

TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS

- 1.1. Dubliuotų ugniasienių įranga;
- 1.2. Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti to paties gamintojo tinklo saugumo įrangą;
- 1.3. Specializuotas vieno gamintojo programinis sprendimas, skirtas kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas;
- 1.4. Dubliuotų ugniasienių įrangos, specializuoto programinio sprendimo skirta valdyti to paties gamintojo tinklo saugumo įrangą bei specializuoto programinio sprendimo, skirta kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas techninės priežiūros (angl. Technical support) ir saugumo prenumeruojamų paslaugų (angl. Security subscription services) palaikymai;
- 1.5. Dubliuotų ugniasienių įrangos, specializuoto programinio sprendimo skirta valdyti to paties gamintojo tinklo saugumo įrangą bei specializuoto programinio sprendimo, skirta kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas konfigūravimo paslaugos

2. PIRKIMO OBJEKTO APIMTYS

- 2.1. Dubliuotų ugniasienių įranga - vnt.;
- 2.2. Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti to paties gamintojo tinklo saugumo įrangą - 1 vnt.;
- 2.3. Specializuotas vieno gamintojo programinis sprendimas, skirtas kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas 1 vnt.;
- 2.4. Priežiūros (angl. Technical support) ir saugumo prenumeruojamų paslaugų (angl. Security subscription services) palaikymai ne trumpiau kaip 36 mėn.;
- 2.5. Konfigūravimo paslaugos – 50 val. Nurodytas valandų kiekis yra maksimalus. Perkantysis subjektas neįsipareigoja išpirkti viso valandų kiekio. Konfigūravimo paslaugos bus perkamos pagal poreikį.
- 2.6. Ofiso ugniasienė – 1 vnt.;
- 2.7. Visos įrangos administravimo, valdymo teisės turi būti perduotos užsakovui, visa įranga, sprendimas turi būti pilnai valdomas tik pačios UAB Energy cells įmonės, kuri esant reikalui galės suteikti prieigas trečiosioms šalims ir jas panaikinti bet kuriuo metu. Taip pat visi įsigyti produktai turi būti tik nauji ir pas gamintoją turi būti registruoti UAB Energy cells įmonės vardu.

3. SUTARTINIŲ ĮSIPAREIGOJIMŲ VYKDYMO VIETA

UAB Energy cells, Ozo g. 12A-1, Vilnius.

4. REIKALAVIMAI PIRKIMO OBJEKTUI

4.1. Esamos situacijos aprašymas

Užsakovo infrastruktūroje yra naudojamos Fortinet gamintojo ugniasienės. Užsakovo valdoma IT infrastruktūra buvo įtraukta į YSII (Ypatingos Svarbos Infrastruktūros Sąrašą) todėl Užsakovas, siekdamas atitikti keliamus reikalavimus, keis dalį turimos tinklo įrangos.

4.2. Pirkimo objekto aprašymas

- 4.2.1. Dubliuotų ugniasienių įranga;

Eil. Nr.	Aprašymas	Reikalavimai
1.	Modelis, gamintojas: Nurodyti gamintoją, modelį, versiją, prekės numerį. (Nurodo Tiekėjas) Turi būti pateikti visų siūlomos įrangos komplektuojančių dalių gamintojo produktų kodai, trumpi aprašymai bei nurodyti komplektuojančių dalių kiekiai. – (Nurodo Tiekėjas)	Būtina
2.	Specializuotas vieno gamintojo aparatinis – programinis sprendimas (angl. appliance).	Būtina
Konstrukcija		
3.	Konstrukcija: Montuojamas į 19 ^o komutacinę spintą. Turi būti pateikiamas su visais reikalingais montavimui į 19 colių komutacinę spintą priedais	Būtina
4.	Sprendimą turi sudaryti du, vienas kitą dubliuojantys įrenginiai.	Būtina
5.	Įrangos elektros maitinimas tiekiamas iš AC 230V 50Hz tinklo. Privalo turėti du maitinimo šaltinius, užtikrinančius nepertraukiamą įrenginio veikimą sugedus vienam iš maitinimo šaltinių.	Būtina
6.	Nemažiau kaip 8 vnt. 1000 Base-TX Ethernet prievadai.	Būtina
7.	Nemažiau 4 vnt. 10 G SFP+ prievadų.	Būtina
8.	Nemažiau 8 vnt. 1 G SFP prievadų.	Būtina
9.	Ne mažiau kaip 1 vnt. 1000 Base-TX Ethernet prievadas įrangos valdymui per komandinę eilutę.	Būtina
10.	Ne mažiau kaip 1 vnt. 1000 Base-TX Ethernet prievadas įrangos aukšto patikimumo funkcijai užtikrinti.	Būtina
11.	Įranga turi būti pateikta su visomis įrangos diegimui reikalingomis medžiagomis/detalėmis.	Būtina
Įrangos funkcijos		
12.	Turi būti ne mažiau kaip 1500 IPsec VPN tunelių palaikymas įrenginys-įrenginys (Gateway-to-Gateway)	Būtina
13.	Turi būti galimybė vienam iš HA įrenginių pakeisti HA statusą (padaryti aktyviu arba pasyviu klasterio elementu)	Būtina
14.	Turi būti galimybė atlikti programinės įrangos atnaujinimą, nesutrikdant ugniasienės, veikiančios HA režimu, duomenų perdavimo.	Būtina
15.	Turi palaikyti IPsec arba lygiaverčių standartų palaikymas;	Būtina
16.	Turi būti ne mažiau kaip 15 000 IPsec vidinio tinklo vartotojų skaičius	Būtina

17.	Turi būti ne mažiau kaip 2 500 000 sesijų vienu metu ir nemažiau kaip 100 000 naujų sesijų per sek.	Būtina
18.	Turi būti ne mažiau kaip 300 000 dešifruotų sesijų vienu metu.	Būtina
19.	Ugniasienės pralaidumas su IPS saugumo funkcionalumu turi būti ne mažesnis kaip 5,0 Gbps (imix paketais);	Būtina
20.	Ugniasienės pralaidumas su saugumo funkcionalumu (IPS, Antivirus, malware apsauga) vienu metu turi būti ne mažesnis kaip 2,5 Gbps;	Būtina
21.	Turi būti ne mažiau kaip 5 000 saugumo taisyklių (angl. Security policy);	Būtina
22.	Turi būti galima padalinti į ne mažiau kaip 3 virtualias sistemas (virtualios ugniasienės). Turi būti pateiktos visos reikalingos licencijos.	Būtina
23.	IPv6 palaikymas.	Būtina
24.	DES, 3DES, ir AES256 šifravimas.	Būtina
25.	Turi būti IKE sertifikato palaikymas (X.509);	Būtina
26.	Apsauga nuo DoS tipo atakų. (Turi būti apsauga nuo įsilaužimų, jų aptikimas ir prevencija (TCP Syn Flood, Land, Ping of Death, ir kt.);	Būtina
27.	Apsauga nuo Malware, Spyware ir bandymų įsilaužti ar kitaip išnaudoti sistemą (angl. IPS/IDS) bei Antivirusinė sistema	Būtina
28.	<p>WEB puslapių kategorizavimas ir valdymas:</p> <ol style="list-style-type: none"> 1. Galimybė administratoriui aprašyti WEB filtravimą pagal URL 2. Turi būti galimybė URL filtravimui ir kategorizavimui pagal pilną URL, t.y. tikrinama URL host ir URI dalys. 3. Kategorizuotų WEB puslapių duomenų bazė 4. Galimybė laikinai suteikti naudotojui prieigą prie uždraustos WEB kategorijos 	Būtina
29.	Turi palaikyti SSL šifruoto srauto inspekciją įrenginyje atitinkamai įkeliant reikiamus sertifikatus.	Būtina
30.	Tinklo srautas turi būti tikrinamas ir analizuojamas realiu laiku.	Būtina
31.	Turi skenuoti HTTP/ SMTP/ POP3/ IMAP/ FTP ir tikrinti duomenų srautą nuo virusų.	Būtina
32.	Turi blokuoti bylas pagal bylos dydį ir tipą.	Būtina
33.	Turi atpažinti ne mažiau kaip 3000 aplikacijų, įskaitant Youtube, Gmail, Twiter, Facebook, web paštus aplikacijų kontrolės funkcija (atpažinimas, blokavimas (angl. Application Control).	Būtina
34.	Turi gebėti dirbti kaip DHCP klientas, DHCP serveris ir atlikti IP adreso pririšimus prie MAC	Būtina

35.	Maršrutizavimas pagal taisykles (angl. Policy-Based Routing) (maršrutizavimas pagal sekančius kriterijus: protokolą, IP adresus, porto numerius)	Būtina
36.	Dinaminis maršrutizavimas (RIP v2, OSPF, BGP) kiekvienoje virtualioje ugniasienėje atskirai	Būtina
37.	IPv6 maršrutizavimas.	Būtina
38.	Turi būti srauto ribojimo funkcionalumas DSCP ir (angl. Traffic shaping), nurodant garantuotą bei maksimalų duomenų srauto dydį naudojant saugumo/srauto taisykles;	Būtina
39.	Turi būti įsibrovimų kaupimas ir raportavimas: Prekės laikinojoje atmintyje, SysLog serveryje, pranešimas el. paštu;	Būtina
40.	Turi palaikyti prievadų loginį grupavimą pagal IEEE 802.3ad ar lygiavertį standartą	Būtina
41.	Įrenginys turi skaidriai nustatyti vartotojų tapatybę (naudojantis Microsoft AD)	Būtina
42.	Saugumo taisyklių kūrimas naudojant vartotojus (USER-ID) bei jų grupes, o ne tik IP adresus	Būtina
43.	Turi gebėti dirbti skaidriame režime (angl.transparent) ir maršrutizavimo režime (angl. routed) skirtingose virtualiose ugniasienėse vienu metu;	Būtina
44.	Gebėti atlikti taisyklėmis paremtą adresų transliavimą (angl.„policy-based NAT“).	Būtina
45.	Turi būti IEEE 802.1Q VLAN palaikymas.	Būtina
46.	Vartotojų grupių autentifikavimas naudojant: <ul style="list-style-type: none"> - LDAP - RADIUS arba TACACS+ 	Būtina
47.	Automatinis įsilaužimų aprašų (angl. signature) duomenų bazės atnaujinimas	Būtina
48.	Saugumo taisyklių apjungimas į saugumo zonas kiekvienoje virtualioje ugniasienėje atskirai	Būtina
49.	Turi būti galimybė įrenginį valdyti per terminalą, SSH, HTTPS, iš centrinės valdymo tarnybinės stoties.	Būtina
50.	Turi būti skirtingų lygių administravimo rolės.	Būtina
51.	Vidinis įvykių žurnalas.	Būtina
52.	Įvykių persiuntimas į nutolusį Syslog ar lygiavertį serverį.	Būtina
53.	Turi palaikyti SNMP v2c arba lygiavertį.	Būtina
54.	Turi būti galima stebėti, riboti, blokuoti aplikacijas.	Būtina
55.	Įrenginys turi generuoti ataskaitas apie tinkle naudojamą programas.	Būtina
56.	Įrenginys turi generuoti ataskaitas apie vartotojo naudojamą programas, prie kokių žiniatinklio puslapių vartotojas jungiasi, vartotojo perduodamus duomenų kiekius.	Būtina

57.	Įrenginys turi generuoti ataskaitas apie aptiktas grėsmes.	Būtina
58.	Turi rodyti geografinį grėsmių atvaizdavimą.	Būtina
Garantija		
59.	<p>Įrenginys turi būti pateikiamas su gamintojo garantija 36 mėnesių (nuo sistemos pateikimo priėmimo-perdavimo akto pasirašymo dienos) ir visom reikalingoms licencijoms šiam periodui. Turi būti gaunami reguliarūs virusų, įsilaužimo aprašai, WEB kategorijos ir jų atnaujinimai. Teikiamas gamintojo palaikymas 24x7 formatu.</p> <p>Garantiniu laikotarpiu turi būti teikiamas nemokamas programinės įrangos klaidų šalinimas. Turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisiuntimas iš gamintojo puslapio;</p>	Būtina

4.2.2. Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti to paties gamintojo tinklo saugumo įrangą;

Eil. Nr.	Aprašymas	Reikalavimai
1.	<p>Modelis, gamintojas: Nurodyti gamintoją, modelį, versiją, prekės numerį. (Nurodo Tiekėjas)</p> <p>Turi būti pateikti visų siūlomos įrangos komplektuojančių dalių gamintojo produktų kodai, trumpi aprašymai bei nurodyti komplektuojančių dalių kiekiai. – (Nurodo Tiekėjas)</p>	Būtina
2.	Specializuotas vieno gamintojo programinis sprendimas, skirtas kaupti įvykių pranešimus iš FortiGate ugniasienių sistemų, juos analizuoti, koreliuoti bei generuoti ataskaitas.	Būtina
3.	Įvykių kaupimo serverio programinė įranga turi veikti virtualizuotoje aplinkoje VMware ESX/ESXi 6.7+, Microsoft Hyper-V 2012 2016, Open Source Xen 4.2+, KVM.	Būtina
4.	<p>Tarnybinės stoties minimalūs parametrai, su kuriais gali veikti centralizuoto valdymo serveris :</p> <ul style="list-style-type: none"> • 16 GB RAM • 4 vCPU • 500GB HDD <p>Neturi būti ribojamas maksimalus RAM, vCPU kiekis.</p>	Būtina
5.	Centralizuota įvykių kaupimo ir apdorojimo sistema turi pilnai integruotis su turimomis FortiGate ugniasienėmis. Integracija turi užtikrinti, kad įvykių kaupimo įrenginys apsijungia į saugumo fabriko sistemą.	Būtina
Reikalavimai programinei įrangai		

6.	Įranga turi būti pateikta su licencija, leidžiančia kaupti įvykių pranešimus iš ne mažiau kaip 5 000 įrenginių. Turi leisti surinkti ne mažiau kaip 5 GB įvykių pranešimų per dieną. Turi leisti saugoti ne mažiau kaip 500GB istorinių įvykių pranešimų.	Būtina
7.	Turi būti galimybė ateityje padidinti surenkamų įvykių pranešimo kiekį iki 20 GB per dieną ir saugoti ne mažiau kaip 10 TB istorinių įvykių pranešimų. Praplėtimo funkcionalumas gali būti realizuotas įsigyjant papildomas licencijas.	Būtina
8.	Įrenginys turi surinkti, analizuoti, koreliuoti įvykių pranešimus.	Būtina
9.	Įrenginys turi generuoti ataskaitas.	Būtina
10.	Turi būti galimybė atlikti paiešką tarp įvykių pranešimų.	Būtina
11.	Turi atvaizduoti įvykius realiu laiku bei istorinius įvykius.	Būtina
12.	Turi būti ne mažiau kaip 20 paruoštų skirtingų ataskaitų šablonų.	Būtina
13.	Turi būti galimybė sukurti savo ataskaitų šablonus.	Būtina
14.	Turi būti galimybė generuoti ataskaitas numatytu laiku.	Būtina
15.	Ataskaitos turi būti pateikiamos PDF, HTML, CSV, XML formatais.	Būtina
16.	Turi būti galimybė persiųsti visus sukaupytus įvykių pranešimus į kitą įvykių pranešimo kaupimo stotį CEF formatu.	Būtina
17.	Turi būti galimybė sukurti skirtingas aplinkas taip logiškai atskirti įrenginius į skirtingas grupes, leisti administratoriams prieiti tik prie tam tikrų įrenginių grupių.	Būtina
18.	Prisijungimas prie centrinio įvykių kaupimo serverio turi būti vykdomas SSH, HTTPS protokolais.	Būtina
19.	Įrenginys analizuodamas gautus įvykius turi nustatyti kiekvieno galinio įrenginio grėsmės lygį pateikdamas jo IP adresą, naudojamą OS.	Būtina
20.	Turi būti galimybė aktyvuoti saugų/kriptuotą duomenų apsikeitimą tarp įvykių kaupimo stoties ir įrenginių.	Būtina
21.	Turi būti užtikrinta, kad administratorius gali matyti ir valdyti tik jam priskirtus įrenginius.	Būtina
22.	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba.	Būtina
23.	Turi būti galimybė kurti roles.	Būtina
24.	Galimybė administratorių tapatybės nustatymui naudoti vienkartinių slaptažodžių generatorius.	Būtina
25.	Administratorių tapatybės nustatymas turi būti atliekamas lokaliai arba per RADIUS, LDAP, TACACS+.	Būtina
26.	Įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas.	Būtina

27.	Turi būti galimybė įvykių žurnalų paiešką vykdyti per įmonės naudojamą FortiGate ugniasienių grafinę sąsają (GUI).	Būtina
Garantija		
28.	Programinė įranga turi būti pateikta su 36 mėnesių 24x7 garantija, kuri suteikia teisę garantijos metu gauti programinės įrangos naujas versijas atnaujinimus ir pataisymus.	Būtina
29.	Pasibaigus garantiniam laikotarpiui (36 mėn.) programinė įranga turibūti atnaujinta, už tolimesni licencijų atnaujinimą po 36 mėn. laikotarpio atsakingas Užsakovas.	Būtina

4.2.3. Specializuotas vieno gamintojo programinis sprendimas, skirtas kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas.

Eil. Nr.	Aprašymas	Reikalavimai
1.	Modelis, gamintojas: Nurodyti gamintoją, modelį, versiją, prekės numerį. (Nurodo Tiekėjas) Turi būti pateikti visų siūlomos įrangos komplektuojančių dalių gamintojo produktų kodai, trumpi aprašymai bei nurodyti komplektuojančių dalių kiekiai. – (Nurodo Tiekėjas)	Būtina
2.	Specializuotas vieno gamintojo programinis sprendimas, skirtas valdyti to paties gamintojo tinklo saugumo įrangą.	Būtina
3.	Centrinio valdymo serverio programinė įranga turi veikti virtualizuotoje aplinkoje VMware ESX/ESXi 6.5+, Microsoft Hyper-V 2012 2016, KVM.	Būtina
4.	Tarnybinės stoties minimalūs parametrai, su kuriais gali veikti centralizuoto valdymo serveris : <ul style="list-style-type: none"> • 16 GB RAM • 4 vCPU • 500 GB HDD 	Būtina
5.	Ugniasienių centrinio valdymo programinė įranga turi sugebėti integruotis su kitais konkurso sąlygose minimais įrenginiais.	Būtina
Reikalavimai programinei įrangai		
6.	Įranga turi būti pateikta su licencija, leidžiančia valdyti ne mažiau kaip 10 įrenginių (fizinis ir virtualius).	Būtina
7.	Centrinio valdymo serverio pagalba turi būti galimybė atlikti šias funkcijas: centralizuotas įrenginių konfigūracijų valdymas, centralizuotas valdomų įrenginių statistikos kaupimas.	Būtina
8.	Prisijungimas prie centrinio valdymo serverio turi būti vykdomas SSH, HTTPS protokolais, JSON API valdymo komandomis.	Būtina

9.	Duomenų apsikeitimas tarp centrinio valdymo serverio ir valdomų įrenginių turi būti šifruojamas.	Būtina
10.	Turi būti galimybė jungti valdomus įrenginius į skirtingas grupes.	Būtina
11.	Turi būti galimybė skirtingos įrenginių (fizinių ir virtualių) grupėms priskirti atskirus administratorius.	Būtina
12.	Turi būti užtikrinta, kad administratorius gali matyti ir valdyti tik jam priskirtus įrenginius.	Būtina
13.	Turi būti galimybė kurti bendrus objektus ir saugumo taisykles, kurios yra naudojamos keliems įrenginiams.	Būtina
14.	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba.	Būtina
15.	Turi būti galimybė kurti roles.	Būtina
16.	Turi būti galimybė bent 10-ies administratorių tapatybės nustatymui naudoti vienkartinį slaptažodžių generatorius. Licencijos turi būti įtrauktos į pasiūlymą.	Būtina
17.	Administratorių tapatybės nustatymas turi būti atliekamas lokaliai arba per RADIUS, LDAP, TACACS+.	Būtina
18.	Įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai, laikas kada buvo atliktas veiksmas.	Būtina
19.	Perkančiajai organizacijai ateityje įsigijus antrą tokią pat sistemą turi būti galimybė apjungti dvi tokias pats centralizuotas valdymo sistemas į aukšto patikimumo sistemą. Aukšto patikimumo sistema turi dirbti Aktyvus/Pasyvus režimu.	Būtina
20.	Turi būti galimybė iš centrinio valdymo serverio išeksportuoti valdymo serverio ir valdymo serverio valdomų įrenginių taisykles.	Būtina
21.	Turi būti galimybė valdomiems įrenginiams centralizuotai įdiegti dinaminis atnaujinimus (antivirus, IPS, pažeidžiamumų aprašai) iš lokaliai saugomos duomenų bazės.	Būtina
Garantija		
22.	Programinė įranga turi būti pateikta su 36 mėnesių 24x7 garantija, kuri suteikia teisę garantijos metu gauti programinės įrangos naujas versijas atnaujinimus ir pataisymus.	Būtina
23.	Pasibaigus garantiniam laikotarpiui programinė įranga turi ir toliau leisti pilnai valdyti to paties gamintojo tinklo įrangą, už tolimesni licencijų atnaujinimą po 36 mėn. laikotarpio atsakingas Užsakovas.	Būtina

4.2.4. Dubliuotų ugniasienių įrangos, specializuoto programinio sprendimo skirta valdyti to paties gamintojo tinklo saugumo įrangą bei specializuoto programinio sprendimo, skirta kaupti įvykių pranešimus iš to paties gamintojo tinklo saugumo įrangos, juos analizuoti, koreliuoti bei generuoti ataskaitas techninės priežiūros (angl. Technical support) ir saugumo prenumeruojamų paslaugų (angl. Security subscription services) palaikymai.

Nr.	Specifikacija	Reikalavimai
1.	Garantiniai įsipareigojimai, techninis aptarnavimas.	<p>Gamintojo garantuojamas įrangos garantinis aptarnavimas. Sekančia dieną siunčiama gamintojui, gamintojas per 3 dienas išsiunčia atgal suremontuotą arba pakeistą.</p> <p>Saugumo paslaugų atnaujinimų teikimas garantiniu laikotarpiu. Paslaugos tipas: Application Control, IPS, Advanced Malware Protection, Web & Video Filtering, Antispam Service, and FortiCare Premium</p> <p>Teisė kreiptis į gamintoją iškilus problemai (paslaugos užtikrinimo tipas ne blogesnis kaip 8x5) internetu, elektroniniu paštu ar telefonu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.</p> <p>Garantinė priežiūra turi būti atliekama kreipiantis į įrangos gamintoją tiesiogiai arba per gamintojo autorizuotą partnerį (angl. Authorized reseller).</p> <p>Tiekėjas turi pateikti nuorodą į gamintojo internetinę prieigą, kuri įgalina naudojant produkto serijinį numerį patikrinti suteiktą gamintojo garantiją internetiniame puslapyje.</p>

4.2.5. Konfigūravimo paslaugos

Tiekėjas numatytooms Paslaugų funkcijoms teikti turi turėti reikiamus kvalifikuotus ir atestuotus specialistus bei turi būti numatęs ir į Paslaugų suteikimo kaštus įskaičiavęs visas reikiamas sąnaudas kokybiškam Paslaugų suteikimui.

Tiekėjas privalo pats aprūpinti savo specialistus visa sutartiniams įsipareigojimams įvykdyti reikalinga įranga, transportu ir bet kokiomis kitomis priemonėmis, reikalingomis kokybiškai Paslaugoms atlikti.

Paslaugas teikia Tiekėjo specialistai atitinkantys Sutarties kvalifikacinius reikalavimus ir turintys paslaugoms teikti reikiamus sertifikatus.

Paslaugų užsakymų vykdymas galimas nuotoliniu būdu naudojant Perkančiojo subjekto suteiktą prieigą, arba atvykstant į įrangos instaliavimo vietą.

4.2.6. Ofiso ugniasienė

Eil. Nr.	Aprašymas	Reikalavimai
1.	<p>Modelis, gamintojas: Nurodyti gamintoją, modelį, versiją, prekės numerį. (Nurodo Tiekėjas)</p> <p>Turi būti pateikti visų siūlomos įrangos komplektuojančių dalių gamintojo produktų kodai, trumpi aprašymai bei nurodyti komplektuojančių dalių kiekiai. – (Nurodo Tiekėjas)</p>	Būtina
2.	Specializuotas vieno gamintojo aparatinis – programinis sprendimas (angl. appliance).	Būtina
Konstrukcija		
3.	Konstrukcija: Montuojamas į 19 ^o komutacinę spintą. Turi būti pateikiamas su visais reikalingais montavimui į 19 colių komutacinę spintą priedais	Būtina

4.	Įrangos elektros maitinimas tiekiamas iš AC 230V 50Hz tinklo. Privalo turėti du maitinimo šaltinius, užtikrinančius nepertraukiamą įrenginio veikimą sugedus vienam iš maitinimo šaltinių.	Būtina
5.	Nemažiau kaip 5 vnt. 1000 Base-TX Ethernet prievadai.	Būtina
6.	Ne mažiau kaip 1 vnt. 1000 Base-TX Ethernet prievadas įrangos valdymui per komandinę eilutę.	Būtina
7.	Įranga turi būti pateikta su visomis Įrangos diegimui reikalingomis medžiagomis/detalėmis.	Būtina
Įrangos funkcijos		
8.	Turi būti ne mažiau kaip 200 IPsec VPN tunelių palaikymas įrenginys-įrenginys (Gateway-to-Gateway)	Būtina
9.	Turi palaikyti IPsec arba lygiaverčių standartų palaikymas;	Būtina
10.	Turi būti ne mažiau kaip 500 IPsec vidinio tinklo vartotojų skaičius	Būtina
11.	Turi būti ne mažiau kaip 700 000 sesijų vienu metu ir nemažiau kaip 35 000 naujų sesijų per sek.	Būtina
12.	Turi būti ne mažiau kaip 55 000 dešifruotų sesijų vienu metu.	Būtina
13.	Ugniasienės pralaidumas su IPS saugumo funkcionalumu turi būti ne mažesnis kaip 1,4 Gbps (imix paketais);	Būtina
14.	Ugniasienės pralaidumas su saugumo funkcionalumu (IPS, Antivirus, malware apsauga) vienu metu turi būti ne mažesnis kaip 700 Mbps;	Būtina
15.	Turi būti ne mažiau kaip 700 saugumo taisyklių (angl. Security policy);	Būtina
16.	Turi būti galima padalinti į ne mažiau kaip 3 virtualias sistemas (virtualios ugniasienės). Turi būti pateiktos visos reikalingos licencijos.	Būtina
17.	IPv6 palaikymas.	Būtina
18.	DES, 3DES, ir AES256 šifravimas.	Būtina
19.	Turi būti IKE sertifikato palaikymas (X.509);	Būtina
20.	Apsauga nuo DoS tipo atakų. (Turi būti apsauga nuo įsilaužimų, jų aptikimas ir prevencija (TCP Syn Flood, Land, Ping of Death, ir kt.);	Būtina
21.	Apsauga nuo Malware, Spyware ir bandymų įsilaužti ar kitaip išnaudoti sistemą (angl. IPS/IDS) bei Antivirusinė sistema	Būtina
22.	WEB puslapių kategorizavimas ir valdymas:	Būtina

	<ol style="list-style-type: none"> 1. Galimybė administratoriui aprašyti WEB filtravimą pagal URL 2. Turi būti galimybė URL filtravimui ir kategorizavimui pagal pilną URL, t.y. tikrinama URL host ir URI dalys. 3. Kategorizuotų WEB puslapių duomenų bazė 4. Galimybė laikinai suteikti naudotojui prieigą prie uždraustos WEB kategorijos 	
23.	Turi palaikyti SSL šifruoto srauto inspekciją įrenginyje atitinkamai įkeliant reikiamus sertifikatus.	Būtina
24.	Tinklo srautas turi būti tikrinamas ir analizuojamas realiu laiku.	Būtina
25.	Turi skenuoti HTTP/ SMTP/ POP3/ IMAP/ FTP ir tikrinti duomenų srautą nuo virusų.	Būtina
26.	Turi blokuoti bylas pagal bylos dydį ir tipą.	Būtina
27.	Turi gebėti dirbti kaip DHCP klientas, DHCP serveris ir atlikti IP adresą pririšimus prie MAC	Būtina
28.	Maršrutizavimas pagal taisykles (angl. Policy-Based Routing) (maršrutizavimas pagal sekančius kriterijus: protokolą, IP adresus, porto numerius)	Būtina
29.	Dinaminis maršrutizavimas (RIP v2, OSPF, BGP) kiekvienoje virtualioje ugniasienėje atskirai	Būtina
30.	IPv6 maršrutizavimas.	Būtina
31.	Turi būti srauto ribojimo funkcionalumas DSCP ir (angl. Traffic shaping), nurodant garantuotą bei maksimalų duomenų srauto dydį naudojant saugumo/srauto taisykles;	Būtina
32.	Turi būti įsibrovimų kaupimas ir raportavimas: Prekės laikinojoje atmintyje, SysLog serveryje, pranešimas el. paštu;	Būtina
33.	Turi palaikyti prievadų loginį grupavimą pagal IEEE 802.3ad ar lygiavertį standartą	Būtina
34.	Įrenginys turi skaidriai nustatyti vartotojų tapatybę (naudojantis Microsoft AD)	Būtina
35.	Saugumo taisyklių kūrimas naudojant vartotojus (USER-ID) bei jų grupes, o ne tik IP adresus	Būtina
36.	Turi gebėti dirbti skaidriame režime (angl.transparent) ir maršrutizavimo režime (angl. routed) skirtingose virtualiose ugniasienėse vienu metu;	Būtina
37.	Gebėti atlikti taisyklėmis paremtą adresų transliavimą (angl.„policy-based NAT“).	Būtina
38.	Turi būti IEEE 802.1Q VLAN palaikymas.	Būtina
39.	Vartotojų grupių autentifikavimas naudojant: <ul style="list-style-type: none"> - LDAP - RADIUS arba TACACS+ 	Būtina
40.	Automatinis įsilaužimų aprašų (angl. signature) duomenų bazės atnaujinimas	Būtina
41.	Saugumo taisyklių apjungimas į saugumo zonas kiekvienoje virtualioje ugniasienėje atskirai	Būtina

42.	Turi būti galimybę įrenginį valdyti per terminalą, SSH, HTTPS, iš centrinės valdymo tarnybinės stoties.	Būtina
43.	Turi būti skirtingų lygių administravimo rolės.	Būtina
44.	Vidinis įvykių žurnalas.	Būtina
45.	Įvykių persiuntimas į nutolusį Syslog ar lygiavertį serverį.	Būtina
46.	Turi palaikyti SNMP v2c arba lygiavertį.	Būtina
47.	Turi būti galima stebėti, riboti, blokuoti aplikacijas.	Būtina
48.	Įrenginys turi generuoti ataskaitas apie tinkle naudojamą programas.	Būtina
49.	Įrenginys turi generuoti ataskaitas apie vartotojo naudojamą programas, prie kokių žiniatinklio puslapių vartotojas jungiasi, vartotojo perduodamus duomenų kiekius.	Būtina
50.	Įrenginys turi generuoti ataskaitas apie aptiktas grėsmes.	Būtina
51.	Turi rodyti geografinį grėsmių atvaizdavimą.	Būtina
Garantija		
52.	Įrenginys turi būti pateikiamas su gamintojo garantija 36 mėnesių (nuo sistemos pateikimo priėmimo-perdavimo akto pasirašymo dienos) ir visom reikalingoms licencijoms šiam periodui. Turi būti gaunami reguliarūs virusų, įsilaužimo aprašai, WEB kategorijos ir jų atnaujinimai. Teikiamas gamintojo palaikymas 24x7 formatu. Garantiniu laikotarpiu turi būti teikiamas nemokamas programinės įrangos klaidų šalinimas. Turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsiuntimas iš gamintojo puslapiu;	Būtina

4.3. Sutartinių įsipareigojimų vykdymo tvarka ir terminai

4.3.1. Teikiant paslaugas, techninę ir programinę įrangą, turi būti vadovaujama Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu ir Nacionaliniu kibernetinių incidentų valdymo planu patvirtintu Lietuvos Respublikos Vyriausybės nutarimu 2018 m. rugpjūčio 13 d. Nr. 818.

4.3.2. Tiekėjas turi atitikti Užsakovo subjekto vidinius teisės aktus, tokius kaip „Minimalūs kibernetiniai saugumo reikalavimai“, tačiau atsižvelgiant į teisinį reglamentavimą dokumentų kiekis ar jų turinys gali kisti.

4.3.3 Įranga turi būti pristatyta ne vėliau kaip per 20 d.d. po sutarties pasirašymo.

4.3.4 Konfigūravimo paslaugos turi būti atliktos ne vėliau kaip per 20 d.d. po Užsakovo nurodymo vykdyti konfigūravimo darbus.

4.3.5 Prekės turi būti naujos, nenaudotos, neatnaujintos gamykliškai (angl. refurbished) ir neturi būti įtrauktos į gamintojo „End-Of-Sale“/„End-Of-Sale announcement“, „End-Of-Support“ sąrašus.

4.4. Sutarties vykdymo metu pateikiama dokumentacija

4.4.1. Atnaujinta Užsakovo kompiuterinio tinklo topologinė schema;

4.4.2. Sukonfigūruotos įrangos IP adresų ir atnaujintų Užsakovo tinklo įrenginių IP adresų sąrašai;

4.4.3. Pateikiami visų sukonfigūruotos įrangos vartotojų prisijungimo duomenys (vartotojų vardai ir slaptažodžiai).

4.4.4. Užsakovas siekia jog jo ir Tiekėjo veiksmai darytų kuo mažesnį poveikį aplinkai, todėl:

- 4.4.4.1. viešojo pirkimo ir sutarties vykdymo metu bendravimas tarp Tiekėjo ir Užsakovo bus vykdomas tik elektroninėmis priemonėmis (CVP IS priemonėmis, telefonu, elektroniniu paštu, ar kt.);
- 4.4.4.2. visa dokumentacija susijusi su Sutarties vykdymu teikiama Užsakovui ir Tiekėjui elektroninėmis priemonėmis (elektroniniu paštu ar kt.);
- 4.4.4.3. sutartis bus pasirašoma tik elektroninėmis priemonėmis (elektroniniu parašu);
- 4.4.4.4. tiekėjas įsipareigoja mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, jeigu bus naudojamos kanceliarinės prekės, jos turi būti pagamintos iš perdirbtų žaliavų arba tinkamos perdirbimui.
- 4.4.4.5. jei įsigyjama prekė turi būti tiekama ar perduodama antrinėje pakuotėje, ji turi atitikti pakuotėms nustatytus minimalius aplinkos apsaugos kriterijus, nebent tai prieštarauja higienos normoms: pakuotės turi būti laikytinos perdirbamosiomis pakuotėmis pagal Lietuvos Respublikos mokesčio už aplinkos teršimą įstatymo nuostatas.

5. PASIŪLYMŲ VERTINIMO BŪDAS

Ekonomiškai naudingiausio pasiūlymo vertinimo kriterijus:

- Kaina
- Sąnaudos (*pagal gyvavimo ciklą*)
- Kokybė
- Kainos ar sąnaudų ir kokybės santykis

7. PIRKĖJO ĮSIPAREIGOJIMAI

7.1. Paslaugų teikėjo personalui Paslaugų atlikimui gali būti suteikta teisė jungtis prie Perkančiojo subjekto technologinio duomenų perdavimo tinklo tik pasirašius duomenų apsaugos konfidencialumo sutartį.

8. PRIEDAI

1 priedas – Minimalūs kibernetiniai saugumo reikalavimai.