PIRKIMO–PARDAVIMO SUTARTIS Nr. SIS-67-V

2018 m. rugpjūčio 22 d.
Vilnius

Valstybės įmonė „Infostruktūra“ (toliau – **Pirkėjas**), juridinio asmens kodas 121738687, registruotos buveinės adresas Pilies g. 23/15, Vilnius, atstovaujama laikinai einančio direktoriaus pareigas, Algimanto Inčiaus, veikiančio pagal 2017 m. vasario 15 d. Lietuvos Respublikos susisiekimo ministro įsakymą Nr. 3P-38, ir UAB „Avedus“ (toliau – **Pardavėjas**), atstovaujama generalinės direktorės Vilmos Škarnulytės, veikiančios pagal įmonės įstatus, laimėjusi 2018 m. birželio 6 d. skelbtą atviro konkurso būdu vykusį viešąjį pirkimą CVP IS Nr. 384571 (toliau – Pirkimas), sudarė šią sutartį (toliau – Sutartis):

1. SUTARTIES OBJEKTAS

1.1. Pardavėjas įsipareigoja parduoti Pirkėjui ugniasienes (toliau – Prekės), o Pirkėjas įsipareigoja priimti jas ir už jas sumokėti šioje sutartyje nurodytą kainą sutarties 6 p. numatyta tvarka.

2. SUTARTIES KAINA

2.1. Sutarčiai taikomas fiksuoto įkainio metodas. Sutartyje nustatyti fiksuoti prekių įkainiai nurodyti Sutarties priede.

2.2. Sutarties kaina **387.701,52** Eur (trys šimtai aštuoniasdešimt septyni tūkstančiai septyni šimtai vienas euras ir penkiasdešimt du euro centai) **be PVM, PVM – 81.417,32** Eur (aštuoniasdešimt vienas tūkstantis keturi šimtai septyniolika eurų ir trisdešimt du euro centai), **469.118,84** Eur (keturi šimtai šešiasdešimt devyni tūkstančiai vienas šimtas aštuoniolika eurų ir aštuoniasdešimt keturi euro centai) **su PVM**. Pirkėjas neįsipareigoja išpirkti viso prekių kiekio. Prekės bus perkamos pagal faktinį pirkėjo poreikį.

2.3. Įkainiai sutarties vykdymo laikotarpiu negalės būti keičiami per visą sutarties vykdymo laikotarpį, išskyrus kai pasikeičia pridėtinės vertės mokestis (PVM). Perskaičiavimas vykdomas po Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo, kuriuo keičiasi mokesčio tarifas, įsigaliojimo dienos. Pasikeitus PVM tarifo dydžiui, nepateiktų prekių įkainiai keičiami (mažinama ar didinama) proporcingai PVM pasikeitusio tarifo dydžiu. Kainos (įkainių) pakeitimas įforminamas papildomu rašytiniu šalių susitarimu.

2.4. Į Prekių įkainius įskaityti visi Pardavėjo mokami mokesčiai, prekės pristatymo ir kitos išlaidos.

2.5. Pirkimo sutarties sąlygos sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias pirkimo sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 17 straipsnyje nustatyti principai ir tikslai, bei esant Viešųjų pirkimų įstatymo 89 straipsnyje nustatytoms sąlygoms.

3. PERKAMOS PREKĖS

3.1. Šia sutartimi Pardavėjas įsipareigoja perleisti prekes, kurių detali specifikacija ir įkainiai nustatyti šios Sutarties priede.

3.2. Jei dėl nuo Pardavėjo nepriklausančių aplinkybių, kurių nebuvo įmanoma numatyti rengiant pirkimo dokumentus ir/ar sutarties sudarymo metu, Pardavėjas negali pristatyti pasiūlyme nurodyto modelio prekių, sutarties šalims išreiškus sutikimą, nekeičiant sutarties kainos, Pardavėjas gali pristatyti kito modelio prekes su sąlyga, kad naujas modelis visiškai atitiks pirkimo dokumentuose ir sutarties priede keliamus reikalavimus ir bus pristatomas už tą pačią kainą.

4. PREKIŲ PRISTATYMO TVARKA

4.1. Pardavėjas įsipareigoja pristatyti prekes savo transportu ne vėliau kaip per 20 (dvidešimt) darbo dienų nuo Pirkėjo užsakyme nurodytos datos. Jei Pardavėjas dėl objektyvių priežasčių negali prekių pristatyti per nurodytą terminą, tai Pirkėjas gali pratęsti prekių pristatymo terminą.

4.2. Prekių pristatymo vieta – Pilies g. 23/15, LT–01123 Vilnius.

5. PREKIŲ KOKYBĖ IR GARANTIJA

5.1. Pardavėjas garantuoja, kad parduodamos Prekės yra be defektų ir jų kokybė, žymėjimas, informacija vartotojui atitinka ES Tarybos Direktyvos 93/42/EEB reikalavimus.

5.2. Pristatant prekes Pardavėjas pateikia prekės vartotojo instrukcijas lietuvių ir anglų kalbomis. Prekių žymėjimas ant pakuotės turi būti valstybine kalba (jei prekės gamintojo nėra žymimos valstybine kalba – pasitelkiant lipdukus ar kt. priemones).

6. ATSISKAITYMAS TARP ŠALIŲ

6.1. Pirkėjas apmoka Pardavėjui už prekes pagal gautas PVM sąskaitas faktūras per 30 (trisdešimt) kalendorinių dienų nuo PVM sąskaitos faktūros gavimo dienos.

6.2. PVM sąskaitos faktūros, sąskaitos faktūros, kreditiniai ir debetiniai dokumentai bei avansinės sąskaitos turi būti teikiami naudojantis informacinės sistemos „E. sąskaita“ priemonėmis. Mokėjimo dokumentų nepateikus „E. sąskaita“ priemonėmis, Pirkėjas turi teisę neatlikti mokėjimo.

7. SUTARTIES ĮVYKDYMO UŽTIKRINIMAS, ATSAKOMYBĖ

7.1. Sutarties įvykdymo užtikrinimo priemonė yra netesybos. Pardavėjo iniciatyva visai arba laikinai nutraukus prekių pardavimą sutartyje nurodytomis kainomis, Pardavėjas moka 50 (penkiasdešimties) proc. dydžio baudą nuo nepateiktų prekių sumos arba užtikrina šių prekių pardavimą sutartyje nurodytomis kainomis, įsigydamas jas iš kito pardavėjo.

7.2. Pardavėjui padidinus prekių kainą ir dėl šios priežasties Pirkėjui nutraukiant galiojančią sutartį, Pardavėjas moka neįvykdytos sutarties sumos dydžio baudą.

7.3. Jei Pirkėjas dėl savo kaltės vėluoja atsiskaityti su Pardavėju per sutarties 6.1 p. numatytą terminą, jis įsipareigoja sumokėti 0,02 (dviejų šimtųjų) proc. dydžio palūkanas nuo nesumokėtos sumos.

8. FORCE MAJEURE

8.1. Force Majeure sąlygos taikomos vadovaujantis LR Vyriausybės 1996 m. liepos 15d. nutarimu Nr. 840 patvirtintomis „Atleidimo nuo atsakomybės dėl nenugalimos jėgos (Force majeure) aplinkybėmis“, taisyklėmis.

9. SUTARTIES GALIOJIMAS IR NUTRAUKIMAS

9.1. Sutartis įsigalioja šalims ją pasirašius ir galioja iki visiško šalių įsipareigojimų pagal šią sutartį įvykdymo, bet ne ilgiau kaip 36 (trisdešimt šešis) mėnesius.

9.2. Pirkėjas turi teisę vienašališkai nutraukti Sutartį, jeigu Pardavėjas ją iš esmės pažeidė:

9.2.1. parduota prekė yra netinkamos kokybės ir jos trūkumų neįmanoma pašalinti per protingą ir Pirkėjui priimtiną terminą;

9.2.2. Pardavėjas nurodytu terminu prekių nepristatė.

9.3. Pardavėjas turi teisę vienašališkai nutraukti Sutartį, jeigu Pirkėjas ją iš esmės pažeidė:

9.3.1. Pirkėjas daugiau kaip du kartus laiku nesumokėjo už Prekes, kai jos buvo perduotos nustatytais terminais;

9.3.2. Pirkėjas daugiau kaip du kartus nepriėmė tinkamoms kokybės Prekių, kai jos buvo perduotos nustatytais terminais.

9.4. Sutartis taip pat gali būti nutraukta Šalių raštišku susitarimu.

9.5. Pirkėjas turi teisę nutraukti Sutartį prieš 15 (penkiolika) kalendorinių dienų apie tai raštu įspėjęs Pardavėją.

10. KITOS SĄLYGOS

10.1. Pardavėjas įsipareigoja išrašomoje PVM sąskaitoje faktūroje vartoti tuos pačius prekių pavadinimus ir mato vnt., kokie yra pridedamoje specifikacijoje. Taip pat ant sąskaitos faktūros privalo užrašyti sutarties numerį ir datą, pagal kurią parduodamos prekės.

10.2. Sutarties vykdymo metu Pardavėjo gauta informacija ir dokumentai yra konfidencialūs. Be išankstinio raštiško Pirkėjo leidimo Pardavėjas neskelbia ir neatskleidžia jokių sutarties nuostatų, išskyrus atvejus, kai tai būtina vykdant sutartį.

10.3. Ginčai, kylantys tarp šalių, sprendžiami šalių derybomis, o nepavykus jų išspręsti – teismine tvarka Lietuvos Respublikos teismuose.

10.4. Sutartis sudaryta dviem egzemplioriais, po vieną šalims, lietuvių kalba. Abu egzemplioriai turi vienodą juridinę galią.

10.5. Pardavėjas patvirtina, kad į parduodamas prekes tretieji asmenys neturi jokių teisių.

10.6. Pridedama:

10.6.1. Sutarties priedas „Tiekėjo pasiūlymas“.

11. ŠALIŲ ADRESAI IR REKVIZITAI

Pirkėjas
VĮ „Infostruktūra“
Pilies g. 23/15, Vilnius
Juridinio asmens kodas 121738687
PVM mokėtojo kodas LT217386811
Tel. (8 5) 239 1708
Faks. (8 5) 279 1331
El. p. info@infostruktura.lt
Atsiskaitomoji sąskaita:
AB SEB bankas
A. s. LT78 7044 0600 0090 8457

Laikinai einantis direktoriaus pareigas
Algimantas Inčius

A.V.

Pardavėjas
UAB „Avedus“
Geležinio Vilko g. 18A, Vilnius
Juridinio asmens kodas:300583901
PVM mokėtojo kodas LT100002530119
Tel. +370 5 204 5441
El. p. info@avedus.lt
Atsiskaitomoji sąskaita:
AB bankas "Swedbank"
A. s. LT03 7300 0100 9676 7590

Generalinė direktorė
Vilma Škarnulytė

A.V.

Pirkimo–pardavimo sutarties
priedas
„Tiekėjo pasiūlymas“

UAB Avedus
Uždaroji akcinė bendrovė, buveinės adrs. M.Katkaus 5A-3, Vilnius, el.paštas info@avedus.lt, tel. 8 5 2045441, duomenys kaupiami ir saugomi VĮ Registrų centras, juridinio asmens kodas 300583901, pridėtinės vertės mokesčio mokėtojo kodas LT100002530119

Valstybės įmonei „Infostruktūra“

PASIŪLYMAS

2018-07-25
(Data)
Vilnius (Sudarymo vieta)

Tiekėjo pavadinimas	UAB Avedus
Tiekėjo adresas	Geležinio Vilko g. 18A, Vilnius
Už pasiūlymą atsakingo asmens vardas, pavardė	Vilma Škarnulytė
Telefono numeris	8 612 92198
Fakso numeris	
El. pašto adresas	vilma@avedus.lt

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:
   1.1. skelbime apie pirkimą;
   1.2. kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose). Teikdamas pasiūlymą, tiekėjas deklaruoja, jog išsamiai susipažino su visomis konkurso sąlygomis, joms neprieštarauja, pateikė visus reikiamus dokumentus, būtinus tam tikroms aplinkybėms pagrįsti arba paneigti.
2. Siūlome:
   2.1.1. Techniniai reikalavimai 1 tipo įrangai be palaikymo

Eil. Nr.	Specifikacija	Reikalavimai	Tiekėjo siūlomos charakteristikos
1.	Įrangos pavadinimas		FortiGate 60E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Visos dalys reikalingos montavimui pateiktos su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	110 – 220 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė prijungti maitinimo šaltinį
7.	Prievadai	Ne mažiau 7 GE RJ-45 plius bent 1 WAN, ir bent 1 DMZ prievadas	7x GE RJ45 prievadai, 2x WAN prievadai, 1x DMZ prievadas
8.	Ugniasienės pralaidumas	Ne mažiau 3 Gbps 1518 byte UDP paketais	3 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 4 Mil paketų per sekundę	4.5 Mpps
10.	Sesijų skaičius	Ne mažiau 1 Mil	1.3 Milijono
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 30 000	30 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 5 000	5 000

13.	Ipsec VPN pralaidumas	Ne mažiau 2 Gbps 512 baitų paketais	2 Gbps 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 180	200
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 450	500
16.	SSL VPN pralaidumas	150 Mbps	150 Mbps

Atnaujinta 2017-11-02

17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 100	100
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1,3 Gbps	1,4 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 150 Mbps	175 Mbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Suderinimas su Syslog, RFC 3195 palaikymas
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą.	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio.	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET
29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais	Yra galimybė filtruoti paketus iš srauto diagnostikos tikslais
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas

32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotojų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)

36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojančio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką.	Yra galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec

54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra

2.1.2. Techniniai reikalavimai 2 tipo įrangai su garantiniu palaikymu 36 mėn.

il. Nr.	**Specifikacija**	**Reikalavimai**	**Tiekėjo siūlomos charakteristikos**
1.	Įrangos pavadinimas		FortiGate 100E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį
7.	Prievadai	Ne mažiau 20 GE RJ-45 iš kurių bent 2 SFP tipo	20x GE RJ45 prievadų, 2x SFP prievadai
8.	Ugniasienės pralaidumas	Ne mažiau 7 Gbps 1518 byte UDP paketais	7,4 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 6,5 Mil paketų per sekundę	6.6 Mpps
10.	Sesijų skaičius	Ne mažiau 2 Mil	2 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 30 000	30 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 4 Gbps 512 baitų paketais	4 Gbps, 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 10000	10 000
16.	SSL VPN pralaidumas	250 Mbps	250 Mbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 300	300
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1,8 Gbps	1.9 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 180 Mbps	190 Mbps

20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto palaikymas valdymo	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET
29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based

38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai

62.	Atnaujinimai pagal nustatyta grafiką (Schedule)	Turi būti	Yra
63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*	*Yra suteikiama gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*

2.1.3. Techniniai reikalavimai 2 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.

Eil. Nr.	Specifikacija	Reikalavimai	Tiekėjo siūlomos charakteristikos
1.	Įrangos pavadinimas		FortiGate 100E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį
7.	Prievadai	Ne mažiau 20 GE RJ-45 iš kurių bent 2 SFP tipo	20x GE RJ45 prievadų, 2x SFP prievadai
8.	Ugniasienės pralaidumas	Ne mažiau 7 Gbps 1518 byte UDP paketais	7,4 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 6,5 Mil paketų per sekundę	6.6 Mpps
10.	Sesijų skaičius	Ne mažiau 2 Mil	2 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 30 000	30 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 4 Gbps 512 baitų paketais	4 Gbps, 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 10000	10 000
16.	SSL VPN pralaidumas	250 Mbps	250 Mbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 300	300
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1,8 Gbps	1.9 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 180 Mbps	190 Mbps

20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET
29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai,	Turi būti	Yra
	administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.		
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra

37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256	DES, 3DES, AES128, AES192, AES256
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra

60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*	Yra g*amintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*

2.1.4. Techniniai reikalavimai 2 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.

Eil. Nr.	**Specifikacija**	**Reikalavimai**	**Tiekėjo siūlomos charakteristikos**
1.	Įrangos pavadinimas		FortiGate 100E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga

4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį
7.	Prievadai	Ne mažiau 20 GE RJ-45 iš kurių bent 2 SFP tipo	20x GE RJ45 prievadų, 2x SFP prievadai
8.	Ugniasienės pralaidumas	Ne mažiau 7 Gbps 1518 byte UDP paketais	7,4 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 6,5 Mil paketų per sekundę	6.6 Mpps
10.	Sesijų skaičius	Ne mažiau 2 Mil	2 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 30 000	30 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 4 Gbps 512 baitų paketais	4 Gbps, 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 10000	10 000
16.	SSL VPN pralaidumas	250 Mbps	250 Mbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 300	300
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1,8 Gbps	1.9 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 180 Mbps	190 Mbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą	Suderinamas su FortiAnalyzer įrenginiu

27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET

29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce

44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256	DES, 3DES, AES128, AES192, AES256
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra

63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*	*Yra gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos*

2.1.5. Techniniai reikalavimai 3 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.

Eil. Nr.	**Specifikacija**	**Reikalavimai**	**Tiekėjo siūlomos charakteristikos**
1.	Įrangos pavadinimas		FortiGate 200E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	110 – 220 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį
7.	Prievadai	Ne mažiau 18 GE RJ-45 iš kurių bent 4 SFP tipo	18x GE RJ45 prievadų, 4x GE SFP prievadai
8.	Ugniasienės pralaidumas	Ne mažiau 19 Gbps 1518 byte UDP paketais	20 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 13 Mil paketų per sekundę	13.5 Mpps
10.	Sesijų skaičius	Ne mažiau 2 Mil	2 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 130 000	135 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 8 Gbps 512 baitų paketais	9 Gbps 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 10000	10 000
16.	SSL VPN pralaidumas	800 Mbps	900 Mbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 300	300

18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 6 Gbps	6 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 1 Gbps	1 Gbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą.	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio.	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET

29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais.	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra

35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką.	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256,
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP

55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*	*Yra gamintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*

2.1.6. Techniniai reikalavimai 3 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.

Eil. Nr.	Specifikacija	Reikalavimai	Tiekėjo siūlomos charakteristikos
1.	Įrangos pavadinimas		FortiGate 200E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	110 – 220 V
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį

7.	Prievadai	Ne mažiau 18 GE RJ-45 iš kurių bent 4 SFP tipo	18x GE RJ45 prievadų, 4x GE SFP prievadai
8.	Ugniasienės pralaidumas	Ne mažiau 19 Gbps 1518 byte UDP paketais	20 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 13 Mil paketų per sekundę	13.5 Mpps
10.	Sesijų skaičius	Ne mažiau 2 Mil	2 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 130 000	135 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 8 Gbps 512 baitų paketais	9 Gbps 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 10000	10 000
16.	SSL VPN pralaidumas	800 Mbps	900 Mbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 300	300
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 6 Gbps	6 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 1 Gbps	1 Gbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą.	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio.	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio

28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET

29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais.	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką.	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų

47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256,
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra

63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*	*Yra gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*

2.1.7. Techniniai reikalavimai 4 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.

Eil. Nr.	Specifikacija	Reikalavimai	Tiekėjo siūlomos charakteristikos
1.	Įrangos pavadinimas		FortiGate 300E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V, 50 – 60 Hz
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį
7.	Prievadai	Ne mažiau 18 GE RJ-45 plius 12 SFP tipo	18x GE RJ45 prievadų, 16x GE SFP prievadų
8.	Ugniasienės pralaidumas	Ne mažiau 30 Gbps 1518 byte UDP paketais	32 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 28 Mil paketų per sekundę	30 Mpps
10.	Sesijų skaičius	Ne mažiau 4 Mil	4 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 250 000	300 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 20 Gbps 512 baitų paketais	20 Gbps, 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 45000	50 000
16.	SSL VPN pralaidumas	2 Gbps	2.5 Gbps

17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 500	500
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 10 Gbps	11 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 6,5 Gbps	6.8 Gbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą.	Suderinamas su FortiAnalyzer įrenginiu

27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio.	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET
29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais.	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra

35.	Vartotojų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką.	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų
47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256,
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP

55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*	*Yra gamintojo garantuojamas 12 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*

2.1.8. Techniniai reikalavimai 4 tipo įrangai palaikančiai sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.

Eil. Nr.	**Specifikacija**	**Reikalavimai**	**Tiekėjo siūlomos charakteristikos**
1.	Įrangos pavadinimas		FortiGate 300E
2.	Įrangos gamintojas		Fortinet
3.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Dalys reikalingos montavimui yra pateiktos kartu su įranga
4.	Įrangos aukštis	Ne daugiau 1 U	1 U
5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V, 50 – 60 Hz
6.	Atsarginis maitinimo šaltinis	Turi būti galimybė pajungti atsarginį maitinimo šaltinį	Yra galimybė pajungti atsarginį maitinimo šaltinį

7.	Prievadai	Ne mažiau 18 GE RJ-45 plius 12 SFP tipo	18x GE RJ45 prievadų, 16x GE SFP prievadų
8.	Ugniasienės pralaidumas	Ne mažiau 30 Gbps 1518 byte UDP paketais	32 Gbps, 1518 baitų UDP paketais
9.	Ugniasienės pralaidumas paketais per sekundę	Ne mažiau 28 Mil paketų per sekundę	30 Mpps
10.	Sesijų skaičius	Ne mažiau 4 Mil	4 Milijonai
11.	Naujų sesijų skaičius per sekundę	Ne mažiau 250 000	300 000
12.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000	10 000
13.	Ipsec VPN pralaidumas	Ne mažiau 20 Gbps 512 baitų paketais	20 Gbps, 512 baitų paketais
14.	Ipsec tunelių skaičius įrenginys – įrenginys (Gateway-to-Gateway)	Ne mažiau 2000	2 000
15.	Ipsec tunelių skaičius klientas – įrenginys (Client-to-Gateway)	Ne mažiau 45000	50 000
16.	SSL VPN pralaidumas	2 Gbps	2.5 Gbps
17.	SSL VPN vartotojų skaičius vienu metu	Ne mažiau 500	500
18.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 10 Gbps	11 Gbps
19.	SSL inspekcijos pralaidumas	Ne mažiau 6,5 Gbps	6.8 Gbps
20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių	Yra galimybė padalinti į 10 virtualių įrenginių
21.	Darbo režimai tinkle	NAT/Route, Transparent	NAT/Route, Transparent
22.	Galimybė išeksportuoti įrenginio nustatymus (Backup)	Turi būti	Yra
23.	Galimybė išeksportuojant įrenginio nustatymus apsaugoti slaptažodžiu	Turi būti	Yra
24.	Integracija su SNMP (Simple Network Management Protocol)	Palaikomos versijos 1,2,3	Galimybė integruoti 1,2,3 versijas
25.	Suderinamumas su Syslog, RFC 3195 palaikymas	Turi būti	Yra
26.	Ugniasienės įvykių kaupimas ir ataskaitų sudarymas išoriniame įrenginyje	Turi būti suderinamas su šiuo metu perkančiosios organizacijos turimu FortiAnalyzer įrenginiu arba tiekėjas kartu su ugniasiene turi pateikti ir įvykių kaupimo ir ataskaitų sudarymo įrangą.	Suderinamas su FortiAnalyzer įrenginiu
27.	Centralizuoto valdymo palaikymas	Turi būti galimybė valdyti visus šio modelio įrenginius iš centrinio, valdymui dedikuoto, įrenginio.	Yra galimybė valdyti visus įrenginius iš centrinio, valdymui dedikuoto įrenginio
28.	Valdymas	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET	WEB (HTTPS), SSH, dedikuotas prievadas, TELNET

29.	Įvykių žurnalų (event log) palaikymas. Sisteminiai, administravimo, VPN, vartotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.	Turi būti	Yra
30.	Diagnostikos priemonės įrangos, tinklo ar sistemos netinamo veikimo priežasties diagnozavimui.	Turi turėti bent galimybę iš srauto išsifiltruoti paketus (packet capture) diagnostikos tikslais.	Yra galimybė filtruoti paketus iš srauto
31.	Nutolusių vartotojų duomenų bazių palaikymas	LDAP, RADIUS, TACACS+, two-factor authentication	LDAP, RADIUS, TACACS+, dviejų žingsnių autentifikavimas
32.	Autorizacijos integracija (single sign on) su	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x	Windows AD, Microsoft Exchange server, Novell eDirectory, Citrix ir Terminal Server Agent, Radius, 802,1x
33.	SSL šifruoto srauto inspekcija	Turi būti	Yra
34.	Galimybė redaguoti pranešimus vartotojams apie WEB puslapių ar laiškų priedų blokavimą	Turi būti	Yra
35.	Vartotjų karantino laiko trukmės nustatymas	Nustatytam laiko tarpui, visam laikui (iki administratorius atliks pakeitimus)	Galima nustatyti atitinkamą laiko tarpą arba karantinuoti visam laikui (iki administratorius atliks pakeitimus)
36.	Botnet serverių IP adresų blokavimas, jų IP adresų duomenų bazių palaikymas	Turi būti	Yra
37.	Antivirusinio skanavimo darbo režimai	Proxy, Flow-based	Proxy, Flow-based
38.	Galimybė atlikti išorinę bylų patikrą, intergracija su servisu „debesyje“.	Turi būti	Yra
39.	Protokolų anomalijų detektavimas	Turi būti	Yra
40.	Karantinavimo pasirinkimas IPS atakos atveju	Atakuojantis IP adresas, atakuojantčio ir aukos IP adresai, prievadas. Galimybė nustatyti karantinavimo laiką.	Galimybė matyti atakuojančio IP adresą, atakuojančio ir aukos IP adresus, prievadą. Galima nustatyti karantinavimo laiką
41.	Atpažįstamų aplikacijų skaičius	Ne mažiau 3000	3 000
42.	Aplikacijų blokavimas (Application Control)	Turi būti	Yra
43.	Aplikacijų, naudojančių servisą debesyje atpažinimas ir kontrolė	Google Docs, Drop box, SalesForce	Google Docs, Drop box, SalesForce
44.	WEB filtravimo darbo režimai	Proxy, flow-based, DNS	Proxy, flow-based, DNS
45.	Galimybė administratoriui aprašyti WEB filtravimą pagal URL.	Turi būti	Yra
46.	Kategorizuotų WEB puslapių duomenų bazėje	Ne mažiau 250 milijonų	250 milijonų

47.	Kategorizuotų WEB puslapių kategorijų	Ne mažiau 80	80
48.	Galimybė laikinai suteikti vartotojui prieigą prie uždraustos WEB kategorijos	Turi būti	Yra
49.	Ugniasienės taisyklės per vartotoją ir per įrenginio tipą	Turi būti	Yra
50.	Galimybė uždrausti keliems vartotojams su tuo pačiu vartotojo vardu jungtis prie VPN	Turi būti	Yra
51.	IPSec kriptavimo algoritmai	DES, 3DES, AES128, AES192, AES256,	DES, 3DES, AES128, AES192, AES256,
52.	IPSec autentifikavimo algortimai	MD5, SHA-1, SHA-256, SHA384, SHA-512	MD5, SHA-1, SHA-256, SHA384, SHA-512
53.	Kitų VPN palaikymas	L2TP, PPTP, GRE over IPSec	L2TP, PPTP, GRE over IPSec
54.	Informacijos (bylų) nutekėjimo prevencijos (DLP) palaikomi protokolai	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP	HTTP POST, HTTP GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
55.	Galimybė realizuoti rezervinį ryšį (WAN) 3G/4G USB modemo pagalba	Turi būti	Yra
56.	Maršrutizavimas	Statinis, dinaminis	Statinis, dinaminis
57.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS
58.	NAT maršrutizavimo protokolai	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN	NAT64, NAT46, static ir dynamic ANT, PAT, Full Cone ANT, STUN
59.	Srauto ribojimas ir QoS per taisyklę (policy) ir aplikaciją	Turi būti	Yra
60.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Programinės įrangos atnaujinimai bus viso aptarnavimo laikotarpiu
61.	Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai.	Turi būti teikiami viso garantinio laikotarpio metu be papildomo mokesčio	Atnaujinimai teikiami viso garantinio laikotarpio metu nemokamai
62.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra

63.	Garantiniai įsipareigojimai, techninis palaikymas	*Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*	*Yra gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei atnaujinimų teikimas garantiniu laikotarpiu (NGFV, App Control, IPS, AV, WEB Filtering, Antispam, Botnet IP/Domain). Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 8x5) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.*

3. ***Finansinis pasiūlymas***

Eil. Nr.	**Modelis [įrašyti siūlomą pavadinimą]**	**Maksimalus kiekis vnt.**	**1 vnt. kaina be PVM**	**Bendra kaina be PVM (3x4=5)**
1.	*2.*	*3.*	*4.*	*5.*
1.	1 tipo įranga be palaikymo	150	380,00	57 000,00
2.	**Įranga su palaikymu 36 mėn.**	**Maksimalus kiekis vnt.**	**1 vnt. kaina per 1 mėn. be PVM**	**Bendra kaina be PVM (3x4x36=5)**
3.	2 tipo įranga su palaikymu 36 mėn.	25	51.13	46 017.00
4.	2 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.	40	75.56	108 806.40
5.	3 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.	15	135.70	73 278.00
6.	4 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 36 mėn.	4	197.76	28 477.44
7.	**Įranga su palaikymu 12 mėn.**	**Maksimalus kiekis vnt.**	**1 vnt. kaina per 1 mėn. be PVM**	**Bendra kaina be PVM (3x4x12=5)**
8.	2 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.	25	157.46	47 238.00
9.	3 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.	5	282.99	16 979.40
10.	4 tipo įranga palaikanti sekantį funkcionalumą (Antimalware, antispam, webfilter, IPS parašų bazių atnaujinimai) 12 mėn.	2	412.72	9 905.28

11	**Bendra pasiūlymo kaina Eur (be PVM)** (*1, 3-6 ir 8-10 eilučių 5-o stulpelio suma*)	387 701.52
12	**21 proc. PVM**	81 417.32
	Bendra pasiūlymo kaina Eur (su PVM)	469 118.84

Bendra viso pasiūlymo kaina (skaičiais ir žodžiais): **Keturi šimtai šešiasdešimt devyni tūkstančiai vienas šimtas aštuoniolika eurų 84 ct. (su PVM)**
PVM, kuris sudaro (skaičiais ir žodžiais): **Aštuoniasdešimt vienas tūkstantis keturi šimtai septyniolika eurų 32 ct.** Bendra viso pasiūlymo kaina (skaičiais ir žodžiais): **Trys šimtai aštuoniasdešimt septyni tūkstančiai septyni šimtai vienas euras 52 ct. (be PVM)**

Mūsų pasiūlymas visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus.

Ši pasiūlyme nurodyta informacija yra konfidenciali:

Eil. Nr.	Pateikto dokumento pavadinimas (rekomenduojama pavadinime vartoti žodį „Konfidencialu“)

Pastabos: 1) Konfidencialia informacija gali būti, įskaitant, bet ja neapsiribojant, komercinė (gamybinė) paslaptis ir konfidencialieji pasiūlymų aspektai. Informacija, kurią viešai skelbti įpareigoja Lietuvos Respublikos įstatymai, negali būti tiekėjo nurodoma, kaip konfidenciali; 2) Nurodant konfidencialią informaciją, rekomenduojama vadovautis Viešųjų pirkimų tarnybos išaiškinimu, kuris paskelbtas Viešųjų pirkimų tarnybos interneto svetainėje, adresu: https://vpt.lrv.lt/lt/naujienos/kaip-turi-buti-suprantamas-konfidencialumas-viesuosiuose-pirkimuose 3)
Atkreiptinas dėmesys, kad vadovaudamasi Viešųjų pirkimų įstatymo 86 straipsnio 9 dalimi, PO paskelbs sudarytą pirkimo sutartį ir laimėtojo pasiūlymą. Todėl tiekėjas turi būti atidus, rengdamas savo pasiūlymą, ir tuo atveju, jei pasiūlyme yra konfidenciali informacija, teikiant pasiūlymą ją aiškiai nurodyti; 4) Tiekėjui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra, todėl papildomai į tiekėją kreipiamasi nebus.

Generalinė
(Pareigo

(paraš

Vilma Škarnulytė
(vardas,)

Pirkėjas:

Laikinai einantis direktoriaus pareigas
Algimantas Inčius

A.V

Pardavėjas:

Generalinė direktorė
Vilma Škarnulytė

A.V.