Toekomstige situatie beschrijving

gemeente DE WOLDEN

Gemeente Hoogeveen

Inhoudsopgave

1 Inleiding

De toekomstige situatie beschrijving is een cruciaal onderwerp dat aandacht verdient in het kader van de aanbestedingsprocedure. Het begrijpen van deze situatie is van belang voor potentiële inschrijvers, omdat het hen in staat stelt om een goed doordacht voorstel te formuleren dat voldoet aan de behoeften en uitdagingen van SWO De Wolden Hoogeveen.

2 De toekomstige netwerkinfrastructuur

De toekomstige netwerkinfrastructuur van SWO moet aan verschillende eisen en trends voldoen om te zorgen voor betrouwbaarheid, prestaties, schaalbaarheid, beveiliging en flexibiliteit. Hier zijn belangrijke aspecten waarop een toekomstige netwerkswitch-infrastructuur en WiFi Access Points, hierna te noemen “netwerkcomponenten”, moet anticiperen.

2.1 Hoge bandbreedte, snelheid en lage latency

Met de toenemende vraag naar dataverkeer en de adoptie van technologieën zoals 5G of WiFi 6, moeten toekomstige netwerkcomponenten in staat zijn om hoge bandbreedte en snelheid te bieden. Dit kan worden bereikt door het gebruik van 10Gbps, 25Gbps, 40Gbps, 100Gbps en hogere snelheden.

2.2 Schaalbaarheid

Ondanks de beperkte groei voor de komende jaren moeten de netwerkcomponenten schaalbaar zijn om nieuwe gebruikers, apparaten en services te ondersteunen zonder grote infrastructurele wijzigingen.

2.3 Convergentie

Toekomstige netwerkcomponenten moeten in staat zijn om verschillende netwerkverkeerstypen te ondersteunen, waaronder data, spraak en video, om te voldoen aan de behoeften van moderne communicatie.

Videovergaderen behoort sinds Corona tot de standaard binnen de digitale werkplekomgeving van SWO. Het ligt in lijn der verwachtingen dat ook bellen via Teams geïntroduceerd gaat worden.

2.4 Energy Efficiency

Milieuvriendelijkheid wordt steeds belangrijker. Efficiënte stroomvoorziening en energiebesparende functies moeten worden geïntegreerd in netwerkcomponenten.

2.5 Open Standaarden en Interoperabiliteit

Het is belangrijk dat de netwerkcomponenten voldoen aan open standaarden, zoals Spanning Tree Protocol (IEEE 802.1D), VLAN (IEEE802.1Q), Quality of Services (IEE802.1p), WiFi 6 (IEEE802.11ax), IPv4 en IPv6, LLDP etc, en in staat zijn om te integreren met diverse andere netwerkapparatuur en -technologieën, in de huidige en toekomstige situatie. Bijvoorbeeld, de nieuwe netwerkcomponenten moeten naadloos aansluiten op de huidige firewall configuratie.

Daarnaast omarmt SWO de ‘Pas toe of leg uit’ en Aanbevolen Open Standaarden zoals is vastgelegd bij Forum Standaardisatie.

2.6 Toekomstbestendigheid

De fabrikant van de netwerkcomponent en de Inschrijver kan goed omgaan met de verwachte technologische veranderingen, hierbij denkende aan aanpassingen op en aanbieden van nieuwe functionaliteit moeten doormiddel van softwarematige aanpassingen of bewegingen richting de cloud.

Resumerend, de toekomstige netwerkinfrastructuur van de SWO moet flexibel, schaalbaar, beveiligd en geoptimaliseerd zijn voor de evoluerende behoeften van moderne organisaties en technologieën. Het is belangrijk om continu op de hoogte te blijven van nieuwe ontwikkelingen in netwerktechnologie om ervoor te zorgen dat de infrastructuur aan de vereisten van de toekomst voldoet.

3 Beveiliging

Netwerkcomponenten moeten robuuste beveiligingsfuncties bieden, zoals microsegmentatie en geavanceerde authenticatie om te voldoen aan de groeiende bedreigingen voor de netwerkbeveiliging. In de toekomstige situatie wil en kan SWO cloud diensten niet uitsluiten en zal hierop geanticipeerd worden.

3.1 Microsegmentatie

Op de netwerkinfrastructuur dient microsegmentatie tot de mogelijkheden te worden geïntroduceerd. De uitgangspunten daarvoor zijn:

- Datacenter laag: Segmentatie op basis van VRF, Private VLAN en laag 3 VLAN's op de switches. Op basis van mix and match wordt per service bekeken wat de beste oplossing is. Deze servers worden statisch in het juiste netwerk geplaatst.
- Access laag: Endpoint isolatie waarbij verkeer wordt geïsoleerd of kan worden gefilterd.

3.2 Toegang

De oplossing zal geschikt moeten zijn om in een later stadium automatisch de mate van toegang tot het netwerk en blokkering te regelen, afhankelijk van ingestelde beleidsregels. Hierbij denkende aan de open standaard 802.1X (Network Access Control) waarmee de netwerkcomponent kan verifiëren of een gebruiker of apparaat gemachtigd is om een verbinding te maken met het netwerk voordat deze toegang krijgt tot netwerkbronnen. Het aansluiten van een niet geauthentiseerd apparaat leidt in ieder geval tot een administrative shutdown van de poort en een melding in/via het monitoringsysteem.

3.3 Identiteiten

De beperkte identiteiten ten behoeve van het beheer / onderhoud van de netwerkcomponenten dienen zorgvuldig te worden vorm gegeven. Hierbij rekening houdend dat SWO steeds meer beweegt richting het afnemen van diensten in de cloud, zoals het gebruik van een identiteitendienst. Met betrekking tot de netwerkcomponenten mag er geen afhankelijkheid van een externe identiteitendienst of andere externe diensten bestaan. Toegang dient bij een netwerkverstoring te allen tijde te worden verkregen door onder andere het introduceren van een breaking glass procedure.

3.4 Richting de cloud

Het afnemen van diensten in de Cloud is wat meer en meer een gegeven is binnen SWO. Ook ziet de SWO dat netwerkvendoren zich met specifieke oplossingen bewegen richting de cloud, dit vanuit o.a. beheergedachte en beveiliging waarbij AI wordt toegepast. Indien zich een dergelijke beweging voordoet, zullen conform de BIO de risico’s worden geïdentificeerd, gemitigeerd en/of geaccepteerd. Een belangrijke handreiking die het SWO hiervoor hanteert, is BIO Thema-uitwerking Clouddiensten.

4 Beschikbaarheid

De hoge beschikbaarheid van het netwerk is een cruciaal aspect van een ICT-infrastructuur. Het verwijst naar de mate waarin diensten operationeel blijven en toegankelijk zijn, zelfs in het geval van storingen, fouten of (on)geplande gebeurtenissen.

Om een hoge beschikbaarheid van het netwerk te waarborgen, is het implementeren van redundantie op verschillende niveaus van het netwerk ingeregeld. Een belangrijk aspect wat hier onderdeel van uitmaakt, is het kunnen detecteren van fouten en deze te herstellen. Dit omvat mechanismen voor het automatisch detecteren van storingen en het schakelen naar redundantie wanneer dat nodig is, zonder handmatige tussenkomst. Te denken valt aan protocollen/technieken zoals STP, VRRP, Stacking, Link Aggregation, bekabelingsredundantie, etc.

Het hebben van een DR-plan is van cruciaal belang voor het herstellen van netwerkservices na grootschalige calamiteiten, zoals cyberaanvallen. Dit omvat het maken van offsite-back-ups, gegevensherstelprocedures en failover-plannen. Het hebben van een DR-plan voor de netwerkcomponenten, die onderdeel uitmaken van de aanbesteding, maakt onderdeel uit van de aanbesteding.

5 Verantwoordelijkheden

SWO wil het beheer deels uitbesteden. Onderstaand staat beschreven hoe SWO hier een invulling aan wil geven.

5.1 Beheerverantwoordelijkheden

Van de Inschrijver wordt verwacht dat deze voor het hardware technische aspect verantwoordelijk is, denkende aan:

- Het plaatsen van de netwerkcomponent in de MER en SER;
- Het leveren wat nodig is in de MER en SER-ruimtes om de netwerkcomponenten in de infrastructuur op te nemen, denkende aan tranceivers, bekabeling etc.;
- Het aansluiten van de netwerkcomponent waarbij de configuratie-instellingen gezamenlijk met de SWO worden vastgesteld en geïmplementeerd;
- De gezondheid en status van de netwerkcomponent monitort;
- Geconstateerde hardware-defecten oplost, in samenwerking met SWO;
- Updates/Upgrades uitvoert.

SWO zal daarentegen meer het configuratie- en beleidsaspect op zich nemen, denkende aan:

- Het netwerkplan waar de Inschrijver in gekend wordt;
- Het beheer op poortniveau;
- Het aansluiten van de apparaten aan het netwerk.

5.2 Incidentbeheer

Het incidentbeheer verzorgt de primaire afhandeling van vragen, wensen en verstoringen, inclusief de communicatie van en naar de melder van het incident.

Het vormen van een 1e, 2e en 3e lijns aanspreekpunt voor vragen en problemen, het in behandeling nemen van geplaatste calls en het bewaken van de continuïteit van de dienstverlening.

De definitie voor 1e, 2e en 3e lijn zoals SWO die hanteert is:

1e lijns-incidenten worden door aangewezen medewerkers van SWO opgepakt en opgelost.

Indien een incident niet zelfstandig kan worden opgepakt, doordat deze te complex van aard is of betrekking heeft op de bij de Inschrijver ondergebrachte dienstverlening, zal dit door aangewezen medewerkers van SWO worden doorgezet naar de **2e lijn**. Die draagt zorg voor de registratie, het routeren van calls naar de betreffende kennisgroep, het bewaken van de voortgang, het oplossen en het afsluiten van de calls.

De **3e lijn** betreft de kennisgroep binnen het serviceteam van de Inschrijver. Deze onderzoekt de oorzaak van het incident en bepaalt de mogelijke oplossing. De oplossing wordt vervolgens uitgevoerd binnen de daartoe gestelde service niveaus.

6 Monitoring, Alerting en Logging

Een uitgebreid beheer- en monitoringssysteem is essentieel om de gezondheid en prestaties van de netwerkinfrastructuur te bewaken en problemen snel op te lossen. Vanuit die gedachte is het hebben van een centraal punt nodig om het beheer van de netwerkcomponenten efficiënt en effectief te laten plaatsvinden.

6.1 Monitoring en Alerting

Een actieve monitoring van het netwerk is essentieel om problemen snel op te sporen. Het gebruik van de juiste tooling kan helpen bij het bewaken van prestaties en het genereren van waarschuwingen bij afwijkingen.

Monitoring van het gehele netwerk, dient deel uit te maken van de oplossing. Hierbij dient o.a. vanuit alerting perspectief aangesloten te worden op Zabbix.

6.2 Updates/Upgrades

Vanuit de management tool dient het mogelijk te zijn om updates/upgrades uit te voeren voor de netwerkcomponenten die voor de aanbesteding van toepassing zijn.

6.3 Logging

Logdata die door netwerkcomponenten wordt geproduceerd dient centraal binnen het netwerkmanagement platform te worden verzameld. In de nabije toekomst moet het mogelijk zijn om deze logdata richting een centraal logplatform door te sturen.