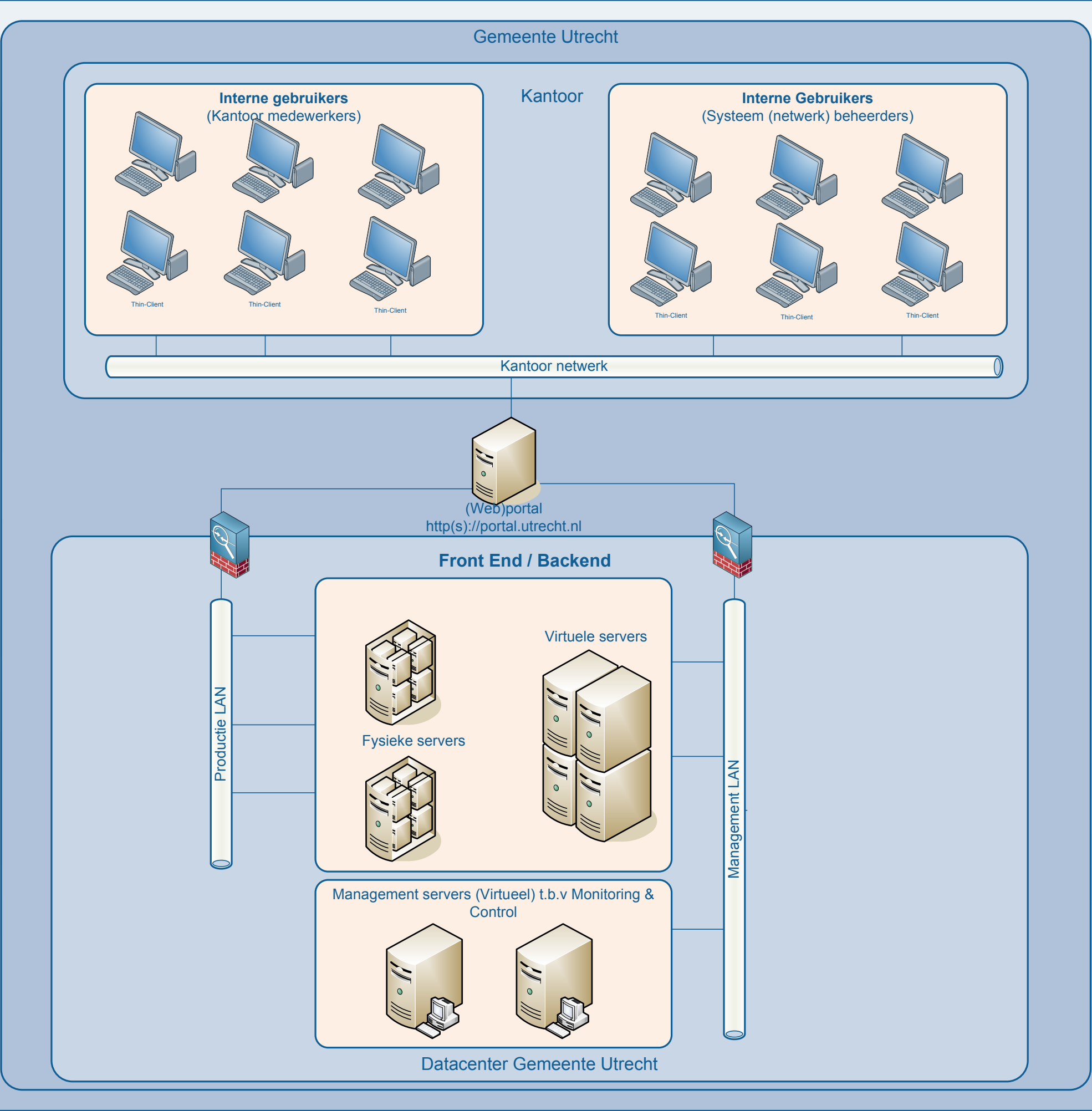
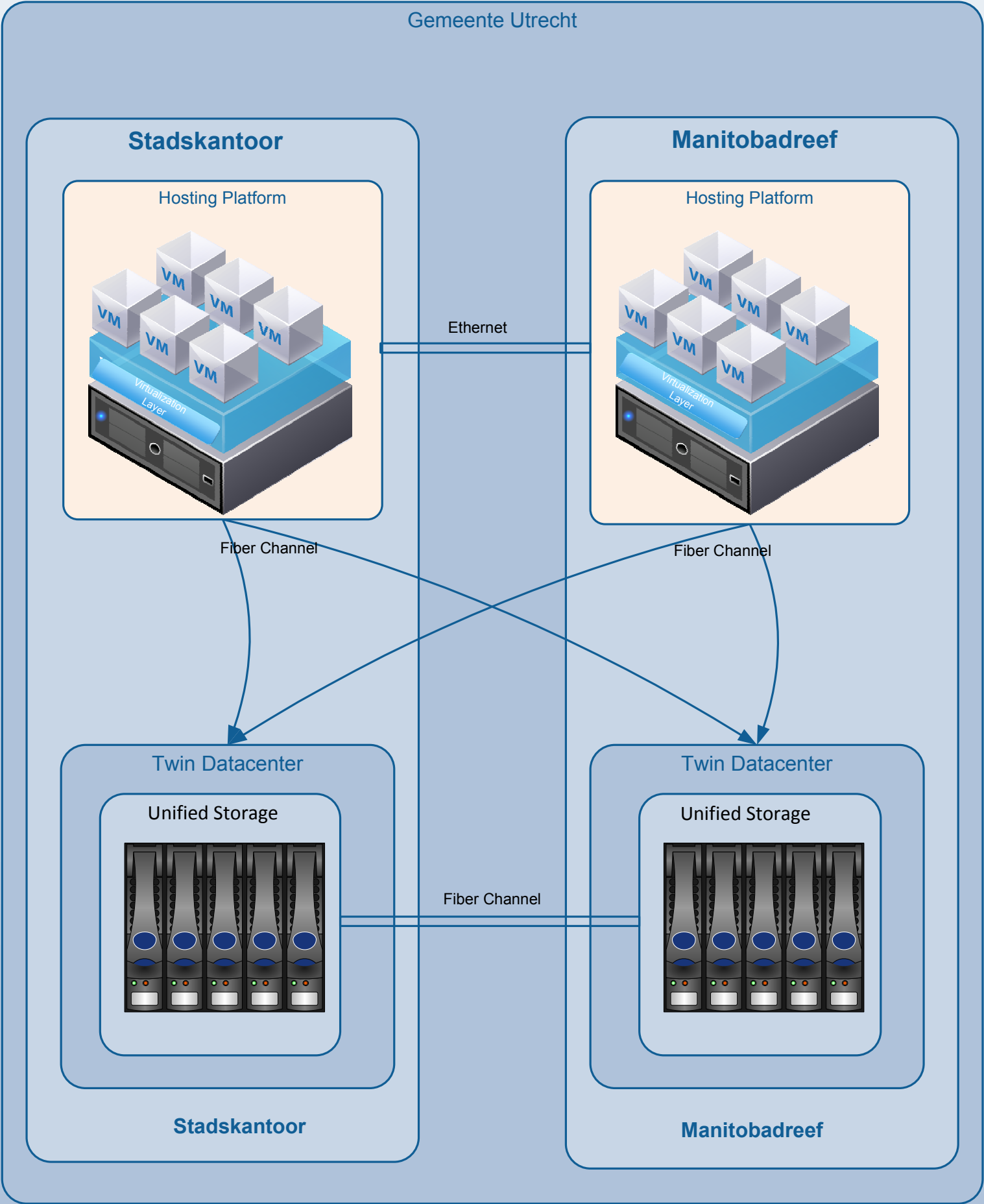




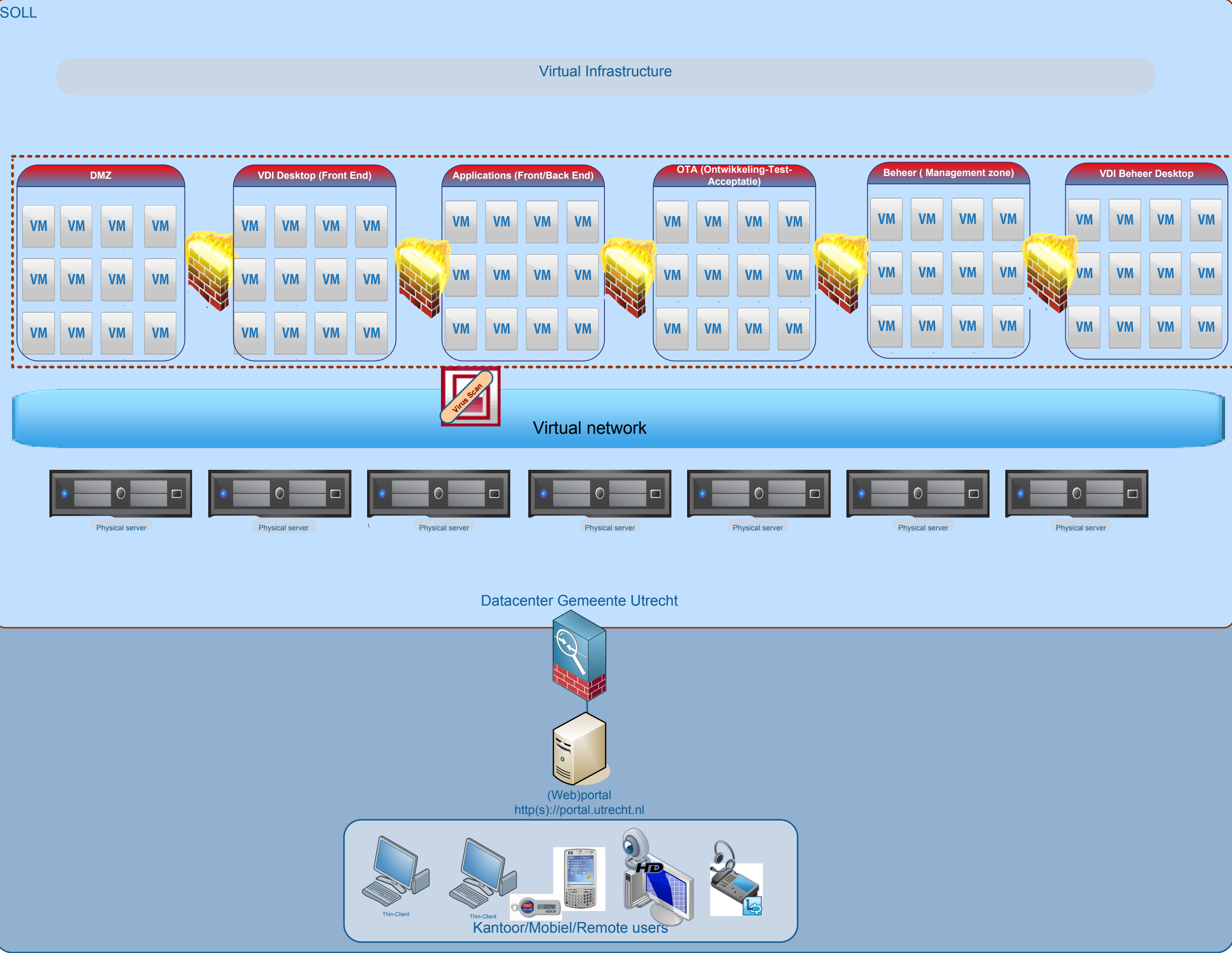
Werkplekken van de Gemeente Utrecht worden aangesloten op een nieuwe virtuele desktop infrastructuur. Vaste werkplekken krijgen de beschikking over een Thin-Client.

Twin Datacenter



De Gemeente Utrecht maakt gebruik van het Twin Datacenter concept. Beide datacenters zijn elkaars spiegelbeeld en er zijn evenveel resources beschikbaar aan beide zijden. 50 % van de beschikbare resource capaciteit in het tweede datacenter (Manitobadreef) komt ten goede aan de OTA omgeving. In de OTA omgeving worden alleen applicaties getest.

Bij uitval van het primaire datacenter zal er een failover plaatsvinden naar het secundaire datacenter waar de services zullen worden opgestart (en vice versa). De OTA omgeving komt in geval van een disaster recovery te vervallen.



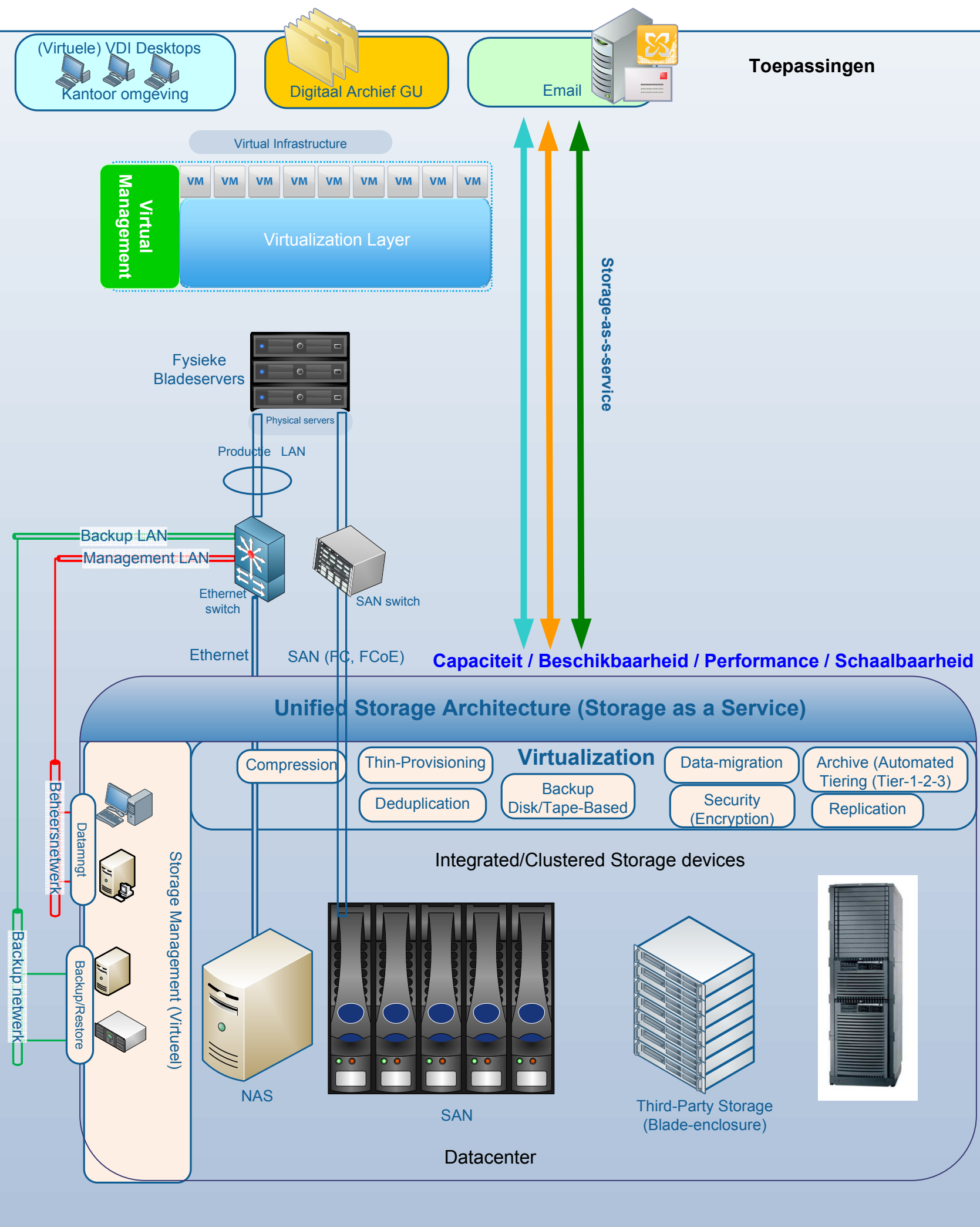
De fysieke servers zijn verspreid over beide datacenters (twin-datacenter concept). De virtuele machines zijn middels virtuele switch (es) aangesloten op de hypervisor laag.

In de virtuele omgeving wordt Zonering en Filtering (Firewall, Content scanning en Virusscanning) toegepast ten behoeve van:

- Scheiding van Domeinen (LAN, Beheer, DMZ)
- Scheiding clients (VDI desktops) en applicaties
- Scheiding van Productie en OTA
- Bescherming tegen netwerk bedreigingen

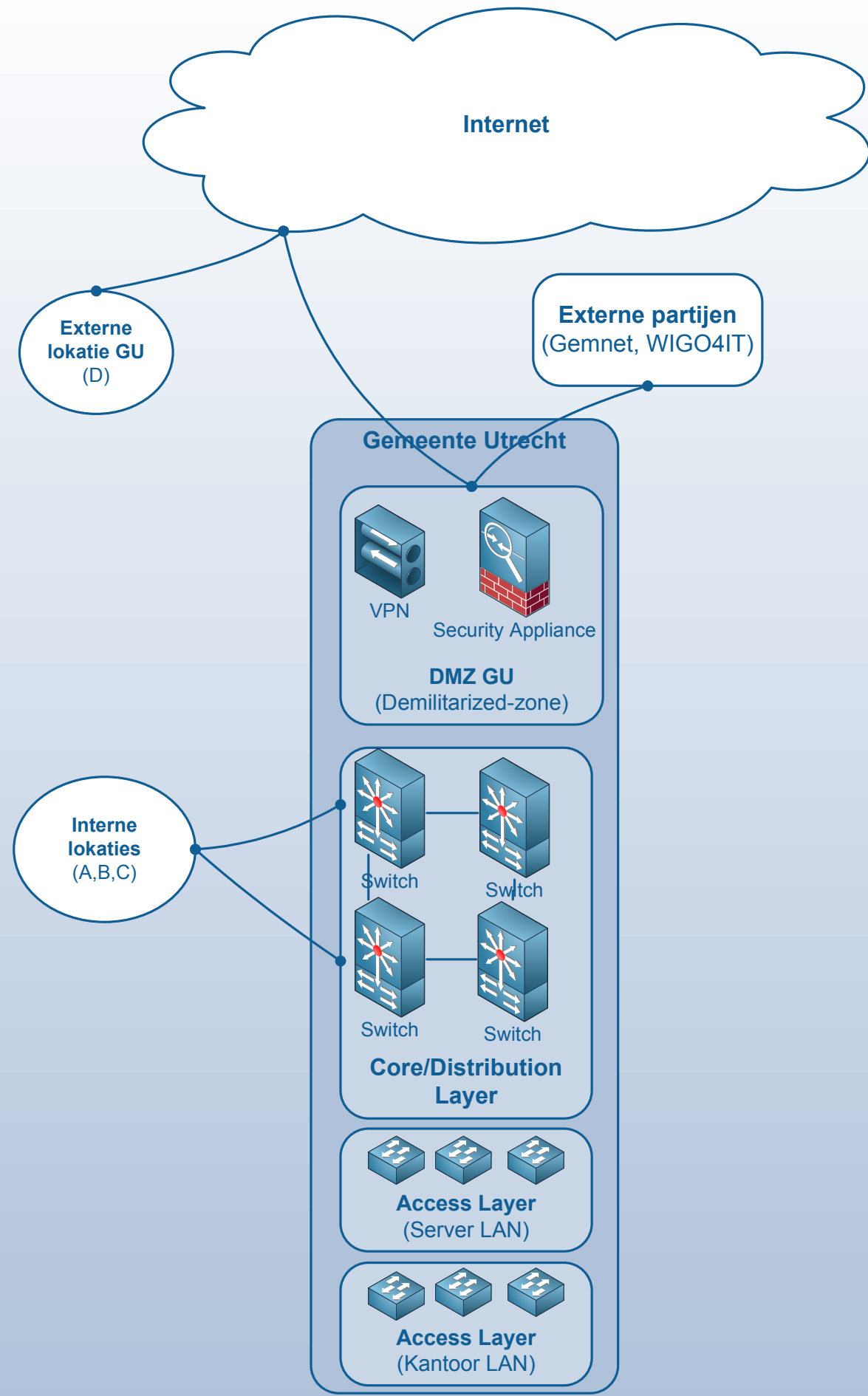
Functionaliteiten zijn verspreid over beide datacenters. OTA daarentegen beperkt zich alleen tot het tweede datacenter. In de OTA omgeving worden alleen applicaties getest.

Virusscanning vindt plaats middels een virtual appliance in de hypervisor laag.



Het storage platform bestaat uit SAN en/of NAS storage. De SAN storage wordt via Fiber Channel (en mogelijk via (FCoE) Fiber Channel-over-Ethernet) ontsloten en de NAS storage via Ethernet. De SAN en NAS storage worden centraal in het datacenter geplaatst.

De storage virtualizatielaag integreert diverse storage functionaliteiten zoals Compressie, Dataduplicatie, Thin-Provisioning, Datamigratie, Tiering (1-2-3), replicatie etc.). De virtualizatielaag biedt aan toepassingen als VDI-desktops, een virtuele disk (LUN of file share) aan. Deze laag verzorgt de clustering van de fysieke storage devices (o.a. van verschillende leveranciers) en maakt het platform hardware onafhankelijk.

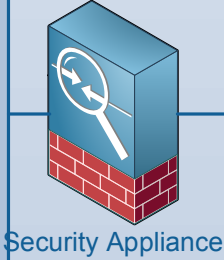
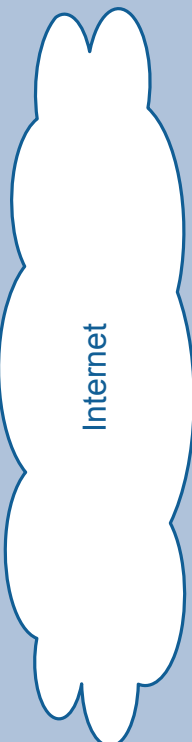


1. Kleine locaties zijn via VPN ontsloten op de DMZ. Er zijn meerdere DMZ netwerken over meerdere locaties.
2. De Core/Distribution Layer bestaat uit 2 aparte lagen: Core Layer en Distribution Layer.

1. Externe locaties (D-locaties) van de Gemeente Utrecht (GU) worden via de DMZ ontsloten. Alle services worden vanuit de twin datacenters van de Gemeente Utrecht geleverd. Ontsluiting van Internet en Externe partijen (GEMnet, WIGO4IT) van de Gemeente Utrecht is gecentraliseerd en is via de DMZ.
2. Grote locaties (A,B,C locaties) van de Gemeente Utrecht worden rechtstreeks gekoppeld met de centrale Backbone switches in de twin datacenters (Stadskantoor en Manitobadreef)
3. Vanaf het LAN (Kantoor, Datacenter en Backbone) is geen rechte koppeling mogelijk met Internet en externe locaties. Alle verkeer (web en mail) gaat door de security appliances en virusscanners.
4. Het interne LAN netwerk van de Gemeente bestaat uit een Kantoor LAN (Interne gebruikers), Datacenter LAN (Servers) en geïntegreerde Core en DistributionLayer.

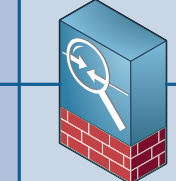
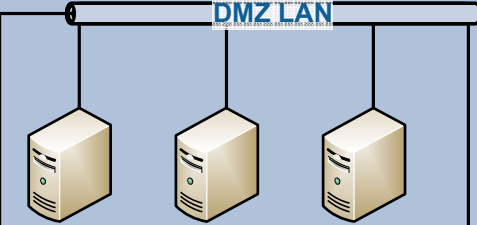
Externe netwerken

Externe partijen
(Gemnet,
WIGO4IT)



Security Appliance

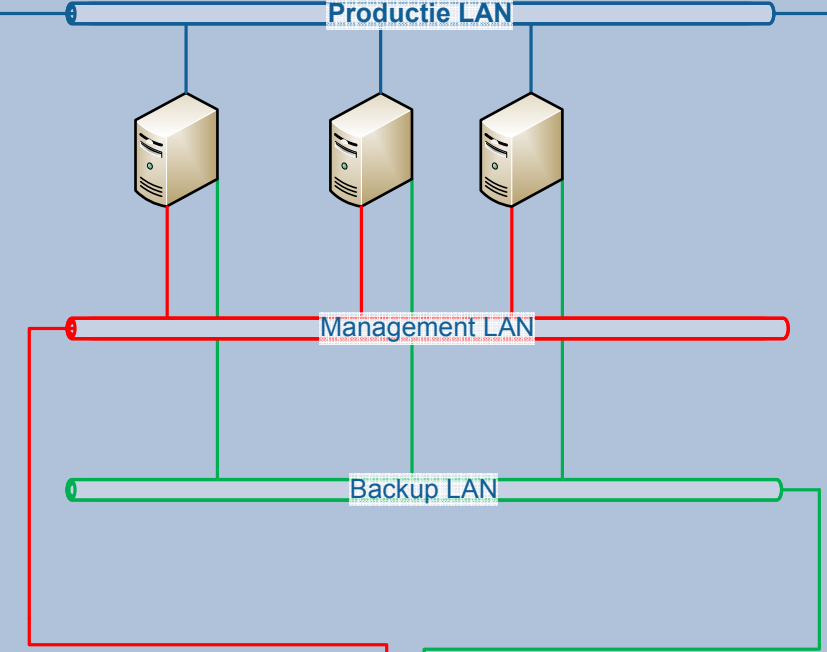
DMZ (Demilitarized-zone)
Gemeente Utrecht



Security Appliance

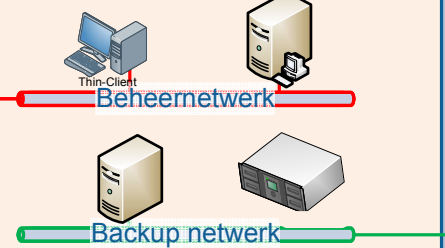
Datacenter Gemeente Utrecht

Front End



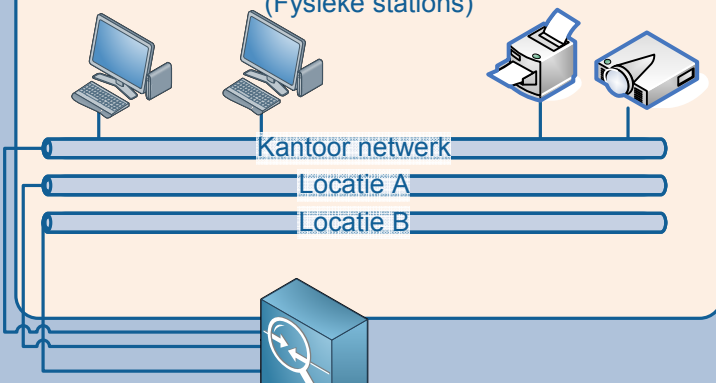
Gemeente Utrecht

Beheerders



Gemeente Utrecht

Interne Gebruikers
(Fysieke stations)



Voor de Gemeente Utrecht worden aparte logische netwerken ingericht.

DMZ

Dit netwerk is uitsluitend vanuit Internet en externe netwerken benaderbaar.

Productie

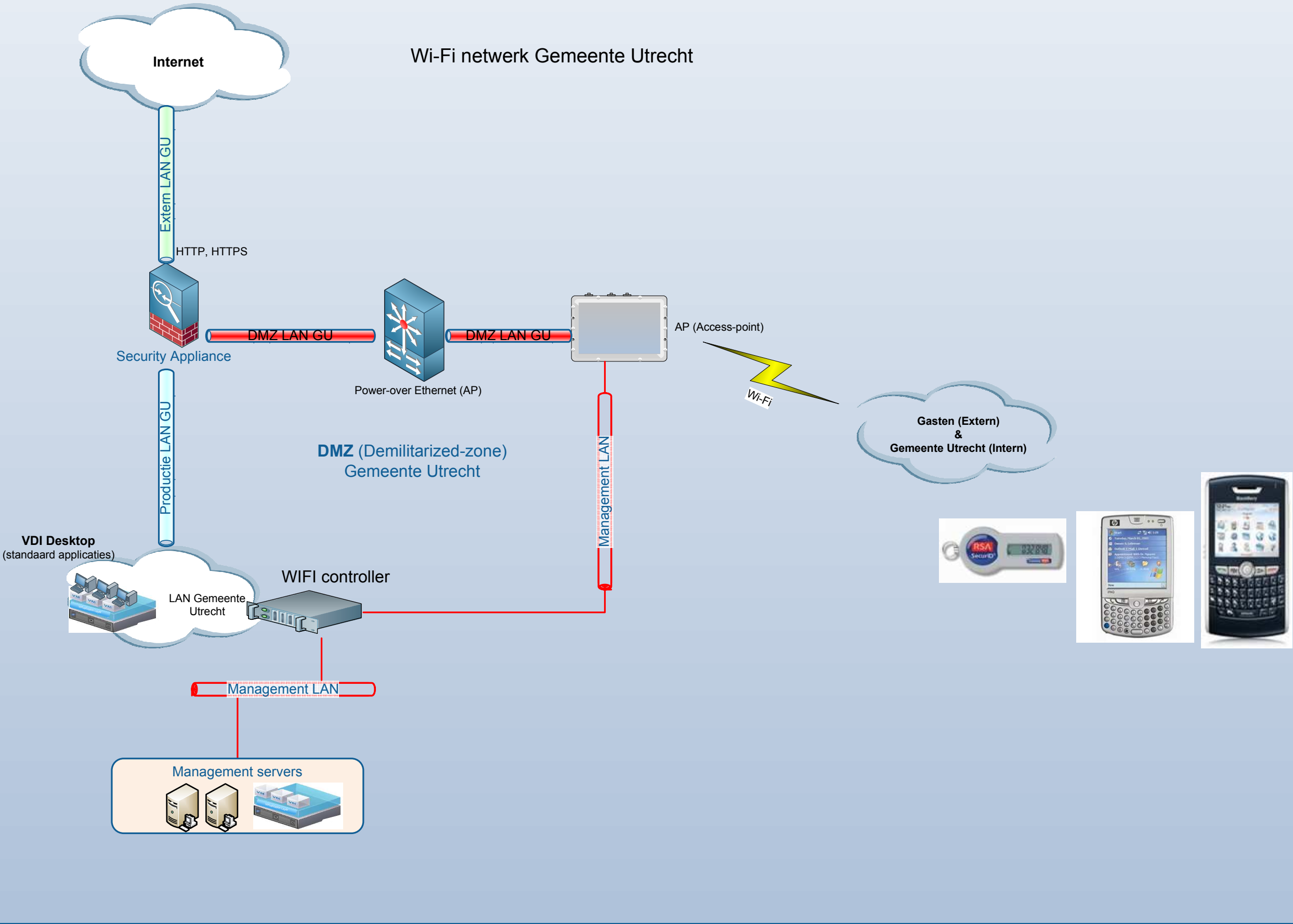
Dit is het netwerk dat gekoppeld wordt met het kantoor netwerk en overige interne locaties van de Gemeente.

Management

Via dit netwerk wordt het beheer op de omgeving uitgevoerd. Het management netwerk is gekoppeld aan het beheerdersnetwerk bij de Gemeente Utrecht waarin zowel de monitoring & control servers als de beheerwerkplekken zijn aangesloten.

Backup

Dit netwerk is aangesloten op het backup netwerk bij de Gemeente Utrecht. Al het backup verkeer loopt via dit netwerk.



Het Wi-Fi netwerk biedt internettoegang voor zowel de Interne medewerkers van de Gemeente als Externen.

Het Wi-Fi netwerk is een beveiligd netwerk. Versleuteling van het netwerk vindt plaats d.m.v. een security policy (WPA2 met een Pre-shared key).

Domstad Productie omgeving

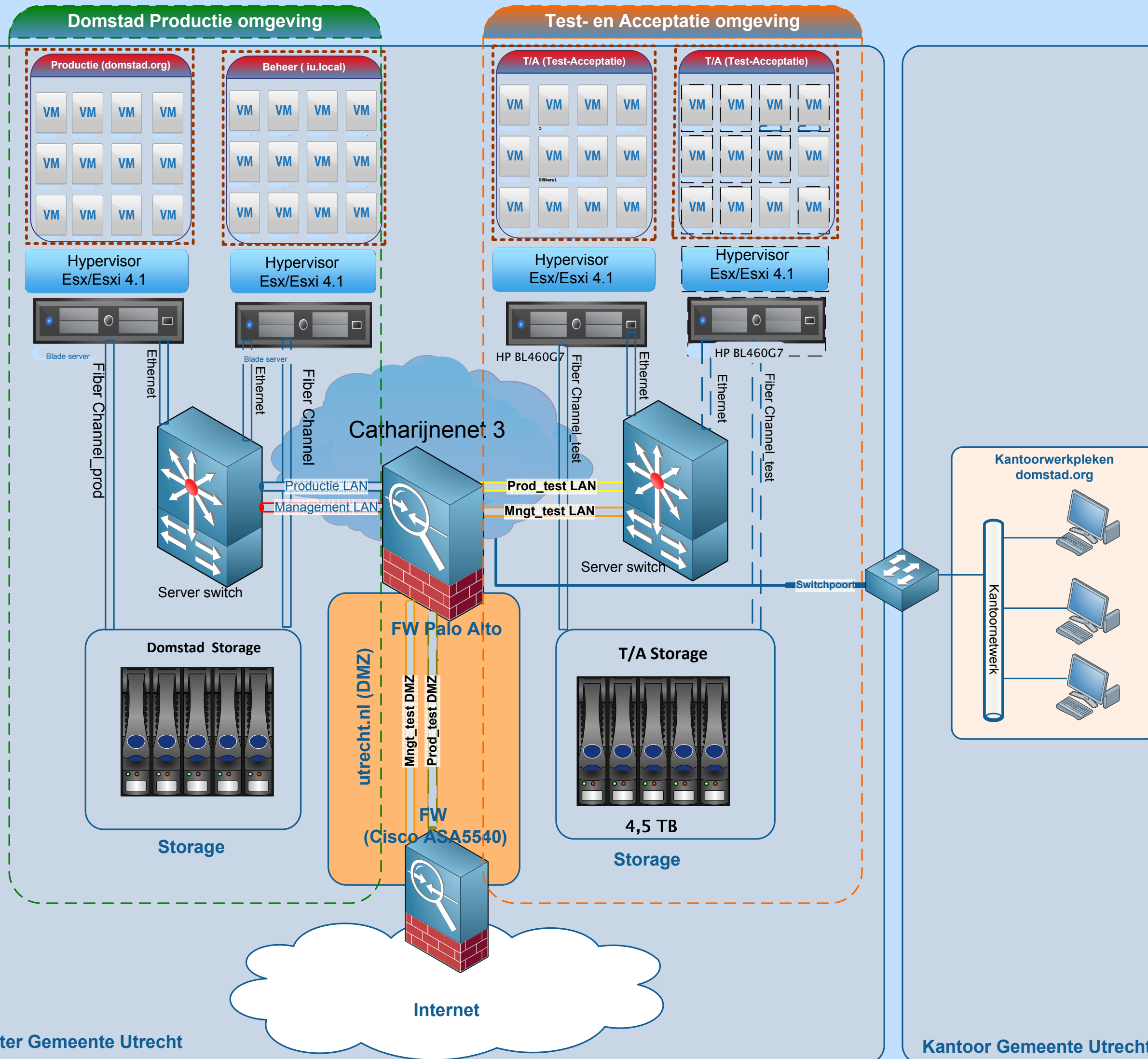
Test- en Acceptatie omgeving

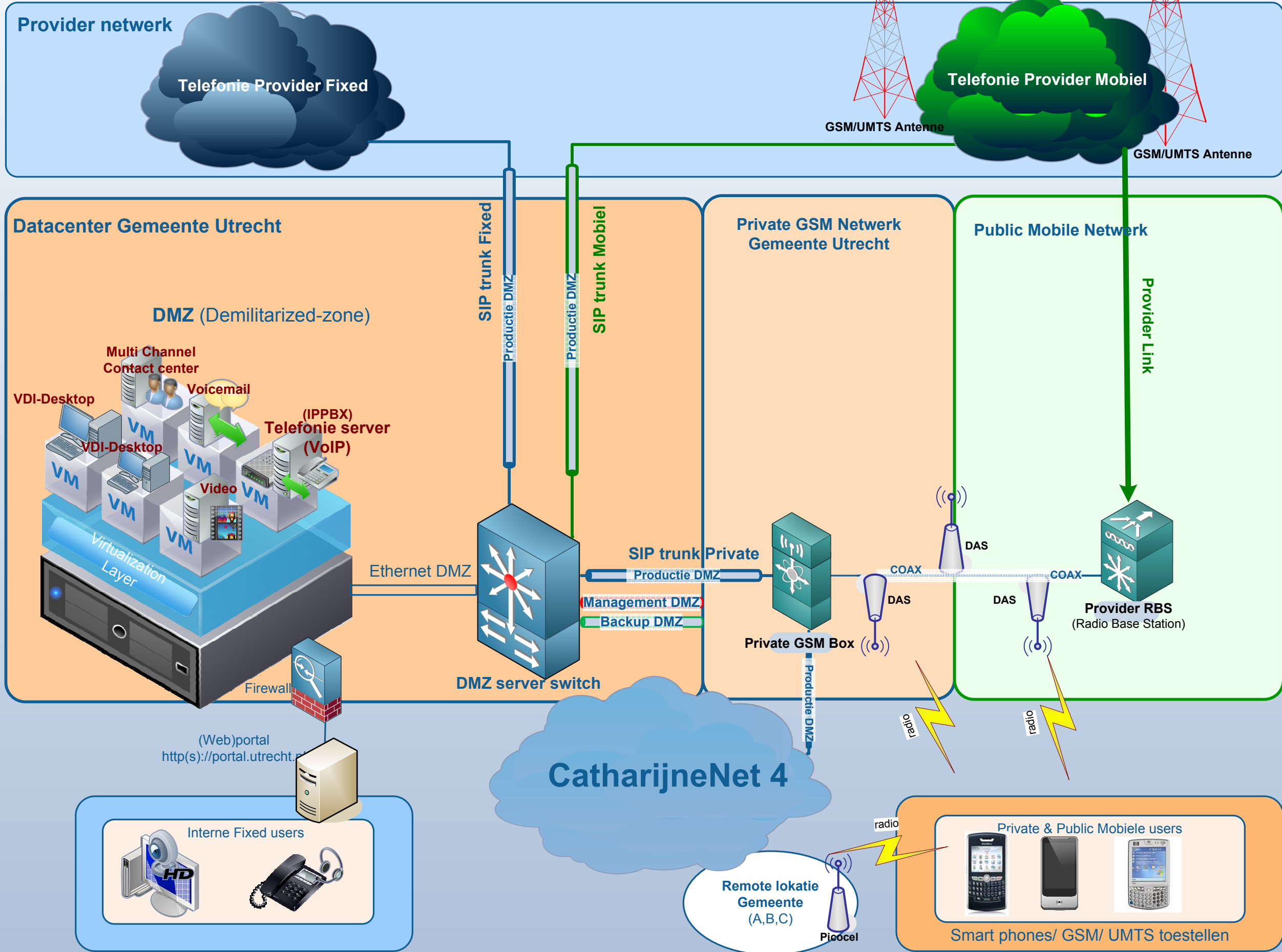
Test- en Acceptatie omgeving (T/A)

- De T/A omgeving is een logisch gescheiden test- en acceptatieomgeving.
- Er wordt gebruik gemaakt van aparte virtuele netwerken voor de T/A omgeving
- De T/A omgeving maakt gebruik van de generieke internetvoorziening.

Datacenter Gemeente Utrecht

Kantoor Gemeente Utrecht





SOLL:

Fixed Network:

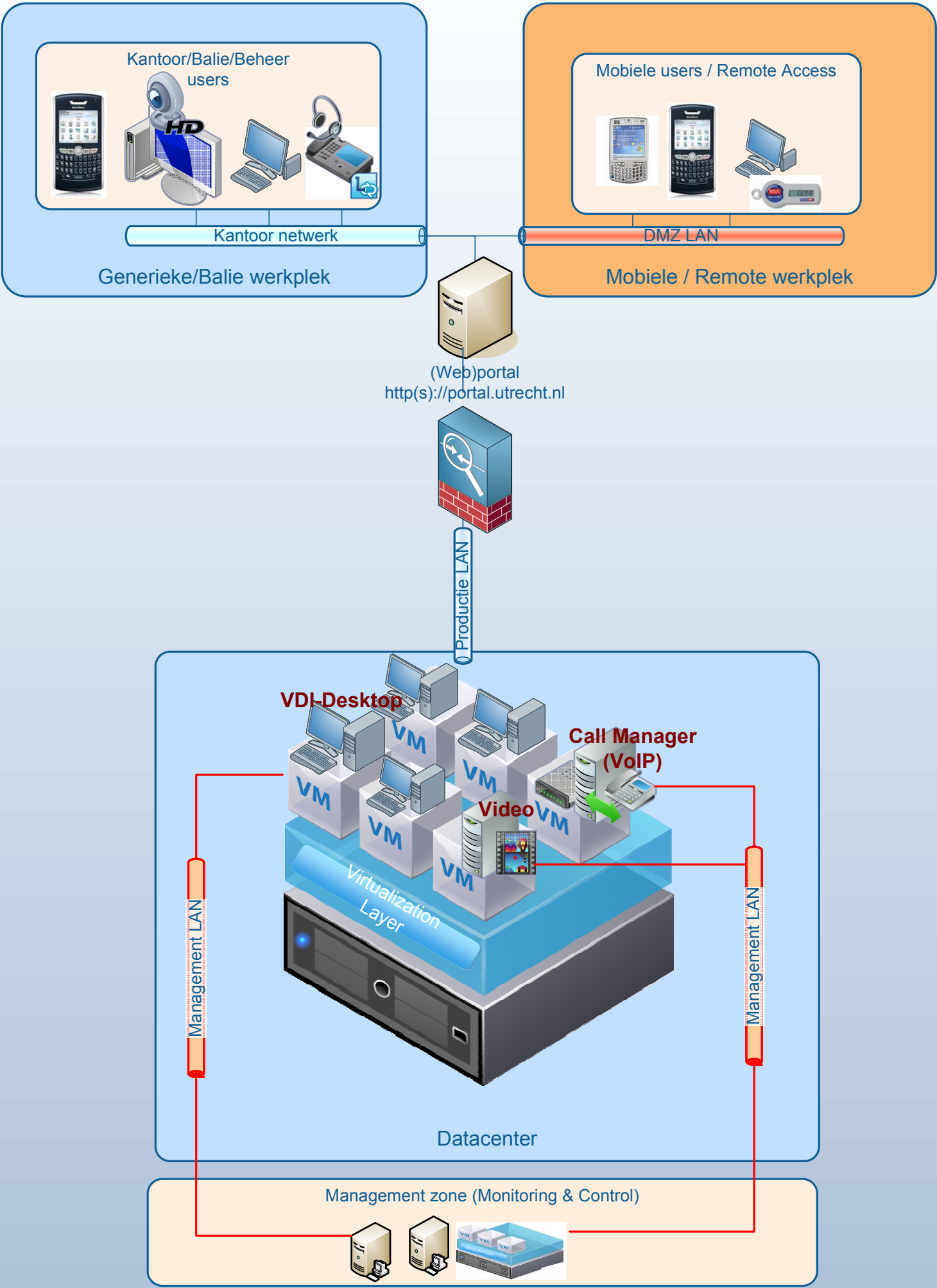
De IPPBX (virtuele appliance) biedt alle telefonie functionaliteiten aan de vast VoIP toestellen op het interne network. De IPPBX is redundant uitgevoerd over beide datacenters en heeft een externe koppeling (SIP trunk Fixed) met het openbare telefonienetwerk. Via dit netwerk wordt de 030- 286xxxx nummerreeks gerouteerd naar alle vaste (VoIP) toestellen op het interne netwerk.

Private GSM Network:

Alle interne medewerkers van de Gemeente Utrecht krijgen de beschikking over private GSM toestel. Dit mobiele toestel is alleen te gebruiken op interne lokaties van de Gemeente (waaronder Stads kantoor en remote lokaties, geclassificeerd als A, B en C). De interne toestellen beschikken allen over een zogenaamde White labeled SIM card en hebben via de Private GSM box onderling een verbinding. De Private GSM box (virtuele appliance) biedt voldoende dekking en signaalsterkte op alle interne locaties. Middels de koppeling (SIP trunk Private) met de IPPBX is er ook een verbinding met de vaste VoIP toestellen. Het aantal Private GSM toestellen bedraagt ongeveer 2500.

Public Mobile Network:

Het aantal interne medewerkers met een mobiel abonnement bedraagt ongeveer 2000. De GSM/ UMTS toestellen kunnen zowel intern als extern, op publieke locaties worden gebruikt. Op publieke locaties is er radio ontvangst via de aanwezige UMTS/GSM antenne van de mobiele provider. In het Stads kantoor is er ontvangst via het indoor DAS systeem (Distributed Antenna system) van de Gemeente. Het DAS heeft een koppeling met de Radio Base Station van de mobiele provider. Het DAS systeem biedt voldoende dekking en signaalsterkte kwaliteit voor zowel de private als public mobile devices. Daarnaast heeft het mobiele netwerk een koppeling (SIP trunk mobiel) met de vaste telefonieomgeving, de zogenaamde vast mobiel integratie. Elke datacenter beschikt over 1 SIP trunk naar het mobiele netwerk van de provider (Twin-datacenter concept).



De fysieke werkplekken (Thin Clients) zijn aangesloten op een virtuele VDI desktop infrastructuur.

Mobiele devices (Smartphones, iPad's, Laptops) van de Gemeente hebben via WiFi (Intern) of via Internet (Remote/ Thuiswerkplek) toegang tot de virtuele desktop omgeving. Toegang is op basis van 2-factor Authentication