Eil.Nr.	Pirkimo dokumentuose nustatyti prekių techniniai rodikliai	Siūlomos prekės techniniai rodikliai
	Bendrieji reikalavimai:	
1.1.	visa pateikiama techninė įranga privalo būti nauja (negali būti atnaujinta, restauruota (angl. refurbished), nenaudota, pateikta nepažeistoje gamyklinėje pakuotėje;	visa pateikiama techninė įranga yra nauja (ne atnaujinta, ne restauruota (angl. refurbished), nenaudota, bus pateikta nepažeistoje gamyklinėje pakuotėje;
1.2.	tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time ar Discontinued);	tiekėjas užtikrina, kad gamintojas nėra paskelbęs žinios apie siūlomos įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time ar Discontinued);
1.3.	tiekėjas turi pateikti nuorodą ir momentinę ekrano nuotrauką (ekranvaizdį) į gamintojo puslapį arba įrangos el. katalogą, kuriame yra tiksli pasiūlymą atitinkančios techninės ar programinės įrangos techninė specifikacija;	Gamintojo nuoroda: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series
1.4.	įrangos dokumentai turi būti lietuvių arba anglų kalba. Užrašai ant įrenginio ir jo dalių turi būti anglų arba lietuvių kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama anglų arba lietuvių kalba;	įrangos dokumentai yra anglų kalba. Užrašai ant įrenginio ir jo dalių yra anglų kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama anglų kalba;
1.5.	tiekėjas į savo pasiūlymą turi įtraukti visą aparatinę ir programinę įrangą bei medžiagas, reikalingas šioje specifikacijoje nurodytiems reikalavimams įvykdyti;	tiekėjas į savo pasiūlymą įtraukia visą aparatinę ir programinę įrangą bei medžiagas, reikalingas šioje specifikacijoje nurodytiems reikalavimams įvykdyti;
1.6.	visos techninės įrangos maitinimo įtampa turi būti 230 V 50 Hz su Europos kontinentinėje dalyje naudojama jungtimi vokiškąją (CEE 7/7);	visos techninės įrangos maitinimo įtampa yra 230 V 50 Hz su Europos kontinentinėje dalyje naudojama jungtimi vokiškąją (CEE 7/7);
1.7.	techninė įranga privalo veikti be sutrikimų, kai temperatūros režimas techninės įrangos įdiegimo patalpoje yra nuo +10 ºC iki +40 ºC, o santykinė oro drėgmė – 70 % ir mažesnė;	techninė įranga veikia be sutrikimų, kai temperatūros režimas techninės įrangos įdiegimo patalpoje yra nuo +10 ºC iki +40 ºC, o santykinė oro drėgmė – 70 % ir mažesnė;
1.8.	tiekėjas privalo pasiūlyme pateikti įrangos ir visų jos sudėtinių dalių gamintojo identifikacinius kodus;	tiekėjas pasiūlyme pateikia įrangos ir visų jos sudėtinių dalių gamintojo identifikacinius kodus: PAN-PA-460, PAN-SVC-BKLN-460-3YR, PAN-PA-400-RACKTRAY, PAN-PWR-50W-AC, PAN-PA-460-ATP-3YR-HA2, PAN-PA-460-ADVURL-3YR-HA2, PAN-PA-460-GP-3YR-HA2.

1.9.	saugumo reikalavimai (netaikoma programinei įrangai):	
1.9.1.	standieji ar puslaidininkiniai diskai (angl. HDD/SSD) ar kitos atminties laikmenos gedimo atveju turi būti keičiamos naujomis. sugedusios atminties laikmenos sunaikinamos pirkėjo patalpose ir tiekėjui negrąžinamos;	standieji ar puslaidininkiniai diskai (angl. HDD/SSD) ar kitos atminties laikmenos gedimo atveju keičiamos naujomis. sugedusios atminties laikmenos sunaikinamos pirkėjo patalpose ir tiekėjui negrąžinamos;
1.9.2.	įrangos gedimo atveju iš instaliacijos vietos remontui išvežamą pas tiekėją (jo atstovą) sugedusią įrangą pirkėjas pateikia be joje sumontuotų standžiųjų ar puslaidininkinių diskų (angl. HDD/SSD) ar kitų atminties laikmenų.	įrangos gedimo atveju iš instaliacijos vietos remontui išvežamą pas tiekėją (jo atstovą) sugedusią įrangą pirkėjas pateikia be joje sumontuotų standžiųjų ar puslaidininkinių diskų (angl. HDD/SSD) ar kitų atminties laikmenų.
1.10.	įranga, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalyje ir 37 straipsnio 10 dalyje numatyta išimtimi, turi nekelti grėsmės nacionaliniam saugumui.	įranga, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalyje ir 37 straipsnio 10 dalyje numatyta išimtimi, nekelia grėsmės nacionaliniam saugumui.
1.11.	įrangos gamintojas privalo užtikrinti Europos Sąjungos RoHS (angl. „Restriction of Hazardous Substances“) direktyvų (2002/95/EC (RoHS 1), 2011/65/EU (RoHS 2), 2015/863 (RoHS 2 amendment)), draudžiančių gamyboje naudoti aplinkai ir žmogaus sveikatai pavojingas medžiagas (pvz., gyvsidabrį, kadmį, šviną, šešiavalentį chromą, o taip pat antipirenus), reikalavimų įvykdymą. Įranga turi atitikti Lietuvos Respublikos kibernetinio saugumo įstatymo (TIS 2 direktyvos) reikalavimus.	įrangos gamintojas užtikrina Europos Sąjungos RoHS (angl. „Restriction of Hazardous Substances“) direktyvų (2002/95/EC (RoHS 1), 2011/65/EU (RoHS 2), 2015/863 (RoHS 2 amendment)), draudžiančių gamyboje naudoti aplinkai ir žmogaus sveikatai pavojingas medžiagas (pvz., gyvsidabrį, kadmį, šviną, šešiavalentį chromą, o taip pat antipirenus), reikalavimų įvykdymą. Įranga atitinka Lietuvos Respublikos kibernetinio saugumo įstatymo (TIS 2 direktyvos) reikalavimus.
Reikalaujami funkciniai, techniniai ir kokybiniai parametrai:		
2.1.	**Konstrukcija:** Įrenginį turi sudaryti aparatinis-programinis sprendimas, skirtas užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, srautų turinio kontrolę. Įrenginys turi turėti ne mažiau kaip 8 10/100/1000 Base-T Ethernet ir (arba) SFP tipo prievadus, įskaitant jų kombinaciją (pvz., 4 10/100/1000 Base-T Ethernet bei 4 SFP tipo prievadai) Įrenginys valdymui turi turėti ne mažiau kaip vieną konsolės prievadą, vieną atskirą 10/100/1000 Base-T Ethernet prievadą ir USB prievadą. Įrenginys turi turėti ne mažiau kaip 2 10/100/1000 Base-T Ethernet prievadus aukšto patikimumo klasterio funkcionalumui. Jei	**Konstrukcija:** Įrenginį sudaro aparatinis-programinis sprendimas, skirtas užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, srautų turinio kontrolę. Įrenginys turi 8 10/100/1000 Base-T Ethernet prievadus. Įrenginys valdymui turi vieną konsolės prievadą, vieną atskirą 10/100/1000 Base-T Ethernet prievadą ir USB prievadą. Įrenginys turi 2 10/100/1000 Base-T Ethernet prievadus aukšto patikimumo klasterio funkcionalumui. Šiam funkcionalumui užtikrinti gali būti panaudoti du prijungimo prievadai, iš reikalaujamų 8 (aštuoni) vnt.

	gamintojo programinė įranga leidžia, šiam funkcionalumui užtikrinti gali būti panaudoti ir ne mažiaus kaip du prijungimo prievadai, iš reikalaujamų 8 (aštuoni) vnt. Įrenginys turi būti sukomplektuotas su visais tvirtinimo elementais ir laikikliais, siekiant jį sumontuoti 19“ komutacinėje spintoje. Elektros maitinimas – kintamos srovės, 220 V įtampos. Įrenginys privalo naudoti dubliuotus, vienas kitą rezervuojančius maitinimo šaltinius.	Įrenginys sukomplektuotas su visais tvirtinimo elementais ir laikikliais, siekiant jį sumontuoti 19“ komutacinėje spintoje. Elektros maitinimas – kintamos srovės, 220 V įtampos. Įrenginys naudoja dubliuotus, vienas kitą rezervuojančius maitinimo šaltinius.
2.2.	**Aukšto patikimumo funkcijos:** Įrenginys turi turėti galimybę dirbti Aktyvus/Pasyvus (angl. „Active/Pasive“) ir Aktyvus / Aktyvus (angl. „Active/Active“) režimais. Turi būti galimybė automatiškai sinchronizuoti konfigūraciją tarp aukšto patikimumo narių. Turi būti galimybė automatiškai sinchronizuoti aktyvias sesijas tarp aukšto patikimumo narių. Turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būna aktyvus. Turi būti įdiegtas aukšto pasiekiamumo (angl. High Availability) sprendimas leidžiantis naudotis vienu išoriniu IP adresu. Aukšto patikimumo sistemos nariai turi stebėti tinklo prievadų būseną. Turi būti galimybė stebėti ar atsiliepia nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai neatsiliepia.	**Aukšto patikimumo funkcijos:** Įrenginys gali dirbti Aktyvus/Pasyvus (angl. „Active/Pasive“) ir Aktyvus / Aktyvus (angl. „Active/Active“) režimais. Yra galimybė automatiškai sinchronizuoti konfigūraciją tarp aukšto patikimumo narių. Yra galimybė automatiškai sinchronizuoti aktyvias sesijas tarp aukšto patikimumo narių. Yra galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būna aktyvus. Bus įdiegtas aukšto pasiekiamumo (angl. High Availability) sprendimas leidžiantis naudotis vienu išoriniu IP adresu. Aukšto patikimumo sistemos nariai gali stebėti tinklo prievadų būseną. Yra galimybė stebėti ar atsiliepia nurodyti IP adresai. Sistema gali automatiškai persijungti jei nurodyti IP adresai neatsiliepia.
2.3.	**Našumas:** Ugniasienės ir programų kontrolės greitaveika ne mažesnė kaip 4.5 Gbps. Įrenginio greitaveika naudojant apsaugą nuo grėsmių (apsauga nuo virusų, piktybinių kodų, įsilaužimų, pažeidžiamumo aptikimas) – ne mažesnė kaip 3 Gbps. IPSEC VPN greitaveika ne mažesnė kaip 2 Gbps. Ne mažiau kaip 350 000 konkurentinių sesijų. Ne mažiau kaip 65 000 naujų sesijų per sekundę. Ne mažiau kaip 4 000 VLAN žymių per įrenginį / prievadą.	**Našumas:** Ugniasienės ir programų kontrolės greitaveika - 4.6 Gbps. Įrenginio greitaveika naudojant apsaugą nuo grėsmių (apsauga nuo virusų, piktybinių kodų, įsilaužimų, pažeidžiamumo aptikimas) – 3 Gbps. IPSEC VPN greitaveika - 2.3 Gbps. 400 000 konkurentinių sesijų. 67 000 naujų sesijų per sekundę. 4 094 VLAN žymių per įrenginį / prievadą. 3 000 virtualių prievadų.

	Ne mažiau, kaip 1 000 virtualių prievadų. Turi būti galimybė sukonfigūruoti ne mažiau du virtualius maršrutizatorius. Virtualūs maršrutizatoriai turi turėti atskiras maršrutizavimo lenteles. Turi būti galimybė sukonfigūruoti ne mažiau 100 saugumo zonų	Yra galimybė sukonfigūruoti 5 virtualius maršrutizatorius. Virtualūs maršrutizatoriai turi atskiras maršrutizavimo lenteles. Yra galimybė sukonfigūruoti 100 saugumo zonų
2.4.	**Įrenginio funkcijos:** Darbo režimai: - Skaidrus; - Maršrutizavimo (L3); - 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 arba lygiavertį. Turi būti galimybė apjungti į vieną loginę tinklo sąsają nemažiau kaip 4 fizines sąsajas. Loginė sąsaja gali būti naudojama kaip L2 arba L3 lygio sąsaja. Turi palaikyti LACP protokolą arba lygiavertį. Įrenginys turi palaikyti IEEE 802.1q protokolą arba lygiavertį. Galimybė VLAN sąsajas kurti tinklo sąsajoms, dirbančioms L2 ir L3 lygyje. Įrenginys turi palaikyti Jumbo paketus arba lygiaverčius. Įrenginys turi palaikyti statinį IP maršrutizavimą, dinaminius maršrutizavimo protokolus: BGP, OSPFv2, OSPFv3, RIPv2 arba lygiaverčius. Sprendimas privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai. Įrenginys turi palaikyti PPPoE (Point-to-Point Protocol over Ethernet) arba lygiavertį. Įrenginys turi palaikyti grakštų BGP perkrovimą (angl. graceful restart) arba lygiavertį. Įrenginys turi palaikyti grupinio transliavimo (angl. multicast) maršruto parinkimą: PIM-SM, PIM-SSM arba lygiavertį. Įrenginys turi palaikyti antros ir trečios versijų IGMP protokolą arba lygiavertį. Įrenginys turi palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio / paskirties zoną,	**Įrenginio funkcijos:** Darbo režimai: - Skaidrus; - Maršrutizavimo (L3); - Pasyvaus stebėjimo (angl. „Sniffer/TAP“). Yra galimybė įrenginį sukonfigūruoti taip, kad jis vienu metu, vienoje sistemoje, dirbtų visais palaikomais darbo režimais. Palaiko 802.3ad. Yra galimybė apjungti į vieną loginę tinklo sąsają 4 fizines sąsajas. Loginė sąsaja gali būti naudojama kaip L2 arba L3 lygio sąsaja. Palaiko LACP protokolą. Įrenginys palaiko IEEE 802.1q protokolą. Yra galimybė VLAN sąsajas kurti tinklo sąsajoms, dirbančioms L2 ir L3 lygyje. Įrenginys palaiko Jumbo paketus. Įrenginys palaiko statinį IP maršrutizavimą, dinaminius maršrutizavimo protokolus: BGP, OSPFv2, OSPFv3, RIPv2. Sprendimas palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai. Įrenginys palaiko PPPoE (Point-to-Point Protocol over Ethernet). Įrenginys palaiko grakštų BGP perkrovimą (angl. graceful restart). Įrenginys palaiko grupinio transliavimo (angl. multicast) maršruto parinkimą: PIM-SM, PIM-SSM. Įrenginys palaiko antros ir trečios versijų IGMP protokolą.

	siuntėjo, gavėjo IP adresą, servisą, vartotojo ID, vartotojų grupę, programą (angl. application) arba lygiavertį. Turi palaikyti IPv6 protokolą arba lygiavertį. Turi palaikyti adresų transliavimą (angl. NAT) statiniam IP, dinaminiam IP, dinaminiam IP ir prievadui (port address translation) arba lygiavertį. Turi palaikyti adresų transliavimą tarp IPv6 ir IPv4 arba lygiavertį. Turi palaikyti DHCP tarnybinės stoties ir DHCP relay funkcijas arba lygiavertes. Įrenginys turi atpažinti ir kontroliuoti programas (angl. application) (pvz., Googlemail, Googletalk,, Facebook ir lygiavertes) nepriklausomai nuo to kokie yra naudojami prievadai, protokolai, naudojamas SSL ar ne. Įrenginys turi saugoti nuo atakų, piktybinių kodų (pvz., virusai, šnipinėjimo programos ir lygiavertės), stabdyti konfidencialios informacijos perdavimą (pvz., pagal raktinius žodžius, pagal IT politiką ir pan.), tikrinti perduodamą srautą nuo virusų. Jei tam būtina licencija, ji privalo būti pateikta kartu su įrenginiu. Turi būti galimybė nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme. Turi būti galimybė įrašyti ne mažiau 40 paketų, susijusių su grėsme. Įrenginys turi atpažinti ir kontroliuoti ne mažiau kaip 4 000 programų. (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Turi būti galimybė apsirašyti savo programą. Turi būti galimybė kiekvienai aplikacijai, individualiai, pačios aplikacijos nustatymuose, nustatyti laiką (angl. timeout), po kurio neaktyvi sesija su ta aplikacija 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 kurti taisykles pagal šalis, t. y. siuntėjo ir (arba) gavėjo laukuose nurodyti šalį.	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). Palaiko IPv6 protokolą. Palaiko adresų transliavimą (angl. NAT) statiniam IP, dinaminiam IP, dinaminiam IP ir prievadui (port address translation). Palaiko adresų transliavimą tarp IPv6 ir IPv4. Palaiko DHCP tarnybinės stoties ir DHCP relay funkcijas. Įrenginys geba atpažinti ir kontroliuoti programas (angl. application) (pvz., Googlemail, Googletalk,, Facebook ir lygiavertes) nepriklausomai nuo to kokie yra naudojami prievadai, protokolai, naudojamas SSL ar ne. Įrenginys geba saugoti nuo atakų, piktybinių kodų (pvz., virusai, šnipinėjimo programos ir lygiavertės), stabdyti konfidencialios informacijos perdavimą (pvz., pagal raktinius žodžius, pagal IT politiką ir pan.), tikrinti perduodamą srautą nuo virusų. Licencija pateikiama kartu su įrenginiu. Yra galimybė nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme. Yra galimybė įrašyti 40 paketų, susijusių su grėsme. Įrenginys geba atpažinti ir kontroliuoti virš 4 000 programų. (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Yra galimybė apsirašyti savo programą. Yra galimybė kiekvienai aplikacijai, individualiai, pačios aplikacijos nustatymuose, nustatyti laiką (angl. timeout), po kurio neaktyvi sesija su ta aplikacija yra uždaroma. Yra 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 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. Saugumo taisyklėse įrenginys turi rodyti kokios aplikacijos aptiktos duomenų srautuose, pakliūvančiuose po ta taisykle. Informacija apie aptiktas aplikacijas privalo būti matoma tiesiogiai pačioje saugumo taisyklėje. Saugumo taisyklėse turi būti galima išfiltruoti nenaudojamas taisykles: Per paskutines 30 (trisdešimt) dienų; Per paskutines 90 (devyniasdešimt) dienų; Niekada nenaudotas (po paskutinio įrenginio perkrovimo). Kaip saugumo taisyklės taikymo kriterijų (angl. policy match criteria) turi būti galima nurodyti konkretų pilną Web svetainės adresą (URL). Saugumo taisyklė taikoma tik tuomet, kai kreipiamasi į taisyklėje nurodytą konkretų Web adresą. Turi būti galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones. 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. Turi būti galimybė suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta. Turi būti galimybė suteikti prieigos teises vartotojams, ir (arba) vartotojų grupėms. Turi būti galimybė įrenginį integruoti su Active Directory, LDAP, Microsoft Terminal Services, RADIUS. Turi būti galimybė integruoti įrenginį su Active Directory, LDAP servisais ir sinchronizuoti vartotojų bei IP adresų informaciją be papildomos programinės įrangos naudojimo.	Yra galimybė kurti taisykles pagal šalis, t. y. siuntėjo ir (arba) gavėjo laukuose nurodyti šalį. Yra galimybė riboti prisijungimų iš vieno šaltinio skaičių pagal siuntėjo IP, gavėjo IP, siuntėjo ir gavėjo IP. Kuriant ugniasienės saugumo taisykles yra galimybė nurodyti siuntėją, gavėją, servisą / prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Servisai / prievadai ir programos taisyklėse nurodomi atskiruose laukuose. Saugumo taisyklėse įrenginys rodo kokios aplikacijos aptiktos duomenų srautuose, pakliūvančiuose po ta taisykle. Informacija apie aptiktas aplikacijas matoma tiesiogiai pačioje saugumo taisyklėje. Saugumo taisyklėse galima išfiltruoti nenaudojamas taisykles: Per paskutines 30 (trisdešimt) dienų; Per paskutines 90 (devyniasdešimt) dienų; Niekada nenaudotas (po paskutinio įrenginio perkrovimo). Kaip saugumo taisyklės taikymo kriterijų (angl. policy match criteria) galima nurodyti konkretų pilną Web svetainės adresą (URL). Saugumo taisyklė taikoma tik tuomet, kai kreipiamasi į taisyklėje nurodytą konkretų Web adresą. Yra galimybė skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones. Yra galimybė suteikti vartotojams prieigą prie programos (-ų) (ne serviso / prievado) nepriklausomai nuo to kokiais TCP, UDP prievadais dirba programa. Yra galimybė nurodyti prie kokių programų vartotojui leidžiama jungtis, o prie kokių neleidžiama, net jei programos dirba tais pačiais TCP, UDP prievadais. Yra galimybė suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta. Yra galimybė suteikti prieigos teises vartotojams, ir (arba) vartotojų grupėms. Yra galimybė įrenginį integruoti su Active Directory, LDAP, Microsoft Terminal Services, RADIUS.

	Turi palaikyti EAP protokolą arba lygiavertį, vartotojų autentifikavimui per RADIUS arba lygiavertį. Integracijai su išorine vartotojų duomenų saugykla turi būti galimybė naudoti API. Turi palaikyti vartotoju tapatybes nustatymą naudojant vartotojo skaitmeninį sertifikatą. Atliekant vartotojo tapatybės nustatymą, turi būti galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse. Turi palaikyti Kerberos protokolą arba lygiavertį. Sprendimas turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. Turi būti galimybė dešifruoti ir tikrinti SSL duomenų srautą, nukreiptą į 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 arba lygiaverčiui. 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 dešifruoti bent TLS 1.2 srautą. Turi gebėti aptikti PQC (angl. Post-quantum cryptography) šifravimo algoritmus sesijose. Aptikus PQC, ugniasienė turi sukurti žurnalinį įvykį (angl. log), gebėti iš ClientHello paketų pašalinti PQC algoritmus arba blokuoti sesiją. Privalo palaikyti RFC 8784 standartą (angl. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security) arba lygiavertį. Įrenginys turi atpažinti programas, bandančias naudoti HTTP CONNECT metodą arba lygiavertį. Turi būti galimybė aptikti Botnet arba lygiavertį. Turi būti galimybė riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus.	Yra galimybė integruoti įrenginį su Active Directory, LDAP servisais ir sinchronizuoti vartotojų bei IP adresų informaciją be papildomos programinės įrangos naudojimo. Palaiko EAP protokolą, vartotojų autentifikavimui per RADIUS. Integracijai su išorine vartotojų duomenų saugykla yra galimybė naudoti API. Palaiko vartotojų tapatybės nustatymą naudojant vartotojo skaitmeninį sertifikatą. Atliekant vartotojo tapatybės nustatymą, yra galimybė vartotojo duomenų paiešką atlikti keliose tapatybės nustatymo tarnybinėse stotyse. Palaiko Kerberos protokolą. Sprendimas gali dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. Yra galimybė dešifruoti ir tikrinti SSL duomenų srautą, nukreiptą į tarnybines stotis. Yra galimybė nurodyti, kurį duomenų srautą dešifruoti, o kurio ne. SSL patikra atliekama visam SSL duomenų srautui, ne tik HTTPS, SMTPS, POP3S, IMAPS arba lygiaverčiui. SSL patikra apima įsilaužimų, pažeidžiamumų aptikimą ir prevenciją, apsaugą nuo virusų, šnipinėjimo programų, perduodamų failų kontrolę, perduodamų duomenų turinio kontrolę, URL filtravimą. Įrenginys gali dešifruoti ir tikrinti SSH duomenų srautą. Įrenginys gali dešifruoti TLS 1.2 srautą. Geba aptikti PQC (angl. Post-quantum cryptography) šifravimo algoritmus sesijose. Aptikus PQC, ugniasienė sukuria žurnalinį įvykį (angl. log), geba iš ClientHello paketų pašalinti PQC algoritmus arba blokuoti sesiją. Palaiko RFC 8784 standartą (angl. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security). Įrenginys geba atpažinti programas, bandančias naudoti HTTP CONNECT metodą.

	Turi būti galimybė atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). Jei tam būtina licencija, ji privalo būti pateikta. Turi būti galimybė sukurti draudžiamų URL ir IP sąrašą. Turi būti galimybė automatiškai, nurodytu periodiškumu, importuoti URL, IP adresus, domenų vardus, kurie bus naudojami saugumo politikose, iš išorinio failo. Turi būti galimybė importuoti ne mažiau kaip 10 000 įrašų. Turi būti galimybė sukurti ir naudoti savo URL grupes. Turi būti galimybė sustabdyti perduodamus .xls, .xlsx, .doc., .docx, .ppt, .pptx, .txt arba lygiaverčio tipo plėtinių rinkmenas, kuriuose randamas apsibrėžtas duomenų šablonas. Turi būti galimybė aptikti apsibrėžtus duomenų šablonus įvairių programų duomenų sraute. Turi būti galimybė šablonus kurti naudojant „regular expression“ arba lygiaverčiu metodu. Turi būti galimybė kontroliuoti perduodamas bylas. Įrenginys turi atpažinti ne mažiau kaip 50 bylų tipų. Bylos tipas turi būti atpažįstamas pagal bylos turinį, o ne išplėtimą. Turi būti galimybė kurti pažeidžiamumo aprašus. Turi būti galimybė kurti kombinuotus pažeidžiamumo aprašus, t. y. aprašus į kuriuos būtų įtraukti keli jau sukurti aprašai. Turi palaikyti ne mažiau kaip 2 500 IPSec VPN tunelių. Turi būti galimybė naudoti FQDN, kaip nutolusio taško adresą, Site-to-Site VPN konfigūracijoje. 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 arba lygiavertį. Nuotolinio prisijungimo vartotojų VPN klientas turi mokėti dirbti IPSEC ir SSL protokolais arba lygiaverčiais. Turi būti galimybė prisijungti ne mažiau nei 500 VPN naudotojų. Jei tam būtina licencija, ji privalo būti pateikta.	Yra galimybė aptikti Botnet. Yra galimybė riboti prisijungimų skaičių pagal siuntėjo, gavėjo IP adresus, servisus, vartotojus. Yra galimybė atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). Licencija bus pateikta. Yra galimybė sukurti draudžiamų URL ir IP sąrašą. Yra galimybė automatiškai, nurodytu periodiškumu, importuoti URL, IP adresus, domenų vardus, kurie bus naudojami saugumo politikose, iš išorinio failo. Yra galimybė importuoti 10 000 įrašų. Yra galimybė sukurti ir naudoti savo URL grupes. Yra galimybė sustabdyti perduodamus .xls, .xlsx, .doc., .docx, .ppt, .pptx, .txt tipo plėtinių rinkmenas, kuriuose randamas apsibrėžtas duomenų šablonas. Yra galimybė aptikti apsibrėžtus duomenų šablonus įvairių programų duomenų sraute. Yra galimybė šablonus kurti naudojant „regular expression“ metodą. Yra galimybė kontroliuoti perduodamas bylas. Įrenginys gali atpažinti 50 bylų tipų. Bylos tipas atpažįstamas pagal bylos turinį, o ne išplėtimą. Yra galimybė kurti pažeidžiamumo aprašus. Yra galimybė kurti kombinuotus pažeidžiamumo aprašus, t. y. aprašus į kuriuos įtraukti keli jau sukurti aprašai. Palaiko 2 800 IPSec VPN tunelių. Yra galimybė naudoti FQDN, kaip nutolusio taško adresą, Site-to-Site VPN konfigūracijoje. Palaiko 3DES, AES256 šifravimo algoritmus. Palaiko SHA-1, SHA-256, SHA-384, SHA-512, 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 turi palaikyti bent Windows 10 64 bit, Mac OS, Linux arba lygiavertes operacines sistemas. Jei tam būtina licencija, ji privalo būti pateikta. Turi būti galimybė sukonfigūruoti vidinio tinklo aptikimą VPN prisijungimo metu tikrinant nurodyto DNS vardo užklausos rezultatą su nurodytu IPv4 arba IPv6 IP adresu. Aptikus vidinį tinklą VPN tunelis neužmezgamas. Turi būti galimybė nustatyti, kokį srautą siųsti / nesiųsti per VPN tunelį priklausomai nuo to, koks yra paskirties domenas, klientinis procesas arba HTTP/HTTPS vaizdo transliavimo programa. Nuotolinio prisijungimo vartotojų VPN klientas turi gebėti jungtis prie VPN išorinių šliuzų pagal prioritetus ir (arba) priklausomai nuo geografinės vietos prie arčiausiai esančio ir geriausiai pasiekiamo išorinio VPN šliuzo. Turi būti galimybė nustatyti, kad vieni VPN šliuzai parenkami automatiškai, o kiti būtų naudojami tik juos išsirinkus VPN kliente rankiniu būdu. Turi būti galimybė nustatyti, kad VPN klientams būtų dalinami skirtingi VPN kliento parametrai bei skirtingi VPN šliuzų sąrašai priklausomai nuo to, kokiai vartotojų grupei priklauso vartotojas ar iš kokio regiono, IP adreso, operacinės sistemos jungiamasi. VPN klientas turi gebėti atlikti sprendimo administratoriaus nustatytas patikras prieš leidžiant vartotojui prisijungti per VPN. Turi būti galimybė atlikti patikras ir viso prisijungimo per VPN metu, kai VPN programinė įranga reguliariai siunčia VPN terminuojančiam taškui / įrenginiui prisijungusio per VPN vartotojo įrenginio būsenos statusą pagal iš anksto sukonfigūruotus patikros kriterijus. Jei patikros metu atrandami atitikimai / neatitikimai sukonfigūruotoms patikroms, vartotojas turi būti neprileidžiamas prie per VPN pasiekiamų resursų, ir VPN programinė įranga turi gebėti informuoti vartotoją su VPN sprendimo administratoriaus iš anksto sukonfigūruotais pranešimais, kuriuose gali būti nuorodos į kitus šaltinius, pvz., nesant antivirusinės programinės įrangos besijungiančio vartotojo kompiuteryje, pateikiamas atitinkamas pranešimas su URL nuoroda, iš kur parsisiųsti antivirusinę programinę įrangą. Šią programinę įrangą VPN vartotojui	Yra galimybė prisijungti 1500 VPN naudotojų. Licencija nebūtina. Nuotolinio prisijungimo vartotojų VPN klientas palaiko Windows 10 64 bit, Mac OS, Linux operacines sistemas. Licencija pateikiama. Yra galimybė sukonfigūruoti vidinio tinklo aptikimą VPN prisijungimo metu tikrinant nurodyto DNS vardo užklausos rezultatą su nurodytu IPv4 arba IPv6 IP adresu. Aptikus vidinį tinklą VPN tunelis neužmezgamas. Yra galimybė nustatyti, kokį srautą siųsti / nesiųsti per VPN tunelį priklausomai nuo to, koks yra paskirties domenas, klientinis procesas arba HTTP/HTTPS vaizdo transliavimo programa. Nuotolinio prisijungimo vartotojų VPN klientas geba jungtis prie VPN išorinių šliuzų pagal prioritetus ir (arba) priklausomai nuo geografinės vietos prie arčiausiai esančio ir geriausiai pasiekiamo išorinio VPN šliuzo. Yra galimybė nustatyti, kad vieni VPN šliuzai parenkami automatiškai, o kiti būtų naudojami tik juos išsirinkus VPN kliente rankiniu būdu. Yra galimybė nustatyti, kad VPN klientams būtų dalinami skirtingi VPN kliento parametrai bei skirtingi VPN šliuzų sąrašai priklausomai nuo to, kokiai vartotojų grupei priklauso vartotojas ar iš kokio regiono, IP adreso, operacinės sistemos jungiamasi. VPN klientas geba atlikti sprendimo administratoriaus nustatytas patikras prieš leidžiant vartotojui prisijungti per VPN. Yra galimybė atlikti patikras ir viso prisijungimo per VPN metu, kai VPN programinė įranga reguliariai siunčia VPN terminuojančiam taškui / įrenginiui prisijungusio per VPN vartotojo įrenginio būsenos statusą pagal iš anksto sukonfigūruotus patikros kriterijus. Jei patikros metu atrandami atitikimai / neatitikimai sukonfigūruotoms patikroms, vartotojas neprileidžiamas prie per VPN pasiekiamų resursų, ir VPN programinė įranga geba informuoti vartotoją su VPN sprendimo administratoriaus iš

	parsisiuntus ir įsirašius į kompiuterį, VPN klientas turi atlikti patikrą ir leisti VPN vartotojui pasiekti resursus. 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 prioretizuoti duomenų paketus. Turi būti galimybė pasirinktam duomenų srautui nustatyti maksimalų pralaidumą. Turi būti galimybė pasirinktam duomenų srautui nustatyti garantuotą pralaidumą. Turi būti galimybė kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t. y. sukurti vieną taisyklę, kuri leistų iš ne mažiau kaip dviejų ar daugiau zonų jungtis į ne mažiau kaip į dvi ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei. Įrenginio laiko sinchronizavimas su NTP arba lygiaverčiu serveriu atliekant autentifikavimą. Sesijų sinchronizavimas atliekant operacinės sistemos atnaujinimą. Turi būti galimybė sugeneruoti „self-signed“ arba lygiavertį sertifikatą. Galimybė importuoti skaitmeninius sertifikatus. Turi palaikyti CRL arba lygiavertį. Turi palaikyti OCSP protokolą arba lygiavertį. Turi būti galimybė importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus. Turi palaikyti 4096 bitų RSA sertifikatus arba lygiaverčius. Turi palaikyti SHA-256, SHA-512, saugios maišos algoritmus arba lygiaverčius. Įrenginys turi galėti atsisiųsti programinės įrangos atnaujinimus iš gamintojo puslapio.	anksto sukonfigūruotais pranešimais, kuriuose gali būti nuorodos į kitus šaltinius, pvz., nesant antivirusinės programinės įrangos besijungiančio vartotojo kompiuteryje, pateikiamas atitinkamas pranešimas su URL nuoroda, iš kur parsisiųsti antivirusinę programinę įrangą. Šią programinę įrangą VPN vartotojui parsisiuntus ir įsirašius į kompiuterį, VPN klientas gali atlikti patikrą ir leisti VPN vartotojui pasiekti resursus. Nuotolinio prisijungimo vartotojų VPN klientas palaiko galimybę griežtai tikrinti pateikiamame vartotojo sertifikate nurodyto vartotojo vardo ir besijungiančio vartotojo prisijungimo vardo atitikimą. Palaiko duomenų srautų ribojimą pagal taikomąją programinę įrangą, vartotoją, siuntėjo, gavėjo IP adresus, tinklo sąsajas. Yra galimybė prioretizuoti duomenų paketus. Yra galimybė pasirinktam duomenų srautui nustatyti maksimalų pralaidumą. Yra galimybė pasirinktam duomenų srautui nustatyti garantuotą pralaidumą. Yra galimybė kurti saugumo taisykles iš karto tarp kelių saugumo zonų, t. y. sukurti vieną taisyklę, kuri leistų iš ne mažiau kaip dviejų ar daugiau zonų jungtis į ne mažiau kaip į dvi ar daugiau zonas, nekuriant atskirų taisyklių kiekvienai tarpzoninei srautų kontrolei. Įrenginio laiko sinchronizavimas su NTP serveriu atliekant autentifikavimą. Sesijų sinchronizavimas atliekant operacinės sistemos atnaujinimą. Yra galimybė sugeneruoti „self-signed“ sertifikatą. Yra galimybė importuoti skaitmeninius sertifikatus. Palaiko CRL. Palaiko OCSP protokolą. Yra galimybė importuoti tarnybinių stočių viešus, privačius raktus ir sertifikatus. Palaiko 4096 bitų RSA sertifikatus.

		Palaiko SHA-256, SHA-512, saugios maišos algoritmus. Įrenginys gali atsisiųsti programinės įrangos atnaujinimus iš gamintojo puslapio.
2.5.	**Įvykių žurnalai, ataskaitos:** Įrenginys turi generuoti ir eksportuoti Netflow v9 ar lygiaverčius įrašus apie duomenų srautus. Įvykių žurnalai turi būti kaupiami įrenginyje. 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 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 bendrą perduodamų duomenų rizikos lygį. Įrenginys turi pateikti informaciją apie duomenų srautus pagal šalis. Įrenginys turi pateikti informaciją apie labiausiai naudojamas taisykles. Turi rodyti geografinį grėsmių atvaizdavimą. Turi rodyti geografinį duomenų srautų atvaizdavimą. Turi būti galimybė nurodytų laiku įvykių žurnalus siųsti į nutolusią darbo vietą / tarnybinę stotį, naudojant SYSLOG ar lygiavertį protokolą, nereikalaujančio jokios specializuotos programinės įrangos duomenų priėmimui.	**Įvykių žurnalai, ataskaitos:** Įrenginys gali generuoti ir eksportuoti Netflow v9 įrašus apie duomenų srautus. Įvykių žurnalai gali būti kaupiami įrenginyje. Peržiūrint įvykių žurnalus, yra galimybė filtruoti įvykius. Įvykių žurnaluose yra fiksuojami administratorių atliekami veiksmai. Įrenginys gali generuoti ataskaitas apie tinkle naudojamas programas. Įrenginys gali generuoti ataskaitas apie aptiktas grėsmes. Yra galimybė sukurti savo ataskaitas. Yra galimybė automatizuoti ataskaitų generavimą. Yra galimybė sugeneruotą ataskaitą išsiųsti nurodytu elektroninio pašto adresu. Įrenginys realiu laiku gali pateikti informaciją apie perduodamus duomenų srautus. Įrenginys gali pateikti informaciją apie bendrą perduodamų duomenų rizikos lygį. Įrenginys gali pateikti informaciją apie duomenų srautus pagal šalis. Įrenginys gali pateikti informaciją apie labiausiai naudojamas taisykles. Rodo geografinį grėsmių atvaizdavimą. Rodo geografinį duomenų srautų atvaizdavimą. Yra galimybė nurodytu laiku įvykių žurnalus siųsti į nutolusią darbo vietą / tarnybinę stotį, naudojant SYSLOG protokolą.
2.6.	**Valdymo funkcijos:** Įrenginyje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginį esant dideliam tinklo aprovimui.	**Valdymo funkcijos:** Įrenginyje yra 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 galimybę įrenginį valdyti per konsolę SSH, HTTPS arba lygiaverte, 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 arba lygiavertes taisykles; - teisė peržiūrėti įvykių žurnalus; - teisė peržiūrėti ataskaitas; - teisė generuoti ataskaitas; - teisė atnaujinti programinę įranga. Galimybė administratorių tapatybės nustatymui naudoti vienkartinių slaptažodžių generatorius. Turi būti suderinama su SYSLOG ir SNMP v3 arba lygiaverčiais standartais. Turi būti galimybė keisti įvykių, siunčiamų SYSLOG protokolu, formatą (laukų išdėstymą). Turi būti galimybė siųsti įvykių žurnalus syslog formatu naudojant TCP protokolą arba SSL, arba lygiavertį. Turi būti galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis. Turi būti galimybė aktyvuoti ankstesnę konfigūraciją. Turi būti saugoma ne mažiau kaip 50 (penkiasdešimt) ankstesnių konfigūracijų. Turi būti galimybė matyti aktyvius sujungimus / sesijas. Turi būti galimybė atlikti eilę skirtingų pakeitimų ugniasienėje per grafinę sąsają ir tuos pakeitimus aktyvuoti vienu metu	Yra galimybė sukurti įrenginio naudotoją, kuris turėtų tik read-only teises (mato visą konfigūraciją, bet keisti nieko negali). Yra galimybė įrenginį valdyti per konsolę SSH, HTTPS, iš centrinės valdymo tarnybinės stoties. Administratorių prieigos teisės kontroliuojamos rolių pagalba. Yra galimybė kurti roles. Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.: - teisė keisti sisteminius įrenginio nustatymus; - teisė kurti, keisti saugumo taisykles; - teisė kurti, keisti NAT taisykles; - teisė peržiūrėti įvykių žurnalus; - teisė peržiūrėti ataskaitas; - teisė generuoti ataskaitas; - teisė atnaujinti programinę įranga. Yra galimybė administratorių tapatybės nustatymui naudoti vienkartinių slaptažodžių generatorius. Yra suderinama su SYSLOG ir SNMP v3 standartais. Yra galimybė keisti įvykių, siunčiamų SYSLOG protokolu, formatą (laukų išdėstymą). Yra galimybė siųsti įvykių žurnalus syslog formatu naudojant TCP protokolą arba SSL. Yra galimybė sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis. Yra galimybė aktyvuoti ankstesnę konfigūraciją. Gali būti saugoma 50 (penkiasdešimt) ankstesnių konfigūracijų. Yra galimybė matyti aktyvius sujungimus / sesijas. Yra galimybė atlikti eilę skirtingų pakeitimų ugniasienėje per grafinę sąsają ir tuos pakeitimus aktyvuoti vienu metu.