Het ROC maakt gebruik van Eduroam voor het draadloze netwerk. In dit kader bezien kan worden gesteld, dat ook Eduroam deel uitmaakt van de centrale toegangsfaciliteiten.

TA-bouwblok: Centrale toegangsfaciliteiten	
(Beknopte) Conceptuele beschrijving van het bouwblok	Centrale toegangsfaciliteiten bestaan uit twee bestandsdelen: 1. Centrale RADIUS-faciliteiten, 2. Centrale IDP (database met identiteiten).

	Eduroam bestaat in dit kader alleen uit centrale RADIUS-faciliteiten die door SURF worden geboden. Het IDP-architectuurbouwblok is aanwezig binnen het ROC en binnen andere onderwijsinstellingen die gebruik maken van Eduraom. Let op: Centrale componenten die in de module Cloud zijn afgebeeld kunnen ook in het 'eigen/onprem' datacenter worden ondergebracht, indien hiertoe goede redenen bestaan. Met andere woorden: een invulling van het principe 'tenzij' (i.e. 'cloud, tenzij') wordt niet van tevoren uitgesloten!
Functies van het bouwblok	Het verlenen van: • Authenticatieservices (AuthC), • Autorisatieservices (AuthZ), • Auditingservices. Eduroam van SURF wordt hierbij alleen gebruikt als 'proxy-omgeving', waarbij RADIUS-verzoeken en RADIUS-antwoorden worden verstuurd tussen de RADIUS-proxy van het ROC en de RADIUS-omgeving van een andere onderwijsinstelling.

Services die het bouwblok biedt (aan de omgeving)	• Toegangsverleningsdienst voor:
	  ○ 'Managed gebruikers' binnen het ROC,
	  ○ 'Managed computers' binnen het ROC (met referte aan ontwerpegel 5.4 (advies wordt gevraagd aan de markt),
	  ○ 'Managed systemen' binnen het ROC,
	  ○ BYOD,
	  ○ Gastgebruik.

Kwaliteitskenmerken	• De oplossing dient geen SPOF te vormen in de AAA-architectuur.
	• De oplossing dient AAA-functies te kunnen uitoefenen voor zowel het bedrade als draadloze netwerk.
	• Uit het oogpunt van afscherming dient de RADIUS-server van Eduroam te worden benaderd middels een RADIUS-proxy. Dit zorgt ervoor, dat de RADIUS-omgeving van het ROC zelf niet in directe verbinding staat met Eduroam.
	• De omgeving moet gedimensioneerd zijn op het aantal concurrent sessies m.b.t. de aantallen gebruikers, computers en systemen dat gebruikmaakt van de NAC-oplossing. Het ROC gaat hierbij uit van de volgende berekening:
	  ○ 75% van de gebruikers = concurrent
	  ○ 75% van alle gebruikers = 12.0000
	  ○ Iedere gebruiker heeft 2 devices tot zijn/haar beschikking = 24.000 RADIUS-sessies
	  ○ Ieder gebruiker wordt ook 'voorzien' van een RADIUS-sessie = 12.000.

	○ Totaal: Minimaal 36.000 RADIUS-sessies. ○ Let op: Hierin zijn niet de getallen verdisconteerd van IoT (zie paragraaf 4.7). Het ROC vraagt de markt om advies t.a.v. het totale aantal concurrent sessies dat ondersteund dient te worden op het niveau van NAC en op basis daarvan een voorstel uit te werken voor de NAC-oplossing. Het ROC gaat hierbij uit van de informatie in deze blauwdruk en de kennis/ervaring van de markt in een gelijksoortige omgeving als die van het ROC). • Ondersteuning van een beschikbaarheid van 99,99% in de keten (definitieve vaststelling in overleg met de markt -> haalbaarheid + betaalbaarheid).

TA-bouwblok: Decentrale toegangsfaciliteiten	
(Beknopte) Conceptuele beschrijving van het bouwblok	Decentrale toegangsfaciliteiten bestaan uit twee bestandsdelen: 1. Bedrade toegangsfaciliteiten, 2. Draadloze toegangsfaciliteiten.
Functies van het bouwblok	Het op een veilige en zorgvuldige wijze voorzien in toegangsverlening tot zowel het bedrade als het draadloze netwerk van het ROC voor gebruikers, computers en systemen.
Services die het bouwblok biedt (aan de omgeving)	• Bedrade en draadloze toegangsverleningsdienst voor: ○ 'Managed gebruikers' binnen het ROC, ○ 'Managed computers' binnen het ROC, ○ 'Managed systemen' binnen het ROC, ○ BYOD, ○ Gastgebruik.
Kwaliteitskenmerken	• Uit het oogpunt van beschikbaarheid dient de oplossing te voorzien in twee RADIUS-sessies: ○ Eén naar RADIUS-server 01, ○ Eén naar RADIUS-server 02. • De oplossing dient zowel IEEE 802.1x als MAB te ondersteunen.

4.4.3.1 Ontwerpregels

Ontwerpregel 5	**Toegansverleningsdienst**
5.1	Toegang tot het bedrade en draadloze netwerk van het ROC dient middels een toegangsverleningsdienst te worden gereguleerd.
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.

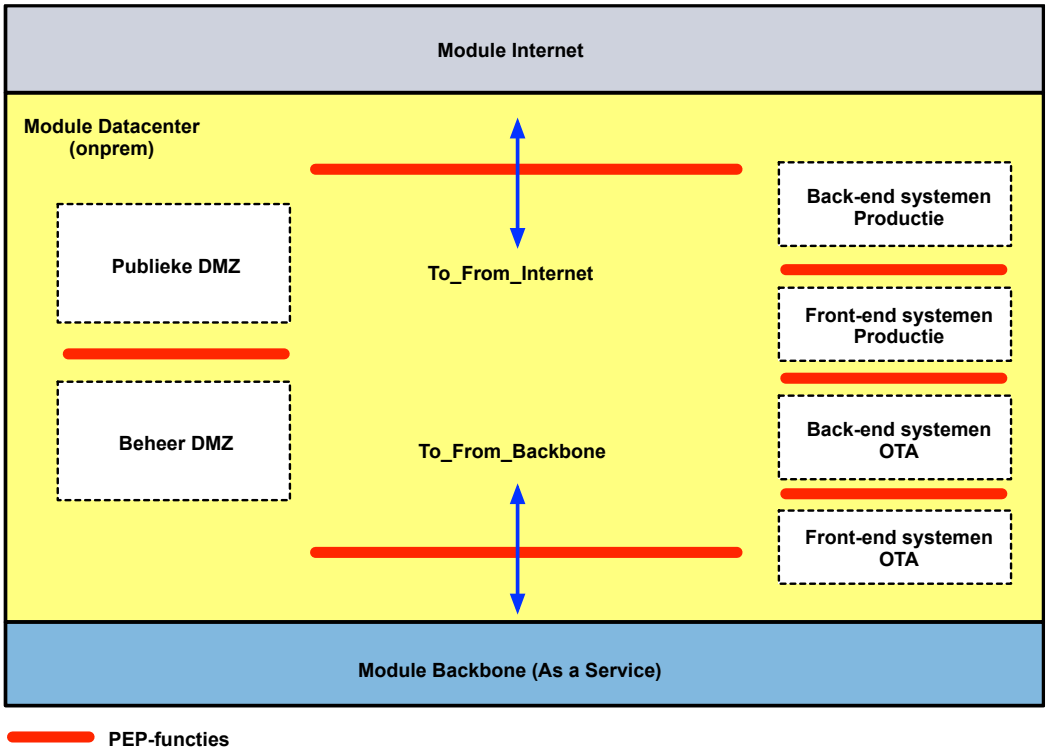
	Indien deze als clouddienst worden afgenomen, dient de IDP van het ROC te worden gebruikt.
5.3	Managed gebruikers van het ROC dienen middels user credentials te kunnen inloggen op het netwerk. Dit op basis van het IEEE 802.1x protocol.
5.4	Managed computers (CYOD) zijn niet meer AD-joined, maar AAD-joined. 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.
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 mee-gestuurd bij het authenticatieverzoek.
5.6	Na authenticatie dienen managed gebruikers/computers automatisch te worden ondergebracht in een zone.
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.
5.8	Foutief inloggen leidt ertoe, dat geen gebruikgemaakt kan worden van het netwerk van het ROC (zowel bedraad als draadloos).
5.9	Indien de centrale RADIUS-faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
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.
5.11	Gasten van het ROC dienen in een zone te worden opgenomen waarmee alleen internet als dienst kan worden benaderd.
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.
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.
5.14	De oplossing dient te kunnen communiceren met een IDP-omgeving van het ROC voor authenticatiedoeleinden voor studenten/medewerkers van het ROC.
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.
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).
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.
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.
5.19	Het is aan de markt te adviseren of de centrale oplossing als appliance, virtual machine of als SaaS-dienst wordt ingezet.

4.5 Module Datacenter onprem – security

4.5.1 PEP-functies

In de onderstaande illustratie is conceptueel afgebeeld op welke posities PEP-functies dienen te worden aangebracht. Zoals in de paragrafen over zonering is aangegeven, dient inter-zoneringsverkeer middels PEP-functies te worden afgehandeld. In deze paragraaf wordt verder niet ingegaan op zonering, maar op de scheiding van functionele bouwblokken binnen het Datacenter (onprem) en t.o.v. aangrenzende modules. Voor meer informatie over de netwerklagen (ABBs) binnen deze module wordt verwezen naar het document Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0.



Figuur 4-6: *Overzicht PEP-functies module Datacenter (onprem)*

Op hoofdlijnen bestaat het Datacenter (onprem) uit de volgende functionele onderdelen[5]:

- 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, DNS-servers, DHCP-servers e.d.

[5] *Hoewel het ROC een 'cloud, tenzij' strategie nastreeft, kan het voorkomen dat (in de tussenliggende tijd) alsnog het onprem datacenter wordt gebruikt voor verschillende functies. Derhalve is het van belang te duiden op welke manier deze functies vanuit IB-perspectief moeten worden ingebed in dit type datacenter.*

- 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.

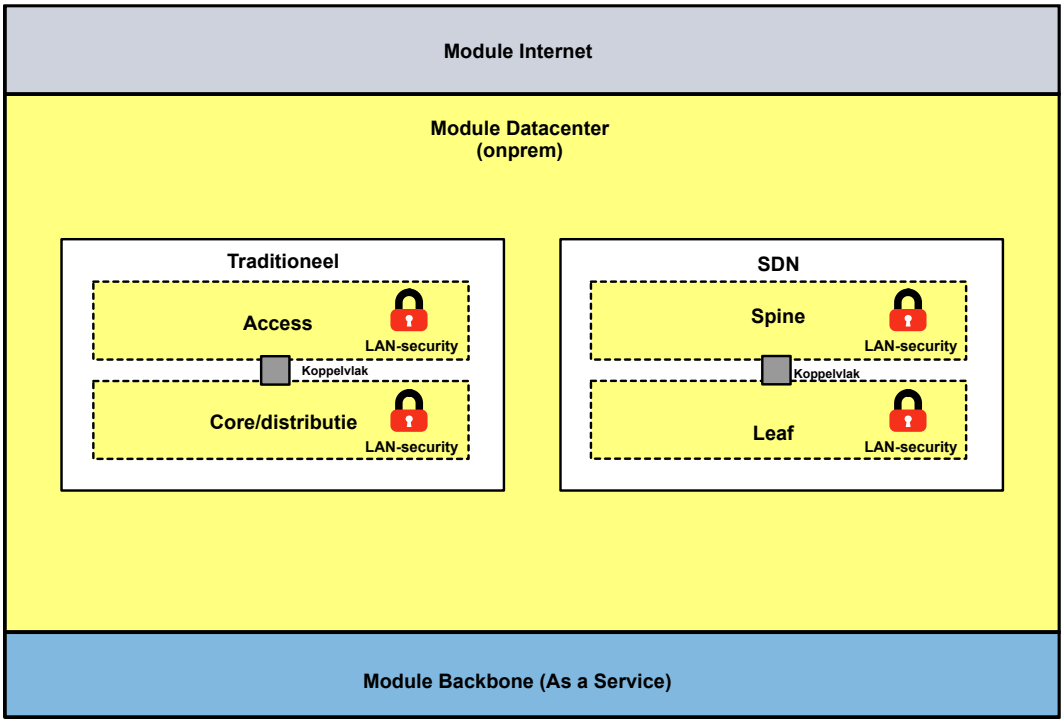
Tussen deze functionele onderdelen dient een 'harde scheidslijn' te bestaan. Met andere woorden: door middel van PEP-functies dienen deze functionele onderdelen van elkaar gescheiden te zijn. Ook binnen deze functionele onderdelen zal op grond van de dataclassificaties scheiding zijn aangebracht middels zonering, waarbij (zoals gezegd) ook PEP-functies gebruikt worden. Voor meer informatie hierover wordt verwezen naar de paragrafen die handelen over zonering.

4.5.1.1 Ontwerpregels

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.
6.2	De randen van het Datacenter (onprem) dienen te zijn afgeschermd van de modules Internet en Backbone middels 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).

4.5.2 LAN-security

LAN-security bestaat uit het nemen van IB-maatregelen op het niveau van de verschillende OSI-lagen. In de onderstaande illustratie is het DC-LAN binnen de module Datacenter (onprem) conceptueel afgebeeld. In het document Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0 is aangegeven, waarom twee verschillende LAN-topologieën zijn beschreven. Voor meer informatie wordt derhalve verwezen naar dit document.



Figuur 4-7: *LAN security traditioneel en SDN-model*

4.5.2.1 Ontwerpregels

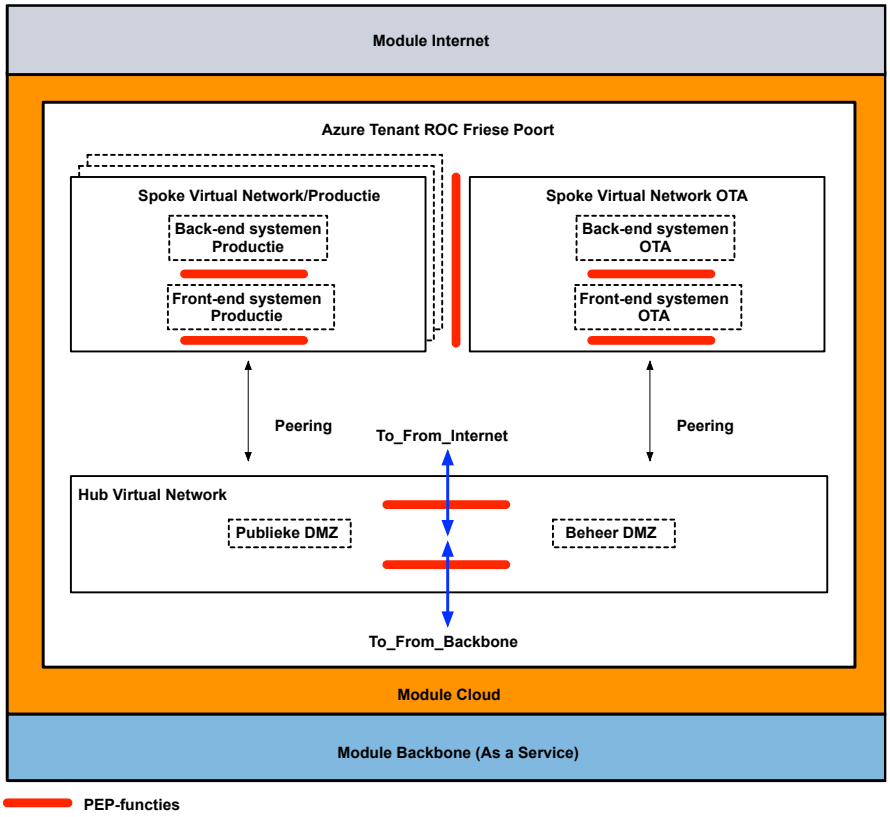
De onderstaande minimalistische set aan maatregelen dient te worden genomen in het kader van LAN-security. Van de markt wordt een advies verwacht welke (aanvullende) maatregelen genomen dienen te worden op grond van best practices en het marktsegment van het ROC (onderwijs/vergelijkbare omgevingen).

Ontwerpregel 7	LAN-security Datacenter (onprem)
7.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
7.2	Overbodige services dienen te worden gedeactiveerd.
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.

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.
7.5	Nodes die deel uitmaken van het DC-LAN dienen zonering te ondersteunen. Hierbij dienen de nodes verkeersscheiding op logisch niveau te ondersteunen.
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.
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.
7.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
7.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
7.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
7.11	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.
7.12	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.

4.6 Azure - security

De infrastructuur van Azure is gebaseerd op een hub-and-spoke-topologie zoals in de onderstaande illustratie is afgebeeld. Voor meer informatie wordt verwezen naar het document Techniek Architectuurblauwdruk architectuurgebied Netwerk v1.0. Van belang is te vermelden, dat ook deze infrastructuur voorzien dient te worden van PEP-functies. De betreffende posities zijn ook in de illustratie afgebeeld.



Figuur 4-8: *Overzicht PEP-functies module Cloud (Azure)*

Tevens is van belang te vermelden, dat IB-maatregelen op het niveau van het LAN niet dezelfde zijn als die binnen de module Datacenter (onprem). Dit heeft te maken met het feit, dat de onderliggende ICT-infrastructuur van Azure in beheer is bij Microsoft en niet bij het ROC. Dit op grond van de principes van 'de clouddatacenter'[6]. Dit laat onverlet, dat op het niveau van het LAN binnen Azure wel degelijk een substantieel aantal PEP-functies kunnen worden aangebracht die de doelstellingen van het ROC op het gebied van IB verwezenlijken.

[6] *Voor meer informatie wordt verwezen naar https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ voor de verschillen tussen onprem, Iaas, PaaS, SaaS*

Ook dit datacenter bestaat op hoofdlijnen uit de volgende 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 shared systemen zoals DNS, NTP e.d. en voor managementsystemen, tooling.
- 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.

Van belang is te vermelden, dat de zoneringsprincipes en scheidingen van functionele onderdelen die zijn beschreven bij de module Datacenter (onprem) ook gelden voor Azure (en clouddatacenters in het algemeen). Tevens moet op deze plaats worden aangegeven, dat de hub-and-spoke-topologie van Azure in de praktijk nog verder moet worden vormgegeven. Te denken valt bijvoorbeeld aan de hoeveelheid spokes, waarin verschillende afdelingen resources kunnen onderbrengen. Dit laat onverlet, dat de infrastructuur gebaseerd blijft op het hub-and-spoke-paradigma met navenante PEP-functies.

De onderstaande minimalistische set aan maatregelen dient te worden genomen in het kader van de hub-and-spoke-topologie van Azure. Van de markt wordt een advies verwacht welke (aanvullende) maatregelen genomen dienen te worden op grond van best practices en het marktsegment van het ROC (onderwijs/vergelijkbare omgevingen).

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.
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.
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.
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.
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.
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.

4.7 Internet of Things (IoT)

Er vindt een grote technologische verschuiving plaats in de wereld die is gecentreerd rond het begrip IoT ofwel Internet of Things. Bij IoT draait alles om het verbinden van objecten die nog niet zijn verbonden aan een netwerk en/of het internet. De meeste objecten in onze huidige wereld zijn niet verbonden met een computernetwerk, maar dit paradigma verandert snel. Eerder niet verbonden objecten die overal om ons heen zijn krijgen de mogelijkheid om te communiceren met andere objecten en mensen, wat op zijn beurt nieuwe diensten en efficiëntie in ons dagelijks leven stimuleert. Dit is het uitgangspunt achter de principes van IoT en het illustreert waarom sommigen theoretiseren dat de uitwerking van IoT net zulke grote veranderingen zal teweegbrengen als de industriële revolutie.

Ook binnen het ROC is deze trend ook volop aanwezig. Er zijn hierbij twee invalshoeken van IoT te onderscheiden:

1. IOT voor productiedoeleinden
2. IOT voor educatieve doeleinden.

Ad 1. IOT voor productiedoeleinden
Binnen het ROC zijn reeds IoT-devices aanwezig die aan een netwerk zijn verbonden. Deze IoT devices zijn bijvoorbeeld IP-camera's en gebouwenbeheersystemen. Op het moment van schrijven d.d. september 2020 zijn deze IoT-devices verbonden door een logisch gescheiden netwerk. Naar de toekomst toe zullen steeds meer toepassingen (e.g. sensors) worden aangebracht voor verschillende doeleinden (e.g. achterhalen bezettingsgraden klaslokalen, temperatuur-, luchtvochtigheidsregulators, andere 'smart city' IOT-objecten binnen de kaders en doelstellingen van het ROC).

Ad 2. IOT voor educatieve doeleinden
Verschillende toepassingsgebieden van IoT maken deel uit van de opleidingen ICT en Techniek. Denk hierbij aan educatieve leerdoeleinden m.b.t. VR/AR-devices, drones, domotica, PLCs, 3D-printers en robots.

In het kader van de voornoemde invalshoeken is het ook steeds belangrijker te beschikken over een platform waarmee:

- Big Data/configuraties centraal kunnen worden opgeslagen,
- Trends en analyses kunnen worden achterhaald/uitgevoerd,
- Machine Learning/Deep Learning mee kan worden uitgevoerd,
- Et cetera.

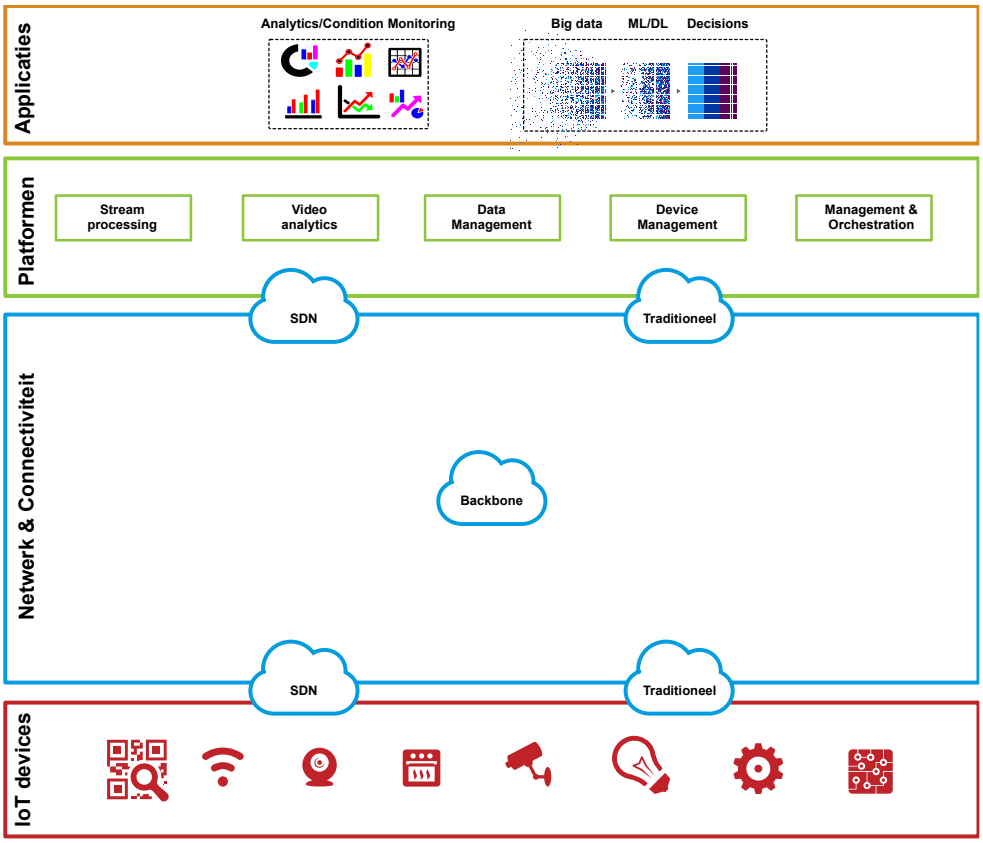
In het kader van deze blauwdruk wordt niet direct ingegaan op vraagstukken die te maken hebben met voornoemde punten. De ICT-infrastructuur van het ROC dient echter wel faciliterend te zijn om voornoemde punten mogelijk te maken.

4.7.1 IoT-model ROC

Hoewel in de literatuur verschillende theoretische IoT-frameworks[7] bestaan, kiest het ROC voor een praktische opzet van IoT binnen haar omgeving. Op de keper beschouwd komt het onderstaande framework overeen met andere theoretische modellen. Uiteindelijk gaat het om de 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.

In de onderstaande illustratie is dit concept afgebeeld.

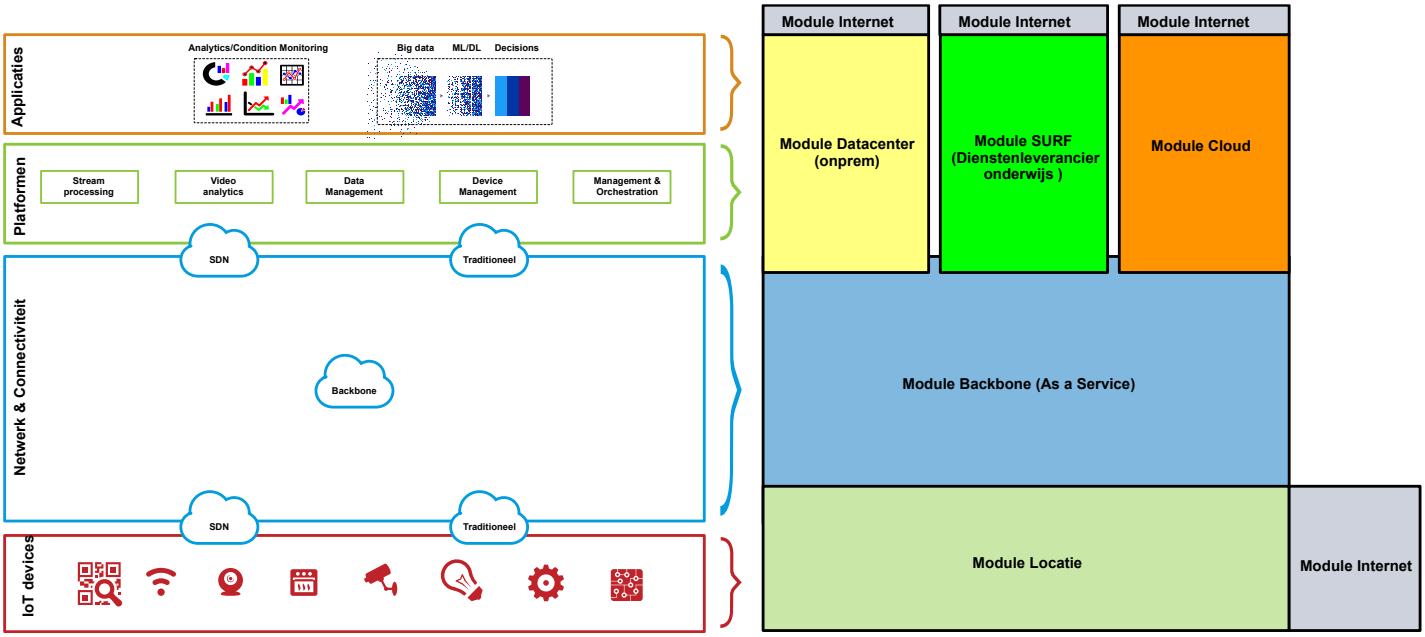


Figuur 4-9: *Overzicht IoT-omgeving ROC*

De verschillende afgebeelde IoT-devices, platformen en applicaties hebben niet als doel absoluut te zijn. Uiteindelijk gaat in het in dezen om de concepten en architectuurbouwblokken die zich in de verschillende lagen bevinden. In het kader van deze blauwdruk gaat het specifiek om het plotten van de

[7] *https://www.onem2m.org/tr-0037/architecture https://www.iotwf.com/resources*

geschetste lagen binnen c.q. in relatie tot de modules waaruit de ICT-infrastructuur van het ROC is opgebouwd. Dit is in de onderstaande illustratie conceptueel afgebeeld.



Figuur 4-10: *Overzicht IoT-lagen in relatie tot de modulaire opbouw van de ICT-infrastructuur*

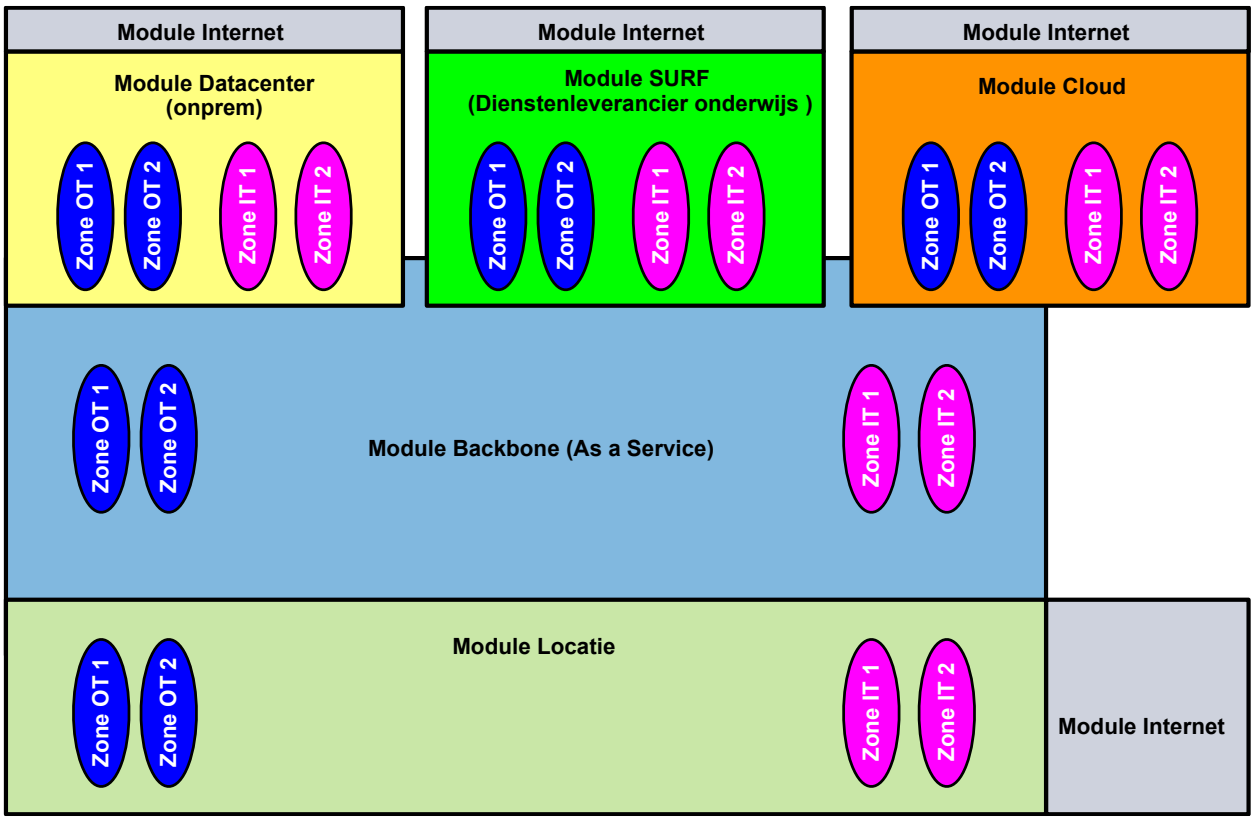
IoT-laag	Relatie met Module/raakvlak
IoT-devices	Module Locatie/ontsluiting door bedraad en draadloos netwerk.
Netwerk & Connectiviteit	Module Locatie/transport van data. Module Backbone/transport van data. Module Internet/transport van data. Module Datacenter ‘onprem’/transport van data. Module SURF/transport van data. Module Cloud/transport van data.
Platformen	Module Cloud/verschillende platformen binnen deze module. Module Datacenter ‘onprem’/eventuele platformen binnen deze module. Module SURF/eventuele platformen binnen deze module.
Applicaties	Module Cloud/verschillende applicaties binnen deze module. Module Datacenter ‘onprem’/eventuele applicaties binnen deze module. Module SURF/eventuele applicaties binnen deze module.

4.7.1.1 Ontwerpregels

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.
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.
9.3	Ontsluiting van IoT-devices dient te zijn gebaseerd op het IP-protocol, waarbij zowel IPv4 als IPv6 ondersteund dienen te worden
9.4	Ontsluiting van IoT-devices dient zowel bedraad als draadloos te kunnen worden uitgevoerd.

4.7.2 Scheiding van en communicatie tussen IT/OT

In de doelsituatie, zoals het ROC deze voor ogen, heeft dient te allen tijde een scheiding te zijn aangebracht tussen IoT-devices (OT) en IT-devices (IT). Dit is in de onderstaande illustratie conceptueel afgebeeld.



Figuur 4-11: *Scheiding IT/OT-omgevingen ROC*

4.7.2.1 Ontwerpregels

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.
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.

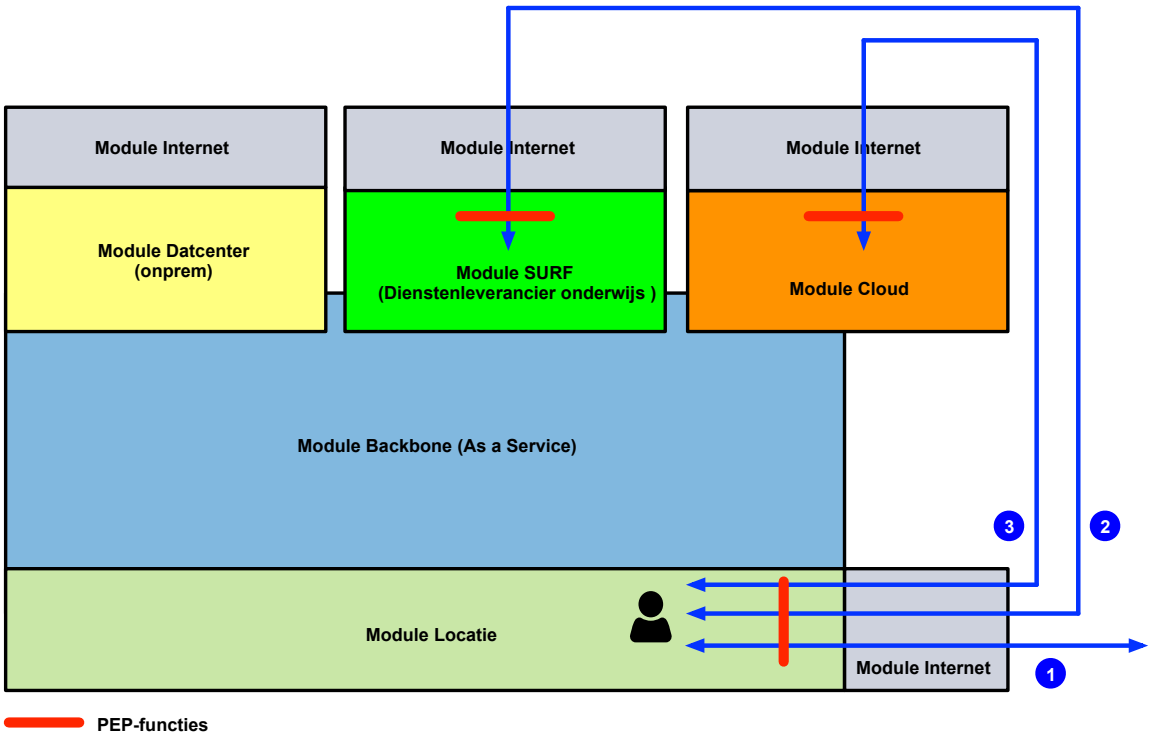
Ontwerpregel 11	Communicatie IT/OT
11.1	Indien tussen IT- en OT-devices (IoT) communicatie nodig is, geschiedt dit middels PEP-functies zoals deze aangebracht dienen te zijn voor inter-

	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. Tevens kan het mogelijk zijn dat 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.

4.8 Use cases/communicatiestromen

4.8.1 Benaderen internet & cloud/SURF-diensten via internet vanaf de module Locatie

Use case 1: Internet browsen en het benaderen van clouddiensten/SURF via internet vanaf de module Locatie



Nr. 1: Internetbrowsen
Gebruikers benaderen het internet middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van internetverkeer naar de centrale onprem datacenters te voorkomen.

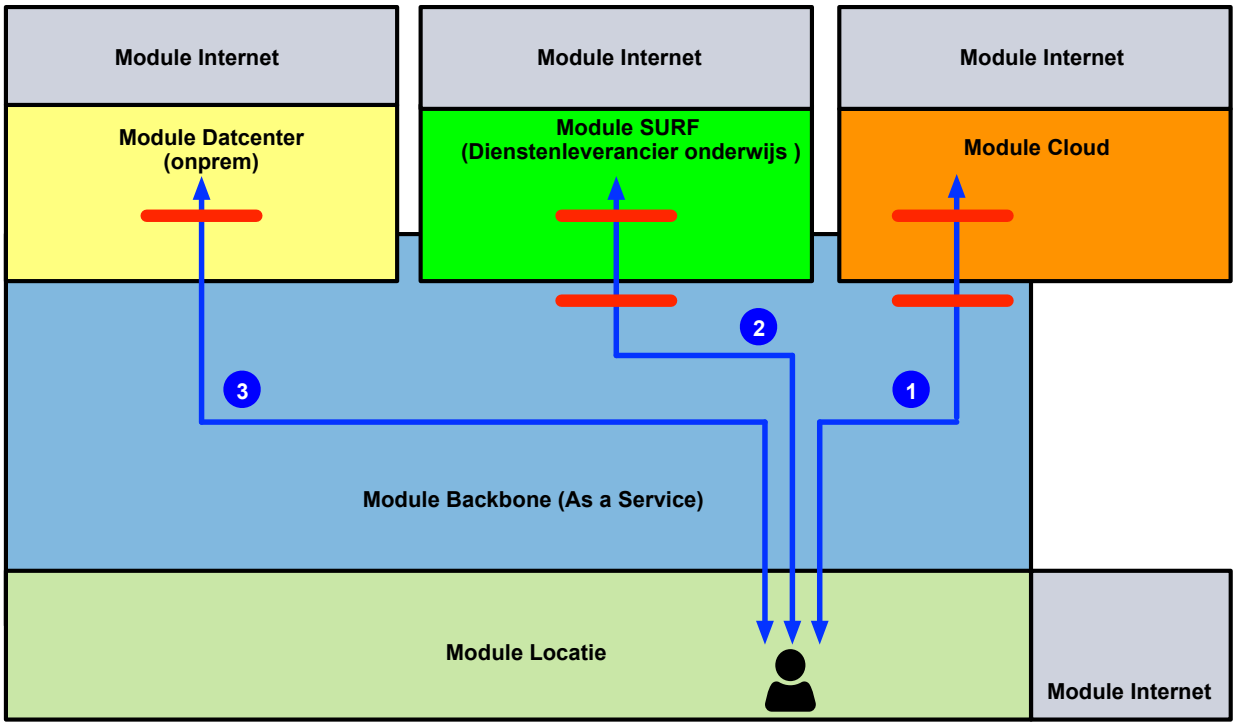
Nr. 2: Diensten SURF aangeboden via internet
Gebruikers benaderen diensten van SURF middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van SURF naar de centrale onprem datacenters te voorkomen.

Nr. 3: SaaS-diensten aangeboden via internet
Gebruikers benaderen SaaS-diensten middels een local internet breakout op het niveau van de module Backbone. Dit om backhauling van SaaS-verkeer naar de centrale onprem datacenters te voorkomen.

PEP-functies dienen te worden toegepast in de modules Backbone (ontsluiting module Locatie), Cloud en SURF. In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.2 Benaderen onprem-diensten, cloud/SURF-diensten direct via de module Backbone

Use case 2: Benaderen onprem-diensten, cloud/SURF-diensten via de module Backbone



Nr. 1: Module Cloud

Gebruikers benaderen diensten in het clouddatacenter middels de module backbone. Het clouddatacenter is hierbij direct op de module Backbone aangesloten. SaaS/PaaS-diensten kunnen hierbij ook direct op de module Backbone aangesloten.

Nr. 2: Diensten SURF

Gebruikers benaderen SURF-diensten direct via de module Backbone. Hierbij is SURF direct op de module Backbone aangesloten.

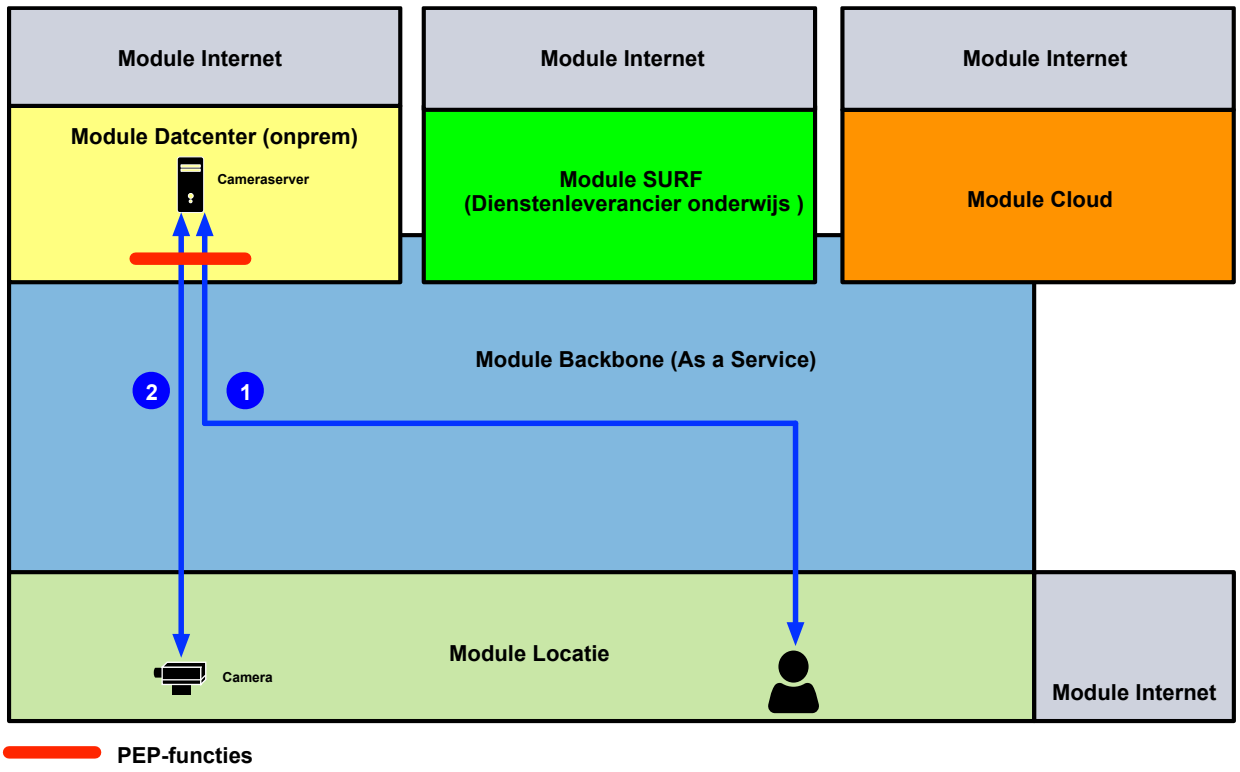
Nr. 3: Diensten onprem-DC

Gebruikers benaderen diensten in het onprem-DC direct via de module Backbone. De module Datacenter (onprem) is direct op de module Backbone aangesloten.

PEP-functies dienen te worden toegepast in de modules Cloud, SURF, Backbone en Datacenter (onprem). In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.3 Opvragen/inzien camerabeelden

Use case 3: Opvragen/inzien camerabeelden



Nr. 1: Camerabeelden

- Een facilitair beheerder bekijkt de live camerabeelden c.q. vraagt oude camerabeelden op vanaf de cameraserver. Dit kan ook de beveiligings-coördinator zijn van de vestiging. Er is geen directe toegang tot de camera's nodig. De gebruikte software heeft alleen toegang tot de cameraserver.
- Een student zit op een centrale locatie en houdt onder toezicht alle camera's van het ROC in de gaten.
- Camera's worden gebruikt in lessituatie, waarbij beelden voor lesdoeleinden gebruikt worden. Hierbij is slechts een klein aantal van de camera's beschikbaar.

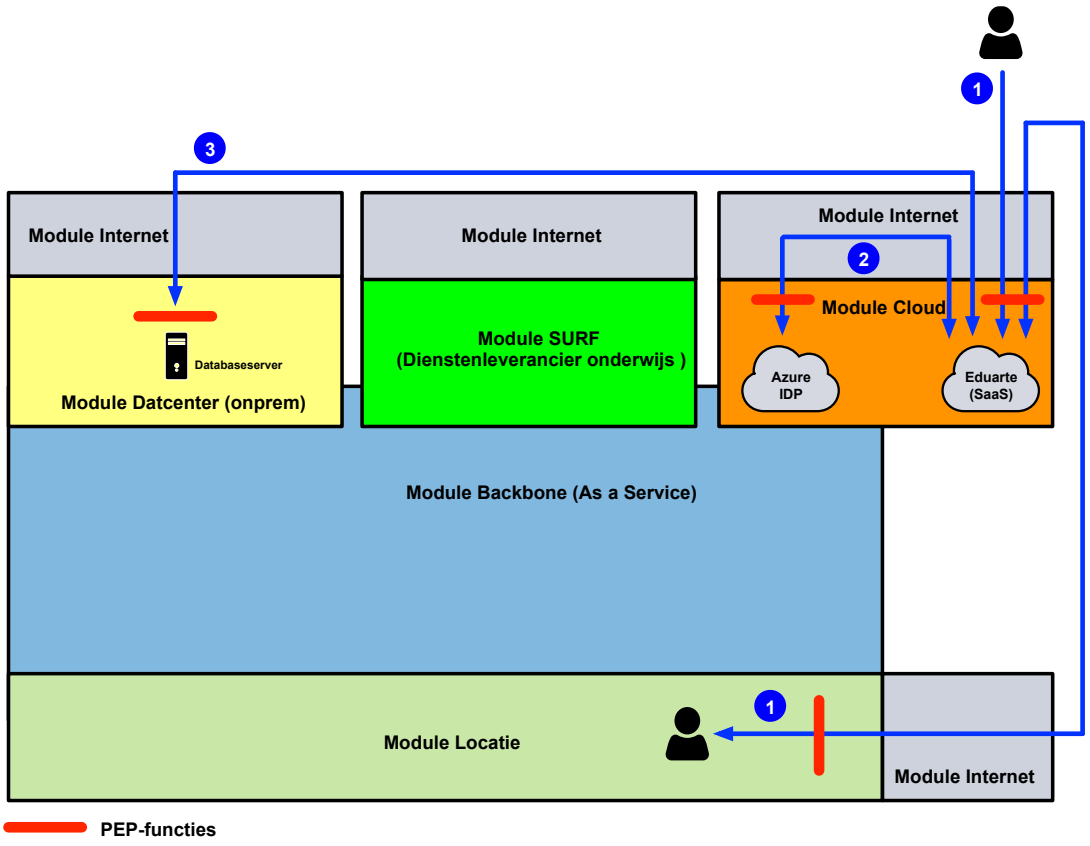
Nr. 2: Machine-to-machine-communicatie

Communicatie tussen de camera's en de cameraserver wordt door de module Backbone afgehandeld.

PEP-functies dienen te worden toegepast in de module Datacenter (onprem). In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.4 Gebruik Eduarte

Use case 4: Gebruik Eduarte



Nr. 1: Benaderen Eduarte

- Gebruikers binnen de module Locatie benaderen Eduarte middels de local internet breakout die door de module Backbone wordt gefaciliteerd.
- Gebruikers buiten de module Locatie banderen Eduarte middels de ‘eigen’ internetverbinding.

Nr. 2: Authenticatieverkeer

Alvorens toegang te krijgen tot Eduarte dienen authenticaties te worden afgehandeld via de IDP van Azure. Hierbij wordt voor communicatiedoeleinden gebruikgemaakt van de module Internet.

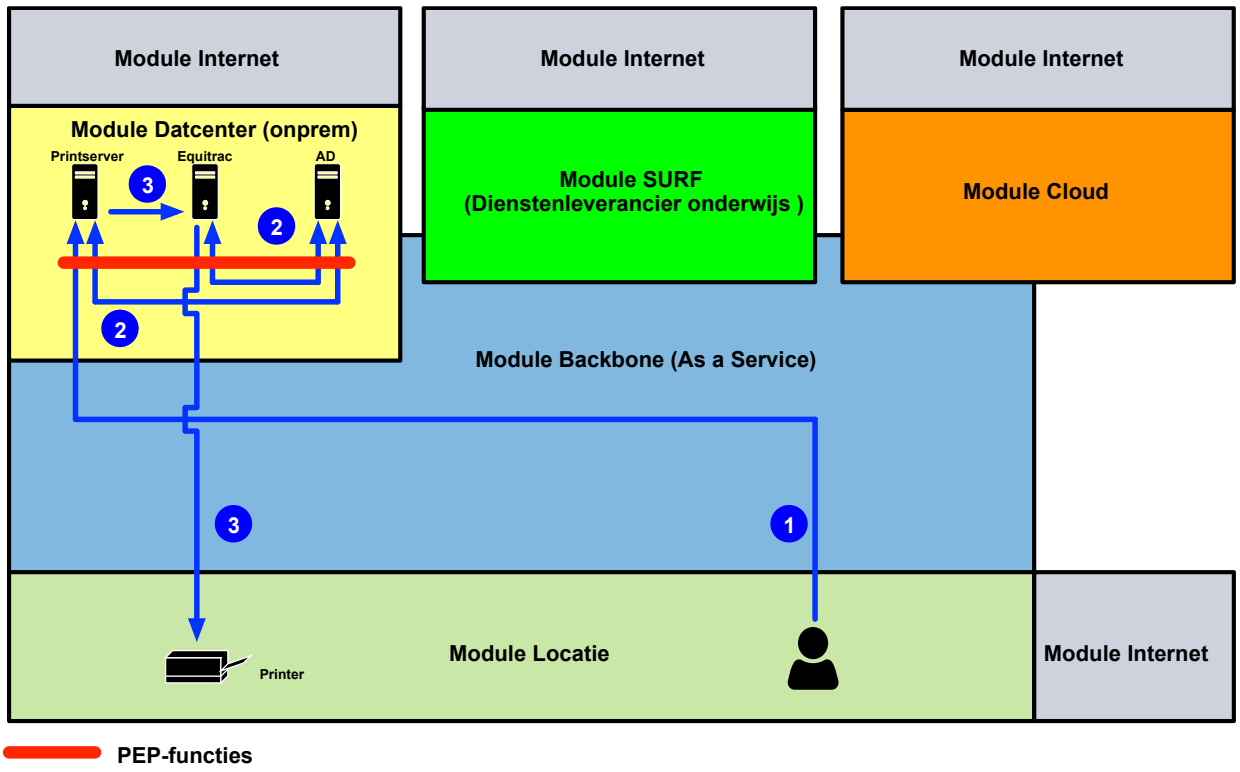
Nr. 3: Replicatieverkeer

Replicatieverkeer in het kader van Eduarte wordt gefaciliteerd door de module Internet, waardoor communicatie mogelijk is tussen Eduarte en de database-server in het onprem datacenter.

PEP-functies dienen te worden toegepast in de modules Locatie, Cloud en Datacenter (onprem). In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.5 Printen

Use case 5: Printen



Nr. 1: Aanvraag printopdracht

Gebruikers in de module Locatie geven een printopdracht waarbij de verkeersstroom door de module Backbone wordt afgehandeld.

Nr. 2: Authenticatieverkeer

- Authenticatie van de printopdracht dient te worden doorgevoerd op het niveau van de AD in het onprem-DC.
- Authenticatie van de Equitrac-server zelf dient op het niveau van de AD in het onprem-DC te worden doorgevoerd.

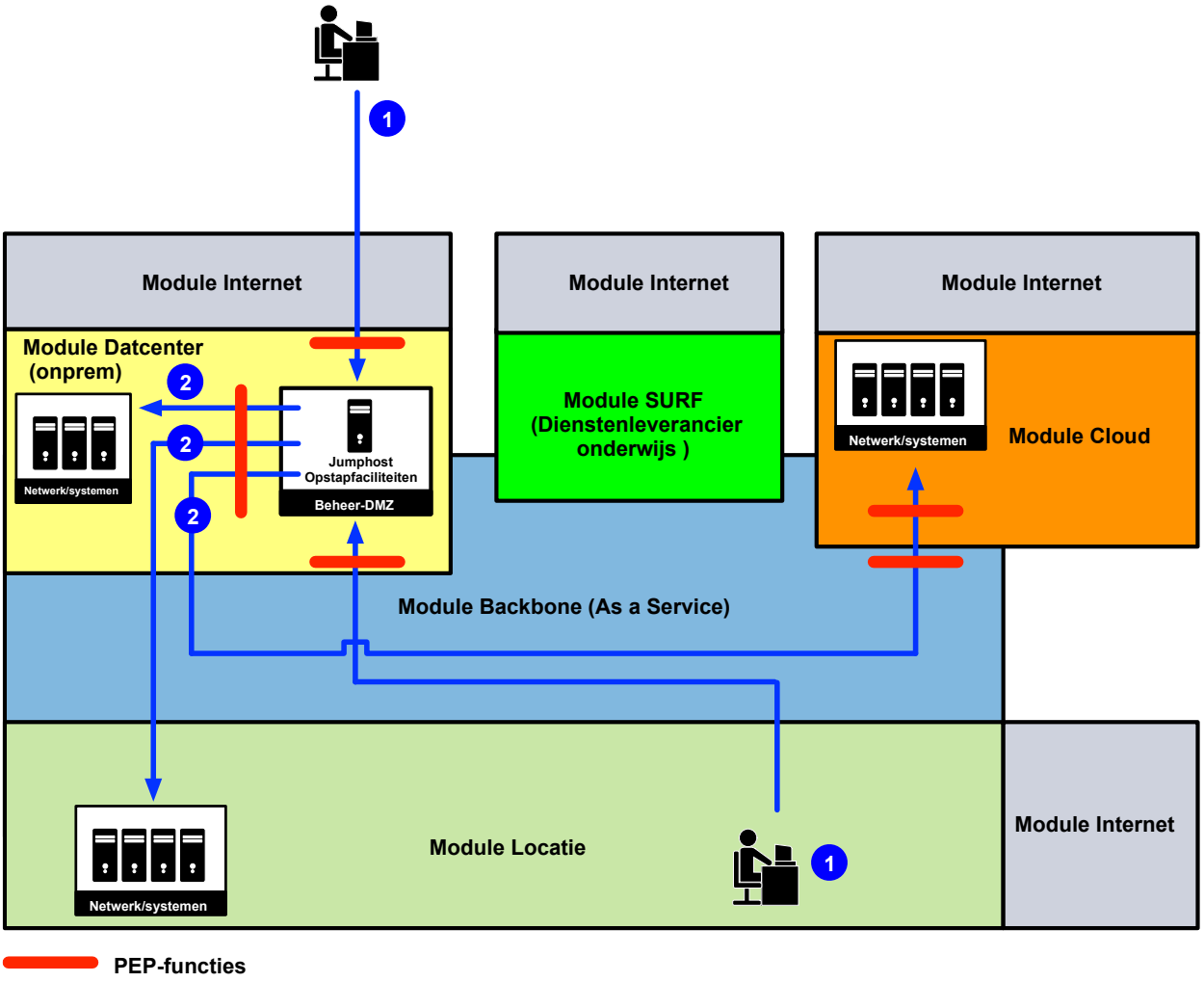
Nr. 3 Uitvoering printopdracht

Na authenticaties dient de verkeerstroom m.b.t. de printopdracht door de module Backbone te worden afgehandeld.

PEP-functies dienen te worden toegepast ibinnen de module Datacenter (onprem). In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.6 Beheer/management

Use case 6-1: Beheer/management – Beheerfaciliteiten module Datacenter (onprem scenario)



Nr. 1: Benadering managementsystemen

Beheerders benaderen opstapfaciliteiten/jumphost die zich in het functionele domein Beheer DMZ-bevinden binnen het Datacenter (onprem). Beheerders kunnen zich zowel buiten het ROC (via het internet) als binnen het ROC (module Locatie) bevinden. Hierbij dient gebruikgemaakt te worden van 2FA.

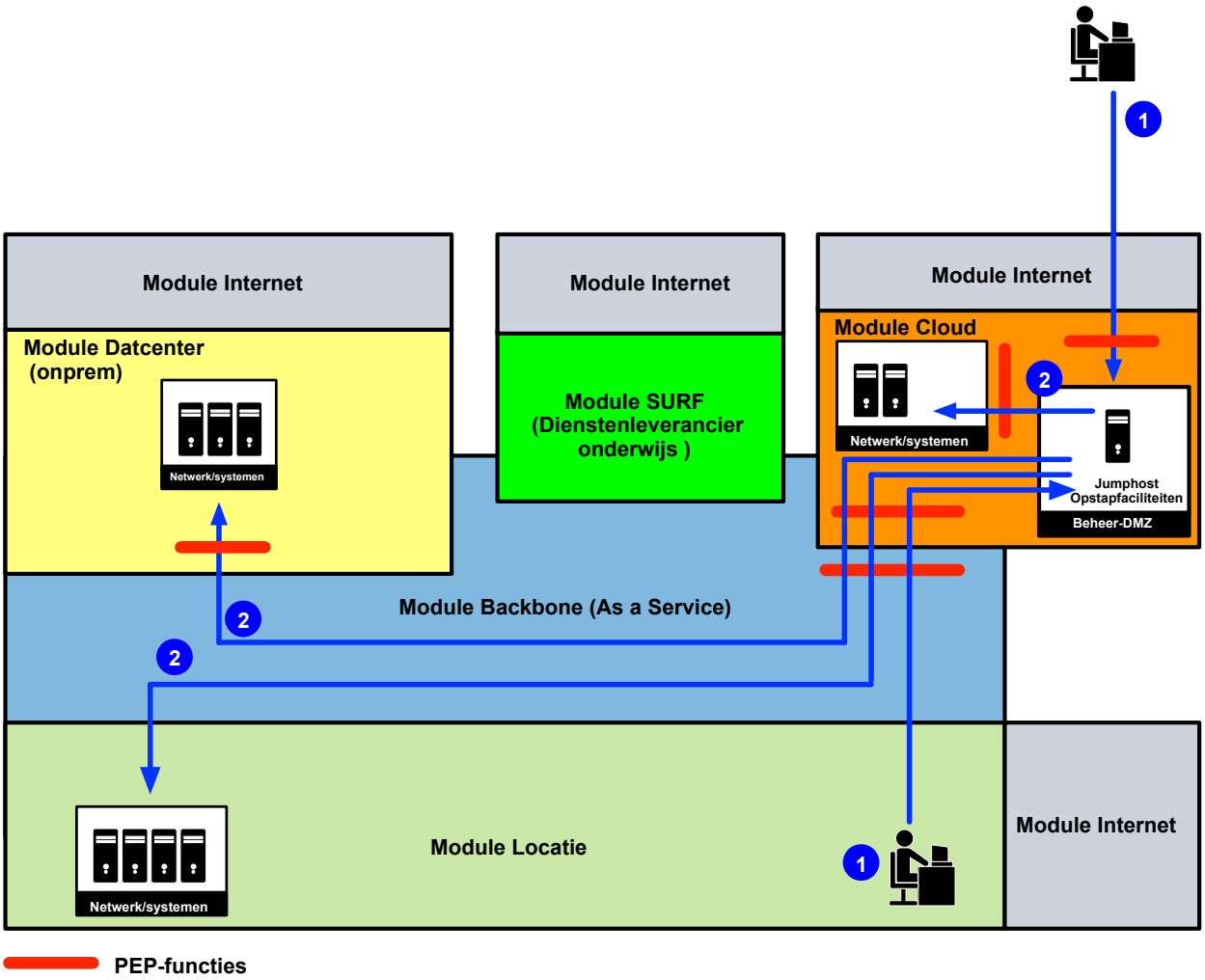
Nr. 2: Beheren van netwerksystemen

Vanuit de Beheer-DMZ worden middels de aangewezen tooling/beheerapplicaties/portals de betreffende netwerksystemen benaderd. Alvorens te kunnen inloggen op deze systemen wordt middels het TACACS-protocol geverifieerd of een beheerder rechten heeft om het device te beheren en zo ja, welk autorisatie-niveau daarbij hoort. Na vaststelling van de identiteit en het autorisatieniveau kunnen de betreffende nodes worden beheerd. Let op: Binnen Azure betreft dit nodes van vendoren die appliances bieden via

bijvoorbeeld de marktplaats. Cloud native nodes worden in de regel middels de azure-portal beheerd.

PEP-functies dienen te worden toegepast in de modules Datacenter (onprem), Cloud en Backbone. In de module SURF worden geen netwerknodes (virtual appliances) ondergebracht, zodat geen communicatie-stromen richting deze module zijn opgenomen. In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

Use case 6-2: Beheer/management – Beheerfaciliteiten Cloud (Azure scenario)



Nr. 1: Benadering managementsystemen

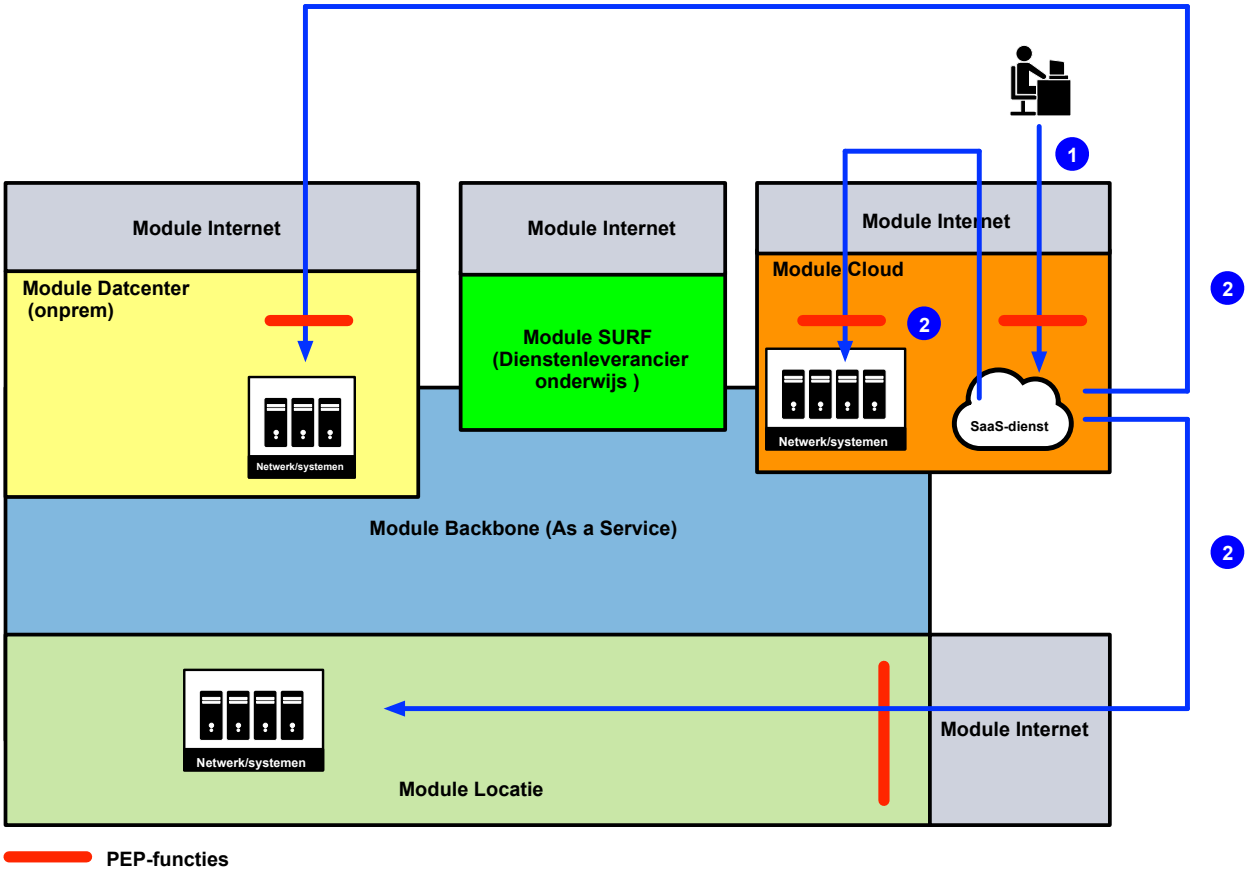
Beheerders benaderen opstapfaciliteiten/jumphost die zich in het functionele domein Beheer DMZ-bevinden binnen Azure. Beheerders kunnen zich zowel buiten het ROC (via het internet) als binnen het ROC (module Locatie) bevinden. Hierbij dient gebruikgemaakt te worden van 2FA.

Nr. 2: Beheren van netwerksystemen

Vanuit de Beheer-DMZ worden middels de aangewezen tooling/beheerapplicaties/portals de betreffende netwerksystemen benaderd. Alvorens te kunnen inloggen op deze systemen wordt middels het TACACS-protocol geverifieerd of een beheerder rechten heeft om het device te beheren en zo ja, welk autorisatie-niveau daarbij hoort. Na vaststelling van de identiteit en het autorisatieniveau kunnen de betreffende nodes worden beheerd. Let op: Binnen Azure betreft dit nodes van vendoren die appliances bieden via de marktplaats. Cloud native nodes worden in de regel middels de azure-portal beheerd.

PEP-functies dienen te worden toegepast in de modules Datacenter (onprem), Backbone en Cloud. In de module SURF worden geen netwerknodes (virtual appliances) ondergebracht, zodat geen communicatiestromen richting deze module zijn opgenomen. In overleg met de markt dienen de betreffende PEP-functies te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

Use case 6-3: Beheer/management – Beheerfaciliteiten SaaS-dienst



Nr. 1: Benadering managementsystemen (SaaS-dienst)

Beheerders benaderen de SaaS-dienst van waaruit het beheer wordt uitgevoerd. Middels authenticatie (2FA) en autorisatie krijgt de beheer toegangsrechten tot de SaaS-dienst. Let op: Indien een SaaS-dienst in Azure is ondergebracht (e.g. zelf ontwikkeld), behoort deze Azure-dienst ook tot deze use case.

Nr. 2: Beheren van netwerksystemen

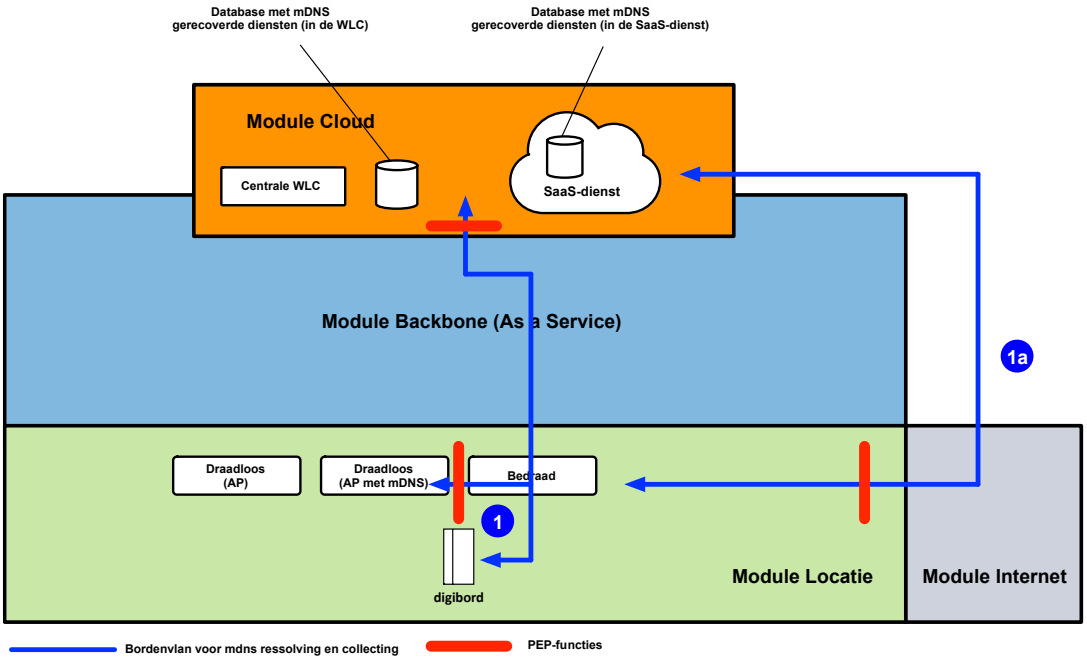
Vanuit de SaaS-dienst worden de systemen benaderd. Aangezien het een SaaS-oplossing betreft, verlopen alle communicatiestromen voor beheer via het internet.

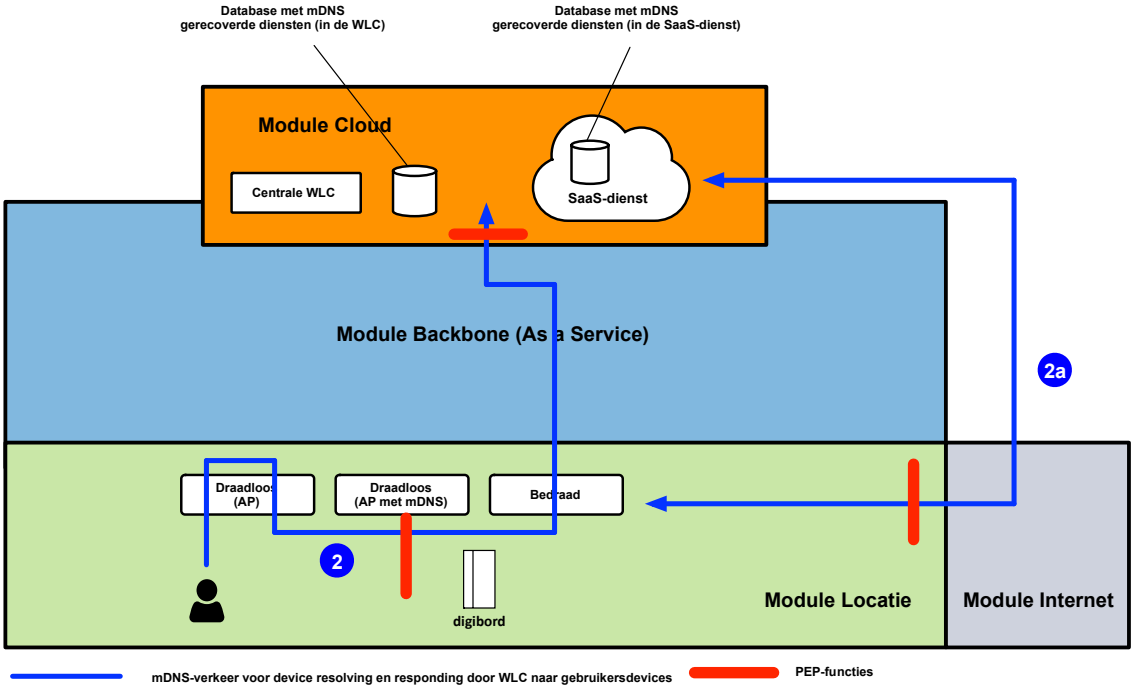
PEP-functies dienen te worden toegepast in de module Cloud (AAA voor de SaaS-dienst), module Cloud indien systemen binnen Azure vanuit de SaaS-dienst worden beheerd, de module Datacenter (onprem) en de module Locatie. In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

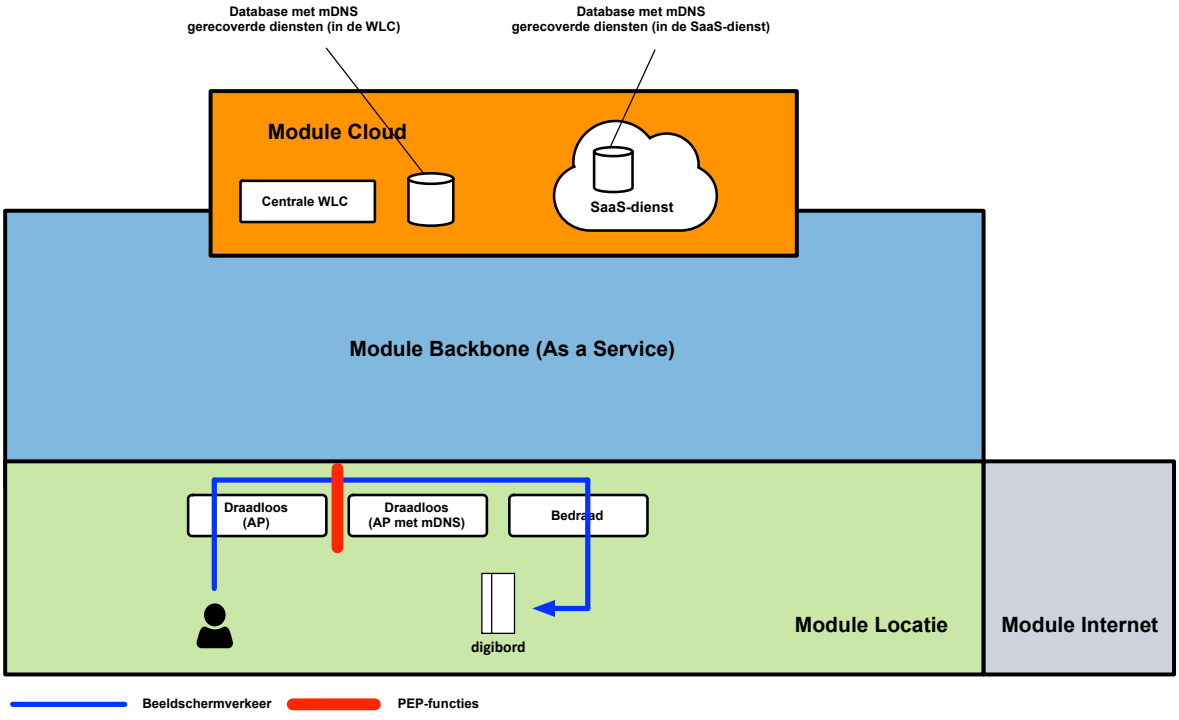
4.8.7 Smartbord

Use case 7: Digibord

In de onderstaande drie figuren is de use case voor Digibord afgebeeld.







<u>Nr. 1: Verzamelen appleplay, chromecast en miracast diensten</u>

Let op: Het ROC staat een 'cloud, tenzij' strategie voor. Dit houdt tevens in, dat de centrale wirelessdienst-verlening vanuit de cloud wordt afgenomen. Dit kan vanuit Azure zijn, maar het kan ook een SaaS-dienst zijn (i.e. communicatiestroom 1a). Communicatiestromen (mDNS resolving & collecting) verlopen naar de clouddienst, tenzij dit door het type dienst/product niet mogelijk is c.q. niet de beste oplossing in de praktijk blijkt te zijn.

<u>Nr. 2: Aanvraag en aanbieden van de appleplay, chromecast en miracast diensten op de wireless netwerken</u>

mDNS-verkeer voor device resolving en responding wordt verstuurd door de WLC naar gebruikersdevices. Indien de WLC als SaaS-dienst wordt afgenomen, verloopt de communicatiestroom via het internet (2a).

<u>Nr 3. Beeldschermverkeer tussen gebruiker en digibord.</u>

Bij voorkeur wordt het beeldschermverkeer lokaal afgehandeld door een local breakout feature, opdat het beeldschermverkeer niet eerst naar de centrale wireless dienstverlening hoeft te worden getransporteerd, waarna het weer wordt teruggestuurd.

PEP-functies dienen te worden toegepast in de module Locatie. Dit in verband met een scheiding tussen de IT-zone (AP & Gebruikers) en OT-zone (digibord). Zie voor meer informatie paragraaf 4.8.8 IOT-generiek, temeer het digibord ook binnen de categorie IoT valt. Over het beheer van de digiborden het volgende:

Een digibord bestaat uit twee devices

1. Android device,
2. Gekoppeld Windowssysteem.

Aangezien beide devices een andere functionaliteit uitoefenen, dienen deze in een eigen zone te worden opgenomen.

Communicatiestromen naar de cloud (use case voor Azure) verlopen via PEP-functies op het niveau van de module Backbone en op het niveau van de module Cloud. Indien de communicatiestroom betrekking heeft op een SaaS-dienst/toepassing, verloopt de communicatiestroom via het internet waarbij op het niveau van de module Locatie PEP-functies zijn aangebracht.

In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

4.8.8 IoT-generiek

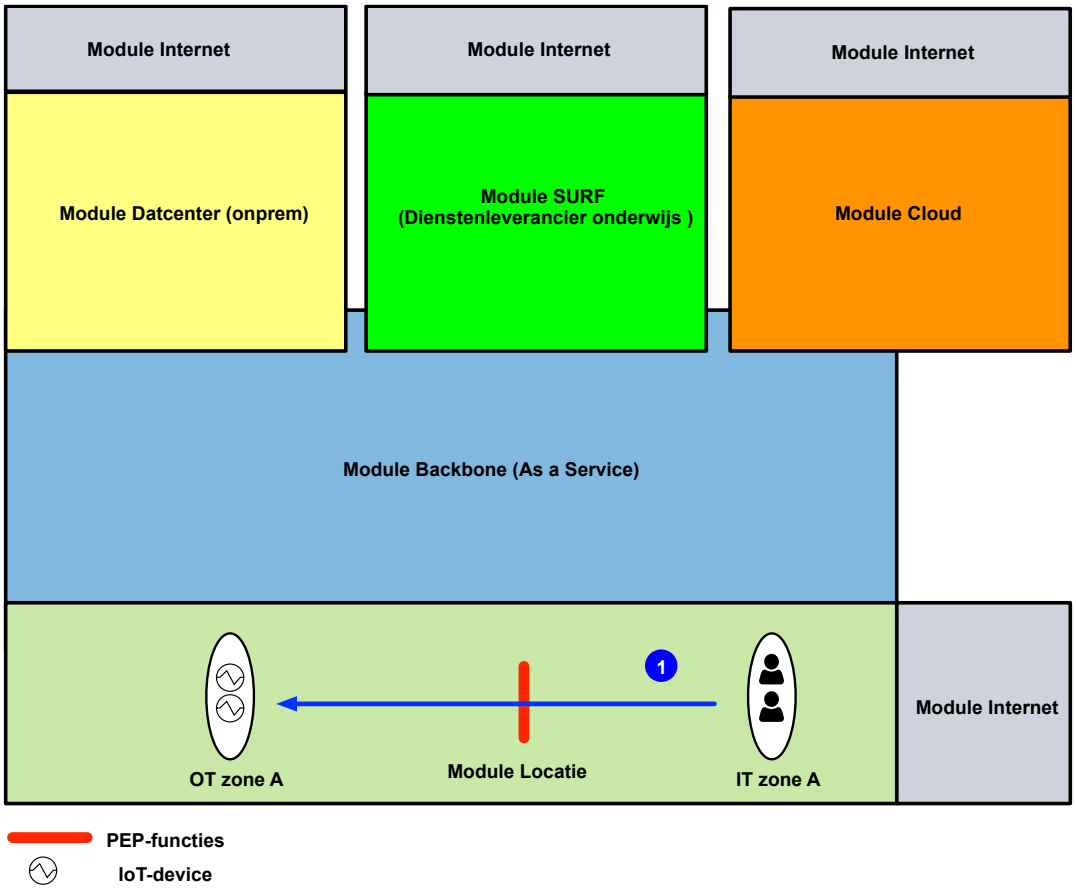
Op deze plaats wordt communicatie in relatie tot IoT apart en generiek behandeld. De IoT-diensten die binnen het ROC gebruikt worden en (mogelijk) zullen worden, zijn hieronder opgesomd. De principes van zonering, PEP en communicatiestromen volgen hetzelfde stramien, waarbij wordt uitgegaan van:

- Aparte OT zones voor IoT-objecten,
- Aparte IT zones,
- Communicatie tussen zones verloopt middels een PEP-functie,
- Beheer van IoT-devices volgen hetzelfde stramien zoals geduid bij use case 6 (Beheer/management).

Domein	Omschrijving
Educatief	• Lasrobots, • Kantbanken, • CNC-banken, • 3d printer, • CNC-snijmachines.
Facilitair/administratief	• Printers, • Labelprinters privasystemen, • Alarmsystemen, • Kluisjes met gebruikers auth, • Kassa’s, • Pinautomaten, • Snoepautomaten en andere cateringautomaten. • IP-camera’s voor facilitair/beveiliging, • Zonnepanelen, • Windmolen, • Narrowcasting, • Franceermachines, • IP-telefoons.
Educatief ICT	• Camera’s voor educatieve doeleinden (beveiligingsopleiding) • Printers, • Apple TV, • Feedtruck app devices. • Kweekkassen, • Nikoservers. • Educatieve homedomotica, • Scheepsimulatoren,

	• Marifoonsimulatoren, Machinekamersimulatoren ‘(URK), Educatieve ICT-devices als WiFi-routertjes, switches et cetera (deze hebben vaak tijdelijk wel internet nodig, maar dienen niet als alternatieve internettoegang voor de ICT-studenten).
Toekomst	• Camera’s op de digiborden voor het lesgeven via streaming faciliteiten, • Internetradio’s, • Google home et cetera, • Weerstations.

Use case 7-1: IoT-generiek/benaderen IoT device vanuit KA (IT)

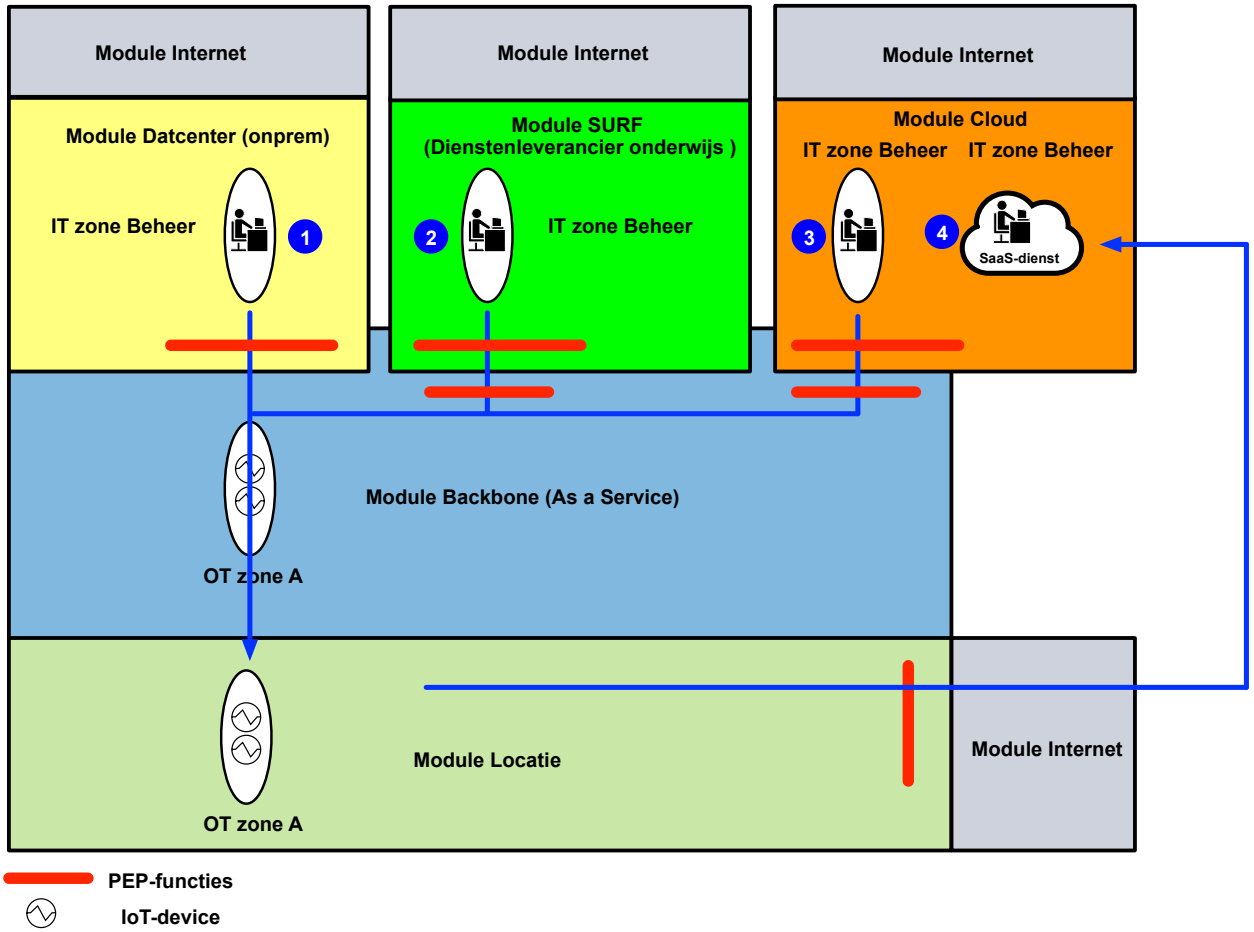


Nr. 1: Benaderen IoT device vanuit KA (IT)

Gebruikers in de module Locatie benaderen vanuit de toegewezen IT-zone de betreffende OT-zone, waarin het specifieke IoT-object is ondergebracht.

PEP-functies dienen te worden toegepast in de module Locatie. In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

Use case 7-2: IoT-generiek/beheer



Nr. 1: Beheer IoT device vanuit module Datacenter (onprem)

IoT-objecten in de OT-zones in de module Locatie worden eveneens vanuit de Beheer DMZ gemanaged. Met andere woorden: Er vindt inter-zoneringsverkeer plaats, waarbij in de module Datacenter (onprem) PEP-functies moeten worden toegepast. Hetzelfde geldt op het niveau van de module Backbone (ontsluiting module Locatie).

Nr. 2: Beheer IoT device vanuit module SURF

Het is mogelijk dat SURF een IoT-dienst aanbiedt die vanuit de module SURF wordt aangeboden. Bij voorkeur wordt de beheercommunicatie (die uit een portalfunctionaliteit kan bestaan) gefaciliteerd door de module Backbone zoals afgebeeld in de illustratie, waarbij inter-zoneringsverkeer plaatsvindt. Dit vanwege de mogelijkheid Quality of Service toe te passen op het niveau van de module Backbone en een goed inzicht te hebben van de beheerverkeersstroom. Het is hierbij van belang op het niveau van de modules SURF (zowel binnen deze module als richting de module Backbone) en Backbone (ontsluiting van de module Locatie) PEP-functies toe te passen. Indien directe communicatie via de module Backbone niet mogelijk

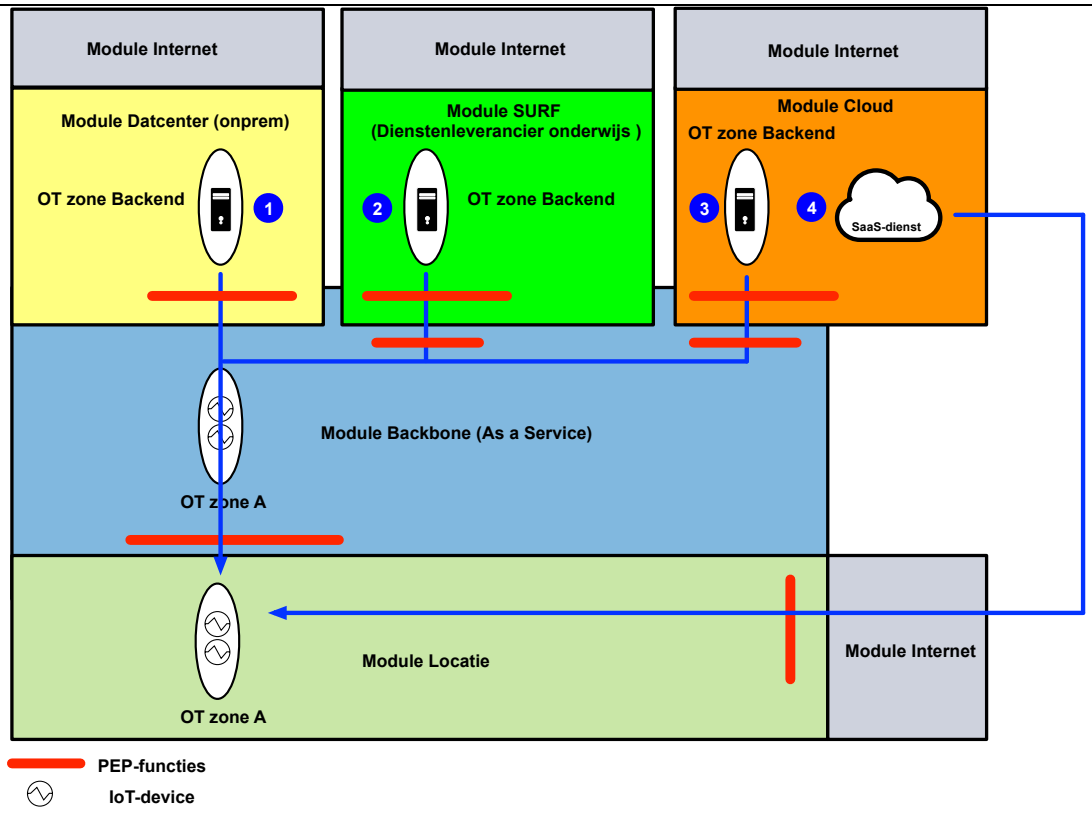
blijkt te zijn vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 3: Beheer IoT device vanuit module Cloud (Azure)
IoT-objecten in de OT-zones in de module Locatie worden eveneens vanuit de Beheer DMZ gemanaged. Met andere woorden: Er vindt inter-zoneringsverkeer plaats, waarbij in de module Cloud (Azure) PEP-functies moeten worden toegepast. Hetzelfde geldt op het niveau van de module Backbone (ontsluiting module Locatie en ontsluiting module Cloud). Bij voorkeur wordt de communicatiestroom gefaciliteerd door de module Backbone in verband met het kunnen toepassen van Quality of Service en vanwege een goed inzicht in de beheerverkeersstroom. Indien directe communicatie via de module Backbone niet mogelijk blijkt te zijn vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 4: Beheer IoT device vanuit SaaS-dienst
IoT-objecten in de OT-zones in de module Locatie worden via het internet beheerd. De SaaS-dienst-ontsluiting vindt immers via het internet plaats.

In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

Use case 7-3: IoT-generiek/data-overdracht



Nr. 1: Data-overdracht naar module Datacenter (onprem)

IoT-objecten kunnen substantieel veel data verzenden voor bijvoorbeeld data-analyses. Hoewel op grond van het principe 'cloud, tenzij' het niet in de lijn der verwachting ligt, dat in de (nabije) toekomst heel veel van dergelijke data naar het onprem datacenter zal worden verstuurd, dient hier wel rekening mee te worden gehouden. Deze data moet middels PEP-functies op het niveau van de modules Backbone (ontsluiting module Locatie) en Datacenter (onprem) worden geaccommodeerd.

Nr. 2: Data-overdracht naar module SURF

Op grond van het 'cloud, tenzij' principe zal meer en meer IoT-data verstuurd (gaan) worden naar 'de cloud'. SURF kan in dit kader als dienstenleverancier optreden voor IoT-diensten. De communicatiestroom vanaf IoT-objecten wordt bij voorkeur gefaciliteerd door de module Backbone in verband met inzicht in verkeersstromen en het toepassen van Quality of Service, waarbij op het niveau van de modules Backbone (ontsluiting module Locatie) en SURF de benodigde PEP-functies moeten worden toegepast. Indien verkeer niet via de module Backbone kan worden getransporteerd vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 3: Data-overdracht naar module Cloud (Azure

Op grond van het 'cloud, tenzij' principe zal meer en meer IoT-data verstuurd (gaan) worden naar 'de cloud'. Het clouddatacenter van Azure kan in dit kader worden gebruikt voor dergelijke IoT-diensten. De communicatiestroom vanaf IoT-objecten wordt bij voorkeur gefaciliteerd door de module Backbone in verband met inzicht in verkeersstromen en het toepassen van Quality of Service, waarbij op het niveau van

de modules Backbone (ontsluiting module Locatie) en Azure de benodigde PEP-functies moeten worden toegepast. Indien verkeer niet via de module Backbone kan worden getransporteerd vanwege de opzet van de IoT-dienst, dient het internet te worden gebruikt. Zie Nr. 4 hieronder. Het betreft dan een SaaS-dienst.

Nr. 4: Data-overdracht m.b.t. SaaS-dienst
Via het internet wordt data-overdracht gefaciliteerd naar de SaaS-dienst.

In overleg met de markt dienen de betreffende PEP-functies en posities exact te worden vastgesteld op grond van vergelijkbare omgevingen als die van het ROC.

5 Bijlage A: Ontwerpregels Technische Architectuur - architectuurgebied Security

5.1 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.
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.
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 beheerverantwoor-delijkheid 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 verkeers-afhandeling 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.
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.

5.2 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’.
2.2	Versleuteling van data mag geen nadelige impact hebben op de diensten die door de module Backbone worden getransporteerd.

5.3 Module Locatie - security

Ontwerpregel 3	LAN-security module Locatie
3.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
3.2	Overbodige services dienen te worden gedeactiveerd op de LAN-nodes.
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.
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.
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.
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.
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.
3.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
3.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
3.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
3.11	De nodes dienen het RADIUS-protocol te ondersteunen in het kader van toegangsbeveiliging middels de principes van IEEE 802.1x en MAB.
3.12	De nodes dienen IEEE 802.1x en MAB te ondersteunen.
3.13	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.
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).
3.15	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.

5.4 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.
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.
4.3	Access points dienen dermate te zijn opgesteld/gepositioneerd, dat deze niet binnen handbereik zijn of eigenmachtig gemaakt kunnen worden.
4.4	De WLC of gelijksoortige centrale draadloze functionaliteit dient verkeersscheiding te ondersteunen in het Distribution Systeem/ ICT-infrastructuur van het ROC.
4.5	Bij het inloggen in een access point of WLC middels de console dient een warning banner tevoorschijn te komen.
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.
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.
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.
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.
4.10	Het productieverkeer dient te zijn gescheiden van het managementverkeer.
4.11	Indien de centrale draadloze faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
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.

5.5 Toegangsbeveiliging

Ontwerpregel 5	Toegansverleningsdienst
5.1	Toegang tot het bedrade en draadloze netwerk van het ROC dient middels een toegangsverleningsdienst te worden gereguleerd.
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.
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.
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.
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 mee-gestuurd bij het authenticatieverzoek.
5.6	Na authenticatie dienen managed gebruikers/computers automatisch te worden ondergebracht in een zone.
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.
5.8	Foutief inloggen leidt ertoe, dat geen gebruikgemaakt kan worden van het netwerk van het ROC (zowel bedraad als draadloos).
5.9	Indien de centrale RADIUS-faciliteiten niet meer functioneren, blijven bestaande gebruikers-, computer- en systeemsessies behouden. Nieuwe sessies worden niet toegestaan.
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.
5.11	Gasten van het ROC dienen in een zone te worden opgenomen waarmee alleen internet als dienst kan worden benaderd.

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.
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.
5.14	De oplossing dient te kunnen communiceren met een IDP-omgeving van het ROC voor authenticatiedoeleinden voor studenten/medewerkers van het ROC.
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.
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).
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.
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.
5.19	Het is aan de markt te adviseren of de centrale oplossing als appliance, virtual machine of als SaaS-dienst wordt ingezet.

5.6 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.
6.2	De randen van het Datacenter (onprem) dienen te zijn afgeschermd van de modules Internet en Backbone middels 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).

Ontwerpregel 7	LAN-security Datacenter (onprem)
7.1	Loops in het netwerk dienen te allen tijde te worden voorkomen.
7.2	Overbodige services dienen te worden gedeactiveerd.
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.
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.
7.5	Nodes die deel uitmaken van het DC-LAN dienen zonering te ondersteunen. Hierbij dienen de nodes verkeersscheiding op logisch niveau te ondersteunen.

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.
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.
7.8	De nodes dienen features te ondersteunen tegen ARP-spoofing.
7.9	De nodes dienen features te ondersteunen tegen IP-spoofing.
7.10	Verkeersscheiding tussen productie en management dient te worden gewaarborgd.
7.11	De nodes dienen het TACACS-protocol te ondersteunen in het kader van device administration.
7.12	Bij het inloggen op een node middels de console dient een warning banner tevoorschijn te komen.

5.7 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.
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.
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.
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.
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.
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.

5.8 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.
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.
9.3	Ontsluiting van IoT-devices dient te zijn gebaseerd op het IP-protocol, waarbij zowel IPv4 als IPv6 ondersteund dienen te worden
9.4	Ontsluiting van IoT-devices dient zowel bedraad als draadloos te kunnen worden uitgevoerd.

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.
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.

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.

6 Bijlage B: Gebruikte afkortingen

Afkorting	Betekenis
AAA	Authentication, Autorization, Accounting
ABB	Architectuur Bouwblok
AAD	Azure Active Directory
AD	Active Directory
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AV	Augmented Reality
BIV	Beschikbaarheid Integriteit Vertrouwelijkheid
BYOD	Bring Your Own Device
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CNC	Computer Numerical Control
CPU	Central Processing Unit
CYOD	Choose Your Own Device
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DC	Datacenter
DNS	Domein Name System
DMZ	Demilitarized Zone
HLD	High Level Design
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IoT	Internet of Things
IT	Information Technology
KA	Kantoorautomatisering
LAN	Local Area Network
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDNS	Multicast DNS
M2M	Machine to Machine
NTP	Network Time Protocol
OT	Operational Technology
OTA	Ontwikkel, Test, Acceptatie

PaaS	Platform As A Service
PDC	Product Diensten Catalogus
PEP	Policy Enforcement Point
PLC	Programmable Logic Controller
RFP	Request For Proposal
PKI	Public Key Cryptography
RADIUS	Remote Authentication Dial-In User Service
RBAC	Roll Based Access Control
SaaS	Software As A Service
SCEP	Simple Certificate Enrollment Protocol
SDN	Software Defined Network
SLA	Service Level Agreement
TA	Technische Architectuur
TACACS	Terminal Access Controller Access-Control System
TLS	Transport Layer Security
U2M	User to Machine
VR	Virtual Reality
WAN	Wide Area Network
WLC	Wireless LAN Controller
WPA	WiFi Protected Access