gemeente Zoetermeer

# NOTA VAN INLICHTINGEN

## Marktconsultatie Firewall

2026-089321

# Nota van Inlichtingen

In dit document zijn de vragen inclusief antwoorden weergegeven die betrekking hebben op de marktconsultatie ‘Firewall’ ten behoeve van Gemeente Zoetermeer.

**Vragen en Antwoorden**

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 1. | **Certificeringen:** | Om marktpartijen tijdig inzicht te geven in de voorgenomen geschiktheidseisen en eventuele verrassingen bij publicatie van de aanbesteding te voorkomen, vernemen wij graag of u al een beeld heeft van de certificeringen, normen en/of kwaliteitskeurmerken die als minimumeis zullen worden gesteld. Kunt u daarnaast aangeven of per eis een gelijkwaardig alternatief wordt geaccepteerd? | U moet denken aan certificering zoals ISO27001/ 27002, ISAE 3402, ISO27017, ISO27018, ISO9001 |
| 2. | **Referenties:** | Om marktpartijen tijdig inzicht te geven in de voorgenomen geschiktheidseisen, vernemen wij graag of u al een indicatie kunt geven van de minimale omvang van de gevraagde referentieopdracht(en), bijvoorbeeld ten aanzien van het aantal gebruikers, werkplekken en/of de contractwaarde. Kunt u daarnaast aangeven of vergelijkbare integrale managed ICT-opdrachten uit andere sectoren als geschikt worden beschouwd, of dat specifiek referenties binnen de (semi)publieke sector worden verlangd? | Zoetermeer heeft ongeveer 1900 medewerkers in dienst, die vrijwel allemaal met een laptop werken vanuit ons kantoor of vanuit huis.<br><br>De contractwaarde van de opdracht kunnen wij slecht bepalen en juist die informatie willen we via deze RFI beter kunnen inschatten<br><br>Andere referenties, mits qua vergelijkbare schaal mogen, (Semi)overheid of zorg heeft wel de voorkeur. |
| 3. | **MDR/XDR-platform:** | welk MDR/XDR-product is in gebruik en welke koppelvlakken (native connector, API, syslog/CEF) worden ondersteund? | Microsoft Defender in combinatie met Microsoft Sentinel |
| 4. | **Hypervisor:** | welk virtualisatieplatform en welke versie(s) draaien er? Service chaining en NGFW-integratie (V3) zijn platformspecifiek (VMware vSphere, Hyper-V, Nutanix). | **Virtualisatieplatform:** Nutanix HCI met Nutanix Flow voor service chaining en microsegmentatie. |
| 5. | **Kubernetes:** | welke distributie (vanilla, AKS, OpenShift, Rancher), on-prem of in Azure, en wat is de reële productieschaal? Voor de prijsindicatie wordt uitgegaan van een fictief volume van 2 | Kubernetes draait nog niet, plan is om later in het jaar een poc op te zetten, dit zal onpremis gaan draaien. Nutanix NKP wordt ingezet |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | clusters / 40 nodes; graag de werkelijke richting zodat de aanpak en prijs kloppen. | |
| 6. | **Bestaande IP-VPN:** | wie beheert de huidige IP-VPN en zijn er technische of contractuele afhankelijkheden die het ontwerp of de plek van internet-breakout beperken? De IP-VPN-kosten hoeven niet geoffreerd te worden, maar het ontwerp hangt er wel van af. | Het beheer en de levering van de huidige IP-VPN-dienst zijn ondergebracht bij een landelijke service provider. De IP-VPN-dienst maakt geen onderdeel uit van de uit te vragen dienstverlening. inschrijvers worden uitgenodigd om een passende oplossing voor te stellen binnen de kaders van de uitvraag. We zien geen technische of contractuele afhankelijkheden die internet-breakout kunnen beperken |
| 7. | **Huidige firewall en migratie** | Welke firewalloplossing is nu in gebruik, en staat de gemeente open voor een vendor-wissel of heeft continuïteit/migratie vanaf de zittende leverancier de voorkeur? | Momenteel wordt gebruikgemaakt van een Next Generation Firewall-oplossing met fysieke en virtuele firewalls. De gemeente is echter gebonden aan de aanbestedingsprocedure en de aanbestedingswetgeving. De uitvraag wordt daarom functioneel en merkonafhankelijk opgesteld. Inschrijvers zijn vrij om een passende oplossing aan te bieden, mits deze voldoet aan de gestelde eisen en wensen. |
| 8. | **Cloud-native/ SSE-model:** | Vandaag routeert al het internet- en SaaS-verkeer van de locaties eerst via de centrale beveiligingsstraat op de hoofdlocatie. De gemeente nodigt nadrukkelijk uit tot alternatieve of cloud-native/agent-based varianten waarbij on-premises hardware vervalt of wordt geminimaliseerd. Hoeveel ruimte is er werkelijk om naar een cloud-geleverd SSE-model (lokale internet-breakout per locatie) te bewegen versus centrale on-prem inspectie behouden? | De huidige nevenlocaties zijn reeds aangesloten op de centrale beveiligingsvoorzieningen en vallen daarmee binnen de bestaande beveiligings- en inspectiearchitectuur. De primaire aanleiding voor deze uitvraag is het verkrijgen van meer zicht en controle op verkeer van gebruikers buiten de gemeentelijke locaties, zoals thuiswerkers. De gemeente staat open voor alternatieve architecturen, waaronder SSE-gebaseerde oplossingen, maar schrijft geen lokale internet-breakout per locatie voor. Inschrijvers worden uitgenodigd een architectuur voor te stellen die aantoonbaar invulling geeft aan de gestelde beveiligings- en beheerdoelstellingen. |
| 9. | **Co-management-verdeling:** | wat is de omvang, het volwassenheidsniveau en de gewenste taakverdeling van het interne IT-team? Welke taken wil de gemeente zelf houden versus beleggen? | Het team dat zich met de Back-end infrastructuur en FW bezighoudt is ongeveer 5 man groot.<br><br>Minimaal zouden wij ook zelf de volgende beheertaken kunnen uitvoeren: wijzigingen aan policies, objecten Routing, VPN en Virtuele IP interfaces. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 10. | **Beheermodel en verantwoordelijkheden** | Hoe zijn de verantwoordelijkheden voor dagelijks beheer, beleidswijzigingen, incidentafhandeling, updates en lifecyclemanagement momenteel verdeeld tussen de interne IT-organisatie en externe dienstverleners? Welke verdeling van verantwoordelijkheden ziet de gemeente voor de toekomstige dienstverlening? | Zie antwoord 9 en we zijn juist graag wat de visie van de markt op dit onderwerp is. Welke ervaring hebben jullie met co-management en hoe waarborgen we gezamenlijk dat structureel geborgd beheer beheersbaar en overzichtelijk blijft. |
| 11. | **Gebruikersgroepen en apparaten** | Welke gebruikersgroepen en typen apparaten vallen binnen de beoogde scope? Graag naast de circa 1.900 medewerkers ook inzicht geven in raadsleden, inhuurkrachten, ketenpartners, externe partijen en niet-gemeentelijk beheerde apparaten. | De beoogde scope is ruwweg wel wat jullie hier zelf als voorbeeldgroepen geven. Verwerk eventueel opschaling van die groepen in het effect op de pricing. Geef goed aan waar u aannames doet en hoe die van invloed zijn op de prijs en of beheerlast |
| 12. | **Digitale werkplek** | Hoe is de huidige digitale werkplek ingericht op het gebied van besturingssystemen, endpointmanagement, device compliance en endpointsecurity? | We maken gebruik van Windows 11, Intune, Defender for Endpoints |
| 13. | **Identity-omgeving** | Welke identity- en accessmanagementoplossingen gebruikt de gemeente momenteel? Welke rol spelen Microsoft Entra ID, Conditional Access, multifactorauthenticatie en privileged access binnen de huidige inrichting? | Entra-ID, Conditional Access, MFA en PIM zijn allemaal ingericht. |
| 14. | **Microsoft Security en Data Protection** | Welke onderdelen van het Microsoft security- en compliance-ecosysteem zijn momenteel in gebruik, in onderzoek of gepland? Denk hierbij aan Microsoft Defender, Sentinel, Purview, sensitivity labels en DLP-functionaliteit. | Zie voorgaande antwoorden. Daarnaast is ook Purview ingericht.<br><br>Sensitivity labels en DLP worden op dit moment minimaal toegepast. |
| 15. | **Bestaand security-ecosysteem** | Kunt u een overzicht geven van de huidige oplossingen op het gebied van netwerksecurity, endpointsecurity, identity, cloudsecurity, databeveiliging en vulnerabilitymanagement, inclusief de belangrijkste onderlinge koppelingen? | Entra-ID, Conditional Access, MFA en PIM zijn allemaal ingericht. We maken gebruik goed gebruik van onze E5 licenties en zetten Defender, Sentinel en Intune in als kern van onze security. Daarnaast hebben we ook Purview ingericht. |
| 16. | **Ticketing en operationele processen** | Van welk ticketing- of ITSM-platform maakt de gemeente gebruik? Hoe worden securityalerts, incidenten, wijzigingen, escalaties en goedkeuringsprocessen momenteel binnen dit systeem afgehandeld? | Topdesk. Ook het RFC proces verloopt via Topdesk |
| 17. | **MDR, XDR, SIEM en SOC** | Welke MDR-, XDR-, SIEM- en SOC-oplossingen of dienstverleners worden momenteel gebruikt? Hoe zijn monitoring, triage, incidentopvolging en de uitwisseling van telemetrie en alerts ingericht? | Microsoft Defender en Intune in combinatie met Microsoft Sentinel leggen de basis voor onze inrichting. Incidentafhandeling gebeurd op basis van Topdesk. |
| 18. | **Netwerkarchitectuur en** | Kunt u de huidige netwerkarchitectuur nader toelichten, inclusief internetbreakout, routing, DNS, proxygebruik, IP-VPN, | Ter toevoeging op marktconsultatie firewall punt 2.2 gebruikt de gemeente geen proxy server, verkeerstromen naar private saas |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | **verkeersstromen** | nevenlocaties, thuiswerkers en de belangrijkste verkeersstromen naar internet, SaaS en private applicaties? | loopt over een VPN tunnel met betreffende leveranciers over Internet en GGI koppelmedium. Een interne split-DNS server wordt gebruikt voor interne bevraging. |
| 19. | **VDI en applicatieomgeving** | Hoe is de centrale VDI-omgeving ingericht en welke internet-, SaaS- en private-applicatiestromen lopen vanuit deze omgeving? Welke gebruikersgroepen en legacyapplicaties maken hiervan gebruik? | De on-prem VDI oplossing wordt met Omnissa onderhouden. Het wordt gezien als reguliere werkplek. |
| 20. | **Multi-user VDI** | Wordt binnen de gemeente gebruikgemaakt van een multi-user VDI-omgeving waarbij meerdere gebruikerssessies vanaf gedeelde servers of hosts worden aangeboden? Zo ja, om welke platformen, gebruikersgroepen en aantallen gelijktijdige gebruikers gaat het? | Nee. |
| 21. | **Kubernetes-omgeving** | Welke Kubernetes-distributie, cloud- of on-premisesomgeving, CNI-technologie, ingress- en egresscomponenten en eventuele service-meshoplossingen worden momenteel gebruikt? | Op dit moment is er nog geen omgeving, later in het jaar wordt er een poc opgezet met Nutanix NKP. |
| 22. | **Dataverwerking en logging** | Welke eisen en interne beleidsuitgangspunten hanteert de gemeente voor de geografische verwerking van verkeer en voor de opslag, bewaartermijn, toegankelijkheid en export van logging en securitytelemetrie? | Verwerking en opslag dienen binnen de EER plaats te vinden. Momenteel wordt de FW logging niet geëxporteerd, in de toekomst zouden wij de telemetrie wel willen opnemen in de SOC-dienstverlening. Ruwe schatting: 18,5 GB per dag aan FW logging. Retentietermijn: minimaal 1 maand op FW. |
| 23. | **Samenhang tussen firewall en SSE** | Welke concrete functionele, technische, operationele of contractuele afhankelijkheden maken het noodzakelijk om de on-premises firewallvoorziening en de SSE-functionaliteit binnen één scope en implementatietraject te behandelen? Kunt u daarbij onderscheid maken tussen de doelstellingen voor datacenter- en netwerkbeveiliging enerzijds en de beveiliging van gebruikers-, internet-, SaaS- en private-applicatieverkeer anderzijds? | Qua implementatie kunnen de twee oplossingen Firewall en SSE oplossing gescheiden worden.<br>Firewall vervanging dient wel volledig uitgevoerd te worden. |
| 24. | | Is het voor de gemeente een eis dat SSE afkomstig is van dezelfde leverancier als de firewall, of is een architectuur waarbij de cloud security volledig hardware-onafhankelijk is eveneens wenselijk? | Nee. |
| 25. | | Aangezien SSE zich aanzienlijk sneller ontwikkelt dan firewallhardware, is het een eis dat beide componenten contractueel afhankelijk van elkaar moeten worden vernieuwd? Of mag dit ook onafhankelijk van elkaar / gescheiden? | De aanbesteding voor de firewall- en SSE-oplossing wordt gecombineerd uitgevoerd. Na afloop van de contractperiode zal de gemeente de gekozen oplossing en aanbestedingsstrategie evalueren en bepalen of een nieuwe aanbesteding noodzakelijk is. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 26. | **Alternatieve afbakening** | Staat de gemeente open voor een alternatief scenario waarin de on-premises firewallvoorziening wordt gecontinueerd of afzonderlijk wordt behandeld, wanneer deze nog voldoet aan de eisen voor beschikbaarheid, lifecycle en informatiebeveiliging, en de vervolguitvraag zich primair richt op de beschreven risico's rondom SSE en het beperkte zicht op internet-, SaaS- en datastromen buiten de gemeentelijke locaties? | Huidige firewall valt onder een eerder aanbestede dienst en kan niet worden gecontinueerd. |
| 27. | | **Beheer en "Single Pane of Glass"**<br>Ten aanzien van vraag 6: Kan de gemeente nader specificeren of onder een 'Single Pane of<br>Glass' wordt verstaan dat on-premises firewalls, cloud-security (SSE/SASE), én logging/analytics<br>vanuit één en dezelfde policy engine en user | De gemeente wil weten of een beoogde oplossing bestaat uit één gecentraliseerde configuratie en monitor inzage tooling. |
| 28. | | **Veiligheid bij Thuiswerken oplossen**<br>a. In hoeverre is het voor de gemeente een harde eis dat de ZTNA/SSE-oplossing voor thuiswerkers<br>niet alleen initieel toegang verleent, maar ook continue security-inspectie (waaronder threat<br>prevention en DLP) uitvoert op al het verkeer naar applicaties, ter preventie van malware, zero-days<br>en dataverlies?<br>b. Aangezien de remote user oplossing gebruik maakt van directe offloading, is het meoizaam om<br>een inschatting toemaken van het totale hoeveelheid verkeer. Kan de Gemeente Zoetermeer hier een<br>indicatie van geven?<br>c. Aangezien we hier te maken hebben met een gemeente zullen alle genoemde locaties in de regio<br>Zoetermeer liggen. Dit hoeft niet per sé te gelden voor de remote users. Kan de gemeente<br>Zoetermeer aangeven of de connecitiviteit van de gebruikers alleen binnen Nederland benodigd is, of<br>is er ook behoefte aan een bredere invulling van de mogelijke locaties. | A Ja<br>B Niet in beeld<br>C 95% van onze connectiviteit vindt plaats binnen Nederland. Omdat we de consequenties van uw vraag op dit punt in relatie tot een gezonde kosten/baten verhouding beter inzichtelijk willen hebben, zien wij graag een suggestie van uw kant wat een verstandige keuze is (en eventueel kort toegelicht wat een alternatief is voor uw voorkeursscenario). |
| 29. | | **Performance en SSL-Decryptie**<br>Is het voor de gemeente een vereiste dat de aangeboden firewall-infrastructuur (zowel on-premises | De perfomance penalty moet dermate minimaal zijn dat de user-experience nagenoeg hetzelfde blijft. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | als cloud) in de praktijk haar volledige gespecificeerde performance behoudt wanneer essentiële beveiligingsfuncties, zoals SSL-decryptie en geavanceerde threat prevention, volledig zijn ingeschakeld? | |
| 30. | | **Kubernetes en native integratie**<br>a. Ten aanzien van vraag 4 (Kubernetes-integratie): Zoekt de gemeente hierbij specifiek naar een oplossing die op netwerkniveau (Layer 7) native in het K8s-cluster (zoals daemonsets of CNI) integreert om verkeer te inspecteren, in plaats van uitsluitend via externe third-party proxyoplossingen of basic API-koppelingen?<br>b. Ten aanzien van vfaag 4 (Kubernetes-integratie): Wat gebruikt de Gemeente Zoetermeer nu voor de “service chaining” en/of voor de bescherming van "het Kubernetes-cluster”? | A. De gemeente gaat een PoC opzetten wat op Nutanix NKP draait, graag een voorstel uitwerken wat hier het beste op aansluit.<br>B. Er is nog geen cluster, dit wordt later dit jaar opgezet. |
| 31. | | **Ruimte voor Innovatie**<br>Als onderdeel van de alternatieve en innovatieve scenario's (vraag 10): Staat de gemeente open voor de inzet van een Enterprise Browser-architectuur om veilig werken op eventuele onbeheerde apparaten (BYOD) of door derden (contractors) te faciliteren, met als doel om afhankelijkheid van zware/complexe VDI-omgevingen te verminderen? | Ja. |
| 32. | | **Planning**<br>In de planning is aangegeven dat inschrijver (mogelijk) in de tweede week van augustus voor een gesprek wordt uitgenodigd. Verzoek is of gezien de vakantieplanningen en de juiste voorbereiding dit verplaatst kan worden naar de laatste week van augustus. | Akkoord. Partijen die geselecteerd worden voor een toelichtingsgesprek worden uitgenodigd vanaf 24 augustus. |
| 33. | **2.4 - Support, RMA & SLA** | Kan de gemeente Zoetermeer bevestigen welke Support SLA als uitgangspunt genomen kan worden voor tariefstelling. Dit om de prijsstelling van inschrijvers goed te kunnen vergelijken. Welke SLA voor remote support en welke SLA voor Onsite support voor vervangende hardware bij defecten? | Onsite support 24x7 inclusief RMA<br>P1 4uur oplostijd<br>P2 24 uur<br><br>Als remote support in de vraag zien wij dat als een verzoek tot |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | | wijziging<br>Remote support: 24x7<br>P1 2 uur oplostijd<br>P2 8 uur<br>P3 48 |
| 34. | **2.4 Co - Management Services** | Kan de gemeente Zoetermeer, ten aanzien van Co-Management, aangeven hoe de gewenste demarcatie in verantwoordelijkheden ligt voor de gemeente Zoetermeer? Dit om de juiste tariefstelling te kunnen bepalen en de inschrijvingen goed te kunnen vergelijken. Voert het team van de gemeente alleen standaard wijzigingen zoals rulebase changes door en liggen de overige beheeractiviteiten bij de partner, of voert het eigen team bijvoorbeel ook software updates en upgrades uit? | Het team dat zich met de Back-end infrastructuur en FW bezighoudt is ongeveer 5 man groot.<br><br>Minimaal zouden wij ook zelf de volgende beheertaken kunnen uitvoeren: wijzigingen aan policy, objecten Routing, VPN en Virtuele IP interfaces. |
| 35. | **2.4 Financiële uitvraag** | Kan de gemeente Zoetermeer aangeven of implementatie-, migratie-, onboarding- en projectmanagementkosten onderdeel dienen uit te maken van het gevraagde as-a-service/abonnementstarief, of dat deze als éénmalige projectkosten mogen worden opgenomen? | Deze kosten mogen als eenmalige projectkosten worden opgenomen, mits (zoals in uw vraag) wel wordt aangegeven welke onderdelen in dit bedrag zijn opgenomen (geen specificatie in kosten). |
| 36. | **2.3 Vraag 10** | Kan de gemeente Zoetermeer toelichten op basis van welke criteria de voorgestelde alternatieve architectuurvarianten zal beoordelen ten opzichte van de gevraagde referentiearchitectuur? Worden deze bijvoorbeeld beoordeeld op security, beheerbaarheid, functionaliteit, toekomstbestendigheid, kosten of een combinatie hiervan? | De gemeente heeft hierin nog geen definitieve keuze gemaakt en staat nadrukkelijk open voor adviezen en inzichten vanuit de markt. Alternatieve architectuurvarianten worden daarom graag meegenomen in de marktconsultatie. |
| 37. | **2.1 Doel van de marktconsultatie** | Welke functionele doelstellingen voor de toekomstige beveiligingsarchitectuur zijn voor de gemeente Zoetermeer het belangrijkst? | Inzicht, controle, schaalbaar en flexibel om in te kunnen spelen op trends/ontwikkelingen. |
| 38. | **2.1 Doel van de marktconsultatie** | Welke uitgangspunten hanteert de gemeente Zoetermeer ten aanzien van integratie met bestaande IT- en securityvoorzieningen? | Integratie met bestaande oplossingen daar waar mogelijk. Minimaal kunnen off-loaden van de telemetrische gegevens naar een alternatieve locatie. Integratie met Nutanix om de zero-trust principes en afhandeling dicht bij de bron te faciliteren is wel een vereiste. |
| 39. | **2.1 Doel van de marktconsultatie** | Zijn er functionele eisen ten aanzien van hergebruik van bestaande investeringen, beheerintegratie of interoperabiliteit? | Interoperabiliteit met Nutanix. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 40. | **2.1 Doel van de marktconsultatie** | Van welke virtualisatieplatform maakt de gemeente Zoetermeer gebruik? | Nutanix HCI met Nutanix Flow voor service chaining en microsegmentatie. |
| 41. | **2.1 Doel van de marktconsultatie** | Is het uitgangspunt het beveiligen van oost-west verkeer binnen de virtualisatieomgeving, of wordt specifiek een architectuur met virtuele Next-Gen Firewalls en service chaining beoogd? | De gemeente heeft als doel om verkeer oost west te filteren met de nodige IDS IPS oplossing, de wijze waarop dit gebeurt staat open. De gemeente sluit geen producten uit die voldoen aan de technische vereiste. |
| 42. | **2.3 Vragen** | Kan de gemeente Zoetermeer aanvullende uitgangspunten verstrekken ten aanzien van de omvang van de omgeving (zoals bandbreedte, verkeersvolumes (per locatie) en gelijktijdig gebruik)? | Zie antwoord op vraag 57,58,71 en 73. |
| 43. | **2.3 Vragen** | Welke eisen stelt de gemeente Zoetermeer aan logging, auditing en retentie van logdata binnen de toekomstige beveiligingsomgeving? | Zie antwoord op vraag 22. |
| 44. | **2.3 Vragen** | Welke eisen stelt de gemeente Zoetermeer aan de beschikbaarheid en continuïteit van de beveiligingsvoorziening (per locatie)? | Enkel de hoofdlocatie (Stadhuis) moet beschermd worden tegen SPOF. Voor overige locatie is een beperkte tijdelijk uitval acceptabel. Herstel van de oplossing kan op die verbindingen op basis van scherpe SLA afspraken rond vervanging van defecte apparatuur. |
| 45. | **2.3 Vragen** | Is het uitgangspunt dat alle gevraagde functionaliteiten afkomstig zijn van één leverancier/platform? | Nee. |
| 46. | **2.3 Vragen** | Welke mate van beheer zou de gemeente Zoetermeer zelf willen behouden binnen het co-managementmodel? | Het team dat zich met de Back-end infrastructuur en FW bezighoudt is ongeveer 5 man groot.<br><br>Minimaal zouden wij ook zelf de volgende beheertaken kunnen uitvoeren: wijzigingen aan policies, objecten Routing, VPN en Virtuele IP interfaces. |
| 47. | **2.3 Vragen** | Welke mate van inzicht en controle wenst de gemeente Zoetermeer over internet- en SaaS-verkeer van gebruikers, ongeacht hun werklocatie? | Ongeacht de locatie waarvandaan gewerkt wordt, de niveau van inzicht en controle moet gelijk zijn aan het niveau dat geldt op onze hoofdlocatie (het Stadhuis). |
| 48. | **Technische scope & architectuur** | **Hypervisor & virtualisatielaag —** Welke hypervisor(s) en versies zijn in gebruik in de twee datacenters van de hoofdlocatie (bijv. VMware vSphere/NSX-T, Microsoft Hyper-V, Nutanix AHV)? Is er een SDN-/overlaylaag (zoals NSX-T) aanwezig waarop service insertion / service chaining kan landen? Dit is bepalend voor de haalbaarheid en vorm van de gevraagde firewall-integratie in de virtualisatielaag. *(§2.1, vraag 3)* | De gemeente gebruikt AHV met Flow. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | | |
| 49. | | **Kubernetes-omgeving —** Welke Kubernetes-distributie of -platform wordt gebruikt (bijv. kubeadm/vanilla, Azure AKS, Red Hat OpenShift, Rancher, VMware Tanzu)? Draaien de clusters on-premises, in Azure of hybride, en welke CNI is in gebruik (bijv. Calico, Cilium, Flannel)? Betreft de beveiligingsscope uitsluitend noord-zuid en egress, of óók expliciet oost-west (pod-to-pod) microsegmentatie binnen de clusters? *(§2.3 vraag* | Plan is om later dit jaar een PoC op te zetten met Nutanix NKP. |
| 50. | | **Identity provider —** Is Microsoft Entra ID de centrale identity provider voor identiteitsgebaseerde toegang en ZTNA? Bestaat er nog een afhankelijkheid van on-premises Active Directory voor de legacy-applicaties en/of de centrale virtuele desktopomgeving? *(§2.3 vraag 1)* | De gemeente beoogd ondersteuning voor zowel Microsoft Identity als on premise legacy applicaties met active directory koppeling. |
| 51. | | **Virtuele desktopomgeving —** Welk VDI-platform wordt gebruikt voor de centrale virtuele desktopomgeving (bijv. Citrix, Omnissa Horizon, Azure Virtual Desktop)? Dit is relevant voor de wijze waarop ZTNA en SSO op deze omgeving worden toegepast. *(§2.2)* | Omnissa Horizon. |
| 52. | | **MDR/XDR-integratie —** Met welk MDR/XDR-platform dient integratie plaats te vinden (bijv. Microsoft Defender XDR/Sentinel, CrowdStrike, SentinelOne, Sophos, Arctic Wolf)? Wordt dit platform door de gemeente zelf beheerd of door een externe SOC/dienstverlener? Welke export-/integratiestandaarden hebben de voorkeur (bijv. Syslog/CEF, native API-push, OpenTelemetry)? *(§2.3 vraag 5)* | Wij maken gebruik van Microsoft Defender/Sentinel als MDR/XDR platform. Beheer valt op dit moment onder de gemeente. Er loopt een traject voor 24/7 SOC dienstverlening waarbij gebruikt wordt gemaakt van het reeds bestaande platform. Op dit moment wordt FW logging niet opgenomen in het MDR/XDR platform, dit zou een optie kunnen zijn in de toekomst. |
| 53. | | **Beheerportaal (Single Pane of Glass) —** Stelt de gemeente de eis van één centraal beheerportaal over álle componenten, of is een geconvergeerd model met enkele onderling gekoppelde | een geconvergeerd model met enkele onderling gekoppelde consoles is acceptabel. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | consoles acceptabel, mits de operationele samenhang (policy, telemetrie, rapportage) aantoonbaar geborgd is? *(§2.3 vraag 6)* | |
| 54. | **Netwerk, connectiviteit & internetuitbraak** | **Internetuitbraakmodel —** Het huidige model routeert al het internet- en SaaS-verkeer van de vaste locaties via de hoofdlocatie (centrale beveiligingsstraat). Wenst de gemeente dit centrale backhaul-model te handhaven, of staat zij open voor lokale/directe internetuitbraak per locatie (richting cloud-PoP) als onderdeel van de SSE-architectuur? Dit heeft grote impact op zowel de architectuur als de sizing. *(§2.2, §2.3)* | De gemeente heeft een voorkeur om het huidige model te handhaven. |
| 55. | | **Locatie on-prem firewalling —** Op welke locaties wordt geleaste on-prem firewall-hardware voorzien: uitsluitend in de twee datacenters van de hoofdlocatie, of óók decentraal op (een deel van) de dertien nevenlocaties en de dark-fiber-locatie? Dit bepaalt in sterke mate de omvang van de hardware-lease. *(§2.1, §2.4)* | Het huidige model voorziet twee firewalls in verschillende ruimtes op een adres, er speelt een mogelijke optie van een verhuizing om een deel van de hardware naar een 2e adres uit te voeren. Deze is redundant is ontsloten. |
| 56. | | **SSL/TLS-inspectie —** Is volledige uitgaande SSL/TLS-decryptie vereist en toegestaan (mede gelet op privacy- en OR-kaders)? De mate van decryptie bepaalt de effectiviteit van SWG/CASB en is bepalend voor de benodigde inspectiecapaciteit (zie ook sectie F). *(§2.1)* | SSL / TLS inspectie wordt uitgevoerd op een gefilterde set van categorieën. |
| 57. | | **Internet-bandbreedte hoofdlocatie —** Wat is de huidige en de verwachte internet-bandbreedte op de hoofdlocatie, inclusief het gebackhaulde verkeer van de dertien nevenlocaties? Zijn er piekprofielen (bijv. piekuren, gelijktijdige gebruikers) bekend? Dit vormt het uitgangspunt voor de doorzet-vragen in sectie F. *(§2.2)* | Verkeer inclusief de nevenlocaties naar buiten betreft een gecombineerde bandbreedte van 4,1 Gbps. Aanvullen met gegevens op 8 juli. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 58. | | **IP-VPN-koppeling —** Wie levert de bestaande IP-VPN (carrier/managed service), wat zijn de bandbreedtes per locatie en zijn er randvoorwaarden of beperkingen ten aanzien van routering en QoS die in het ontwerp gerespecteerd moeten worden? *(§2.3 vraag 2, §2.4)* | De IP-VPN wordt door een landelijke service provider geleverd de bandbreedtes betreffen:<br><br>2x 100/10<br>4x 200/40<br>3x 200/20<br>5x dit jaar te realiseren 200/40<br>2x 1000mbps (hoofdlocatie)<br>1x 100/100<br><br>Op dit moment zijn er geen randvoorwaarde of beperkingen t.a.v. routering of QoS |
| 59. | | **IP-VPN** – Wat is de einddatum van het IP-VPN contract? Dit in verband met de haalbaarheid van een eventuele alternatieve architectuur. | Het huidige IP-VPN-contract loopt ten minste tot september 2028. Naar verwachting zal voorafgaand aan deze einddatum een nieuwe aanbesteding voor een raamovereenkomst worden gestart.<br>Binnen de huidige overeenkomst bestaat bovendien de mogelijkheid om bestaande IP-VPN-aansluitingen om te zetten naar internetaansluitingen indien daar behoefte aan ontstaat. |
| 60. | | **IP-VPN** is de IP-VPN redundant ontsloten op de centrale locatie? Zo ja op welke wijze? | Ja deze is redundant ontsloten op verschillende hardware met UTP en Fiber. |
| 61. | | **Dark-fiber-locatie —** Wat is de functie van de via dark fiber gekoppelde locatie (bijv. derde datacenter, uitwijklocatie, kritische site), en welke beveiligingsfunctionaliteit is daar gewenst? *(§2.2)* | Datacenter en uitwijklocatie. |
| 62. | | **Internet Is de centrale Internet ontsluiting redundant, via meerdere providers ontsloten?** | Redundant via zelfde provider. |
| 63. | **Co-management & dienstverlening** | **Verdeling co-management (RACI) —** Welke beheertaken wenst het interne IT-team zelf te behouden (bijv. policy changes, eerstelijns incidentafhandeling) en welke wenst de gemeente bij de partner te beleggen? Is er een gewenste RACI-verdeling, of | Zie antwoord 9. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | een uitgangspunt qua volwassenheidsniveau van het interne team? *(§2.3 vragen 7–9)* | |
| 64. | | **SLA & servicevenster —** Welke SLA-niveaus en service-/onderhoudsvensters worden verwacht (bijv. reactie- en hersteltijden per prioriteit, 24×7 versus kantoortijden, beschikbaarheidsnormen)? Is Nederlandstalige support een vereiste? *(§2.1, §2.4)* | Zie antwoord 33. |
| 65. | **Compliance & soevereiniteit** | Compliancekaders — Welke kaders zijn van toepassing en dienen aantoonbaar te worden ondersteund (bijv. BIO, ENSIA, NIS2, ISO 27001, NEN 7510, SOC 2)? Worden hierbij specifieke certificeringen van de oplossing en/of de dienstverlener verlangd? *(§1.2)* | Zie antwoord op vraag 1. |
| 66. | | Datasoevereiniteit & -residentie — Stelt de gemeente eisen aan de geografische locatie waar verkeersinspectie, policy-enforcement, logging én het beheer-/control-plane plaatsvinden (EU/Nederland)? Vloeien er eisen voort uit overheids- of datasoevereiniteitsbeleid die wij in de architectuur moeten verwerken (bijv. een on-premises beheervlak)? *(§1.2, §2.1)* | Zie antwoord op vraag 22. |
| 67. | **Commercieel & transitie** | Gebruikersaantal — Betreffen de 1900 gebruikers named users of concurrent users? Zijn hierin externen/inhuur en serviceaccounts begrepen, en hoeveel devices/endpoints dienen te worden voorzien van een (ZTNA-)agent? *(§2.1, §2.4)* | 1900 named users. |
| 68. | | **Lease- & financieringsconstructie —** Is een echte operationele lease (off-balance, as-a-service) een harde eis? Mag de leverancier zelf als lessor optreden, of dient een | Nee, lease is geen harde eis. De leverancier mag zelf de lessor zijn. Voor een eigendoms- of buy-out scenario zien wij graag de visie van de markt onderbouwd terug in uw beantwoording. Wij leren graag. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | financieringspartij betrokken te zijn? Wat is het gewenste eigendoms-/buy-out-scenario aan het einde van de looptijd (na 4 jaar, respectievelijk na 4+2)? *(§2.1, §2.4)* | |
| 69. | | **Migratie & transitie —** Het huidige contract loopt uiterlijk 1 oktober 2027 af. Wat is het gewenste implementatie- en transitievenster, en zijn er randvoorwaarden ten aanzien van co-existentie met de huidige firewall-omgeving tijdens de migratie? Kan de huidige firewall-leverancier/-techniek bekend worden gemaakt in verband met de transitie-aanpak? *(§1.2)* | Wij zijn hier vooral nieuwsgierig naar uw ervaring en wijze van aanpak. We zien hier graag terug wat uw gangbare doorlooptijd en aanpak is. Wie nu leverancier is, is voor dit stadium (RFi) niet relevant. |
| 70. | | **Alternatieve scenario's —** Mogen alternatieve architectuurvarianten die bepaalde on-prem hardwarecomponenten minimaliseren of laten vervallen, afwijken van de in §2.1 genoemde on-prem-uitgangspunten (zoals service chaining in de hypervisor), mits aan dezelfde security- en businessdoelstellingen wordt voldaan? Voor het alternatief wordt een aparte, parallelle kostentabel gevraagd: verwacht de gemeente dit alternatief in dezelfde reactie of als separaat document? *(§2.3 vraag 10, §2.4)* | Het zelfde document, en naar wens uitgewerkt in 2 scenario's. |
| 71. | **Sizing & capaciteit t.b.v. de financiële uitvraag (§2.4)** | De financiële uitvraag in §2.4 vraagt om een as-a-service tarief, maar het document bevat geen capaciteits- of performancegegevens voor de on-premises firewall- en virtualisatiecomponenten. Deze gegevens zijn bepalend voor het correct dimensioneren van de geleaste appliances en daarmee voor een realistische, marktconforme invulling van de kostentabel. Zonder deze informatie kunnen wij uitsluitend op basis van ruime aannames offreren, wat doorgaans leidt tot hogere marges of voorbehouden. Wij verzoeken de gemeente daarom onderstaande gegevens te delen; indicatieve waarden of bandbreedtes volstaan. | Voor de gemeente locaties wordt er nu afgedaan met een througput van IDS / IPS controle van 7,5 Gbps.<br>Alle aangegeven diensten worden gebruikt.<br><br>De gemeente gebruikt momenteel en wil blijven gebruiken:<br>- Sandboxing<br>- Detectie en blokkering van malware- en botnetcommunicatie (Command & Control verkeer)<br>- Antivirus<br>- Applicatieherkenning en applicatiecontrole<br>- Gebruikers- en groepsgebaseerd beleid<br>- Content Inspectie / Threat Prevention |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | Per cluster van vragen is aangegeven op welke regel van de kostentabel deze betrekking heeft.<br><br>**Gevraagde doorzet (Threat Prevention) —** Welke firewall performance en belangrijker welke Threat Prevention performance (met IPS, Anti-Virus, Anti-Bot en sandboxing gelijktijdig actief) wordt per datacenter verwacht? *(§2.4)* | - DNS Threat Protection<br>- URL Filtering / Web Filtering<br>- SSL decryptie uitgaand<br>- SSL decryptie inkomend<br>- File Type Control |
| 72. | | **Doorzet mét TLS-decryptie —** Welke perfroamnce is vereist met HTTPS-/TLS-inspectie actief? *(§2.4, vgl. §2.1)* | 3Gbps. |
| 73. | | De piekwaarden voor het aantal gelijktijdige sessies (concurrent sessions) en nieuwe sessies per seconde zijn momenteel niet volledig inzichtelijk. De gemeente stelt daarom voor de oplossing te dimensioneren op basis van de huidige firewallcapaciteit van circa 1,4 miljoen gelijktijdige sessies en 145.000 nieuwe sessies per seconde. | De piekwaarden voor het aantal gelijktijdige sessies (concurrent sessions) en nieuwe sessies per seconde zijn momenteel niet volledig inzichtelijk. De gemeente stelt daarom voor de oplossing te dimensioneren op basis van de huidige firewallcapaciteit van circa 1,4 miljoen gelijktijdige sessies en 145.000 nieuwe sessies per seconde. |
| 74. | | **Interfaces & poortdichtheid —** Welke poortdichtheid en interface-snelheden zijn vereist per datacenter (1/10/25/40/100 GbE, koper of glas), inclusief de interface voor de dark-fiber-verbinding? *(§2.4)* | De gemeente beschikt over een redundante firewallinfrastructuur met een netwerkcapaciteit van 2 × 10 Gbps. Alle virtuele interfaces maken gebruik van deze onderliggende connectiviteit. Tevens worden de dark-fiberverbinding via de switching netwerkinfrastructuur ontsloten. |
| 75. | | **HA-model —** Heeft de gemeente een voorkeur voor active/standby, active/active of een schaalbare (hyperscale-)orchestratie over de twee datacenters? *(§2.2, §2.4)* | Active/passive. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 76. | | **Site-to-site VPN —** Welke IPsec-VPN performance en hoeveel gelijktijdige site-to-site tunnels moeten worden ondersteund? *(§2.4)* | De gemeente heeft momenteel 20 VPN tunnels gelijktijdig in gebruik. |
| 77. | | **Groei & looptijd —** Met welke groei moeten wij rekenen over de contractduur? *(§2.4)* | 10-15% (op basis van de verwachte personele groei). |
| 78. | | **Hosts & clusters —** Hoeveel hypervisor-hosts (bijv. ESXi) en clusters zijn er, en hoeveel vCPU/RAM is per host beschikbaar voor security-service-VM's? (De licentie-eenheid van de virtualisatie-integratie is doorgaans per host of per vCPU.) *(§2.4)* | 8 Hypervisors, met genoeg resources. |
| 79. | | **Oost-west volume & workloads —** Welk volume aan oost-west-verkeer moet in de virtualisatielaag worden geïnspecteerd, en hoeveel VM's/workloads moeten worden beschermd? *(§2.1, §2.4)* | De gemeente bouwt zijn Oost-West verkeer inspectie nog steeds uit uiteindelijk komen we op een +/- van 180 VM's. |
| 80. | ***Regel "Kubernetes Security"*** | **Volume-detail —** Naast het opgegeven fictieve volume (2 clusters / 40 nodes): wat is het verwachte aantal pods en het aantal vCPU per node? *(§2.4)* | Later dit jaar wordt er een PoC opgezet, voor nu nog niks over te zeggen. |
| 81. | | **Functionele scope —** Welke functionaliteit is in scope: uitsluitend posture (CSPM/KSPM), of ook runtime-protectie (CWPP), image scanning, admission control en API-/ingress-security (WAF)? En vallen er IaaS/PaaS-omgevingen buiten Kubernetes ook onder deze regel? *(§2.1, §2.4)* | Graag in deze marktverkenning een voorstel uitwerken wat voor ons het beste is. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | | |
| 82. | ***Regel "Gebruikslicenties" — SSE voor 1900 gebruikers*** | **Tiering & devices —** Hebben alle 1900 gebruikers de volledige SSE-suite (SWG + CASB + ZTNA) nodig, of zijn er gebruikersprofielen/tiers met verschillende behoeften? En hoeveel devices/endpoints per gebruiker krijgen een agent? (Zie ook vraag 17 voor named/concurrent.) *(§2.4)* | Alle 1900 gebruikers hebben de volledige SSE-suite nodig. Elke gebruiker heeft een laptop en telefoon waar een agent op dient te komen. |
| 83. | ***Regels "Co-Management Services" en "Support, RMA & SLA"*** | **Change- & incidentvolume —** Welke indicatie kan de gemeente geven van het aantal policy changes per maand en het verwachte incidentvolume? *(§2.4)* | Momenteel wordt er zonder CO managment gemiddels 50 changes per maand aangedragen.Incidenten zien wij een gemiddelde van 10 – 15 incidenten per maand. |
| 84. | | **Logging & retentie —** Welk log-volume (events/sec of GB/dag) en welke log-retentietermijn worden verwacht? | Zie antwoord op vraag 22. |
| 85. | | Scope gebruikers<br>Het document hanteert "1900 gebruikers" als grondslag voor de prijsindicatie. Kan de gemeente verduidelijken of dit aantal uitsluitend vaste medewerkers betreft, of dat ook tijdelijke krachten, contractors, raadsleden en/of gastgebruikers in dit aantal zijn inbegrepen? Daarnaast: is dit het actuele aantal of een planningsgetal voor de contractduur? | 1900 named users. |
| 86. | | Locatie-inventarisatie<br>Het document vermeldt dertien nevenlocaties via IP-VPN en één locatie via dark fiber, maar verstrekt geen gegevens over bandbreedte per locatie, gebruikersaantallen per site of de kritikaliteit van de locaties. Is de gemeente bereid een (geanonimiseerde) locatie-inventarisatie te verstrekken zodat | Zie antwoord vraag 58 voor IP-VPN locaties.<br>De dark fiber koppeling heeft een bandbreedte van 10gb. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | inschrijver de on-premises hardware correct kunnen dimensioneren? | |
| 87. | | Definitie "blinde vlek" thuiswerkers<br><br>De huidige situatie beschrijft een blinde vlek bij thuiswerkers door split-tunneling: cloud- en SaaS-verkeer omzeilt de centrale firewall. Valt het dichten van deze blinde vlek expliciet binnen de scope van deze uitvraag? En zo ja: verwacht de gemeente dit via een agent-based endpoint-component, of via een andere methode zoals een cloud-gebaseerde SSE | Ja het dichten van de blinde vlek valt expliciet in binnen de opdracht. Hoe dit inzicht kan worden verschaft horen we graag van jullie. |
| 88. | | Business driver marktconsultatie<br><br>De huidige situatie beschrijft een beperkt zicht op SaaS- en internetverkeer van externe gebruikers als gevolg van split tunneling. Wordt het oplossen van deze zichtbaarheid- en controleproblematiek beschouwd als de primaire business driver van deze marktconsultatie, of zijn er andere doelstellingen die voor de gemeente minstens zo zwaar wegen? | Verhogen van de algehele security is de belangrijkste business-driver naast dat de wij inkoop-technisch verplicht zijn een vervanging/acquisitie traject te gaan starten. |
| 89. | | MDR/XDR platform<br>De gemeente vraagt integratie met "de bestaande MDR/XDR-oplossing", maar noemt geen specifiek platform. Kan de gemeente het gebruikte MDR/XDR-platform benoemen, of minimaal aangeven welke integratiestandaarden worden ondersteund (bijv. CEF, Syslog, OpenTelemetry, STIX/TAXII, native API)? Dit is noodzakelijk om een realistische integratiearchitectuur te kunnen beschrijven. | Zie antwoord op vraag 52. |
| 90. | | Kubernetes: aard van de clusters<br>Voor de prijsindicatie wordt uitgegaan van 2 clusters en 40 nodes. Zijn dit productieclusters met gevoelige (gemeente)data, of betreft het ontwikkel- en testomgevingen? Het beveiligingsniveau en de bijbehorende solution design verschillen hier wezenlijk in. | Later dit jaar wordt een PoC opgezet. Als eerste wordt het een test cluster. Later bestaat de kans dat dit productie wordt. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 91. | | Verdeling co-management<br>De gemeente vraagt een co-management model, maar geeft geen indicatie van de gewenste taakverdeling. Kan de gemeente een richtinggevende indicatie geven van de beoogde verdeling. Bijvoorbeeld de verhouding tussen inschrijver beheer en intern IT-beheer, zodat inschrijver het juiste serviceniveau en het bijbehorende aantal ingebakken FTE-equivalenten kunnen bepalen? | Het team dat zich met de Back-end infrastructuur en FW bezighoudt is ongeveer 5 man groot.<br><br>Minimaal zouden wij ook zelf de volgende beheertaken kunnen uitvoeren: wijzigingen aan policies, objecten Routing, VPN en Virtuele IP interfaces. |
| 92. | | Goedkeuringsbevoegdheid bij policy changes<br>Bij wijzigingsbeheer (policy changes) is het essentieel dat helder is wie de definitieve goedkeuringsbevoegdheid heeft bij een firewall policy wijziging, met name wanneer er verschil van inzicht bestaat tussen de gemeente en inschrijver over de impact of de uitvoering. Kan de gemeente haar verwachting hieromtrent toelichten? | De gemeente heeft een voorkeur voor co-management maar is in deze markconsultatie benieuwd naar de mening in de markt waar er wordt samengewerkt op het security platform. |
| 93. | | SLA-parameters<br>Het document benoemt "Support, RMA & SLA" als kostenelement in de TCO-tabel, maar vermeldt geen concrete SLA-parameters. Kan de gemeente minimaal de volgende parameters specificeren:<br>Gewenste beschikbaarheid (uptime) van de firewalloplossing<br>Maximale hersteltijd bij een volledige uitval (RTO)<br>Gewenste responstijd bij incidenten (P1/P2/P3)<br>Hardware RMA: next business day of 4-uurs vervanging? | Zie opmerking bij vraag 33. |
| 94. | | Risico bij voortijdige contractbeëindiging (operationele lease)<br>Het document vraagt een operationele leaseconstructie voor hardware, waarbij artikel 3 de gemeente het recht voorbehoudt de marktconsultatie (en impliciet ook een toekomstig contract) te staken. Bij een operationele lease is de inschrijver gedurende de contractduur eigenaar van de apparatuur. Hoe gaat de gemeente om met het restwaarde-risico van de hardware bij voortijdige beëindiging van het contract? Wordt hier in de aanbestedingsdocumenten een regeling voor opgenomen? | Deze vraag is naar ons inzien niet relevant voor deze RFI. Wellicht kunt u in de beantwoording een aanname doen t.a.v. deze vraag en laten zien hoe dit mogelijk van invloed is op het incalculeren van rest risico in de prijs of dat u dit afgewikkeld zou willen zien in een clausule/paragraaf in een exitplan. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| 95. | | Afbakening IP-VPN versus SD-WAN overlay<br>De gemeente stelt dat de kosten van de bestaande IP-VPN buiten scope vallen. Indien inschrijver (alternatieve scenario's) een oplossing voorstelt waarbij een SD-WAN overlay wordt geïntroduceerd bovenop of ter vervanging van de IP-VPN, hoe dient de inschrijver in dat geval de kostensplitsing in de TCO-tabel te hanteren? | Beschrijf en maak een inschatting van de kosten die het alternatief zou kosten. Dan zijn wij zelf in staat de afweging te maken of dit voor ons rendabel of kosten-technisch interessant is. |
| 96. | | Eén-op-één gesprekken<br>Zou het i.v.m. beschikbaarheid van collega's in de vakantieperiode ook mogelijk zijn om dit gesprek in de 3e week van augustus te plannen? | Ja dat is mogelijk. |
| 97. | | Vertrouwelijkheid aangeleverde informatie<br>Artikel 3 stelt dat deelnemende partijen geen aanspraak maken op auteursrecht van aangeleverde informatie en dat de gemeente hier vrijelijk over beschikt, ook extern. Inschrijver vraagt of de gemeente bereid is toe te staan dat inschrijver bij indiening een expliciete vertrouwelijkheidsmarkering kunnen aanbrengen op bedrijfsvertrouwelijke onderdelen (zoals **bedrijfseigen** architectuurdiagrammen of prijsmodellen), en hoe de gemeente hiermee omgaat in het openbare verslag. | De gemeente onderkent dat inschrijvingen bedrijfsvertrouwelijke informatie kunnen bevatten, zoals bedrijfseigen architectuurdiagrammen of prijsmodellen. Dit staat los van artikel 3: dat artikel regelt uitsluitend het gebruiksrecht van de gemeente ten aanzien van de aangeleverde informatie en blijft onverkort van toepassing.<br>Inschrijvers kunnen bij indiening onderdelen die zij als bedrijfsvertrouwelijk beschouwen expliciet markeren, met een korte onderbouwing waarom openbaarmaking hen onevenredig zou benadelen. De gemeente houdt hier bij het opstellen van het eigen gunningsverslag rekening mee en zal als bedrijfsvertrouwelijk gemarkeerde onderdelen niet specifiek benoemen of citeren in openbaar gemaakte stukken.<br>Voor verzoeken van derden om openbaarmaking (bijvoorbeeld op grond van de Wet open overheid) geldt dat de gemeente een eigen wettelijke afweging maakt aan de hand van de uitzonderingsgronden van art. 5.1 Woo, waaronder de bescherming van concurrentiegevoelige bedrijfs- en fabricagegegevens. Een vertrouwelijkheidsmarkering wordt daarbij als zwaarwegende aanwijzing betrokken, maar biedt geen absolute garantie tegen openbaarmaking; dit is een wettelijk kader waarover de gemeente geen afwijkingen kan overeenkomen. |
| 98. | | Firewall fabrikanten<br>Wordt bij de voorbereiding van de aanbesteding waarde gehecht aan de positionering van leveranciers in onafhankelijke | Ja, echter is de positie in de gartner magic quadrant nog niet definitief bepaald er wordt gedacht aan de "leaders" op het aangeboden product. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | marktanalyses zoals Gartner Magic Quadrant, of wordt primair beoordeeld op functionele fit, architectuur, dienstverlening en TCO?<br>We zien in veel aanbestedingen terugkomen dat er wordt gevraagd om 1 van de “leaders” in het Gartner Magic Quadrant van Hybrid Mesh Firewalls, vandaar deze vraag. | |
| 99. | | Strategische richting<br>Heeft de gemeente reeds een voorkeursarchitectuur voor ogen (SSE, SASE, Hybrid Mesh Firewall) of staat zij volledig open voor alternatieve architecturen die dezelfde doelstellingen realiseren? | De gemeente staat open voor alternatieve architectuur. |
| 100. | | Leveranciersstrategie<br>Gaat de voorkeur uit naar één geïntegreerde leverancier voor NGFW, SSE, beheerportaal en Kubernetes-security, of staat de gemeente open voor een best-of-breed oplossing bestaande uit meerdere fabrikanten? | Integratie van verschillende portalen maakt overzicht houden makkelijk, maar best of breed levert weer andere voordelen op. Juist deze RFi is bedoeld om die afweging mogelijk te kunnen maken. Vooralsnog hebben we geen voorkeur. |
| 101. | | huidige omgeving<br>Kan de gemeente inzicht geven in de huidige firewallfabrikant, het huidige licentiemodel en eventuele ervaringen of aandachtspunten die meegenomen moeten worden in een toekomstige oplossing? | We vergelijken de huidige omgeving niet met wat er komen gaat, te meer omdat onze informatiebehoefte voornamelijk op SSE zit (en natuurlijk een indicatie voor de integratie met de hardware FW). |
| 102. | | Cloudstrategie<br>Wat is de verwachte verhouding tussen toekomstige on-premises workloads en cloud workloads gedurende de contractperiode van 4+2 jaar? | Gemeente ziet een vergroting van Saas oplossingen bij nieuwe en vernieuwde producten. We weten dat er de aankomende 2 jaar 3 ‘grote’ applicaties gaan verhuizen van on premise naar SaaS. De precieze impact op dataverkeer is in dit stadium nog niet bekend. Het uitgangspunt voor de inschaling van capaciteit kunt u baseren op de huidige informatie. |
| 103. | | Kubernetes<br>Is het genoemde Kubernetes-platform reeds operationeel of betreft dit een toekomstige ontwikkeling? Welke distributie(s) worden gebruikt of voorzien? | Dit is een toekomstige ontwikkeling. Plan is om dit met Nutanix NKP op te zetten. |
| 104. | | Datalocatie en compliance<br>Zijn er eisen ten aanzien van Europese dataverwerking, datasoevereiniteit of specifieke certificeringen zoals BIO, NIS2, ISO27001 of ENSIA? | Certificering: zie antwoord op vraag 1.<br>EER dataverwerking: zie antwoord op vraag 22. |
| 105. | | Migratie | Nee de gemeente verwacht geen side by side migratie maar een in place. |

| # | Onderwerp | Vraag | Antwoord |
|---|---|---|---|
| | | Verwacht de gemeente een gefaseerde migratie waarbij bestaande firewallomgevingen tijdelijk naast de nieuwe oplossing blijven bestaan? | |
| 106. | | Beheer (Single Pane of Glass)<br>Heeft de gemeente een voorkeur voor één volledig geïntegreerd beheerportaal van één leverancier, of is federatief beheer met gekoppelde portalen eveneens acceptabel? | Geen voorkeur. |
| 107. | | IP-VPN<br>Om de afhankelijkheid van de hoofdlocatie te beperken zou het een suggestie kunnen zijn op de nevenlocaties te voorzien van een local internet breakout. Is een dergelijke oplossing voor de gemeente Zoetermeer acceptabel? | Dit zou acceptabel zijn zolang alle onpremise resources beschikbaar gemaakt kunnen worden met voldoende snelheid. Denk ook over telefoons, printers. |
| 108. | | Integratie Kubernetes en Hypervisor<br>Heeft de gemeente Zoetermeer als doel met deze integraties om informatie uit te wisselen tussen de platformen en de firewalls zodat er op een dynamische manier policies kunnen worden toegepast? | Voor nu is er nog geen kubernetes cluster, plan is om dit later dit jaar op te zetten op Nutanix NKP. Graag ontvangen wij een advies wat volgens jullie het meest flexibel is maar ook de beste bescherming geeft. |
| 109. | | MDR/XDR en firewall integratie<br>Is het voor de gemeente Zoetermeer acceptabel als een intelligente logcollector wordt gebruikt voor de firewall omgeving? Deze collector kan dan gefilterde en waardevolle informatie sturen naar de MDR/XDR omgeving. | Ja. |