

## UŽSAKYMAS

### 1. SĄVOKOS IR SUTRUMPINIMAI

- 1.1. **Pirkėjas:** UAB „Ignitis grupės paslaugų centras“
- 1.2. **Atnaujintas varžymasis** – teisės aktuose, Preliminariojoje sutartyje nustatytais sąlygomis ir tvarka vykdomas atnaujintas Tiekėjų varžymasis dėl Sutarties sudarymo.
- 1.3. **Atnaujintas pasiūlymas** – teisės aktuose, Preliminariojoje sutartyje nustatytais sąlygomis ir tvarka teikiamas atnaujintas pasiūlymas dėl Sutarties sudarymo.
- 1.4. **Pasiūlymas** – Tiekėjo raštu pateiktų dokumentų ir elektroninėmis priemonėmis pateiktų duomenų visuma.
- 1.5. **Preliminarioji sutartis** – Pirkėjo ir Tiekėjo sutartis, sudaryta 2022 m. kovo mėn. 2 d., SUT-163-22.
- 1.6. **Tiekėjas** – Preliminariąją sutartį su Pirkėju sudaręs ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė.
- 1.7. **Laimėjęs tiekėjas** – Atnaujintame varžymesi laimėjusį Atnaujintą pasiūlymą pateikęs Tiekėjas, su kuriuo Pirkėjas sudaro Sutartį.
- 1.8. **Prekės** – saugumo funkcijos įranga (Ugniasienės).
- 1.9. **Sutartis** – sutartis, sudaroma tarp Laimėjusio tiekėjo ir Pirkėjo dėl Pirkimo objekto.
- 1.10. **Prekių užsakymas** – Sutarties pagrindu Tiekėjui tekstiniu pranešimu, elektroniniu paštu ir/ar per Pirkėjo nurodytą informacinę sistemą teikiamas rašytinis Prekių užsakymas, kuris laikomas Tiekėjo gautu po 24 (dvidešimt keturių) valandų nuo jo išsiuntimo Preliminariosios sutarties SD nurodytais Tiekėjo kontaktais ar kita Šalių sutarta forma.

### 2. UŽSAKYO OBJEKTAS

Saugumo funkcijos įranga (Ugniasienės).

### 3. UŽSAKYO OBJEKTO APIMTYS

- 3.1. Ugniasienės – 2 vnt.

### 4. PREKIŲ TIEKIMO VIETA

Laisvės pr. 10, 04215 Vilnius.

### 5. REIKALAVIMAI UŽSAKYO OBJEKTUI

- 5.1. Techniniai reikalavimai pateikiami lentelėje Nr.1:

Lentelė Nr.1 Ugniasienės techniniai reikalavimai

| Eil. Nr.   | Aprašymas  | Reikalavimai |
|--|--|--------------|
| 1.   | <b>Modelis, gamintojas:</b> Nurodyti gamintoją, modelį, versiją, prekės numerį. ( <i>Nurodo Tiekėjas</i> )<br>Turi būti pateikti visų siūlomos įrangos komplektuojančių dalių gamintojo produktų kodai, trumpi aprašymai bei nurodyti komplektuojančių dalių kiekiai. ( <i>Nurodo Tiekėjas</i> ) | Būtina       |
| <b>A dalis – nekeičiami esminiai reikalavimai:</b> |  |              |
| <b>Įrangos funkcijos</b>                           |  |              |
| 2.   | Turi gebėti dirbti skaidriame režime (angl. <i>transparent</i> ) ir maršrutizavimo režime (angl. <i>routed</i> ).  | Būtina       |
| 3.   | Gebėti atlikti taisyklėmis paremtą adresų transliavimą (angl. <i>policy-based NAT</i> ).   | Būtina       |
| 4.   | Turi būti IEEE 802.1Q VLAN palaikymas  | Būtina       |
| 5.   | Vartotojų grupių autentifikavimas naudojant:<br>a) LDAP arba RADIUS arba TACACS+;<br>b) Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių. Slaptažodį turi būti galima sudaryti iš ne mažiau kaip 12 (dvylikos) simbolių;  | Būtina       |

| Eil. Nr.   | Aprašymas   | Reikalavimai |
|--|---|--------------|
|  | <ul style="list-style-type: none"> <li>c) Turi būti galima nustatyti didžiausią leistiną naudotojo mėginimų įvesti teisingą slaptažodį skaičių;</li> <li>d) Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu.</li> </ul>   |              |
| 6.   | Automatinis įsilaužimų aprašų (angl. <i>signature</i> ) duomenų bazės atnaujinimas.   | Būtina       |
| 7.   | Saugumo taisyklių apjungimas į saugumo zonas kiekvienoje virtualioje ugniasienėje atskirai.   | Būtina       |
| 8.   | Įrenginys turi būti valdomas per komandinę eilutę ir grafinę sąsają.  | Būtina       |
| 9.   | Turi būti skirtingų lygių administravimo rolės.   | Būtina       |
| 10.  | Vidinis įvykių žurnalas.  | Būtina       |
| 11.  | Įvykių persiuntimas į nutolusį Syslog ar lygiavertį serverį.  | Būtina       |
| 12.  | Turi palaikyti SNMP v1 ir v2c.  | Būtina       |
| 13.  | Turi būti galima stebėti, riboti, blokuoti aplikacijas.   | Būtina       |
| <b>Garantija</b>                                       |   |              |
| 14.  | <ul style="list-style-type: none"> <li>a) Įrenginys turi būti pateikiami su gamintojo garantija 60 mėnesių (nuo sistemos pateikimo priėmimo-perdavimo akto pasirašymo dienos) ir visom reikalingoms licencijoms šiam periodui. Turi būti gaunami reguliarūs virusų, įsilaužimo aprašai, WEB kategorijos ir jų atnaujinimai. Teikiamas gamintojo palaikymas 8x5 formatu.</li> <li>b) Garantiniu laikotarpiu turi būti teikiamas nemokamas programinės įrangos klaidų šalinimas. Programinės įrangos klaidų šalinimas turi būti vykdomas kaip įmanoma per trumpesnį laiko periodą nuo Pirkėjo pranešimo Tiekėjui išsiuntimo dienos. Turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisuntimas iš gamintojo puslapio.</li> </ul> | Būtina       |
| <b>B dalis - Pakeistos techninės charakteristikos:</b> |   |              |
| 15.  | Turi būti specializuotas vieno gamintojo aparatinis – programinis sprendimas (angl. <i>appliance</i> ).   | Būtina       |
| <b>Konstrukcija</b>                                    |   |              |
| 16.  | Turi būti galima montuoti į 19 colių komutacinę spintą. Įranga turi būti pateikiama su visais montavimui reikalingais priedais.   | Būtina       |
| 17.  | Įrenginys turi būti ne didesnis kaip 2U   | Būtina       |
| 18.  | <ul style="list-style-type: none"> <li>a) Įrangos elektros maitinimas tiekiamas iš AC 230 V 50 Hz tinklo.</li> <li>b) Įranga privalo turėti du maitinimo šaltinius, užtikrinančius nepertraukiamą įrenginio veikimą sugedus vienam iš maitinimo šaltinių.</li> <li>c) Įranga turi būti pateikta kartu su maitinimo kabeliais su IEC C14 kištuku. Kabeliai turi būti skirti jungimui į rozečių blokus su IEC C13 lizdais.</li> </ul>   | Būtina       |
| 19.  | <p>Turi būti:</p> <ul style="list-style-type: none"> <li>a) ne mažiau kaip 4 (keturi) 100G (QSFP+ arba QSFP28) lizdai.</li> <li>b) ne mažiau kaip 4 (keturi) 25G SFP28 lizdai.</li> <li>c) ne mažiau kaip 12 (dvylika) 1G/10G SFP/SFP+ lizdų (kiekvienas iš lizdų privalo palaikyti SFP ir SFP+ standarto prievadų modulius.)</li> <li>d) ne mažiau kaip 8 (aštuoni) 1G/10G RJ45 tipo lizdai.</li> </ul>  | Būtina       |

| Eil. Nr.   | Aprašymas   | Reikalavimai |
|--|---|--------------|
|  | <p>Visi tinklo lizdai fiziškai turi būti realizuoti viename įrenginyje nenaudojant papildomų išorinių įrenginių (pvz. komutatoriai, kontrolieriai, srautų balansavimo įranga ir pan.)</p> <p>Įranga turi būti pateikta kartu su:</p> <ul style="list-style-type: none"> <li>4 (keturiais) 10G-SR SFP+ moduliais;</li> </ul>                                   |              |
| 20.  | Turi turėti ne mažiau kaip 2 (du) dedikuotus pajungimo į aukšto patikimumo telkinį prievadus.   | Būtina       |
| 21.  | Turi būti ne mažiau kaip 1 (vienas) RJ-45 arba USB prievadas įrangos valdymui per komandinę eilutę.   | Būtina       |
| 22.  | Įranga turi būti pateikta su visomis įrangos diegimui reikalingomis medžiagomis/detalėmis.  | Būtina       |
| <b>Įrangos sujungimo į aukšto patikimumo telkinį funkcijos</b> |   |              |
| 23.  | Įrenginys turi turėti galimybę dirbti Aktyvus/Pasyvus (angl. „Active/Passive“) ir Aktyvus/Aktyvus (angl. „Active/Active“) režimais.   | Būtina       |
| 24.  | Turi būti galimybė automatiškai sinchronizuoti konfigūraciją ir aktyvias sesijas tarp aukšto patikimumo telkinio narių.   | Būtina       |
| 25.  | Turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis aukšto patikimumo telkinio narys visada būna aktyvus.  | Būtina       |
| 26.  | Aukšto patikimumo telkinio nariai turi stebėti tinklo prievadų būseną.  | Būtina       |
| 27.  | Turi būti galimybė stebėti ar atsiliepia nurodyti IP adresai. Aukšto patikimumo telkinio sistema turi automatiškai persijungti jei nurodyti IP adresai neatsiliepia.  | Būtina       |
| 28.  | Turi būti galimybė naudoti geografiškai paskirstytą aukšto patikimumo klasterį, kurį sudarytų kiti aukšto patikimumo klasteriai, dirbantys Aktyvus/Pasyvus arba Aktyvus/Aktyvus režimais. Šiame geografiškai paskirstytame aukšto patikimumo klasteryje turi būti palaikomi ne mažiau kaip 8 (aštuoni) nariai, kurie turi sinchronizuoti sesijas tarpusavyje. | Būtina       |
| <b>Našumas</b>   |   |              |
| 29.  | Ugniasienės pralaidumas turi būti ne mažesnis kaip 50 Gb/s su įjungtu aplikacijos detektavimu (appmix paketais);  | Būtina       |
| 30.  | Įrenginio pralaidumas naudojant apsaugą nuo grėsmių (apsauga nuo virusų, programų kontrolės, piktybinių kodų, įsilaužimų, pažeidžiamumų aptikimas) turi būti ne mažesnė kaip 32 Gb/s.   | Būtina       |
| 31.  | IPSec VPN greitaveika turi būti ne mažesnė kaip 20 Gb/s.  | Būtina       |
| 32.  | Turi būti ne mažiau kaip 4500000 konkurentinių sesijų.  | Būtina       |
| 33.  | Turi būti ne mažiau kaip 250000 naujų sesijų per sekundę.   | Būtina       |
| 34.  | Sesijų skaičius turi būti įgyvendinamas vieno įrenginio pagalba, nenaudojant papildomų įrenginių, kurie paskirstytų įeinančius ar išėinančius srautus.  | Būtina       |
| 35.  | Turi būti ne mažiau kaip 4000 VLAN žymių per įrenginį/prievadą.   | Būtina       |
| 36.  | Turi būti ne mažiau kaip 4000 virtualių prievadų.   | Būtina       |
| 37.  | Turi būti leidžiama sukonfigūruoti ne mažiau kaip 20 virtualių maršrutizatorių. Virtualūs maršrutizatoriai turi turėti atskiras maršrutizavimo lenteles.  | Būtina       |
| 38.  | Turi būti leidžiama sukonfigūruoti ne mažiau kaip 4000 saugumo zonų.  | Būtina       |

| Eil. Nr.  | Aprašymas   | Reikalavimai                                    |
|---|---|---|
| 39.   | Turi būti funkcionalumas, leidžiantis įrenginį padalinti į ne mažiau kaip 10 virtualių sistemų.   | Būtina  |
| 40.   | Turi būti galimybė plėsti virtualių sistemų kiekį iki ne mažiau kaip 20.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 41.   | Turi būti leidžiama vienoje virtualioje sistemoje naudoti daugiau kaip vieną virtualų maršrutizatorių.  | Būtina  |
| <b>Įrenginio pagrindinės palaikomos funkcijos</b> |   |   |
| 42.   | Turi palaikyti statinį IP maršrutizavimą, dinامينius maršrutizavimo protokolus: BGP, OSPFv2, OSPFv3, RIPv2.   | Būtina  |
| 43.   | Sprendimas privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.<br>Turi leisti nurodyti sprendimo tinklo prievado IP adresą tuo atveju, jei konkretus tinklo prievadas turi sukonfigūruotą daugiau nei vieną IP adresą.   | Būtina  |
| 44.   | Turi palaikyti Security Group Tag (SGT) EtherType arba lygiavertį sprendimą.  | Būtina  |
| 45.   | Sprendimas turi palaikyti BFD (bidirectional forwarding detection) protokolą.   | Būtina  |
| 46.   | Įrenginys turi palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną, siuntėjo, gavėjo IP adresą, servisą, vartotojo ID, vartotojų grupę, programą (angl. application).<br>Turi būti leidžiama sukonfigūruoti paketų grąžinimą per tą patį tinklo prievadą, iš kurio atėjo pirminis paketas neatsižvelgiant į maršrutizavimo lentelėje nurodytą geriausią kelią iki paskirties adreso. | Būtina  |
| 47.   | Turi palaikyti adresų transliavimą (angl. NAT) statiniam IP, dinaminiam IP, dinaminiam IP ir prievadui (angl. port address translation).  | Būtina  |
| 48.   | Turi palaikyti FQDN objektus paskirties adresų transliavimo taisyklėse.   | Būtina  |
| 49.   | Turi leisti sukurti ne mažiau kaip 5000 NAT taisyklių.  | Būtina  |
| 50.   | Turi palaikyti adresų transliavimą tarp IPv6 ir IPv4.   | Būtina  |
| 51.   | Turi atpažinti ir kontroliuoti programas (angl. application) nepriklausomai nuo to kokie yra naudojami prievadai, protokolai, naudojamas SSL/TLS ar ne.   | Būtina  |
| 52.   | Turi gebėti saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdyti konfidencialios informacijos perdavimą (pvz., pagal raktinius žodžius, pagal IT politiką), tikrinti perduodamą srautą nuo virusų.<br>Turi būti galimybė naudoti gamintojo pateikiamus dinamiškai atnaujinamus kenksmingų IP adresų sąrašus.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 53.   | Turi būti galimybė aktyvuoti apsaugos mechanizmą, gebantį aptikti C2 (ang. Command and Control) komunikacijas per HTTP, HTTP2, SSL realiu laiku pasinaudojant ML (angl. machine learning) algoritmais.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 54.   | TCP sesijos užmezgimo metu turi leisti blokuoti TCP SYN ir SYN-ACK paketus, kuriuose yra duomenų.<br>Turi leisti blokuoti netvarkingas TCP sesijas, kurios neatitinka standarto (pvz., TCP SYN ar SYN-ACK paketus kuriuose be TCP antraštės yra duomenų).   | Būtina  |
| 55.   | Turi leisti sukonfigūruoti apsaugą nuo DoS atakų.   | Būtina  |

| Eil. Nr. | Aprašymas  | Reikalavimai                                    |
|----------|--|---|
| 56.      | Turi leisti blokuoti žvalgybos atakas, kai skenuojami TCP ir UDP protokolų prievadai. Turi būti leidžiama apsirašyti išimtis, kam netaikyti šios apsaugos.   | Būtina  |
| 57.      | Turi būti galimybė sukonfigūruoti DNS apsaugos mechanizmą, realiu laiku siunčiant aptiktas DNS užklausas patikrai į gamintojo teikiamą debesijos paslaugą.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 58.      | Turi būti galimybė patikrinti DNS užklausas pagal įrenginyje parsiusią lokalų DNS užklausų paketą tuo atveju, jei ryšys su gamintojo reikiama DNS debesijos patikros paslauga yra sutrikęs.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 59.      | DNS apsaugos mechanizmas turi gebėti: <ul style="list-style-type: none"> <li>a) aptikti DNS tuneliavimą;</li> <li>b) aptikti dinamiškai generuojamus domenų vardus (ang. DGA, Domain generation algorithm);</li> <li>c) apsaugoti nuo DNS Rebinding atakos;</li> <li>d) aptikti ir blokuoti dinaminis DNS įrašus (DDNS);</li> <li>e) aptikti ir blokuoti piktybiniu kodu (ang. malware) užkrėstus domenų;</li> <li>f) aptikti ir blokuoti naujai sukurtus (t.y., ne senesnius kaip 1 mėnesio) domenų;</li> <li>g) aptikti ir blokuoti reklaminių žymų ir marketingo stebėjimo domenų;</li> <li>h) aptikti ir blokuoti DNS užklausas, kuriomis kreipiamasi į botnet užkrėstų kompiuterių valdymo centrus;</li> <li>i) aptikti ir blokuoti DNS užklausas į socialinės inžinerijos sukčiavimo puslapius, skirtus išvilioti konfidencialius duomenis (ang. phishing);</li> <li>j) aptikti ir blokuoti DNS užklausas į puslapius, kurie padėtų vartotojams apeiti taikomas saugumo priemones naudojant anoniminius tarpinius serverius (angl. anonymizer, proxy avoidance);</li> <li>k) perrašyti DNS užklausas į kenkėjiškus puslapius nukreipiant į nurodytą įrenginio ar išorinį IP adresą (ang. DNS sinkholing).</li> </ul> | Išplėtimo galimybė įsigijus papildomą licenciją |
| 60.      | Įrenginys turi gebėti analizuoti DNS užklausas šifruotame DNS sraute, kuris nukreiptas į kitus DNS serverius HTTPS protokolu (ang. DoH - DNS-over-HTTPS).  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 61.      | Turi būti galimybė DNS apsaugos mechanizmui kategorizuoti ir leisti pasirinkti skirtingus veiksmus skirtingoms DNS kategorijoms. Pvz., blokuoti malware kategoriją, tačiau leisti grayware kategoriją.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 62.      | Turi būti galimybė nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme. Turi būti galimybė įrašyti ne mažiau kaip 40 paketų, susijusių su grėsme.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 63.      | Turi atpažinti ir kontroliuoti ne mažiau kaip 4000 programų. (Tos pačios programos skirtingos versijos turi būti skaičiuojamos kaip viena programa).   | Būtina  |
| 64.      | Turi būti leidžiama apsirašyti savo aplikaciją ir naudoti savo sukurtą aplikacijos signatūrą. Sukurtą aplikaciją turi būti galima naudoti saugumo taisyklėse.  | Būtina  |
| 65.      | Turi būti leidžiama kiekvienai aplikacijai, individualiai, pačios aplikacijos nustatymuose, nustatyti laiką (angl. timeout), po kurio neaktyvi sesija su ta aplikacija yra uždaroma.   | Būtina  |

| Eil. Nr. | Aprašymas  | Reikalavimai                                    |
|----------|--|---|
| 66.      | Turi būti leidžiama saugumo taisyklėse naudoti aplikacijų filtrus, kuriuose būtų galima įjungti filtravimą tik naujai sprendimo gamintojo sukurtoms aplikacijoms taip užtikrinant, kad saugumo taisyklė praleistų naujas aplikacijas, kurios gali turėti plataus masto arba didelės įtakos poveikį.          | Būtina  |
| 67.      | Turi būti leidžiama 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. | Būtina  |
| 68.      | Turi būti leidžiama kurti taisykles pagal šalis, t. y. siuntėjo ir/arba gavėjo laukuose nurodyti šalį.   | Būtina  |
| 69.      | Turi būti leidžiama riboti prisijungimų iš vieno šaltinio skaičių pagal siuntėjo IP, gavėjo IP, siuntėjo ir gavėjo IP.   | Būtina  |
| 70.      | Kuriant ugniasienės saugumo taisykles turi būti leidžiama nurodyti siuntėją, gavėją, servisą/prievadą, programą, taikytinas apsaugos priemonės, vartotoją, vartotojų grupę.  | Būtina  |
| 71.      | Kuriant ugniasienės saugumo taisykles, kaip saugumo taisyklės taikymo kriterijų (ang. policy match criteria) turi būti galima nurodyti konkretų pilną Web svetainės adresą (URL ir URI). Saugumo taisyklė taikoma tik tuomet, kai kreipiamasi į taisyklėje nurodytą konkretų Web adresą.                     | Būtina  |
| 72.      | Servisai/prievadai ir programos saugumo taisyklėse turi būti nurodomi atskiruose laukuose.   | Būtina  |
| 73.      | Saugumo taisyklėse įrenginys turi rodyti, kokios aplikacijos aptiktos duomenų srautuose, pakliūvančiuose po nustatyta saugumo taisyklę. Informacija apie aptiktas aplikacijas privalo būti matoma tiesiogiai pačioje saugumo taisyklėje.   | Būtina  |
| 74.      | Saugumo taisyklėse turi būti galima išfiltruoti nenaudojamas taisykles.<br>Pasirinkimai turi būti neblogesni nei:<br>a) per paskutines 30 dienų;<br>b) per paskutines 90 dienų;<br>c) niekada nenaudotas (po paskutinio įrenginio perkrovimo).   | Būtina  |
| 75.      | Saugumo taisyklėse turi būti matoma kada pirmą ir paskutinį kartą buvo panaudota taisyklė.   | Būtina  |
| 76.      | Saugumo taisyklėse turi būti matoma kada taisyklė buvo sukurta ir kada modifikuota.  | Būtina  |
| 77.      | Turi būti galimybė nurodyti, kad vartotojai gali jungtis tik prie organizacinių (angl. enterprise) SaaS aplikacijų, o prie vartotojiškų (angl. consumer) SaaS aplikacijų prisijungimas būtų draudžiamas. Kontrolė atliekama modifikuojant ar įterpiant HTTP Header informaciją.                              | Išplėtimo galimybė įsigijus papildomą licenciją |
| 78.      | Turi būti galimybė įterpti ir modifikuoti HTTP Header vertę HTTP užklausoje. Įterpiant ar modifikuojant HTTP Header vertę, turi būti galima nurodyti: administratoriaus nustatytą (ang. custom) Header pavadinimą (ang. name), Header vertę (ang. value).  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 79.      | Turi būti leidžiama naudoti žymas (angl. tags), pagal kurias vartotojai būtų dinamiškai grupuojami. Žymų informacija gali būti gaunama iš trečiųjų šalių produktų (kaip SIEM) siekiant įvertinti vartotojų rizikos lygį.   | Būtina  |

| Eil. Nr. | Aprašymas  | Reikalavimai                                    |
|----------|--|---|
| 80.      | Žymų informacija taip pat gali būti gaunama iš įrenginio žurnalinių įvykių užfiksuotos veiklos, pvz., jei vartotojas pasisiuntė kenkėjišką programinę įrangą arba bandė suvesti korporatyvinius kredencialus internetiniame puslapyje, įrenginys automatiškai priskirtų atitinkamą žymą prie vartotojo ir IP adreso susiejimo. Naudojant tokį žymų priskyrimą suveiktų saugumo taisyklė, kuri blokuotų vartotojo prieigą arba prašytų papildomai autorizotis įrenginio pateikiamame autorizavimosi portale (ang. captive portal).  | Būtina  |
| 81.      | Turi leisti suteikti prieigos teises tik vartotojams, kurių tapatybė yra patvirtinta.  | Būtina  |
| 82.      | Turi nustatyti vartotojų tapatybę, neprašydamas suvesti vartotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba programinės įrangos (agento) pagalba.   | Būtina  |
| 83.      | Įrenginys turi mokėti išnagrinėti (angl. parse) gaunamą informaciją apie vartotojus iš SYSLOG paketų pagal įrenginio administratoriaus aprašytus filtrus, bei šią informaciją pritaikyti vartotojų identifikavimui.  | Būtina  |
| 84.      | Turi leisti integruoti įrenginius su Active Directory, LDAP servais ir sinchronizuoti vartotojų bei IP adresų informaciją be papildomos programinės įrangos naudojimo.   | Būtina  |
| 85.      | Turi leisti integruoti su Okta, Google, Azure IdP (ang. Identity Provider) vartotojų autentifikavimui.   | Būtina  |
| 86.      | Turi leisti dinamiškai susieti IP adresą su vartotojo atributais pagal jo AD/LDAP autentifikavimą.   | Būtina  |
| 87.      | Jei vartotojo tapatybė nebuvo nustatyta skaidriai, vartotojui turi būti parodomas puslapis, kuriame jis turi įvesti tapatybę patvirtinančius duomenis.   | Būtina  |
| 88.      | Turi būti leidžiama kontroliuoti vartotojų, dirbančių terminalinėje aplinkoje (MS Windows Terminal server) prieigos teises. Įrenginys turi skirti terminalinėje aplinkoje dirbančių vartotojų duomenų srautus ir kontroliuoti kiekvieno vartotojo prieigos teises.   | Būtina  |
| 89.      | Turi būti leidžiama sertifikatu apsaugoti ryšį tarp sprendimo ir terminaliniame serveryje veikiančios programinės įrangos, kuri nustato vartotojų duomenų srautus.   | Būtina  |
| 90.      | Turi būti galimybė aptikti ir blokuoti vartotojų pateikiamus korporatyvinius kredencialus puslapiuose, kurie atlieka sukčiavimo atakas (angl. phishing).   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 91.      | <ul style="list-style-type: none"> <li>a) Atliekant vartotojo tapatybės nustatymą turi būti atliekama vartotojo duomenų paieška keliose tapatybės nustatymo tarnybinėse stotyse.</li> <li>b) Turi leisti nurodyti RADIUS, LDAP, TACACS+, Kerberos tarnybines stotis bei lokalią vartotojų duomenų bazę ir sudėlioti šiuos autorizacijos metodus atitinkama tvarka sąrašuose, pagal kuriuos būtų daroma patikra atliekant vartotojų autorizaciją.</li> <li>c) Turi leisti nustatyti, kad konkretus autorizacijos metodas iš nurodytųjų būtų parinktas pagal vartotojo varde matomą domeno vardą.</li> </ul> | Būtina  |
| 92.      | Atliekant vartotojo tapatybės nustatymą, turi būti gaunami vartotojo tapatybės duomenys iš trečiųjų šalių syslog šaltinių  | Būtina  |

| Eil. Nr. | Aprašymas  | Reikalavimai                                    |
|----------|--|---|
|          | (igaliotųjų serverių (angl. proxy, exchange), belaidžio ryšio kontrolierių, tinklo prieigos kontrolės sprendimų (NAC)).  |   |
| 93.      | Turi būti leidžiama nurodyti, kurį duomenų srautą dešifruoti, o kurio ne.<br>Turi būti gamintojo integruoti sąrašai su dešifravimo išimtimis srautams, kuriems negalima taikyti dešifravimo dėl žinomų priežasčių.   | Būtina  |
| 94.      | Turi būti leidžiama sukonfigūruoti vartotojams galimybę atsisakyti srauto dešifravimo, pereinančio per įrenginį. Vartotojams pateikiamas informacinis pranešimas apie srauto dešifravimą naršant HTTPS puslapiuose. Vartotojui nesutikus tolimesnis naršymas draudžiamas HTTPS puslapiuose.  | Būtina  |
| 95.      | Turi leisti kopijuoti dešifruotą srautą ir perduoti pasirinktu prievadu tolimesnei analizei išoriniams įrenginiams (angl. Decryption Mirror).  | Būtina  |
| 96.      | a) Turi būti leidžiama sulaikyti ir perduoti dešifruotą srautą į trečiųjų šalių saugumo įrenginį ar saugumo įrenginių seką, kurioje atliekamos papildomos saugumo patikros. Trečiųjų šalių saugumo įrenginio ar saugumo įrenginių sekos grąžintas srautas turi būti vėl užšifruojamas ir toliau perduodamas numatytam srauto gavėjui.<br>b) Turi būti leidžiama sukonfigūruoti daugiau nei vieną saugumo įrenginių seką, paskirstyti dešifruotą srautą per kelias saugumo įrenginių sekas. | Būtina  |
| 97.      | Turi dešifruoti ir tikrinti SSH duomenų srautą.  | Būtina  |
| 98.      | Turi dešifruoti TLS 1.2 ir TLS 1.3 srautą.   | Būtina  |
| 99.      | Turi gebėti aptikti PQC (ang. Post-quantum cryptography) šifravimo algoritmus sesijose. Aptikus PQC, ugniasienė turi sukurti žurnalinį įvykį (ang. log), gebėti iš ClientHello paketų pašalinti PQC algoritmus arba blokuoti sesiją.   | Būtina  |
| 100.     | Turi atlikti VXLAN tunelių srauto inspektavimą su galimybe parinkti VNI sesijos raktą.   | Būtina  |
| 101.     | Turi būti galimybė atlikti prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas).  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 102.     | Turi būti galimybė aktyvuoti URL filtravimo mechanizmą, kuris turi gebėti tikrinti, aptikti, dinamiškai kategorizuoti ir blokuoti kenksmingas svetaines realiu laiku, apsaugai nuo zero-day atakų.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 103.     | Turi būti galimybė aptiktus failus automatiškai siųsti ir jų saugumą analizuoti išorinėje gamintojo smėliadėžėje (ang. sandbox). Signatūras iš smėliadėžės ugniasienė turi gauti realiu laiku, naujų atakų prevencijai.  | Išplėtimo galimybė įsigijus papildomą licenciją |
| 104.     | Papildomai apsaugai nuo zero-day atakų, turi būti galimybė ugniasienei realiu laiku analizuoti perduodamus PE (portable executable) tipo failus. Failų analizė turi būti vykdoma pačioje ugniasienėje ir turi būti paremta machine learning modeliu, kuriuo aptinkami kenkėjiški failai, kuriems dar nėra sukurtos gamintojo teikiami atpažinimo šablonai (angl. signatures). Aptiktas kenkėjiškas failas turi būti blokuojamas.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 105.     | Turi automatiškai, nurodytu periodiškumu, importuoti URL, IP adresus, domėnų vardus, kurie bus naudojami saugumo politikose, iš išorinio failo. Turi būti galimybė importuoti ne mažiau kaip 50000 įrašų.  | Būtina  |



| Eil. Nr.                           | Aprašymas   | Reikalavimai                                    |
|------------------------------------|---|---|
| 106.                               | Turi būti gamintojo teikiami Microsoft 365, Azure, AWS, Google Cloud debesijos paslaugų naudojami dinaminiai IP adresų sąrašai, kuriuos turi būti galima panaudoti saugumo politikose.  | Būtina  |
| 107.                               | Turi leisti sukurti ir naudoti savo URL grupes.   | Būtina  |
| 108.                               | Turi būti galimybė atliekant URL filtravimą įrašyti į LOG pranešimus skirtingas HTTP protokolo antraštes, tokias kaip User-Agent, Referer, X-Forwarded-For.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 109.                               | Turi aptikti apsibrėžtus duomenų šablonus įvairių programų duomenų sraute. Turi būti leidžiama kurti šablonus naudojant „regular expression“. Aptikus šabloną, turi būti galimybė sustabdyti perduodamus failus (DLP/Data Filtering). | Būtina  |
| 110.                               | Turi kontroliuoti perduodamas bylas. Įrenginys turi atpažinti ne mažiau kaip 50 bylų tipų. Bylos tipas turi būti atpažįstamas pagal bylos turinį, o ne išplėtimą.   | Būtina  |
| 111.                               | Turi palaikyti ne mažiau kaip 9000 IPsec VPN tunelių.   | Būtina  |
| 112.                               | Privalo palaikyti RFC 8784 standartą (angl. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security).   | Būtina  |
| 113.                               | Turi palaikyti, be papildomų licencijų, nuotolinį vartotojų prisijungimą VPN klientu per SSL VPN Windows ir macOS operacinėms sistemoms.  | Būtina  |
| 114.                               | Turi būti galimybė nustatyti, kokį srautą siųsti/nesiųsti per VPN tunelį priklausomai nuo to, koks yra paskirties domenas, klientinis procesas arba HTTP/HTTPS video transliavimo programa.   | Išplėtimo galimybė įsigijus papildomą licenciją |
| 115.                               | Turi būti leidžiama sukurti ne mažiau kaip 25000 saugumo taisyklių.   | Būtina  |
| 116.                               | Įrenginys turi gebėti dirbti kaip IPv4 DHCP serveris ir IPv6 DHCP klientas, bei palaikyti prefixų delegaciją/priskyrimą.  | Būtina  |
| <b>Įvykių žurnalai, ataskaitos</b> |   |   |
| 117.                               | Įvykių žurnalai turi būti kaupiami įrenginyje ir siunčiami į centrinę valdymo tarnybinę stotį.  | Būtina  |
| 118.                               | Žurnaliniai įvykiai turi būti siunčiami į žurnalinių įvykių surinkimo serverius pagal nustatytus žurnalinių įvykių atributus nurodant ne vien kritiškumo lygį, bet naudojant vartotojo apsirašytus filtrus.                           | Būtina  |
| <b>Valdymo funkcijos</b>           |   |   |
| 119.                               | Įrenginyje turi būti atskiri valdymo ir duomenų analizės moduliai, kad būtų užtikrinta galimybė valdyti įrenginius esant dideliame tinklo aptarnavimui.   | Būtina  |
| 120.                               | Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti smulkiai apibrėžtos administratoriaus teisės. Turi būti leidžiama kurti roles.   | Būtina  |
| 121.                               | Turi būti leidžiama keisti įvykių, siunčiamų SYSLOG protokolu, formatą (laukų išdėstymą).   | Būtina  |
| 122.                               | Turi būti leidžiama siųsti įvykių žurnalus SYSLOG formatu naudojant TCP protokolą arba SSL.   | Būtina  |
| 123.                               | Turi būti leidžiama integruoti įrenginius su išorinėmis paslaugomis, automatizacijos tikslais naudojant XML API ir REST API.  | Būtina  |
| 124.                               | Turi būti galima sukurti, nuskaityti, pakeisti, ištrinti statinius bei dinامينius objektus, saugumo profilius, saugumo taisykles, NAT taisykles, ugniasienės prievadų, saugumo zonų, IPsec  | Būtina  |

| Eil. Nr.         | Aprašymas  | Reikalavimai |
|------------------|--|--------------|
|                  | tunelių, nuotolinio prisijungimo VPN konfigūraciją pasinaudojant REST API.   |              |
| 125.             | Turi būti detali REST API prieigos kontrolė skirtingiems administratoriams. Turi būti galima nustatyti kuris administratorius kuriuos nustatymus gali keisti, kuriuos tik matyti, kurių nematyti. Pvz. administratorius gali keisti saugumo politikas, tačiau negali keisti tinklo prievadų nustatymų ir visai nemato maršrutavimo konfigūracijos. | Būtina       |
| 126.             | Turi būti galima sulyginti einamąją įrenginio konfigūraciją su ankstesnėmis konfigūracijomis.  | Būtina       |
| 127.             | Turi būti leidžiama aktyvuoti ankstesnę konfigūraciją. Turi būti saugoma ne mažiau kaip 50 ankstesnių konfigūracijų.   | Būtina       |
| 128.             | Ugniasienėje daromi pakeitimai neturi aktyvuotis iškart. Prieš aktyvuojant pakeitimus, turi būti galimybė atlikti eilę skirtingų pakeitimų grafinėje aplinkoje ir komandinėje eilutėje, ir juos aktyvuoti vienu metu (ang. commit).  | Būtina       |
| <b>Garantija</b> |  |              |
| 129.             | a) Reakcijos laikas turi būti ne ilgesnis kaip 8 (aštuonios) darbo valandos.<br>b) Garantiniu laikotarpiu sugedęs įrenginys, jo moduliai ir dalys privalo būti pakeisti ne ilgiau kaip per 3 (tris) darbo dienas nuo Pirkėjo pranešimo Tiekėjui išsiuntimo dienos.   | Būtina       |
| 130.             | Siūlomoje įrangoje turi būti įdiegta naujausia gamintojo operacinė sistema, įskaitant esamus operacinės sistemos atnaujinimus.   | Būtina       |

## 6. ĮSIPAREIGOJIMŲ VYKDYMO TERMINAI IR TVARKA

6.1. Taikomi Preliminariojoje sutartyje numatyti terminai.

6.2. Prekės turi būti pristatytos ne vėliau kaip per 60 (*šešiasdešimt*) dienų nuo Prekių užsakymo pateikimo dienos.