

Aansluitvoorwaarden NMA

v1.0 definitief

Maximale beschikbaarheid, beheerste veiligheid



Louis de Wolff

	Authorisatie	Naam	Datum	Paraaf
Opgesteld door	Technisch adviseur	Louis de Wolff	8 oktober 2019	
Goedgekeurd door	Configuratiebeheer	Johannes Bloemendaal	8 oktober 2019	
	CISO MET	Wim van Asperen	8 oktober 2019	
Vrijgegeven door	Asset manager NMA	Ron van Rijswijk	8 oktober 2019	

Document historie

Datum	Versie	Omschrijving
9 mei 2019	0.1	Eerste concept versie
26 september 2019	0.2	Diverse suggesties verwerkt en verbeteringen doorgevoerd.
8 oktober 2019	1.0	Eerste formele versie

Inhoud

Document historie	2
1 Inleiding	4
2 Procesflows	5
2.1 Procesflow netwerkaansluiting	5
2.2 Procesflow Interconnectie	6
2.3 Procesflow fysieke toegang tot de NMA kast	7
2.4 Procesflow aanbrengen applicatiebekabeling	8
3 Installatievoorwaarden	9
3.1 Inleiding	9
2.1 Fysieke toegang tot het netwerk	9
4 Regels voor het gebruik van NMA	11
4.1 Algemeen	11
4.2 Binnen het eigen VPN	11
4.3 Verkeer tussen VPN's van NMA	14
4.4 Verkeer naar externe (onveilige) netwerken	15
Bijlage 1 Device Specification form	16
Bijlage 2 Switchpoortaanvraag	18

1 Inleiding

Netwerk Metro Amsterdam (NMA) is een gemeentelijk datanetwerk bedoeld voor intern dataverkeer van de diverse organisatorische clusters van de gemeente Amsterdam. Het netwerk is opgezet vanuit Metro en Tram (Cluster Ruimte en Economie), maar kan ook door de andere clusters worden gebruikt.

NMA is technisch zo opgezet dat vele gebruikers naast elkaar eigen virtuele netwerken kunnen inrichten. Apparatuur die in zo'n virtueel netwerk wordt aangesloten, kan communiceren met alle apparatuur die van hetzelfde virtuele netwerk gebruik maakt. Ook verbindingen met apparatuur die tot een ander virtueel netwerk of een extern netwerk behoort is mogelijk, maar dient apart te worden ingeregeld.

NMA heeft een hoge standaard voor de beschikbaarheid, integriteit en vertrouwelijkheid van de data die over NMA wordt verstuurd. Om dit te kunnen garanderen zijn allerlei technische maatregelen in NMA genomen. Naast deze technische maatregelen zijn er ook een aantal procedurele maatregelen en regels die moeten worden gevolgd door de gebruikers van NMA.

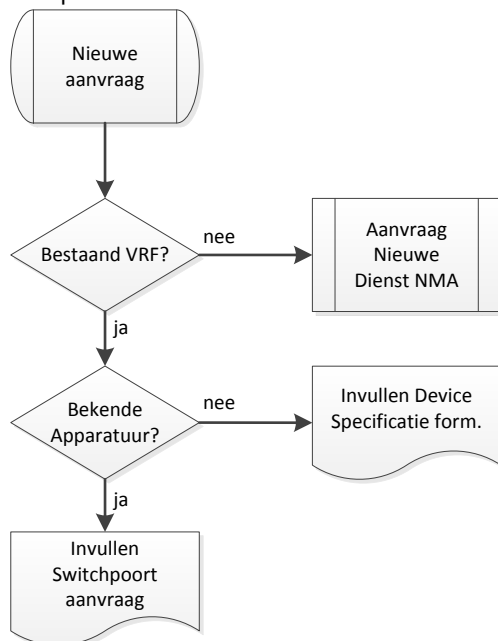
Dit document bevat de aansluitvoorwaarden van NMA. Een ieder die een aansluiting op NMA wenst zal voor de realisatie van zo'n aansluiting aan de in dit document geformuleerde procedures en regels moeten voldoen. Dit is nodig om de structuur en integriteit van het netwerk te behouden.

Hoofdstuk 2 bevat een toelichting op de processen die zijn opgesteld om aansluitingen naar NMA te realiseren. Hoofdstuk 3 bevat de installatietechnische voorwaarden voor een aansluiting op NMA. Hoofdstuk 4 bevat de regels voor het gebruik van NMA wanneer de aansluiting is gerealiseerd. In de bijlage wordt een voorbeeld gevonden van de aansluitformulieren voor NMA.

2 Procesflows

2.1 Procesflow netwerkaansluiting

Voor het realiseren van een nieuwe aansluiting op NMA dient de volgende procesflow te worden doorlopen:



Figuur 1 Procesflow netwerkaansluiting

Deze procesflow zorgt ervoor dat alle noodzakelijk details voor een aansluiting bekend worden. Globaal zijn de aanvragen in drie types te onderscheiden:

Geheel nieuwe dienst

Van een nieuwe dienst is sprake zodra er een apart Virtual Private Network (VPN) moet worden ingericht. Van een VPN is sprake zodra twee of meer gebruikers van NMA exclusief met elkaar willen communiceren over NMA. Het verkeer van een VPN is afgescheiden van de overige gebruikers van het netwerk.

VPN of VRF

Een Virtual Private Network (VPN) is de algemeen in de markt gangbare term voor een virtueel exclusief netwerk voor gebruikers. De technische implementatie in NMA is echter Virtual Routing and Forwarding (VRF)¹. Functioneel wordt hetzelfde bedoeld, echter binnen NMA wordt gesproken van een VRF als functioneel een VPN wordt bedoeld.

¹ Zie ook https://en.wikipedia.org/wiki/Virtual_routing_and_forwarding

Nieuwe apparatuur in een bestaande dienst

Indien een bestaande dienst nieuwe apparatuur² gaat inzetten (en daarmee gaat verbinden met een bestaand VPN), dan dient voor deze nieuwe apparatuur een Device Specification Form te worden ingevuld. Dit formulier specificeert de verkeersstromen van de nieuwe apparatuur. Met deze specificatie kan het netwerk worden geconfigureerd om op de diverse verkeersstromen de juiste Quality of Service markering te plaatsen zodat deze stromen correct in NMA worden afgehandeld.

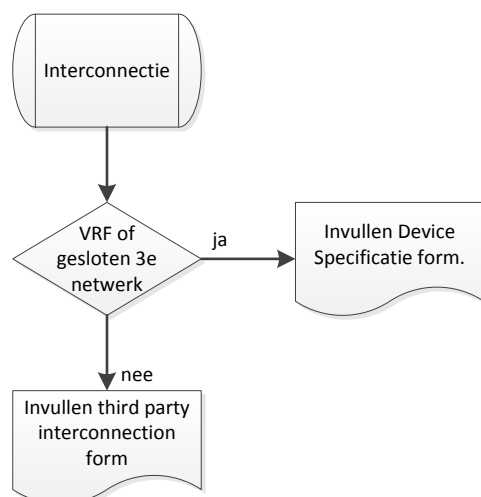
Bekende apparatuur aansluiten

Voor het aansluiten van bekende apparatuur heeft alleen een switchpoortaanvraag te worden ingevuld. Met dit formulier kan worden aangegeven waar de apparatuur wordt afgewerkt die aangesloten moet worden.

Een voorbeeld van deze formulieren kan worden gevonden in Bijlage 1 Device Specification form en Bijlage 2 Switchpoortaanvraag.

2.2 Procesflow Interconnectie

Apparatuur die in een VPN wordt aangesloten en daarmee binnen het NMA domein valt, kan een communicatiebehoefte hebben met apparatuur die zich in een ander VPN van NMA bevindt of met apparatuur die zich geheel buiten NMA bevindt. Voor dergelijke verbindingen dient het proces Interconnectie te worden gevolgd.



Figuur 2 Procesflow Interconnectie

Voor een interconnectie met apparatuur in een ander netwerk zijn er twee mogelijkheden: een gesloten netwerk van een derde of een extern (onveilig) netwerk. Het verschil tussen beide kwalificaties is de wijze waarop de interconnectie tussen NMA en het derde netwerk tot stand wordt gebracht. Een extern (onveilig) netwerk Wordt volgens eens stringenter veiligheidsregime

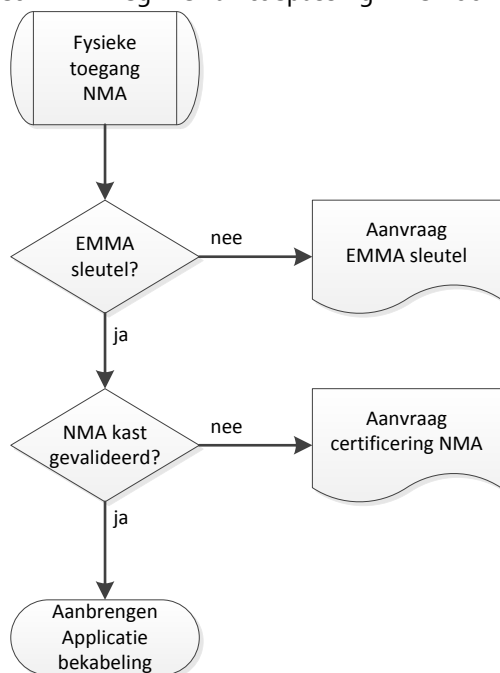
² Dat is apparatuur die niet nog niet in het veld is toegepast. Vrijgave in de IPOC dient te worden gedaan alvorens deze apparatuur in het veld kan worden toegepast.

aangesloten op NMA dan een gesloten netwerk van derde. Een gesloten netwerk van een derde kan een VPN op NMA zijn, maar kan ook een netwerk buiten NMA zijn. Standaard wordt een netwerk buiten NMA beschouwd als een extern (onveilig) netwerk. Dit betekent dat er bij interconnectie met zo'n netwerk maximale beschermingsmaatregelen worden getroffen. Voor een dergelijke interconnectie dient een third party Interconnection form te worden ingevuld.

Een VPN of een netwerk buiten NMA kan ook worden beschouwd als een 'gesloten netwerk van derde'. De beoordeling of een netwerk deze kwalificatie krijgt wordt gedaan door de CISO van MeT. Dit is overigens geen garantie dat deze kwalificatie daarna onbeperkt van kracht blijft. Security incidenten of een veranderd security beleid kan ervoor zorgen dat een netwerk wordt gedegradeerd of gepromoveerd naar resp. een extern netwerk of een gesloten netwerk van derde. In dat geval zullen alle interconnecties met dat netwerk opnieuw moeten worden ingericht.

2.3 Procesflow fysieke toegang tot de NMA kast

Wanneer een aansluiting op NMA moet worden gerealiseerd dient er toegang te worden verkregen tot de NMA kast waarin zich de Access switches bevinden. Voor toegang tot de technische ruimtes waarin de NMA kasten zich bevinden en voor toegang tot de NMA kast zelf is het EMMA regime van toepassing. Hiervoor is de volgende procesflow van toepassing:



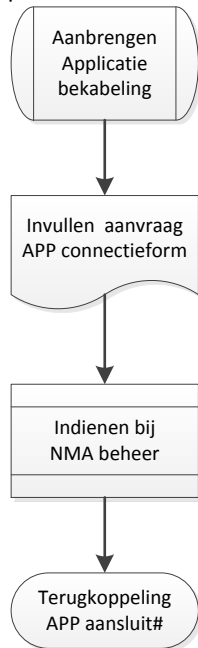
Figuur 3 Procesflow fysieke toegang

De essentie van deze procesflow is:

1. Het verkrijgen van een EMMA sleutel waardoor toegang tot de technische ruimtes mogelijk wordt.
2. Het verkrijgen van de benodigde rechten op de EMMA sleutel om ook daadwerkelijk de benodigde deuren te kunnen openen.

2.4 Procesflow aanbrengen applicatiebekabeling

Wanneer er nieuwe applicatiebekabeling moet worden afgewerkt op het Applicatiepatchpanel in de NMA kast dan is er voor het aanvragen van een poort op het Applicatiepatchpanel de volgende procedure van toepassing:



Figuur 4 Aanvraag patchpunt op ApplicatiePatchpanel

Nota Bene: Het afwerken van applicatiebekabeling (de bekabeling naar de objecten in een locatie) kan uitsluitend op het applicatiepatchpanel worden gedaan. De technisch beheerder van NMA (Thales) beheert de aansluitingen op het applicatiepatchpanel.

3 Installatievoorwaarden

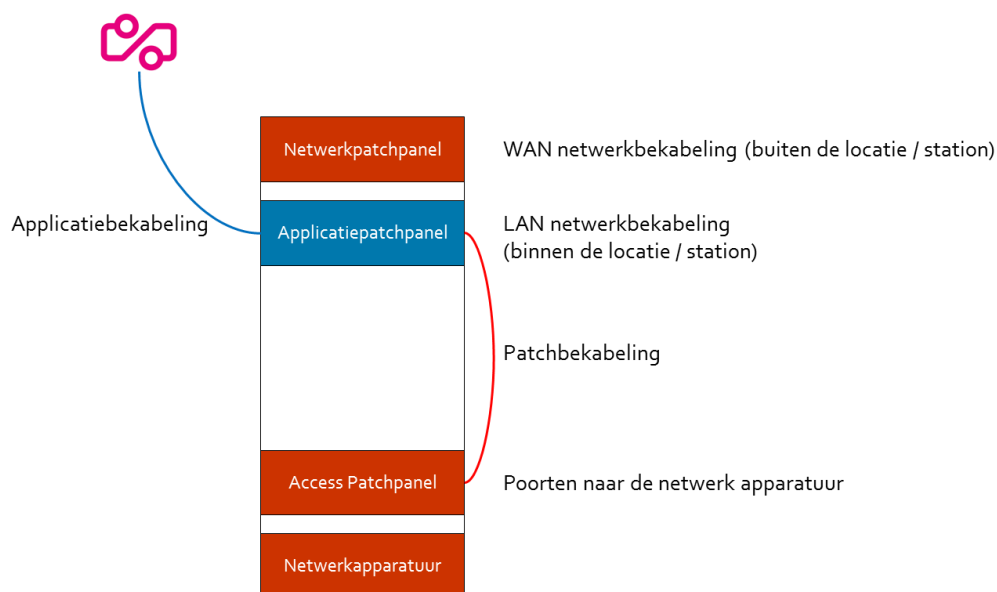
3.1 Inleiding

Zoals in hoofdstuk 2 aangegeven welke processen moeten worden gevolgd om toegang te krijgen tot de NMA netwerkkasten. In dit hoofdstuk staan de aanwijzingen voor het werken in de NMA kast.

2.1 Fysieke toegang tot het netwerk

In Figuur 5 is de standaardindeling van een netwerkkast weergegeven. Een netwerkkast bevat altijd de volgende onderdelen:

Netwerkpatchpanel	Op het netwerkpatchpanel is de glasvezelbekabeling afgewerkt die naar buiten het station (of de locatie) gaat (Coren nodes of andere locaties). Praktisch gezien is dit altijd glasvezelbekabeling.
Applicatiepatchpanel	Hierop wordt de applicatiebekabeling en de LAN bekabeling afgewerkt. De applicatiebekabeling is de bekabeling die naar de objecten op de locatie gaat. De LAN bekabeling is de bekabeling die naar de netwerkapparatuur op de locatie gaat. De Applicatiebekabeling kan zowel UTP als glasvezelbekabeling zijn. In Figuur 5 is een voorbeeld gegeven van de aansluiting van een OVCP poortje op het netwerk.
Access Patchpanel	Hierop worden de Access poorten van de netwerkapparatuur afgewerkt.
Netwerk apparatuur	Dit is de netwerkapparatuur. Deze apparatuur is verbonden met het netwerkpatchpanel (voor verbindingen naar het netwerk) en het Access Patchpanel.



Figuur 5 Principetekening netwerkkast

Aansluiting op NMA wordt altijd gerealiseerd via het Applicatie Patchpanel. Dit is het patchpanel waarop de aan te sluiten apparatuur wordt afgewerkt. Aansluiting geschiedt aan de achterzijde van het patchpanel door het afwerken van een contraplug in het patchpanel. Uitsluitend de blauwe bekabeling (zie Figuur 5) mag worden aangebracht. Patchpunten op het applicatiepatchpanel worden door de technisch beheerder van het NMA (Thales) uitgegeven gzie de procesflow hiervoor in paragraaf 2.4 Procesflow aanbrengen applicatiebekabeling.

4 Regels voor het gebruik van NMA

Ook nadat een aansluiting op NMA is gerealiseerd zijn er regels van toepassing voor het gebruik van het NMA. Deze regels zijn nodig om de integriteit, veiligheid en beschikbaarheid van data die getransporteerd wordt te kunnen waarborgen.

4.1 Algemeen

Binnen het NMA kunnen verschillende soorten aansluitingen worden gevraagd. Afhankelijk van het soort aansluiting zijn er verschillende regels van toepassing. Relevant hierbij is wie de verantwoording heeft voor de integriteit met NMA verbonden eindapparatuur. Het beveiligingsregime van NMA is erop gericht om de aangesloten apparatuur in een VRF te beschermen tegen ongewenste invloeden van buiten. Het is echter aan de eigenaar van deze apparatuur om zelf te bepalen welke beveiligingsmaatregelen hier worden getroffen. Het NMA 'bewaakt' of er geen onbekende gebruikers tot het VRF toegang proberen te krijgen. Als wel toegestane gebruikers echter virussen of malware verspreiden in het VRF dan zal dit niet door het NMA worden gedetecteerd.

4.2 Binnen het eigen VPN

IP adressering

Voor de IP adressering van apparatuur die op NMA wordt aangesloten worden per dienst (bijv. CTS, ICS, etc.) adresranges uitgegeven. Met deze IP adressen wordt de routing op het netwerk gedaan en dat maakt dat voor iedere T1, T2 of T3 locatie verschillend IP adresranges door de NMA beheerder worden uitgegeven. Bij de aanvraag van een nieuw VPN wordt door de beheer van het NMA een IP adresrange vastgesteld voor het gehele NMA. Deze range wordt verdeeld in subranges die over de locaties (Tier 1 – Tier 3 nodes) van NMA.

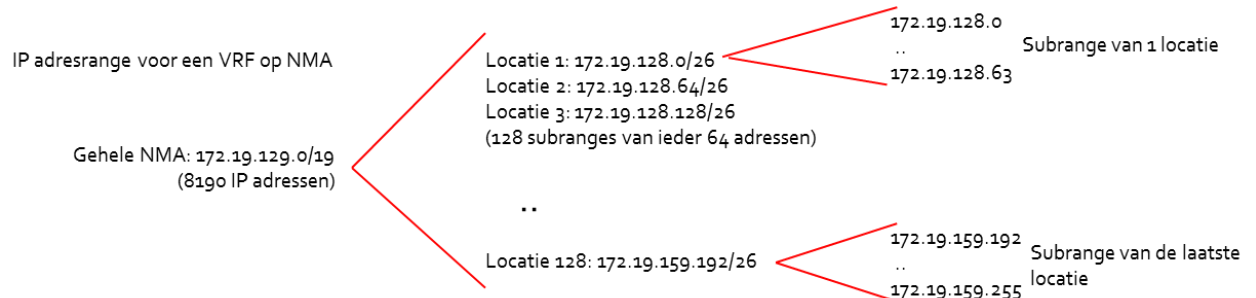
Een voorbeeld van een range die voor een VPN wordt uitgegeven is:

172.19.128.0/19 deze range bevat 8190 IP adressen en loopt daarmee van 172.19.128.0 – 172.19.159.255. Deze range wordt opgedeeld in 128 subranges van 64 IPadressen voor maximaal 128 locaties (T1, T2 of T3 nodes).

Zo'n subrange is in dit voorbeeld bijvoorbeeld 172.19.130.0/26. Deze subrange loopt van 172.19.130.0 - 172.19.130.63.

De gebruiker van een VRF kan per aangesloten locatie de IP adressen uit de betreffende subrange zelf toekennen met uitzondering van de eerste 10 adressen van de subrange. Deze adressen voor het netwerk zelf gereserveerd.

Resumerend:



Uit de subranges per locatie (64 adressen) kunnen vrijelijk IP adressen worden toegekend aan de eindapparatuur. De eerste 10 adressen zijn gereserveerd voor het netwerk en het laatste adres uit zo'n subrange is altijd het broadcast adres. Voor de IP adresrange 172.19.128.0/26 kan daarmee genummerd worden van 172.19.128.10 – 172.19.128.62. Adres 172.19.128.63 is daarmee het broadcast adres voor deze subrange.

Gebruik van een DHCP server

Het is toegestaan om een DHCP server in een VPN te plaatsen die automatisch IP adressen uit de juiste adresranges toekent aan de aangesloten apparatuur. Deze DHCP server dient dan in één of beide van de datacenters te worden geplaatst. Bij de aanvraag van het VPN zal dan wel moeten worden opgegeven dat er gebruik wordt gemaakt van een centrale DHCP server om ervoor te zorgen hiervoor in de routers in NMA de benodigde DHCP relay agents worden geconfigureerd. Deze DHCP relay agent zorgt ervoor dat DHCP requests van aangesloten apparatuur naar de centrale DHCP server in het datacenter worden gestuurd.

Class of Service / Differentiated Services Code Point

Het NMA is ingericht op het transporteren van data tussen gebruikers van NMA. Deze data wordt bij de entree van het netwerk gemarkeerd conform de afgesproken Class of Service (COS)/Differentiated Services Code Point(DSCP). Het heeft geen zin om als eindgebruiker te trachten zelf deze markering aan te brengen binnen de IP pakketten. Bij de entree van het netwerk zal deze 'eigen' kwalificatie worden overschreven door de afgesproken kwalificatie. Als een niet afgesproken verkeersstroom wordt aangeboden dan zal deze verkeersstroom de laagste COS/DSCP markering krijgen (Best Effort). Daarmee vervalt automatisch de afgesproken beschikbaarheidsgarantie voor deze verkeersstroom.

Vrijgave van apparatuur op een poort

Bij aansluiting op NMA geldt dat de in de switchpoortaanvraag opgegeven apparatuur wordt vrijgegeven op de in dat formulier opgegeven poorten. Zodra deze apparatuur is aangesloten kan deze niet meer worden uitgewisseld met andere apparatuur. Als dit toch wordt gedaan, dan zal de poort automatisch administratief worden gesloten. Openen is daarna alleen nog mogelijk via de beheerder van het netwerk.

Virussen/Malware/Trojans etc.

Het netwerk transporteert alleen de data tussen de gebruikers van een VPN. Dit verkeer wordt verder niet bekeken of opgeslagen; alleen getransporteerd tussen gebruikers van het netwerk. Indien er een gebruiker virussen/malware of ander ongewenst verkeer zal versturen, dan zal het netwerk niet ingrijpen. De gebruikers van het VPN zijn zelf verantwoordelijk voor de integriteit van door hen aangesloten apparatuur. Deze maatregelen kunnen door NMA alleen worden gehandhaafd als geen eigen netwerkapparatuur wordt aangesloten.

Gebruik van eigen netwerkapparatuur

Het aansluiten van eigen netwerkapparatuur is niet toegestaan. NMA voorziet de connectiviteit het volledige netwerk tot en met de eindapparatuur. De reden hiervoor is dat binnen NMA een beveiligingsregime van toepassing is. Dit regime bevat maatregelen die voorkomen dat onbekende apparatuur of onbekende applicaties van NMA gebruik maken om zo toegang te krijgen tot de op NMA aangesloten apparatuur.

Software en updates van software

De toegepaste hard- en software van apparatuur in het VPN dient vrijgegeven te zijn in de testomgeving (IPOC) van Metro en Tram. Dit is om er zeker van te zijn dat de apparatuur in de geïntegreerde omgeving functioneert als verwacht.

Samenvattend zijn de volgende regels van toepassing binnen een VRF:

- Alleen de in de switchpoortaanvraag opgegeven apparatuur mag worden aangesloten op de opgegeven poorten.
- IP adressering moet conform de bij de aanvraag van de VPN vrijgegeven IP adresranges. Gebruik van een DHCP server is toegestaan, mits aangekondigd zoals hiervoor beschreven.
- Niet opgegeven verkeersstromen worden conform de laagste prioriteitsklasse in het netwerk afgehandeld. Op deze verkeersstromen vervallen de afgesproken beschikbaarheidsgaranties.
- Eenmaal aangesloten apparatuur wordt 'gelocked' op de poort. Vrijgave van de poort voor andere apparatuur kan alleen door de poort door NMA beheer te laten flushen.
- De gebruiker van een VRF is zelf verantwoordelijk voor de integriteit van de aangesloten apparatuur.
- Gebruik van netwerkapparatuur is niet toegestaan.

4.3 Verkeer tussen VPN's van NMA

Koppelingen tussen verschillende VPN's via de firewall

Binnen het NMA zijn er twee soorten transportdiensten (via VPN's) mogelijk. Deze zijn:

1. Transportdiensten volledig onder de verantwoordelijkheid van Metro en Tram: dit zijn transportdiensten die worden geleverd voor en tussen installaties/systemen waarvan MeT de eigenaar is.
2. Transportdiensten voor en tussen installaties/systemen onder de verantwoordelijkheid van derden: dit zijn alle transportdiensten die met het NMA voor andere gebruikers (eigenaren) worden geleverd.

Ad 1 Voor transportdiensten van Metro en Tram geldt ten aanzien van Interconnectie dat dit uitsluitend mogelijk is op twee manieren afhankelijk van het type netwerk waarmee de interconnectie wordt gemaakt. Deze type netwerken en wijze van interconnectie zijn:

- a) Gesloten netwerken van derden: dit soort netwerken kan direct met de Interne firewall worden verbonden voor interconnectie. Verkeer wat naar een bestemming buiten het eigen VPN moet altijd via de interne firewall worden gerouteerd. Het is niet toegestaan om eindapparatuur met meer dan 1 VPN te verbinden. Dit is ook niet toegestaan als dit op een apart netwerk interface gebeurt. Verkeer tussen VPN's in NMA of tussen een VPN van NMA en een gesloten netwerk van een derde wordt afgehandeld conform de specificatie zoals opgegeven in de Device Interconnection form. Dit betekent dat niet gespecificeerde verkeersstromen niet worden doorgelaten. Dit is ter bescherming van alle aangesloten apparatuur binnen een VRF.
- b) Externe (onveilige netwerken): met deze netwerken kan uitsluitend worden verbonden met de externe firewall.

De classificatie die een netwerk krijgt (extern of gesloten netwerk van derde) wordt vastgesteld per netwerk vastgesteld door de Asset Manager en vastgelegd in het beveiligingsregime van het NMA.

Ad 2 Voor transportdiensten in het NMA voor derden is Metro en Tram niet verantwoordelijk voor de beveiliging van de netwerken waarmee zij worden verbonden. Dit betekent dat deze koppelingen direct (zonder firewalls) worden gerealiseerd. NMA heeft beveiligingsmaatregelen genomen voor het beschermen van de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevensstromen in (en dus alleen binnen) het NMA. NMA kan geen aansprakelijkheid nemen voor de (kwaliteit van de) gegevens die door andere systemen en netwerken worden aangeleverd of uitgelezen.

Voorwaarden voor interconnectie naar een ander VPN binnen NMA

Om een interconnectie naar een ander VPN binnen NMA te realiseren dient te worden voldaan aan de volgende eisen:

- Aangesloten apparatuur dient te zijn vrijgegeven in de Ontwikkeling, Test, Acceptatie en Productie omgeving van Metro en Tram³.
- De software en besturingsystemen van de aangesloten apparatuur dient bijgewerkt te zijn met de meest recente versie van door de software leverancier vrijgegeven release of

³ De termen IPOC (Integrale Proof of Concept) of OTAP (Ontwikkel, Test, Acceptatie en Productie) omgeving worden beiden gebruikt. Bedoeld wordt echter dezelfde testomgeving voor vrijgave van nieuwe of gewijzigde apparatuur in het areaal.

bugfix. Afwijking hiervan is alleen mogelijk met opgaaf van redenen en na goedkeuring door NMA beheer en de CISO.

- Er dient een duidelijk afgesproken onderhoudsregime van toepassing te zijn.

4.4 Verkeer naar externe (onveilige) netwerken

Alle netwerken die niet behoren tot de interne netwerken of interne gesloten netwerken van derden behoren automatisch tot de onveilige netwerken. Dit betekent dat een verbinding naar deze netwerken uitsluitend mogelijk is via de centrale firewall cluster van het NMA. De standaardmethodiek voor een dergelijke aansluiting is een versleutelde tunnel over het Internet of een private verbinding naar de firewall cluster van het NMA. De aanvraag van een dergelijke verbinding wordt gedaan met het invullen van het 'third party interconnection form'. Er zijn geen specifieke eisen waaraan een extern netwerk moet voldoen voor interconnectie, wel worden eisen gesteld aan de wijze waarop de versleuteling van de verbinding wordt gedaan. In het algemeen kan worden gesteld dat alleen verbindingen naar externe netwerken voor beheerapplicaties worden toegestaan.

Bijlage 1 Device Specification form

Ethernet port 1		
Ethernet port 1 description	Please give a detailed description of the function of this Ethernet port and its relation to other ethernet ports in the network, in the Datacenter, at DMA or at a 3rd party that it communicates with, including or appending drawings or low level designs with this document would greatly be appreciated.	
Physical port Specifications	Type of port (check 1 box)	
	☐ Fast Ethernet RJ45 10/100 Mbps CAT6 UTP	☐ Fast Ethernet SFP-SX 100 Mbps Multimode Fiber
	☐ Gigabit Ethernet RJ45 10/100/1000 Mbps CAT6 UTP	☐ Gigabit Ethernet SFP-SX 1000 Mbps Multimode Fiber
	☐ Other: Please specify	
	Speed settings only applicable for RJ45 ports (check 1 box)	
	☐ Auto negotiate speed settings	☐ Fixed 10 Mbps
	☐ Fixed speed 1000 Mbps	☐ Fixed 100 Mbps
	Speed settings only applicable for RJ45 ports (check 1 box)	
	☐ Auto negotiate duplex settings	☐ Fixed Half duplex
	☐ Fixed Full Duplex	
Power over Ethernet (check 1 box)		
☐ POE disabled	☐ 802.3af (POE 15,4W)	
☐ 802.3at (POE+ 36W)		
Profinet (check 1 box)		
☐ Profinet Disabled	☐ Profinet enabled	
Ethernet VLAN / MPLS L3VPN Specifications	Ethernet VLAN / MPLS L3VPN (check 1 box)	
	☐ OVCP-ALGEMEEN	☐ CBI-ALGEMEEN
	☐ STATION-INTERCOMS	☐ STATION-TELEFONIE
	☐ STATION-DRIS	☐ STATION-CAMERA
	☐ KA-ALGEMEEN	☐ SCL-ALGEMEEN
	☐ Other: Please specify	
L3 Services	L3 Services (check 1 box)	
	☐ DHCP Helper : Please specify DHCP server IP address (to be supplied by partner contractor)	
	☐ NTP (NTP server IP adress will be supplied by Thales)	
	☐ Other: Please specify	

17

Bijlage 2 Switchpoortaanvraag

Object	Kast	Switch	Poi	Router	VRfid	VRfnaam	IPaddress	DefGateway	Opmerking
Printer	GVB-ND-NK3-Printer	D.NK3.06.18	NAS-ND-35	p1/3	NDR-ND-01	132	GVB-OFFICE	10.93.65.75	10.93.65.65
Werkplek Citrix	GVB-ND-NK3-WP-Citrix-01	D.NK3.06.19	NAS-ND-35	p1/4	NDR-ND-01	132	GVB-OFFICE	10.93.65.76	10.93.65.65
Werkplek Citrix	GVB-ND-NK3-WP-Citrix-02	D.NK3.06.15	NAS-ND-35	p1/5	NDR-ND-01	132	GVB-OFFICE	10.93.65.77	10.93.65.65
wifi (plafond)	GVB-ND-NK3-WIFI-01	D.NK.3.06.13	NAS-ND-31	p3/5	NDR-ND-01	135	GVB-MANAGEMENT	10.93.161.75	10.93.161.65
Telefoon	GVB-ND-NK3-Tel01	D.NK3.06.17	NAS-ND-31	p3/7	NDR-ND-01	24	STATION-TELEFONIE	172.19.130.10-62	172.19.130.1
Telefoon	GVB-ND-NK3-Tel02	D.NK3.06.14	NAS-ND-31	p3/8	NDR-ND-01	24	STATION-TELEFONIE	172.19.130.10-62	172.19.130.1
wifi (plafond)	GVB-ND-NK3-WIFI-02	D.NK.3.06.22	NAS-ND-31	p3/6	NDR-ND-01	135	GVB-MANAGEMENT	10.93.161.76	10.93.161.65
zuiltje	GVB-ND-NK3-Zuiltje	D.NK.3.06.20	NAS-ND-35	p1/6	NDR-ND-01	132	GVB-OFFICE	10.93.65.78	10.93.65.65
Telefoon	GVB-ND-NK3-Tel03	D.NK.3.06.22	NAS-ND-31	2/8	NDR-ND-01	24	STATION-TELEFONIE	172.19.130.10-62	10.93.161.65
netpresenter	GVB-ND-NK3-netpresenter	D.NK3.06.21	NAS-ND-35	p1/7	NDR-ND-01	132	GVB-OFFICE	10.93.65.79	10.93.65.65
Paniekknop		D-NK3-06.23				130		10.93.1.15	10.93.1.1