**3.pielikums**

konkursa “Tīkla komutatoru, moduļu un piekļuves licenču iegāde A korpusam”,

identifikācijas Nr. SKUS 2016/252, nolikumam

**Tehniskā specifikācija/tehniskais piedāvājums**

1. **Datu tīkla agregācijas komutatoru, daudzfaktoru autentifikācijas, tīkla piekļuves autentifikācijas un autorizācijas programmatūras risinājuma un attālinātās piekļuves VPN risinājuma iegāde – vispārējās prasības:**

Pretendentam jānodrošina visu piedāvāto komponentu ieviešana Pasūtītāja tīklā, sākotnējā konfigurēšana atbilstoši Pasūtītāja vajadzībām, šo piegādāto risinājumu savstarpēja integrācija un integrācija ar Pasūtītāja rīcībā esošiem risinājumiem.

Ar Pasūtītāja rīcībā esošiem risinājumiem jāsaprot Microsoft Active Directory, Fortinet ugunsmūri, Hewlett-Packard un Extreme Networks datu tīkla komutatori, {php}IPAM (phpipam.net) IP adrešu pārvaldības risinājums.

Integrācijas ietvaros jānodrošina, ka tīkla piekļuves autentifikācijas un autorizācijas risinājums tiek integrēts ar Pasūtītāja IP adrešu pārvaldības risinājumu, Pasūtītāja tīklā esošajām dažādu ražotāju datu tīkla komutācijas iekārtām, tai skaitā Fortinet ugunsmūri, Microsoft Active Directory, Pretendenta piedāvāto daudzfaktoru autentifikācijas risinājumu, Pretendenta piedāvāto tīkla attālinātās piekļuves VPN risinājumu tā, lai tīkla piekļuves autentifikācijas un autorizācijas risinājums nodrošinātu piekļuvi Pasūtītāja datortīklam tikai Pasūtītāja atļautām iekārtām un lietotājiem. Savukārt Pretendenta piedāvāto daudzfaktoru autentifikācijas risinājumu nepieciešams integrēt ar Pasūtītāja Microsoft Active Directory un tīkla attālinātās piekļuves VPN risinājumu tā, lai to varētu izmantot attālinātās piekļuves autorizācijas procesā lietotāju autentifikācijai.

Tīkla attālinātās piekļuves VPN risinājumu jāintegrē ar Microsoft Active Directory, tīkla piekļuves autentifikācijas un autorizācijas risinājumu un Pretendenta piedāvāto daudzfaktoru autentifikācijas risinājumu.

Visai piedāvātajai aparatūrai un programmatūrai jānodrošina 5 (piecu) gadu ražotāja atbalsts.

Aparatūras atbalsta ietvaros jānodrošina bojāto iekārtu nomaiņa ne vēlāk kā nākošajā darba dienā.

Iekārtu un programmatūras ieviešanas, konfigurācijas un integrācijas darbus jāveic 30 (trīsdesmit) dienu laikā no visu iekārtu un programmatūras piegādes brīža vai brīža, kad Pasūtītājs nodrošinājis darba fronti, atkarībā no tā, kurš no šiem darbu uzsākšanas priekšnoteikumiem iestājas vēlāk.

**1.1. Datu tīkla agregācijas komutators *(2 gab.)***

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Prasības** | **Norāde - atsauce informatīvajos materiālos vai virtuālajā katalogā** |
| 1. | Jānodrošina virtuālā datu centra komutācijas iekārtas funkcionalitāte, kur 2(divas) un vairāk fiziskas komutācijas iekārtas kopumā strādā kā viena virtuāla L2/L3 ierīce; |  |
| 2. | Jānodrošina portu, kuri atrodas dažādās fiziskajās komutācijas iekārtās, agregācija (LACP); |  |
| 3. | Jānodrošina visai virtualizētai komutācijas iekārtai kopīga maršrutēšanas tabula, kopīgi VRF, kopīga Spanning Tree protokola apstrāde kā vienai iekārtai; |  |
| 4. | Jebkuras 1(vienas) fiziskās komutācijas iekārtas avārijas gadījumā pārējām komutācijas iekārtām ir jāpārņem visa virtualizētās komutācijas iekārtas funkcionalitāte un jāatjauno pakešu komutācija ne ilgāk kā 50ms laikā; |  |
| 5. | Iekšējās datu plūsmas ātrums virtualizētajā komutācijas iekārtā nedrīkst būt zemāks par 40 Gbps Full Duplex (kopā 80Gbps); |  |
| 6. | Virtualizētajai komutācijas iekārtai, nepārtraucot tās darbību, jānodrošina vairāku vienlaicīgu konfigurāciju saglabāšanu iekārtā un programmatūras atjaunošanu visai virtualizētajai komutācijas iekārtai. |  |
| 7. | Piedāvātā virtualizētā komutācijas iekārta jāpiegādā kopā ar nepieciešamo dokumentāciju digitālā formātā – instalācijas pamācībām, konfigurēšanas rokasgrāmatu, komandu rokasgrāmatu vai citu nepieciešamo dokumentāciju komutācijas iekārtas funkcionalitātes nodrošināšanai. |  |
| 8. | Protokolu un funkciju atbalsta prasības ir jāattiecina gan uz fizisko, gan arī uz virtualizēto komutācijas iekārtu. |  |
| 9. | Piedāvājumā ir jāiekļauj visi nepieciešamie adapteri, kabeļi un citas palīgierīces fizisko komutācijas iekārtu savstarpējai saslēgšanai vienotā virtualizētā komutācijas iekārtā, ņemot vērā, ka fiziskās iekārtas tiks izvietotas vienā 19” aparatūras skapī viena zem otras. |  |
| 10. | Piedāvājumā ir jāiekļauj 5 (pieci) SFP Gigabit Ethernet optiskie adapteri, kas ir paredzēti darbam ar daudzmodu optisko kabeli, izmantojot viļņa garumu 850nm, un nodrošina stabilu datu pārraidi attālumos vismaz līdz 300m, 62 (sešdesmit divi) SFP Gigabit Ethernet optiskie adapteri, kas ir paredzēti darbam ar vienmodu optisko kabeli, izmantojot viļņa garumu 1310nm, un nodrošina stabilu datu pārraidi attālumos vismaz līdz 10km, 12 (divpadsmit) SFP Gigabit Ethernet adapteri, kas paredzēti darbam ar vara vītā pāra kabeli, 1 (viens) SFP+ 10 Gigabit Ethernet optiskais adapteris, kas ir paredzēts darbam ar daudzmodu optisko kabeli, 4 (četri) SFP+ 10 Gigabit Ethernet optiskie adapteri, kas ir paredzēti darbam ar vienmodu optisko kabeli, izmantojot viļņa garumu 1310nm, un nodrošina stabilu datu pārraidi attālumos vismaz līdz 10km un 4 (četri) QSFP 40 Gigabit Ethernet optiskie adapteri, kas ir paredzēti darbam ar vienmodu optisko kabeli, izmantojot viļņa garumu 1310nm, un nodrošina stabilu datu pārraidi attālumos vismaz līdz 10km |  |
| 11. | Virtualizētajai komutācijas iekārtai jāsastāv no 2 (divām) un ir jābūt paplašināmai vismaz līdz 4 (četrām) fiziskām komutācijas iekārtām, kur katra no tām atbilst šādām prasībām: |  |
| 12. | Tai ir jānodrošina vismaz 2 (divi) karsti nomaināmi un rezervēti (1+1) barošanas bloki darbam ar 220V 50Hz maiņstrāvu. Barošanas blokiem ir jābūt identiskiem, lai tos varētu aizvietot ar rezerves vienību; |  |
| 13. | Pie maksimālās noslodzes tās elektroenerģijas patēriņš nedrīkst pārsniegt 550W stundā; |  |
| 14. | Tai ir jānodrošina savstarpēji rezervētu (1+1) un karsti nomaināmu dzesēšanas ventilatoru moduļu darbība, kas nodrošina gaisa plūsmu virzienā no iekārtas aizmugures un priekšpusi – Ethernet interfeisu pusi (Back to Front); |  |
| 15. | Montējama 19” aparatūras skapī un nepārsniedz 1U augstumu; |  |
| 16. | Vienai fiziskai iekārtai jānodrošina vismaz 48 (četrdesmit astoņi) 10 Gigabit Ethernet SFP+ interfeisi un vismaz 4 (četri) 40 Gigabit Ethernet QSFP+ interfeisi. QSFP+ interfeisus drīkst izmantot fizisko iekārtu saslēgšanai virtualizētā komutācijas iekārtā; |  |
| 17. | Jānodrošina sekojošas veiktspējas prasības L2 un L3 līmeņos: |  |
| 18. | Caurlaides spēja >=1200 Gb/s (wirespeed), >=900 Mp/s; |  |
| 19. | Maršrutēšanas tabulas izmērs – vismaz 16000 ieraksti |  |
| 20. | MAC adrešu tabulas izmērs – vismaz 120000 ieraksti. |  |
| 21. | Jānodrošina Jumbo frames atbalsts visos interfeisos; |  |
| 22. | Jānodrošina sekojošu IPv6 funkcionalitāti: |  |
| 23. | RFC 2460 – IPv6 Specification |  |
| 24. | RFC 2740 – OSPFv3 for IPv6 |  |
| 25. | RFC 3315 – DHCPv6 (client) |  |
| 26. | RFC 4862 – IPv6 Stateless Address Auto-configuration; |  |
| 27. | Jānodrošina sekojošu maršrutēšanas protokolu darbību: |  |
| 28. | RIP (RFC 1058 un RFC 2453), RIPv2 (RFC 1723) un RIPng (RFC 2080) |  |
| 29. | OSPF v2 (RFC 2328) |  |
| 30. | OSPFv3 for IPv6 (RFC 5340) |  |
| 31. | BGPv4 (RFC 1771) |  |
| 32. | VRRP (RFC 3768) |  |
| 33. | BGP/MPLS IP Virtual Private Networks (VPNs) (RFC 4364) |  |
| 34. | OSPF as the Provider/Customer Edge Protocol for RFC 4364 (RFC 4577) |  |
| 35. | Jāatbalsta sekojošus protokolus: |  |
| 36. | IEEE 802.1ag – Service Layer OAM |  |
| 37. | IEEE 802.1D – MAC Bridges |  |
| 38. | IEEE 802.1p – Priority |  |
| 39. | IEEE 802.1Q – VLANs |  |
| 40. | IEEE 802.1w – Rapid Reconfiguration of Spanning Tree |  |
| 41. | IEEE 802.1X – Port Based NAC |  |
| 42. | IEEE 802.3ad – Link Aggregation Control Protocol (LACP) |  |
| 43. | IEEE 802.3ae – 10-Gigabit Ethernet |  |
| 44. | IEEE 802.3x – Flow Control |  |
| 45. | RFC 768 – UDP |  |
| 46. | RFC 792 – ICMP |  |
| 47. | RFC 793 – TCP |  |
| 48. | RFC 826 – ARP |  |
| 49. | RFC 854 – TELNET |  |
| 50. | RFC 1350 – TFTP Protocol (revision 2) |  |
| 51. | RFC 2131 – DHCP |  |
| 52. | RFC 3046 – DHCP Relay Agent Information Option |  |
| 53. | IEEE 802.1AB – Link Layer Discovery Protocol (LLDP) |  |
| 54. | Jānodrošina sekojošu drošības risinājumu darbība: |  |
| 55. | IEEE 802.1X |  |
| 56. | Port mirroring |  |
| 57. | CFD (IEEE 802.1ag) |  |
| 58. | OAM (IEEE 802.3ah) |  |
| 59. | Jānodrošina RMON (RFC 2819), sFlow (RFC 3176) vai Netflow (RFC 3954) datu plūsmas analīzei; |  |
| 60. | Jānodrošina komutācijas iekārtas pārraudzība un vadība, izmantojot CLI (konsole un SSHv2), SNMPv3 un centralizētu vadības risinājumu. |  |

* 1. **Daudzfaktoru autentifikācijas risinājums *(1.gab)***

|  |  |  |
| --- | --- | --- |
| **Nr.p.k.** | **Minimālais nepieciešamais** | **Pretendenta piedāvājums:**nodrošina / nenodrošina |
| 1. | Risinājumam jānodrošina elastīga divu un vairāk faktoru autentifikācija |  |
| 2. | Pirmajam autentifikācijas faktoram jānodrošina autentifikācija ar piedāvāto tīkla autentifikācijas un autorizācijas programmatūras risinājumu, nodrošinot drošu autentifikāciju gan dažāda piekļuves līmeņa Pasūtītāja iekšējiem lietotājiem, gan ārējiem lietotājiem, piemēram, ārpakalpojuma sniedzējiem, nodrošinot diferencētas lietotāju tiesības atbilstoši veicamajai funkcijai |  |
| 3. | Otrajam autentifikācijas faktoram jānodrošina iespēja izmantot mobilo ierīču aplikāciju, kas pieejama Apple iOS un Android platformām |  |
| 4. | Jānodrošina iespēja izmantot arī citu otrā faktora autentifikāciju, kā arī papildus ieviest trešo faktoru, ja tāda nepieciešamība rodas |  |
| 5. | Otrā faktora autentifikācijas risinājumam jānodrošina vismaz 200 vienlaicīgi reģistrētu lietotāju ar iespēju šo risinājumu paplašināt vismaz līdz 5000 reģistrētiem lietotājiem, iegādājoties tikai atbilstoši licenci bez aparatūras/programmatūras nomaiņas |  |
| 6. | Otrā faktora autentifikācijas risinājumam jānodrošina vismaz 200 vienlaicīgu lietotāju autentifikāciju neierobežotam autentificējamo servisu skaitam, piemēram, visiem reģistrētajiem lietotājiem ir jāvar izmantot gan VPN servisu, gan autentifikācijas tīmekļa lapās, gan citus resursus, kuri tiks integrēti ar šo autentifikācijas risinājumu |  |
| 7. | Otrā faktora autentifikācijas mobilai aplikācijai jānodrošina atslēgas glabāšana mobilās ierīces īpaši aizsargātā atmiņā. Tai ir jānodrošina slepenās atslēgas ģenerēšanu, uzglabāšanu un lietošanu mobilo ierīču HSM (*Hardware Security Module*) bez tehniskas iespējas šo slepeno atslēgu eksportēt vai nokopēt ārpus HSM moduļa. Risinājumam jānodrošina šo atslēgu aizsardzība ne sliktāk kā to veic attiecīgi mobilo ierīču ražotāju Google Pay un Apple Pay autentifikācijas mehānismi |  |
| 8. | Otrā faktora autentifikācijas risinājuma centrālajām komponentēm ir jāvar nodrošināt augstu pieejamību, tās izvietojot divos datu centros / serveru telpās. Piegādātajam risinājumam ir jāietver visa nepieciešamā programmatūra un licences šāda risinājuma darbināšanai augstas pieejamības režīmā. |  |
| 9. | Otrā faktora autentifikācijas risinājuma centrālajām komponentēm ir jāvar darboties virtualizētā vidē, tai skaitā Pasūtītāja rīcībā esošajos serveros ar Microsoft HyperV virtualizācija programmatūru. |  |
| 10. | Otrā faktora autentifikācijas risinājumam jāietver Radius Proxy funkcionalitāte, lai nodrošinātu iespēju integrēt Otrā faktora autentifikāciju arī citām ierīcēm, kas izmanto RADIUS protokolu. |  |
| 11. | Radius Proxy risinājumam ir jānodrošina darbība augstas pieejamības režīmā, nodrošinot gan klientus autentificējošām ierīcēm divus neatkarīgus RADIUS savienojumus, gan rezervētus savienojumus ar Otrā faktora autentifikācijas risinājuma centrālajām komponentēm |  |
| 12. | Otrā faktora autentifikācijas risinājumam jābūt pieejamam API, SDK un dokumentācijai ar piemēriem ārējo integrāciju izveidei ar citām IT sistēmām, piemēram, tīmekļa lapas autentifikācijas risinājuma izveidei. Risinājumam jānodrošina vismaz REST API, kā arī aplikāciju interfeiss vismaz .NET, PHP un Ruby izstrādes vidēm |  |
| 13. | Piedāvātajam Daudzfaktoru autentifikācijas risinājumam jānodrošina integrācija ar Pasūtītāja rīcībā esošo Microsoft Active Directory serveri |  |

* 1. **Tīkla piekļuves autentifikācijas un autorizācijas programmatūras risinājums (1.gab**

|  |  |  |
| --- | --- | --- |
| **Nr.p.k.** | **Minimālais nepieciešamais** | **Pretendenta piedāvājums:**nodrošina / nenodrošina |
| 1. | Autentificējamo vienību (galiekārtu un lietotāju) skaits | Ne mazāk kā 5000 vienlaicīgi |  |
| 2. | Risinājuma funkcionālās prasības | Risinājums nodrošina:\* lietotāju un iekārtu autentifikāciju un uz kategorijām bāzētu tīkla piekļuves piešķiršanu dažādu ražotāju bezvadu, vadu un virtuālajiem privātajiem tīkliem\* politiku konfigurācijas veidnes un kļūmju novēršanas *(troubleshooting)* rīkus\* pašapkalpošanās iekārtu piekļuvi ar risinājumā iebūvētu sertificēšanas institūciju CA *(Certificate Authority)*\* mobilo iekārtu pārvaldības, interneta drošības un SIEM *(security information and events management)* risinājumu integrācijas iespēju\* SSO *(Single sign-on)* atbalstu ar SAML 2.0\* pašapkalpošanās portālu viesu kategorijas lietotājiem |  |
| 3. | Sistēmas rezervēšanas prasības | Jānodrošina risinājuma vienlaicīga darbība divos datu centros vienotā klāsterī un automātisku klāstera programmatūras atjaunināšanos |  |
| 4. | Lietojams kā virtuālā pakotne | Risinājums atbalsta sekojošas virtualizācijas platformas - VMWare ESXi no versijas 4.1 līdz 6.0 un Microsoft Hyper-V Server 2012 R2 un Hyper-V uz Microsoft Windows Server 2012 R2  |  |
| 5. | Atbalstītie AAA servisi | RADIUS, TACACS+, Kerberos |  |
| 6. | Lietotāju un iekārtu autentifikācijas un autorizācijas mehānismi | Risinājuma nodrošina autentifikāciju un autorizāciju uz informācijas bāzes, kas iegūta no Web pārlūka, iekārtas MAC adreses, 802.1X vai speciāla aģenta programmatūras Windows, Mac OS X un Linux datoriem  |  |
| 7. | Lietotāju tīkla piekļuves diferenciācija | Risinājums nodrošina lietotāju tīkla piekļuves diferenciāciju balstoties uz lomu piešķīrumiem, kuru pamatā ir vairāki RADIUS atribūti un to kombinācijas, tai skaitā tos var definēt lietojot regulārās izteiksmes (*Regular Expression, regex).* |  |
| 8. | Sadarbība ar tīkla iekārtām | Risinājums nodrošina sadarbību ar tīkla iekārtām lietojot RADIUS, RADIUS CoA, TACACS+, SNMP, SSH |  |
| 9. | Vairāku identitātes avotu vienlaicīga lietošana | Risinājums atbalsta vairāku identitātes avotu vienlaicīgu izmantošanu |  |
| 10. | Piekļuves ierobežošana | Risinājums nodrošina lietotāja piekļuves tīklam ierobežošanu visos veidos, ko ar RADIUS atribūtu un TACACS palīdzību atbalsta tīkla iekārtas |  |
| 11.  | Atskaites, analīzes un problēmu apstrādes rīki | Risinājumā iebūvēti lietotāja definējamas atskaites, analīzes un problēmu apstrādes rīki |  |
| 12. | Interaktīvas politiku simulācijas un pārraudzības režīma lietotnes | Risinājumā pieejamas interaktīvas politiku simulācijas un pārraudzības režīma lietotnes |  |
| 13. | Ieviešanas veidnes jebkuram tīkla veidam, identitātes avotam un gala iekārtai | Risinājumā pieejamas ieviešanas veidnes ar ražotāja specifiskiem RADIUS, TACACS+ u.c. parametriem jebkuram tīkla iekārtu veidam, identitātes avotam un gala iekārtai |  |
| 14. | Administratora/operatora droša piekļuve  | Risinājums nodrošina administratora/operatora drošu piekļuvi izmantojot kriptogrāfisku sertifikātu un TLS protokolu |  |
| 15. | IPSec tuneļu atbalsts | Risinājums atbalsta IPSec tuneļus |  |
| 16. | Protokolu un ietvaru *(framework)* atbalsts | Risinājums nodrošina vismaz sekojošu ietvaru un protokolu atbalstu:• RADIUS, RADIUS CoA, TACACS+, web authentication, SAML v2.0 • EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) • PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD) • TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP) • EAP-TLS • PAP, CHAP, MSCHAPv1 un 2, EAP-MD5 • NAC, Microsoft NAP • Windows machine authentication • MAC auth • Auditācijas pierakstus (uz portu un ievainojamību skanējumu balstīti nosacījumi) • Online Certificate Status Protocol (OCSP) • SNMP vispārējo MIB, SNMP privātos MIB • Common Event Format (CEF), Log Event Extended Format (LEEF) • TLS 1.2  |  |
| 17. | Identitātes avotu atbalsts | Risinājums atbalsta vismaz sekojošus identitātes avotus:• Microsoft Active Directory • RADIUS • Jebkura LDAP savietojama direktorija • Jebkurš ODBC-savietojams SQL serveris • Token serveris • Risinājumā iebūvētā SQL datu bāze, statisks saraksts • Kerberos• HTTP |  |
| 18. | RFC standartu atbalsts | Risinājums atbalsta vismaz sekojošus RFC standartus: 2246, 2248, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 4017, 4137, 4849, 4851, 5216, 528, 7030  |  |
| 19. | Interneta autentifikācijas protokolu projektu *(Internet draft)* atbalsts | Risinājums atbalsta vismaz Protected EAP versijas 0 un 1, Microsoft CHAP paplašinājumus, dinamisku nodrošinājumu *(provisioning)* lietojot EAP-FAST un TACACS+  |  |
| 20. | Iekārtu profilēšanas metodes | Risinājums atbalsta iekārtu profilēšanu pēc DHCP, TCP, MAC OUI, SNMP vai ar aģenta palīdzību |  |
| 21. | Integrācija ar trešo pušu risinājumiem | Risinājums atbalsta iespēju to integrēt ar trešo pušu Web lietotnēm un mobilo iekārtu pārvaldības risinājumiem lietojot RESTful API; REST/SOAP/XML API integrācijai ar citām lietotnēm |  |

* 1. **VPN risinājuma tehniskās prasības (1.gab).**

.

|  |  |  |
| --- | --- | --- |
| **Nr.p.k.** | **Minimālais nepieciešamais** | **Pretendenta piedāvājums** |
| 1. | Kopējā veiktspēju neizmantojot kriptēšanu:Iekārtai jānodrošina kopējais datu saņemšanas/nosūtīšanas ātrums vismaz – 1,8 Gbit/s (1400 baiti UDP)Reālas plūsmas (multiprotokolu) kopējais datu pārbaudes ātrums vismaz 900 Mbit/s  |  |
| 2. | Kopējā veiktspēja kriptēšanas režīmā:Iekārtai jānodrošina kopējais datu saņemšanas/nosūtīšanas ātrums izmantojot 3DES/AES IPsec VPN kriptēšanu vismaz - 250 Mbit/s; |  |
| 3. | Tīkla interfeisi - 8 GbE (10/100/1000BaseT)  |  |
| 4. | Iekārtas operatīvā atmiņa - 8GB vai vairāk; |  |
| 5. | Nodrošina vienlaicīgu pieslēgumu skaits – 250000. |  |
| 6. | Iekārtai vienlaicīgi jānodrošina VPN (IPSEC) tuneļus – 300. |  |
| 7. | Virtuālo interfeisu (VLAN) atbalsts - līdz 100 VLANiem |  |
| 8. | Nodrošina datu tīkla plūsmas pārbaudi OSI 7 līmenī (aplikācijas līmenī). |  |
| 9. | Jāatbalsta IKE un IPSec VPN standarti. Jāatbalsta X.509 sertifikāti un CRL (certificate revocation lists) - nodrošina VPN šifrēšanas protokolus 3DES/DES/AES. |  |
| 10. | Jādarbojas kā SSL vārtejai (gateway). Jānodrošina paplašināšanas iespējas līdz 300 SSL tuneļiem. |  |
| 11. | Ir iespējams darbināt ugunsmūri OSI 2. līmenī (strādā kā Layer 2 Transparent Firewall). |  |
| 12. | Nodrošina iespēju darbināt Iekārtu redundances režīmā - (bojājuma gadījumā otrais ugunsmūris pārņem pilnu funkcionalitāti). Iespēja darboties gan active-standby (viens ugunsmūris funkcionē, otrais pārņem funkcijas tikai pirmā bojājuma gadījumā), gan active-active (abi ugunsmūri pilda ugunsmūra funkcijas – load balancing) failover režīmā. |  |
| 13. | Nodrošina virtual firewall funkcionalitāti - (viena fiziskā Iekārta var nodrošināt vismaz 2 neatkarīgu ugunsmūru funkcijas). Paplašināms līdz 5 virtuāliem ugunsmūriem. |  |
| 14. | Nodrošina aplikāciju un protokolu inspekciju un pārbaudi - pārbauda sekojošus protokolus un to informācijas saturu - Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), SQL\*Net, Network File System (NFS), H.323 Versions 1-4, Session Initiation Protocol (SIP, Real-Time Streaming Protocol (RTSP) |  |
| 15. | DHCP client/server un DHCP relay funkciju atbalsts. |  |
| 16. | Atbalsta integrāciju ar RADIUS autentifikācijas un autorizācijas servisiem. |  |
| 17. | Nodrošina maršrutēšanas protokolu atbalstu - RIPv2, OSPF. |  |
| 18. | NAT/PAT atbalsts - tīkla adrešu translēšana. |  |
| 19. | IPSEC over PAT - caur šo ugunssienu var darboties IPSEC tuneļi (Iekārta ir IPSEC trafika plūsmas ceļā) pat ja Iekārta strādā PAT režīmā. |  |
| 20. | Nodrošina PPPoE atbalstu.  |  |
| 21. | Nodrošina gan CLI (komandrindas interfeisu), gan web-based GUI administrēšanu bez papildus programmnodrošinājuma maksas; |  |
| 22. | Nodrošina pieslēgšanos administrēšanas vajadzībām – https, ssh protokolu atbalsts; |  |
| 23. | Nodrošina SNMP, tcp/udp Syslog atbalstu. |  |
| 24. | Žurnālpierakstiem un paziņojumiem ir jābūt pilnībā integrējamiem Pasūtītāja IBM Qradar logfailu analīzes risinājumā. |  |
| 25. | VPN risinājumam jānodrošina vismaz 100 vienlaicīgu lietotāju VPN piekļuve Pasūtītāja tīklam izmantojot kriptētus tuneļus |  |
| 26. | VPN risinājumam jānodrošina nepieciešamā klienta programmatūra vismaz Windows 10, 8.1, 8, 7, Mac OS X 10.8 un vēlāku versiju, Linux Intel (x64) platformām. |  |
| 27. | VPN klienta programmatūru Windows un MAC OS X vidēm autentificētiem lietotājiem ir jāvar instalēt tieši no VPN koncentratora ierīces. |  |
| 28. | VPN risinājumam jānodrošina attālinātās piekļuves datu pārraides kriptēšana, izmantojot AES-256 un 3DES-168 algoritmus |  |
| 29. | VPN risinājumam jānodrošina attālinātās piekļuves politiku automātiska centralizēta izplatīšana VPN klientu datoriem |  |
| 30. | Tīkla administratoram jābūt iespējai centralizēti pārvaldīt nodalītas vai pilnīgas tīkla piekļuves tunelēšanas politiku un IP adrešu piešķiršanas mehānismus VPN savienojumos |  |
| 31. | VPN risinājumam jānodrošina attālinātu tīkla piekļuvi izmantojot vismaz šādas tunelēšanas tehnoloģijas atkarībā no attālā tīkla ierobežojumiem: DTLS, TLS (HTTP virs TLS/SSL) , IPsec IKEv2  |  |

**Ar SPECIFIKĀCIJU iepazinos, piekrītu izpildīt un nodrošināt augstāk minētās prasības:**

Paraksts:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(Pretendenta paraksttiesīgā persona vai pilnvarotais pārstāvis)

2016. gada \_\_\_\_\_. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_