Bijlage 2 – Programma van Eisen

Behorend bij

Firewalls

Zaaknummer: 3925246
Datum: ~~13 juni 2024~~
Gewijzigd: 9 juli 2024
Versie: Definitief

INHOUDSOPGAVE

1 Inleiding bij het Programma van Eisen

Dit document beschrijft aan welke eisen de aangeboden de Oplossing/Externe Firewalls dienen te voldoen. Het programma van eisen is gestructureerd op basis van de Project Start Architectuur (PSA). In hoofdstuk 2 en verder worden per onderdeel van de PSA (applicatiecomponent, applicatiefunctie) de architectuur requirements nader uitgewerkt in één of meer aanvullende eisen.

Let op: de architectuur requirements zijn eveneens eisen waaraan voldaan moet worden.

2 Functionele eisen externe Firewalls

Nr.	Omschrijving
2.1	De Opdracht bestaat uit levering van firewall (hardware) componenten (A-merk), bijbehorende licentie en derdelijns support inclusief implementatie en migratie zoals omschreven in paragraaf 1.5 Beschrijving van de opdracht. De Inschrijver dient volledig te kunnen voldoen aan de opdrachtomschrijving.
2.2	De firewall moet gedurende de levensduur up to date gehouden kunnen worden door Opdrachtgever. Opdrachtnemer stelt de hiervoor benodigde updates en patches aan Opdrachtgever beschikbaar.
2.3	De Oplossing dient voort te komen in de kwadranten leaders van het 'Magic Quadrants for network firewalls' van Gartner. Hierbij passend in de lijst van de A-merk definitie zoals b.v. Checkpoint, Fortinet en Palo Alto.
2.4	Het network design van Opdrachtgever beschrijft het 2DC design. Dit design bestaat uit 2 gelijkwaardige datacenter locaties. Om dit te faciliteren kennen de locaties een eenduidig en gelijk Network Access- en Security beleid op en tussen de locaties. Afwijken van dit beleid, door het introduceren van afwijkende hardware en daarmee separate security policies per device/locatie, betekent sterk verminderde samenhang tussen de locaties. Dit heeft grote gevolgen voor de aangesloten klanten en de dienstverlening van Opdrachtgever. De aangeboden Oplossing dient binnen deze kaders te passen.
2.5	Management van de firewall apparatuur en security policies moet door een 'single pane of glass' service door Opdrachtnemer worden ondersteund. Deze service moet bestaan uit gescheiden management- en analytics functionaliteiten, om de redundantie en beschikbaarheid van system resources te garanderen.
2.6	~~De firewall moet ten minste 8x 100GE QSFP poorten en 16x 25GE SFP28 poorten bevatten~~. De output van de huidige firewall is 4x 10GbE SFP+ poorten en 8x 1GbE RJ45 poorten en 2x 1/10GbE SFP+. De nieuwe firewall moet minimaal aan deze eis voldoen.
2.7	Beheer dient te worden uitgevoerd via een hoog beschikbaar centraal managementsysteem. Middels een set aan volledig geautomatiseerde interfaces moet het mogelijk zijn om diensten te creëren, modificeren en verwijderen en de diensten te optimaliseren gebaseerd op metrics als capaciteit en resiliency. Al deze functionaliteiten, inclusief gerelateerde performance metrics en events moeten beschikbaar worden gesteld via een open gepubliceerde, gedocumenteerde en vrij te gebruiken API. Het volledige beheer dient mogelijk te zijn via deze API. Daarnaast dient er een GUI beschikbaar te zijn die dezelfde functionaliteiten aanbiedt.
2.8	De Oplossing dient inclusief eventuele benodigde trainingen gedurende de implementatieperiode voor drie medewerkers van Opdrachtgever geleverd te worden.
2.9	De Oplossing dient inclusief de benodigde documentatie m.b.t. de firewalls, zoals handleidingen, tutorials, enz. geleverd te worden. De documentatie dient in het

	Nederlands of Engels opgesteld te zijn.
2.10	Bij inkomend verkeer vanaf internet dient SSL-inspectie te worden gedaan. In de toekomst kan bij herziening beleid de mogelijkheid ontstaan dat tevens SSL inspectie bij uitgaand verkeer vereist is.
2.11	De Oplossing ondersteunt de integratie met on-premises Active Directory om regels en logging aan AD-objecten te kunnen koppelen.
2.12	Aan de Microsoft Azure Cloud dient te worden gekoppeld middels een ExpressRoute.
2.13	Firewall cluster moet een active-active oplossing zijn met ondersteuning van virtuele firewall instances.
2.14	Failover dient mogelijk te zijn zonder packetdrops.
2.15	Firewall moet een zogeheten NextGen Firewall zijn (NGFW) met IPS/IDS, advanced threat preventie, deep packet inspection, website filtering, anti-virus, identity management (ActiveDirectory).
2.16	Firewall beschikt over VPN functionaliteit t.b.v. remote access indien gewenst.

3 Implementatie eisen externe Firewalls

Nr.	Omschrijving
3.1	Opdrachtnemer dient als onderdeel van haar inschrijving een implementatieplan in (subgunningscriterium 3). Dit implementatieplan betreft een blauw druk van een definitief implementatieplan die 4 weken na definitieve gunning tussen Opdrachtgever en Opdrachtnemer wordt afgestemd. Bij de nadere uitwerking van het implementatieplan geldt: - Opdrachtnemer stelt een technisch ontwerp en detailontwerp op en laat deze goedkeuren door Opdrachtgever. - Opdrachtnemer is verantwoordelijk voor trainingen en kennisoverdracht aan het personeel van Opdrachtgever, zodat zij in staat zijn om de nieuwe firewall-oplossing effectief te beheren en te onderhouden. Dit geldt ook voor de overdracht van verantwoordelijkheden van de Opdrachtnemer naar de interne IT-afdeling van Opdrachtgever na voltooiing van de implementatie en migratie, inclusief trainings- en ondersteuningsactiviteiten. - Opdrachtnemer is verantwoordelijk voor een goedlopende integratie met de bestaande IT-infrastructuur, inclusief netwerkapparatuur, applicaties en andere systemen - Opdrachtnemer is verantwoordelijk voor het testen en valideren van de Externe Firewalls. Opdrachtnemer maakt een plan op, waaruit Opdrachtgever de zekerheid heeft dat deze correct functioneert en effectief beschermt tegen bedreigingen. - Opdrachtgever wil zo veel mogelijk zekerheid dat de aangeboden oplossing voldoet aan de specificaties. Opdrachtnemer is verantwoordelijk voor de oplevering van een acceptatietest en procedure waarmee dit getoetst kan worden. - Opdrachtnemer is verantwoordelijk voor uitgebreide documentatie en rapportage van de implementatie en migratie, inclusief configuratie-instructies, logboeken, incidentrapporten en andere relevante documentatie. Voortgangsrapportages worden gedurende de implementatieperiode maandelijks opgeleverd. – Opdrachtnemer verzorgt 4 weken na live fase ondersteuning en pakt eventuele kinderziektes aan.

	Opdrachtnemer signaleert tijdig knelpunten, is aanspreekpunt tijdens de uitvoering en treedt op als projectleider om daarmee te zorgen voor afstemming van de activiteiten.
3.2	De transitie dient zo te worden georganiseerd dat er geen verstoringen optreden in het bedrijfsproces. In overleg met de Opdrachtgever worden de momenten bepaald waarop werkzaamheden worden verricht die het bedrijfsproces kunnen verstoren. De inschrijver dient hierbij rekening te houden dat dit type werkzaamheden mogelijk buiten kantoortijden dient te worden uitgevoerd.
3.3	De start van de implementatie vindt plaats na ingangsdatum overeenkomst en wordt uiterlijk in Q1 2025 afgerond.
3.4	Opdrachtnemer evalueert met Opdrachtgever de eerste 6 maanden om de 6 weken en daarna tweemaal per jaar de gang van zaken met betrekking tot de Overeenkomst.

4 Algemene Eisen

Nr.	Omschrijving
4.1	(Technische) documentatie wordt continu up-to-date gehouden door opdrachtnemer en de laatste versie wordt actief gedeeld met Opdrachtgever.
4.2	Medewerkers van de Opdrachtnemer, die in enige mate toegang hebben tot de verzamelde gegevens, zijn gescreend op integriteit, waarbij de minimale eis is dat werknemer bij indiensttreding aan Inschrijver een specifiek voor de functie geldende Verklaring omtrent Gedrag (VOG-verklaring) heeft overlegd, die bij indiensttreding niet ouder is dan 3 maanden.

5 Exit-plan \ Retransitie

Nr.	Omschrijving
5.1	Na gunning levert Inschrijver binnen 6 maanden een Exit-plan waarin minimaal onderstaande punten beschreven worden: • Verantwoordelijkhedenmatrix met daarin de verantwoordelijkheid per organisatie ten tijde van de ontvlechting. • Verwachte doorlooptijden per activiteit. • De kosten die Inschrijver voor de ontvlechtingswerkzaamheden in rekening brengt. Dit kan zijn een all-in prijs of op basis van een uurtarief.
5.2	Indien Inschrijver de werkzaamheden uit een Exit-plan op basis van een uurtarief factureert, dient in het Exit-plan een maximum aantal uren benoemd te worden.
5.3	Indien Inschrijver de werkzaamheden uit een Exit-plan op basis van een uurtarief factureert, zal facturatie op basis van het werkelijk aantal bestede uren plaatsvinden.
5.4	Indien Inschrijver de werkzaamheden uit een Exit-plan op basis van een uurtarief factureert, zal nooit meer dan het in het Exit-plan genoemde maximum aantal uren gefactureerd worden.
5.5	Inschrijver werkt jaarlijks het Exit-plan bij. Het laatst geaccordeerde (door beide partijen getekend) Exit-plan zal gebruikt worden.
5.6	Overeengekomen uurtarieven in het Exit-plan mogen niet meer geïndexeerd worden dan conform de in de GIBIT 2023 art. 11.8 genoemde prijsindexatie.
5.7	Een all-in prijs voor een Exit-plan mag niet meer geïndexeerd worden dan conform de in de GIBIT 2023 art. 11.8 genoemde prijsindexatie. Uitbreiding van een all-in prijs voor een Exit-plan vanwege een meer uitgebreide dienstverlening dient toegelicht te worden door Inschrijver.

6 Dienstniveau (SLA/DAP)

6.1 Inleiding

De dienstverlening t.a.v. zowel support, preventief en correctief onderhoud m.b.t. externe Firewalls maakt deel uit van de SLA.

Opdrachtgever verwacht binnen de support afspraken minimaal de volgende aandachtsgebieden:

- Hardware ondersteuning en support.
- Ondersteuning op verzoek bij het in stand houden van een gezonde externe Firewall omgeving t.a.v. fixes/updates en upgrades
- Ondersteuning bij incidenten en probleemanalyse met name voor derdelijns support
- Vervanging van defecte apparatuur
- Advieswerkzaamheden

Uitgangspunt vanuit de Opdrachtgever is dat de betreffende beheerders de 1e en 2e lijns vraagstukken en standaard fixes/updates met lage impact zelfstandig oplossen dan wel implementeren. Mocht onverhoopt ondersteuning binnen de context van 1e en 2e lijns vraagstukken en/of fixes en updates nodig zijn dan kan men conform SLA een beroep doen op ondersteuning op basis van vooraf afgenomen strippenkaart ondersteuning. Updates en fixes zijn bij de prijs inbegrepen. Het door Opdrachtnemer beschikbaar stellen van fixes en updates is kosteloos.

6.1.1 Dienstverlening

Servicedienst verstoringen is op basis van 7*24 uur.
Het standaard supportvenster loopt daarbij van maandag t/m vrijdag van 08:00-17:00.

Prioriteit	Responsetijd (max)	Oplostijd (max)	Norm	Support	Melding
P1 (calamiteit)	15 minuten	4 klokuren	95%	7*24 uur Incl feestdagen	Telefonisch
P2 (urgent)	60 minuten	8 werkuren	95%	7*24 uur Incl feestdagen	Telefonisch
P3 (middel)	240 minuten	16 werkuren	95%	Ma-Vr 08:00-17:00	Mail/Portal
P4 (laag)	240 minuten	40 werkuren	95%	Ma-Vr 08:00-17:00	Mail/Portal

Definitie responstijd: De tijd waarbinnen de Opdrachtnemer reageert op de melding.

Definitie oplostijd: De tijd die verstrijkt tussen het aanmelden van een verzoek of melding bij de Opdrachtnemer en het moment waarop Opdrachtnemer de verstoring heeft verholpen, dan wel een workaround heeft geïmplementeerd.

6.1.2 Beschikbaarheid Serviceafdeling

- 24/7 beschikbaar voor incidentenmanagement
- Gedurende reguliere tijden ma-vr | 08:00-17:00
  - Via email
  - Telefonisch
  - Via Digitaal service portaal
    - Storingen melden
    - Prioriteit/Urgentie koppelen

- Procesvoortgang volgen
- Inzicht geleverde prestaties

- Buiten reguliere kantoortijden minimaal telefonische bereikbaarheid
- In geval urgente melding met P1 classificatie: telefonische melding

Opdrachtgever bepaalt de urgentie van de melding.

Bij urgente verstoring waarbij het gehele of groot deel van het systeem buiten gebruik raakt en/of normale bedrijfsvoering blokkeert zal de storing met zeer hoge prioriteit (P1 Calamiteit) worden opgepakt. Werkzaamheden en communicatie t.a.v. verstoringen vinden plaats in en met overleg van de Opdrachtgever.

6.1.3 Impact en urgentie definitietabel

Urgentie	Urgentie	Impact		
		Hoog	Middel	Laag
	Hoog	P1	P2	P3
	Middel	P2	P3	P4
	Laag	P3	P4	P4

Bepalen impact	
Hoog	- Er is/dreigt ernstig productieverlies, die mogelijk kan resulteren in een hoge - Inkomensderving en/of hoge schadeclaim voor de gemeente en/of niet meer voldoen aan de wettelijke verplichtingen en/of; - De verstoring heeft gevolgen voor de bedrijf kritische processen en/of; - Meer dan 50% van de medewerkers van de klant kan niet werken en/of; - Dienstverlening naar burgers is verstoord; - Er is sprake van een serieuze security dreiging
Middel	- Er is/dreigt productieverlies wat mogelijk kan resulteren in een inkomstenderving en/of schadeclaims voor de gemeente en/of; - De verstoring raakt een groot deel van de medewerkers (10% of meer van alle eindgebruikers van de klant) of een of meerdere niet bedrijf kritische processen.
Laag	- Er is geen productieverlies, en/of; - De verstoring raakt één of enkele medewerkers, die niet werken met bedrijf kritische processen.

Bepalen Urgentie	
Hoog	- Dienstverlening moet direct hersteld worden, en/of; - Er is geen workaround of andere tijdelijke oplossing beschikbaar om verder te kunnen werken.
Middel	- De dienstverlening hoeft niet direct hersteld te worden, maar wel zo spoedig mogelijk, en/of; De werkzaamheden (bij gebruiker) zijn redelijk eenvoudig uit te stellen, terwijl er geen workaround of andere tijdelijke oplossing beschikbaar is om verder te kunnen werken.
Laag	- De oplossing kan langere tijd op zich laten wachten, en/of; - Er is een workaround of andere tijdelijke oplossing beschikbaar, zodat er verder gewerkt worden.

6.1.4 Correctief melding incident

Werkzaamheden bij het melden en oplossen van een correctief incident:

- Registratie van het incident
- Identificatie van benodigde reparaties/werkzaamheden
- Opstellen van rapportages
- Terugkoppeling aan betrokken partijen
- Analyse van het incident
- Implementatie van een oplossing
- Afsluiting van het incident

6.1.5 Strippenkaart

Op basis van het expertise niveau van de betrokken beheerders van de Opdrachtgever wenst de Opdrachtgever een strippenkaart constructie te hanteren voor specifieke ondersteuning op verzoek.

Basis expertise beheer Opdrachtgever	Activiteit op verzoek	Strippenkaart	SLA
Beheer & Support	1e en 2e lijns ondersteuning op verzoek	[X]	
	3e lijns ondersteuning		[X]
	Ondersteuning bij Calamiteit		[X]
	Support on site		[X]
Reguliere patches en updates	Ondersteuning bij implementatie op verzoek	[X]	
	Ondersteuning bij kritische cq majeure upgrades met hoge impact		[X]
Backup maken	Ondersteuning bij terugzetten backup	[X]	
Overig	Advies en consultancy		[X]

6.1.6 Algemeen

De documentatie van de omgeving wordt door de Opdrachtnemer goed bijgehouden. Dit omvat het bijhouden van informatie over de installaties, betreffende externe Firewalls in de omgeving van de Opdrachtgever.

Er zijn faciliteiten beschikbaar voor remote support middels Teamviewer, zodat er op afstand i onder begeleiding van medewerkers van de Opdrachtgever preventief en correctief onderhoud kan worden uitgevoerd. Dit maakt het mogelijk om problemen op te lossen zonder fysiek aanwezig te hoeven zijn.

Er wordt optimale aandacht besteed aan de betrokken installaties door jaarlijks preventief onderhoud. Jaarlijks wordt er een rapportage opgesteld waarin de algehele systeemstatus wordt beschreven. Daarnaast worden er aanbevelingen en verbetervoorstellen gedaan en vindt er een evaluatie plaats in samenspraak met de Opdrachtgever.

7 Ondersteunende eisen

Eis nr.	Beschrijving
7.1	Opdrachtnemer levert minimaal vijf jaar ondersteuning en onderhoud op de apparatuur vanaf het moment dat deze is opgeleverd aan en is geaccepteerd door Opdrachtgever (zowel voor de huidige installed base als nieuw te leveren apparatuur).
7.2	Opdrachtnemer is geautoriseerd voor het leveren van ondersteuning en onderhoud van de externe Firewall infrastructuur oplossing.
7.3	Het is Opdrachtnemer slechts toegestaan het onderhoud te stoppen of niet meer te kunnen garanderen op het moment dat de betreffende apparatuur door de eindfabrikant “end of service”/”end of support” wordt verklaard. Opdrachtnemer kan Opdrachtgever in dergelijk geval verzoeken om desbetreffende apparatuur te vervangen of vernieuwen. Zo lang patches en upgrades van de benodigde software beschikbaar zijn, worden die ter beschikking gesteld aan Opdrachtgever zonder extra kosten
7.4	Opdrachtnemer voorziet in één telefonisch loket waar 24 uur per dag alle dagen van het jaar tijdens werktijden (van 8:00 uur tot en met 17:00 uur Nederlandse tijd) vragen en calamiteiten en incidenten aangaande de externe Firewall infrastructuur worden gemeld en buiten de werktijden alleen calamiteiten en 3^{e} lijns incidenten worden gemeld.
7.5	De Opdrachtnemer stelt een Nederlandssprekende servicedesk binnen de grenzen van de EU ter beschikking aan Opdrachtgever, dit is geen robot.
7.6	Incidenten moeten in ieder geval telefonisch en daarnaast per e-mail en/of portal kunnen worden gemeld.
7.7	Gesprekspartner is een inhoudsdeskundige op het gebied van firewalls en/of beveiliging (afhankelijk van de vraagstelling) op minimaal het niveau van 2e lijn.
7.8	De servicedesk beantwoordt vragen binnen één werkdag tenzij anders overeengekomen.
7.9	Opdrachtgever bepaalt de prioriteit t.a.v. impact en urgentie call.
7.10	Opdrachtgever kan de afhandeling van alle incidenten en/of storingen volgen in een portal dat door de leverancier ter beschikking wordt gesteld.
7.11	Updates van meldingen en/of lopend incident worden door Opdrachtnemer tevens (na telefonisch contact) via mail verstuurd aan Opdrachtgever.
7.12	Portal is voorzien van 2FA (two factor authentication).

7.13	Remote toegang op de omgeving van de externe Firewalls zal middels Teamviewer van de Opdrachtgever worden aangeboden.
7.14	Opdrachtnemer voert tijdens ieder incident of storing een analyse uit om daarna een oplossing door te voeren voor het verhelpen van het incident. Opdrachtnemer voert periodiek (minimaal per kwartaal) analyses uit ter verbetering van de gehele beschikbaarheid van de dienst. Na een kritisch incident (P3/P4) kan Opdrachtgever vragen om een Root Cause Analysis (RCA) van dit incident. Opdrachtnemer stelt deze zonder extra kosten ter beschikking.
7.15	Opdrachtnemer signaleert trends in de aangemelde incidenten en vragen die kunnen wijzen op structurele problemen.
7.16	Het beschikbaar stellen van updates en patches zijn bij de prijs inbegrepen.
7.17	In geval van nieuwe reguliere software updates of patches met lage impact op de externe firewalls voert Opdrachtgever deze zelfstandig uit.
7.18	In geval van nieuwe software updates of patches met hoge impact op de externe Firewall omgeving zal de implementatie op basis van gezamenlijkheid worden uitgevoerd. De Updates en patches worden pas uitgevoerd na toestemming van de Opdrachtgever. Eventuele ondersteuning vanuit de Opdrachtnemer kan via een strippenkaart in rekening worden gebracht.
7.19	Opdrachtnemer is verantwoordelijk voor de snelheid van de dienstverlening. Het staat Opdrachtnemer vrij zelf vervanging en reservedelen te verzorgen, dan wel hier bij eindfabrikant een contract voor te sluiten. Deze eventuele maatregelen zijn bij de prijs van de Opdrachtnemer inbegrepen en leveren geen meerprijs op voor de Opdrachtgever.
7.20	Van iedere klacht en bijbehorende afhandeling over de uitvoering van de Opdracht dient de Opdrachtnemer de Opdrachtgever kopieën te zenden. Het beleid van Opdrachtgever is dat de Opdrachtnemer voor alle klachten en storingen het eerste aanspreekpunt is. Vanzelfsprekend dient Opdrachtnemer bij hem ingediende klachten correct af te handelen.