TECHNINĖ SPECIFIKACIJA

I pirkimo dalis: *Duomenų apsaugos įrenginys – 1 vnt.*

1. Bendrieji reikalavimai

1.1. Visa pateikiama techninė įranga privalo būti nauja (negali būti atnaujinta, restauruota (angl. *Refurbished*), nenaudota, pateikta nepažeistoje gamyklinėje pakuotėje;

1.2. Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. *End of lifetime* ar *Discontinued*);

1.3. Įrangos dokumentai turi būti lietuvių arba anglų kalba. Užrašai ant įrenginio ir jo dalių turi būti anglų arba lietuvių kalba. Gamintojo interneto svetainėje - paieška atliekama anglų arba lietuvių kalba;

1.4. Visos programinės įrangos (jei tokia yra pateikiama) licencija turi būti suteikiama neribotam laikui;

1.5. Techninė įranga privalo veikti be sutrikimų, kai temperatūros režimas techninės įrangos įdiegimo patalpoje yra nuo +10 ºC iki +40 ºC, o santykinė oro drėgmė – 70 proc. ir mažesnė;

1.6. Tiekėjas turi pateikti siūlomos įrangos ir visų jos sudėtinių dalių gamintojo identifikacinius kodus. Nepateikus šios informacijos pasiūlymas laikomas neatitinkančiu techninių reikalavimų.“

1.7. Saugumo reikalavimai:

1.7.1. Standieji ar puslaidininkiniai diskai (angl. *HDD/SSD*) ar kitos atminties laikmenos gedimo atveju turi būti keičiamos naujomis. Sugedusios atminties laikmenos sunaikinamos pirkėjo patalpose ir tiekėjui negrąžinamos;

1.7.2. Įrangos gedimo atveju iš instaliacijos vietos remontui išvežamą pas tiekėją (jo atstovą) sugedusią įrangą pirkėjas pateikia be joje sumontuotų standžiųjų ar puslaidininkinių diskų (angl. *HDD/SSD*) ar kitų atminties laikmenų;

1.7.3. Turi atitikti Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalį. Pirkėjas, atlikdamas pirkimo procedūras, įvertina visus galinčius kelti grėsmę nacionalinio saugumo interesams rizikos veiksnius ir sprendžia, ar šiame pirkime gali dalyvauti tiekėjai, jų subtiekėjai ir ūkio subjektai, kurių pajėgumais remiamasi, kurie nėra registruoti (jeigu tiekėjas, jų subtiekėjas ar ūkio subjektas, kurio pajėgumais remiamasi, yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje šio straipsnio 4 dalyje nurodytus tarptautinius susitarimus;

1.7.4. Pirkėjas, vadovaudamasi Viešųjų pirkimų įstatymo 17 straipsnio 5 dalimi pirkime neleidžia dalyvauti tiekėjams (juridiniams asmenims)/subtiekėjams (juridiniams asmenims), kurie nėra registruoti Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje Pasaulio prekybos organizacijos sutartį dėl viešųjų pirkimų ir kitus tarptautinius susitarimus. Taip pat pirkime neleidžiama dalyvauti tiekėjams (fiziniams asmenims)/subtiekėjams (fiziniams asmenims), kurie nėra deklaravę gyvenamosios vietos Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje Pasaulio prekybos organizacijos sutartį dėl viešųjų pirkimų ir kitus tarptautinius susitarimus;

1.8. Tiekėjas turi užtikrinti, kad įsigyjamoje įrangoje nebūtų įdiegta jokios papildomos programinės įrangos, kuri nėra būtina tokios įrangos funkcionalumui užtikrinti. Paaiškėjus, kad įrangoje yra įdiegta kenkimo programinė įranga, tai būtų traktuojama kaip reikalavimų neatitikimas ir sutarties sąlygų nesilaikymas:

1.8.1. Įranga grąžinama tiekėjui arba keičiama nauja lygiaverte ar geresne, tačiau saugumo reikalavimus atitinkančia įranga;

1.8.2. Tiekėjas padengia pirkimo proceso metu pirkėjo patirtą materialinę žalą.

1.9. Įrangos gamintojas privalo užtikrinti Europos Sąjungos *RoHS* (angl. *„Restriction of Hazardous Substances“*) direktyvos (2011/65/EU), draudžiančios gamyboje naudoti aplinkai ir žmogaus sveikatai pavojingas medžiagas (pvz., gyvsidabrį, kadmį, šviną, šešiavalentį chromą, o taip pat antipirenus), reikalavimų įvykdymą. Tiekėjas kartu su pasiūlymu turi pateikti atitiktį reikalavimams įrodančius dokumentus: gamintojo atitikties deklaracijos kopiją ar nuorodą į gamintojo puslapį arba kitus lygiaverčius dokumentus.

2. Specialieji reikalavimaiEil. Nr.	**Parametrai**	**Reikalavimai**
1	**2**	**3**
2.1.	Slaptumo aspektai	Siūlomas įrenginys turi būti patvirtintas NATO Karinio komiteto memorandumu (angl. *Military Committee Memorandum*).
2.2.	Apsauga nuo informatyvaus elektromagnetinio spinduliavimo (angl. Tempest)	Turi būti sertifikuota pagal NATO dokumento SDIP-27 Tempest A lygio (angl. Level A) keliamus reikalavimus ir sertifikavimas turi galioti neribotai.
2.3.	Suderinamumas	Įranga turi būti suderinama su *Thales TCE 114 Key Generation Center* ir *Thales TCE 671 Security Management Center*.
2.4.	Matmenys	2.4.1. Montuojamas į 19 colių spintą (montuoti reikalingos detalės turi būti pridedamos); 2.4.2. ne aukštesnis kaip 1RU (angl. *Rack Unit*).
2.5.	Sąsajos	2.5.1. „Nesaugios“ (angl. Black) pusės įrangą turi būti galima prijungti: 2.5.1.1. 10/100/1000 Mbps Ethernet sąsaja su RJ-45 jungtimi; 2.5.1.2. 100BaseFX sąsaja su dviguba (angl. Dual) LC jungtimi, 2.5.1.3. 1000BaseSX sąsaja su dviguba (angl. Dual) LC jungtimi. 2.5.2. „Saugios“ (angl. Red) pusės įrangą turi būti galima prijungti: 2.5.2.1. 10/100/1000 Mbps Ethernet sąsaja su RJ-45 jungtimi; 2.5.2.2. 100BaseFX sąsaja su dviguba (angl. Dual) LC jungtimi, 2.5.2.3. 1000BaseSX sąsaja su dviguba (angl. Dual) LC jungtimi.
2.6.	Palaikomi protokolai	2.6.1. Turi palaikyti RFC791 (IPv4); 2.6.2. Turi palaikyti RFC2460 (IPv6).
2.7.	Paslaugos kokybė	Turi palaikyti QoS (angl. *Quality of Service*).
2.8.	Valdymas	Turi turėti galimybę valdyti duomenų apsaugos įrenginį tiek nuotoliniu būdu, tiek tiesiogiai, naudojant duomenų apsaugos įrenginio valdymo panelę.
2.9.	Greitaveika	Dvipusio duomenų perdavimo greitaveika (angl. F*ull duplex data rate*) ne mažesnė kaip 1500 Mbit/s.

2. Specialieji reikalavimaiEil. Nr.	Parametrai	Reikalavimai
1	2	3
2.10.	Gaišties laikas	Ne daugiau kaip 0,1 ms.
2.11.	Kriptografinių raktų įkėlimo sąsajos	2.11.1. Turi turėti šias kriptografinių raktų įkėlimo sąsajas: 2.11.1.1. DS-101 (AN/CYZ-10 DTD); 2.11.1.2. DS-102 (KOI-18); 2.11.1.3. ISO 7816 (Smartcard).
2.12.	Ištrynimo galimybė	Turi turėti greitojo kriptografinių raktų ištrynimo galimybę nesant maitinimo iš elektros tinklo.
2.13.	Komplektavimas	2.13.1. Įrenginys turi turėti visas reikalingas priemones kriptografiniams raktams įkelti iš lustinių kortelių (angl. *Smart Card*), DTD ir KOI-18, nesutrikdant įrenginio darbo (duomenų apsaugos); 2.13.2. Įrenginys turi būti komplektuojamas su to paties gamintojo ne mažiau kaip 2 (dviem) optiniais adapteriais (*1000BaseSX* sąsaja, dvigubos (angl. *Dual*) *LC* daugiamodžių (angl. *Multimode*) tipo optinės jungtys, 2.13.3. Įrenginys turi būti komplektuojamas su to paties gamintojo ne mažiau kaip 2 (dviem) kabeliais prijungimui prie *Ethernet*; 2.13.4. Įrenginys turi būti komplektuojamas su to paties gamintojo elektros maitinimo adapteriu prijungimui prie 230V 50Hz elektros tinklo su Europos kontinentinėje dalyje naudojamomis jungtimis CEE 7/7 arba CEE 7/16; 2.13.5. Visi priedai reikalingi įrenginio sumontavimui į 19 colių spintą (ne mažiau kaip 10 vnt. varžtų ir ne mažiau kaip 10 vnt. veržlių įrangos montavimui į 19 colių telekomunikacijų spintą, ne mažiau kaip 10 vnt. medžiaginių *Velcro* dirželių (ilgis ne mažiau 20 cm)).
2.14.	Garantijos trukmė ir sąlygos	2.14.1. Garantinis laikotarpis – 60 (šešiasdešimt) mėnesių nuo įrangos perdavimo-priėmimo akto pasirašymo dienos; 2.14.2. Garantiniu laikotarpiu turi būti nemokamai teikiami gamintojo programinės įrangos atnaujinimai (angl. *Upgrades*, *Updates*); 2.14.3. Garantinio remonto trukmė privalo trukti ne ilgiau kaip 60 kalendorinių dienų (neskaičiuojant transportavimo laiko). Jei sugedusios įrangos per šį laikotarpį pataisyti neįmanoma – ji pakeičiama ekvivalentiška nauja; 2.14.4. Garantinis laikotarpis skaičiuojamas nuo priėmimo-perdavimo akto pasirašymo dienos; 2.14.5. Garantinio laikotarpio metu, tiekėjas privalo atlikti garantinį remontą savo lėšomis, įskaitant transportavimo išlaidas.
2.15.	Pristatymas	Duomenų apsaugos įrenginys pristatomas per 270 kalendorinių dienų nuo Sutarties įsigaliojimo dienos į

2. Specialieji reikalavimaiEil. Nr.	Parametrai	Reikalavimai
1	2	3
		Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos, atliekantį Nacionalinės šifrų paskirstymo tarnybos funkcijas, adresu Gedimino pr. 40, 01110 Vilnius.

II pirkimo dalis: *Ugniasienė (BLACK) – 1 vnt.*

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
1.	Įrenginio tipas	Specializuotas įrenginys, susidedantis iš techninės bei programinės įrangos. Visa įrenginyje instaliuota programinė įranga yra specializuota programinė įranga numatytoms funkcijoms atlikti, užtikrinanti įrenginio veikimo patikimumą bei saugumą.
2.	Suderinamumas	Siūlomas įrenginys turi būti pilnai suderinamas su pirkėjo naudojama centralizuota ugniasienių valdymo programine įranga „Fortinet FortiManager“ FMG-VM64 ir FortiAnalyzer 7.6.x ir aukštesne versija bei gebėti užmegzti IPSec VPN tunelį su turima Fortigate įranga. Įrenginyje negali būti įmontuotų bevielio ryšio įrenginių komponentų. Gali būti pateikiamas analogiško funkcionalumo įrenginys suderinamas su kita kartu pateikiama ir į pasiūlymo kainą įtraukta analogiška ugniasienių valdymo ir žurnalinių įrašų surinkimo ir agregavimo sistema (toliau - Sistema). Sistema turi veikti atskiroje techninėje platformoje, pasiūlyme įtrauktas jos garantinio palaikymo ir atnaujinimo laikotarpis nemažesnis nei ugniasienių garantinio palaikymo laikotarpis.
3.	Korpuso tipas	„Desktop“ tipo arba montuojamas į 19 colių komutacinę spintą. Įrenginio aukštis turi būti ne daugiau 1U. Pridedamas montavimo į 19' colių komutacinę spintą komplektas.
4.	El. maitinimo šaltinis	Neintegruotas arba integruotas maitinimo šaltinis
5.	El. maitinimas	240V AC
6.	Prievadų konfigūracija	• Integruotų 10/100/1000 Ethernet (RJ45 tipo) prievadų skaičius - ne mažiau 10 vnt.; • Iš jų ne mažiau 2 vnt. optiniai prievadai, 1Gbps • USB prievadas; • Konsolės prievadas.
7.	Optiniai moduliai	2 vnt. 1000 Base-SX SFP LC, palaikančių 500 metrų Multi Mode fiber sujungimą;
8.	Vidinis diskas	Ne mažesnės nei 120 GB talpos kietas diskas
9.	Įrenginio našumas	• Ugniasienės greitaveika - ne mažiau 10 Gbps; • Ugniasienės vėlinimas - ne daugiau nei 3.5 mikro sekundės; • Lygiagrečių sesijų kiekis - ne mažiau nei 1500000. vnt.; • Naujų sesijų per sekundę kiekis - ne mažiau nei 45 000 vnt.; • IPSec VPN palaikoma greitaveika - ne mažiau 6,5 Gbps; • SSL-VPN palaikoma greitaveika - ne mažiau 950 Mbps; • Įsilaužimų prevencijos (IPS) greitaveika – ne mažiau 1,4 Gbps.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
10.	Bendro pobūdžio ugniasienės funkcijos	• Veiklos tipas - NAT, PAT, Transparent (Bridge); • “Policy-Based NAT” funkcionalumas; • “VLAN Tagging (802.1Q)” funkcionalumas; • Vartotojų grupių autentifikacija; • “SIP/H.323 NAT Traversal” funkcionalumas; • “STP forwarding” funkcionalumas; • Keičiami saugos profiliai; • Neapribotas vidinių vartotojų skaičius.
11.	Įrenginio VPN funkcijos ir našumas	Turi palaikyti šiuos VPN funkcionalumus: • IPSec, SSL-VPN dedikuotų tunelių palaikymas; • 3DES, AES256 kriptavimo algoritmus; • “Dead Peer Detection” funkcionalumas; • “IPSec NAT Traversal” funkcionalumas; • Automatinis IPSec konfigūravimas; • SHA-1, SHA-256,SHA-512, MD5 autentifikacijos palaikymas; • Palaikomų IPSec VPN tunelių kiekis, – įrenginys-įrenginys ne mažiau 150 vnt; • Palaikomų IPSec VPN tunelių kiekis, – įrenginys-klientas ne mažiau 300 vnt; • Palaikomų VPN tunelių kiekis (SSL-VPN) – ne mažiau 150 vnt.
12.	Virtualių ugniasienių palaikymas	Virtualių ugniasienių palaikymas: • Turi palaikyti virtualias ugniasienes; • Įrenginys pateikiamas su galimybe padalinti į ne mažiau 3 virtualių ugniasienių, reikalingos licencijos pateikiamos kartu su įrenginiu.
13.	IPS funkcijos	Turi palaikyti šiuos IPS funkcionalumus: • Darbas IPS režime; • Darbas IDS režime; • Protokolų anomalijų palaikymas; • Modifikuotų taisyklių rinkinių (*angl. signature*) palaikymas; • Automatinis įsilaužimų duomenų bazės atnaujinimas; • IPv6 palaikymas.
14.	Antiviruso funkcijos	Turi palaikyti šiuos antiviruso funkcionalumus: • Įrenginys turi tikrinti duomenų srautą nuo virusų; • Turi turėti „AntiSpyware“ ir „WormPrevention“ funkcionalumą; • Turi skenuoti HTTP/SMTP/POP3/IMAP/FTP/IM ir kriptuotus SSL VPN tunelius; • Automatinis virusų duomenų bazės naujinimas; • Infekuotų ir įtartinų bylų karantino palaikymas; • Bylų blokavimas pagal bylos dydį ir tipą.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
15.	Srautų valdymas	Turi būti: • Duomenų srauto ribojimas pagal ugniasienės taisykles; • Duomenų srauto ribojimas pagal IP adresą; • Duomenų srauto ribojimas pagal aplikaciją; • Diferencijuotų servisų palaikymas (*angl. DiffServ*); • Garantijų/maksimalaus srauto/Prioritetų dėliojimas Minimalaus pralaidumo užtikrinimas; • Maksimalaus pralaidumo apribojimas; • Viršijančio srauto blokavimas (*angl. traffic policing*).
16.	Srautų paskirstymas	Turi būti: • Srauto balansavimas pagal L3 ,L4 ir L7 OSI tinkle lygmenų informaciją; • HTTP ir HTTPS multepliksavimas; • HTTP session/cookie išsilaikymas; • Srauto paskirstymo metodai: Statinis, pagal mažiausią sesijų skaičių (*angl. roundrobin)*, pagal mažiausią atsako laiką (*angl. roundtriptime*) - *weighted*. • „SSL offload“ funkcionalumas.
17.	Duomenų persiuntimo kontrolė	Turi būti šios duomenų persiuntimo kontrolės funkcijos: • Įrenginys turi turėti galimybę tikrinti duomenų srautą; • Duomenų srauto stebėjimas ir kontrolė; • Siunčiamų duomenų patikrinimas remiantys „RegEx“ baze; • Konfigūruojami veiksmai – blokuoti, stebėti; • Atpažįsta daugelį bylų formatų.
18.	Tinklai/Maršrutizavimo funkcionalumas	Turi būti: • Dviejų ISP palaikymas vienu metu; • DHCP Client, DHCP Server, DHCP relay funkcionalumai; • Policy-Based maršrutizavimas pagal taisykles; • Dinaminis maršrutizavimas IPv4 (RIP v1 & v2, OSPF, BGP, Multicast, IS-IS); • Dinaminis maršrutizavimas IPv6 (RIP v1, OSPF, BGP); • Įvairių saugumo zonų palaikymas su tarp zoninių maršrutizavimų; • Maršrutizavimas tarp virtualių potinklių, tarp virtualių įrenginių; • Statinis IPv4 ir IPv6 maršrutizavimas.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
19.	Valdymas/ Administravimo funkcionalumas	Turi būti: • Konsolinis kabelis; • WebUI (HTTP/HTTPS) ir komandinės eilutės; • Telnet / SecureCommand Shell (SSH); • Administravimas pagal roles; • Kelių kalbų palaikymas, viena iš jų privalo būti anglų kalba; • Administratorių ir Vartotojų lygiai; • Atnaujinimas ir keitimai per FTP ir WebUI; • SNMP; • Centralizuotas kelių įrenginių valdymas per specializuota tuo paties gamintojo įrenginį; • Dviejų programinės įrangos (*angl. firmware*) versijų talpinimas vienu metu pastovioje atmintyje; • Srauto balansavimas/paskirstymas; • Konfigūracijos archyvavimas ir versijavimas įrenginyje.
20.	Sisteminiai įrašai/Stebėjimas	Turi būti: • Vidinis įvykių žurnalas; • Įvykių persiuntimas į nutolusį „Syslog“ serverį; • Grafinis realaus laiko ir istorinis stebėjimas; • SNMP; • E-mail įspėjimai apie virusus ir atakas; • VPN tunelių stebėjimas; • Galimas nuodugnesnis stebėjimas pasirenkant to paties gamintojo sisteminių įrašu stebėjimo įrangą.
21.	Vartotojų autentifikavimas	Vartotojų autentifikavimas turi būti realizuojama šiais būdais: • Lokalūs vartotojai; • Integracija su Windows AD arba lygiavertė; • Išorinių RADIUS/LDAP/TACACS+ tarnybų palaikymas; • Xauth per RADIUS IPSEC VPN tuneliams; • Autentifikavimas sertifikatais (PKI); • Dviejų faktorių autentifikavimo palaikymas.
22.	P2P/IM valdymas ir aplikacijų kontrolė	Turi atpažinti ne mažiau kaip 2000 aplikacijų, įskaitant „Youtube“, „Gmail“, „Twiter“, „Facebook“, Web paštus. Turi galėti stebėti, riboti, blokuoti aplikacijas.
23.	Aprašų duomenų bazės	Aprašų duomenų bazės turi būti to paties gamintojo, jei naudojamos trečių šalių aprašų bazės jos gali būti tik kaip papildomos, o ne pagrindinės.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
24.	Garantija	Gamintojo garantuojamas 60 (šešiasdešimties) mėn. garantinis aptarnavimas bei atnaujinimų teikimas garantiniu laikotarpiu (virusų, piktybinių programų, įsilaužimų aprašų,) nuo prekių perdavimo-priėmimo akto pasirašymo dienos. Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) 24x7 sąlygomis internetu, elektroniniu paštu, turi būti suteikta prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
25.	Sertifikatai	Siūloma įranga turi turėti CE, FCC ir UL arba lygiaverčius sertifikatus. Tiekėjas privalo kartu su pasiūlymu pateikti šių sertifikatų kopijas arba nuorodas į oficialias duomenų bazes, kuriose galima patikrinti sertifikatų galiojimą ir atitiktį. Sertifikatai gali būti pateikti elektroniniu arba popieriniu formatu
26.	Pristatymas	Ugniasienė (BLACK) pristatoma per 35 kalendorines dienas nuo Sutarties įsigaliojimo dienos į Lietuvos Respublikos užsienio reikalų ministeriją adresu: J. Tumo-Vaižganto g. 2, 01108 Vilnius.

III pirkimo dalis: *Ugniasienė (RED) – 1 vnt.*

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
1.	Įrenginio tipas	Specializuotas įrenginys, susidedantis iš techninės bei programinės įrangos. Visa įrenginyje instaliuota programinė įranga yra specializuota programinė įranga numatytoms funkcijoms atlikti, užtikrinanti įrenginio veikimo patikimumą bei saugumą.
2.	Suderinamumas	Siūlomas įrenginys turi būti pilnai suderinamas su pirkėjo naudojama centralizuota ugniasienių valdymo programine įranga „Fortinet FortiManager“ FMG-VM64 ir Fortianalyzer 7.6.x ir aukštesne versija bei gebėti užmegzti IPSec VPN tunelį su turima Fortigate įranga. Įrenginyje negali būti įmontuotų bevielių įrenginių komponentų, bei įrenginys turi būti sertifikuotas Tempest B lygiui. Alternatyviai gali būti pasiūlytas analogiško funkcionalumo įrenginys, suderinamas su kita, kartu pasiūlyme pateikiama ir į pasiūlymo kainą įtraukta analogiška ugniasienių valdymo bei žurnalinių įrašų surinkimo ir agregavimo sistema (toliau – Sistema). Sistema turi veikti atskiroje techninėje platformoje, pasiūlyme įtrauktas jos garantinio palaikymo ir atnaujinimo laikotarpis nemažesnis nei ugniasienių garantinio palaikymo laikotarpis. Įrenginys palaiko ir pateikiamas su ne mažesne nei 7.0 FORTI OS versija.
3.	Korpuso tipas	„Desktop“ tipo arba montuojamas į 19 colių komutacinę spintą. Įrenginio aukštis turi būti ne daugiau 1U. Pridedamas montavimo į 19' colių komutacinę spintą komplektas
4.	El. maitinimo šaltinis	Neintegruotas arba integruotas maitinimo šaltinis
5.	El. maitinimas	240V AC
6.	Prievadų konfigūracija	• Integruotų 10/100/1000 Ethernet (RJ45 tipo) prievadų skaičius - ne mažiau 10 vnt.; • Iš jų ne mažiau 2 vnt. optiniai prievadai, 1Gbps, LC multimode, arba pateikiami keitikliai sertifikuoti TEMPEST B lygiui • USB prievadas; • Konsolės prievadas.
7.	Optiniai moduliai	2 vnt. 1000 Base-SX SFP LC, palaikančių 500 metrų Multi Mode fiber sujungimą;
8.	Vidinis diskas	Ne mažesnės nei 120 GB talpos kietas diskas

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
9.	Įrenginio našumas	• Ugniasienės greitaveika - ne mažiau 10 Gbps; • Ugniasienės vėlinimas - ne daugiau nei 3.5 mikro sekundės; • Lygiagrečių sesijų kiekis - ne mažiau nei 1500000. vnt.; • Naujų sesijų per sekundę kiekis - ne mažiau nei 45 000 vnt.; • IPSec VPN palaikoma greitaveika - ne mažiau 6,5 Gbps; • SSL-VPN palaikoma greitaveika - ne mažiau 950 Mbps; • Įsilaužimų prevencijos (IPS) greitaveika – ne mažiau 1,4 Gbps.
10.	Bendro pobūdžio ugniasienės funkcijos	• Veiklos tipas - NAT, PAT, Transparent (Bridge); • “Policy-Based NAT” funkcionalumas; • “VLAN Tagging (802.1Q)” funkcionalumas; • Vartotojų grupių autentifikacija; • “SIP/H.323 NAT Traversal” funkcionalumas; • “STP forwarding” funkcionalumas; • Keičiami saugos profiliai; • Neapribotas vidinių vartotojų skaičius.
11.	Įrenginio VPN funkcijos ir našumas	Turi palaikyti šiuos VPN funkcionalumus: • IPSec, SSL-VPN dedikuotų tunelių palaikymas; • 3DES, AES256 kriptavimo algoritmus; • “Dead Peer Detection” funkcionalumas; • “IPSec NAT Traversal” funkcionalumas; • Automatinis IPSec konfigūravimas; • SHA-1, SHA-256,SHA-512, MD5 autentifikacijos palaikymas; • Palaikomų IPSec VPN tunelių kiekis, - įrenginys-įrenginys ne mažiau 150 vnt; • Palaikomų IPSec VPN tunelių kiekis, - įrenginys-klientas ne mažiau 300 vnt; • Palaikomų VPN tunelių kiekis (SSL-VPN) - ne mažiau 150 vnt.
12.	Virtualių ugniasienių palaikymas	Virtualių ugniasienių palaikymas: • Turi palaikyti virtualias ugniasienes; • Įrenginys pateikiamas su galimybe padalinti į ne mažiau 3 virtualių ugniasienių, reikalingos licencijos pateikiamos kartu su įrenginiu.
13.	IPS funkcijos	Turi palaikyti šiuos IPS funkcionalumus: • Darbas IPS režime; • Darbas IDS režime; • Protokolų anomalijų palaikymas; • Modifikuotų taisyklių rinkinių (*angl. signature*) palaikymas; • Automatinis įsilaužimų duomenų bazės atnaujinimas; • IPv6 palaikymas.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
14.	Antiviruso funkcijos	Turi palaikyti šiuos antiviruso funkcionalumus: • Įrenginys turi tikrinti duomenų srautą nuo virusų; • Turi turėti „AntiSpyware“ ir „WormPrevention“ funkcionalumą; • Turi skenuoti HTTP/SMTP/POP3/IMAP/FTP/IM ir kriptuotus SSL VPN tunelius; • Automatinis virusų duomenų bazės naujinimas; • Infekuotų ir įtartinų bylų karantino palaikymas; • Bylų blokavimas pagal bylos dydį ir tipą.
15.	Srautų valdymas	Turi būti: • Duomenų srauto ribojimas pagal ugniasienės taisykles; • Duomenų srauto ribojimas pagal IP adresą; • Duomenų srauto ribojimas pagal aplikaciją; • Diferencijuotų servisų palaikymas (*angl. DiffServ*); • Garantijų/maksimalaus srauto/Prioritetų dėliojimas Minimalaus pralaidumo užtikrinimas; • Maksimalaus pralaidumo apribojimas; • Viršijančio srauto blokavimas (*angl. traffic policing*).
16.	Srautų paskirstymas	Turi būti: • Srauto balansavimas pagal L3 ,L4 ir L7 OSI tinkle lygmenų informaciją; • HTTP ir HTTPS multepliksavimas; • HTTP session/cookie išsilaikymas; • Srauto paskirstymo metodai: Statinis, pagal mažiausią sesijų skaičių (*angl. roundrobin)*, pagal mažiausią atsako laiką (*angl. roundtriptime*) - *weighted*. • „SSL offload“ funkcionalumas.
17.	Duomenų persiuntimo kontrolė	Turi būti šios duomenų persiuntimo kontrolės funkcijos: • Įrenginys turi turėti galimybę tikrinti duomenų srautą; • Duomenų srauto stebėjimas ir kontrolė; • Siunčiamų duomenų patikrinimas remiantys „RegEx“ baze; • Konfigūruojami veiksmai – blokuoti, stebėti; • Atpažįsta daugelį bylų formatų.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
18.	Tinklai/Maršrutizavimo funkcionalumas	Turi būti: • Dviejų ISP palaikymas vienu metu; • DHCP Client, DHCP Server, DHCP relay funkcionalumai; • Policy-Based maršrutizavimas pagal taisykles; • Dinaminis maršrutizavimas IPv4 (RIP v1 & v2, OSPF, BGP, Multicast, IS-IS); • Dinaminis maršrutizavimas IPv6 (RIP v1, OSPF, BGP); • Įvairių saugumo zonų palaikymas su tarp zoninių maršrutizavimų; • Maršrutizavimas tarp virtualių potinklių, tarp virtualių įrenginių; • Statinis IPv4 ir IPv6 maršrutizavimas.
19.	Valdymas/ Administravimo funkcionalumas	Turi būti: • Konsolinis kabelis; • WebUI (HTTP/HTTPS) ir komandinės eilutės; • Telnet / SecureCommand Shell (SSH); • Administravimas pagal roles; • Kelių kalbų palaikymas; • Administratorių ir Vartotojų lygiai; • Atnaujinimas ir keitimai per FTP ir WebUI; • SNMP; • Centralizuotas kelių įrenginių valdymas per specializuota tuo paties gamintojo įrenginį; • Dviejų programinės įrangos (*angl. firmware*) versijų talpinimas vienu metu pastovioje atmintyje; • Srauto balansavimas/paskirstymas; • Konfigūracijos archyvavimas ir versijavimas įrenginyje.
20.	Sisteminiai įrašai/Stebėjimas	Turi būti: • Vidinis įvykių žurnalas; • Įvykių persiuntimas į nutolusį „Syslog“ serverį; • Grafinis realaus laiko ir istorinis stebėjimas; • SNMP; • E-mail įspėjimai apie virusus ir atakas; • VPN tunelių stebėjimas; • Galimas nuodugnesnis stebėjimas pasirenkant to paties gamintojo sisteminių įrašu stebėjimo įrangą.
21.	Vartotojų autentifikavimas	Vartotojų autentifikavimas turi būti realizuojama šiais būdais: • Lokalūs vartotojai; • Integracija su Windows AD arba lygiavertė; • Išorinių RADIUS/LDAP/TACACS+ tarnybų palaikymas; • Xauth per RADIUS IPSEC VPN tuneliams; • Autentifikavimas sertifikatais (PKI); • Dviejų faktorių autentifikavimo palaikymas.

Eil. Nr.	Parametrai	Reikalavimai
1	**2**	**3**
22.	P2P/IM valdymas ir aplikacijų kontrolė	Turi atpažinti ne mažiau kaip 2000 aplikacijų, įskaitant „Youtube“, „Gmail“, „Twiter“, „Facebook“, Web paštus. Turi galėti stebėti, riboti, blokuoti aplikacijas.
23.	Aprašų duomenų bazės	Aprašų duomenų bazės turi būti to paties gamintojo, jei naudojamos trečių šalių aprašų bazės jos gali būti tik kaip papildomos, o ne pagrindinės.
24.	Garantija	Gamintojo garantuojamas 60 (šešiasdešimties) mėn. garantinis aptarnavimas bei atnaujinimų teikimas garantiniu laikotarpiu (virusų, piktybinių programų, įsilaužimų aprašų) nuo prekių perdavimo-priėmimo akto pasirašymo dienos. Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) 24x7 sąlygomis internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
25.	Sertifikatai	Siūloma įranga turi turėti CE, FCC ir UL arba lygiaverčius sertifikatus. Tiekėjas privalo kartu su pasiūlymu pateikti šių sertifikatų kopijas arba nuorodas į oficialias duomenų bazes, kuriose galima patikrinti sertifikatų galiojimą ir atitiktį. Sertifikatai gali būti pateikti elektroniniu arba popieriniu formatu.
26.	Pristatymas	Ugniasienė (RED) pristatoma per 175 kalendorines dienas nuo Sutarties įsigaliojimo dienos į Lietuvos Respublikos užsienio reikalų ministeriją adresu: J. Tumo-Vaižganto g. 2, 01108 Vilnius.