KOMPIUTERINĖS IR PROGRAMINĖS ĮRANGOS VIEŠOJO PIRKIMO SUTARTIS

2016 m. gruodžio 6 d. Nr. (1.10-04-2)-22-483 /2016
VILNIUS

Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos (toliau – UŽSAKOVAS), atstovaujama viršininko pavaduotojo Vyganto Ivanausko, veikiančio pagal Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko 2016 m. kovo 31 d. įsakymą Nr. V-151 „Dėl įgaliojimų suteikimo“, ir UAB „ATEA“ (jungtinės veiklos partneris UAB „Santa Monica Networks“) (toliau - TIEKĖJAS), atstovaujama direktoriaus pavaduotojo Valdo Jusiaus, veikiančio pagal 2016-01-05 įgaliojimą Nr. 160105/3 (toliau abu vadinami ŠALIMIS, kiekvienas atskirai – ŠALIMI), remdamosi įvykusio Kompiuterinės ir programinės įrangos viešojo pirkimo, atlikto atviro konkurso būdu (toliau – KONKURSAS), rezultatais, vadovaudamosi Lietuvos Respublikos viešųjų pirkimų įstatymu, Lietuvos Respublikos civiliniu kodeksu, sudarė šią sutartį (toliau – SUTARTIS). TIEKĖJUI pateikti KONKURSO dokumentai ir KONKURSO DOKUMENTŲ paaiškinimai bei TIEKĖJO pateiktas pasiūlymas toliau yra vadinami „KONKURSO DOKUMENTAIS“. Jeigu SUTARTIS nenustato kitaip, SUTARTYJE naudojamos sąvokos reiškia tą patį, ką ir KONKURSO DOKUMENTUOSE naudojamos sąvokos.

1. SUTARTIES DALYKAS

1.1. SUTARTIES dalykas – Kompiuterių tinklo įranga (toliau - PREKĖS) ir jų pristatymas UŽSAKOVUI (toliau - PREKIŲ TIEKIMAS). SUTARTIES dalykas detalizuotas SUTARTIES priede Nr.1 „PREKIŲ TIEKIMO techninė specifikacija“.

1.2. Visa nauda, kurią TIEKĖJAS suteiks UŽSAKOVUI SUTARTIES galiojimo metu, vykdydamas SUTARTIES nuostatas, toliau vadinama – PREKIŲ TIEKIMO rezultatu.

1.3. SUTARTYJE nustatyti PREKIŲ TIEKIMUI ir TIEKĖJUI privalomi reikalavimai, visi KONKURSO DOKUMENTUOSE, su PREKIŲ TIEKIMU susiję, numatyti TIEKĖJUI kaip privalomi po SUTARTIES sudarymo, tačiau neįkelti į SUTARTIES tekstą reikalavimai bei kituose dokumentuose, į kuriuos daro nuorodą KONKURSO DOKUMENTAI, nustatyti PREKIŲ TIEKIMUI ir TIEKĖJUI kaip privalomi po SUTARTIES sudarymo reikalavimai, toliau SUTARTYJE vadinami REIKALAVIMAIS.

1.4. PREKIŲ TIEKIMAS turi būti vykdomas pagal REIKALAVIMUS.

2. KAINA IR ATSISKAITYMAS

2.1. UŽSAKOVAS TIEKĖJUI avanso nemoka, t.y. iš anksto su TIEKĖJU neatsiskaito.

2.2. PREKIŲ TIEKIMO kaina yra 199631,85 (šimtas devyniasdešimt devyni tūkstančiai šeši šimtai trisdešimt vienas euras aštuoniasdešimt penki centai) su pridėtinės vertės mokesčiu (toliau - PVM):

Eil. Nr.	Pavadinimas	Kiekis, vnt. (a)	Vieneto kaina, Eurais be PVM (b)	Suma, Eurais be PVM (c=a*b)
1.	A tipo kompiuterių tinklo maršrutizatorius	15	1315,00	19725,00
2.	B tipo kompiuterių tinklo maršrutizatorius	20	3513,00	70260,00
3.	Kompiuterių tinklo srauto valdymo įrenginys	2	37500,00	75000,00
			Suma iš viso be PVM:	164985,00
			PVM suma:	34646,85
			Suma iš viso Eurais su PVM:	199631,85

2.3. UŽSAKOVAS atsiskaito su TIEKĖJU už faktiškai atliktą PREKIŲ TIEKIMĄ. Mokėjimas už PREKIŲ TIEKIMO atlikimą vykdomas dalimis per 14 dienų laikotarpį nuo PVM sąskaitos faktūros ir PREKIŲ TIEKIMO dalies priėmimo - perdavimo akto pasirašymo dienos.

2.4. Pagrindas pasirašyti kiekvieną atitinkamą PREKIŲ TIEKIMO dalies priėmimo - perdavimo aktą, atsiranda tik tada, kai visi TIEKĖJO įsipareigojimai, susiję su PREKIŲ TIEKIMO dalies atlikimu, yra tinkamai įvykdyti. PREKIŲ TIEKIMAS nėra tinkamai atliktas ir PREKIŲ TIEKIMO rezultato elementas (sudėtinė dalis pagal Civilinį kodeksą) yra netinkamos kokybės, kai jis neatitinka KONKURSO DOKUMENTUOSE nustatytų reikalavimų ar neturi savybių, kurios būtinos tokiam PREKIŲ TIEKIMO rezultato elementui, kad jį būtų galima naudoti pagal įprastinę ir specialią paskirtį.

2.5. Pagrindas pateikti PVM sąskaitą faktūrą atsiranda po atitinkamo PREKIŲ TIEKIMO dalies priėmimo - perdavimo akto pasirašymo ir kai visi TIEKĖJO įsipareigojimai, susiję su tokiai PVM sąskaitai faktūrai tenkančiu PREKIŲ TIEKIMO dalies atlikimu, yra tinkamai įvykdyti.

2.6. SUTARTIES 2.3 punkte minimas atsiskaitymas įvykdomas atitinkamą sumą pervedus į SUTARTYJE nurodytą TIEKĖJO sąskaitą.

2.7. PREKIŲ TIEKIMO kaina dėl kainų lygio pasikeitimo ar pasikeitusių mokesčių neperskaičiuojama.

3. PREKIŲ TIEKIMAS

3.1. PREKIŲ TIEKIMĄ atlieka TIEKĖJAS UŽSAKOVUI.

3.2. Visi REIKALAVIMAI (visos sąlygos) susiję su PREKIŲ tiekimu, SUTARTYJE tampa TIEKĖJO įsipareigojimais.

3.3. PREKIŲ TIEKIMAS vykdomas dalimis. TIEKĖJAS įsipareigoja pradėti tiekti PREKES po SUTARTIES pasirašymo ir atitinkamo raštiško užsakymo gavimo dienos. Užsakyme nurodomi tiekiamų PREKIŲ kiekiai ir adresai, kuriais reikia pristatyti PREKES. PREKĖS turi būti pristatytos, UŽSAKOVO nurodytais adresais Lietuvos Respublikoje per 30 kalendorinių dienų nuo raštiško užsakymo gavimo dienos.

3.4. TIEKĖJAS PREKES privalės sunešti į UŽSAKOVO patalpose esančias sandėliavimo ar eksploatavimo (instaliavimo) patalpas, PREKIŲ pervežimo važtaraštis pasirašomas tik po to kai visos PREKĖS randasi UŽSAKOVO sandėliavimo patalpose. PREKIŲ TIEKIMO dalies priėmimo - perdavimo aktas ir PVM sąskaita faktūra pasirašomi po to kai PREKĖS pilnai sumontuotos, sukonfigūruotos ir patikrintas jų darbingumas, jei tokias paslaugas numato SUTARTIS.

3.5. PREKIŲ TIEKIMO atlikimas bus forminamas PREKIŲ TIEKIMO dalies priėmimo - perdavimo aktu, kurį (dviem egzemplioriais) pasirašo TIEKĖJO ir UŽSAKOVO įgalioti atstovai.

3.6. TIEKĖJAS turi pateikti visą, siūlomoms PREKĖMS, gamintojo numatytą dokumentaciją. Dokumentacija turi būti lietuvių arba anglų kalba.

3.7. Visos PREKĖS turi būti naujos, nenaudotos, pristatomos originaliame gamykliniame įpakavime „brand new“, gamykliškai atnaujinti “renew“, „refurbished“, „remarked“ komponentai neleistini.

3.8. Į visus PREKIŲ komplektus turi įeiti visi reikalingi kabeliai, adapteriai ir kitos sudedamosios dalys bei medžiagos, reikalingos sujungti perkamas PREKES, kaip tai numato gamintojas. Įrangos elektros maitinimas turi būti pritaikytas -220V, 50 Hz maitinimo įtampai. Maitinimo kabeliai turi tikti Lietuvoje naudojamiems kištukiniams lizdams.

3.9. PREKIŲ kiekis, nurodytas SUTARTYJE, yra tik orientacinis skaičius ir negali būti pagrindas reikalauti iš UŽSAKOVO pirkti visą numatomą PREKIŲ kiekį. PREKIŲ pirkimas priklauso tiktai nuo UŽSAKOVO poreikių ir valios, todėl SUTARTIMI UŽSAKOVAS neįsipareigoja pirkti viso SUTARTYJE nurodyto, UŽSAKOVO planuojamo pirkti PREKIŲ kiekio.

3.10. TIEKĖJO atstovai PREKIŲ TIEKIMO klausimais su UŽSAKOVO atstovais bendrauja lietuvių kalba.

4. ŠALIŲ ATSAKOMYBĖ

4.1. ŠALYS privalo susilaikyti nuo bet kokių veiksmų, kurie galėtų pakenkti kitai ŠALIAI.

4.2. Jeigu TIEKĖJAS neįvykdo arba netinkamai įvykdo SUTARTYJE numatytus įsipareigojimus, UŽSAKOVAS turi teisę pareikalauti atlyginti SUTARTIES sąlygų nevykdymu ar netinkamu vykdymu jam padarytus nuostolius.

4.3. Už TIEKĖJO vėlavimą atlikti atitinkamą PREKIŲ TIEKIMO dalį numatomi delspinigiai - 0,06 procento nuo PREKIŲ TIEKIMO dalies (užsakymo) kainos, už kiekvieną pavėluotą dieną, bet ne daugiau kaip 5 procentai nuo SUTARTIES vertės.

4.4. Už UŽSAKOVO vėlavimą atsiskaityti su TIEKĖJU numątomi delspinigiai - 0,06 procento nuo vėluojamos apmokėti sumos, už kiekvieną pavėluotą dieną, bet ne daugiau kaip 5 procentai nuo SUTARTIES vertės. UŽSAKOVUI delspinigiai neskaičiuojami, jeigu vėlavimas atsiranda dėl netinkamo UŽSAKOVO finansavimo.

4.5. Jeigu TIEKĖJAS savo iniciatyva anksčiau laiko nori nutraukti SUTARTĮ, TIEKĖJAS gali ją nutraukti tik raštu įspėjęs UŽSAKOVĄ prieš 10 kalendorinių dienų. TIEKĖJAS taip pat įsipareigoja per 5 darbo dienas nuo UŽSAKOVO reikalavimo kompensuoti UŽSAKOVUI visus nuostolius, atsiradusius dėl tokio SUTARTIES nutraukimo.

4.6. TIEKĖJUI pritaikytų pagal SUTARTĮ sankcijų sumos gali būti dengiamos iš priklausančių TIEKĖJUI pagal SUTARTĮ gautinų sumų.

4.7. Jeigu naudojimosi PREKIŲ TIEKIMO rezultatu metu paaiškės, kad UŽSAKOVUI atitenkanti TIEKĖJO perduota susijusi su PREKIŲ TIEKIMU dokumentacija yra nepilna, ir jos nepakanka, kad

įvykdyti kokį nors iš SUTARTYJE numatytų PREKIŲ TIEKIMO tikslų, su tuo susijusius UŽSAKOVO nuostolius padengs TIEKĖJAS.

5. PREKIŲ TIEKIMO KOKYBĖ

5.1. PREKIŲ TIEKIMO kokybė turi atitikti REIKALAVIMUS ir Civilinio kodekso nuostatas.

5.2. Siūlomų PREKIŲ kokybė privalo atitikti Lietuvos Respublikoje ir Europos Sąjungoje galiojančius standartus. Siūlomos PREKĖS turi būti sertifikuotos naudojimui Lietuvos Respublikoje, jei tai numato Lietuvos Respublikos teisės aktai.

5.3. Visoms PREKĖMS ar jų dalims, elementams (sudėtinėms dalims, pagal Civilinį kodeksą), kuriems pagal Civilinį kodeksą būtų galimybė sutartiniu įsipareigojimu suteikti kokybės garantijos terminą, pirkimo sutartimi suteikiamas SUTARTYJE ir Civiliniame kodekse numatytas kokybės garantijos terminas. TIEKĖJO atsakomybė už kokybės garantiją užtikrinama taip, kaip numato SUTARTIS ir Civilinis kodeksas, t.y. nėra nustatyti jokie kiti TIEKĖJO suteikiamos kokybės garantijos užtikrinimo ar atsakomybės už kokybės garantiją apribojimai. PREKIŲ ir jų dalių, elementų kokybės garantijos termino eiga prasideda nuo su tokių PREKIŲ ar jų dalimi, elementais susijusios PVM sąskaitos – faktūros pasirašymo dienos. Kokybės garantijos termino eiga sustabdoma laikotarpiui nuo pranešimo apie PREKIŲ ar jų dalių, elementų trūkumą iki tokio PREKIŲ ar jų dalių, elementų trūkumo pašalinimo momento. Jeigu tam tikroms PREKĖMS ar jų dalims, elementams KONKURSO DOKUMENTAI reikalauja suteikti, arba PREKIŲ ar jų dalių gamintojas standartiškai suteikia ilgesnį kokybės garantijos terminą, taikomas toks ilgesnis kokybės garantijos terminas.

5.4. Perkamos įrangos gamintojo garantinis aptarnavimas atliekamas gamintojo sertifikuotame techniniame centre, apie tai turi būti skelbiama gamintojo internetiniame portale.

6. SUTARTIES GALIOJIMAS, PAKEITIMAS IR NUTRAUKIMAS

6.1. SUTARTIS įsigalioja nuo jos pasirašymo dienos ir galioja iki pilno ŠALIŲ įsipareigojimų įvykdymo.

6.2. SUTARTIS sudaroma 1 metų laikotarpiui.

6.3. UŽSAKOVAS turi teisę nutraukti SUTARTĮ, jeigu TIEKĖJAS SUTARTIES galiojimo laikotarpiu pagal galiojančius teisės aktus praranda teisę užsiimti ūkine komercine ar kitokia, būtina PREKIŲ TIEKIMO atlikimui, veikla.

6.4. Jeigu TIEKĖJAS netinkamai vykdo SUTARTĮ, UŽSAKOVAS gali ją nutraukti įspėjęs TIEKĖJĄ prieš 10 kalendorinių dienų.

6.5. Visi SUTARTIES pakeitimai, papildymai, priedai galioja, jeigu jie yra sudaryti raštu ir patvirtinti abiejų ŠALIŲ įgaliotų atstovų parašais.

6.6. SUTARTIES sąlygos SUTARTIES galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias SUTARTIES sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 3 straipsnyje nustatyti principai ir tikslai ir yra gautas Viešųjų pirkimų tarnybos sutikimas.

6.7. UŽSAKOVAS pasilieka teisę atsisakyti visų PREKIŲ ar PREKIŲ dalies pirkimo, jeigu jis neturės pakankamo, nuo jo nepriklausančio finansavimo, arba PREKIŲ ar PREKIŲ dalies pirkimo nereikės vykdant įstatymais jam priskirtas funkcijas, arba dėl kitų priežasčių. Šiuo atveju jokios sankcijos, numatytos SUTARTYJE UŽSAKOVUI netaikomos. Minėto atsisakymo atveju UŽSAKOVAS sumoka tik už iki atsisakymo faktiškai pateiktą pagal SUTARTĮ PREKIŲ dalį.

6.8. REIKALAVIMUOSE numatytas PIRKIMO SUTARTIES ĮVYKDYMO UŽTIKRINIMAS yra neatsiejamas SUTARTIES priedas. Jeigu PIRKIMO SUTARTIES ĮVYKDYMO UŽTIKRINIMAS pasibaigia anksčiau, nei yra pilnai įvykdomi TIEKĖJO įsipareigojimai pagal SUTARTĮ, TIEKĖJAS privalo PIRKIMO SUTARTIES ĮVYKDYMO UŽTIKRINIMĄ pratęsti. Atlikti PREKIŲ TIEKIMĄ esant negaliojančiam PIRKIMO SUTARTIES ĮVYKDYMO UŽTIKRINIMUI TIEKĖJUI draudžiama, tačiau tai nestabdo PRIEKIŲ TIEKIMO terminų.

7. NENUGALIMOS JĖGOS APLINKYBĖS (FORCE MAJEURE)

7.1. Nė viena iš SUTARTIES ŠALIŲ neatsako už prisiimtų įsipareigojimų visišką ar dalinį neįvykdymą, jeigu ji įrodo, kad įsipareigojimų neįvykdė dėl nenugalimos jėgos aplinkybių (Force Majeure).

7.2. ŠALIS, kuri dėl nenugalimos jėgos aplinkybių negali įvykdyti savo įsipareigojimų, privalo nedelsdama, bet ne vėliau kaip per 5 dienas nuo aplinkybių atsiradimo ar paaiškėjimo, raštu informuoti apie tai kitą ŠALĮ. Pranešime išdėstyti faktai turi būti patvirtinti kompetentingos valdžios institucijos. Jeigu nenugalimos jėgos aplinkybės užsitęsia ilgiau kaip tris mėnesius, ŠALYS tarpusavio susitarimu gali nutraukti SUTARTĮ.

7.3. Nenugalimos jėgos aplinkybėmis yra laikomos aplinkybės, apibrėžtos Civilinio kodekso 6.212 straipsnyje ir Atleidimo nuo atsakomybės esant nenugalimos jėgos aplinkybėms taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840.

8. KITOS NUOSTATOS

8.1. SUTARTIES punktų pavadinimai nustatomosios galios neturi – jų tikslas yra tik palengvinti SUTARTIES nuostatų paiešką.

8.2. Kilus tarp ŠALIŲ ginčams dėl SUTARTIES, jie sprendžiami ŠALIŲ derybomis, o nesusitarus – Lietuvos Respublikos teisės aktų nustatyta tvarka.

8.3. SUTARTIS sudaryta 2 egzemplioriais, turinčiais vienodą juridinę galią. Kiekvienai iš ŠALIŲ įteikiamas vienas SUTARTIES egzempliorius.

8.4. SUTARTIS turi šį priedą - Priedas Nr. 1 „PREKIŲ TIEKIMO techninė specifikacija".

9. ŠALIŲ REKVIZITAI

9.1. ŠALYS privalo nedelsdamos raštu pranešti viena kitai apie SUTARTYJE nurodytų rekvizitų pasikeitimą.

9.2. ŠALIŲ rekvizitai yra tokie:

UŽSAKOVAS:
Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos
Vasario 16-sios g. 14, LT-01514 Vilnius
Telefonas: (8 5) 268 7800
Faksas: (8 5) 212 5604
Įmonės kodas: 188659752
Atsiskaitomoji sąskaita:
LT64 7044 0600 0032 5933
AB SEB bankas

Viršininko pavaduotojas

Vygantas Ivanauskas

TIEKĖJAS:
UAB „ATEA"
J. Rutkausko g. 6, Vilnius
Įmonės kodas: 122588443
PVM kodas LT225884413
Telefonas: (8 5) 239 7830
El. paštas: info@atea.lt
Atsiskaitomoji sąskaita:
LT03 2140 0300 0132 7814
Nordea Bank AB Lietuvos skyrius

Direktoriaus pavaduotojas

Valdas Jusius

2016-12-06 sutarties Nr. (1.10-04-2)-22-183/a
Priedas Nr. 1

PREKIŲ TIEKIMO techninė specifikacija

Kompiuterių tinklo įranga.

Techniniai reikalavimai:

1. **A tipo kompiuterių tinklo maršrutizatorius:**

Eil. Nr.	Parametro pavadinimas	Reikalaujamos parametrų reikšmės	Siūlomos parametrų reikšmės
1.	Gamintojas ir modelis	Nurodyti	HPE Aruba 2920 24G POE+ Switch
2.	Konstrukcija	Turi būti montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis.	Atitinka. Yra montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis.
3.	Elektros maitinimas	220 V AC.	Atitinka. 220 V AC.
4.	Prievadai	Turi būti ne mažiau 24 10/100/1000Base-TX prievadų su automatiniu greitaveikos atpažinimu, su IEEE 802.3at PoE+ (kiekviename RJ45 10/100/1000Base-TX prievade). Turi būti ne mažiau kaip 4 dvigubos paskirties prievadai, kurie funkcionuoja kaip RJ45 10/100/1000BaseT arba SFP 1000BaseX. Turi būti galimybė komutatorių papildyti moduliu, palaikančiu 10GBASE-T arba 10G SFP+ sąsajas. Galimybė plėsti iki 4 vnt. 10Gb jungčių.	Atitinka. 24 10/100/1000Base-TX prievadų su automatiniu greitaveikos atpažinimu, su IEEE 802.3at PoE+ (kiekviename RJ45 10/100/1000Base-TX prievade). Yra 4 dvigubos paskirties prievadai, kurie funkcionuoja kaip RJ45 10/100/1000BaseT arba SFP 1000BaseX. Yra galimybė komutatorių papildyti moduliu, palaikančiu 10GBASE-T arba 10G SFP+ sąsajas. Yra galimybė plėsti iki 4 vnt. 10Gb jungčių.
5.	Prievadų elektros maitinimas	Turi būti ne mažiau kaip 15,4 W galios kiekvienam komutatoriaus PoE+ prievadui aptarnauti.	Atitinka. Yra ne mažiau kaip 15,4 W galios kiekvienam komutatoriaus PoE+ prievadui aptarnauti.
6.	Našumas	Turi būti vidinis L2 našumas ne mažiau 126 Gb/s.	Atitinka. Yra vidinis L2 našumas ne mažiau 126 Gb/s.
7.	Plėtros galimybės	Turi būti galimybė komutatorių papildyti grupavimo (angl. stacking) moduliu.	Atitinka. Yra galimybė komutatorių papildyti grupavimo (angl. stacking) moduliu.
8.	Palaikomi standartai	IEEE 802.1D Spanning-Tree; IEEE 802.1w Rapid Spanning Tree; IEEE 802.1s MSTP; IEEE 802.1Q VLAN; IEEE802.1p CoS; IEEE 802.3ad prievadų loginis apjungimas; IEEE 802.1ab su LLDP-MED plėtiniu; IEEE 802.1v; IEEE 802.3af Power over Ethernet; IEEE 802.3at Power over Ethernet.	Atitinka. IEEE 802.1D Spanning-Tree; IEEE 802.1w Rapid Spanning Tree; IEEE 802.1s MSTP; IEEE 802.1Q VLAN; IEEE802.1p CoS; IEEE 802.3ad prievadų loginis apjungimas; IEEE 802.1ab su LLDP-MED plėtiniu; IEEE 802.1v; IEEE 802.3af Power over Ethernet; IEEE 802.3at Power over Ethernet.
9.	Srauto valdymas	Turi palaikyti nemažiau 1022 VLAN vienu metu. Turi būti galimybė kurti	Atitinka. Palaiko nemažiau 1022 VLAN vienu metu. Yra galimybė kurti VLAN

		VLAN pagal fizinį prievadą; IEEE 802.1Q VLAN ID palaikymas iki 4094. Turi palaikyti ne mažiau 16000 fizinių MAC adresų. Turi būti „voice“ VLAN palaikymas (naudojant LLDP-MED automatinis VLAN priskirimas prievadui su pajungtu IP telefonu). Turi būti „multicast“ srauto valdymas IGMP snooping. Turi būti „broadcast“ srauto valdymo mechanizmas.	pagal fizinį prievadą; IEEE 802.1Q VLAN ID palaikymas iki 4094. Palaiko ne mažiau 16000 fizinių MAC adresų. Yra „voice“ VLAN palaikymas (naudojant LLDP-MED automatinis VLAN priskirimas prievadui su pajungtu IP telefonu). Yra „multicast“ srauto valdymas IGMP snooping. Yra „broadcast“ srauto valdymo mechanizmas.
10.	Saugumo funkcijos	Vartotojų autentifikavimas IEEE802.1X protokolu ir WEB sąsajos pagalba (web-based authentication); Galimybė autentifikuoti vartotoją pagal MAC adresą; Galimybė autentifikuoti nemažiau dviejų vartotojų per prievadą naudojant skirtingus autentifikavimo metodus (IEEE802.1/Web based/Mac based); TACACS+, RADIUS, SSH, SSL, SFTP, Telnet, SNTP, Syslog protokolų palaikymas; Galimybė apriboti prisijungimą pagal MAC adresus (MAC address locking); BPDU paketų apsauga (BPDU Guard); STP apsauga (STP Root Guard); Tinklo prieigos resursų valdymas.	Atitinka. Vartotojų autentifikavimas IEEE802.1X protokolu ir WEB sąsajos pagalba (web-based authentication); Yra galimybė autentifikuoti vartotoją pagal MAC adresą; Yra galimybė autentifikuoti nemažiau dviejų vartotojų per prievadą naudojant skirtingus autentifikavimo metodus (IEEE802.1/Web based/Mac based); TACACS+, RADIUS, SSH, SSL, SFTP, Telnet, SNTP, Syslog protokolų palaikymas; Yra galimybė apriboti prisijungimą pagal MAC adresus (MAC address locking); BPDU paketų apsauga (BPDU Guard); STP apsauga (STP Root Guard); Tinklo prieigos resursų valdymas.
11.	Valdymo galimybės	Turi būti valdymas: SNMP v1/v2/v3, Telnet, SSH v1/v2, Command Line Interface (CLI), WEB interface. Operacinės sistemos ir konfigūracijos persiuntimas TFTP protokolu. Turi būti srautų stebėjimo funkcija RMON. Turi būti galimybė priskirti prievadams administratoriui priimtinus vardus. Turi būti dviejų vidinės programinės įrangos “firmware” versijų laikymas Prekėje (dual flash image).	Atitinka. Yra valdymas: SNMP v1/v2/v3, Telnet, SSH v1/v2, Command Line Interface (CLI), WEB interface. Operacinės sistemos ir konfigūracijos persiuntimas TFTP protokolu. Yra srautų stebėjimo funkcija RMON. Yra galimybė priskirti prievadams administratoriui priimtinus vardus. Yra dviejų vidinės programinės įrangos “firmware” versijų laikymas Prekėje (dual flash image).
12.	Garantiniai įsipareigojimai	Prekėms turi būti suteikta ne trumpesnė kaip 3 (trejų) metų garantija, kurios metu: - turi būti nemokamas programinės įrangos klaidų šalinimas garantiniu laikotarpiu. Programinės įrangos klaidų šalinimas turi būti vykdomas kaip įmanoma per trumpesnį laiko periodą, bet ne vėliau kaip per 10 (dešimt) darbo dienas nuo Pirkėjo	Atitinka. Prekėms yra suteikta 3 (trejų) metų garantija, kurios metu: - Nemokamas programinės įrangos klaidų šalinimas garantiniu laikotarpiu. Programinės įrangos klaidų šalinimas yra vykdomas kaip įmanoma per trumpesnį laiko periodą, bet ne vėliau kaip per 10 (dešimt) darbo dienas nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos; - Yra programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisiuntimas iš gamintojo puslapio;

		pranešimo Pardavėjui išsiuntimo dienos; - turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisiuntimas iš gamintojo puslapio; garantiniu laikotarpiu sugedęs komutatorius, jo moduliai ir dalys privalo būti pakeisti ne ilgiau kaip per 10 (dešimt) darbo dienų nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos.	garantiniu laikotarpiu sugedęs komutatorius, jo moduliai ir dalys bus pakeisti ne ilgiau kaip per 10 (dešimt) darbo dienų nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos.

2. B tipo kompiuterių tinklo maršrutizatorius:

Eil. Nr.	Parametro pavadinimas	Reikalaujamos parametrų reikšmės	Siūlomos parametrų reikšmės
1.	Gamintojas ir modelis	Nurodyti	HPE Aruba 2920 48G POE+ 740W Switch
2.	Konstrukcija	Turi būti montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis.	Atitinka. Yra montuojamas į 19" komutacinę spintą, pateikiamas su montavimo detalėmis.
3.	Elektros maitinimas	220 V AC.	Atitinka. 220 V AC.
4.	Prievadai	Turi būti ne mažiau 48 10/100/1000Base-TX prievadų su automatiniu greitaveikos atpažinimu, su IEEE 802.3at PoE+ (kiekviename RJ45 10/100/1000Base-TX prievade). Turi būti galimybė komutatorių papildyti moduliu, palaikančiu 10 GBASE-T arba 10 G SFP+ sąsajas. Galimybė plėsti iki 4 vnt. 10 Gb jungčių.	Atitinka. 48 10/100/1000Base-TX prievadų su automatiniu greitaveikos atpažinimu, su IEEE 802.3at PoE+ (kiekviename RJ45 10/100/1000Base-TX prievade). Yra galimybė komutatorių papildyti moduliu, palaikančiu 10 GBASE-T arba 10 G SFP+ sąsajas. Galimybė plėsti iki 4 vnt. 10 Gb jungčių.
5.	Prievadų elektros maitinimas	Turi būti ne mažiau kaip 15,4 W galios kiekvienam komutatoriaus PoE+ prievadui aptarnauti.	Atitinka. Yra ne mažiau kaip 15,4 W galios kiekvienam komutatoriaus PoE+ prievadui aptarnauti.
6.	Našumas	Turi būti vidinis L2 našumas ne mažiau 176 Gb/s.	Atitinka. Yra vidinis L2 našumas ne mažiau 176 Gb/s.
7.	Plėtros galimybės	Turi būti galimybė komutatorių papildyti grupavimo (angl. stacking) moduliu.	Atitinka. Yra galimybė komutatorių papildyti grupavimo (angl. stacking) moduliu.
8.	Palaikomi standartai	IEEE 802.1D Spanning-Tree; IEEE 802.1w Rapid Spanning Tree; IEEE 802.1s MSTP; IEEE 802.1Q VLAN; IEEE802.1p CoS; IEEE 802.3ad prievadų loginis apjungimas; IEEE 802.1ab su LLDP-MED plėtiniu; IEEE 802.1v; IEEE 802.3af Power over Ethernet; IEEE 802.3at Power over Ethernet.	Atitinka. IEEE 802.1D Spanning-Tree; IEEE 802.1w Rapid Spanning Tree; IEEE 802.1s MSTP; IEEE 802.1Q VLAN; IEEE802.1p CoS; IEEE 802.3ad prievadų loginis apjungimas; IEEE 802.1ab su LLDP-MED plėtiniu; IEEE 802.1v; IEEE 802.3af Power over Ethernet; IEEE 802.3at Power over Ethernet.
9.	Srauto valdymas	Turi palaikyti nemažiau 1022 VLAN vienu metu. Turi būti galimybė kurti	Atitinka. Palaiko nemažiau 1022 VLAN vienu metu. Yra galimybė kurti VLAN

		VLAN pagal fizinį prievadą; IEEE 802.1Q VLAN ID palaikymas iki 4094. Turi palaikyti ne mažiau 16000 fizinių MAC adresų. Turi būti „voice" VLAN palaikymas (naudojant LLDP-MED automatinis VLAN priskirimas prievadui su pajungtu IP telefonu). Turi būti „multicast" srauto valdymas IGMP snooping. Turi būti „broadcast" srauto valdymo mechanizmas.	pagal fizinį prievadą; IEEE 802.1Q VLAN ID palaikymas iki 4094. Palaiko ne mažiau 16000 fizinių MAC adresų. Yra „voice" VLAN palaikymas (naudojant LLDP-MED automatinis VLAN priskirimas prievadui su pajungtu IP telefonu). Yra „multicast" srauto valdymas IGMP snooping. Yra „broadcast" srauto valdymo mechanizmas.
10.	Saugumo funkcijos	Vartotojų autentifikavimas IEEE802.1X protokolu ir WEB sąsajos pagalba (web-based authentication); Galimybė autentifikuoti vartotoją pagal MAC adresą; Galimybė autentifikuoti nemažiau dviejų vartotojų per prievadą naudojant skirtingus autentifikavimo metodus (IEEE802.1/Web based/Mac based); TACACS+, RADIUS, SSH, SSL, SFTP, Telnet, SNTP, Syslog protokolų palaikymas; Galimybė apriboti prisijungimą pagal MAC adresus (MAC address locking); BPDU paketų apsauga (BPDU Guard); STP apsauga (STP Root Guard); Tinklo prieigos resursų valdymas.	Atitinka. Vartotojų autentifikavimas IEEE802.1X protokolu ir WEB sąsajos pagalba (web-based authentication); Galimybė autentifikuoti vartotoją pagal MAC adresą; Galimybė autentifikuoti nemažiau dviejų vartotojų per prievadą naudojant skirtingus autentifikavimo metodus (IEEE802.1/Web based/Mac based); TACACS+, RADIUS, SSH, SSL, SFTP, Telnet, SNTP, Syslog protokolų palaikymas; Galimybė apriboti prisijungimą pagal MAC adresus (MAC address locking); BPDU paketų apsauga (BPDU Guard); STP apsauga (STP Root Guard); Tinklo prieigos resursų valdymas.
11.	Valdymo galimybės	Turi būti valdymas: SNMP v1/v2/v3, Telnet, SSH v1/v2, Command Line Interface (CLI), WEB interface. Operacinės sistemos ir konfigūracijos persiuntimas TFTP protokolu. Turi būti srautų stebėjimo funkcija RMON. Turi būti galimybė priskirti prievadams administratoriui priimtinus vardus. Turi būti dviejų vidinės programinės įrangos "firmware" versijų laikymas Prekėje (dual flash image).	Atitinka. Yra valdymas: SNMP v1/v2/v3, Telnet, SSH v1/v2, Command Line Interface (CLI), WEB interface. Operacinės sistemos ir konfigūracijos persiuntimas TFTP protokolu. Yra srautų stebėjimo funkcija RMON. Yra galimybė priskirti prievadams administratoriui priimtinus vardus. Yra dviejų vidinės programinės įrangos "firmware" versijų laikymas Prekėje (dual flash image).
12.	Garantiniai įsipareigojimai	Prekėms turi būti suteikta ne trumpesnė kaip 3 (trejų) metų garantija, kurios metu: - turi būti nemokamas programinės įrangos klaidų šalinimas garantiniu laikotarpiu. Programinės įrangos klaidų šalinimas turi būti vykdomas kaip įmanoma per trumpesnį laiko periodą, bet ne vėliau kaip per 10 (dešimt) darbo dienas nuo Pirkėjo	Atitinka. Prekėms suteikta 3 (trejų) metų garantija, kurios metu: - Nemokamas programinės įrangos klaidų šalinimas garantiniu laikotarpiu. Programinės įrangos klaidų šalinimas vykdomas kaip įmanoma per trumpesnį laiko periodą, bet ne vėliau kaip per 10 (dešimt) darbo dienas nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos; - Yra programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisiuntimas iš gamintojo puslapio;

		pranešimo Pardavėjui išsiuntimo dienos; - turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisiuntimas iš gamintojo puslapio; garantiniu laikotarpiu sugedęs komutatorius, jo moduliai ir dalys privalo būti pakeisti ne ilgiau kaip per 10 (dešimt) darbo dienų nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos.	garantiniu laikotarpiu sugedęs komutatorius, jo moduliai ir dalys bus pakeisti ne ilgiau kaip per 10 (dešimt) darbo dienų nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos.

3. Kompiuterių tinklo srauto valdymo įrenginys:

Eil. Nr.	Parametro pavadinimas	Reikalaujamos parametrų reikšmės	Siūlomos parametrų reikšmės
1.	Gamintojas ir modelis	Nurodyti	Palo Alto Networks PA-3020
2.	Konstrukcija	Įrenginiai turi būti montuojami į 19 colių komutacinę spintą (montavimui reikalingos detalės turi būti pateiktos kartu su įranga); Įrenginio aukštis neturi viršyti 1 RU; Jei siūlomas programinis sprendimas, tai kartu su programine įranga turi būti pateikiami 2 vnt. serverių kurie atitiktų 3 – 8 punktuose nurodytus reikalavimus.	Įrenginiai montuojami į 19 colių komutacinę spintą (montavimui reikalingos detalės pateiktos kartu su įranga); Įrenginio aukštis 1 RU.
3.	Paskirtis	specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, srautų turinio kontrolę;	specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, srautų turinio kontrolę;
4.	Diskai	įrenginiuose naudojami kietieji diskai, įrenginiai turi būti pateikiami su SSD tipo arba lygiaverčiais diskais; diskai turi būti ne mažesnės kaip 120 GB talpos;	įrenginiuose naudojami kietieji diskai, įrenginiai pateikiami su SSD tipo; diskai 120 GB talpos;
5.	Tinklo prievadai	kiekvienas įrenginys turi turėti ne mažiau kaip 12 10/100/1000 Base-T Ethernet prievadų;	kiekvienas įrenginys turi 12 10/100/1000 Base-T Ethernet prievadų;
6.	Plėtros galimybės	į kiekvieną įrenginį turi būti galimybė įdiegti ne mažiau kaip 6 1 G papildomus optinius prievadus (angl. *SFP*);	į kiekvieną įrenginį yra galimybė įdiegti 8 1 G papildomus optinius prievadus (angl. *SFP*);
7.	Apjungimo galimybės	kiekvienas įrenginys turi turėti ne mažiau kaip 2 dedikuotus 10/100/1000 Base-T tinklo prievadus, skirtus apjungti įrenginius į aukšto patikimumo sistemą;	kiekvienas įrenginys turi 2 dedikuotus 10/100/1000 Base-T tinklo prievadus, skirtus apjungti įrenginius į aukšto patikimumo sistemą;
8.	Valdymas	kiekvienas įrenginys valdymui turi turėti ne mažiau kaip vieną konsolės prievadą ir vieną atskirą 10/100/1000 Base-T Ethernet prievadą;	kiekvienas įrenginys valdymui turi vieną konsolės prievadą ir vieną atskirą 10/100/1000 Base-T Ethernet prievadą;
9.	Aukšto patikimumo funkcijos	sprendimas turi mokėti dirbti Aktyvus/Pasyvus (angl. *Active/Pasive*) ir Aktyvus/Aktyvus (angl. *Active/Active*) režimais;	sprendimas moka dirbti Aktyvus/Pasyvus (angl. *Active/Pasive*) ir Aktyvus/Aktyvus (angl. *Active/Active*) režimais;

		sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį; konfigūracija tarp aukšto patikimumo narių turi būti automatiškai sinchronizuojama; aukšto patikimumo sistema turi užtikrinti, kad persijungimo metu aktyvios sesijos nenutrūktų; turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būna aktyvus; aukšto patikimumo sistemos nariai turi stebėti tinklo prievadų, duomenų perdavimo krypties (angl. *path*) būsenas; turi būti galimybė iš kiekvieno nario stebėti ar atsiliepia nurodyti IP adresai; sistema turi automatiškai persijungti jei nurodyti IP adresai neatsiliepia.	sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį; konfigūracija tarp aukšto patikimumo narių automatiškai sinchronizuojama; aukšto patikimumo sistema užtikrina, kad persijungimo metu aktyvios sesijos nenutrūktų; galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būna aktyvus; aukšto patikimumo sistemos nariai stebi tinklo prievadų, duomenų perdavimo krypties (angl. *path*) būsenas; galimybė iš kiekvieno nario stebėti ar atsiliepia nurodyti IP adresai; sistema gali automatiškai persijungti jei nurodyti IP adresai neatsiliepia.
10.	Įrenginio našumas	ugniasienės ir programų kontrolės greitaveika ne mažesnė kaip 1.8 Gbps.; vartotojų skaičius neribotas; įrenginio greitaveika naudojant apsaugą nuo grėsmių (apsauga nuo virusų, piktybinių kodų, įsilaužimų, pažeidžiamumų aptikimas) ne mažesnis kaip 1 Gbps.; IPSEC VPN greitaveika ne mažesnė kaip 450 Mbps.; ne mažiau kaip 900 IPSec VPN tunelių/tunelių sąsajų; ne mažiau kaip 900 konkurentinių SSL VPN vartotojų; ne mažiau kaip 200000 konkurentinių sesijų; ne mažiau kaip 45000 naujų sesijų per sekundę; ne mažiau kaip 4000 VLAN įrenginiui/sąsajai; turi būti galimybė sukonfigūruoti ne mažiau kaip 10 virtualių maršruto parinktuvų; virtualūs maršruto parinktuvai turi turėti atskiras maršrutizavimo lenteles; turi būti galimybė sukurti po kelis virtualius maršruto parinktuvus kiekvienoje virtualioje sistemoje; turi būti galimybė sukonfigūruoti ne mažiau kaip 35 saugumo zonas; turi būti galimybė plėsti virtualių sistemų skaičių iki ne mažiau kaip 5. Plėtimo galimybė gali būti realizuojama įsigyjant papildomas licencijas.	ugniasienės ir programų kontrolės greitaveika 2 Gbps.; vartotojų skaičius neribotas; įrenginio greitaveika naudojant apsaugą nuo grėsmių (apsauga nuo virusų, piktybinių kodų, įsilaužimų, pažeidžiamumų aptikimas) 1 Gbps.; IPSEC VPN greitaveika 500 Mbps.; 1000 IPSec VPN tunelių/tunelių sąsajų; 1000 konkurentinių SSL VPN vartotojų; 200000 konkurentinių sesijų; 50000 naujų sesijų per sekundę; 4000 VLAN įrenginiui/sąsajai; galimybė sukonfigūruoti 10 virtualių maršruto parinktuvų; virtualūs maršruto parinktuvai turi atskiras maršrutizavimo lenteles; galimybė sukurti po kelis virtualius maršruto parinktuvus kiekvienoje virtualioje sistemoje; galimybė sukonfigūruoti 40 saugumo zonas; galimybė plėsti virtualių sistemų skaičių iki 6. Plėtimo galimybė realizuojama įsigyjant papildomas licencijas.
11.	**Įrenginio palaikomos funkcijos**	darbo režimai: - skaidrus (visiškai neįtakojantis išorinius tinklo L2/L3 nustatymus); - maršrutizavimo (L2, L3);	darbo režimai: - skaidrus (visiškai neįtakojantis išorinius tinklo L2/L3 nustatymus); - maršrutizavimo (L2, L3); pasyvaus stebėjimo (angl. *Sniffer/TAP*).

		pasyvaus stebėjimo (angl. *Sniffer/TAP*). Turi būti galimybė įrenginį sukonfigūruoti taip, kad jis vienu metu, vienoje sistemoje, dirbtų visais palaikomais darbo režimais; turi palaikyti 802.3ad.; turi būti galimybė apjungti į vieną loginę tinklo sąsają nemažiau kaip 8 fizines sąsajas; loginė sąsaja gali būti naudojama kaip L2 arba L3 lygio sąsaja; turi palaikyti LACP protokolą; įrenginys turi palaikyti IEEE 802.1q protokolą; VLAN sąsajos gali būti kuriamos tinklo sąsajoms, dirbančioms L2 ir L3 lygyje; įrenginys turi palaikyti ne mažesnius kaip 8192 baitų dydžio Jumbo paketus; įrenginys turi palaikyti statinį IP maršrutizavimą, dinaminius maršrutizavimo protokolus: BGP, OSPFv2, OSPFv3, RIPv2; įrenginys turi palaikyti PPPoE (angl. *Point-to-Point Protocol over Ethernet*); įrenginys turi palaikyti grakštų BGP perkrovimą (angl. *graceful restart*); įrenginys turi palaikyti grupinio transliavimo (angl. *multicast*) maršrutizavimą: PIM-SM, PIM-SSM; įrenginys turi palaikyti antros ir trečios versijų IGMP protokolą; įrenginys turi palaikyti politika pagrįstą maršrutizavimą (angl. *Policy based routing*) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą, vartotojo ID, vartotojų grupę, programą (angl. *application*); įrenginys turi palaikyti galimybę nukreipti dešifruoto srauto kopiją į trečiųjų šalių įrenginius, sprendimus, kurie sugeba kaupti ir analizuoti duomenų paketus; turi palaikyti IPv6 protokolą; turi palaikyti adresų transliavimą (angl. *NAT*) statiniam IP, dinaminiam IP, dinaminiam IP ir prievadui (angl. *port address translation*); turi palaikyti DHCP tarnybinės stoties, ir DHCP relay funkcijas; įrenginys turi atpažinti ir kontroliuoti programas (angl. *application*) (pvz.: Googlemail, Googletalk, Skype, Facebook ir t. t.) nepriklausomai nuo to kokie yra naudojami prievadai, protokolai, naudojamas SSL ar ne; įrenginys turi saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdyti konfidencialios informacijos	Galimybė įrenginį sukonfigūruoti taip, kad jis vienu metu, vienoje sistemoje, dirbtų visais palaikomais darbo režimais; palaiko 802.3ad.; galimybė apjungti į vieną loginę tinklo sąsają nemažiau kaip 8 fizines sąsajas; loginė sąsaja gali būti naudojama kaip L2 arba L3 lygio sąsaja; palaiko LACP protokolą; įrenginys palaiko IEEE 802.1q protokolą; VLAN sąsajos gali būti kuriamos tinklo sąsajoms, dirbančioms L2 ir L3 lygyje; įrenginys palaiko ne mažesnius kaip 8192 baitų dydžio Jumbo paketus; įrenginys palaiko statinį IP maršrutizavimą, dinaminius maršrutizavimo protokolus: BGP, OSPFv2, OSPFv3, RIPv2; įrenginys palaiko PPPoE (angl. *Point-to-Point Protocol over Ethernet*); įrenginys palaiko grakštų BGP perkrovimą (angl. *graceful restart*); įrenginys palaiko grupinio transliavimo (angl. *multicast*) maršrutizavimą: PIM-SM, PIM-SSM; įrenginys palaiko antros ir trečios versijų IGMP protokolą; įrenginys palaiko politika pagrįstą maršrutizavimą (angl. *Policy based routing*) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą, vartotojo ID, vartotojų grupę, programą (angl. *application*); įrenginys palaiko galimybę nukreipti dešifruoto srauto kopiją į trečiųjų šalių įrenginius, sprendimus, kurie sugeba kaupti ir analizuoti duomenų paketus; palaiko IPv6 protokolą; palaiko adresų transliavimą (angl. *NAT*) statiniam IP, dinaminiam IP, dinaminiam IP ir prievadui (angl. *port address translation*); palaiko DHCP tarnybinės stoties, ir DHCP relay funkcijas; įrenginys atpažįsta ir kontroliuoja programas (angl. *application*) (pvz.: Googlemail, Googletalk, Skype, Facebook ir t. t.) neprikląusomai nuo to kokie yra naudojami prievadai, protokolai, naudojamas SSL ar ne; įrenginys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdo konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką); galimybė nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme; galimybė įrašyti ne mažiau kaip 40 paketų, susijusių su grėsme; įrenginys atpažįsta ir kontroliuoja ne mažiau kaip 1500 programų (tos pačios

		perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką); turi būti galimybė nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme; turi būti galimybė įrašyti ne mažiau kaip 40 paketų, susijusių su grėsme; įrenginys turi atpažinti ir kontroliuoti ne mažiau kaip 1500 programų (tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa); turi būti galimybė apsirašyti savo programą; turi būti galimybė kiekvienai programai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma; turi būti galimybė kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros programos ar programų grupės, nenurodant serviso/prievado kuriuo dirba programa, t. y. vartotojas gali prisijungti prie nurodytos programos nepriklausomai nuo to kokį servisą/prievadą naudoja programa; turi būti galimybė aptikti kenkėjišką veiklą vidiniame tinkle, identifikuojant kompromituotą vartotoją (angl. *host*); turi būti galimybė kurti taisykles pagal šalis, t. y. siuntėjo ir/arba gavėjo laukuose nurodyti šalį; turi būti galimybė riboti prisijungimų iš vieno šaltinio skaičių pagal siuntėjo IP, gavėjo IP, siuntėjo ir gavėjo IP; kuriant ugniasienės saugumo taisykles turi būti galimybė nurodyti siuntėją, gavėją, servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę; servisai/prievadai ir programos taisyklėse turi būti nurodomi atskiruose laukuose; turi būti galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones; pagal nutylėjimą įrenginys turi blokuoti visas programas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos; įrenginys turi naudoti teigiamą saugumo kontrolės modelį; turi būti galimybė suteikti vartotojams prieigą prie programos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba programa; turi būti galimybė nurodyti prie kokių programų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei programos dirba tais pačiais TCP, UDP prievadais;	programos skirtingos versijos skaičiuojamos kaip viena programa); galimybė apsirašyti savo programą; galimybė kiekvienai programai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma; galimybė kurti saugumo taisykles, kurios leistų vartotojams jungtis tik prie tam tikros programos ar programų grupės, nenurodant serviso/prievado kuriuo dirba programa, t. y. vartotojas gali prisijungti prie nurodytos programos nepriklausomai nuo to kokį servisą/prievadą naudoja programa; galimybė aptikti kenkėjišką veiklą vidiniame tinkle, identifikuojant kompromituotą vartotoją (angl. *host*); galimybė kurti taisykles pagal šalis, t. y. siuntėjo ir/arba gavėjo laukuose nurodyti šalį; galimybė riboti prisijungimų iš vieno šaltinio skaičių pagal siuntėjo IP, gavėjo IP, siuntėjo ir gavėjo IP; kuriant ugniasienės saugumo taisykles galimybė nurodyti siuntėją, gavėją, servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę; servisai/prievadai ir programos taisyklėse nurodomi atskiruose laukuose; galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones; pagal nutylėjimą įrenginys gali blokuoti visas programas išskyrus tas, kurios yra apibrėžtos saugumo taisyklėse kaip leistinos; įrenginys naudoja teigiamą saugumo kontrolės modelį; galimybė suteikti vartotojams prieigą prie programos/ų (ne serviso/prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba programa; galimybė nurodyti prie kokių programų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei programos dirba tais pačiais TCP, UDP prievadais; galimybė suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta; galimybė suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms; įrenginys nustato vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., *Active directory* arba programinės įrangos (agento) pagalba; galimybė integruoti įrenginį su *Active Directory*, LDAP servisais ir sinchronizuoti vartotojų bei IP adresų informaciją be papildomos programinės

		turi būti galimybė suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta; turi būti galimybė suteikti prieigos teises vartotojams, ir/arba vartotojų grupėms; įrenginys turi nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., *Active directory* arba programinės įrangos (agento) pagalba; turi būti galimybė integruoti įrenginį su *Active Directory*, LDAP servisais ir sinchronizuoti vartotojų bei IP adresų informaciją be papildomos programinės įrangos naudojimo; įrenginys turi sugebėti dalintis šia informacija su kitais to paties gamintojo įrenginiais; turi būti galimybė įrenginį integruoti su *Active Directory*, LDAP, *Microsoft Terminal Services*, RADIUS; turi būti galimybė naudoti API integracijai su išorine vartotojų duomenų saugykla; turi būti galimybė dinamiškai susieti IP adresą su vartotojo atributais pagal jo AD/LDAP autentifikaciją; jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis; turi būti galimybė kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (angl. *MS Windows Terminal server*) prieigos teises; įrenginys turi skirti terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises; turi būti galimybė kurti dinamines objektų grupes, kur IP adresai nėra statiškai pririšti prie objekto, o yra nustatomi automatiškai. Vmware aplinkoje iš Vcenter gaunama informacija apie virtualias mašinas, jų tipus ir IP adresus. Turi palaikyti Vmware ESX(i) 4.1 ir 5.0.; turi būti galimybė virtualizuotose aplinkose automatiškai aptikti naujų virtualių mašinų IP adresus; turi palaikyti vartotojų tapatybės nustatymą, naudojant vartotojo skaitmeninį sertifikatą; nustatant vartotojo tapatybę, turi būti galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse;	įrangos naudojimo; įrenginys sugeba dalintis šia informacija su kitais to paties gamintojo įrenginiais; galimybė įrenginį integruoti su *Active Directory*, LDAP, *Microsoft Terminal Services*, RADIUS; galimybė naudoti API integracijai su išorine vartotojų duomenų saugykla; galimybė dinamiškai susieti IP adresą su vartotojo atributais pagal jo AD/LDAP autentifikaciją; jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis; galimybė kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (angl. *MS Windows Terminal server*) prieigos teises; įrenginys skiria terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoja kiekvieno vartotojo prieigos teises; galimybė kurti dinamines objektų grupes, kur IP adresai nėra statiškai pririšti prie objekto, o yra nustatomi automatiškai. Vmware aplinkoje iš Vcenter gaunama informacija apie virtualias mašinas, jų tipus ir IP adresus. Palaiko Vmware ESX(i) 4.1 ir 5.0.; galimybė virtualizuotose aplinkose automatiškai aptikti naujų virtualių mašinų IP adresus; palaiko vartotojų tapatybės nustatymą, naudojant vartotojo skaitmeninį sertifikatą; nustatant vartotojo tapatybę, galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse; nustatant vartotojo tapatybę, galimybė gauti vartotojų tapatybės duomenis iš trečiųjų šalių syslog šaltinių (įgaliotieji serveriai (*proxy*, *exchange*), belaidžio ryšio kontroleriai, tinklo prieigos kontrolės sprendimai (NAC)); palaiko Kerberos protokolą; įrenginys dešifruoja ir tikrina įeinantį ir išeinantį SSL duomenų srautą; galimybė dešifruoti ir tikrinti SSL duomenų srautą, nukreiptą į įmonės tarnybines stotis; galimybė nurodyti, kurį duomenų srautą dešifruoti, o kurio ne; SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS; SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo programų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą;

		nustatant vartotojo tapatybę, turi būti galimybė gauti vartotojų tapatybės duomenis iš trečiųjų šalių syslog šaltinių (įgaliotieji serveriai (*proxy, exchange*), belaidžio ryšio kontroleriai, tinklo prieigos kontrolės sprendimai (NAC)); turi palaikyti Kerberos protokolą; įrenginys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą; turi būti galimybė dešifruoti ir tikrinti SSL duomenų srautą, nukreiptą į įmonės tarnybines stotis; turi būti galimybė nurodyti, kurį duomenų srautą dešifruoti, o kurio ne; SSL patikra turi būti atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS; SSL patikra turi apimti įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo programų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą; įrenginys turi dešifruoti ir tikrinti SSH duomenų srautą; įrenginys turi palaikyti HSM modulius, kuriuose būtų saugomi skaitmeniniai raktai ir sertifikatai; įrenginys turi dešifruoti TLS 1.2 srautą; įrenginys turi atpažinti programas, bandančias naudoti HTTP CONNECT metodą; turi būti galimybė aptikti Botnet; turi būti galimybė riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus; turi būti galimybė atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę; turi būti galimybė sukurti draudžiamų URL ir IP sąrašą; turi būti galimybė sukurti ir naudoti savo URL grupes; turi būti galimybė sustabdyti perduodamus .xls, .xlsx, .doc., .docx, .ppt, .pptx, .txt tipo failus, kuriuose randamas apsibrėžtas duomenų šablonas; turi būti galimybė aptikti apsibrėžtus duomenų šablonus įvairių programų duomenų sraute; turi būti galimybė šablonus kurti naudojant „regular expression“; turi būti galimybė kontroliuoti perduodamas bylas; įrenginys turi atpažinti ne mažiau kaip 50 bylų tipų;	įrenginys dešifruoja ir tikrina SSH duomenų srautą; įrenginys palaiko HSM modulius, kuriuose būtų saugomi skaitmeniniai raktai ir sertifikatai; įrenginys dešifruoja TLS 1.2 srautą; įrenginys atpažįsta programas, bandančias naudoti HTTP CONNECT metodą; galimybė aptikti Botnet; galimybė riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus; galimybė atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę; galimybė sukurti draudžiamų URL ir IP sąrašą; galimybė sukurti ir naudoti savo URL grupes; galimybė sustabdyti perduodamus .xls, .xlsx, .doc., .docx, .ppt, .pptx, .txt tipo failus, kuriuose randamas apsibrėžtas duomenų šablonas; galimybė aptikti apsibrėžtus duomenų šablonus įvairių programų duomenų sraute; galimybė šablonus kurti naudojant „regular expression“; galimybė kontroliuoti perduodamas bylas; įrenginys atpažįsta ne mažiau kaip 50 bylų tipų; bylos tipas atpažįstamas pagal bylos turinį, o ne išplėtimą; galimybė kurti pažeidžiamumų aprašus; galimybė kurti kombinuotus pažeidžiamumų aprašus, t. y. aprašus į kuriuos būtų įtraukti keli jau sukurti aprašai; palaiko IPSEC; palaiko 3DES, AES256 arba lygiaverčius šifravimo algoritmus; palaiko SHA-1, SHA-256, SHA-384, SHA-512, arba lygiaverčius saugios maišos algoritmus; palaiko, be papildomų licencijų, nuotolinį vartotojų prisijungimą per SSL VPN; nuotolinio prisijungimo vartotojų VPN klientas moka dirbti IPSEC ir SSL protokolais; nuotolinio prisijungimo vartotojų VPN klientas palaiko Windows XP, Windows Vista (32bit, 64 bit), Windows 7 (32bit, 64 bit), Mac OS ar lygiavertes operacines sistemas; nuotolinio prisijungimo vartotojų VPN klientas palaiko galimybę griežtai tikrinti pateikiamame vartotojo sertifikate nurodyto vartotojo vardo ir besijungiančio vartotojo prisijungimo vardo atitikimą;

		bylos tipas turi būti atpažįstamas pagal bylos turinį, o ne išplėtimą; turi būti galimybė kurti pažeidžiamumų aprašus; turi būti galimybė kurti kombinuotus pažeidžiamumų aprašus, t. y. aprašus į kuriuos būtų įtraukti keli jau sukurti aprašai; turi palaikyti IPSEC; turi palaikyti 3DES, AES256 arba lygiaverčius šifravimo algoritmus; turi palaikyti SHA-1, SHA-256, SHA-384, SHA-512, arba lygiaverčius saugios maišos algoritmus; turi palaikyti, be papildomų licencijų, nuotolinį vartotojų prisijungimą per SSL VPN; nuotolinio prisijungimo vartotojų VPN klientas turi mokėti dirbti IPSEC ir SSL protokolais; nuotolinio prisijungimo vartotojų VPN klientas turi palaikyti Windows XP, Windows Vista (32bit, 64 bit), Windows 7 (32bit, 64 bit), Mac OS ar lygiavertes operacines sistemas; nuotolinio prisijungimo vartotojų VPN klientas turi palaikyti galimybę griežtai tikrinti pateikiamame vartotojo sertifikate nurodyto vartotojo vardo ir besijungiančio vartotojo prisijungimo vardo atitikimą; turi palaikyti duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas; turi būti galimybė atlikti diffserv bitų reikšmių nustatymą paketuose; turi būti galimybė duomenų paketams suteikti prioritetus; turi būti galimybė pasirinktam duomenų srautui nustatyti maksimalų pralaidumą; turi būti galimybė pasirinktam duomenų srautui nustatyti garantuotą pralaidumą; turi būti galimybė duomenų srautų valdymo statistiką atvaizduoti grafinių būdu; turi būti galimybė uždrausti naudotis internetine paieška „google“ ir „yahoo“, jeigu vartotojo naršyklėje nėra nustatyti griežčiausieji paieškos nustatymai (angl. *safe search enforcement*); turi būti galimybė kurti saugumo taisykles iškarto tarp kelių saugumo zonų, t.y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei;	palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas; galimybė atlikti diffserv bitų reikšmių nustatymą paketuose; galimybė duomenų paketams suteikti prioritetus; galimybė pasirinktam duomenų srautui nustatyti maksimalų pralaidumą; galimybė pasirinktam duomenų srautui nustatyti garantuotą pralaidumą; galimybė duomenų srautų valdymo statistiką atvaizduoti grafinių būdu; galimybė uždrausti naudotis internetine paieška „google“ ir „yahoo“, jeigu vartotojo naršyklėje nėra nustatyti griežčiausieji paieškos nustatymai (angl. *safe search enforcement*); galimybė kurti saugumo taisykles iškarto tarp kelių saugumo zonų, t.y. sukurti vieną taisyklę, kuri leistų iš 2 ar daugiau zonų jungtis į 2 ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei; įrenginio laiko sinchronizavimas su NTP serveriu atliekant autentifikaciją; galimybė atliekant URL filtravimą įrašyti į LOG pranešimus skirtingas HTTP protokolo antraštes, tokias kaip User-Agent, Referer, X-Forwarded-For; galimybė URL filtravimui ir kategorizavimui pagal pilną URL, t.y. tikrinama URL host ir URI dalys; atskiria skirtingų kategorijų WEB kategorijų turinius esančius toje pačioje internetinėje svetainėje; sesijų sinchronizavimas atliekant operacinės sistemos atnaujinimą.

		įrenginio laiko sinchronizavimas su NTP serveriu atliekant autentifikaciją; turi būti galimybė atliekant URL filtravimą įrašyti į LOG pranešimus skirtingas HTTP protokolo antraštes, tokias kaip User-Agent, Referer, X-Forwarded-For; turi būti galimybė URL filtravimui ir kategorizavimui pagal pilną URL, t.y. tikrinama URL host ir URI dalys; turi atskirti skirtingų kategorijų WEB kategorijų turinius esančius toje pačioje internetinėje svetainėje; sesijų sinchronizavimas atliekant operacinės sistemos atnaujinimą.	
12.	Skaitmeniniai sertifikatai	turi būti galimybė sugeneruoti „self-signed“ sertifikatą; galimybė importuoti skaitmeninius sertifikatus; turi palaikyti CRL; turi palaikyti OCSP protokolą; turi būti galimybė importuoti tarnybinių stočių viešus, privačius raktus.	galimybė sugeneruoti „self-signed“ sertifikatą; galimybė importuoti skaitmeninius sertifikatus; palaiko CRL; palaiko OCSP protokolą; galimybė importuoti tarnybinių stočių viešus, privačius raktus.
13.	Įvykių žurnalai, ataskaitos	įrenginys turi generuoti ir eksportuoti *Netflow v9* ar lygiaverčius įrašus apie duomenų srautus; įrašuose turi būti informacija apie vartotojus ir taikomąją programinę įrangą; įvykių žurnalai turi būti kaupiami įrenginyje ir siunčiami į centrinę valdymo tarnybinę stotį; peržiūrint įvykių žurnalus, turi būti galimybė filtruoti įvykius; įvykių žurnaluose turi būti fiksuojami administratorių atliekami veiksmai; įrenginys turi generuoti ataskaitas apie tinkle naudojamas programas; įrenginys turi generuoti ataskaitas apie vartotojo naudojamas programas, prie kokių žiniatinklio puslapių vartotojas jungiasi, vartotojo perduodamus duomenų kiekius; įrenginys turi generuoti ataskaitas apie aptiktas grėsmes; turi būti galimybė sukurti savo ataskaitas; turi būti galimybė automatizuoti ataskaitų generavimą; turi būti galimybė sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu; įrenginys realiu laiku turi pateikti informaciją apie perduodamus duomenų srautus; įrenginys turi pateikti informaciją apie naudojamos taikomosios programinės įrangos rizikos lygį; įrenginys turi pateikti informaciją apie bendrą perduodamų duomenų rizikos lygį;	įrenginys gali generuoti ir eksportuoti *Netflow v9* ar lygiaverčius įrašus apie duomenų srautus; įrašuose yra informacija apie vartotojus ir taikomąją programinę įrangą; įvykių žurnalai kaupiami įrenginyje ir siunčiami į centrinę valdymo tarnybinę stotį; peržiūrint įvykių žurnalus, galimybė filtruoti įvykius; įvykių žurnaluose fiksuojami administratorių atliekami veiksmai; įrenginys gali generuoti ataskaitas apie tinkle naudojamas programas; įrenginys gali generuoti ataskaitas apie vartotojo naudojamas programas, prie kokių žiniatinklio puslapių vartotojas jungiasi, vartotojo perduodamus duomenų kiekius; įrenginys gali generuoti ataskaitas apie aptiktas grėsmes; galimybė sukurti savo ataskaitas; galimybė automatizuoti ataskaitų generavimą; galimybė sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu; įrenginys realiu laiku gali pateikti informaciją apie perduodamus duomenų srautus; įrenginys gali pateikti informaciją apie naudojamos taikomosios programinės įrangos rizikos lygį; įrenginys gali pateikti informaciją apie bendrą perduodamų duomenų rizikos lygį; įrenginys gali pateikti informaciją apie duomenų srautus pagal šalis;

		įrenginys turi pateikti informaciją apie duomenų srautus pagal šalis; įrenginys turi pateikti informaciją apie labiausiai naudojamas taisykles; įrenginys turi pateikti informaciją apie dažniausiai lankomas svetaines, svetainių grupes; turi rodyti geografinį grėsmių atvaizdavimą; turi rodyti geografinį duomenų srautų atvaizdavimą; turi būti galimybė nurodytu laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį.	įrenginys gali pateikti informaciją apie labiausiai naudojamas taisykles; įrenginys gali pateikti informaciją apie dažniausiai lankomas svetaines, svetainių grupes; gali rodyti geografinį grėsmių atvaizdavimą; gali rodyti geografinį duomenų srautų atvaizdavimą; galimybė nurodytu laiku įvykių žurnalus siųsti į nutolusią darbo vietą/tarnybinę stotį.
14.	Valdymo funkcijos	įrenginyje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui; turi būti galimybė sukurti įrenginio naudotoją, kuris turėtų tik read-only teises (mato visą konfigūraciją, bet keisti nieko negali); turi būti galimybė įrenginį valdyti per konsolę, SSH, HTTPS, iš centrinės valdymo tarnybinės stoties; administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba; turi būti galimybė kurti roles; turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti NAT taisykles; • teisė kurti, keisti SSL dešifravimo taisykles; • teisė kurti, keisti QoS taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas; • teisė atnaujinti programinę įranga; • teisė atnaujinti aprašus; teisė matyti vartotojų vardą įvykių žurnalų įrašuose. Galimybė administratorių tapatybės nustatymui naudoti vienkartinių slaptažodžių generatorius; turi būti suderinama su SYSLOG arba lygiaverčiu standartu ir SNMP v3; turi būti galimybė keisti įvykių, siunčiamų SYSLOG protokolų, formatą (laukų išdėstymą); turi būti galimybė siųsti įvykių žurnalus syslog formatu naudojant TCP protokolą arba SSL;	įrenginyje yra atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui; galimybė sukurti įrenginio naudotoją, kuris turėtų tik read-only teises (mato visą konfigūraciją, bet keisti nieko negali); galimybė įrenginį valdyti per konsolę, SSH, HTTPS, iš centrinės valdymo tarnybinės stoties; administratorių prieigos teisės kontroliuojamos rolių pagalba; galimybė kurti roles; galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti NAT taisykles; • teisė kurti, keisti SSL dešifravimo taisykles; • teisė kurti, keisti QoS taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas; • teisė atnaujinti programinę įranga; • teisė atnaujinti aprašus; • teisė matyti vartotojų vardą įvykių žurnalų įrašuose. Galimybė administratorių tapatybės nustatymui naudoti vienkartinių slaptažodžių generatorius; suderinama su SYSLOG arba lygiaverčiu standartu ir SNMP v3; galimybė keisti įvykių, siunčiamų SYSLOG protokolų, formatą (laukų išdėstymą); galimybė siųsti įvykių žurnalus syslog formatu naudojant TCP protokolą arba SSL; automatiškai daromos konfigūracijų kopijos;

		automatiškai turi būti daromos konfigūracijų kopijos; turi būti galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis; turi būti galimybė aktyvuoti ankstesnę konfigūraciją; turi būti saugoma ne mažiau kaip 50 ankstesnių konfigūracijų; turi būti galimybė matyti aktyvius sujungimus; turi būti galimybė atlikti eilę skirtingų pakeitimų ugniasienėje per grafinę sąsają ir tuos pakeitimus aktyvuoti vienu metu; turi būti galimybė automatiškai ištrinti žurnalinius įvykius ir ataskaitas po nustatyto laiko.	galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis; galimybė aktyvuoti ankstesnę konfigūraciją; saugoma ne mažiau kaip 50 ankstesnių konfigūracijų; galimybė matyti aktyvius sujungimus; galimybė atlikti eilę skirtingų pakeitimų ugniasienėje per grafinę sąsają ir tuos pakeitimus aktyvuoti vienu metu; galimybė automatiškai ištrinti žurnalinius įvykius ir ataskaitas po nustatyto laiko.
15.	Palaikymas	įrenginiams turi būti suteiktas ne trumpesnis kaip 36 mėn. garantinis laikotarpis; įrenginiai turi būti pateikti su visom licencijomis, leidžiančiomis ne trumpiau kaip 36 mėn. gauti virusų, piktybinių programų, pažeidžiamumų, įsilaužimų aprašų, atnaujinimus, bei atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę; įrenginys turi galėti automatiškai atsisiųsti pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL duomenų bazę iš gamintojo puslapio; įrenginys turi galėti automatiškai atsisiųsti programinės įrangos atnaujinimus iš gamintojo puslapio.	įrenginiams suteiktas 36 mėn. garantinis laikotarpis; įrenginiai pateikti su visom licencijomis, leidžiančiomis 36 mėn. gauti virusų, piktybinių programų, pažeidžiamumų, įsilaužimų aprašų, atnaujinimus, bei atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę; įrenginys gali automatiškai atsisiųsti pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL duomenų bazę iš gamintojo puslapio; įrenginys gali automatiškai atsisiųsti programinės įrangos atnaujinimus iš gamintojo puslapio.

UŽSAKOVAS:

Viršininko pavaduotojas

Vygantas Ivanauskas

A.V.

TIEKĖJAS:

Direktoriaus pavaduotojas

Valdas Jusius

A.V.