3 priedas

Blue Bridge MSP

Uždaroji akcinė bendrovė, J. Jasinskio g. 16A, LT-03163 Vilnius, tel. (8 5) 252 6060, el. p. info@bluebridge.lt, duomenys apie įmonę kaupiami ir saugomi VĮ Registrų centras juridinių asmenų registre, 301489547, LT100003708514

VšĮ „Plačiajuostis internetas“

PASIŪLYMAS PIRKIME

UGNIASIENĖS

2024-11-21 Nr. RST241121LAG01-1
Vilnius

Tiekėjo pavadinimas	Blue Bridge MSP, UAB
Tiekėjo adresas	J. Jasinskio g. 16A, LT-03163 Vilnius
Asmens, pasirašiusio pasiūlymą vardas, pavardė, pareigos	
Telefono numeris	
El. pašto adresas	

/Pastaba. Pildoma, jei tiekėjas ketina pasitelkti subrangovą (-us), subtiekėją (-us), ar subteikėją (-us)/

Subrangovo (-ų), subtiekėjo (-ų) ar subteikėjo (-ų) pavadinimas (-ai)	-
Subrangovo (-ų), subtiekėjo (-ų) ar subteikėjo (-ų) adresas (-ai)	-
Įsipareigojimų dalis (procentais), kuriai ketinama pasitelkti subrangovą (-us), subtiekėją (-us) ar subteikėją (-us)	-

Dalyvis pasiūlyme privalo išviešinti subtiekėjus, kurių pajėgumais, t. y. siekdamas atitikti kvalifikacijos reikalavimus, remiasi, taip pat nurodyti ir kitus žinomus subtiekėjus.

Eil. nr.	Pavadinimas, kodas ir adresas	Numatomos tiekti prekės	Pirkimo sutarties dalis pasiūlymo kainoje, kuriai ketinama pasitelkti subtiekėjus
			Proc.
Subtiekėjai, kurių pajėgumais remiamasi įrodinėjant kvalifikacijos atitiktį			
	-	-	
		Viso:	
Kiti žinomi subtiekėjai, kurie bus pasitelkti vykdant pirkimo sutartį ir kurių pajėgumais nesiremiama įrodinėjant kvalifikacijos atitikties			
		Viso:	

Informacija apie specialistus, kuriais bus remiamasi įrodinėjant tiekėjo kvalifikaciją ir vykdant pirkimo sutartį, tačiau jie nėra tiekėjo ar tiekėjo pasitelkiamo (-ų) subtiekėjo (-ų) darbuotojai pasiūlymo pateikimo metu, bet laimėjimo atveju būtų įdarbinti:

Eil. nr.	Vardas ir pavardė	Specialisto dabartinė darbovietė
-	-	-

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:
1) Pirkimo skelbime, paskelbtame Centrinėje viešųjų pirkimų informacinėje sistemoje;
2) Pirkimo sąlygose (jų paaiškinimuose, papildymuose (jeigu tokių bus).

Pažymime, kad esame nuodugniai susipažinę su visais pirkimo dokumentais ir jų sąlygomis bei pateikdami šį pasiūlymą sutinkame su visais pirkimo dokumentų reikalavimais ir sąlygomis.

2. Atsižvelgdami į pirkimo dokumentuose išdėstytas sąlygas, teikiame savo pasiūlymą.

3. Mes siūlome perkamą pirkimo objektą, kurio detalus aprašymas tiksliai atitinka pirkimo dokumentuose nurodytus reikalavimus.

4. Siūlomo pirkimo objekto (taip, kaip jis aprašytas pirkimo dokumentuose) kaina nurodyta šioje lentelėje:

Eil. Nr.	Pirkimo objektas	Mato vnt.	Kiekis	Įkainis, Eur be PVM	Viso kaina, Eur be PVM	Viso kaina, Eur su PVM
1	2	3	4	5	6 (4*5)	7
1	Interneto ugniasienės */nurodyti gamintoją ir modelį/*	Vnt.	2	16615,00	33230,00	40208,30
2	4G ugniasienės */nurodyti gamintoją ir modelį/*	Vnt.	2	1700,00	3400,00	4114,00
Bendra pasiūlymo kaina:					*36630,00*	*44322,30*

Bendra pasiūlymo kaina, 44322,30 Eur su PVM* (suma žodžiais – keturiasdešimt keturi tūkstančiai trys šimtai dvidešimt du eurai ir trisdešimt centų.)

Į šią sumą įeina visos išlaidos ir visi mokesčiai, taip pat ir PVM, kuris sudaro 7692,30 Eur.

* *Į nurodomas kainas turi būti įskaičiuota: PVM, kiti galimi mokesčiai bei visos kitos išlaidos. Tiekėjas turi nurodyti kainą Eur su PVM, kai jis yra PVM mokėtojas arba Eur be PVM, jei tiekėjas yra ne PVM mokėtojas. Tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, jis nurodo priežastis, dėl kurių PVM nemoka.*

5. Mes siūlome šiuos parametrus pagal ekonominio naudingumo vertinimo kriterijus:

Vertinimo kriterijai	Siūlomas parametras
Antras kriterijus: FortiManager centralizuoto valdymo palaikymas (T_1)	FortiManager centralizuoto valdymo palaikymas visoms siūlomoms ugniasienėms *(R_{p1}): <u>atitinka</u>.*
Trečias kriterijus: Įvykių žurnalų (syslog) siuntimas į FortiAnalyzer (T_2)	*Įvykių žurnalų (syslog) siuntimas į FortiAnalyzer* visoms siūlomoms ugniasienėms *(R_{p2}): <u>atitinka</u>.*

PASTABA. Tiekėjas kartu su pasiūlymu turi pateikti ekonominio naudingumo vertinimui siūlomų parametrų atitiktį patvirtinančius dokumentus. Tiekėjui kartu su pasiūlymu nepateikus siūlomų parametrų atitiktį įrodančių dokumentų, atitinkamo parametro reikšmė bus lygi 0.

6. PREKIŲ ATITIKTIES TECHNINĖS SPECIFIKACIJOS REIKALAVIMAMS LENTELĖ

Interneto ugniasienių techninės savybės

Eil. Nr.	Parametrai	Minimalūs reikalavimai	Konkretūs tiekėjo siūlomų Prekių parametrai ir nuoroda į atitiktį pagrindžiantį dokumentą
	Gamintojas	Nurodyti gamintoją.	Fortinet Inc.
	Produkto pavadinimas	Nurodyti produkto pavadinimą, modelį ir kodą. Kartu su pasiūlymu atskirame dokumente turi būti pateiktas pilnas komplektuojamų komponentų sąrašas su gamintojo kodais, kiekiais ir pavadinimais.	**FG-121G-BDL-950-60** Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) **FC1-10-EMS04-428-01-60** FortiClient VPN/ZTNA Agent Subscriptions for 25 endpoints, includes on-prem EMS and FortiCare Premium. **FTM-ELIC-50** Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic license certificate. **FN-TRAN-LX 1GE** SFP LX transceiver module, 10km range, -40C to 85C, over SMF, for systems with SFP and SFP/SFP+ slots. **FN-TRAN-SFP+LR** 10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots Pridedamas dokumentas: „Produktų kodai ir kiekiai“.
	Sprendimo architektūra ir sudedamosios dalys	Interneto ugniasienių sprendimas turi būti sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t. y. kiekviena ugniasienė turi dirbti	Interneto ugniasienių sprendimas yra sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t. y. kiekviena ugniasienė dirba

		kaip nepriklausomas narys ir turi būti galima narius sujungti į aukšto patikimumo telkinį. Aukšto patikimumo telkinys turi veikti esant 100 km atstumui tarp įrenginių. Turi būti pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aušto patikimumo telkinio narius.	kaip nepriklausomas narys ir galima narius sujungti į aukšto patikimumo telkinį. Aukšto patikimumo telkinys veikia esant 100 km atstumui tarp įrenginių. Yra pateikta visa aparatinė-programinė įranga ir licencijos, leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aušto patikimumo telkinio narius.
	Surinkimo reikalavimai	Interneto ugniasienių sprendimo nario įranga turi būti specializuotas aparatinis-programinis įrenginys arba modulinis įrenginys su vidiniais arba išoriniais moduliais komplektuojamas paties gamintojo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais.	Interneto ugniasienių sprendimo nario įranga yra specializuotas aparatinis-programinis įrenginys. Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtais sprendimais.
	Korpusas	Ugniasienės pateikiamos su visais montavimui į standartinę 19 colių įrangos montavimui skirtą spintą reikalingais priedais. (įskaitant bet neapsiribojant tvirtinimo elementais). Aukštis ne didesnis kaip 1 U.	Ugniasienės pateikiamos su visais montavimui į standartinę 19 colių įrangos montavimui skirtą spintą reikalingais priedais. (įskaitant, bet neapsiribojant tvirtinimo elementais). Aukštis 1 U.
	Maitinimo šaltinis	Dubliuoti (du ar daugiau), pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Ugniasienių sprendimo narys turi veikti sugedus vienam maitinimo šaltiniui. Pritaikyti 230 V, 50 – 60 Hz kintamos srovės elektros tinklui.	Dubliuoti (du), pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Ugniasienių sprendimo narys veiks sugedus vienam maitinimo šaltiniui. Pritaikyti 230 V, 50 – 60 Hz kintamos srovės elektros tinklui.
	Tinklo prievadai	Tinklo prievadų kiekis: - Ne mažiau, kaip 8 vnt. 1000 BaseT prievadų; - Ne mažiau, kaip 8 vnt. 1000 BaseX SFP prievadų;	Tinklo prievadų kiekis: - 8 vnt. 1000 BaseT prievadų; - 8 vnt. 1000 BaseX SFP prievadų;

		- Ne mažiau, kaip 4 vnt. 10 GBase SFP+ prievadų. Tiekėjas kartu su kiekviena ugniasiene privalo pateikti po 2 vnt. 1000 Base LX SFP ir 4 vnt 10 GBase LX SFP+, pilnai suderinamus su siūlomomis ugniasienėmis.	- 4 vnt. 10 GBase SFP+ prievadų. Su kiekviena ugniasiene bus pateikta po 2 vnt. 1000 Base LX SFP ir 4 vnt 10 GBase LX SFP+, pilnai suderinami su siūlomomis ugniasienėmis.
	Valdymo prievadai	Ne mažiau kaip 1 konsolės prievadas;	1 konsolės prievadas;
	Pajungimo į aukšto patikimumo telkinį prievadai.	Prievadų kiekis ir tipas: - ne mažiau kaip 2 vnt. dubliuojantys vienas kitą. Šių prievadų skaičius turi būti papildomas, neturi būti įtrauktas į 7 punkte numatytą tinklo prievadų skaičių.	Prievadų kiekis ir tipas: - 2 vnt. dubliuojantys vienas kitą. Šių prievadų skaičius yra papildomas, neįtrauktas į 7 punkte numatytą tinklo prievadų skaičių.
	Vidinė saugykla	Ne mažiau kaip 480 GB SSD.	480 GB SSD.
	Palaikomi standartai / protokolai	Interneto ugniasienių sprendimo narys privalo palaikyti: - kiekvienas tinklo duomenų srauto fizinis prievadas privalo palaikyti VLAN pagal 802.1Q arba lygiavertį standartą; - LACP arba lygiavertį protokolą suderinamą su HP ir Cisco komutatorių sujungimu; - bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą; - 802.3ad arba lygiavertį standartą. Turi būti galima apjungti į vieną loginę tinklo sąsają ne mažiau kaip 2 fizines sąsajas.	Interneto ugniasienių sprendimo narys palaiko: - kiekvienas tinklo duomenų srauto fizinis prievadas palaiko VLAN pagal 802.1Q standartą; - LACP protokolą, suderinamą su HP ir Cisco komutatorių sujungimu; - protokolus: Netflow, IPFIX; - 802.3ad standartą. Galima apjungti į vieną loginę tinklo sąsają 2 fizines sąsajas.
	VLAN palaikymas	Ne mažiau kaip 4000 VLAN žymių per įrenginį arba prievadą.	4000 VLAN žymių per įrenginį arba prievadą.
	Ugniasienės greitaveika	Interneto ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų	Interneto ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su

		atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą – ne mažiau kaip 5 Gbps.	aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą – 6,7 Gbps.
	Ugniasienės greitaveika	Interneto ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS), kenkėjiškų kodų, antivirusine patikra realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą - ne mažiau kaip 2,5 Gbps.	Interneto ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS), kenkėjiškų kodų, antivirusine patikra realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą - 2,8 Gbps.
	IPsec VPN greitaveika	Ne mažiau kaip 30 Gbps.	35 Gbps.
	IPsec tunelių skaičius naudojant vartotojų / klientų prisijungimą prie ugniasienės	Ne mažiau kaip 300.	500.
	Maksimalus sesijų skaičius vienu metu	Ne mažiau kaip 2000000.	Ne mažiau kaip 3000000.
	Maksimalus naujų sesijų skaičius per sekundę	Ne mažiau kaip 100000.	Ne mažiau kaip 140000.
	Suminis saugumo taisyklių skaičius per ugniasienę	Ne mažiau kaip 4000.	Ne mažiau kaip 10000.
	Aukšto patikimumo savybės	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: - nario pajungimas į aukšto patikimumo telkinį, kuris gali	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: - nario pajungimas į aukšto patikimumo telkinį, kuris

		dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; - turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; - automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; - automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; - turi būti galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.	gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; - yra būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; - automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; - automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; - yra galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema automatiškai persijungia, jei nurodyti IP adresai tampa neaktyviais.
	Įrangos virtualizavimas	Turi būti funkcionalumas, leidžiantis interneto ugniasienių sprendimo narį sudalinti į ne mažiau kaip 5 virtualius įrenginius.	Yra funkcionalumas, leidžiantis interneto ugniasienių sprendimo narį sudalinti į 10 virtualių įrenginių.
	Ugniasienės darbo režimai	Ne mažiau kaip : - maršrutizavimo tarp skirtingų tinklų (OSI L3); - skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);	Darbo režimai : - maršrutizavimo tarp skirtingų tinklų (OSI L3); - skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);
	Maršrutizavimas	Interneto ugniasienių sprendimo narys privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). Ugniasienė privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.	Interneto ugniasienių sprendimo narys palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). Ugniasienė palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.

	PBR funkcionalumas	Interneto ugniasienių sprendimo narys privalo palaikyti politika pagrįstą maršrutizavimą (angl. policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.	Interneto ugniasienių sprendimo narys palaiko politika pagrįstą maršrutizavimą (angl. policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.
	Dinaminio maršrutizavimo protokolai	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: - BGP; - OSFP v2 ir v3; - RIP v2.	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintus protokolus: - BGP; - OSFP v2 ir v3; - RIP v2.
	OSPF funkcionalumas	Interneto ugniasienių sprendimo narys privalo turėti grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.	Interneto ugniasienių sprendimo narys turi grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.
	Srauto balansavimas	Interneto ugniasienių sprendimo narys privalo gebėti balansuoti serveriams skirtą srautą. Turi būti palaikomi ne mažiau kaip Round robin ir Least session srauto balansavimo metodai.	Interneto ugniasienių sprendimo narys geba balansuoti serveriams skirtą srautą. Palaikomi Round robin ir Least session srauto balansavimo metodai.
	BFD palaikymas	Interneto ugniasienių sprendimo narys privalo palaikyti BFD (angl. bidirectional forwarding detection) protokolą.	Interneto ugniasienių sprendimo narys palaiko BFD (angl. bidirectional forwarding detection) protokolą.
	IPv6 palaikymas	Interneto ugniasienių sprendimo narys privalo palaikyti IPv6 protokolą.	Interneto ugniasienių sprendimo narys palaiko IPv6 protokolą.
	Adresų transliavimo funkcionalumas	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: - NAT64; - statinis adresų transliavimas; - dinaminis adresų transliavimas keičiant prievadus (PAT).	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: - NAT64; - statinis adresų transliavimas; - dinaminis adresų transliavimas keičiant prievadus (PAT).

	Integracija su SNMP (angl. Simple Network Management Protocol) įrenginio būsenos stebėjimui	Privalo palaikyti SNMP protokolo 2 ir 3 versijas.	Palaiko SNMP protokolo 2 ir 3 versijas.
	Suderinamumas su Syslog	Interneto ugniasienių sprendimo narys turi būti suderinamas su Syslog standartu.	Interneto ugniasienių sprendimo narys suderinamas su Syslog standartu.
	Žurnalinių įvykių (angl. event log) palaikymas	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus žurnalinius įvykius: - sisteminiai; - administravimo; - VPN; - naudotojų autentifikavimo; - maršrutizavimo; - saugos incidentų įvykiai.	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintus žurnalinius įvykius: - sisteminiai; - administravimo; - VPN; - naudotojų autentifikavimo; - maršrutizavimo; - saugos incidentų įvykiai.
	Žurnalinių įvykių kaupimas	Interneto ugniasienių sprendimo narys privalo gebėti įvykių žurnalus siųsti į Perkančiosios organizacijos turimą nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą SIEM sistemą.	Interneto ugniasienių sprendimo narys geba įvykių žurnalus siųsti į Perkančiosios organizacijos turimą nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą SIEM sistemą.
	Diagnostikos priemonės	Privalomas srauto / paketų nuo konkrečios sąsajos „įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	Yra srauto / paketų nuo konkrečios sąsajos „įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.
	Nutolusių naudotojų duomenų bazių palaikymas	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: - LDAP; - RADIUS; - TACACS+;	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintas duomenų bazes: - LDAP; - RADIUS; - TACACS+; - dviejų lygių (angl. two-factor) autentifikaciją.

		- dviejų lygių (angl. two-factor) autentifikaciją.	
	Autorizacijos integracija (angl. single sign on)	Interneto ugniasienių sprendimo narys privalo turėti integracijas su žemiau įvardintomis arba lygiavertėmis sistemomis: - Windows AD; - Microsoft Exchange server; - RADIUS; - 802.1x.	Interneto ugniasienių sprendimo narys turi integracijas su žemiau įvardintomis sistemomis: - Windows AD; - Microsoft Exchange server; - RADIUS; - 802.1x.
	SSL šifruotas srautas	Interneto ugniasienių sprendimo narys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. Interneto ugniasienių sprendimo narys privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Privalo būti galimybė nurodyti kuris duomenų srautas turi būti dešifruojamas.	Interneto ugniasienių sprendimo narys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą. Interneto ugniasienių sprendimo narys palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Yra galimybė nurodyti, kuris duomenų srautas turi būti dešifruojamas.
	DoS apsauga	Interneto ugniasienių sprendimo narys privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.	Interneto ugniasienių sprendimo narys leidžia riboti sesijų ir paketų per sekundę skaičius jų šaltiniui arba adresatui.
	Apsauga nuo grėsmių	Interneto ugniasienių sprendimo narys turi saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdyti konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrinti perduodamą srautą nuo virusų. Virusų, kenkėjiškų kodų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip interneto ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui. Turi būti galimybė naudoti gamintojo pateikiamus dinamiškai	Interneto ugniasienių sprendimo narys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdo konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrina perduodamą srautą nuo virusų. Virusų, kenkėjiškų kodų aprašai pateikiami nemokamai (įskaičiuoti į pasiūlymo kainą) tokiam pačiam kaip interneto ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui. Yra galimybė naudoti gamintojo pateikiamus dinamiškai

		atnaujinamus kenksmingų IP adresų sąrašus.	atnaujinamus kenksmingų IP adresų sąrašus.
	IPS funkcionalumas	Interneto ugniasienių sprendimo narys privalo turėti žemiau įvardintą funkcionalumą: - įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. Funkcionalumas nemokamai (turi būti įtraukta į pasiūlymo kainą) turi veikti ne trumpesniu nei įrangos garantinis laikotarpiu. - turi būti galimybė užblokuoti atakuojantį IP adresą; - leisti nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme.	Interneto ugniasienių sprendimo narys turi žemiau įvardintą funkcionalumą: - įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. Funkcionalumas nemokamai (įtraukta į pasiūlymo kainą) veikia tokiu pačiu kaip įrangos garantinis laikotarpiu. - yra galimybė užblokuoti atakuojantį IP adresą; - leisti nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme.
	Protokolų anomalijos	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: - protokolų anomalijų aptikimas; - protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: - protokolų anomalijų aptikimas; - protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą.
	Aplikacijų valdymas	Interneto ugniasienių sprendimo narys privalo palaikyti: - aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 2000 aplikacijų (tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienės garantinio aptarnavimo laikotarpiui;	Interneto ugniasienių sprendimo narys palaiko: - aplikacijų identifikavimą ir kontrolę. Gali identifikuoti 2000 aplikacijų (tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (įskaičiuoti į pasiūlymo kainą) tokiam pačiam kaip ugniasienės garantinio aptarnavimo laikotarpiui;

		- aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.	- aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.
	URL filtravimas	Interneto ugniasienių sprendimo narys privalo palaikyti: - prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). URL duomenų bazė pateikiama nemokamai (arba įskaičiuota į pasiūlymo kainą) netrumpesniam kaip interneto ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiu; - nuosavų draudžiamų URL sąrašų kūrimas; - URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo.	Interneto ugniasienių sprendimo narys palaiko: - prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). URL duomenų bazė pateikiama nemokamai (įskaičiuota į pasiūlymo kainą) tokiam pačiam kaip interneto ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui; - nuosavų draudžiamų URL sąrašų kūrimas; - URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo.
	Duomenų srautų kontrolės taisyklės	Kuriant duomenų srautų kontrolės taisyklės privalo būti galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Privalo būti galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.	Kuriant duomenų srautų kontrolės taisykles yra galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Yra galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.
	Duomenų srautų kontrolės taisyklių naudojimo stebėjimas	Interneto ugniasienių sprendimo narys privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).	Interneto ugniasienių sprendimo narys rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).

	VPN funkcionalumas	Interneto ugniasienių sprendimo narys privalo turėti žemiau įvardintą VPN funkcionalumą: - leisti redaguoti SSL VPN portalą; - leisti naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); - nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais; - nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) privalo būti to paties gamintojo kaip ir siūlomos ugniasienės gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. Jei siūlomas skirtingo gamintojo VPN klientas (programinė įranga) nei ugniasienės gamintojas, turi būti pateikti skirtingų gamintojų raštiški patvirtinimai, kad siūlomas sprendimas yra visiškai suderinamas bendram darbui su ugniasiene; - nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui; - nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti naršyklę naudotojo autentifikacijai SAML protokolu; - nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti interneto turinio filtravimo funkcionalumą; - nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti programinės	Interneto ugniasienių sprendimo narys turi žemiau įvardintą VPN funkcionalumą: - leidžia redaguoti SSL VPN portalą; - leidžia naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); - nuotolinio prisijungimo naudotojo VPN klientas moka dirbti IPSec ir SSL protokolais; - nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) yra to paties gamintojo kaip ir siūlomos ugniasienės gamintojas, suderinamas bendram darbui. - nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui; - nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti naršyklę naudotojo autentifikacijai SAML protokolu; - nuotolinio prisijungimo naudotojo VPN klientas palaiko interneto turinio filtravimo funkcionalumą; - nuotolinio prisijungimo naudotojo VPN klientas palaiko programinės įrangos pažeidžiamumų aptikimo funkcionalumą. Su ugniasienėmis kartu pateikiama 50 vnt. nuotolinio prisijungimo VPN kliento licencijų.

		įrangos pažeidžiamumų aptikimo funkcionalumą. Su ugniasienėmis kartu pateikiama ne mažiau kaip 50 vnt. nuotolinio prisijungimo VPN kliento licencijų. **Su ugniasiene turi būti pateikta ne mažiau kaip 50 vnt. antro faktoriaus (2FA) prisijungimo raktų.**	Su ugniasiene pateikiama 50 vnt. antro faktoriaus (2FA) prisijungimo raktų.
	IPSec kriptografijos algoritmai	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptografijos algoritmus: - AES128; - AES256.	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec kriptografijos algoritmus: - AES128; - AES256.
	IPSec maišos algoritmai	Interneto ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus: - SHA-256; - SHA-512.	Interneto ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec maišos algoritmus: - SHA-256; - SHA-512.
	Srauto ribojimas	Interneto ugniasienių sprendimo narys privalo leisti riboti srautą ir taikyti QoS per taisyklę (angl. policy).	Interneto ugniasienių sprendimo narys leidžia riboti srautą ir taikyti QoS per taisyklę (angl. policy).
	Aprašų, atnaujinimas	Ugniasienė privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.	Ugniasienė gali automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.
	Konsultacijos	Į ugniasienių kainą turi būti įskaičiuota ne mažiau kaip 25 val. konsultacijų siūlomos techninės ir programinės įrangos diegimo, administravimo, problemų šalinimo klausimais.	Į ugniasienių kainą įskaičiuota 25 val. konsultacijų siūlomos techninės ir programinės įrangos diegimo, administravimo, problemų šalinimo klausimais.
	Garantiniai įsipareigojimai, techninis aptarnavimas	Visiems techninės ir programinės įrangos komponentams, turi būti suteikta ne trumpesnė nei 60 mėn. gamintojo garantija. Gamintojo garantuojamas nemokamas garantinis	Visiems techninės ir programinės įrangos komponentams bus suteikta 60 mėn. gamintojo garantija. Gamintojo garantuojamas nemokamas garantinis

		aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus). Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas). Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). Gedimo atveju gamintojas ar tiekėjas per 1 (vieną) darbo dieną turi pakeisti sugedusį įrenginį (angl. NBD). Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis.	aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus). Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas). Yra teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). Gedimo atveju gamintojas ar tiekėjas per 1 (vieną) darbo dieną gali pakeisti sugedusį įrenginį (angl. NBD). Yra prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis.

4G ugniasienių techninės savybės

Eil. Nr.	**Parametrai**	**Minimalūs reikalavimai**	**Konkretūs tiekėjo siūlomų Prekių parametrai ir nuoroda į atitiktį pagrindžiantį dokumentą**
1.	Gamintojas	Nurodyti gamintoją.	Fortinet Inc.
2.	Produkto pavadinimas	Nurodyti produkto pavadinimą, modelį ir kodą. Kartu su pasiūlymu atskirame dokumente turi būti pateiktas pilnas komplektuojamų	**FG-40F-3G4G** FortiGate-40F-3G4G 5 x GE RJ45 ports (including 1 x WAN Port, 4 x Internal Ports) with Embedded 3G/4G/LTE wireless

		komponentų sąrašas su gamintojo kodais, kiekiais ir pavadinimais.	wan module, 3 external SMA WWAN antennas included **FC-10-F40FG-247-02-60** FortiGate-40F-3G4G 5 Year FortiCare Premium Support **SP-RACKTRAY-02** Rack mount tray for all FortiGate E series and F series desktop models and backward compatible with SP-RackTray-01. For list of compatible FortiGate products, visit Documentation website. Pridedamas dokumentas: „Produktų kodai ir kiekiai“.
3.	Surinkimo reikalavimai	4G ugniasienių įranga turi būti specializuotas aparatinis-programinis įrenginys arba modulinis įrenginys su vidiniais arba išoriniais moduliais komplektuojamas paties gamintojo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais.	4G ugniasienių įranga yra specializuotas aparatinis-programinis įrenginys. Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtais sprendimais.
4.	Korpusas	4G ugniasienės pateikiamos su visais montavimui į standartinę 19 colių įrangos montavimui skirtą spintą reikalingais priedais. (įskaitant bet neapsiribojant tvirtinimo elementais). Aukštis ne didesnis kaip 1 U.	4G ugniasienės pateikiamos su visais montavimui į standartinę 19 colių įrangos montavimui skirtą spintą reikalingais priedais. (įskaitant bet neapsiribojant tvirtinimo elementais). Aukštis 1 U.
5.	Maitinimo šaltinis	Pritaikyti 230 V, 50 – 60 Hz kintamos srovės elektros tinklui.	Pritaikytas 230 V, 50 – 60 Hz kintamos srovės elektros tinklui.
6.	Tinklo prievadai	Tinklo prievadų kiekis: - Ne mažiau, kaip 5 vnt. 1000 BaseT prievadų.	Tinklo prievadų kiekis: - 5 vnt. 1000 BaseT prievadų.

7.	Valdymo prievadai	Ne mažiau kaip 1 konsolės prievadas;	1 konsolės prievadas.
8.	3G/4G modemas	Turi turėti savyje įmontuotą modemą palaikantį ne mažiau kaip 2 SIM korteles.	Turi savyje įmontuotą modemą, palaikantį 2 SIM korteles.
9.	Palaikomi standartai / protokolai	4G ugniasienės privalo palaikyti: - kiekvienas tinklo duomenų srauto fizinis prievadas privalo palaikyti VLAN pagal 802.1Q arba lygiavertį standartą; - LACP arba lygiavertį protokolą suderinamą su HP ir Cisco komutatorių sujungimu; - bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą; - 802.3ad arba lygiavertį standartą. Turi būti galima apjungti į vieną loginę tinklo sąsają ne mažiau kaip 2 fizines sąsajas.	4G ugniasienės palaiko: - kiekvienas tinklo duomenų srauto fizinis prievadas palaiko VLAN pagal 802.1Q standartą; - LACP protokolą, suderinamą su HP ir Cisco komutatorių sujungimu; - protokolus: Netflow, IPFIX ; - 802.3ad standartą. Galima apjungti į vieną loginę tinklo sąsają 2 fizines sąsajas.
10.	VLAN palaikymas	Ne mažiau kaip 4000 VLAN žymių per įrenginį arba prievadą.	4000 VLAN žymių per įrenginį arba prievadą.
11.	Ugniasienės greitaveika	4G ugniasienių greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą – ne mažiau kaip 900 Mbps.	4G ugniasienių greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą – 990 Mbps.
12.	IPsec VPN greitaveika	Ne mažiau kaip 3 Gbps.	4,4 Gbps
13.	IPsec tunelių skaičius naudojant vartotojų / klientų prisijungimą prie ugniasienės	Ne mažiau kaip 200.	250

14.	Maksimalus sesijų skaičius vienu metu	Ne mažiau kaip 600000.	700000
15.	Maksimalus naujų sesijų skaičius per sekundę	Ne mažiau kaip 30000.	35000
16.	Suminis saugumo taisyklių skaičius per ugniasienę	Ne mažiau kaip 4000.	4000
17.	Aukšto patikimumo savybės	4G ugniasienės privalo palaikyti žemiau įvardintą funkcionalumą: - nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; - turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; - automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; - automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; - turi būti galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.	4G ugniasienės palaiko žemiau įvardintą funkcionalumą: -nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; -yra būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; -automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; -automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; -yra galimybė iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema automatiškai persijungia, jei nurodyti IP adresai tampa neaktyviais.
18.	Įrangos virtualizavimas	Turi būti funkcionalumas, leidžiantis 4G ugniasienes sudalinti į ne mažiau kaip 5 virtualius įrenginius.	Yra funkcionalumas, leidžiantis 4G ugniasienes sudalinti į 10 virtualių įrenginių.

19.	Ugniasienės darbo režimai	Ne mažiau kaip : - maršrutizavimo tarp skirtingų tinklų (OSI L3); - skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);	Darbo režimai : -maršrutizavimo tarp skirtingų tinklų (OSI L3); -skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);
20.	Maršrutizavimas	4G ugniasienės privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). Ugniasienės privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.	4G ugniasienės palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). Ugniasienė palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.
21.	PBR funkcionalumas	4G ugniasienės privalo palaikyti politika pagrįstą maršrutizavimą (angl. policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.	Palaiko politika pagrįstą maršrutizavimą (angl. policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.
22.	Dinaminio maršrutizavimo protokolai	4G ugniasienės privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: - BGP; - OSFP v2 ir v3; - RIP v2.	Palaiko žemiau įvardintus protokolus: -BGP; -OSFP v2 ir v3; -RIP v2.
23.	OSPF funkcionalumas	4G ugniasienės privalo turėti grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.	Turi grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.
24.	Srauto balansavimas	4G ugniasienės privalo gebėti balansuoti serveriams skirtą srautą. Turi būti palaikomi ne mažiau kaip Round robin ir Least session srauto balansavimo metodai.	Geba balansuoti serveriams skirtą srautą. Palaikomi Round robin ir Least session srauto balansavimo metodai.

25.	BFD palaikymas	4G ugniasienės privalo palaikyti BFD (angl. bidirectional forwarding detection) protokolą.	Palaiko BFD (angl. bidirectional forwarding detection) protokolą.
26.	IPv6 palaikymas	4G ugniasienės privalo palaikyti IPv6 protokolą.	Palaiko IPv6 protokolą.
27.	Adresų transliavimo funkcionalumas	4G ugniasienės privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: - NAT64; - statinis adresų transliavimas; - dinaminis adresų transliavimas keičiant prievadus (PAT).	Palaiko žemiau įvardintą funkcionalumą: -NAT64; -statinis adresų transliavimas; -dinaminis adresų transliavimas keičiant prievadus (PAT).
28.	Integracija su SNMP (angl. Simple Network Management Protocol) įrenginio būsenos stebėjimui	Privalo palaikyti SNMP protokolo 2 ir 3 versijas.	Palaiko SNMP protokolo 2 ir 3 versijas.
29.	Suderinamumas su Syslog	4G ugniasienės turi būti suderinamos su Syslog standartu.	Suderinamas su Syslog standartu.
30.	Žurnalinių įvykių (angl. event log) palaikymas	4G ugniasienės privalo palaikyti žemiau įvardintus žurnalinius įvykius: - sisteminiai; - administravimo; - VPN; - naudotojų autentifikavimo; - maršrutizavimo; - saugos incidentų įvykiai.	Palaiko žemiau įvardintus žurnalinius įvykius: -sisteminiai; -administravimo; -VPN; -naudotojų autentifikavimo; -maršrutizavimo; -saugos incidentų įvykiai.
31.	Žurnalinių įvykių kaupimas	4G ugniasienės privalo gebėti įvykių žurnalus siųsti į Perkančiosios organizacijos turimą nuotolinį – centralizuotą įvykių	Geba įvykių žurnalus siųsti į Perkančiosios organizacijos turimą nuotolinį – centralizuotą įvykių

		žurnalų kaupimui skirtą SIEM sistemą.	žurnalų kaupimui skirtą SIEM sistemą.
32.	Diagnostikos priemonės	Privalomas srauto / paketų nuo konkrečios sąsajos „įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	Yra srauto / paketų nuo konkrečios sąsajos „įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.
33.	Nutolusių naudotojų duomenų bazių palaikymas	4G ugniasienės privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: - LDAP; - RADIUS; - TACACS+; - dviejų lygių (angl. two-factor) autentifikaciją.	Palaiko žemiau įvardintas duomenų bazes: -LDAP; -RADIUS; -TACACS+; -dviejų lygių (angl. two-factor) autentifikaciją.
34.	Autorizacijos integracija (angl. single sign on)	4G ugniasienės privalo turėti integracijas su žemiau įvardintomis arba lygiavertėmis sistemomis: - Windows AD; - Microsoft Exchange server; - RADIUS; - 802.1x.	Turi integracijas su žemiau įvardintomis sistemomis: -Windows AD; -Microsoft Exchange server; -RADIUS; -802.1x.
35.	SSL šifruotas srautas	4G ugniasienės turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. 4G ugniasienės privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Privalo būti galimybė nurodyti kuris duomenų srautas turi būti dešifruojamas.	Dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą. Palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Yra galimybė nurodyti, kuris duomenų srautas turi būti dešifruojamas.
36.	DoS apsauga	4G ugniasienės privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.	Leidžia riboti sesijų ir paketų per sekundę skaičius jų šaltiniui arba adresatui.

37.	Aplikacijų valdymas	4G ugniasienės privalo palaikyti: - aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 2000 aplikacijų (tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienės garantinio aptarnavimo laikotarpiui; - aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.	4G ugniasienės palaiko: -aplikacijų identifikavimą ir kontrolę. Gali identifikuoti 2000 aplikacijų (tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (įskaičiuoti į pasiūlymo kainą) tokiam pačiam kaip ugniasienės garantinio aptarnavimo laikotarpiui; -aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.
38.	Duomenų srautų kontrolės taisyklės	Kuriant duomenų srautų kontrolės taisyklės privalo būti galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Privalo būti galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.	Kuriant duomenų srautų kontrolės taisykles yra galimybė nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Yra galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.
39.	Duomenų srautų kontrolės taisyklių naudojimo stebėjimas	4G ugniasienės privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).	Rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).
40.	VPN funkcionalumas	4G ugniasienės privalo turėti žemiau įvardintą VPN funkcionalumą: - leisti redaguoti SSL VPN portalą; - nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais;	4G ugniasienės turi žemiau įvardintą VPN funkcionalumą: - leidžia redaguoti SSL VPN portalą; - nuotolinio prisijungimo naudotojo VPN klientas moka dirbti IPSec ir SSL protokolais; - nuotolinio prisijungimo naudotojo SSL VPN klientas

		- nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) privalo būti to paties gamintojo kaip ir siūlomos ugniasienės gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. Jei siūlomas skirtingo gamintojo VPN klientas (programinė įranga) nei ugniasienės gamintojas, turi būti pateikti skirtingų gamintojų raštiški patvirtinimai, kad siūlomas sprendimas yra visiškai suderinamas bendram darbui su ugniasiene; - nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui;	(programinė įranga) yra to paties gamintojo kaip ir siūlomos ugniasienės gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. - nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui;
41.	IPSec kriptografijos algoritmai	4G ugniasienės privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptografijos algoritmus: - AES128; - AES256.	Palaiko žemiau įvardintus IPSec kriptografijos algoritmus: -AES128; -AES256.
42.	IPSec maišos algoritmai	4G ugniasienės privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus: - SHA-256; - SHA-512.	palaiko žemiau įvardintus IPSec maišos algoritmus: -SHA-256; -SHA-512.
43.	Srauto ribojimas	4G ugniasienės privalo leisti riboti srautą ir taikyti QoS per taisyklę (angl. policy).	Leidžia riboti srautą ir taikyti QoS per taisyklę (angl. policy).
44.	Aprašų, atnaujinimas	4G ugniasienės privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.	Gali automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.
45.	Garantiniai įsipareigojimai,	Visiems techninės ir programinės įrangos komponentams, turi būti	Visiems techninės ir programinės įrangos komponentams bus

	techninis aptarnavimas	suteikta ne trumpesnė nei 60 mėn. gamintojo garantija. Gamintojo garantuojamas nemokamas garantinis aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus). Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas). Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). Gedimo atveju gamintojas ar tiekėjas per 1 (vieną) darbo dieną turi pakeisti sugedusį įrenginį (angl. NBD). Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis.	suteikta 60 mėn. gamintojo garantija. Gamintojo garantuojamas nemokamas garantinis aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus). Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas). Suteikiama teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). Gedimo atveju gamintojas ar tiekėjas per 1 (vieną) darbo dieną gali pakeisti sugedusį įrenginį (angl. NBD). Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis.

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Nacionalinio saugumo deklaracija	1
2.	Įgaliojimas	1
3.	Deklaracija dėl prekių garantijos	2

4.	Deklaracija dėl atsarginių dalių	1
5.	Atitiktis RoHS reikalavimams	2
6.	Fortinet ISO sertifikatai	2
7.	Gamintojo raštas dėl prekių pakuotės	1
8-9	Prekių datasheet	23
10.	Prekių kodai_KONFIDENCIALU	1

1 *lentelė.* Šiame pasiūlyme yra pateikta konfidenciali informacija***:

Eil. Nr.	Pateikto dokumento pavadinimas
1.	Prekių kodai_KONFIDENCIALU

***Pildyti tuomet, jei bus pateikta konfidenciali informacija. Tiekėjas negali nurodyti, kad konfidencialus yra pasiūlymo įkainis arba, kad visas pasiūlymas yra konfidencialus.