Provincie Noord-Brabant

Blauwdruk Security Architectuur

ICT/Netwerkbeheer

Auteur
Martijn Vuik

Datum
25-01-2019

Inhoud

1 Documentbeheer

1.1 Auteur(s)

Naam	Functie	Organisatie
Martijn Vuik	Sr. Netwerk & Security Architect	PNB

1.2 Revisiehistorie

Versie	Datum	Door	Wijzigingen
0.1	29-11-2018	Martijn Vuik	Opzet document
0.9	30-12-2018	Martijn Vuik	Verdere invulling document op grond van: • gesprekken PNB, • aangeleverde gegevens PNB. Aanpassingen: • figuur 3-1, 3-2, 3-3, 3-4 en beschrijvingen.
1.0	25-01-2019	Martijn Vuik	Update op grond van laatste feedback

1.3 Contactlijst

Naam	Functie	Contactgegevens	Organisatie
Paul Jansen in de Wal	Project Manager	Tel: +31 681256246 Email: pjansenidwal@brabant.nl	PNB
Martijn Vuik	Sr. Netwerk & Security Architect	Tel: +31 655551618 Email: martijn.vuik@quality.nl	PNB

1.4 Distributielijst

Naam	Functie	Rol	RACI	Organisatie
Marcel van Bijnen	Algemeen Directeur	Algemeen Directeur	A	PNB
Paul Jansen in de Wal	Project manager	Opdrachtnemer project	R	PNB
Ruud van der Lee	Informatie architect	Aanreiken / bewaken architectuurkaders	C	PNB
Frank Gerwig			C	PNB
Peter van den Boogaard	Chief information security officer	Aanreiken / bewaken kaders informatieveiligheid	C	PNB
Ruud Aarts	Information security officer	Aanreiken / bewaken kaders informatieveiligheid	C	PNB

1.5 Referentiemateriaal

Document	Versie	Auteur
Maatregelen (BIO) versus bouwstenen beveiligingsinfrastructuur 2 okt 2018		Paul Jansen in de Wal
3_2_BIO_versie_1_0_PR	1.0	Overheid
Cloud Ambitie Provincie Noord-Brabant	14	Ruud van der Lee

ISO27001		ISO-standaard, vastgelegd door NEN
PRL webfiltering versie 29-1-2018	versie 29-1-2018	Paul Jansen in de Wal
PRL Vervanging Firewalls versie 1-4-2018	versie 1-4-2018	Paul Jansen in de Wal
Basis Infrastructuur Omgeving.vsdx	1.1	P.H.W. van den Boogaard
Corsa Omgeving.vsdx	1.1	P.H.W. van den Boogaard
Exchange-Omgeving.vsdx	1.1	P.H.W. van den Boogaard
Architectuuroverzicht CP.vsdx	1.0	P.H.W. van den Boogaard
Architectuuroverzicht KE.vsdx	1.0	P.H.W. van den Boogaard
Architectuuroverzicht KO.vsdx	1.1	P.H.W. van den Boogaard
Architectuuroverzicht KP.vsdx	1.0	P.H.W. van den Boogaard
Architectuuroverzicht PO.vsdx	1.0	P.H.W. van den Boogaard

1.6 Gebruikte afkortingen

AAA:	Authentication, Authorization, Accounting
AV:	Antivirus
BIO:	Baseline Informatiebeveiliging Overheid
BIV:	Beschikbaarheid Integriteit Vertrouwelijkheid
BYOD:	Bring Your Own Device
CIA:	Confidentiality Integrity Availability
DC:	Datacenter
DMARC:	Domain Message Authentication Reporting & Conformance
DKIM:	Domain Keys Identified Mail
DLP:	Data Leakage (Lost) Prevention
DMZ:	Demilitarized Zone
DoS:	Denial of Service
FP:	Forward Proxy
HLD:	High Level Design
HTTPS:	Hyper Text Transfer Protocol Secure
IAM:	Identity and Access Management
IE:	Internet Explorer
IEEE:	Institute of Electrical and Electronics Engineers
iOS:	Iphone Operating System
IP:	Internet Protocol
IPS:	Intrusion Prevention System
ISO:	International Organization for Standardization
LAN:	Local Area Network
LB:	Load Balancing
LLD:	Low Level Design
MAC:	Media Access Control
M2M:	Machine-to-Machine
MAB:	MAC Authentication Bypass
MAM:	Mobile Application Management
MS:	Microsoft
NAC:	Network Access Control
NEN:	Nederlandse Norm
OS:	Operating System
OOB:	Out of Band (Management)
PAC:	Proxy Auto Config
PEP:	Policy Enforcement Point

PKI	Public Key Infrastructure
PNB	Provincie Noord-Brabant
PSA:	Project Start Architectuur
RADIUS:	Remote Authentication Dial-In User Service
RBAC:	Role Based Access Control
RFP	Request for Proposal
RP:	Reverse Proxy
SAAS:	Software As A Service
SFP:	Small Form Factor Pluggable
SNMP:	Simple Mail Transfer Protocol
SSH:	Secure Shell
SSL:	Secure Sockets Layer
SQL:	Structured Query Language
TACACS:	Terminal Access Controller Access-Control System
TLS:	Transport Layer Security
U2M:	User-to-Machine
URL:	Uniform Resource Locator
VLAN:	Virtual Local Area Network
VPN:	Virtual Private Network
WAN:	Wide Area Network
WLAN:	Wireless Local Area Network

2 Inleiding

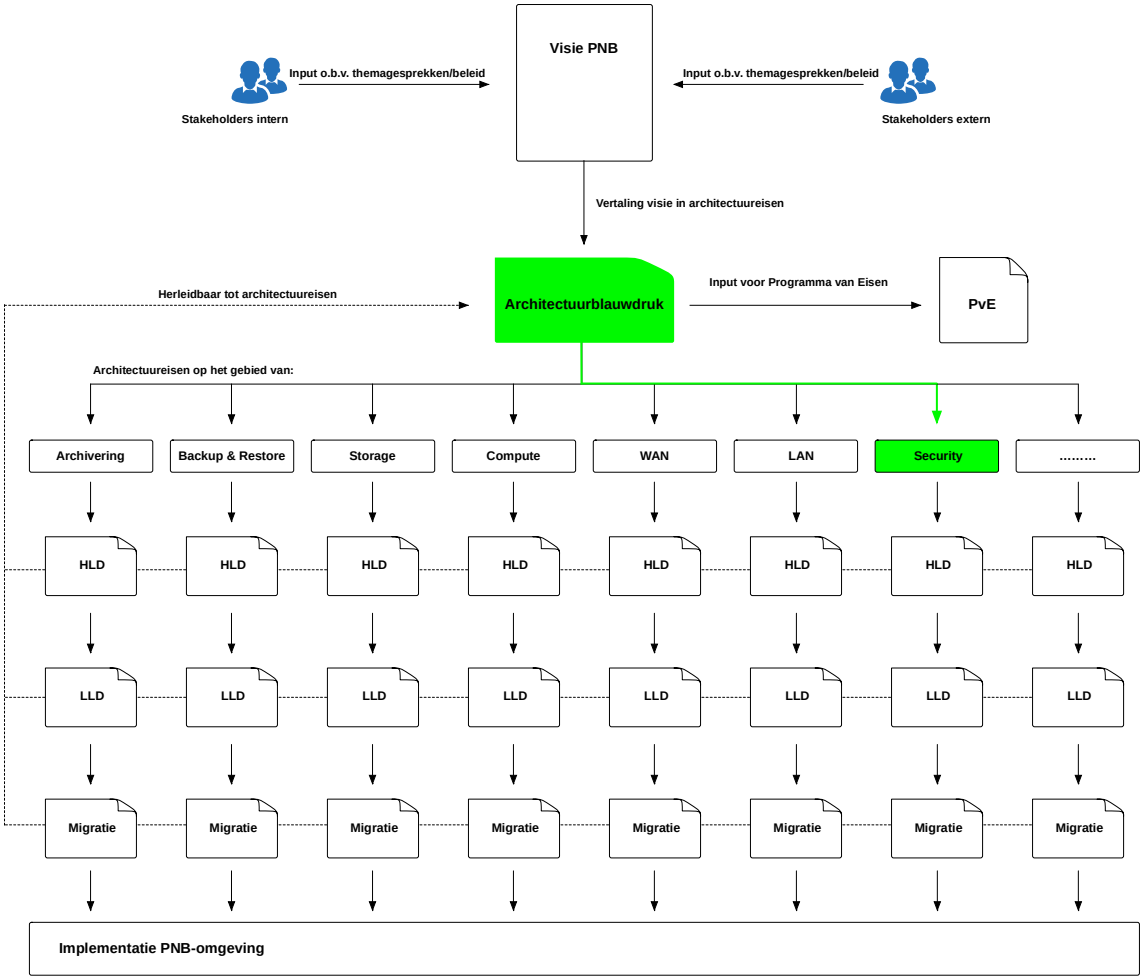
2.1 Werken onder architectuur

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 blauwdruk voor de security architectuur bevat een samenhangende beschrijving van de door PNB gebruikte diensten, informatie-uitwisseling en infrastructurele onderdelen in het kader van security en 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 security worden gedragen door het senior management/ raad van bestuur.

Doelstelling blauwdruk voor security architectuur?
In de blauwdruk worden de volgende onderwerpen beschreven:

- De vertaalslag van de visie van PNB naar de security-dienstverlening op verschillende gebieden/domeinen,
- De standaarden die bij het (integraal) ontwerpen van de security-dienstverlening dienen te worden toegepast,
- Relaties naar Technische Ontwerpen. De beschreven/geïllustreerde security-functies worden door een architectuureis gevolgd. Deze dienen te worden opgevolgd bij de creatie van onderliggende Technische Ontwerpen als High Level Designs, PSAs, Low Level Design et cetera.

Positie van de blauwdruk security architectuur?
In de illustratie op de volgende pagina is de positie van de architectuurblauwdruk weergegeven. Een architectuurblauwdruk wordt gebruikt als management- en stuurinstrument en is de spil in het web voor afgeleide documentatie en voor input in het kader van RFP-trajecten. Door in alle afgeleide documentatie de architectuureisen (ontwerpregels) vanuit de architectuurblauwdruk als leidraad te nemen, zijn alle functioneel en technisch uitgewerkte onderdelen herleidbaar tot aan de betreffende eisen in deze architectuurblauwdruk. Op deze manier ontstaat een consistent architectuurlandschap, waarbij onderdelen in samenhang worden ontworpen. Dit zowel binnen domeinen als in relatie tot aanpalende domeinen.



Figuur 2-1: *Positie architectuurblauwdruk*

2.2 Scope

In dit document wordt het domein ‘security’ behandeld, hetgeen groen is afgebeeld in de illustratie. Op het moment van schrijven is de scope als volgt:

- Het vastleggen van eisen op het gebied van de security architectuur van PNB, waarbij de technische architectuur van de security-dienstverlening het vertrekpunt is. Binnen deze scope vallen:
  - Beveiligingseisen LAN, DC-LAN, DMZ-LAN,
  - Beveiligingseisen forward proxy,
  - Beveiligingseisen reverse proxy,
  - Beveiligingseisen mail scanning,
  - PKI op het niveau van de technische architectuur; dit wil zeggen dat organisatorische, procesmatige en procedurele onderdelen niet zijn beschreven,
  - Toegangscontrole voor het bedrade netwerk.

Op het moment van schrijven zijn (derhalve) de volgende onderdelen out of scope. Het vastleggen/beschrijven van:

- processen en procedures met betrekking tot de security architectuur, incluis PKI,

- organisatorische rollen/taakverdeling in het kader van de security architectuur (e.g.: autorisatiematrices, HRM-onderdelen, jurdische onderdelen m.b.t. PKI),
- opstapomgevingen/toolingsystemen i.h.k.v. IAM, anders dan beschrijvingen op het gebied van communicatiestromen en te benutten managementprotocollen,
- een totaaloplossing voor NAC, anders dan het bedrade netwerk met MAB als 'authenticatiemechanisme',
- security met betrekking tot componenten op het gebied van compute, storage, backup & restore, archiving, anders dan DLP-gerelateerde onderdelen.

Hoewel op het moment van schrijven de bovengenoemde zaken out of scope zijn voor opname en uitwerking in dit document, is voor enkele onderwerpen wel ruimte opgenomen voor toekomstige vastleggingen.

2.3 Stakeholders

De volgende stakeholders zijn betrokken bij de totstandkoming van de blauwdruk security architectuur:

- De personen die zijn benoemd in de distributielijst,
- Senior Management/Raad van Bestuur.

2.4 Doelgroep

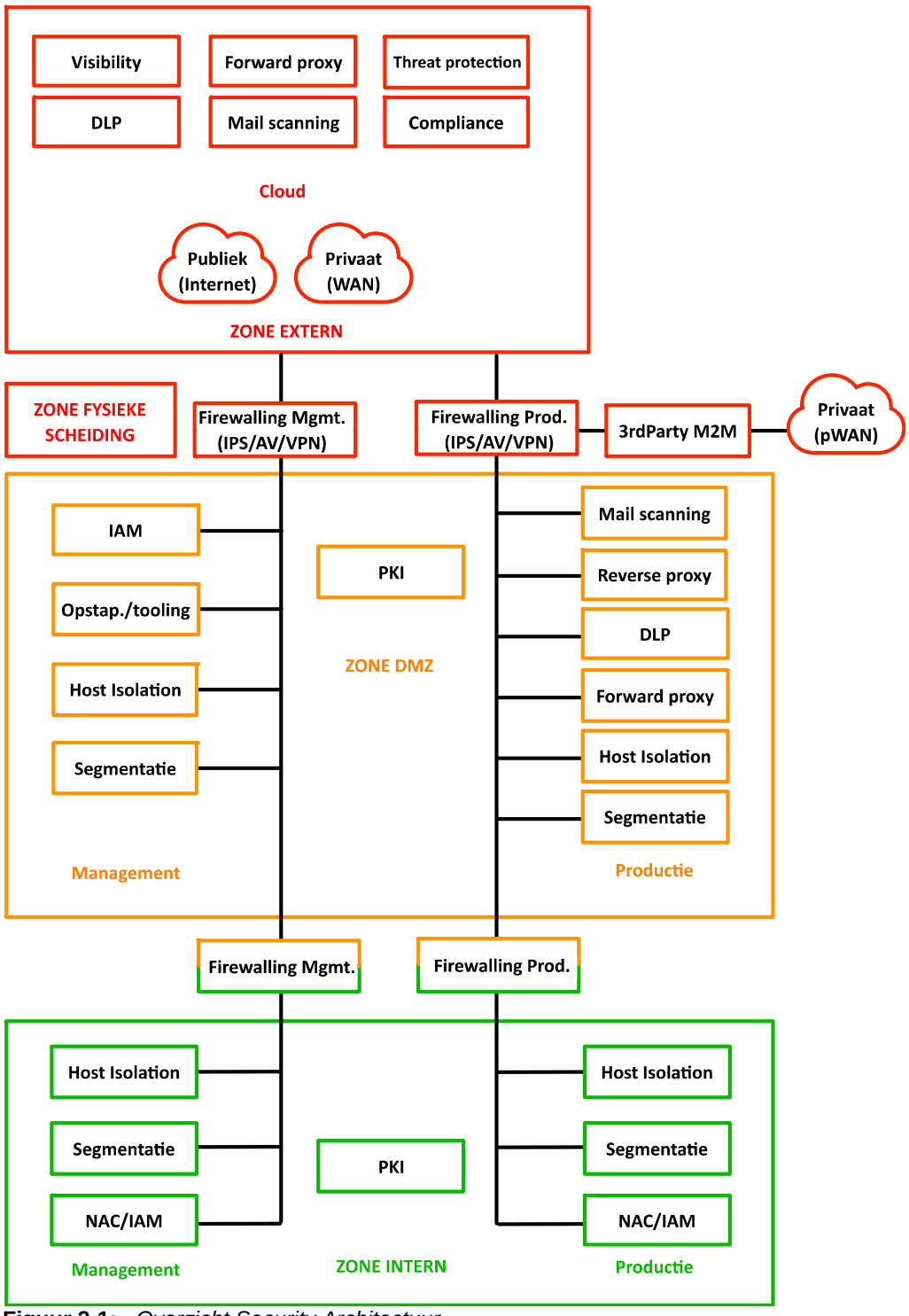
Dit document is bestemd voor:

- Senior Management/Raad van Bestuur PNB,
- Leden van het Design Office PNB,
- Consultants (Business, Informatie, Technisch), zowel intern als extern,
- Domeinverantwoordelijken voor implementatie en operatie.

3 Beveiligingsarchitectuur PNB

3.1 Generiek overzicht

In het onderstaande overzicht is de security architectuur van PNB generiek afgebeeld.



Figuur 3-1: *Overzicht Security Architectuur*

3.2 Dataclassificatie

PNB hanteert de volgende dataclassificatie.

[Opname in later stadium/separaat topic/buiten resultaatopdracht 2]

Ontwerpregel 1: *T.b.d.*

Ontwerpregel 2: *T.b.d.*

Ontwerpregel 3: *T.b.d.*

3.3 Zonering

Ontwerpregel 4: *Het netwerk van PNB dient te zijn ondergebracht in verschillende zones op basis van door PNB opgestelde beveiligingsrichtlijnen en dataclassificatie.*

Ontwerpregel 5: *Het netwerk van PNB dient ten minste te voorzien in de zones intern, DMZ, extern en fysieke scheiding.*

3.3.1 Zone intern

Deze zone biedt systemen en gebruikers toegang tot het netwerk van PNB. Met andere woorden: gebruikerssystemen als laptops, tablets, PCs maar ook printers en serversystemen zijn in deze zone ondergebracht. De zone intern grenst aan de zone DMZ, waarbij een firewallvoorziening de toegang tussen deze zones reguleert.

Ontwerpregel 6: *De zones intern en DMZ dienen middels een firewallfunctie van elkaar te zijn afgeschermd. Dit geldt voor de productiefirewall en managementfirewall.*

3.3.2 Zone DMZ

De zone DMZ bevindt zich tussen de zone intern en de zone extern en fungeert als buffer tussen deze zones. De zone DMZ heeft als doel het realiseren van veilige dataoverdracht en communicatie van en naar de externe zone.

Ontwerpregel 7: *De zones DMZ en extern dienen middels een firewallfunctie van elkaar te zijn afgeschermd.*

Ontwerpregel 8: *Forward proxies dienen te zijn ondergebracht in de zone DMZ.*

Ontwerpregel 9: *Reverse proxies dienen te zijn ondergebracht in de zone DMZ.*

Ontwerpregel 10: *E-mail proxies dienen te zijn ondergebracht in de zone DMZ.*

Ontwerpregel 11: *Systemen voor DLP-doeleinden dienen te zijn ondergebracht in de zone DMZ.*

Ontwerpregel 12: *IAM-systemen dienen te zijn ondergebracht in de zone DMZ.*

Ontwerpregel 13: *Opstapomgevingen en toolingsystemen dienen te zijn ondergebracht in de zone DMZ.*

3.3.3 Zone extern

De zone extern bevindt zich in de perimeter van het netwerk van PNB en accommodeert de internetopgang. De internetopgang wordt onder andere gebruikt door eindgebruikers, DC-serversystemen (e.g.: updates), DMZ-serversystemen (e.g.: updates). De zone extern grenst aan de zone DMZ. De zone extern verbindt eveneens WAN-verbindingen met het netwerk van PNB.

Ontwerpregel 14: *De zones extern en DMZ dienen middels een firewallfunctie van elkaar te zijn afgeschermd. Dit geldt voor de productiefirewall als managementfirewall.*

Ontwerpregel 15: *Publieke koppelingen als het internet (niet-vertrouwd) alsmede WAN-koppelingen met derde partijen (niet-vertrouwd) dienen te worden afgemonteerd op de externe firewall.*

3.3.4 Zone fysieke scheiding

Ontwerpregel 16: *De zone 'fysieke scheiding' bevat onderdelen die eenvoudig kunnen worden afgestoten (e.g.: apparatuur derde partijen).*

3.4 Segmentatie

Om het beveiligingsniveau verder te verhogen worden segmenten aangebracht binnen een zone. Hierdoor is het mogelijk risico's verder te isoleren op het niveau van een zone. Dit is in tabel 3-1 conceptueel afgebeeld voor een generieke zone.

Ontwerpregel 17: *Binnen een zone dient de beveiliging verder te kunnen worden verhoogd door het toepassen van netwerksegmentatie.*

Tabel 3-1: *Segmentatie binnen zone*

Zone
Segment a
Segment b
Segment c
Segment d
Segment e

Om het beveiligingsniveau binnen een segment verder te verhogen dient microsegmentatie te kunnen worden toegepast. Dit is in tabel 3-2 conceptueel afgebeeld voor een generiek segment.

Tabel 3-2: *Microsegmentatie*

Segment
Isolatie a
Isolatie b
Isolatie c
Isolatie d
Isolatie e

Ontwerpregel 18: *Binnen een segment dient de beveiliging verder te kunnen worden verhoogd door het toepassen van microsegmentatie.*

3.5 PKI

[Opname in later stadium/separaat topic/buiten resultaatopdracht 2]

Ontwerpregel 19: *T.b.d.*

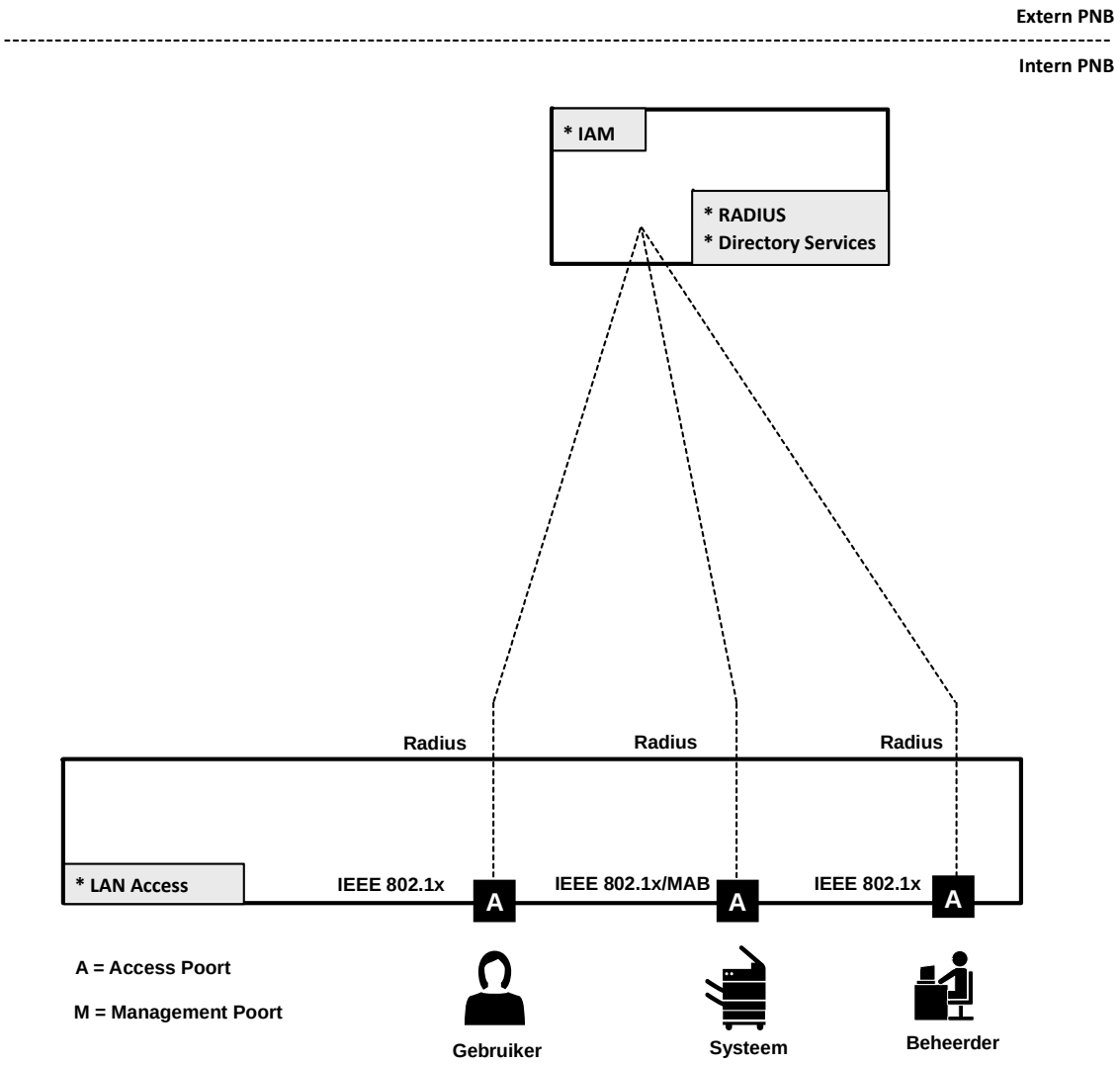
Ontwerpregel 20: *T.b.d.*

Ontwerpregel 21: *T.b.d.*

3.6 Identity & Access Management

3.6.1 NAC

In de onderstaande illustratie is het concept NAC generiek afgebeeld. Zowel gebruikers als systemen dienen eerst te worden geauthentiseerd en geautoriseerd, voordat toegang wordt verleend tot het netwerk van PNB.



Figuur 3-2: *Overzicht NAC*

Ontwerpregel 22: *Toegang tot het bedrade netwerk door onvertrouwde devices is niet toegestaan.*

Ontwerpregel 23: *Op het moment van schrijven kan worden volstaan met het centraal administreren van MAC-adressen van trusted devices, waarmee MAB kan worden toegepast.*

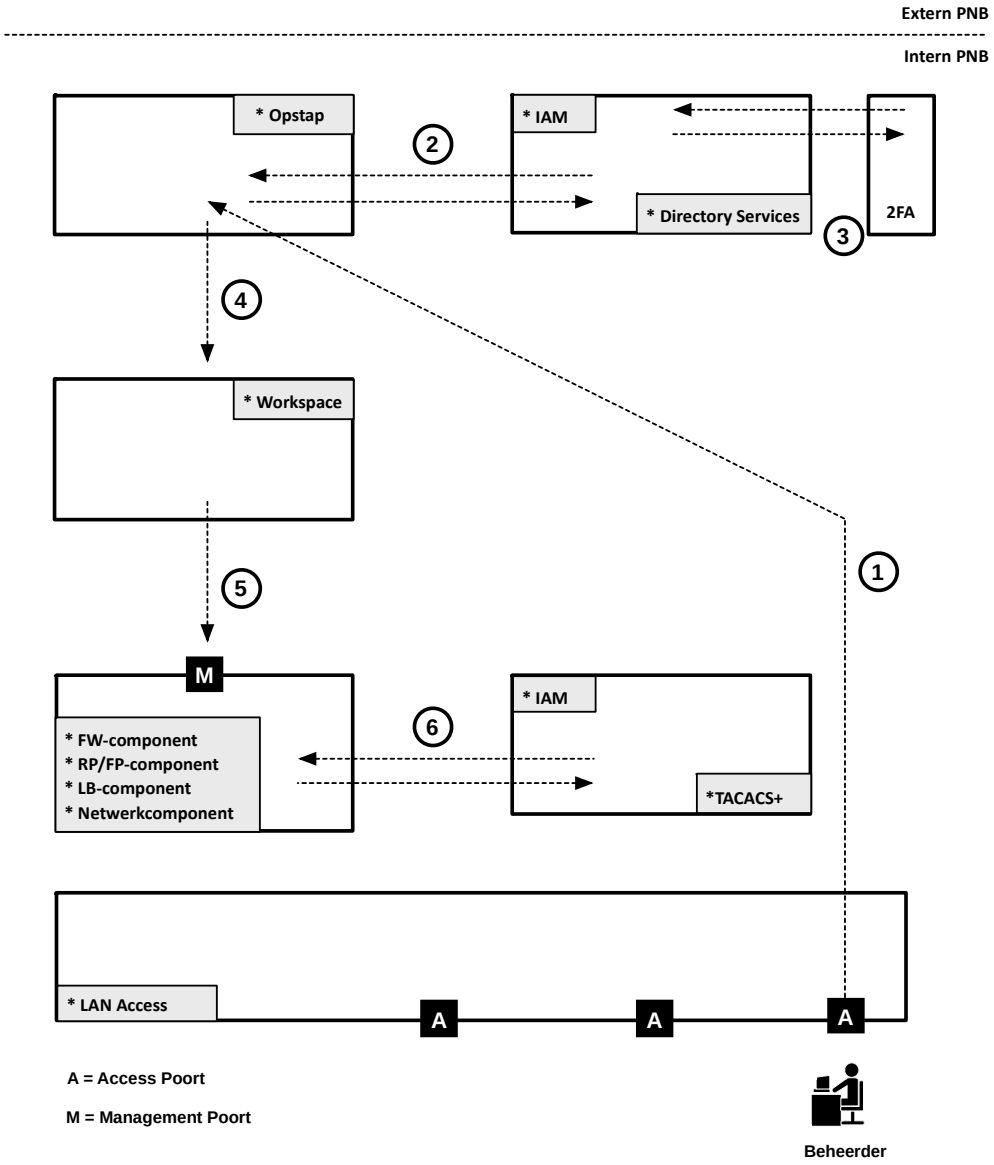
Ontwerpregel 24: *Het dient mogelijk te zijn een gebruiker of systeem dynamisch te plaatsen in een segment.*

Ontwerpregel 25: *Het dient mogelijk te zijn een netwerkpoort waaraan een gebruiker of systeem gekoppeld is dynamisch te voorzien van een toegangslijst, opdat een gebruiker of systeem beperkt kan worden in de toegestane communicatiemogelijkheden.*

Ontwerpregel 26: *De NAC-oplossing dient functioneel uitbreidbaar te zijn om de dienstverlening op het gebied van security aan te passen naargelang de huidige stand van zaken (i.e.: nieuwe/aangepaste eisen PNB).*

3.6.2 Device administration

Intern
Het beheer van netwerk- en securitycomponenten dient met beveiliging als uitgangspunt te worden uitgevoerd. In de onderstaande illustratie is het beheer van deze componenten conceptueel afgebeeld.



Figuur 3-3: *Overzicht device administration (intern)*

Ontwerpregel 27: *Het beheer van netwerk- en securitycomponenten dient vanuit een centrale opstapomgeving te worden uitgevoerd (nr. 1).*

Ontwerpregel 28: *In de IAM-omgeving worden de user credentials en toegangsrechten op basis van RBAC geverifieerd (nr. 2.)*

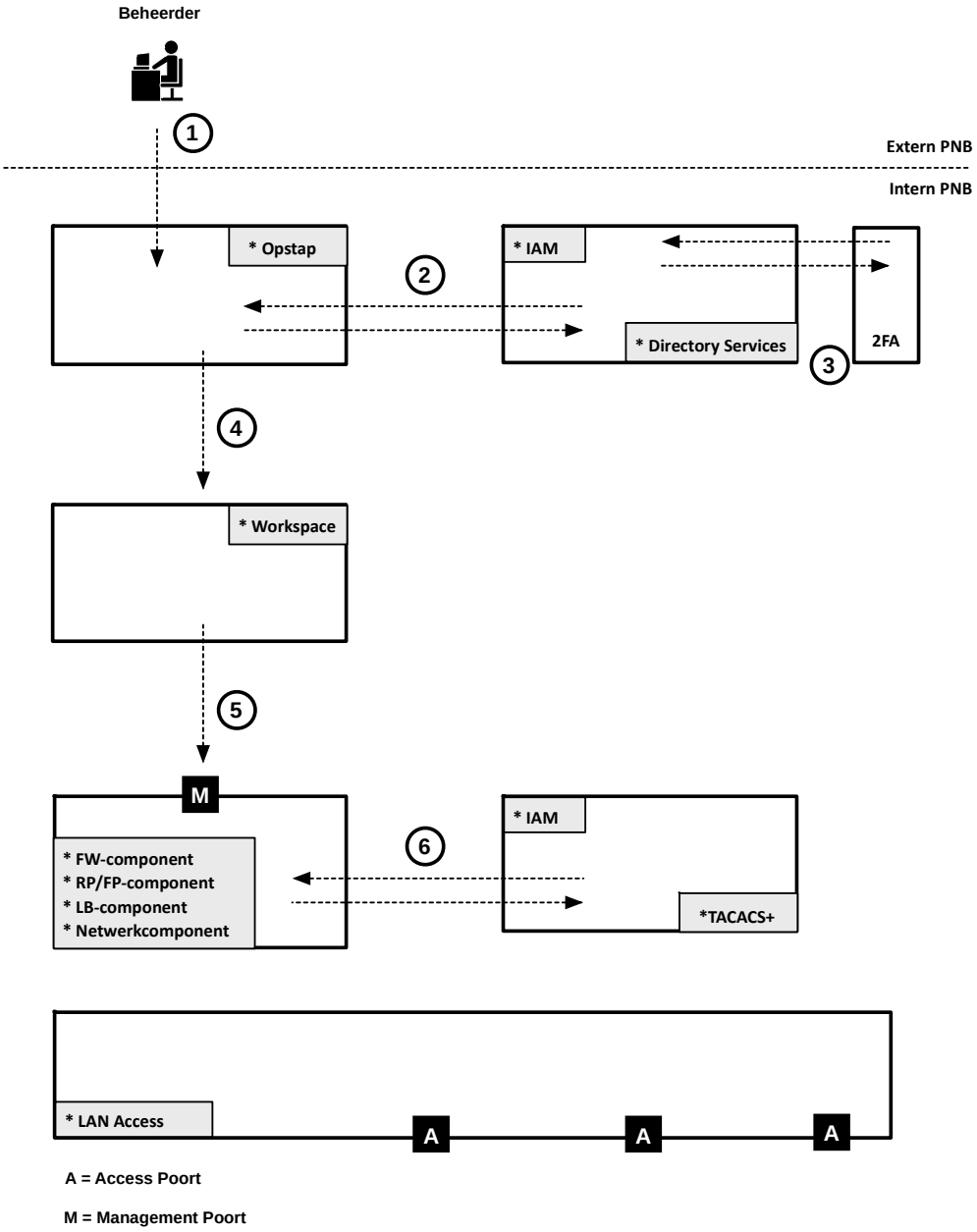
Ontwerpregel 29: *User authenticatie dient middels 2FA te worden gerealiseerd (nr. 3).*

Ontwerpregel 30: *Na IAM-onderdelen/functies te hebben doorlopen dient een op RBAC gebaseerde workspace (tooling) te worden gecreëerd (nr. 4).*

Ontwerpregel 31: *Het beheer van netwerk- en securitycomponenten dient te worden uitgevoerd middels managementprotocollen met ingebouwde beveiligingsfuncties (e.g.: SSH, HTTPS)(nr. 5).*

Extern (remote access)

Het remote beheer van netwerk- en securitycomponenten dient met beveiliging als uitgangspunt te worden uitgevoerd. In de onderstaande illustratie is het beheer van deze componenten conceptueel afgebeeld.



Figuur 3-4: *Overzicht device administration (extern)*

Ontwerpregel 32: *Het beheer van netwerk- en securitycomponenten dient vanuit een centrale opstapomgeving te worden uitgevoerd (nr. 1).*

Ontwerpregel 33: *In de IAM-omgeving worden de user credentials en toegangsrechten op basis van RBAC geverifieerd (nr. 2.)*

Ontwerpregel 34: *User authenticatie dient middels 2FA te worden gerealiseerd (nr. 3).*

Ontwerpregel 35: *Na IAM-onderdelen/functies te hebben doorlopen dient een op RBAC gebaseerde workspace (tooling) te worden gecreëerd (nr. 4).*

Ontwerpregel 36: *Het beheer van netwerk- en securitycomponenten dient te worden uitgevoerd middels managementprotocollen met ingebouwde beveiligingsfuncties (e.g.: SSH, HTTPS)(nr. 5).*

3.6.3 Mobile Application Management

Ontwerpregel 37: *Leverancier, hardware en software zijn bekend in de markt.*

Ontwerpregel 38: *Producten hebben zich bewezen.*

Ontwerpregel 39: *Systemen evolueren mee in functionaliteit met de huidige stand van de techniek en spelen ook in op trends op het gebied van dreiging versus beveiliging.*

Ontwerpregel 40: *SAAS is een pré, maar on premise of hybride uitvoeringen zijn zeker mogelijk afhankelijk van de functionaliteiten.*

Ontwerpregel 41: *Een (virtuele) appliance heeft de voorkeur boven server software installatie op een OS.*

Ontwerpregel 42: *Virtuele appliances zijn niet mogelijk in de DMZ-zone on premise bij PNB.*

Ontwerpregel 43: *Server software moet passen op Windows Server 2012.*

Ontwerpregel 44: *Als voor opslag een externe database wordt gebruikt zijn dat MS SQL Server of Oracle.*

Ontwerpregel 45: *Centraal management met een grafische interface.*

Ontwerpregel 46: *Eenvoudig schaalbaar systeem.*

Ontwerpregel 47: *Verwerkingseenheden kunnen redundant worden uitgevoerd om uitval te verkleinen.*

Ontwerpregel 48: *Op afstand beheerbaar via een internet browser (IE, Firefox of Chrome).*

Ontwerpregel 49: *Microsoft Active Directory integratie.*

Ontwerpregel 50: *Gescheiden management interface is een pré.*

Ontwerpregel 51: *Supportdesk functionaliteiten vanuit het systeem is een pré (helpdesk tooling).*

Ontwerpregel 52: *Support en ondersteuning van de leverancier.*

Ontwerpregel 53: *Passend op voorkomende besturingssystemen zoals Android, iOS, Windows.*

Ontwerpregel 54: *Scheiding tussen persoonlijke en provinciale toepassingen.*

Ontwerpregel 55: *Encryptie van data in verbinding en opslag.*

Ontwerpregel 56: *Mogelijkheid om data op afstand te wissen.*

Ontwerpregel 57: *Mogelijkheid om applicaties te (de-)installeren.*

Ontwerpregel 58: *Mogelijkheid om applicaties af te dwingen.*

Ontwerpregel 59: *Mogelijkheid om onderscheid te maken tussen verschillende gebruikersgroepen.*

Ontwerpregel 60: *Toegangsbeveiliging voor gebruik toepassingen/apps afdwingen.*

Ontwerpregel 61: *De toepassing dient IPv6 ready te zijn.*

3.7 Security componentniveau

3.7.1 Netwerk switch

Ontwerpregel 62: *De netwerk switch beschikt over een separate OOB interface voor management-doeleinden.*

Ontwerpregel 63: *De netwerk switch dient managementprotocollen met ingebouwde beveiligings-functies te ondersteunen conform de meest actuele standaarden (e.g.: SNMPv3, SSHv2, HTTPS (TLS)). Managementprotocollen zonder ingebouwde beveiligings-functies zijn niet toegestaan (e.g.: Telnet).*

Ontwerpregel 64: *De netwerk switch dient zowel het RADIUS- als TACACS+ protocol te ondersteunen.*

Ontwerpregel 65: *Toegang tot de netwerk switch is gebaseerd op het principe van least privileges ten aanzien van verschillende levels binnen het systeem (RBAC).*

Ontwerpregel 66: *Fysieke en logische Interfaces van de netwerk switch zijn afgeschermd door wachtwoorden (e.g.: console access (fysiek) versus inbound/OOB management via een managementprotocol).*

Ontwerpregel 67: *Niet gebruikte services dienen te worden gedeactiveerd, opdat zo min mogelijk systeemkwetsbaarheden kunnen optreden.*

Ontwerpregel 68: *Op het niveau van de control plane dienen passende maatregelen getroffen te worden om DoS-aanvallen en man-in-the-middle-aanvallen te voorkomen.*

Ontwerpregel 69: *Op het niveau van de data plane dienen passende maatregelen getroffen te worden om DoS-aanvallen en man-in-the-middle-aanvallen te voorkomen.*

Ontwerpregel 70: *De netwerk switch op LAN-niveau dient IEEE 802.1x capable te zijn.*

Ontwerpregel 71: *De netwerk switch op DMZ-niveau dient host isolation te ondersteunen.*

Ontwerpregel 72: *De hardware van de netwerk switch op DC-niveau dient redundant te zijn uitgevoerd, incluis power supplies.*

Ontwerpregel 73: *De netwerk switch dient IPv6 ready te zijn.*

Ontwerpregel 74: *Data-in-transit dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-in-transit
☐ Data-in-transit hoeft niet te worden beschermd.

Management interface [Administrators]						
BIV-classificatie van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certicaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					

	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certicaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certicaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certicaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Authenticatie-informatie administrator -> TACACS+-server						
BIV-classificatie van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					

Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source

	☐ Niet vereist

Data(-in-transit) vanaf randapparatuur/gebruikers die zijn aangesloten op de switch wordt op het niveau van applicaties versleuteld. De switch zelf reguleert in dit kader geen data-in-transit.

Ontwerpregel 75: *Data-at-rest dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-at-rest
☐ Data-at-rest hoeft niet te worden beschermd

Informatie data store						
Non-volatile geheugen van de netwerk switch						
BIV-classificatie van de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Niveau encryptie						
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encryptie ☐ Field encryptie					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Key lengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
Versleuteling van backup van data	☐ Ja ☐ Nee					
Message authentication code (MAC)						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Key lengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					

3.7.2 Netwerk firewall [generiek]

Ontwerpregel 76: *De firewall is appliance based.*

Ontwerpregel 77: *De firewall dient te passen binnen een rack/bestaande opbouw en inrichting van een datacenter van PNB.*

Ontwerpregel 78: *De appliance dient te kunnen worden gevirtualiseerd.*

Ontwerpregel 79: *De hardware van de firewall dient redundant te zijn uitgevoerd, incluis power supplies. De appliance dient te kunnen worden geclusterd.*

Ontwerpregel 80: *De firewall dient minimaal 3 miljoen sessies te ondersteunen.*

Ontwerpregel 81: *De firewall dient managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform de meest actuele standaarden (e.g.: SNMPv3, SSHv2, HTTPS (TLS)). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g.: Telnet).*

Ontwerpregel 82: *Het FW-systeem dient het TACACS+ protocol te ondersteunen.*

Ontwerpregel 83: *Toegang tot het FW-systeem is gebaseerd op het principe van least privileges ten aanzien van verschillende levels binnen het systeem (RBAC).*

Ontwerpregel 84: *De firewall dient te voorzien in integratiemogelijkheden met andere componenten die deel uitmaken van de beveiligingsarchitectuur van PNB.*

Ontwerpregel 85: *De firewall is vanuit één centrale management-/beheeromgeving te beheren.*

Ontwerpregel 86: *De firewall dient te beschikken over een aparte management interface.*

Ontwerpregel 87: *De firewall is voorzien van een beheertool (management station) die meerdere firewalls simultaan kan aansturen en uitlezen.*

Ontwerpregel 88: *De FW management-/beheeromgeving is voorzien van een (online) helpfunctionaliteit.*

Ontwerpregel 89: *De FW management-/beheeromgeving is gebruiksvriendelijk en intuïtief.*

Ontwerpregel 90: *Het FW-systeem kent een Dashboard functie, waarmee in één oogopslag de status van het systeem is af te lezen.*

Ontwerpregel 91: *Het dashboard toont informatie over een aantal variabelen, waaronder: a. Verdachte activiteiten b. Incidentenlijst c. Systeemwaarschuwingen.*

Ontwerpregel 92: *Het FW-systeem voorziet in een alertfunctionaliteit voor het afgeven van alerts met betrekking tot de toestand van het systeem.*

Ontwerpregel 93: *Het FW-systeem geeft een alert bij (dreigende) overbelasting van het systeem.*

Ontwerpregel 94: *Het FW-systeem voorziet in een rollback-mogelijkheid waardoor aangebrachte wijzigingen eenvoudig zijn terug te draaien.*

Ontwerpregel 95: *De firewall dient te kunnen worden voorzien van updates en patches die geen downtime of negatieve impact veroorzaken in een redundante opstelling.*

Ontwerpregel 96: *Het geheel aan firewallvoorzieningen/beheervoorzieningen voorziet in logging-mogelijkheden.*

Ontwerpregel 97: *De logging kan middels het SYSLOG-protocol worden opgeslagen in een aparte omgeving, anders dan de combinatie van centrale firewallvoorzieningen.*

Ontwerpregel 98: *De logging kan worden uitgelezen middels de beheerinterface.*

Ontwerpregel 99: *Het FW-systeem voorziet in een audit-trail, opdat inzichtelijk is welke wijzigingen binnen het systeem zijn aangebracht.*

Ontwerpregel 100: *Het FW-systeem dient IPv6 ready te zijn.*

Ontwerpregel 101: *Data-in-transit dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-in-transit
☐ Data-in-transit hoeft niet te worden beschermd.

Managementinterface beheertool						
BIV-classificatie van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					

Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Managementinterface firewall [connectie met beheertool]						
BIV-classificatie van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					

Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source

	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol Algoritme Versie Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

De productie-interfaces van de firewall verwerken verkeersstromen, waarbij de versleuteling van het verkeer reeds op het niveau van applicatie is doorgevoerd (e.g.: HTTPS). De firewall zelf reguleert in dit kader niet de versleuteling van data(-in-transit).

Ontwerpregel 102: *Data-at-rest dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-at-rest
☐ Data-at-rest hoeft niet te worden beschermd

Informatie data store						
Harddisk managementstation						
BIV-classificatie van de data in de data store	B		I		V	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Niveau encryptie						
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encrypte ☐ Field encryptie					
Encryptie						
Encryptie van data-at-rest	☐ Ja		Protocol			
			Algoritme			
			Versie			
			Key lengte			
			Certificaat	☐ Self-signed ☐ Trusted source		
	☐ Niet vereist					
Versleuteling van backup van data	☐ Ja	☐ Nee				
Message authentication code (MAC)						
	☐ Ja		Protocol			
			Algoritme			

		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Informatie data store							
Hard disk firewall							
BIV-classificatie van de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encrypte							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encryptie ☐ Field encryptie						
Encryptie							
	☐ Ja		Protocol				
			Algoritme				
			Versie				
			Key lengte				
			Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist						
Versleuteling van backup van data	☐ Ja		☐ Nee				
Message authentication code (MAC)							
	☐ Ja		Protocol				
			Algoritme				
			Versie				
			Key lengte				
			Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist						

3.7.3 Netwerk firewall [intern/DMZ]

Ontwerpregel 103: *De hardware van de firewall beschikt over minimaal 4 poorten, per appliance, van 10 Gbit/s (SFP+).*

Ontwerpregel 104: *De hardware van de firewall beschikt over minimaal 8 poorten, per appliance, van 1 Gbit/s (SFP of RJ45).*

Ontwerpregel 105: *De firewall throughput moet minimaal 20 Gbit/s bedragen.*

Ontwerpregel 106: *De firewall throughput met IPS en application scanning moet minimaal 10 Gbit/s bedragen.*

3.7.4 Netwerk firewall [extern/DMZ]

Ontwerpregel 107: *De hardware van de firewall beschikt over minimaal 4 poorten, per appliance, van 10 Gbit/s (SFP+).*

Ontwerpregel 108: *De hardware van de firewall beschikt over minimaal 8 poorten, per appliance, van 1 Gbit/s (SFP of RJ45).*

Ontwerpregel 109: *De firewall throughput moet minimaal 20 Gbit/s bedragen.*

Ontwerpregel 110: *De firewall throughput met IPS en application scanning moet minimaal 10 Gbit/s bedragen.*

3.7.5 Forward proxy onprem

Ontwerpregel 111: *Leverancier, hardware en software zijn bekend in de markt.*

Ontwerpregel 112: *Producten hebben zich bewezen.*

Ontwerpregel 113: *Systemen evolueren mee in functionaliteit met de huidige stand van de techniek en spelen ook in op trends op het gebied van dreiging versus beveiliging.*

Ontwerpregel 114: *Een (virtuele) appliance heeft de voorkeur boven server software installatie op een OS.*

Ontwerpregel 115: *Virtuele appliances zijn niet mogelijk in de DMZ-zone on premise bij PNB.*

Ontwerpregel 116: *Server software moet passen op Windows Server 2012.*

Ontwerpregel 117: *Als voor opslag een externe database wordt gebruikt zijn dat MS SQL Server of Oracle*

Ontwerpregel 118: *De forward proxy is appliance based. SAAS is een pré, maar on premise of hybride uitvoeringen zijn zeker mogelijk afhankelijk van de functionaliteiten.*

Ontwerpregel 119: *Eenvoudig schaalbaar systeem.*

Ontwerpregel 120: *De forward proxy dient te passen binnen een rack/bestaande opbouw en inrichting van een datacenter van PNB.*

Ontwerpregel 121: *De forward proxy beschikt over minimaal 1 Gbit/s netwerk interface.*

Ontwerpregel 122: *De appliance kan autonoom functioneren.*

Ontwerpregel 123: *De appliance kan geclusterd functioneren.*

Ontwerpregel 124: *Het systeem voorziet in een beheertool.*

Ontwerpregel 125: *Het geheel aan appliances is vanuit één centrale beheertool te beheren.*

Ontwerpregel 126: *Op afstand beheerbaar via een internet browser (IE, Firefox of Chrome).*

Ontwerpregel 127: *De beheerinterface is voorzien van een (online) helpfunctionaliteit.*

Ontwerpregel 128: *De beheertool voorziet in uitgebreide beheeropties voor SSL-scanning.*

Ontwerpregel 129: *Mogelijkheid om te kiezen uit toelaatbare poorten en protocollen.*

Ontwerpregel 130: *De beheerinterface is intuïtief en gebruiksvriendelijk.*

Ontwerpregel 131: *Het systeem voorziet in een loggingfunctionaliteit.*

Ontwerpregel 132: *Gescheiden management interface is een pré.*

Ontwerpregel 133: *De logging is middels de beheerinterface uit te lezen.*

Ontwerpregel 134: *De logging kan middels het SYSLOG-protocol worden opgeslagen in een aparte omgeving, anders dan de combinatie van RP-voorzieningen.*

Ontwerpregel 135: *Realtime functie voor het monitoren van dataverkeer.*

Ontwerpregel 136: *Geeft (realtime) inzicht in de gebruikte resources.*

Ontwerpregel 137: *De forward proxy heeft integratiemogelijkheden met Microsoft Active Directory.*

Ontwerpregel 138: *Aanmaken policies voor gebruikersgroepen.*

Ontwerpregel 139: *Filteren van URL's.*

Ontwerpregel 140: *Filteren en instellen filters o.b.v. categorie.*

Ontwerpregel 141: *Mogelijke detectie schadelijke software.*

Ontwerpregel 142: *De forward proxy heeft ondersteuning voor SSL-verkeer op basis van een third party certificaat.*

Ontwerpregel 143: *Controleert op juistheid en actualiteit van beveiligingscertificaten.*

Ontwerpregel 144: *Het FP-systeem kent een Dashboard functie, waarmee in één oogopslag de status van het systeem is af te lezen.*

Ontwerpregel 145: *Het dashboard toont informatie over een aantal variabelen, waaronder: a. Verdachte activiteiten b. Incidentenlijst c. Systeemwaarschuwingen.*

Ontwerpregel 146: *Het FP-systeem geeft een alert bij (dreigende) overbelasting van het systeem.*

Ontwerpregel 147: *Het FP-systeem geeft een alert bij (dreigende) overschrijding van het aantal gelicentieerde gebruikers.*

Ontwerpregel 148: *Notificatiemogelijkheden voor beheerders.*

Ontwerpregel 149: *Het FP-systeem geeft een alert indien een download is mislukt.*

Ontwerpregel 150: *Het FP-systeem voorziet in een uitgebreide rapportagefunctionaliteit m.b.t. proxy- en webfiltergegevens.*

Ontwerpregel 151: *Het FP-systeem voorziet in een audit-trail, opdat inzichtelijk is welke wijzigingen binnen het systeem zijn aangebracht.*

Ontwerpregel 152: *Het FP-systeem voorziet in real-time monitoring m.b.t. proxy- en webfiltergegevens.*

Ontwerpregel 153: *Het FP-systeem voorziet in uitgebreide configuratiemogelijkheden.*

Ontwerpregel 154: *Het FP-systeem voorziet in functionaliteiten voor 'Policy Management'.*

Ontwerpregel 155: *Het dient mogelijk te zijn websites uit te sluiten van SSL-scanning.*

Ontwerpregel 156: *Het dient mogelijk te zijn uitzonderingen te maken op basis van URLs, gebruikers en apparatuur.*

Ontwerpregel 157: *Een keuzemogelijkheid om bepaalde gegevens niet te loggen is een pré (bijvoorbeeld het niet opslaan van gebruikersnamen).*

Ontwerpregel 158: *Autorisatie binnen het RP-systeem kan ingeregeld worden op basis van RBAC (role based access control).*

Ontwerpregel 159: *De FP dient managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform de meest actuele standaarden (e.g.: SNMPv3, SSHv2, HTTPS (TLS)). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g.: Telnet).*

Ontwerpregel 160: *Het RP-systeem dient het TACACS+ protocol te ondersteunen.*

Ontwerpregel 161: *Het RP-systeem voorziet in de mogelijkheid PAC-files te gebruiken.*

Ontwerpregel 162: *Het RP-systeem dient IPv6 ready te zijn.*

Ontwerpregel 163: *Data-in-transit dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-in-transit
☐ Data-in-transit hoeft niet te worden beschermd.

Management interface beheertool						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.

Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)		
Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol Algoritme	
		Versie Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme Versie Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Managementinterface proxy [connectie met beheertool]						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
	☐ Ja	Protocol Algoritme Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
Message authentication code (MAC)						
	☐ Ja	Protocol				
		Algoritme				

		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Productie-interface Proxy						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					

Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Ontwerpregel 164: *Data-at-rest dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-at-rest
☐ Data-at-rest hoeft niet te worden beschermd

Informatie data store

Harddisk Forward Proxy							
BIV-rating van de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encryptie							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encrypte ☐ Field encryptie						
Encryptie							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						
Versleuteling van backup van data	☐ Ja ☐ Nee						
Message authentication code (MAC)							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						

Informatie data store							
Harddisk managementstation							
BIV-rating van de data in de data store	B		I		V		
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encrypte							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encrypte ☐ Field encryptie						
Encryptie							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						
Versleuteling van backup van data	☐ Ja ☐ Nee						
Message authentication code (MAC)							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						

3.7.6 Reverse proxy

Ontwerpregel 165: *Connecties die vanuit de zone extern richting de zone intern worden geïnitieerd dienen te verlopen via een Reverse Proxy functionaliteit. Dit geldt zowel voor U2M- als M2M-communicatie.*

Ontwerpregel 166: *Data-in-transit dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-in-transit
☐ Data-in-transit hoeft niet te worden beschermd.

Managementinterface Reverse Proxy						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
	☐ Ja	Protocol				
		Algoritme Versie Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
Message authentication code (MAC)						
	☐ Ja	Protocol Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
	☐ Ja	Protocol Algoritme Versie				
		Key lengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					

Productie-interface Reverse Proxy						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				

		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme Versie Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol Algoritme	
		Versie Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol Algoritme	
		Versie Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Ontwerpregel 167: *Data-at-rest dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-at-rest
☐ Data-at-rest hoeft niet te worden beschermd

Informatie data store							
Hard disk Reverse Proxy							
BIV-rating van de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encrypte							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encryptie ☐ Field encryptie						
Encryptie							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						
Versleuteling van backup van data	☐ Ja ☐ Nee						
Message authentication code (MAC)							

	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

3.7.7 E-mail Proxy

Ontwerpregel 168: *Leverancier, hardware en software zijn bekend in de markt.*

Ontwerpregel 169: *Producten hebben zich bewezen.*

Ontwerpregel 170: *Systemen evolueren mee in functionaliteit met de huidige stand van de techniek en spelen ook in op trends op het gebied van dreiging versus beveiliging.*

Ontwerpregel 171: *SAAS is een pré, maar on premise of hybride uitvoeringen zijn zeker mogelijk afhankelijk van de functionaliteiten.*

Ontwerpregel 172: *Een (virtuele) appliance heeft de voorkeur boven server software installatie op een OS.*

Ontwerpregel 173: *Virtuele appliances zijn niet mogelijk in de DMZ-zone on premise bij PNB.*

Ontwerpregel 174: *Server software moet passen op Windows Server 2012.*

Ontwerpregel 175: *Als voor opslag een externe database wordt gebruikt zijn dat MS SQL Server of Oracle.*

Ontwerpregel 176: *Centraal management met een grafische interface.*

Ontwerpregel 177: *Eenvoudig schaalbaar systeem.*

Ontwerpregel 178: *Verwerkingseenheden kunnen redundant worden uitgevoerd om uitval te verkleinen.*

Ontwerpregel 179: *Op afstand beheerbaar via een internet browser (IE, Firefox of Chrome).*

Ontwerpregel 180: *Microsoft Active Directory integratie.*

Ontwerpregel 181: *Gescheiden management interface is een pré.*

Ontwerpregel 182: *Supportdesk functionaliteiten vanuit het systeem is een pré (helpdesk tooling).*

Ontwerpregel 183: *Support en ondersteuning van de leverancier.*

Ontwerpregel 184: *Filteren van spam, phishing en commercial bulk berichten.*

Ontwerpregel 185: *URL filtering.*

Ontwerpregel 186: *Gescheiden filtermogelijkheden o.b.v. in-, uitgaande en interne e-mail.*

Ontwerpregel 187: *Antivirus/antimalware scan.*

Ontwerpregel 188: *Uitgebreide mogelijkheden tot instellen van beveiligingsprotocollen zoals SPF, DKIM en DMARC.*

Ontwerpregel 189: *Uitgebreide mogelijkheden om handmatig policies aan te maken voor de verwerking van e-mail.*

Ontwerpregel 190: *Mogelijkheid om berichten te filteren diverse onderdelen van de e-mail.*

Ontwerpregel 191: *Mogelijkheid om berichten te filteren op bestandsbijlagen.*

Ontwerpregel 192: *Self service voor gebruikers.*

Ontwerpregel 193: *Notificatiemogelijkheden voor beheerders en gebruikers.*

Ontwerpregel 194: *Mogelijkheid om e-mail versleuteld te versturen en om dit mogelijk af te dwingen.*

Ontwerpregel 195: *Rewriting op e-mail.*

Ontwerpregel 196: *Spamreport voor de gebruiker is een pré.*

Ontwerpregel 197: *URL-wrap voor verdachte URL's is een pré.*

Ontwerpregel 198: *Sanboxen of realtime scanning van URL's en/of uitvoerbare bestanden is een pré.*

Ontwerpregel 199: *Uitgebreide log- en rapportagetooling.*

Ontwerpregel 200: *Data-in-transit dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-in-transit
☐ Data-in-transit hoeft niet te worden beschermd.

Management-interface beheertool						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
Message authentication code (MAC)						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Key lengte				
		Certificaat	☐ Self-signed ☐ Trusted source			
	☐ Niet vereist					

Management-interface Proxy [connectie met beheertool]						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					
Encryptie						
	☐ Ja	Protocol				
		Algoritme				
		Versie				
		Sleutellengte				

		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Productie-interface Proxy						
BIV-rating van de data die door de interface gaat	B	t.b.d	I	t.b.d.	V	t.b.d.
Type verkeer	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)					

Encryptie			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Message authentication code (MAC)			
	☐ Ja	Protocol	
		Algoritme	
		Versie	
		Sleutellengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
	☐ Ja	Protocol	
		Algoritme	
		Versie	

		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

Ontwerpregel 201: *Data-at-rest dient op de volgende manier te worden beschermd:*

[Dit onderdeel wordt verder vormgegeven in het kader van PKI i.v.m. keuzen encryptie]

Data-at-rest
☐ Data-at-rest hoeft niet te worden beschermd

Informatie data store							
Harddisk Proxy							
BIV-rating van de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encrypte							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encryptie ☐ Field encryptie						
Encryptie							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						
Versleuteling van backup van data	☐ Ja ☐ Nee						
Message authentication code (MAC)							
	☐ Ja	Protocol					
		Algoritme					
		Versie					
		Key lengte					
		Certificaat	☐ Self-signed ☐ Trusted source				
	☐ Niet vereist						

Informatie data store							
Harddisk managementstation							
BIV-ratin gvan de data in de data store	B	t.b.d	I	t.b.d.	V	t.b.d.	
Type data	☐ Authenticatie-informatie ☐ Overige data (e.g. configuratie data)						
Niveau encrypte							
Type data encryptie	☐ Disk encryptie ☐ File encryptie ☐ Tabel encrypte ☐ Field encryptie						
Encryptie							
Encryptie van data-at-rest	☐ Ja	☐ Component level					
		Protocol					
		Algoritme					
		Versie					
		Key lengte					

		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		
Versleuteling van backup van data	☐ Ja ☐ Nee		
Message authentication code (MAC)			
MAC van data-at-rest	☐ Ja	☐ Component level	
		Protocol	
		Algoritme	
		Versie	
		Key lengte	
		Certificaat	☐ Self-signed ☐ Trusted source
	☐ Niet vereist		

3.7.8 DLP onprem

Ontwerpregel 202: *Data Leakage (Lost) Prevention dient te worden toegepast voor de meest cruciale onprem systemen (i.e. SAP, Corsa, MS File servers, E-mail).*

Ontwerpregel 203: *Data Leakage (Lost) Prevention mag deel uitmaken van de forward proxy omgeving.*

Ontwerpregel 204: *Data Leakage (Lost) Prevention mag deel uitmaken van de email proxy.*

Ontwerpregel 205: *Data Leakage (Lost) Prevention dient te voorzien in integratiemogelijkheden met DLP-componenten in de cloud.*

3.8 Security cloudniveau

3.8.1 Mail proxy

Ontwerpregel 206: *Met uitzondering van fysieke onprem-afmetingen gelden dezelfde functies/eisen zoals beschreven bij de onprem-componenten. Zie hiervoor paragraaf 3.7.7.*

Ontwerpregel 207: *De e-mail proxy dient te voorzien in integratiemogelijkheden met onprem mail proxy (hybride oplossing).*

3.8.2 DLP

Ontwerpregel 208: *Data Leakage (Lost) componenten kunnen op een gebruiksvriendelijke wijze middels een GUI worden geconfigureerd.*

Ontwerpregel 209: *Data Leakage (Lost) componenten dienen te voorzien in integratiemogelijkheden met onprem Data Leakage (Lost) componenten (hybride oplossing).*

3.8.3 Forward proxy

Ontwerpregel 210: *Met uitzondering van fysieke onprem-afmetingen gelden dezefde functies/eisen zoals beschreven bij de onprem-componenten. Zie hiervoor paragraaf 3.7.5.*

Ontwerpregel 211: *De forward proxy dient te voorzien in integratiemogelijkheden met de onprem forward proxy (hybride oplossing).*

3.8.4 Visibility

Ontwerpregel 212: *Het dient mogelijk te zijn om op een eenvoudige manier middels een GUI inzicht te krijgen in het applicatielandschap zoals dat is aangebracht in de cloud (e.g.: gebruik van diensten geleverd door een CASB-provider).*

Ontwerpregel 213: *Het dient mogelijk te zijn om op een eenvoudige manier middels een GUI inzicht te krijgen in gebruikersstatistieken. Traceerbaarheid van personen/gebruikers die online toepassingen hebben benut is hierbij een vereiste (e.g.: gebruik van diensten geleverd door een CASB-provider).*

Ontwerpregel 214: *Het dient mogelijk te zijn om op een eenvoudige manier middels een GUI inzicht te krijgen in device-statistieken. Traceerbaarheid van de type devices en locatiebepalingen waarmee/waarvandaan toegang tot applicaties is verschaft is hierbij een vereiste (e.g.: gebruik van diensten geleverd door een CASB-provider).*

3.8.5 Threat protection

Ontwerpregel 215: *Het dient mogelijk te zijn ongewenste gebruikers, devices en versies van toepassingen de toegang tot cloud services te ontzeggen middels adaptive access controls (e.g.: gebruik van diensten geleverd door een CASB-provider).*

Ontwerpregel 216: *Het dient mogelijk te zijn verdachte patronen van gebruikers en devices eenvoudig te kunnen achterhalen middels user and entity behaviour analytics (e.g.: gebruik van diensten geleverd door een CASB-provider).*

Ontwerpregel 217: *Malware identificatie en (automatisch) herstel (remediation) dient mogelijk te zijn (e.g.: gebruik van diensten geleverd door een CASB-provider).*

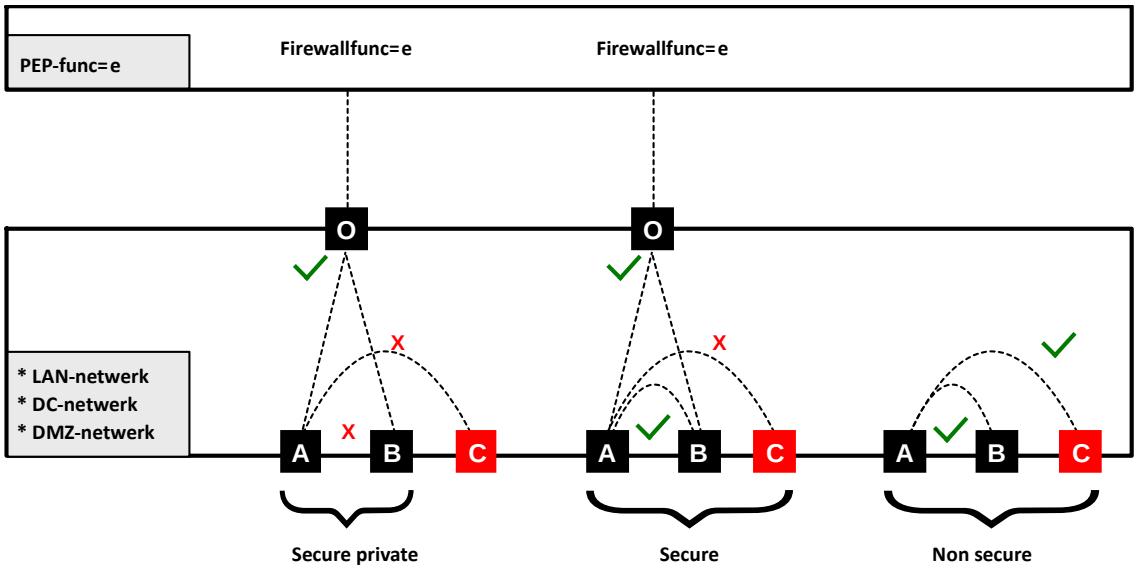
3.8.6 Compliance

Ontwerpregel 218: *Vigerende wet- en regelgeving, al dan niet opgelegd door externe (overheids)organisaties, zijn ook van toepassing op data in de cloud.*

Ontwerpregel 219: *Alvorens data in de cloud onder te brengen, dient voor de betreffende data bekeken te worden of en zo ja op welke wijze deze conform vigerende wet- en regelgeving kan worden ondergebracht in de cloud.*

3.9 Communicatiemodellen

Binnen het netwerk van PNB worden verschillende communicatiemodellen onderkend. Dit geldt voor het LAN-netwerk, het DC-netwerk en het DMZ-netwerk. In figuur 3-5 zijn deze modellen conceptueel afgebeeld.



A = Access Poort

O = Ontsluitende poort

Figuur 3-5: *Communicatiemodellen PNB*

Ontwerpregel 220: *Het netwerk van PNB dient te voorzien in een model Secure private, waarbij host isolation kan worden toegepast. Communicatie tussen hosts in hetzelfde segment en met hosts in een ander segment dient door een firewallfunctie te worden gereguleerd.*

Ontwerpregel 221: *Het netwerk van PNB dient te voorzien in een model Secure, waarbij communicatie tussen hosts in hetzelfde segment is toegestaan. Communicatie met hosts in een ander segment dient door een firewallfunctie te worden gereguleerd.*

Ontwerpregel 222: *Het netwerk van PNB dient te voorzien in een model None Secure, waarbij communicatie tussen hosts in hetzelfde segment en met hosts in een ander segment is toegestaan zonder de tussenkomst van een firewallfunctie.*

Ontwerpregel 223: *Serversystemen dienen te zijn voorzien van een softwarematige firewall (host based firewalling) in het kader van 'security zo dicht mogelijk bij de bron'.*

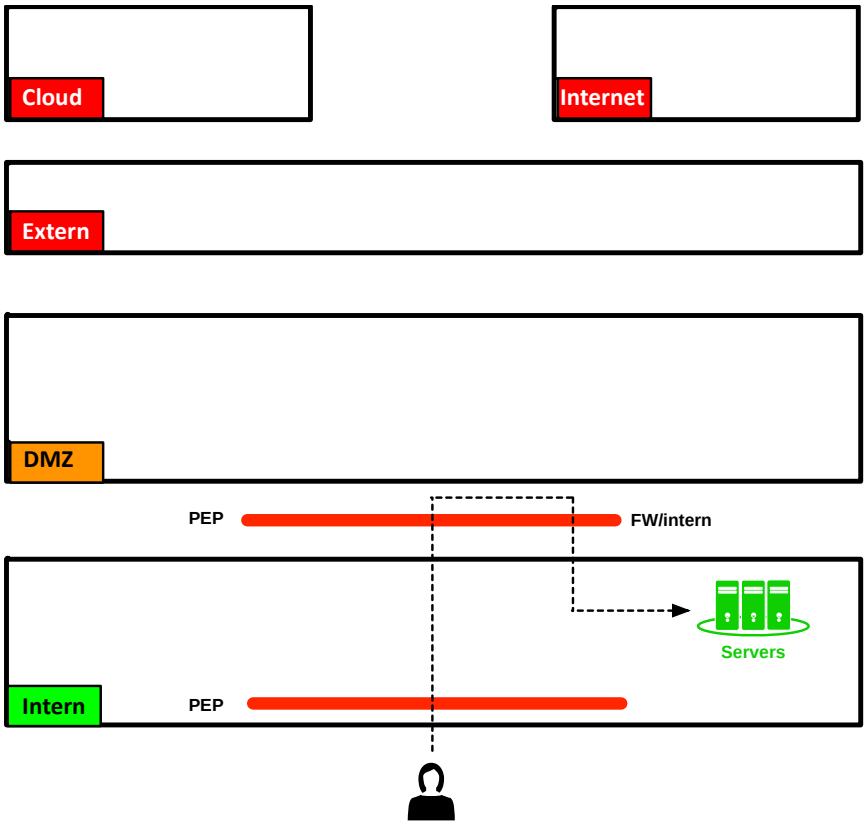
3.10 Communicatiestromen PNB/U2M

In deze paragraaf zijn communicatiestromen afgebeeld die zich kunnen voordoen met betrekking tot de PNB-omgeving. De communicatiestromen zijn op hoofdlijnen afgebeeld; hybride vormen zijn niet opgenomen. Dit laat onverlet dat hybride vormen van cloud proxies, e-mail proxies, e-mailsystemen (onprem/online) of een combinatie daarvan wel degelijk mogelijk zijn. Op grond van de op dat moment gangbare uitgangspunten en stand van zaken zal tijdens het schrijven van afgeleide documenten zoals High Level Designs hiermee rekening gehouden moeten worden. De illustraties in deze paragraaf dienen derhalve te worden beschouwd als algemene richtlijnen op het gebied van Policy Enforcement Points. Ook de uitwerking van Policy Enforcement Points zal in afgeleide documentatie moeten worden geconcretiseerd op basis van de architectuureisen voor betreffende PEP-functies zoals opgenomen in deze architectuurblauwdruk. Voor iedere use case kunnen, zo niet moeten immers andere PEP-functies worden ingezet.

3.10.1 Use case 1: onprem -> onprem

Gebruikssituaties onder meer:

- Corsa (raadpleging en registratie),
- SAP,
- File servers.



Figuur 3-6: *Communicatie U2M/onprem -> onprem*

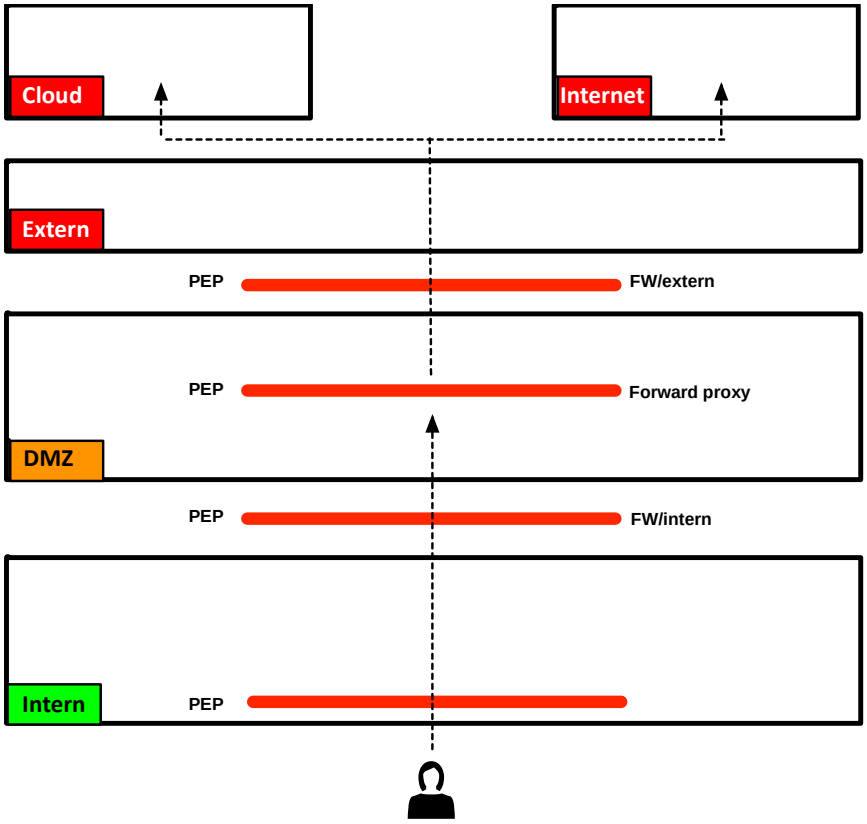
Ontwerpregel 224: *U2M/onprem -> onprem: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern -> onprem servers.*

Ontwerpregel 225: *U2M/onprem -> onprem: Serversystemen zijn afgeschermd door de FW/intern die het verkeer reguleert tussen gebruikers en serversystemen.*

3.10.2 Use case 2: onprem -> cloud/internet (1)

Gebruikssituaties (onprem forward proxy):

- Cloudapplicaties (e.g.: O365),
- Informatieverzameling. E.g.:
  - onderzoek/raadplegen openbare bronnen,
  - kappitel (daisy),
  - BRP-gegevens,
- I-babs,
- Formdesk,
- Internetbrowsen.



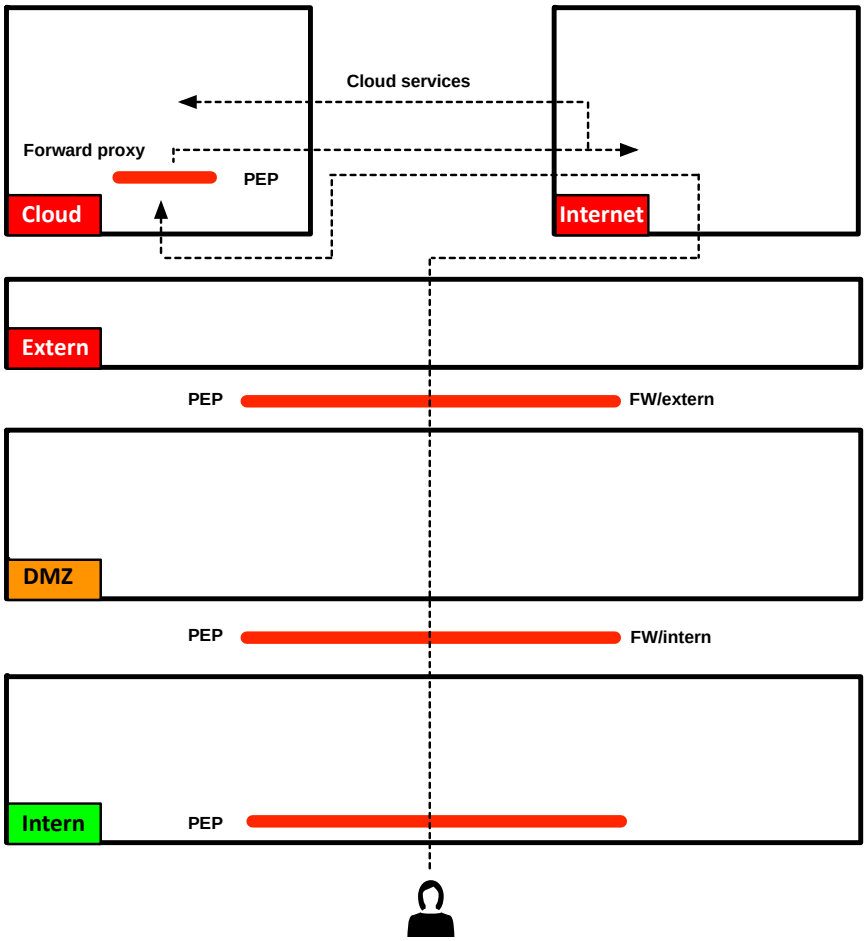
Figuur 3-7: *Communicatie U2M/onprem -> cloud/internet*

Ontwerpregel 226: *U2M/onprem -> cloud/internet: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern), forward proxy onprem, FW/extern.*

3.10.3 Use case 2: onprem -> cloud/internet (2)

Gebruikssituaties (cloud forward proxy):

- Cloudapplicaties (e.g.: O365),
- Informatieverzameling. E.g.:
  - onderzoek/raadplegen openbare bronnen,
  - kappitel (daisy),
  - BRP-gegevens,
- I-babs,
- Formdesk,
- Internetbrowsen.



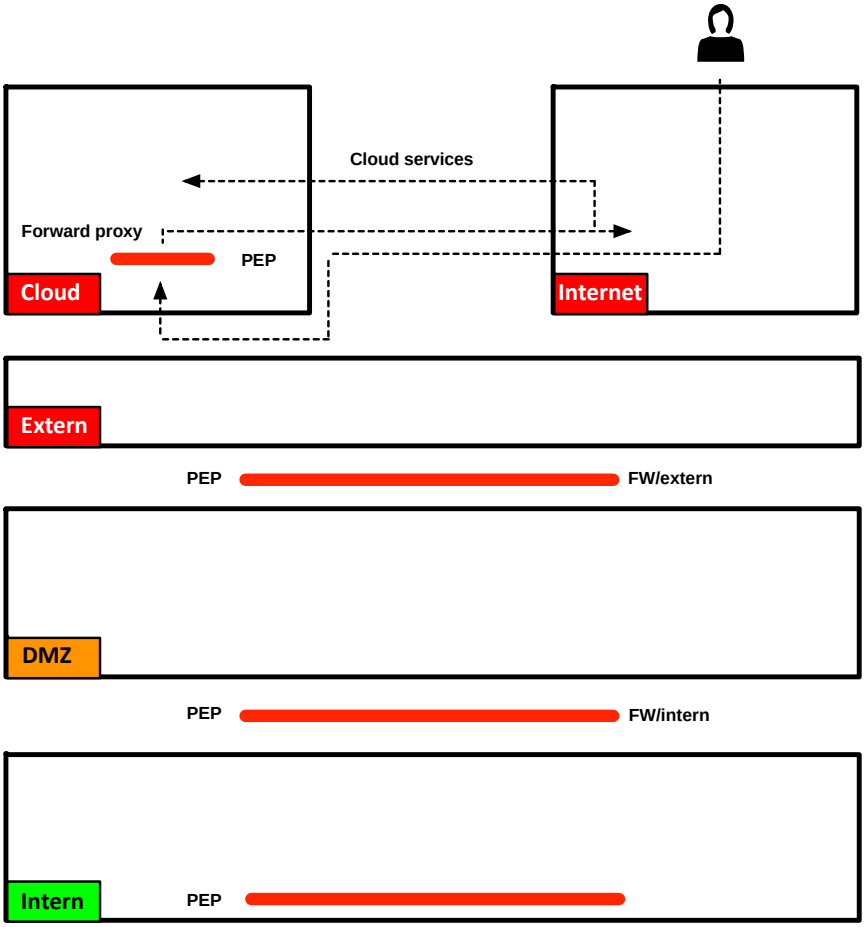
Figuur 3-8: *Communicatie U2M/onprem -> cloud/internet*

Ontwerpregel 227: *U2M/onprem -> cloud/internet: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern, FW/extern, forward proxy cloud -> internet | cloud services.*

3.10.4 Use case 2: onprem -> cloud/internet (3)

Gebruikssituaties (cloud forward proxy):

- Cloudapplicaties (e.g.: O365),
- Informatieverzameling. E.g.:
  - onderzoek/raadplegen openbare bronnen,
  - kappitel (daisy),
  - BRP-gegevens,
- I-babs,
- Formdesk,
- Internetbrowsen.



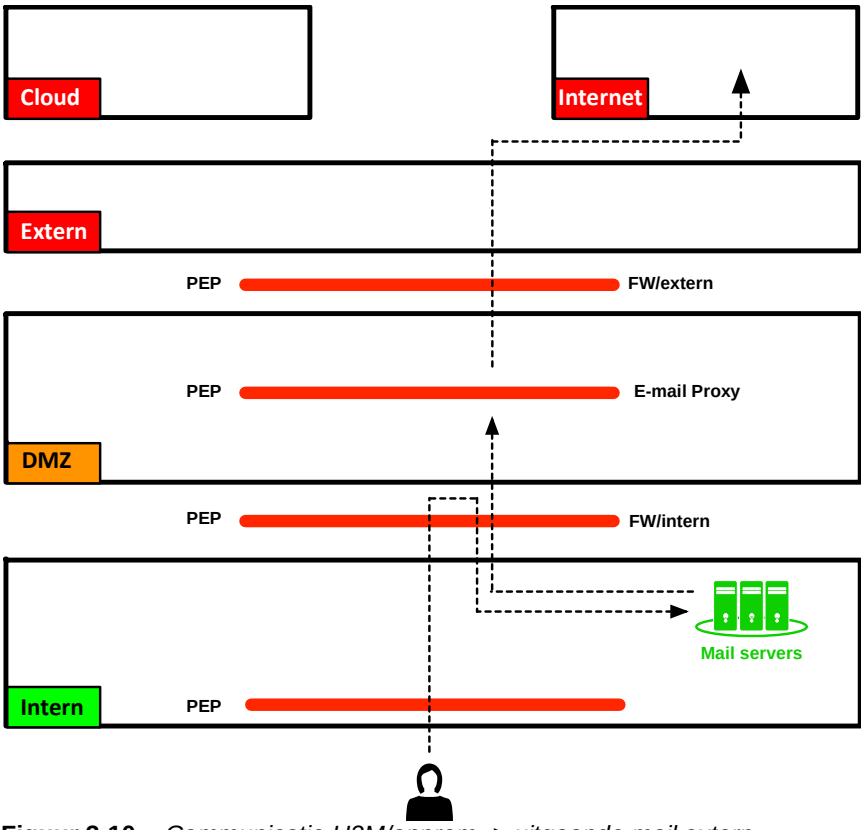
Figuur 3-9: *Communicatie U2M/cloud -> cloud/internet*

Ontwerpregel 228: *U2M/cloud -> cloud/internet: Communicatie dient te verlopen middels de PEP-functies forward proxy cloud -> internet | cloud services.*

3.10.5 Use case 3: onprem -> uitgaande mail (1)

Gebruikssituaties (onprem e-mail proxy, onprem mail servers):

- Mail boxes onprem -> externe mail derde partijen.



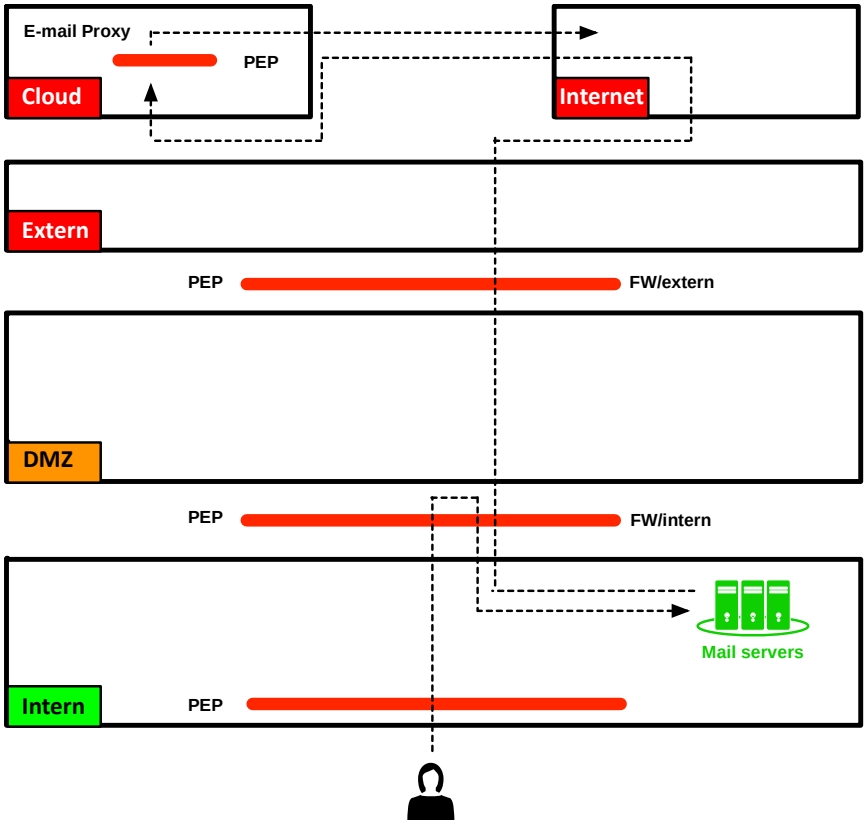
Figuur 3-10: *Communicatie U2M/onprem -> uitgaande mail extern*

Ontwerpregel 229: *U2M/onprem -> uitgaande mail: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern, e-mail proxy onprem, FW/extern -> externe mail servers.*

3.10.6 Use case 3: onprem -> uitgaande mail (2)

Gebruikssituaties (cloud e-mail proxy, onprem mail servers):

- Mailboxes onprem -> externe mail derde partijen.



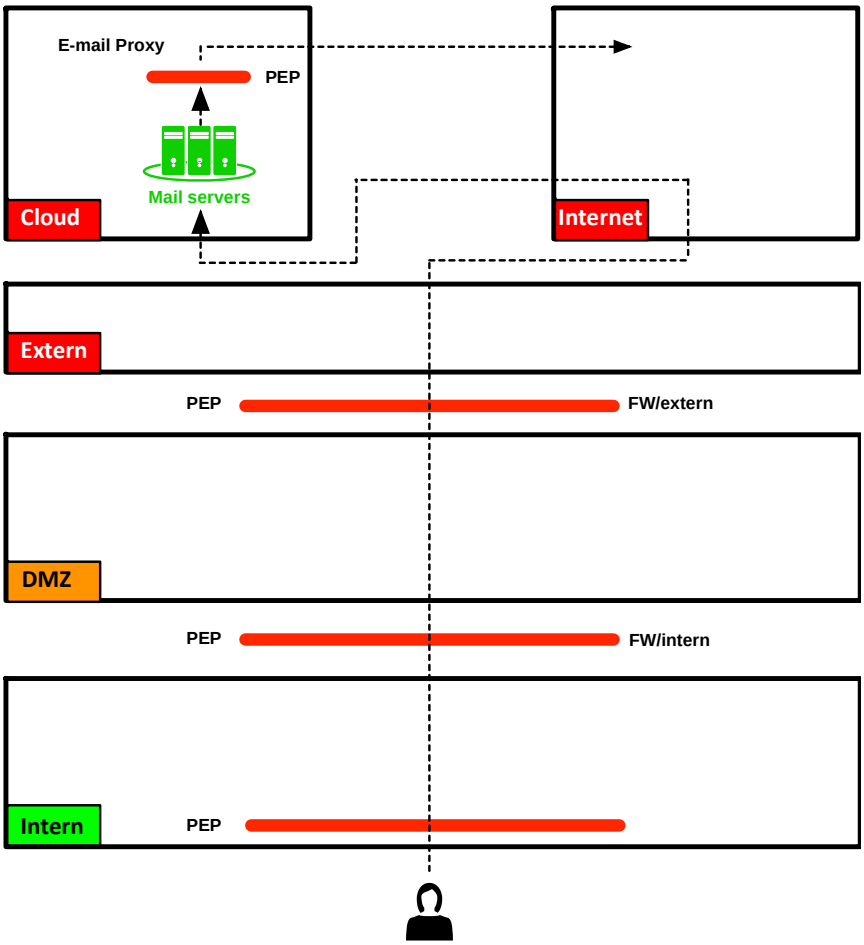
Figuur 3-11: *Communicatie U2M/onprem -> uitgaande mail extern*

Ontwerpregel 230: *U2M/onprem -> uitgaande mail: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern, FW/extern, e-mail proxy cloud -> externe mail servers.*

3.10.7 Use case 3: cloud -> uitgaande mail (3)

Gebruikssituaties (cloud e-mail proxy, cloud mail servers):

- Mailboxes cloud -> externe mail derde partijen.



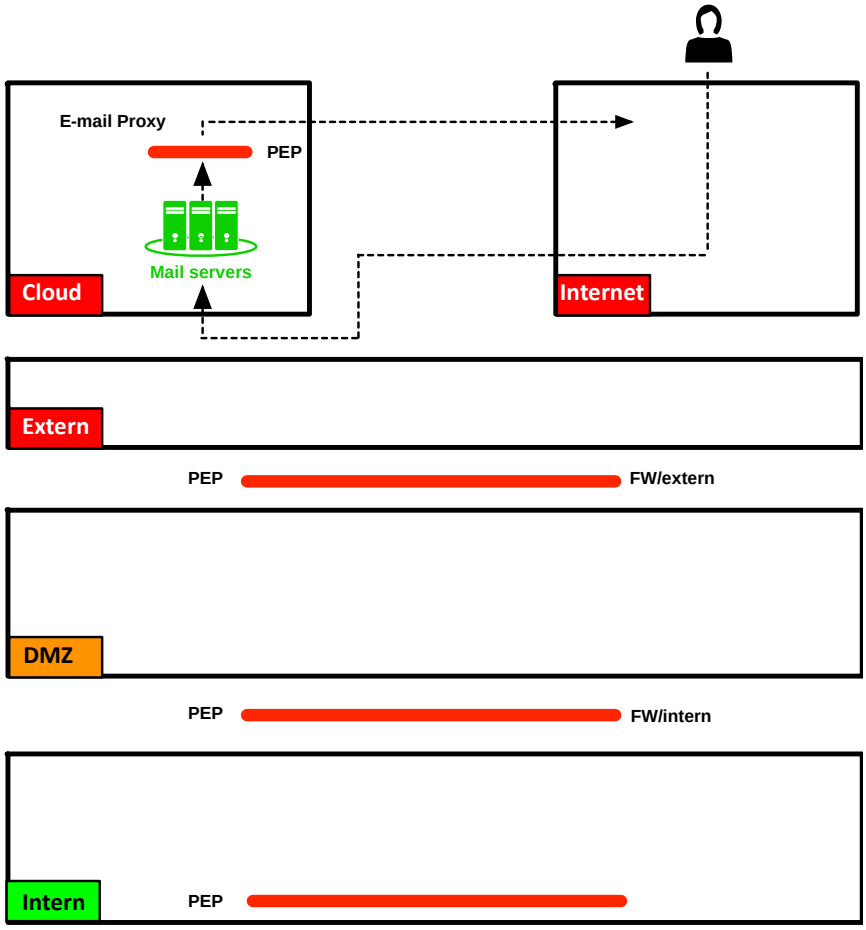
Figuur 3-12: *Communicatie U2M/cloud -> uitgaande mail extern*

Ontwerpregel 231: *U2M/cloud -> uitgaande mail: Communicatie dient te verlopen middels de PEP-functies NAC, FW/intern, FW/extern, e-mail proxy cloud -> externe mail servers.*

3.10.8 Use case 3: cloud -> uitgaande mail (4)

Gebruikssituaties (cloud e-mail proxy, cloud mail servers):

- Mailboxes cloud -> externe mail derde partijen.



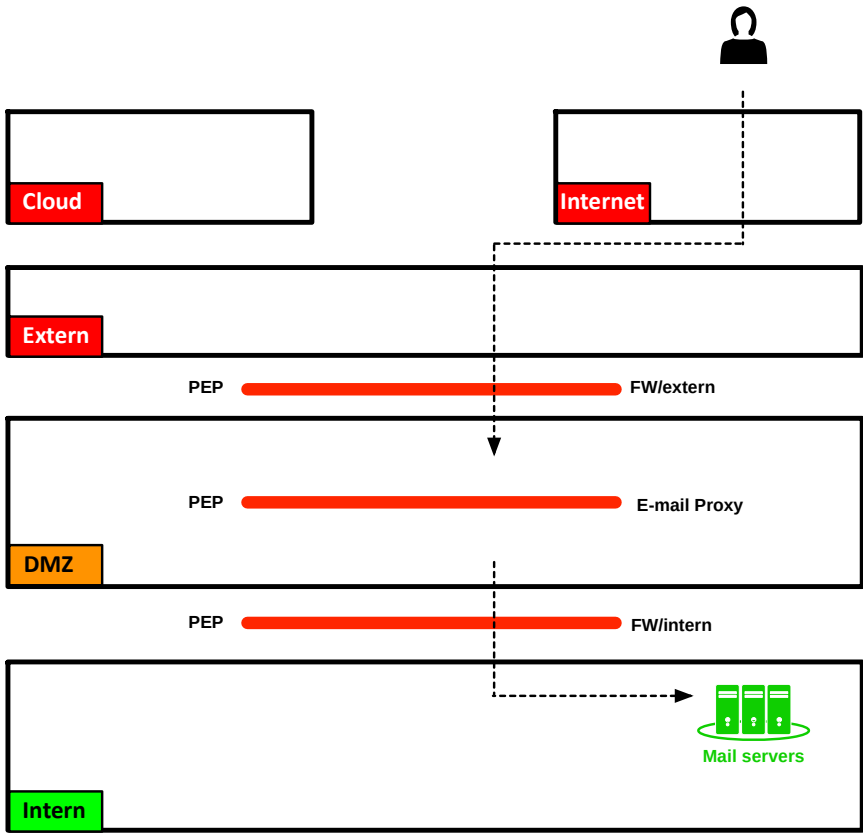
Figuur 3-13: *Communicatie U2M/cloud -> uitgaande mail extern*

Ontwerpregel 232: *U2M/cloud -> uitgaande mail: Communicatie dient te verlopen middels de PEP-functies e-mail proxy cloud -> externe mail servers.*

3.10.9 Use case 4: Inkomende mail -> onprem (1)

Gebruikssituaties (onprem e-mail proxy, onprem mail servers):

- Inkomende mail afkomstig van derde partijen,



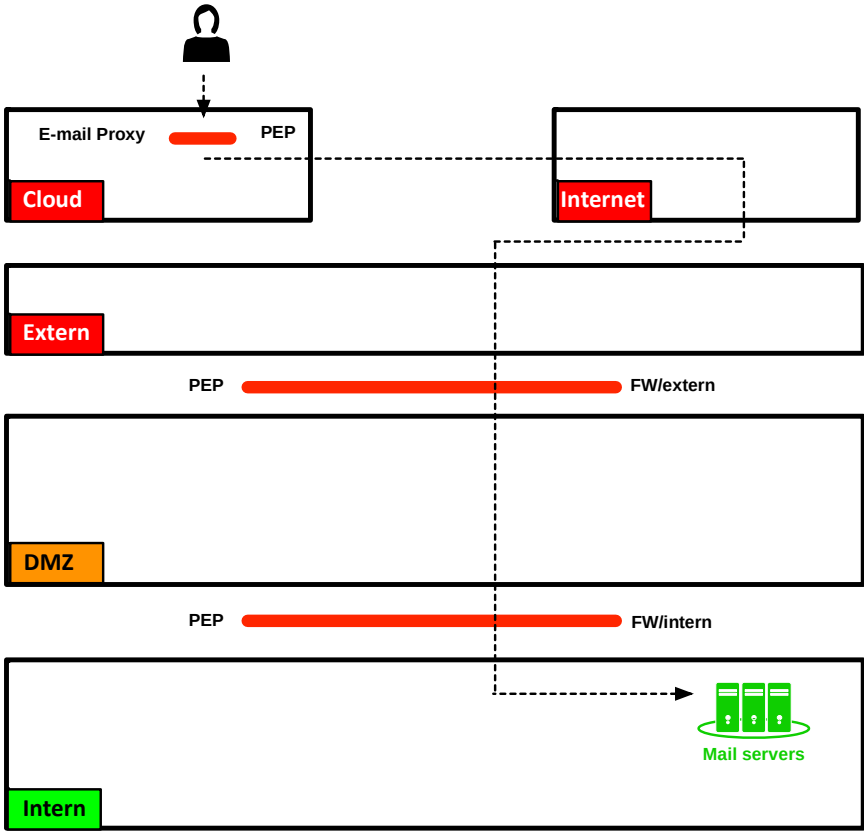
Figuur 3-14: *Communicatie U2M/inkomende mail -> onprem*

Ontwerpregel 233: *U2M/onprem -> inkomende mail: Communicatie dient te verlopen middels de PEP-functies FW/extern, e-mail proxy onprem, FW/intern -> interne mailservers.*

3.10.10 Use case 4: Inkomende mail -> onprem (2)

Gebruikssituaties (cloud e-mail proxy, onprem mail servers):

- Inkomende mail afkomstig van derde partijen,



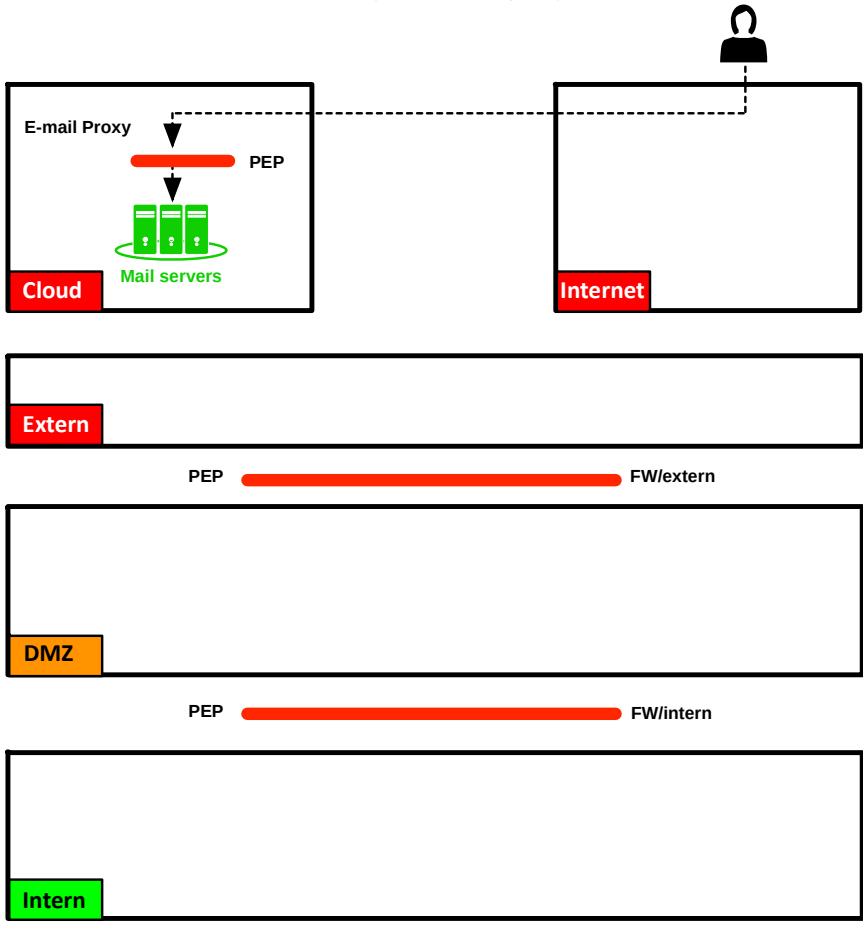
Figuur 3-15: *Communicatie U2M/inkomende mail -> onprem*

Ontwerpregel 234: *U2M/onprem -> inkomende mail: Communicatie dient te verlopen middels de PEP-functies e-mail proxy cloud, FW/extern, FW/intern -> interne mailservers.*

3.10.11 Use case 4: Inkomende mail -> onprem (3)

Gebruikssituaties (cloud e-mail proxy, cloud mail servers):

- Inkomende mail afkomstig van derde partijen



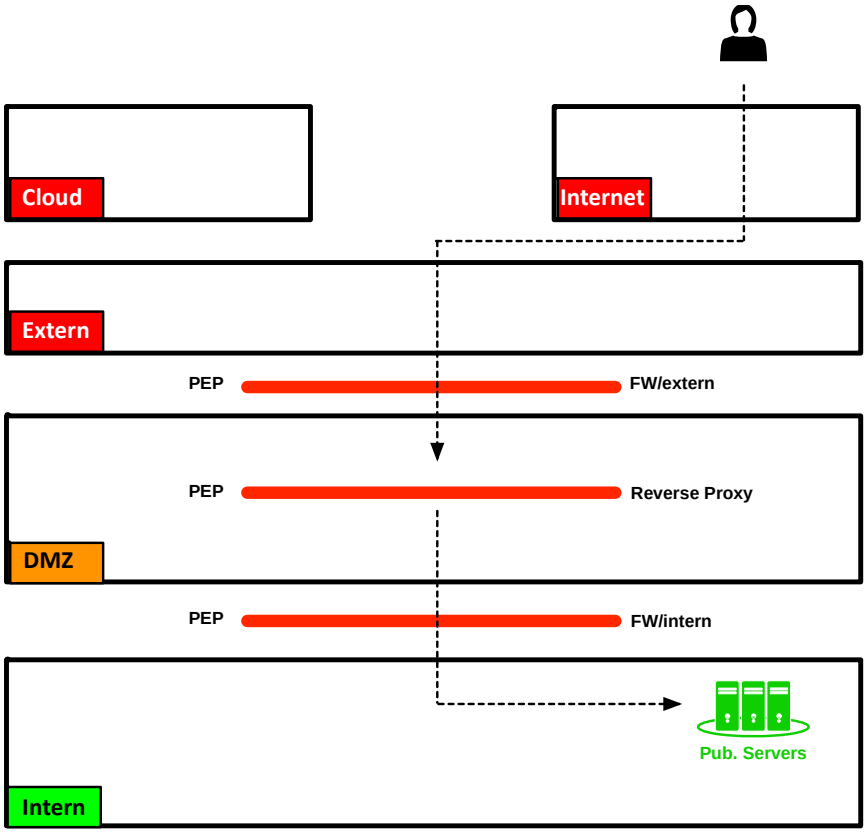
Figuur 3-16: *Communicatie U2M/inkomende mail -> cloud*

Ontwerpregel 235: *U2M/cloud -> inkomende mail: Communicatie dient te verlopen middels de PEP-functies e-mail proxy cloud ->interne mailservers.*

3.10.12 Use case 5: Reverse Proxy

Gebruikssituaties:

- Toegang door PNB gepubliceerde diensten.



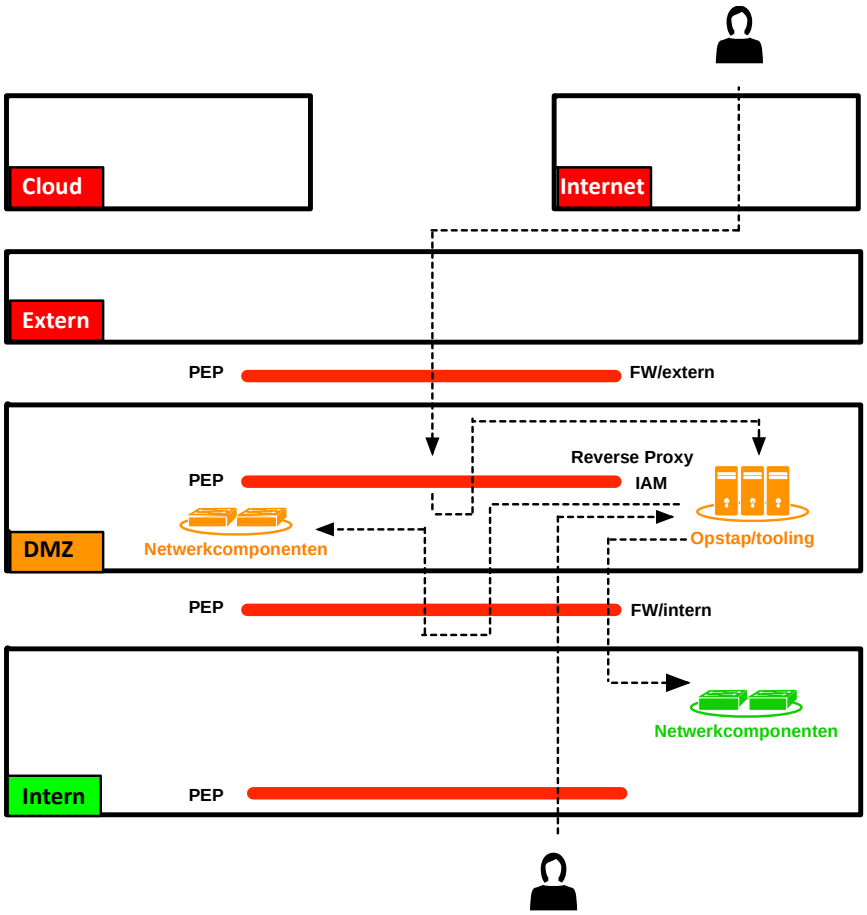
Figuur 3-17: *Communicatie U2M//reverse proxy*

Ontwerpregel 236: *U2M/reverse proxy: Communicatie dient te verlopen middels de PEP-functies FW/extern, reverse proxy, FW/intern -> gepubliceerde diensten.*

3.10.13 Use case 6: Beheer

Gebruikssituaties:

- Toegang remote beheer (externe beheerorganisatie, interne beheerorganisatie),
- Toegang interne beheerorganisatie.



Figuur 3-18: *Communicatie U2M//beheer*

Ontwerpregel 237: *U2M/beheer remote: Communicatie dient te verlopen middels de PEP-functies FW/extern, reverse proxy, IAM-constructies opstap (2FA), workspace-toebedeling/tooling (RBAC).*

Ontwerpregel 238: *U2M/beheer intern: Communicatie dient te verlopen middels de PEP-functies NAC, FW/Intern, IAM-constructies opstapomgeving (2FA), workspace-toebedeling/tooling (RBAC).*

Ontwerpregel 239: *Managementsessies naar netwerkcomponenten dienen centraal vanaf de workspace/tooling-omgeving te worden geïnitieerd, waarbij communicatiestromen door de PEP-functies FW/Intern dienen te verlopen.*

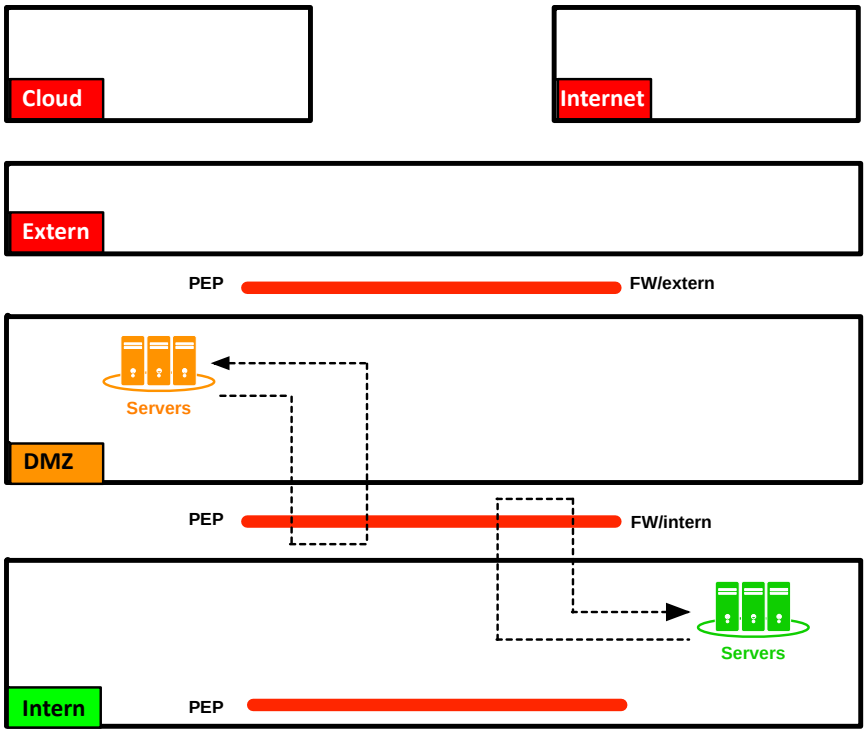
Ontwerpregel 240: *De toegangsrechten tot een netwerkcomponent worden middels NAC/device administration gereguleerd in de DMZ-omgeving (TACACS+omgeving, niet ingetekend).*

3.11 Communicatiestromen PNB/M2M

3.11.1 M2M/use case 1: onprem -> onprem binnen zone

Gebruikssituaties onder meer:

- Bizztalk, Corsa, SIS,
- Corsa, Fileserver Corsa, Xential servers, Corsa database,
- Exchange server, Exchange database.



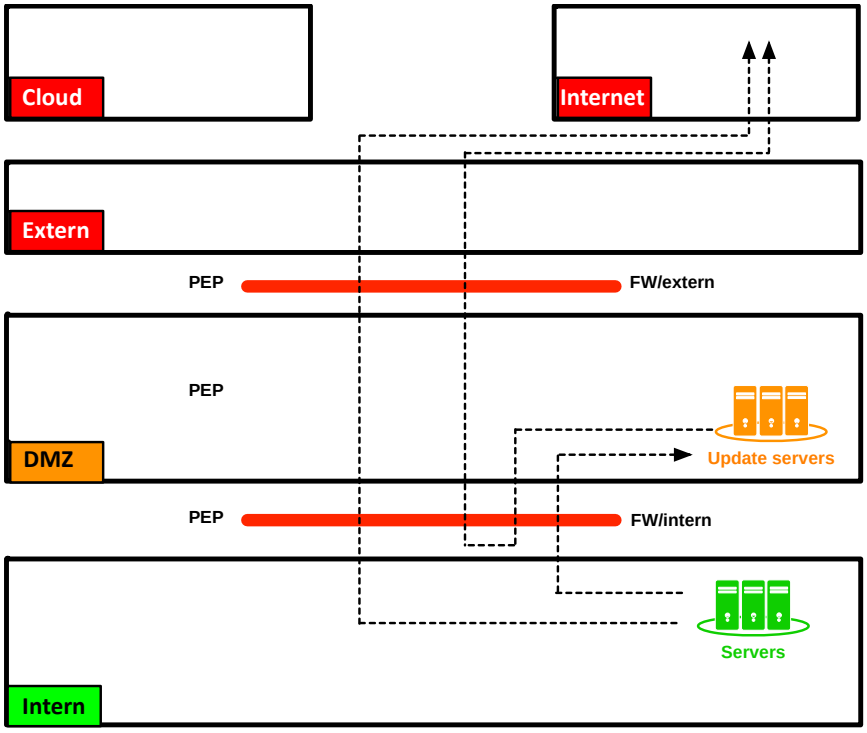
Figuur 3-19: *Communicatie M2M/onprem -> onprem (binnen zone)*

Ontwerpregel 241: *M2M/onprem -> onprem (binnen zone): Directe communicatie tussen serversystemen in hetzelfde segment en tussen verschillende segmenten is niet toegestaan zonder tussenkomst van de interne FW.*

3.11.2 M2M/use case 2: onprem -> onprem tussen zones

Gebruikssituaties onder meer:

- Windows update services.



Figuur 3-20: *Communicatie M2M/updateservers (tussen zones)*

Ontwerpregel 242: *M2M/onprem -> onprem (tussen zones): Het updaten van servers dient te geschieden middels updatefaciliteiten die zijn ondergebracht in de DMZ-omgeving. Deze updatefaciliteiten maken verbinding met updatefaciliteiten die middels het internet bereikbaar zijn. De PEP-functies die worden doorlopen zijn: FW/intern, updatefaciliteiten (intern), FW/extern -> updatefaciliteiten (extern).*

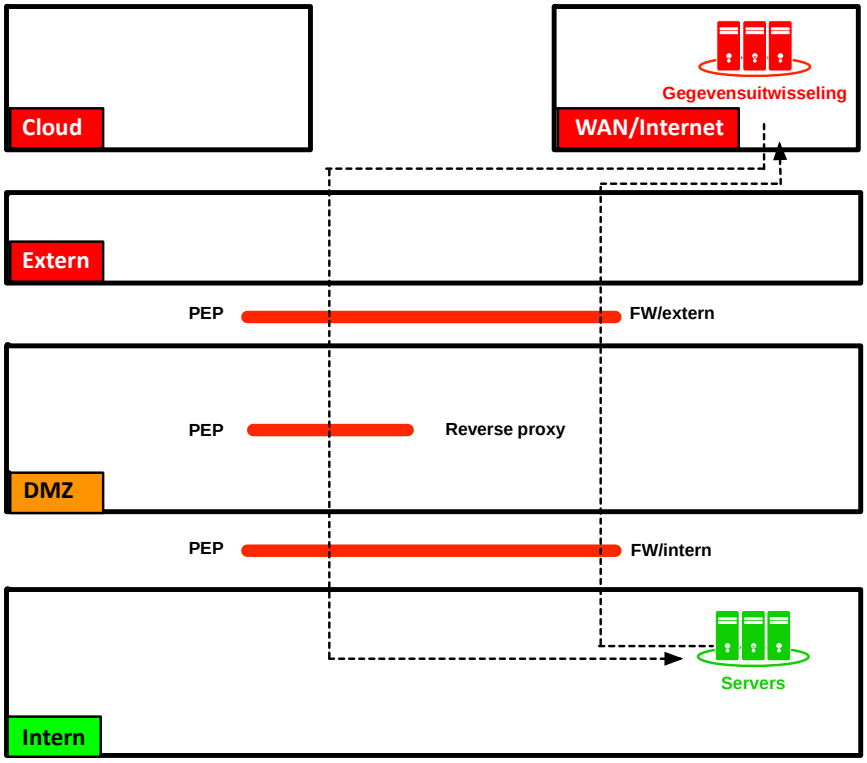
Ontwerpregel 243: *M2M/onprem -> onprem (tussen zones): Indien geen updatefaciliteiten beschikbaar zijn/bestaan voor bepaalde servers dienen deze servers middels de PEP-functies FW/intern FW/extern -> updatefaciliteiten (extern) de betreffende updates te downloaden.*

Ontwerpregel 244: *Uitgaande verbindingen, hetzij met hetzij zonder updatefaciliteiten (intern), dienen te worden beperkt tot alleen de voor communicatie noodzakelijke subnetten, poorten en services. Dit dient te worden afgedwongen op het niveau van de firewalls.*

3.11.3 M2M/use case 3: Gegevensuitwisseling

Gebruikssituaties:

- Gegevensuitwisseling overheidsinstanties.



Figuur 3-21: *Communicatie M2M/gegevensuitwisseling*

Ontwerpregel 245: *M2M/gegevensuitwisseling: Indien gegevens vanaf PNB-serversystemen dienen te worden geupload naar externe partijen (hetzij middels het WAN, hetzij middels het internet ontsloten) dienen de volgende PEP-functies te worden uitgevoerd: FW/intern, FW/extern -> externe overheidsorganisatie.*

Ontwerpregel 246: *M2M/gegevensuitwisseling: Indien gegevens naar PNB-serversystemen dienen te worden gedownload vanaf externe partijen (hetzij middels het WAN, hetzij middels het internet ontsloten) dienen de volgende PEP-functies te worden uitgevoerd: FW/extern, reverse proxy -> interne servers PNB.*

Ontwerpregel 247: *Verbindingen die vanaf externe partijen worden geïnitieerd in de richting van PNB dienen te worden getermineerd in de DMZ middels de reverse proxy.*

Ontwerpregel 248: *Gegevensuitwisseling vanaf/naar PNB dient op het niveau van het netwerk te worden beperkt tot alleen de voor communicatie noodzakelijke subnetten, poorten en services. Dit dient te worden afgedwongen op het niveau van de firewalls (inkomende/uitgaande sessies) en de reverse proxy (inkomende sessies).*

4 Appendix A: Overzicht ontwerpregels

4.1 Dataclassificatie

4.2 Zonering

4.3 Segmentatie

4.4 PKI

4.5 NAC

4.6 Mobile Application Management

4.7 Netwerk switch

4.8 Netwerk firewall

4.9 Forward proxy on prem

4.10 Reverse proxy

4.11 Mail scanning

4.12 DLP

4.13 Mail scanning cloud

4.14 DLP cloud

4.15 Forward proxy cloud

4.16 Visibility cloud

4.17 Threat protection cloud

4.18 Compliance cloud

4.19 Communicatiemodellen

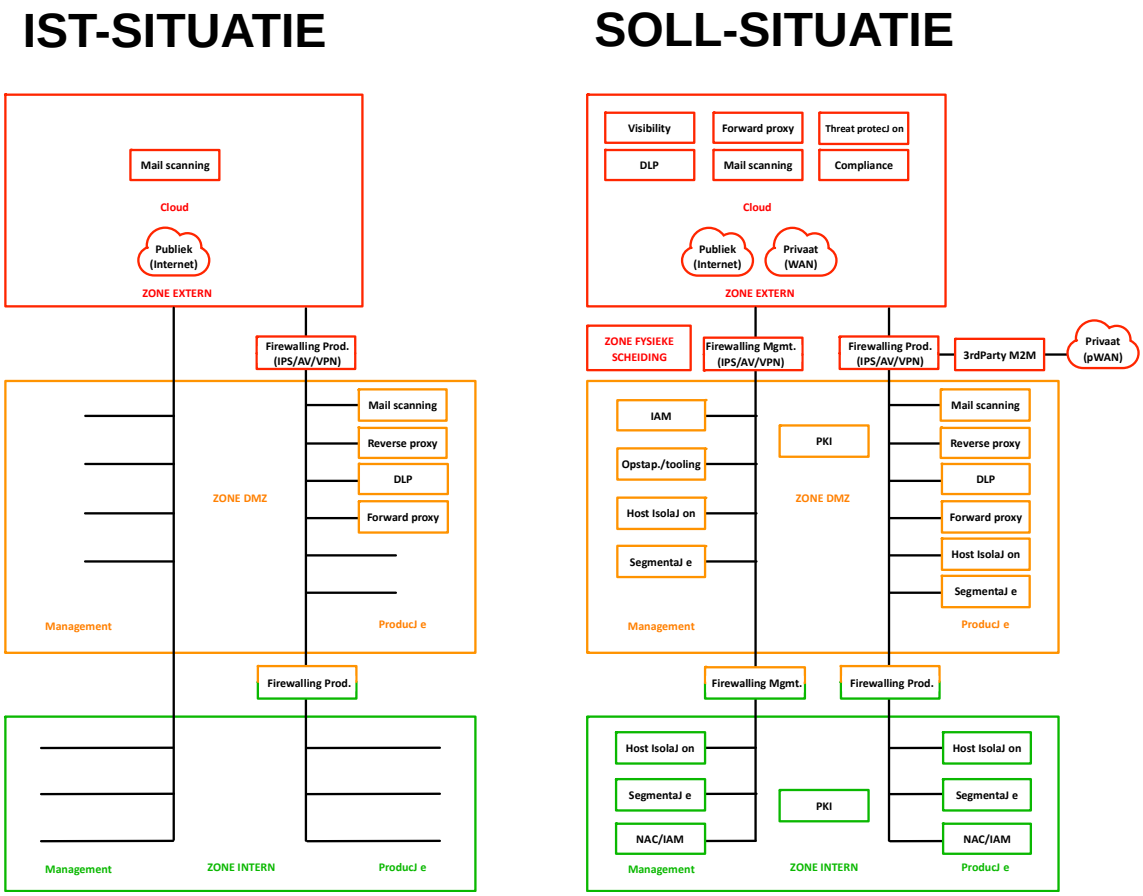
4.20 Communicatiestromen U2M

4.21 Communicatiestromen M2M

4.22 Migratie

5 Appendix A: IST/SOLL-situatie security-architectuur PNB

In de onderstaande illustratie zijn de IST-situatie (links) en SOLL-situatie (rechts) afgebeeld.



Figuur 5-1: *Migratie IST -> SOLL*

Ontwerpregel 249: *In afgeleide HLDs dient per functioneel bouwblok (of bouwblokken) op de hoofdlijn beschreven te worden op welke wijze vanuit de IST- de SOLL-situatie kan worden bereikt. Indien het betreffende topic 'dermate complex' is, kan een separaat migratiedesign worden geschreven dat de migratiestappen verder uitdiept.*