TECHNINĖ SPECIFIKACIJA

I pirkimo dalis: *Duomenų šifravimo 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 (jei nenurodyta kitaip);

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 (jei nenurodyta kitaip);

1.6. tiekėjas privalo pasiūlyme pateikti įrangos ir visų jos sudėtinių dalių gamintojo identifikacinius kodus;

1.7. saugumo reikalavimai (netaikoma programinei įrangai):

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. Užsakovas, 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. Užsakovas, 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 turi pateikti atitiktį reikalavimams įrodančius dokumentus: gamintojo atitikties deklaracijos kopiją ar nuorodą į gamintojo puslapį, arba kitus lygiaverčius dokumentus. Tiekėjas gali pateikti kitus lygiaverčius įrodymus, kuriais patvirtinama siūlomos įrangos atitiktis kitiems žaliojo pirkimo reikalavimams.

2. **Duomenų šifravimo įrenginys**:

2.1. Slaptumo aspektai: siūlomas įrenginys turi būti NATO Karinio komiteto memorandumu (angl. *Military Committee Memorandum*) patvirtintas, kad yra tinkamas įslaptintos informacijos, žymimos slaptumo žyma COSMIC TOP SECRET, slaptumui užtikrinti.

2.2. Apsauga nuo informatyvaus elektromagnetinio spinduliavimo (angl. *Tempest*): sertifikuota pagal NATO dokumento SDIP-27 *Tempest* A lygio (angl. *Level A*) keliamus reikalavimus ir sertifikavimas turi galioti neribotai.

2.3. Šifravimo raktai: turi naudoti *Thales TCE 114 Key Generation Center* sugeneruotus šifravimo raktus ir turėti galimybę būti valdomas *Thales TCE 671 Security Management Centre* pagalba.

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 šifratorių tiek nuotoliniu būdu, tiek tiesiogiai, naudojant šifratoriaus valdymo panelę.

2.9. Greitaveika: dvipusio duomenų perdavimo greitaveika (angl. F*ull duplex data rate*) ne mažesnis kaip 1500 Mbit/s.

2.10. Gaišties laikas: ne daugiau kaip 0,1 ms.

2.11. Kriptografinių raktų įkėlimo sąsajos. Turi turėti šias kriptografinių raktų įkėlimo sąsajas:

2.11.1. DS-101 (AN/CYZ-10 DTD);

2.11.2. DS-102 (KOI-18);

2.11.3. ISO 7816 (Smartcard).

2.12. Ištrynimo galimybė: turi turėti greitojo šifravimo raktų ištrynimo galimybę nesant maitinimo iš elektros tinklo.

2.13. Komplektavimas:

2.13.1. įrenginys turi turėti visas reikalingas priemones šifravimo raktams įkelti iš lustinių kortelių (angl. *Smart Card*), DTD ir KOI-18, nesutrikdant įrenginio darbo (duomenų šifravimo);

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 – ne trumpesnis kaip 60 mėnesių;

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 darbus savo lėšomis, įskaitant transportavimo išlaidas.

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

Eil. Nr.	**Parametrai**	**Reikalavimai**
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 Perkančiosios organizacijos 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. Reglamentuota Forti OS versija.
3.	Korpuso tipas	„Desktop“ tipo arba montuojamas į 19“ komutacinę spintą. Įrenginio aukštis turi būti ne daugiau 1U. Pridedamas montavimo į 19" komutacinę spintą komplektas.

Eil. Nr.	Parametrai	Reikalavimai
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 valdymo 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.
10.	Bendro pobūdžio ugniasienės funkcijos	• Veiklos tipas - NAT, PAT, Transparent (Bridge); • “Policy-Based NAT” funkcionalumas; • “VLAN Tagging (802.1Q)” funkcionalumas arba lygiavertis standartas; • 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 arba lygiaverčius šifravimo 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.

Eil. Nr.	Parametrai	Reikalavimai
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 šifruotus 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
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.
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.

Eil. Nr.	Parametrai	Reikalavimai
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 mėn. garantinis aptarnavimas bei atnaujinimų teikimas garantiniu laikotarpiu (virusų, piktybinių programų, įsilaužimų aprašų,). 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. Turi būti galimybė pratęsti garantinio aptarnavimo laikotarpį iki ne mažiau 60 mėn.
25.	Sertifikatai	Turi turėti CE, FCC ir UL arba lygiaverčius sertifikatus.

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

Eil. Nr.	Parametrai	Reikalavimai
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 Perkančiosios organizacijos 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. 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. Reglamentuota FORTI OS versija.
3.	Korpuso tipas	„Desktop“ tipo arba montuojamas į 19“ komutacinę spintą. Įrenginio aukštis turi būti ne daugiau 1U. Pridedamas montavimo į 19" komutacinę spintą komplektas

Eil. Nr.	Parametrai	Reikalavimai
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 valdymo 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.
10.	Bendro pobūdžio ugniasienės funkcijos	• Veiklos tipas - NAT, PAT, Transparent (Bridge); • “Policy-Based NAT” funkcionalumas; • “VLAN Tagging (802.1Q)” funkcionalumas arba lygiavertis standartas; • 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 arba lygiaverčius šifravimo 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.

Eil. Nr.	Parametrai	Reikalavimai
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 šifruotus 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
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.
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
24.	Garantija	Gamintojo garantuojamas 60 mėn. garantinis aptarnavimas bei atnaujinimų teikimas garantiniu laikotarpiu (virusų, piktybinių programų, įsilaužimų aprašų). 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. Turi būti galimybė pratęsti garantinio aptarnavimo laikotarpį iki ne mažiau 60 mėn.
25.	Sertifikatai	Turi turėti CE, FCC ir UL arba lygiaverčius sertifikatus.

IV pirkimo dalis: *VoIP telefono aparatas, TEMPEST A – 10 vnt.*

Reikalavimai
1.1. VoIP telefono aparatas bus naudojamas Cisco technologijomis paremtame ir Perkančiosios organizacijos valdomame tinkle; 1.2. VoIP telefono aparatas privalo turėti: 1.2.1. viso formato skaitmenų klaviatūrą (0-9, #, *); 1.2.2. ne mažiau kaip 4 programuojamus funkcijų mygtukus; 1.2.3. ne mažiau kaip 5 programuojamus linijų mygtukus; 1.2.4. meniu valdymo mygtukus, leidžiančius keisti telefono nustatymus, peržiūrėti praleistus/gautus/iškviestus bei rinktus numerius, pasiekti balso paštą; 1.2.5. garso reguliavimo mygtuką leidžiantis nustatyti pokalbio bei skambučio garsumą; 1.2.6. integruotą ne mažesnį kaip 5 colių (12,7 cm) spalvinį ekraną. Rezoliucija ne mažesnė kaip 800 x 480 taškų. Ekrane turi būti rodomas skambinančiojo pavadinimas (numeris) ir renkamas numeris; 1.2.7. ragelį, spalvotą ekraną, integruotą vaizdo kamerą; 1.2.8. garsiakalbį (angl. speaker) ir mikrofoną (angl. microphone), bei veikiantį „laisvų rankų“ (angl. Hands-free) funkcionalumą. 1.3. Maitinimas: maitinimo šaltinis gali būti vidinis (integruotas) ir užtikrinantis TEMPEST filtravimą. Turi būti pateikti elektros maitinimo kabeliai VoIP telefono prijungimui prie nepertraukiamo maitinimo šaltinio (angl. UPS) ir tiesiogiai prie elektros maitinimo tinklo (230 V, 50 Hz). 1.4. Reikalavimai kodeksams: 1.4.1. privalo palaikyti balso kodeksus: G.711a, G.711, G.722, G.729a; 1.4.2. privalo palaikyti vaizdo kodeksą: H.264/AVC. 1.5. Vaizdo kamera: ne prastesnės kokybės kaip 720p HD. 1.6. Garso kokybė: ne prastesnė kaip plačiajuostė (angl. Wideband). 1.7. Prijungimas prie tinklo: 1.7.1. VoIP telefono aparatas turi būti jungiamas prie duomenų ir balso perdavimo tinklo per daugiamodes (angl. multimode) dvigubas (angl. duplex) LC 1000BaseSX tipo optines jungtis; 1.7.2. telefone turi būti integruotas ne lėtesnis kaip Gigabit Ethernet komutatorius, palaikantis

802.1Q VLAN žymėjimą ir turintis ne mažiau kaip 2 (du) 1000BaseSX daugiamodžius (angl. multimode) dvigubus (angl. duplex) LC tipo prievadus (VoIP telefono ir kompiuterio prijungimui prie duomenų ir balso perdavimo tinklo).

1.8. Palaikomi tinklo protokolai:

1.8.1. Session Initiation Protocol (SIP);

1.8.2. Session Description Protocol (SDP);

1.8.3. IPv4 ir IPv6;

1.8.4. User Datagram Protocol (UDP);

1.8.5. Dynamic Host Configuration Protocol (DHCP);

1.8.6. Gratuitous Address Resolution Protocol (GARP);

1.8.7. Domain Name System (DNS);

1.8.8. Trivial File Transfer Protocol (TFTP);

1.8.9. Secure Hypertext Transfer Protocol (HTTPS);

1.8.10. VLAN;

1.8.11. Real-Time Transport Protocol (RTP);

1.8.12. Real-Time Control Protocol (RTCP);

1.8.13. Cisco Peer-to-Peer Distribution Protocol (PPDP);

1.8.14. Cisco Discovery Protocol (CDP);

1.8.15. LLDP (including LLDP-MED).

1.9. Eksploatacijos temperatūra ir santykinė drėgmė:

1.9.1. eksploatacijos temperatūra turi būti ne mažesniame diapazone kaip nuo +5°C iki +40°C;

1.9.2. eksploatacijos santykinė drėgmė ne mažesniame diapazone kaip nuo 20 iki 90 proc. be kondensacijos.

1.10. Sandėliavimo temperatūra: ne mažesniame diapazone kaip nuo -10°C iki 60°C.

1.11. Priedai:

1.11.1. privalo būti pateikti, ne mažiau kaip 1 vnt. daugiamodis (angl. multimode) optinis komutacinis (angl. patch) kabelis su dvigubomis (angl. duplex) LC jungtimis viename gale ir SC jungtimis kitame gale. Optinio kabelio ilgis 1 m. Optinio kabelio klasė (angl. optical mode): ne prastesnė kaip OM3;

1.11.2. privalo būti pateiktas, ne mažiau kaip 1 vnt. daugiamodis (angl. multimode) optinis komutacinis (angl. patch) kabelis su dvigubomis (angl. duplex) LC jungtimis viename gale ir SC jungtimis kitame gale. Optinio kabelio ilgis 3 m. Optinio kabelio klasė (angl. optical mode): ne prastesnė kaip OM3.

1.12. Meniu kalbos pasirinkimas: turi turėti galimybę pasirinkti meniu lietuvių ir anglų kalbomis.

1.13. Naudojimo instrukcija: turi būti pateikta naudojimo instrukcija lietuvių arba anglų kalba.

1.14. Apsauga nuo informatyvaus elektromagnetinio spinduliavimo (angl. TEMPEST):

1.14.1. Tiekėjas privalo pateikti laboratorijos, kurioje atliekami TEMPEST įrangos matavimai, akreditacijos (patvirtinimo) pažymėjimą. Laboratorija privalo būti akredituota (patvirtinta) NATO šalies nacionalinės saugumo agentūros funkcijas atliekančios įstaigos ar jos įgaliotos įstaigos;

1.14.2. visa siūloma TEMPEST įranga privalo būti identifikuota, t. y. jai privalo būti suteiktas pavadinimas ir internete ar pateiktuose dokumentuose privalo būti pateikta įrangos specifikacija ir informacija, kad ši įranga atitinka aktualios redakcijos NATO SDIP 27 A lygio (angl. Level A) keliamus reikalavimus;

1.14.3. Pirkėjas, perkantis TEMPEST įrangą, prieš pasirašant pirkimo sutartį (arba ją įsigijęs) gali patikrinti, ar šios įrangos tiekėjo pateikta sertifikuota TEMPEST įranga atitinka deklaruojamą

apsaugos nuo TEMPEST lygį/zoną sertifikuotoje TEMPEST laboratorijoje. Tokiu atveju TEMPEST laboratorijai bus perduoti įrangos pavyzdžiai bei atlikti kontroliniai matavimai. Paaiškėjus, kad įranga neatitinka aktualios redakcijos, pasiūlymo pateikimo metu, NATO SDIP-27 A lygio reikalavimų, tai būtų traktuojama kaip reikalavimų neatitikimas ir sutarties sąlygų nesilaikymas. Tokiu atveju įranga grąžinama Tiekėjui arba keičiama nauja lygiaverte aktualios redakcijos NATO SDIP-27 A lygio reikalavimus atitinkančia įranga.

1.15. Licencijos:

1.15.1. į siūlomos įrangos kainą turi būti įtrauktos visos licencijas, programinis bei aparatinis (angl. software, hardware) aprūpinimas, įrangos veikimui užtikrinti. Įrangos funkcionavimui ir reikalaujamiems funkcionalumams užtikrinti reikalingos licencijos turi būti suteikiamos neribotam laikui;

1.15.2. turi būti pateiktos licencijos reikalingos telefono aparatui naudoti su skambučių valdymo programine įranga Cisco Unified Communications Manager naujausia versija;

1.15.3. jei gamintojas nenumato neriboto laikotarpio, tuomet licencijos, programinis bei aparatinis aprūpinimas turi būti suteiktas ne mažesniam kaip 60 mėn. laikotarpiui.

1.16. Tiekiamai įrangai turi būti suteikta ne mažiau kaip 60 mėn. gamintojo garantija.

1.17. Visos reikalingos licencijos turi būti patalpintos wan@mil.lt paskyroje.