Openbare Europese aanbesteding

Connectiviteit via wifi en ethernet

Bijlage 08 – Functionele omschrijving huidige situatie

Datum : 1 mei 2023

Deze bijlage is integraal onderdeel van de Aanbestedingsleidraad van deze aanbesteding.

deltion college

In deze bijlage zijn de volgende onderwerpen opgenomen:

08.1 Inleiding

Het doel van deze functionele omschrijving is de aanbieder inzicht te geven in het functioneren van het huidige netwerk van Deltion College. Dit functioneren komt terug in de lijst met eisen en wensen en “use cases”. De beschreven functionaliteiten moeten ook in het nieuwe netwerk werken. Technisch mag de opzet wel verschillen.

08.2 Enterprise netwerk

Het Deltion College eist dat de nieuwe netwerkinfrastructuur van ‘enterprise’ niveau is. Hiermee wordt bedoeld dat de netwerkinfrastructuur alle functionaliteiten bevat die noodzakelijk worden geacht in een netwerkinfrastructuur van deze omvang (concurrent clients piek is ongeveer 50.000). Denk aan:

- Centraal beheer
- Configuratie op basis van template en automation
- Toegang (door netwerkclients) op basis van identiteit.
- ‘Security’ is een integraal onderdeel van de oplossing en configuratie.
- Bescherming tegen algemeen bekende netwerkproblemen. Bijvoorbeeld: OSI-laag-2 loops.
- Broadcast en multicast filtering.
- Een intelligent radio managementsysteem.
- Ondersteuning van alle hedendaagse standaarden.
- Toekomstvast:
  - Verwachte adoptie van nieuwe standaarden.
  - Schaalbaar ontwerp.

De wens is te werken met leveranciers uit het ‘leaders’ kwadrant van het ‘Enterprise Wired and Wireless LAN Infrastructure’.

08.3 Fysieke opbouw

De Deltion campus bestaat uit twaalf gebouwen die fysiek onderling zijn verbonden (niet vanuit een netwerk technische invalshoek) via een centrale hal (de Boulevard). Buiten de campus zijn er externe locaties waar Deltion onderwijs aanbiedt: Gebouw Grijs, Lux38 (CEN in diagram 8.1), Sprint Lyceum (BAG in diagram 8.1), Praktijkhal Opleiding Transport en Logistiek, Werkplaats Opleiding Motorvoertuigentechniek en De Hooglaer (zie ook **Bijlage 2 Locaties en plattegrond van de Campus**).

De externe locatie hebben hun eigen vezels. De campus kent twee serverruimten: één in gebouw Bordeaux en één in gebouw Olijf.

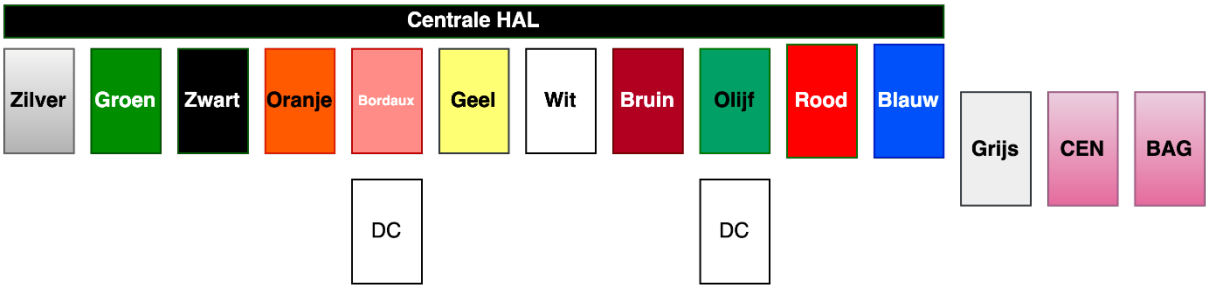

Diagram 8.1: Overzicht gebouwen

In elk gebouw zijn meerdere patchkasten waar switches geplaatst zijn met verbindingen naar een centrale ruimte in dat gebouw. In sommige gevallen betreft het kleine patchkasten met maar één access switch, deze enkele access switch is dan verbonden via de uplink naar de access switches in een centrale ruimte. Deltion noemt deze kleine patchkasten ACP's. Vanaf de centrale ruimte in elk gebouw zijn er verbindingen naar de serverruimtes.

Op basis van de fysieke eigenschappen van de Deltion campus zal de netwerkinfrastructuur volgens een bepaald principe moeten worden opgebouwd.

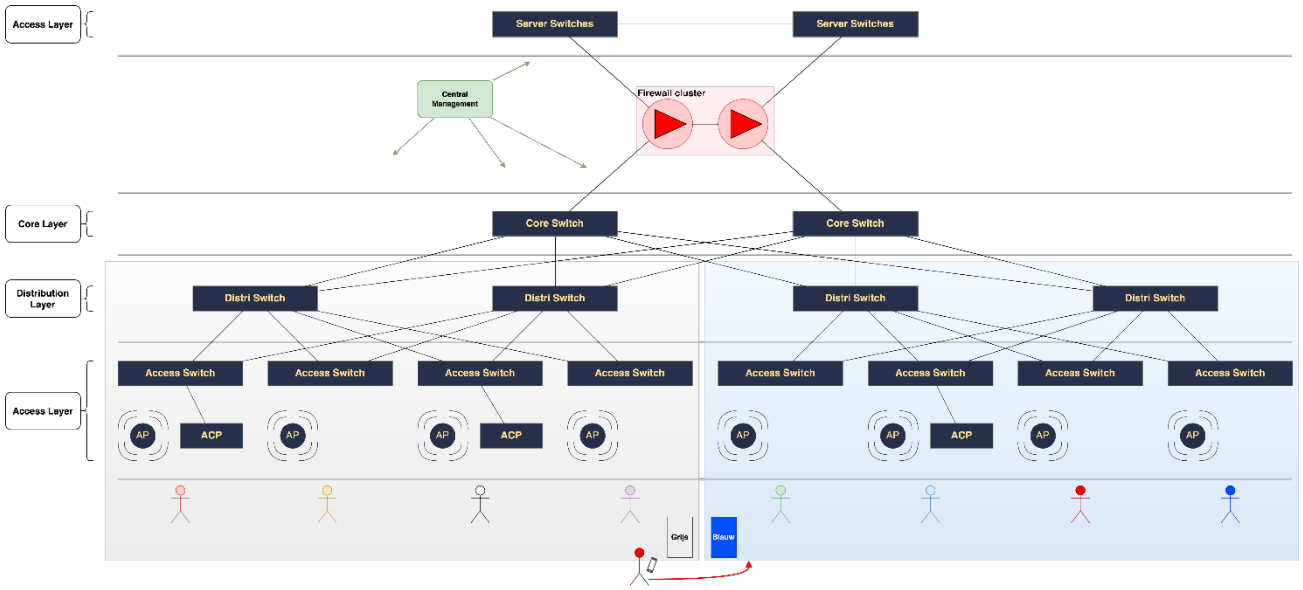

Diagram 8.2: Overzicht ontwerp fysiek

Een traditioneel 'core – distribution – access layer' ontwerp zoals weergegeven in diagram 8.2 is de huidige fysieke opzet, maar is zeker geen must.

Bij het installeren of vervangen van apparatuur in de 'Access Layer' detecteren switches dat een 'Access Switch' of Wi-Fi access point wordt aangesloten en configureren de switchpoorten waarop wordt aangesloten automatisch volgens een template. De aangesloten apparatuur maakt verbinding met de centrale beheeromgeving, upgrade naar de gewenste firmware versie en ontvang een configuratie volgens een template.

Beheer van alle switches en wifi wordt centraal uitgevoerd vanuit één integraal managementsysteem.

08.4 Netwerk security

Het netwerk van Deltion College is opgedeeld in verschillende zones en subzones waartussen filtering plaatsvindt op basis van het ‘least privilege’ principe. Dat houdt in dat datastromen alleen worden toegestaan indien noodzakelijke voor de werking van het systeem.

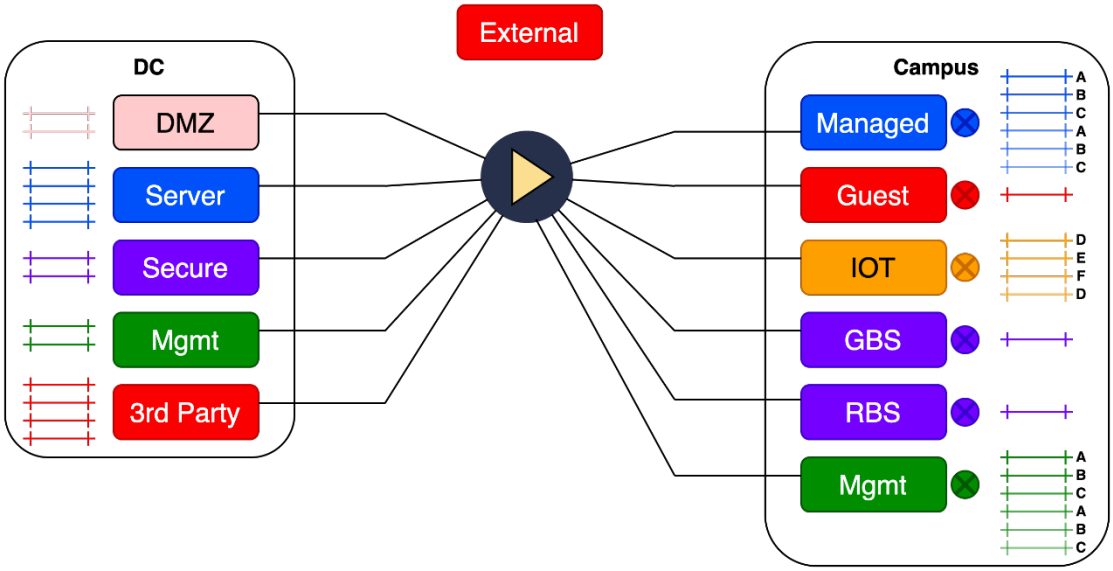

Diagram 8.3: Overzicht netwerkzones

Diagram 8.3 geeft weer welke netwerkzones bestaan binnen het netwerk van Deltion. De centrale firewall is het koppelvlak tussen alle zones en op basis van de firewall policy wordt bepaald welke datastromen wel en niet zijn toegestaan. In het datacenter is dit in de huidige omgeving opgelost door verschillende subnetten en vlans te configureren die via de centrale firewall worden gerouteerd. Deze configuratie moet ook mogelijk zijn in de aangeboden netwerkinfrastructuur.

De situatie op de campus is complexer:

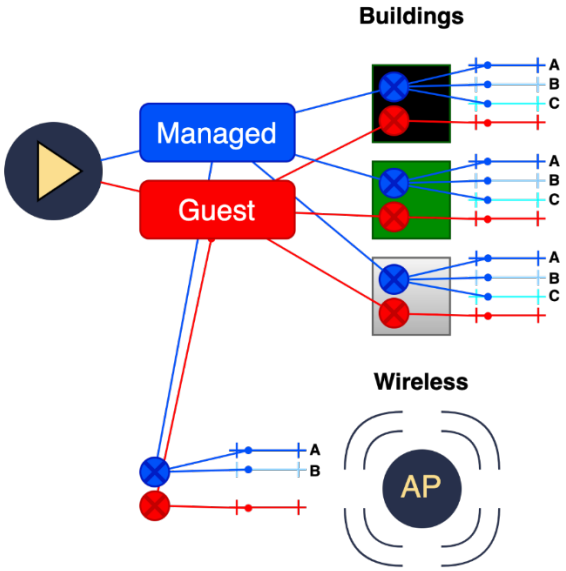

Diagram 8.4: Overzicht netwerkzones campus

- Op elke distributie switch is per netwerkzone een VRF gedefinieerd. Elke VRF is via een aparte logische interface gekoppeld met de centrale firewall. Het voorbeeld met drie gebouwen plus Wi-Fi en twee VRF's levert al acht koppeling op de centrale firewall, in werkelijkheid zijn er meer VRF's en meer gebouwen.
- Subzones (A, B en C) worden op de distributieswitches met ACL's geconfigureerd. Deze ACL's zijn om het beheersbaar te houden eenvoudig. Hieronder een vereenvoudigd voorbeeld:
  - allow subzone A <--> subzone A (alleen als onderling verkeer tussen hosts nodig is)
  - allow subzone B <--> subzone B (alleen als onderling verkeer tussen hosts nodig is)
  - allow subzone A --> subzone B (alleen als verkeer tussen subzone A en B nodig is)
  - block zone <--> zone
  - allow any (dit wordt op de centrale firewall gefilterd)
- Wi-Fi wordt centraal gerouteerd, vanwege de huidige op tunnels gebaseerde oplossing.

De functionele gedachte achter bovenstaande traditionele manier van configureren blijft als eis staan.

- Filtering tussen netwerkzones door de centrale firewall.
- Blokkeren van lokaal verkeer binnen een subzone en andere subzones binnen de netwerkzone wordt gerealiseerd binnen de LAN-infrastructuur.
- Basale filtering tussen subzones binnen een netwerkzone indien noodzakelijk wordt gerealiseerd binnen de LAN-infrastructuur.

De uitdaging in de huidige configuratie zit in het volgende:

- Alle routing vindt plaats op de distributieswitches en de centrale firewall. Tussen de firewall en elke VRF is een logische koppeling. Door de hoeveelheid distributieswitches en VRF's zijn er veel logische koppeling die het geheel onoverzichtelijk maken.
- Beheersen van datastromen binnen een zone en subzones wordt geconfigureerd middels ACL's. Dit wordt via de CLI met de hand gedaan per distributiesswitch.

Vereenvoudigen zonder verlies van functionaliteit is een vereiste.

08.5 Toegang tot de netwerk access laag

Toegang tot de netwerk access laag geschiedt altijd middels een vorm van authenticatie een succesvolle authenticatie resulteert in een bepaalde autorisatie. In het huidige netwerk een rol (Wi-Fi) en/of VLAN.

Beheerde werkplekken authentiseren middels een 802.1x, eap-tls middels een via Intune of AD GPO verkregen certificaat.

IOT-systemen authentiseren middels een WPA2-PSK die per type systeem zijn uitgegeven (DPSK of MPSK) en MAC-authenticatie of alleen MAC-authenticatie bij een bedrade aansluiting. Een hoop andere typen apparatuur authentiseert op basis van MAC-authenticatie.

In alle bovenstaande gevallen geschiedt dit via Radius en wordt een rol of vlan toegewezen door de Radius server.

Naast bovenstaande wordt eduroam aangeboden. (https://eduroam.org/).

Tot slot zijn er verschillende gastennetwerken waarbij een externe gastenportal op Aruba Clearpass gehost wordt. Toegang geschiedt op basis van een gastenaccount of bij een evenement met alleen een gebruikersvoorwaarden acceptatie. De samenwerking met Aruba Clearpass voor authenticatie is een vereiste.