



**TS PRIEDAS NR. 2 UGNIASIENIŲ
TECHNINĖ SPECIFIKACIJA**

1. SAŲOKOS IR SUTRUMPINIMAI

Pirkėjas – Atsakinga vandentvarkos asociacija „VANDENS JĖGA“

Tiekėjas – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.

Sutartis - sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.

Techninė specifikacija arba TS – dokumentas, kuriame apibūdintas pirkimo objektas.

Prekės – TS nurodytas pirkimo objektas.

2. REIKALAVIMAI PIRKIMO OBJEKTUI

3. PIRKIMO OBJEKTAS

Lentelė Nr. 1

<i>Pirkimo objekto pavadinimas^d</i>			Tinklo ugniasienė A tipo
<i>Perkamas Kiekis^{dl}</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>			<i>4 mėn.</i>
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąrašė, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos gamintojas	Nurodyti.	



1.4.	Įrangos aukštis	Ne daugiau 1 U.
1.5.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz.
1.6.	Prievadai	Ne mažiau 5x GE RJ-45; Ne mažiau 1 x USB; Ne mažiau 1x konsolės prievado RJ45.
1.7.	Ugniasienės pralaidumas	Ne mažiau 4.5 Gbps.
1.8.	Ipsec tunelių palaikomas skaičius	Ne mažiau 180.
1.9.	Ipsec VPN pralaidumas (Gateway-to-Gateway)	Ne mažiau 4 Gbps.
1.10.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1 Gbps.
1.11.	SSL inspekcijos pralaidumas	Ne mažiau 200 Mbps.
1.12.	NGFW pralaidumas	Ne mažiau 800 Mbps.
1.13.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių.
1.14.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 2 000.
1.15.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.
1.16.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiku atliekamos užklausos pagrindu.
1.17.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (SSL inspection)).
1.18.	Failų tikrinimas smėliadėžėje	Turi būti galimybė papildomai tikrinti failus gamintojo smėliadėžėje.
1.19.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.20.	OT IPS apsauga	IPS detektavimas turi apsaugoti nuo OT tinklo atakų.
1.21.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, resetuoti sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.22.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.23.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus. Turi kontroliuoti industrines sistemų aplikacijas ir protokolus.
1.24.	Ugniasienės darbo režimai	NAT/Route, Transparent.
1.25.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.



1.26.	Valdymas	WEB (HTTPS), SSH, TELNET.
1.27.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti.
1.28.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketų srautą.
1.29.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (policy routing) .
1.30.	DNS serverio režimas	Turi palaikyti DNS serverio režimą.
1.31.	Dinaminio maršrutizavimo protokolai	BGP4, OSPF v2 ir v3, RIP v1 ir v2, ISIS.
1.32.	VXLAN palaikymas	Turi būti.
1.33.	EMAC-VLAN palaikymas	Turi būti.
1.34.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.35.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.
1.36.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, vartotojų grupę, aplikaciją, sujungimo kokybę.
1.37.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.38.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.
1.39.	Ugniasienėje integruotas bevielio ryšio stotelių (AP) kontrolieris	Turi gebėti valdyti tiek lokaliai esančias, tiek nutolusias bevielio ryšio stoteles; palaikyti autorizaciją PSK, WPA Personal, 802.1x ir captive portal pagrindu; detektuoti bevielio ryšio kanalo atakas (wireless IDS); gebėti blokuoti vartotoją galimybę naudotis nesankcionuotai prie tinklo prijungtomis bevielio ryšio stotelėmis; palaikyti fasat roaming ir AP load balancing funkcionalumą.
1.40.	Ugniasienėje integruotas Komutatorių kontrolieris	Turi gebėti valdyti komutatorius, leisti konfigūruoti bent VLAN, PoE, prievado greitaveiką iš ugniasienės grafines aplinkos,
1.41.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
1.42.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>



1.43.	Kokybė	Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametrų nei nurodyta šioje specifikacijoje arba geresnių parametrų.	

Lentelė Nr. 2

<i>Pirkimo objekto pavadinimas</i>		Tinklo ugniasienė B tipo	
<i>Perkamas Kiekis</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąraše, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos aukštis	Ne daugiau 1 U.	
1.4.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz.	
1.5.	Prievadai	Ne mažiau 5x GE RJ-45; Ne mažiau 1 x USB; Ne mažiau 1x konsolės prievado RJ45.	
1.6.	LTE ryšio palaikymas	Įrenginyje turi būti integruotas LTE modulis	
1.7.	SIM kortelių skaičius	Įrenginys turi palaikyti ne mažiau 2 SIM kortelių vienu metu	
1.8.	Ugniasienės pralaidumas	Ne mažiau 4.5 Gbps.	



1.9.	Ipsec tunelių palaikomas skaičius (Gateway-to-Gateway)	Ne mažiau 180.
1.10.	Ipsec VPN pralaidumas	Ne mažiau 4 Gbps.
1.11.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 1 Gbps.
1.12.	SSL inspekcijos pralaidumas	Ne mažiau 200 Mbps.
1.13.	NGFW pralaidumas	Ne mažiau 800 Mbps.
1.14.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių.
1.15.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 2 000.
1.16.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.
1.17.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiku atliekamos užklausos pagrindu.
1.18.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (SSL inspection)).
1.19.	Failų tikrinimas smėliadėžėje	Turi būti galimybė papildomai tikrinti failus gamintojo smėliadėžėje.
1.20.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.21.	OT IPS apsauga	IPS detektavimas turi apsaugoti nuo OT tinklo atakų.
1.22.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, resetuoti sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.23.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.24.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus. Turi kontroliuoti industrines sistemų aplikacijas ir protokolus.
1.25.	Ugniasienės darbo režimai	NAT/Route, Transparent.
1.26.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.
1.27.	Valdymas	WEB (HTTPS), SSH, TELNET.
1.28.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti.
1.29.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketų srautą.



1.30.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (policy routing) .
1.31.	DNS serverio režimas	Turi palaikyti DNS serverio režimą.
1.32.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS.
1.33.	VXLAN palaikymas	Turi būti.
1.34.	EMAC-VLAN palaikymas	Turi būti.
1.35.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.36.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.
1.37.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, vartotojų grupę, aplikaciją, sujungimo kokybę.
1.38.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.39.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.
1.40.	Ugniasienėje integruotas bevielio ryšio stotelių (AP) kontrolieris	Turi gebėti valdyti tiek lokaliai esančias, tiek nutolusias bevielio ryšio stoteles; palaikyti autorizaciją PSK, WPA Personal, 802.1x ir captive portal pagrindu; detektuoti bevielio ryšio kanalo atakas (wireless IDS); gebėti blokuoti vartotoją galimybę naudotis nesankcionuotai prie tinklo prijungtomis bevielio ryšio stotelėmis; palaikyti fasat roaming ir AP load balancing funkcionalumą.
1.41.	Ugniasienėje integruotas Komutatorių kontrolieris	Turi gebėti valdyti komutatorius, leisti konfigūruoti bent VLAN, PoE, prievado greitaveiką iš ugniasienės grafinės aplinkos,
1.42.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančią resursų, tarp jų ir programinės įrangos bibliotekos.
1.44.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>
1.45.	Kokybė	<i>Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	



3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametru nei nurodyta šioje specifikacijoje arba geresnių parametru.

Lentelė Nr. 3

<i>Pirkimo objekto pavadinimas</i>		Tinklo ugniasienė C tipo	
<i>Perkamas Kiekis</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąraše, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos aukštis	Ne daugiau 1 U.	
1.4.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz.	
1.5.	Prievadai	Ne mažiau 5x GE RJ-45; Ne mažiau 1 x USB; Ne mažiau 1x konsolės prievado RJ45.	
1.6.	5G ryšio palaikymas	Įrenginyje turi būti integruotas 5G modulis	
1.7.	SIM kortelių skaičius	Įrenginys turi palaikyti ne mažiau 2 SIM kortelių vienu metu	
1.8.	Išorinės antenos	Ne mažiau 5 vnt. antenų su SMA jungtimis	
1.9.	Ugniasienės pralaidumas	Ne mažiau 4.5 Gbps.	
1.10.	Ipssec tunelių palaikomas skaičius (Gateway-to-Gateway)	Ne mažiau 180.	
1.11.	Ipssec VPN pralaidumas	Ne mažiau 4 Gbps.	
1.12.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 2 Gbps.	



1.13.	SSL inspekcijos pralaidumas	Ne mažiau 1.2 Gbps.
1.14.	NGFW pralaidumas	Ne mažiau 1.2 Gbps.
1.15.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių.
1.16.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 2 000.
1.17.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.
1.18.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiku atliekamos užklausos pagrindu.
1.19.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (SSL inspection)).
1.20.	Failų tikrinimas smėliadėžėje	Turi būti galimybė papildomai tikrinti failus gamintojo smėliadėžėje.
1.21.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.22.	OT IPS apsauga	IPS detektavimas turi apsaugoti nuo OT tinklo atakų.
1.23.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, resetuoti sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.24.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.25.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus. Turi kontroliuoti industrines sistemų aplikacijas ir protokolus.
1.26.	Ugniasienės darbo režimai	NAT/Route, Transparent.
1.27.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.
1.28.	Valdymas	WEB (HTTPS), SSH, TELNET.
1.29.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti.
1.30.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketų srautą.
1.31.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (policy routing) .
1.32.	DNS serverio režimas	Turi palaikyti DNS serverio režimą.
1.33.	Dinaminio maršrutizavimo protokolai	BGP4, OSFP v2 ir v3, RIP v1 ir v2, ISIS.
1.34.	VXLAN palaikymas	Turi būti.
1.35.	EMAC-VLAN palaikymas	Turi būti.



1.36.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.37.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.
1.38.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, vartotojų grupę, aplikaciją, sujungimo kokybę.
1.39.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.40.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.
1.41.	Ugniasienėje integruotas Komutatorių kontrolieris	Turi gebėti valdyti komutatorius, leisti konfigūruoti bent VLAN, PoE, prievado greitaveiką iš ugniasienės grafinės aplinkos,
1.42.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančią resursų, tarp jų ir programinės įrangos bibliotekos.
1.43.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>
1.44.	Kokybė	<i>Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametru nei nurodyta šioje specifikacijoje arba geresnių parametru.	



Lentelė Nr. 4

<i>Pirkimo objekto pavadinimas</i>		Tinklo ugniasienė D tipo	
<i>Perkamas Kiekis</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąrašė, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos aukštis	Ne daugiau 1 U.	
1.4.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz.	
1.5.	Prievadai	Ne mažiau 10x GE RJ-45; Ne mažiau 1 x USB; Ne mažiau 1x konsolės prievado RJ45.	
1.6.	Ugniasienės pralaidumas	Ne mažiau 9.5 Gbps.	
1.7.	Ipssec tunelių palaikomas skaičius	Ne mažiau 180.	
1.8.	Ipssec VPN pralaidumas (Gateway-to-Gateway)	Ne mažiau 7 Gbps.	
1.9.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 2.3 Gbps.	
1.10.	SSL inspekcijos pralaidumas	Ne mažiau 1.3 Gbps.	
1.11.	NGFW pralaidumas	Ne mažiau 1.3 Gbps.	
1.12.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių.	
1.13.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 5 000.	
1.14.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.	
1.15.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiku atliekamos užklausos pagrindu.	



1.16.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (SSL inspection).
1.17.	Failų tikrinimas smėliadėžėje	Turi būti galimybė papildomai tikrinti failus gamintojo smėliadėžėje.
1.18.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.19.	OT IPS apsauga	IPS detektavimas turi apsaugoti nuo OT tinklo atakų.
1.20.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, resetuoti sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.21.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.22.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus. Turi kontroliuoti industrines sistemų aplikacijas ir protokolus.
1.23.	Ugniasienės darbo režimai	NAT/Route, Transparent.
1.24.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.
1.25.	Valdymas	WEB (HTTPS), SSH, TELNET.
1.26.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti.
1.27.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketų srautą.
1.28.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (policy routing) .
1.29.	DNS serverio režimas	Turi palaikyti DNS serverio režimą.
1.30.	Dinaminio maršrutizavimo protokolai	BGP4, OSPF v2 ir v3, RIP v1 ir v2, ISIS.
1.31.	VXLAN palaikymas	Turi būti.
1.32.	EMAC-VLAN palaikymas	Turi būti.
1.33.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.34.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.
1.35.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, vartotojų grupę, aplikaciją, sujungimo kokybę.
1.36.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.37.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.



1.38.	Ugniasienėje integruotas bevielio ryšio stotelių (AP) kontrolieris	Turi gebėti valdyti tiek lokaliai esančias, tiek nutolusias bevielio ryšio stoteles; palaikyti autorizaciją PSK, WPA Personal, 802.1x ir captive portal pagrindu; detektuoti bevielio ryšio kanalo atakas (wireless IDS); gebėti blokuoti vartotoją galimybę naudotis nesankcionuotai prie tinklo prijungtomis bevielio ryšio stotelėmis; palaikyti fasat roaming ir AP load balancing funkcionalumą.
1.39.	Ugniasienėje integruotas Komutatorių kontrolieris	Turi gebėti valdyti komutatorius, leisti konfigūruoti bent VLAN, PoE, prievado greitaveiką iš ugniasienės grafinės aplinkos,
1.40.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
1.41.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimitos.</i>
1.42.	Kokybė	<i>Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametrų nei nurodyta šioje specifikacijoje arba geresnių parametrų.	



Lentelė Nr. 5

<i>Pirkimo objekto pavadinimas</i>		Tinklo ugniasienė E tipo	
<i>Perkamas Kiekis</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąrašė, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos aukštis	Ne daugiau 1 U.	
1.4.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz.	
1.5.	Kartu komplektuojami prievadų moduliai (angl. transceivers) ir kabeliai	Kartu su kiekvienu komutatoriumi turi būti pateikiama to paties gamintojo ne mažiau kaip: 2 vnt. 10G SFP+ LC/LC	
1.6.	Prievadai	Ne mažiau 8x GE RJ-45; Ne mažiau 2x SFP+; Ne mažiau 1x USB; Ne mažiau 1x konsolės prievado RJ45.	
1.7.	Ugniasienės pralaidumas	Ne mažiau 25 Gbps.	
1.8.	Ipssec tunelių palaikomas skaičius (Gateway-to-Gateway)	Ne mažiau 200.	
1.9.	Ipssec VPN pralaidumas	Ne mažiau 24 Gbps.	
1.10.	SSL VPN pralaidumas	Ne mažiau 1.3 Gbps.	
1.11.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 4 Gbps.	
1.12.	SSL inspekcijos pralaidumas	Ne mažiau 2.5 Gbps.	
1.13.	NGFW pralaidumas	Ne mažiau 2.5 Gbps.	
1.14.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių.	



1.15.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 4500.
1.16.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.
1.17.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiku atliekamos užklausos pagrindu.
1.18.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (SSL inspection)).
1.19.	Failų tikrinimas smėliadėžėje	Turi būti galimybė papildomai tikrinti failus gamintojo smėliadėžėje.
1.20.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.21.	OT IPS apsauga	IPS detektavimas turi apsaugoti nuo OT tinklo atakų.
1.22.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, resetuoti sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.23.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.24.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus. Turi kontroliuoti industrines sistemų aplikacijas ir protokolus.
1.25.	Ugniasienės darbo režimai	NAT/Route, Transparent.
1.26.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.
1.27.	Valdymas	WEB (HTTPS), SSH, TELNET.
1.28.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti.
1.29.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketų srautą.
1.30.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (policy routing) .
1.31.	DNS serverio režimas	Turi palaikyti DNS serverio režimą.
1.32.	Dinaminio maršrutizavimo protokolai	BGP4, OSPF v2 ir v3, RIP v1 ir v2, ISIS.
1.33.	VXLAN palaikymas	Turi būti.
1.34.	EMAC-VLAN palaikymas	Turi būti.
1.35.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.36.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.



1.37.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, vartotojų grupę, aplikaciją, sujungimo kokybę.
1.38.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.39.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.
1.40.	Ugniasienėje integruotas bevielio ryšio stotelių (AP) kontrolieris	Turi gebėti valdyti tiek lokaliai esančias, tiek nutolusias bevielio ryšio stoteles; palaikyti autorizaciją PSK, WPA Personal, 802.1x ir captive portal pagrindu; detektuoti bevielio ryšio kanalo atakas (wireless IDS); gebėti blokuoti vartotoją galimybę naudotis nesankcionuotai prie tinklo prijungtomis bevielio ryšio stotelėmis; palaikyti fasat roaming ir AP load balancing funkcionalumą.
1.41.	Ugniasienėje integruotas Komutatorių kontrolieris	Turi gebėti valdyti komutatorius, leisti konfigūruoti bent VLAN, PoE, prievado greitaveiką iš ugniasienės grafines aplinkos,
1.42.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
1.43.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimitos.</i>
1.44.	Kokybė	<i>Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
	Visa pateikiama įranga privalo būti ne prastesnių parametru nei nurodyta šioje specifikacijoje arba geresnių parametru.	



Lentelė Nr. 6

<i>Pirkimo objekto pavadinimas</i>		Tinklo ugniasienė F tipo	
<i>Perkamas Kiekis</i>			
<i>Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)</i>		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąraše, reikalavimui dėl nacionalinio saugumo	
1.3.	Įrangos suderinamumas	Turi būti suderintas HA pajungimui (angl. Active-Active, Active-Passive, Clustering)	
1.4.	Montavimas	Įranga turi būti pritaikyta montuoti į 19 colių spintą ir pateikiama su visais reikalingais montavimui priedais.	
1.5.	Įrangos aukštis	Ne daugiau 1 U	
1.6.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	
1.7.	Atsarginis maitinimo šaltinis	Įrenginys turi turėti ne mažiau kaip 2 karšto keitimo maitinimo šaltinius, užtikrinančius nepertraukiamą įrangos veikimą sugedus vienam iš maitinimo šaltinių.	
1.8.	Priedavai	Ne mažiau 4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP	
1.9.	Optiniai moduliai	Įrangos vienetą turi būti: • ne mažiau kaip 4 vnt. 10G SFP+(10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots); Jeigu siūlomi kito, nei ugniasienių įrangos gamintojo optiniai moduliai, turi būti pateikti oficialūs optinių modulių gamintojo dokumentai arba nuorodos į optinių modulių gamintojo tinklapius, kuriuose būtų pateikiama suderinamumą su siūloma ugniasienių įranga patvirtinanti informacija.	
1.10.	Ugniasienės pralaidumas	Ne mažiau 39 Gbps	
1.11.	Naujų sesijų skaičius per sekundę	Ne mažiau 140 000	
1.12.	Sesijų skaičius	Ne mažiau 3 000 000	



1.13.	Ipsec tunelių palaikomas skaičius įrenginys-įrenginys „Gateway-to-Gateway“	Ne mažiau 2 000
1.14.	Ipsec tunelių palaikomas skaičius klientas – įrenginys „Client-to-Gateway“	Ne mažiau 16 000
1.15.	SSL VPN pralaidumas	Ne mažiau 1,5 Gbps
1.16.	Ipsec VPN pralaidumas(512 byte)	Ne mažiau 35 Gbps
1.17.	Apsaugos nuo įsilaužimų maksimalus pralaidumas (IPS)	Ne mažiau 5 Gbps
1.18.	SSL inspekcijos pralaidumas	Ne mažiau 1,5 Gbps
1.19.	NGFW pralaidumas	Ne mažiau 3 Gbps
1.20.	Sistemos virtualizavimas	Turi būti galimybė padalinti į 10 virtualių įrenginių. Kiekviena virtuali ugniasienė turi palaikyti tokį pat funkcionalumą kaip ir fizinė ugniasienė.
1.21.	Ugniasienės taisyklių skaičius per visą sistemą	Ne mažiau 10 000
1.22.	Botnet serverių IP adresų blokavimas	Turi būti galimybė blokuoti reguliariai atnaujinamos botnet serverių IP adresų duomenų bazės pagrindu.
1.23.	Antivirusinė apsauga	Turi būti galimybė aptikti virusus tiek reguliariai atnaujinamos duomenų bazės pagrindu, tiek realiu laiko atliekamos užklausos pagrindu.
1.24.	Antivirusinės apsaugos darbo režimai	Proxy, Flow-based (Galimybė tikrinti šifruotą srautą (angl. SSL inspection)).
1.25.	IPS detektavimas	Atnaujinama IPS duomenų bazė, protokolų anomalijų detektavimas, detektavimas srauto lygio pagrindu, galimybė sukurti savo IPS aprašus.
1.26.	IPS blokavimo galimybės	Galimybė taikyti veiksmus: blokuoti, nutraukti (angl. reset) sujungimą, stebėti, karantinuoti įsilaužėlio IP, įsilaužėlio ir aukos IP, prievadą.
1.27.	Kitas IPS funkcionalumas	Galimybė detektuoti atakas srauto kopijoje (IDS sniffer mode), galimybė įrašyti atakos paketus, galimybė nurodytiems IP adresams sukurti išimtis IPS aprašų taikymui.
1.28.	Aplikacijų kontrolė	Turi palaikyti atnaujinamą aplikacijų duomenų bazę, apimančią kelis tūkstančių aplikacijų. Aplikacijų suskirstymas į daugiau nei 15 kategorijų. Turi būti galimybė kurti savo aplikacijų aprašus.
1.29.	Debesų aplikacijų kontrolė	Turi gebėti kontroliuoti populiarias debesų aplikacijas, tokias kaip Salesforce, Google Docs and Dropbox, Amazon AWS, Microsoft OneDrive ir pan..
1.30.	WEB turinio kontrolės darbo režimai	Proxy, flow-based, DNS
1.31.	WEB turinio kontrolė	Web turinio kontrolė URL duomenų bazės pagrindu; Blokuoti interneto naršymą pagal adresą (URL), raktinius žodžius / frazes. Duomenų bazė turi apimti kelis šimtus milijonų URL adresų ir turi būti suskirstyta į kategorijas. Turi būti galimybė kurti savo sąrašus pagal URL adresus, MIME header, turinį. Turi būti galimybė integruoti trečių šalių duomenų bazes.



1.32.	WEB turinio kontrolės funkcionalumas	Galimybė numatytam laikui (laikinei) naudotojui ar naudotojų grupei taikyti kitą apsaugos profilį. Galimybė filtruoti / blokuoti Java Applet, ActiveX, cookie, HTTP POST; fiksuoti įvykių žurnale paieškos žodžius. Turi būti galimybė daryti URL sąrašus, kuriems WEB turinio tikrinimas neatliekamas.
1.33.	Ugniasienės darbo režimai	NAT/Route, Transparent
1.34.	Ugniasienės funkcionalumas	Galimybė taisyklėse naudoti URL ir aplikacijas kaip objektus. Galimybė kurti taisykles pagal naudotojus ir įrenginius. VoIP srauto palaikymas: SIP/H.323 /SCCP NAT traversal, RTP pin holing.
1.35.	Duomenų praradimo prevencija (DLP)	Galimybė aptikti: žymėtas bylas (angl. watermarking); bylas pagal kontrolines sumas (angl. fingerprinting); pagal bylos tipą, dydį, turinį, jei šifruota.
1.36.	Duomenų praradimo prevencijos (DLP) funkcionalumas	Galimybė blokuoti, tik registruoti įvykių techninių įrašų žurnale, karantinuoti naudotoją, IP adresą arba prievadą.
1.37.	Pašto apsauga (angl. Antispam)	Brūkalo aptikimas: pagal IP adresą, URL ir laiškų kontrolinių sumų duomenų bazes; HELO DNS Lookup, return email DNS check, Black/White List metodais.
1.38.	DoS apsauga	Atakų sąrašas, kurių poveikis gali būti minimizuojamas: TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding.
1.39.	Taisyklių objektai	Iš anksto nustatyti ir naudotojo sukurti; objektai ir objektų grupės; IP adresai, potinkliai, IP adresų ruožai, GeolP, FQDN; dinamiškai atnaujinamos objektų duomenų bazės.
1.40.	Įrenginių atpažinimas	Turi atpažinti įrenginius ir OS, juos automatiškai klasifikuoti; Turi palaikyti autentifikaciją pagal MAC adresus.
1.41.	SSL inspekcija	Turi gebėti SSL šifruotame sraute atlikti aplikacijų kontrolės, AV, web filtravimo ir DLP patikrą.
1.42.	SSL inspekcijos galimybės	Turi gebėti kopijuoti dešifruotą srautą (angl. SSL MITM mirroring); atlikti pilną SSL tikrinimą arba SSL sertifikato tikrinimą; turi būti galimybė aprašyti išimtis atskiroms web kategorijoms ar adresams.
1.43.	Valdymas	WEB (HTTPS), SSH, konsolė RS-232, TELNET
1.44.	Galimybė išjungti nenaudojamą funkcionalumą grafiniame valdyme (GUI)	Turi būti
1.45.	Galimybė priskirti objektams, Prievadams, įrenginiams žymes (angl. tags)	Turi būti galimybė matyti priskirtas žymes monitoringe ir ataskaitose.
1.46.	Techninių žurnalų įrašų kaupimas	Turi būti techninių žurnalų įrašų (angl. event log) palaikymas. Galimybė juos saugoti lokaliai, siųsti juos į Syslog serverius, serverius debesyje, integracija su SIEM, SOC.
1.47.	Techninių žurnalų įrašai	Perduotas srautas, sesijos su pažeidimais, netaisyklingi paketai, sistemos įvykiai ir administratorių atlikti veiksmai, maršrutizavimo, VPN, naudotojų atlikti veiksmai ir WIFI įvykiai.
1.48.	Diagnostikos priemonės	Turi būti galimybė įrašyti paketus, sekti pasirinktą sesiją arba paketą srautą.
1.49.	Kiti įvykiai	Turi būti sisteminiai, administravimo, VPN, naudotojų autentifikavimo, maršrutizavimo, WiFi susiję įvykiai.



1.50.	Sistemos virtualizavimas	Turi būti galimybė padalinti į ne mažiau kaip 10 virtualių įrenginių.
1.51.	Maršrutizavimas	Statinis, dinaminis, maršrutizavimas pagal taisykles (angl. policy base routing).
1.52.	Dinaminio maršrutizavimo protokolai	BGP4, OSPF v2 ir v3, RIP v1 ir v2, ISIS
1.53.	Turinio maršrutizavimas	WCCP, ICAP
1.54.	NAT konfigūravimas	Per taisykles (angl. policy) per įrenginį
1.55.	Palaikomi NAT	NAT64, NAT46, static ir dynamic NAT, PAT, Full Cone NAT, STUN
1.56.	L2 prievadų darbo režimai	Port aggregated, loopback, VLANs (802.1Q ir Trunking), virtualūs aparatiniai, programiniai ir VLAN komutatoriai.
1.57.	EMAC-VLAN palaikymas	Turi būti
1.58.	Srauto balansavimas tarp kelių WAN prievadų	Palaikomi balansavimo algoritmai: by volume, sessions, source-destination IP, Source IP, spillover.
1.59.	WAN sujungimo kokybės patikra (SLA)	Patikra ping ir HTTP probe metodais. Stebimi parametrai: latency, jitter, packet loss.
1.60.	WAN sujungimo parinkimo kriterijai	Pagal IP adresą, naudotojų grupę, aplikaciją, sujungimo kokybę.
1.61.	Srauto valdymas	Srauto ribojimas ir QoS valdymas per taisyklę, per aplikaciją. Maksimalus ir garantuotas pralaidumas, maksimalus sujungimo skaičius per IP, TOS ir DiffServ palaikymas. Srauto ribojimas per aplikaciją ir URL kategoriją.
1.62.	WAN optimizacija	Palaikomi WAN optimizacijos protokolai: CIFS, FTP, HTTP(S), MAPI, TCP. Protokolų optimizacija ir podėliavimas (WEB caching).
1.63.	Galimybė pasirinktiems URL adresams nevykdyti podėliavimo (angl. WEB caching)	Turi būti galimybė sukonfigūruoti URL adresą šabloną (angl. pattern).
1.64.	Explicit proxy funkcionalumas	Galimybė sukonfigūruoti FTP, HTTP, HTTPS protokolus; Proxy auto config (PAC) funkcionalumo palaikymas; Proxy autentifikacija — per IP ir per sesiją; Transparent proxy funkcionalumas.
1.65.	IPv6 palaikymas	Valdymas per IPv6, IPv6 maršrutizavimas, srauto patikra IPv6 srautui, NAT46, NAT64, IPv6 IPsec VPN
1.66.	Aukšto patikimumo (HA) telkinio darbo režimai	Turi būti galimybė apjungti du įrenginius active-passive, active-active, virtual clusters, VRRP metodais.
1.67.	HA diegimo galimybės	Turi palaikyti full mesh HA, HA with link Agregation diegimo galimybes.
1.68.	Integruoti serveriai	Įrenginys turi turėti integruotus DHCP, NTP, DNS serverius ir DNS proxy servisą.
1.69.	Gamintojo servais	Gamintojas turi užtikrinti galimybę įrenginiui naudotis NTP, DDNS, DNS servais.
1.70.	IPSec kriptavimo ir autentifikavimo algoritmai	Turi palaikyti: DES, 3DES, AES128, AES192, AES256; MD5, SHA-1, SHA-256, SHA-384, SHA-512; Diffie-Hellman 1,2,5,14.
1.71.	Integracija, standartai ir protokolai	Turi palaikyti SNMP v1,v2c,v3, SNMP trapų siuntimą, sFlow v5, Netflow v9.0; RFC 3195; WebTrends WELF.
1.72.	Tinklo saugos priemonių ekosistema	Turi sklandžiai integruotis su to pačio gamintojo pašto apsaugos, WEB serverių apsaugos, WEB srauto kešavimo, smėliadėžės (angl. Sandbox) įrenginiais;



		galimybė centralizuotai analizei automatiškai siųsti ne tik techninius žurnalų įrašus (angl. logs), bet ir informaciją apie topologiją, įrenginių žymes ir pan.
1.73.	Centralizuotas valdymas	Turi palaikyti centralizuoto valdymo galimybę iš specializuoto įrenginio arba serviso; palaikyti lokaliai arba nuotoliniu būdu vykdomus skriptus.
1.74.	Vizualizacija	Turi interaktyviai ir grafiškai atvaizduoti naudotojų, įrenginių, tinklo ir saugumo aspektus; atvaizduoti fizinę ir loginę tinklo topologiją; gebėti atvaizduoti šitos ir žemiau esančių ugniasienių agreguotą informaciją.
1.75.	Automatizacija	Turi gebėti automatiškai karantinuoti (blokuoti) įrenginį access lygmeniu, jeigu pastarasis yra arba prijungtas prie to pačio gamintojo komutatoriaus arba WiFi stotelės arba turi įdiegtą atitinkamą programinę įrangą. Karantinuojamas įrenginys neturi pasiekti sekančio įrenginio tinkle.
1.76.	Autentifikacija	Turi palaikyti LDAP, Radius, TACACS+, dviejų lygių (faktorių) autentifikaciją; palaikyti single-sign-on funkcionalumą ir integraciją su WindowsAD, MS Exchange ir Terminal Server agentais, POP3/POP3S, 802.1x ir captive portal autentifikacija; palaikyti PKI ir X.509 sertifikatus.
1.77.	Atitikimų reikalavimams patikra	Turi būti galimybė automatiškai audituoti tinklo saugumo elementus, tikrinant esamos situacijos atitikimą gerosioms praktikoms, pateikti rezultatus ir rekomendacijas; tikrinti klientinių įrenginių atitikimą saugumo reikalavimams (per įdiegtą programinę įrangą).
1.78.	Išplėstinė apsaugos sistema (angl. Advance Threat Protection)	Turi būti galimybė pasirinktus bylų tipus siųsti papildomai patikrai į smėliadėžes (angl. sandbox), esančias debesyje arba lokaliai; galimybė dinamiškai gauti duomenų bazių atnaujinimus iš bylų patikros sistemų.
1.79.	IOC (angl. Indicator of compromise) funkcionalumas	Integracijoje su kitomis tinklo saugumo priemonėmis turi gebėti ugniasienės grafinėje aplinkoje atvaizduoti informaciją apie užkrėtus įrenginius, kai tokia informacija pateikiama iš kito tinklo saugumo analizės įrenginių/priemonių.
1.80.	Ugniasienėje integruotas bevielio ryšio stotelių (AP) valdiklis	Turi gebėti valdyti tiek lokaliai esančias, tiek nutolusias bevielio ryšio stoteles; palaikyti autorizaciją PSK, WPA Personal, 802.1x ir captive portal pagrindu; detektuoti bevielio ryšio kanalo atakas (wireless IDS); gebėti blokuoti naudotoją galimybę naudotis nesankcionuotai prie tinklo prijungtomis bevielio ryšio stotelėmis; palaikyti fast roaming ir AP load balancing funkcionalumą.
1.81.	Ugniasienėje integruotas komutatorių valdiklis	Turi gebėti valdyti komutatorius, leisti konfigūruoti VLAN, PoE iš ugniasienės grafinės aplinkos.
1.82.	Surinkimo reikalavimai	Ugniasienė turi būti nauja, nenaudota, pateikta gamykliniame įpakavime, be išorinių pažeidimų, pastebimų nusidėvėjimo požymių, turi veikti visos ugniasienės gamintojo numatytos funkcijos. Gamykliškai atnaujinti komponentai (angl. „Refurbished“) neleistini.
1.83.	Garantiniai įsipareigojimai, techninis palaikymas	Gamintojo garantuojamas 36 mėn. nemokamas garantinis aptarnavimas, bei saugumo servisų atnaujinimų teikimas garantiniu laikotarpiu: IPS, OT, Application Control aprašų atnaujinimas. Teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu ar faksu. Prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekos.
1.84.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>



1.85.	Kokybė	Tiekėjas patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametrų nei nurodyta šioje specifikacijoje arba geresnių parametrų.	

Lentelė Nr. 7

Pirkimo objekto pavadinimas		4/5G maršrutizatorius A tipo	
Perkamas Kiekis			
Prekių pristatymo terminas (įskaitant montavimą ir kt. TS nurodytas paslaugas)		4 mėn.	
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija	Tiekėjas siūlo [Tiekėjas turi įrašyti kur reikia reikšmę arba trumpą aprašymą, patvirtinantį atitikimą techniniam reikalavimui (įrašai „Taip“, „Atitinka“, „Tenkina“, „+“, „<... yra ne mažesnis kaip ...>“, „<... bus ne didesnis kaip ...>“ ar pan., negalimi)]
1.	Perkamas objektas		
1.1.	Modelis, gamintojas	Nurodyti ir pateikti siūlomo modelio nuorodą gamintojo svetainėje.	
1.2.	Kilmės šalis	Kai prekė yra BVPŽ kodų sąraše, reikalavimui dėl nacionalinio saugumo	
1.3.	Tipas	Specializuotas vieno gamintojo įrenginys skirtas išplėsti perkančiosios organizacijos perkamų ugniasienių galimybes, užtikrinant 4G/5G ryšį.	
1.4.	El. maitinimas	Turi būti galimybė įrenginį maitinti per RJ45 tinklo kabelį (PoE). Įrenginys turi būti suderinamas su IEEE 802.3at standartu arba analogišku.	
1.5.	Korpusas	Turi būti galimybė įrenginį statyti ant stalo ir montuoti ant sienos. Su įrenginiu turi būti pateiktos visos reikalingos tvirtinimo detalės.	
1.6.	Prievadai	Ne mažiau: 5 vnt. GE RJ45 prievadų; 1 GE SFP prievado 1 USB 2.0	



1.7.	Valdymas	Pilnas valdymas turi būti užtikrinamas iš ugniasienės be poreikio jungtis prie įrenginio
1.8.	Funkcionalumo palaikymas	<ul style="list-style-type: none"> ● VXLAN ● VLAN ● OSFP ● IPSEC ● RADIUS ● SD-WAN
1.9.	Integruoti moduliai	Įrenginys savyje turi turėti integruota 4G/5G modemą. Integruotas modemas turi būti suderinamas su Europoje naudojamais mobiliųjų tinklų dažniais. Modemas turi gebėti dirbti su ne prastesniais nei 5G/LTE/GNSS tinklais. Turi būti galimybė įdėti ne mažiau kaip 2 sim korteles. Integruotas modemas turi palaikyti ne prastesnį nei 20 kategorijos LTE ryšį.
1.10.	Įrenginio antenos ir radijo parametrai	Įrenginys turi turėti ne mažiau kaip 4 vnt. ant korpuso iš išorės tvirtinamas antenas. Turi palaikyti 4 x 4 MIMO.
1.11.	Suderinamumas	Įrenginys turi būti pilnai suderinamas su perkančiosios organizacijos perkamomis ugniasienėmis ir gebėti dirbti kaip išorinis jų modulis
1.12.	Komplektavimas	Įrenginys turi būti komplektuojamas su PoE maitinimo šaltiniu suderinamu su standartu IEEE 802.3at arba komplektuojamas su maitinimo šaltiniu skirtu perkamam įrenginiui pagal užsakovo pageidavimą.
1.13.	Trūkumų šalinimas	<i>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias, nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>
1.14.	Kokybė	<i>Tiekėjas patvirtina, kad perduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Kiti reikalavimai	
3.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
3.2.	Visa pateikiama įranga privalo būti ne prastesnių parametru nei nurodyta šioje specifikacijoje arba geresnių parametru.	

ⁱ Jeigu techninėje specifikacijoje yra nurodytas konkretus perkamos prekės tipas, modelis, ženklas, taikomas standartas ar kita konkreti apibūdinanti informacija, Pirkėjui yra priimtina lygiavertė prekė, atitinkanti techninėje specifikacijoje nurodytos prekės parametrus ar taikomus standartus.

Šiame dokumente vartojami terminai „turi būti“, „turi turėti“, „turi leisti“, „turi būti galimybė“, „turi būti sukurtas (-a)“ yra lygiaverčiai ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą



funkcionalumą ar suteikti atitinkamas paslaugas. Funkcionalumas, kuris yra nurodytas būsimuoju laiku (bus, leis, apims ir t.t.) nurodo siekiamą įgyvendinti būseną ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą.

ⁱⁱ Kai nurodytas tikslus Prekių kiekis, Pirkėjas įsipareigoja išpirkti visą nurodytą prekių kiekį.