Technische Infrastructuur Gemeente Zaanstad

Bestemd voor de Europese aanbesteding VTH

Inhoudsopgave

1 Inleiding 3

2 Standaarden ICT Infrastructuur Gemeente Zaanstad 4

2.1 Database 4

2.2 Basiswerkplek 4

2.3 PC server 4

2.4 Midrange server 4

2.5 Netwerk 4

2.6 Netwerk Apparatuur 4

2.7 Storage 5

2.8 Streaming media protocollen 5

2.9 Standaard firewall poorten 5

2.10 Twee factor Authenticatie (2FA) 5

1 Inleiding

De Europese aanbesteding VTH betreft de selectie en implementatie van een nieuw Vergunningverlening, Toezicht en Handhaaf systeem.

In dit document zijn de standaarden voor de technische infrastructuur beschreven van de Gemeente Zaanstad. Indien uw oplossing On Premise geleverd wordt dan dient deze te kunnen functioneren conform de in dit document beschreven standaarden.

2 Standaarden ICT Infrastructuur Gemeente Zaanstad

2.1 Database

Database:	Oracle 12c (12.2.0.1)
Tools:	Standaard Oracle tools
Client:	Oracle 12c (32 en 64 bits)

Database:	Microsoft SQL server 2016 of Microsoft SQL Server 2012
Tools:	SQL Server Management Studio
Client:	ODBC koppeling / OLEDB / Native Client 2012

2.2 Basiswerkplek

Hardware:	VMWare View Virtual desktop 2 vCPU met 8GB memory
Besturingssoftware:	Windows 10 Enterprise versie 1803
KA omgeving:	Office 2016 Professional Plus
Internet explorer:	Versie 11 onder Windows 10
Applicatie distributie:	App-V 5.1

2.3 PC server

Hardware (rack):	HP ProLiant DL380p / DL360p / Dell PowerEdge R640 / R740

Besturingssoftware:	Windows Server 2012 R2 x64 of Windows Server 2016 x64
Virtualisatie	VMware ESXi 6.5

2.4 Midrange server

Hardware:	IBM S922
Besturingssoftware:	AIX Versie 7.2

2.5 Netwerk

Netwerk:	Ethernet 1Gb / 10Gb / 40Gb
Protocols:	TCP/IP, OSPF, (BGP Internet)

Afstanden tussen de twee data centers max 6,5 km

2.6 Netwerk Apparatuur

Firewall:	Palo Alto PA-3250
Switches:	Juniper EX2300, EX4300, EX4600, QFX5100
Routers:	Juniper QFX5100
Applicatie Proxy:	F5 BigIP, APM
Loadbalancer:	F5 Networks BIG-IP 4200 (TMOS 14.1.x) LTM en APM Wordt gebruikt in DMZ en intern
Wifi:	Aruba networks 802.11 a,b,g en n
802.1x:	Aruba clearpass
IPAM / DNS / DHCP:	Infoblox trinzic 1410 zonder GRID

2.7 Storage

SAN Switch:	HPE SN3000B
SAN/NAS:	VNX5200 (file & block)/Fujitsu DX100/DX200/Isilon X210
Protocol:	CIFS/NFS/Fiber Channel
FC speed:	16GB

2.8 Streaming media protocollen

Bestands formaat: alle bestanden die door Microsoft media player afgespeeld kunnen worden zonder extra plugins.
Geen MMS omdat dit een oude Microsoft standaard is die niet meer ondersteund word door Microsoft.
Geen ondersteuning van Quicktime en Realmedia.

2.9 Standaard firewall poorten

De standaard poorten die naar buiten open staan zijn:
HTTP poort 80 deze gaat via de Proxy naar de firewall
FTP poort 21/22
HTTPS poort 443 deze gaat via de Proxy naar de firewall
SMTP poort 25 deze gaat via de Barracuda anti spam firewall

De standaard poorten die naar binnen open staan zijn:
SMTP poort 25 deze gaat via de Barracuda anti spam firewall
Geen poorten direct naar binnen maar via een F5 of server in de DMZ
Web server in principe achter de F5 in de DMZ zodat deze SSL off loading / balancing / authenticatie kan doen.

2.10 Twee factor Authenticatie (2FA)

Redundante Vasco Identikey Server
Type tokens: Vasco Digipass for Mobile Enterprise Security en DP300 tokens

Streaming media protocollen

Max grootte: 128kbs

Bestands formaat:

- Alle bestanden die door Microsoft media player afgespeeld kunnen worden zonder extra plugins.
- Geen MMS omdat dit een oude Microsoft standaard is die niet meer ondersteund word door Microsoft.
- Geen ondersteuning van Quicktime en Realmedia.

Standaard firewall poorten

De standaard poorten die naar buiten open staan zijn:

- HTTP poort 80 deze gaat via de Proxy naar de firewall
- FTP poort 21/22
- HTTPS poort 443 deze gaat via de Proxy naar de firewall
- SMTP poort 25 deze gaat via de Barracuda anti spam firewall

De standaard poorten die naar binnen open staan zijn:

- SMTP poort 25 deze gaat via de Barracuda anti spam firewall
- Geen poorten direct naar binnen maar via een F5 of server in de DMZ
- Web server in principe achter de F5 in de DMZ zodat deze SSL off loading / balancing / authenticatie kan doen.

Twee factor Authenticatie (2FA)

Redundante Vasco Identikey Server

Type tokens: Vasco Digipass for Mobile Enterprise Security en DP300 tokens