Bijlage 7 – A

Technische beschrijving Netwerkvervanging

Veiligheidsregio Twente

Behorende bij Aanbestedingsdocumenten Netwerkvervanging 2022 Switches, Routers en Migratieadvies

Referentienummer 202201ICT/MS

TenderNed – kenmerk 345188

Maart 2022

Inhoudsopgave

1. Inleiding 2
1.1 Veiligheidsregio Twente 2
1.2 Doel 3
1.3 Opbouw 4
1.4 Methode 4
2. Situatieschets 5
2.1 Huidige situatie 5
2.2 Toekomstige situatie 6
3. Netwerkoverzicht 7
3.1 Bouwstenen 7
3.1.1 Hoofdlocaties 7
3.1.2 Kazernelocatie type 1 7
3.1.3 Kazernelocatie type 2 8
3.1.4 WAN-netwerk (trusted) 8
3.1.5 Internet (untrusted) 8
3.2 Scope 8
4. Server-Access 9
4.1 Functionele Beschrijving 9
4.2 Functionele Eisen 9
5. Locatie-koppeling 10
5.1 Functionele Beschrijving 10
5.2 Functionele Eisen 10
6. LAN Access 11
6.1 Functionele Beschrijving 11
6.2 Functionele Eisen 12
7. Netwerkbeheer 13
7.1 Functionele Beschrijving 13
7.2 Functionele Eisen 13
8. NAC 14
8.1 Functionele Beschrijving 14
8.2 Functionele Eisen 15

1. Inleiding

1.1 Veiligheidsregio Twente

Veiligheidsregio Twente (hierna te noemen als VRT) is een samenwerkingsverband van 14 gemeenten, gebaseerd op de Wet Gemeenschappelijke Regelingen en geeft uitvoering aan de taken en bevoegdheden van de Wet Veiligheidsregio's. De samenwerking betreft de gemeenten Almelo, Borne, Dinkelland, Enschede, Haaksbergen, Hellendoorn, Hengelo, Hof van Twente, Losser, Oldenzaal, Rijssen-Holten, Tubbergen, Twenterand en Wierden.
De bestuurlijke organisatie van Veiligheidsregio Twente bestaat uit het algemeen bestuur en het dagelijks bestuur en de voorzitter. In het algemeen bestuur zijn de burgemeesters van alle 14 deelnemende gemeenten vertegenwoordigd; het dagelijks bestuur wordt gevormd door vijf burgemeesters, inclusief de voorzitter. Veiligheidsregio Twente wordt ambtelijk aangestuurd door de Veiligheidsdirectie, bestaande uit de secretaris (voorzitter), de commandant van de brandweer, de directeur Publieke Gezondheid, de korpschef politie en de coördinerend gemeentesecretaris. De Veiligheidsregio Twente heeft primair tot doel de Wet veiligheidsregio's uit te voeren, meer in het bijzonder de taken zoals genoemd in artikel 10 van de Wet Veiligheidsregio's.
Voor meer informatie over VRT wordt verwezen naar de website www.vrtwente.nl.

Brandweer Twente is een integraal onderdeel van de VRT. Alle 14 Twentse gemeenten maken deel uit van Brandweer Twente. In Twente zijn in totaal 36 locaties. Bij Brandweer Twente werken ongeveer 800 vrijwilligers en 250 beroeps. De vrijwilligers zijn de ruggengraat van de dagelijkse brandweerzorg, het grootschalig optreden en de rampenbestrijdingsorganisatie. Voor meer informatie over Brandweer Twente wordt verwezen naar de website www.brandweer.nl/twente

1.2 Doel

VRT is voornemens haar netwerkinfrastructuur te vernieuwen. Het is verouderd en is aan vervanging toe. De VRT wil hiermee weer een stabiel en toekomstbestendige infrastructuur aan de eindgebruikers aanbieden. Derhalve wens VRT van gegadigden te ontvangen:

- Voor de levering van apparatuur t.b.v. van de infrastructuur een investeringsoverzicht
- Advies over een te volgen migratietraject waarbij er zo weinig mogelijk verstoringen optreden tijdens de migratie.
- Plan van aanpak op waarin expliciet beschreven staat hoe de bestaande infrastructuur wordt vervangen door de aangeboden producten met als uitgangspunt dat er zo min mogelijk verstoringen optreden voor de eindgebruikers.
- Een planning met de geschatte doorlooptijden
- De benodigde inspanning die van de VRT wordt verwacht.
- Te verwachten opleidingskosten voor 2 netwerkbeheerders

Dit document beschrijft de eisen die VRT stelt aan het nieuwe netwerk. Dit document vormt het belangrijkste basisdocument voor het maken van de high level en low level designdocumenten.
Het document bevat:

- Een abstract functioneel overzicht met de belangrijkste bouwstenen van de infrastructuur;
- Een overzicht van de functionele eisen per bouwsteen;
- Per eis een indicatie van de belangrijkheid of prioriteit.

Op basis van deze informatie ontstaat een duidelijk beeld van welke functionaliteiten het netwerk dient te bieden en wat de volgorde van belangrijkheid is van de verschillende eisen. VRT heeft de wens om zoveel mogelijk naar de Cloud te gaan, de bestaande infrastructuur moet omwille van lifecycle management vernieuwd te worden. De functionaliteit die er nu is moet zoveel mogelijk worden geconsolideerd worden en hoeft niet verder geïnnoveerd te worden. Daarnaast bestaan de behoefte om de complexiteit te verminderen.

1.3 Opbouw

Dit document is opgedeeld in drie delen. Het eerste deel staat in hoofdstuk 2 en schetst de huidige situatie en geeft een beeld van de toekomstige situatie.
Deel 2 (hoofdstuk 3) behandelt het conceptuele beeld van het toekomstige netwerk waarin de verschillende bouwstenen worden benoemd en hoe deze bouwstenen aan elkaar gekoppeld zijn.
Het derde deel beschrijft alle functionele eisen voor de bouwstenen. Om structuur en overzicht te bewaren is dit deel opgedeeld in meerdere hoofdstukken. Ieder hoofdstuk behandelt een bouwsteen.

1.4 Methode

De inventarisatie van de eisen is gebaseerd op de functionele gebieden van het netwerk. De eisen zijn opgesomd in tabellen met een korte beschrijving en een prioriteit. Voor de indicatie van prioriteiten wordt de MoSCoW methode gehanteerd. In deze methode bestaan vier niveaus van prioriteit (zie Tabel 1).

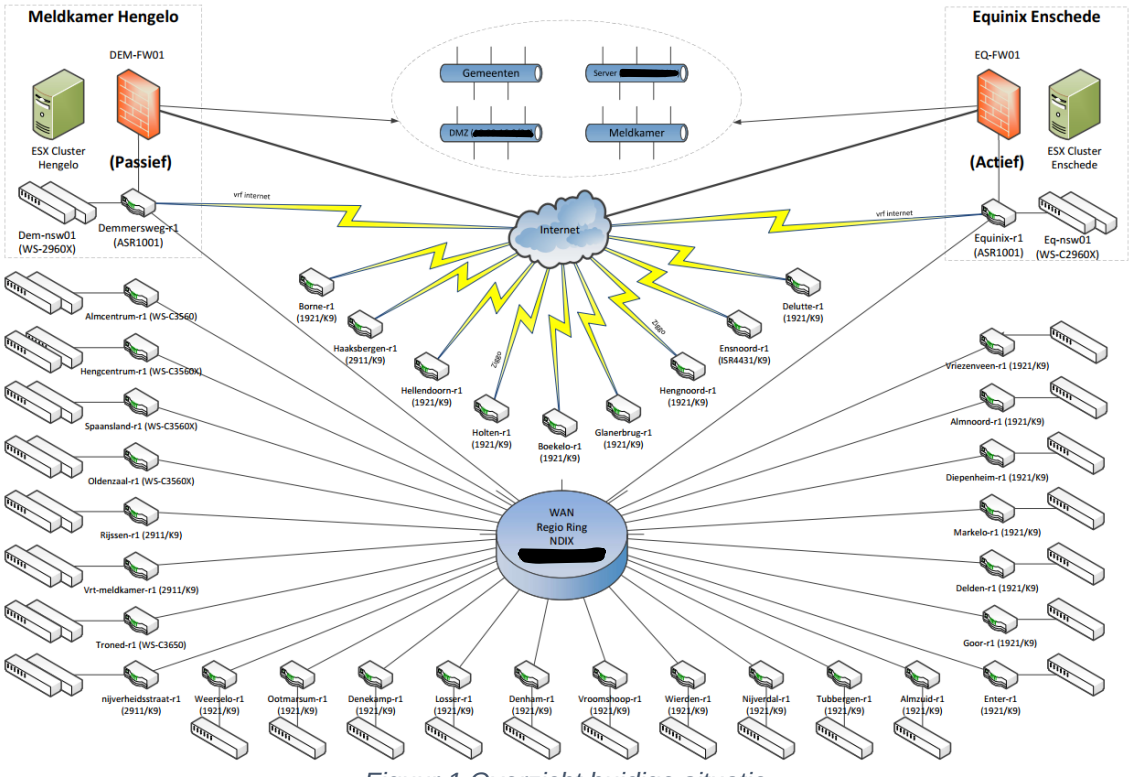
PrioriteitCode	Omschrijving	Betekenis
M	Must have	Aan deze eis dient zeker te worden voldaan in het eindresultaat.
S	Should have	Deze eis is zeer belangrijk, maar gelijkwaardige functionaliteit of een workaround is acceptabel.
C	Could have	Deze eis is een nice-to-have, mits binnen budget
W	Won't have	Deze eis wordt niet meegenomen op dit moment, maar wordt genoemd voor toekomstig gebruik.

Tabel 1 MoSCoW

2. Situatieschets

2.1 Huidige situatie

VRT beschikt over een 36-tal access-locaties, veelal gevestigd in brandweerkazernes. Daarnaast zijn een tweetal centrale (hoofdlocaties) waar zich o.a. de centrale server, storage-apparatuur en firewall bevindt. (Zie Figuur 1). De locatie Troned is afwijkend op de andere locatie. Dit betreft een groot oefenterrein waar op verschillende locatie netwerk verbindingen benodigd zijn. In Bijlage 7- B Programma van Eisen is hier ook een aanvullende opmerking over te vinden.
De brandweerkazernes zijn voorzien van diverse typen Cisco switches, deze zijn niet voorzien van NAC (netwerk access control). Koppeling met de hoofdlocaties wordt verzorgd door een regionaal L2 datanetwerk of door middel van VPN-verbindingen via internet.
Het draadloze netwerk is gebaseerd op 802.11ac access points en kan volledig worden beheerd via de Cisco Meraki cloud.
Al het dataverkeer wordt op de vestigingen in lokale vlans uit gekoppeld en gerouteerd naar de hoofdlocatie. Gastverkeer wordt getransporteerd via een laag 2 (vlan) verbinding naar de centrale firewall of direct uit gekoppeld naar internet.
Elke locatie is voorzien van eigen subnetten en vlans, er zijn geen restricties binnen het “trusted” netwerk.
De apparatuur van de VRT wordt deels gemanaged in de lokale AD en deels in Intune. Verwachting is dat dit volledig naar Intune verschuift.



Figuur 1 Overzicht huidige situatie

2.2 Toekomstige situatie

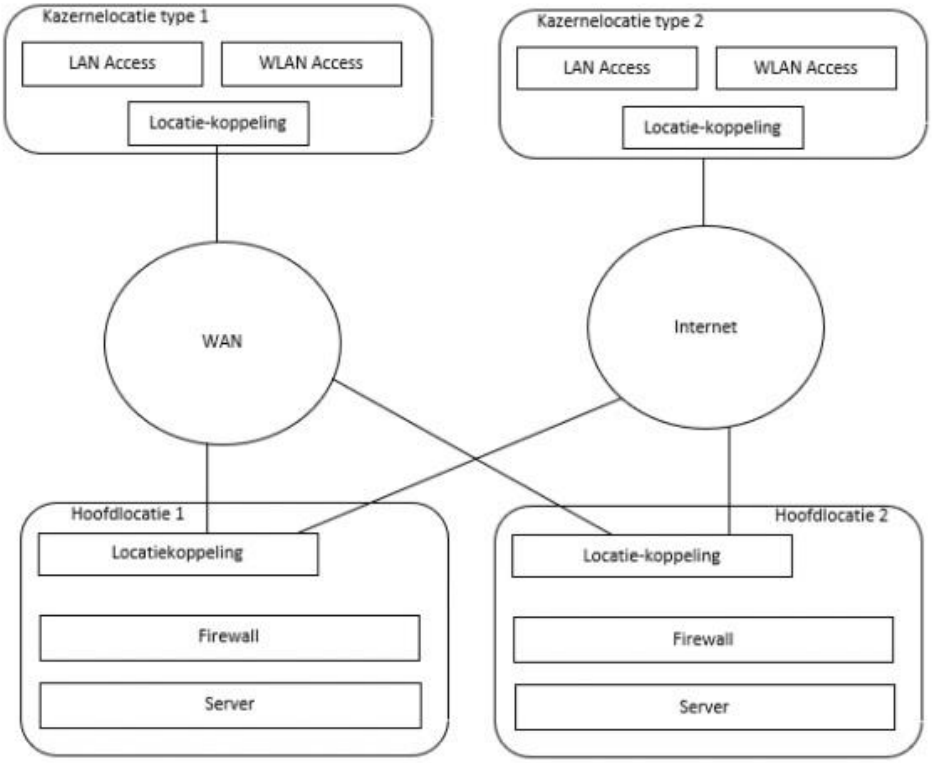
De netwerkapparatuur op de locaties kan centraal beheerd worden en voorzien worden van configuratie of firmware-updates. De apparatuur op locaties maakt automatisch verbinding met een centraal (cloud-based) platform, waar centraal beheer kan worden gedaan en de verkeersstromen worden geanalyseerd.
Dit platform kan d.m.v. machine-learning gedrag van applicaties, “voorspellen” wat het netwerk doet.
De configuratie op de apparatuur is compact, er is een mogelijkheid dat al het verkeer op een centrale locatie wordt uit gekoppeld.
Apparaten op het netwerk worden geauthentiseerd en de apparaten binnen de netwerkomgeving krijgen een eigen rol op het netwerk, ongeacht waar men connectie maakt.
De verschillende apparaten zijn logisch van elkaar gescheiden op het netwerk (zien elkaar niet), eventuele onderling connecties zijn alleen gecontroleerd mogelijk.
De server-access laag zorgt voor hoog-beschikbare en hoog-performante verbindingen tussen de lokale serveromgeving en het netwerk. De switches en security-appliances ondersteunen allemaal SDN-gebaseerde concepten.
De verbindingen tussen de locaties zijn gerouteerd, om eventuele loops te voorkomen. Iedere locatie moet zelfstandig kunnen opereren (zelfs bij uitval WAN).

3. Netwerkoverzicht

In dit hoofdstuk staat een conceptueel overzicht van het netwerk. De individuele bouwstenen die het netwerk vormen, vormen het startpunt van de inventarisatie van functionele eisen.

3.1 Bouwstenen

De netwerkinfrastructuur bestaat uit de volgende onderdelen: (Zie Figuur 2)



Figuur 2 Conceptueel netwerkoverzicht

3.1.1 Hoofdlocaties

Op deze locaties bevindt zich de interne serveromgeving, de centrale core-firewall en routing apparatuur. Tevens vormen deze locaties het koppelpunt van externe verbindingen naar internet, gemeenten, meldkamer en de WAN-omgeving. De beide hoofdlocaties zijn via directe DWDM verbindingen gerouteerd gekoppeld.
De centrale routing apparatuur (2 x hoofdrouters actief/passief) verzorgd routering van alle locaties, coreswitches en firewall.

3.1.2 Kazernelocatie type 1

Op deze locaties bevinden zich bedraad en draadloze access netwerken. De locaties zijn gekoppeld met de hoofdlocaties via het WAN-netwerk (L2 100/1000 Mbit).

3.1.3 Kazernelocatie type 2

Op deze locaties bevindt zich bedraad en draadloze access netwerken. Deze locaties zijn gekoppeld met de hoofdlocaties via VPN-verbindingen over internet.

3.1.4 WAN-netwerk (trusted)

Het WAN-netwerk is gebaseerd op verbindingen via zowel het regionale netwerk van Regio Twente alsook verbindingen via het netwerk van de provider NDiX . Deze transparante ethernet verbindingen worden extern beheerd en bieden laag 2 (vlan) connectiviteit op basis van Point-to-point of point-to-multipoint.

3.1.5 Internet (untrusted)

Internet-koppelingen zijn redundant aanwezig op beide hoofdlocaties. Centrale internet-breakout vindt hier plaats. Op (type 2) locaties bevinden zich ook internetverbindingen en worden gebruikt voor de VPN-koppeling met de hoofdlocatie. De firewalls maken geen onderdeel uit van deze aanbesteding

3.2 Scope

De volgende functionele bouwstenen zijn geïdentificeerd in het netwerk:

- Server access
- Routering
- Firewall
- Locatie-koppeling
- LAN-access
- WLAN-access
- Voorzieningen voor centraal beheer/management door de Veiligheidsregio Twente
- NAC
- Advies basisconfiguratie en migratie
- Training beheerder

Van deze bouwstenen zijn firewall en WLAN-access buiten scope.

4. Server-Access

4.1 Functionele Beschrijving

Server access wordt gevormd door het deel van het netwerk waar centrale apparatuur zoals servers, firewalls en appliances gekoppeld worden. De belangrijkste functionaliteit voor de server-access zijn:

- Koppelvlak voor alle serverinterfaces (LAN);
- Koppelvlak voor alle centrale apparatuur (firewall, controllers, VPN-appliance en routers).

De beschikbaarheid van de server-access apparatuur dient zo hoog mogelijk te zijn, bijvoorbeeld door het uitvoeren van de betreffende apparatuur in een cluster of stack. Hierbij moeten eventuele updates kunnen worden uitgevoerd, zonder dat de gehele omgeving hiervan hinder (downtime) ondervindt.
De apparatuur dient zover mogelijk te worden voorzien van redundant uitgevoerde componenten zoals bijvoorbeeld voedingen, of in het geval van chassis, management.
Apparatuur dient geplaatst te kunnen worden in serverracks, voor optimale koeling moet de fan-richting aangepast kunnen worden.

De apparatuur dient voorzien te zijn van poorten die een snelheid van 100, 1000, 10000 Mbit/s ondersteunen. (minimaal aantal poorten 54 per stack)

4.2 Functionele Eisen

De functionele eisen voor server-access kunt u vinden in het document “Bijlage 7 – B Programma van Eisen”

5. Locatie-koppeling

5.1 Functionele Beschrijving

De locatie-koppeling wordt gevormd door apparatuur die zorgt voor de ontsluiting van een (kazerne)locatie met een extern netwerk, zoals WAN of internet.
We onderscheiden hierbij twee soorten:

- Koppelingen over een trusted netwerk (WAN bijv. regionaal netwerk of NDiX);
- Koppelingen over een untrusted netwerk (internet).

De belangrijkste functionaliteit van de locatie-koppeling is:

- Ontsluiting bieden van locaties naar de hoofdlocaties.

Trusted netwerk
De locatie-koppeling moeten een routering bieden naar de hoofdlocatie, hierbij moet er gebruik gemaakt kunnen worden van dynamische routeringsprotocollen zoals OSPF.
Voor de kleinere locaties kan deze locatiekoppeling ook gecombineerd worden in de LAN-access apparatuur.

Untrusted netwerk
De apparatuur voor het untrusted netwerk versleutelt alle communicatie en kan direct worden aangesloten op een internet feed. Hierbij zijn NGFW-capabiliteit vereist (IPS/IDS en malwaredetectie)

Alle apparatuur moet automation en orchestration vanuit een centrale (cloud) portal ondersteunen. De apparatuur dient zoveel mogelijk uniform te worden geconfigureerd, indien mogelijk zelfs volledig automated. Alle apparatuur moet voorzien zijn van minimaal 1 uplink en 4 downlink UTP-ethernetpoorten. Ook hier moet het middels een routering mogelijk zijn om alle verkeer naar de hoofdlocatie te sturen, hierbij moet er gebruik gemaakt kunnen worden van dynamische routeringsprotocollen zoals OSPF. eHet koppelvlak voor de WAN van deze locaties is Ethernet/UTP.

5.2 Functionele Eisen

De functionele eisen voor locatie-koppeling kunt u vinden in het document “Bijlage 7 – B Programma van Eisen”

6. LAN Access

6.1 Functionele Beschrijving

LAN-access wordt gevormd door het deel van het netwerk waar bekabelde eindgebruikersapparatuur op wordt aangesloten zoals Pc's, laptops, printers maar ook access-points.
De belangrijkste functionaliteiten van het LAN zijn:

- Veilige toegang bieden voor gebruikers tot het productienetwerk/datacenter;
- Veilige toegang bieden voor overige apparatuur tot het productienetwerk/datacenter;
- Ontsluiting bieden richting WLAN access-points;
- Aanbieden van logische gescheiden netwerken voor bijvoorbeeld gasten en leveranciers en specials.

Vanwege het eenvoud principe dient er bij voorkeur gebruik gemaakt te worden van een enkel type access-switch op alle locaties. Deze fysieke access-switches dienen te kunnen worden samengevoegd tot één logische switch, ook bekend als “stacking”. Hierbij dient de stack minimaal 5 switches te ondersteunen, waarbij het eenvoudig en zonder downtime mogelijk moet zijn een stack uit te breiden. De locatie Troned is hierop uitgezonderd omdat er meerdere switches over grote afstanden gekoppeld dienen te worden. In het Excel bestand vindt u meer informatie over deze locatie en hoe de glasvezel koppelingen lopen naar de verschillende patch/switch locaties.
Zowel IP-telefoons als de WLAN access-point gebruiken PoE voor stroomvoorziening. Om geen onderscheid te hoeven maken in access-switches of poorten dienen alle access-switches op alle poorten bij voorkeur PoE+ (802.3at) te ondersteunen.
Uitval van een access-switch zal altijd leiden tot downtime voor de apparatuur die lokaal op deze switch zit aangesloten. Daarom dient een access-switch zo snel mogelijk vervangen te kunnen worden. Bijvoorbeeld door middel van een auto-provisioning mechanisme (zero touch deployment).
Uitval van een access-switch welke onderdeel is van een stack mag niet voor downtime zorgen voor andere switches in de stack.
In de access-laag dienen de switches te kunnen worden voorzien van redundant uitgevoerde componenten zoals bijvoorbeeld voedingen.
Omdat er verschillende soorten randapparatuur op het netwerk aangesloten zullen worden dienen alle poorten een snelheid van 10,100 en 1000Mbit te ondersteunen op basis van UTP-bekabeling met RJ-45 connectoren. Deze interfaces dienen daarnaast autosensing en handmatige speed/duplex instellingen te ondersteunen.
LAN-access dient ook QoS ondersteuning te bieden.

De LAN-access dient een veilige toegang te bieden voor gebruikers tot het productiewerk. Hiervoor dient het netwerk Network Access Control (NAC) te ondersteunen waarbij onbekende devices alleen toegang tot een gast- netwerk verkrijgen. De LAN-access dient ten behoeve van NAC 802.1x EAP en MAB-authenticatie te ondersteunen. Het dient mogelijk te zijn middels authenticatie dynamisch in een bepaald LAN-segment geplaatst te worden.
Het is wenselijk een eindgebruiker middels de NAC tooling te kunnen traceren tot een fysieke poort.

De access-switches dienen een underlay/overlay en/of SDN-concept te ondersteunen om automation en orchestration vanuit centrale tooling mogelijk te maken.
Het is een sterke wens om de inrichting van de LAN-access voor de verschillende locaties zo uniform mogelijk te houden en het aantal unieke netwerken (VLAN’s) zo veel mogelijk te beperken.
Verkeer tussen gebruikers op het netwerk dient zoveel mogelijk beperkt te worden (client-isolation).

6.2 Functionele Eisen

De functionele eisen voor lan-access kunt u vinden in het document “Bijlage 7 – B Programma van Eisen”

7. Netwerkbeheer

7.1 Functionele Beschrijving

De functie netwerkbeheer maakt het beheer van netwerkcomponenten mogelijk. De functie bestaat uit hard- en software die samen het netwerkbeheer vormen.
Bij voorkeur wordt alle netwerkapparatuur vanuit centrale beheer tooling beheerd/geconfigureerd.
De netwerkbeheer tooling dient hierbij concepten als ‘automation’ en ‘orchestration’ te ondersteunen. Het snel en geautomatiseerd kunnen aanmaken van een nieuw logisch segment is hierbij een voorbeeld. De tooling dient het maken van policies voor microsegmentatie te ondersteunen.
De reeds aanwezige centrale tooling van de WLAN-omgeving, dient bij voorkeur te integreren of direct beschikbaar te zijn vanuit de nieuwe beheeromgeving.
Authenticatie voor het inloggen op netwerkcomponenten dient middels de centrale directory plaatsvinden.
De beheer tooling dient te voorzien in authenticatie en autorisatie waarbij meerdere autorisatie groepen gecreëerd kunnen worden met verschillende toegangsrechten tot de netwerkcomponenten.
Beheerverkeer dient logisch gescheiden te zijn van productieverkeer.

7.2 Functionele Eisen

De functionele eisen voor netwerk-beheer kunt u vinden in het document “Bijlage 7 – B Programma van Eisen”

8. NAC

8.1 Functionele Beschrijving

De functie Network Access Control (NAC) maakt veilige toegang tot de LAN- en WLAN-access mogelijk. Toegang tot het netwerk wordt gerealiseerd door het authentiseren en autoriseren van randapparatuur en/of gebruikers tegen de NAC-policy server.
De belangrijkste functies van NAC zijn:

- Authentiseren en autoriseren van toegang tot het netwerk voor alle gebruikers en devices op het LAN;
- Authentiseren en autoriseren van toegang tot het netwerk voor alle gebruikers en devices op het WLAN;
- Optioneel: Automatische profiling van randapparatuur;
- Integratie met de bestaande Active Directory domeinen;
- Integratie met tooling waaronder Intune;
- Integratie met de firewall-oplossing (PaloAlto).

De NAC-oplossing dient redundant uitgevoerd te zijn zodat beschikbaarheid tegen de 100% aanzit. Uitval van één locatie of tijdens upgrade mag geen invloed hebben op de beschikbaarheid. Om deze reden dient de NAC-oplossing redundant te zijn uitgevoerd over minimaal twee locaties.
De belangrijkste functie van NAC is het toegang geven tot het netwerk aan de hand van wie je bent en welk device je gebruikt. Hierbij dient gebruik te kunnen worden gemaakt van meerdere statische kenmerken zoals username/password of certificaten, maar ook attributen afkomstig uit AD en Intune. Naast deze statische kenmerken dient optioneel ook profiling van randapparatuur mogelijk te zijn. Middels profiling kan randapparatuur automatisch herkend en vervolgens gegroepeerd worden om specifieke autorisatie-profielen te kunnen realiseren.
Vertrouwde randapparatuur en gebruikers kunnen volledig toegang krijgen tot een bepaald segment (VLAN) van het productienetwerk.
Ook in het geval van onbekende of nieuwe randapparatuur dienen deze automatisch in een gasten netwerk geplaatst te kunnen worden. Dit netwerk dient middels een gastenportaal beperkte toegang tot bijvoorbeeld enkel internet te geven.
Reguliere 802.1x protocollen waaronder Kerberos, EAP-TLS maar ook MAC Authentication dienen ondersteund te worden.
Eveneens dient de NAC-oplossing geïntegreerd te kunnen worden met de bestaande Active Directory Domein, Azure AD en Intune . Daarnaast moet gegevensuitwisseling met PaloAlto mogelijk zijn.

8.2 Functionele Eisen

De functionele eisen voor NAC kunt u vinden in het document “Bijlage 7 – B Programma van Eisen”