

Wifi- en netwerkomgeving

- Wifi 6E (802.11AX inclusief onderliggende versies);
- 2.4, 5 en 6 GHz frequentie en mogelijkheid om deze netwerken tegelijkertijd aan te zetten (TRIPLE RADIO);
- Signaalsterkte tussen -30 dBm (uitstekend) en -60 dBm (minimaal voor goede connectiviteit);
- Gebruik door aantal gebruikers, gastgebruikers met een device ratio van 3:1;
- Het dagelijkse dataverkeer in Annex XIII Dagelijkse dataverkeer wifi- en netwerkomgevingen;
- Bij overschakeling accesspoints geen (ver)storing in de wifiverbinding;
- Uitval van een accesspoint mag niet leiden tot verlies van een verbinding;
- Meerdere (cliënt) VLAN's te ondersteunen en mogelijkheid bieden om meerdere wifinetwerken (leerlingen, medewerkers, gasten, etc.) aan te kunnen maken;
- Accessswitches worden redundant middels de 10 GB aansluitingen aangesloten op de distributieswitches;
- Co channel interferentie wordt voorkomen of tot een minimum beperkt;
- Ondersteunt draadloze toegangscontrolesystemen, zoals slimme sloten en beveiligingscamera's, die zorgen voor veilige toegang en toezicht binnen het gebouw;
- Faciliteert het gebruik van Building Management Systems (BMS) die verschillende gebouwfuncties (verwarming, ventilatie, airconditioning, verlichting) centraal beheren en automatiseren;
- Verzamelen data van verschillende systemen en apparaten binnen het gebouw, wat kan worden gebruikt voor realtime monitoring, voorspellend onderhoud en optimalisatie van gebouwprestaties;

Beveiliging en authenticatie

De wifi- en netwerkomgeving moet ten minste de volgende authenticatie- en encryptiewijzen ondersteunen en beschikbaar zijn voor toepassing door de Aanbestedende dienst: WPA2-Enterprise, WPA2-PSK, WPA2, WPA3, 802.1X, 802.XX, MAC-adressen, 'Captive Portal' en 'Certificate Based Authentication', TKIP en AES, profiling op type devices/ op vast en draadloos netwerk, Intune, MAC authenticatietabel, certificaten als sources.

Alle hardware

- Inschrijver levert hardware die voldoet aan de minimale specificaties in Annex XII.A Minimale specificaties en van een merk in het leader kwadrant van Annex XII.B Gartner Magic Quadrant wired and wireless LAN. Let op: Levering van hardware het merk Huawei is niet toegestaan.
- Dual stack IPv4/IPv6
- Verlopen licenties op de hardware mag niet leiden tot uitval functionaliteit

Accesspoint

- Voorzien van een PoE-aansluiting type 3 of 4 PoE (compatible met accessswitch)
- Geen externe antenne
- Roaming mag niet leiden tot connectiviteit issues
- Mogelijkheid redundant (2x) aansluiten op aparte accessswitches

WLAN-controller

- Iedere WLAN-controller is redundant uitgevoerd
- Kan worden voorzien van live upgrades

Accessswitch

- Op iedere switch of switch-stack dient ten minste 25% van de totale poortcapaciteit vrij te blijven voor toekomstige uitbreidingen
- Iedere switch of switch-stack dient te voorzien in een PoE-vermogen dat minstens 125% bedraagt van het maximaal benodigde PoE-vermogen voor alle actieve poorten die Inschrijver gebruikt voor zijn aangeboden wifi- en netwerkomgeving ongeacht het aantal poorten of het PoE-type (PoE, PoE+, of PoE++) (let op: deze overcapaciteit bedraagt te allen tijde minimaal 80 watt)
- Iedere switch of stack (afhankelijk van de indeling) dient afzonderlijk geüpdatet of geüpgraded te kunnen worden zonder de functionaliteit van het netwerk te beïnvloeden
- Alle poorten zijn voorzien van een PoE-aansluiting type 3 of 4 (compatible met accesspoint)
- Vier (4) 10 Gbit/sec poorten
- Overige poorten 1 Gbit/sec
- Hybride poort configuratie (Colorless ports)
- Stacking optie

Authenticatie en beveiliging

Network Access Control

- Controleert de identiteit van gebruikers en apparaten voordat ze toegang krijgen tot het netwerk
- Bepaalt welke netwerkbronnen toegankelijk zijn voor geauthenticeerde gebruikers en apparaten, afhankelijk van hun rol of beleidsregels
- Faciliteert veilige netwerktoegang voor gasten, vaak met beperkte privileges en tijdsgebonden toegang
- Controleert of apparaten voldoen aan beveiligingsbeleid en normen voordat ze toegang krijgen, zoals up-to-date antivirussoftware, patches, en firewall-instellingen
- Biedt oplossingen of stappen om niet-conforme apparaten te helpen voldoen aan de vereisten
- Plaatst apparaten in specifieke VLAN's op basis van hun rol, type, of nalevingsstatus om het netwerk te segmenteren en de beveiliging te verbeteren
- Past gedetailleerdere segmentatie toe binnen het netwerk om de verspreiding van bedreigingen te minimaliseren
- Verhindert apparaten die niet voldoen aan de beveiligingsvereisten om verbinding te maken met het netwerk
- Plaatst potentieel onveilige apparaten in een quarantainezone voor verdere beoordeling en correctie
- Houdt het netwerkverkeer en de status van verbonden apparaten in realtime bij
- Biedt gedetailleerde rapporten over toegangsgebeurtenissen, naleving, en beveiligingsincidenten voor analyse en auditing
- Firewall configuratie
- MAC based authenticatie
- EAP TLS/ EAP PEAP
- Govroam-integratie
- Gasten netwerk/ verlooptijd vrij configureerbaar
- Profiling op basis van verschillende sources (VLANs, rechten en bandbreedte toewijzen)