2022-07-29 Nr. PSL220707EDR2-01

**UGNIASIENĖ**
**TECHNINĖ SPECIFIKACIJA**

Lietuvos sveikatos mokslų universiteto ligoninė Kauno klinikos (toliau Kauno klinikos) užtikrindamos kompiuterinio tinklo saugumą perka kompiuterinio tinklo perimetro ugniasienės sprendimą. Perkamas dubliuotas ugniasienės sprendimas, slaptažodžių raktų programinė įranga, žurnalinių įvykių valdymo platforma ir ugniasienių įrangos diegimo darbai.

Reikalavimai pateikiamai įrangai pateikiami Lentelėse Nr. 1, Nr. 2, Nr. 3. Darbai susiję su ugniasienių diegimu pateikiami Lentelėje Nr. 4.

Perkama įranga privalo būti nauja ir nenaudota, pateikiama originalioje gamintojo pakuotėje, gamykliškai atnaujinti komponentai (angl. „Refurbished“) neleistini.

Pardavėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).

Jei po pasiūlymo pateikimo (sutarties galiojimo metu) įranga nebegaminama ar sutrikęs jos tiekimas ir tiekėjas nebeturi galimybės jos tiekti, gali būti tiekiama kita to paties gamintojo (naujesnio modelio) įranga, analogiškų ar geresnių techninių savybių, nei siūlyta. Būtina pateikti gamintojo patvirtinimą, kad nėra galimybės pristatyti siūlytą įrangą.

Siūlomos įrangos gamintojas turi būti registruotas NATO arba ES priklausančioje valstybėje.

Jei iš šiose techninėse specifikacijose pateiktų duomenų būtų galima daryti prielaidą apie konkrečius pirkimo objekto modelius ar tiekimo šaltinius, konkrečius technologinius procesus ar prekių ženklus, patentus, tipus, konkrečią kilmę ar gamybą, laikoma, kad jie yra orientaciniai ir tiekėjai gali siūlyti lygiaverčius ar geresnius sprendimus.

Visa pateikiama įranga, licencijos, techninio palaikymo sutartys, turi būti užregistruotos gamintojo sistemoje, perkančiosios organizacijos vardu.

Tiekėjas turi pateikti dokumentus, įrodančius siūlomos įrangos parametrų teisingumą ir atitikimą techniniams reikalavimams, nurodytiems pirkimo dokumentų techninėje specifikacijoje. Tiekėjas turi pateikti gamintojo parengtus techninius aprašus, bukletus, katalogus anglų arba lietuvių kalbomis. Tiekėjas taip pat turi pateikti nuorodas į gamintojo interneto tinklalapį, kuriame perkančiosios organizacijos vertintojai galėtų patikrinti teikiamų duomenų autentiškumą. Perkančioji organizacija turi teisę reikalauti pateikti katalogų ir techninių aprašų originalus, o tiekėjui jų nepateikus – pasiūlymą atmesti.

Tiekėjas, teikdamas pasiūlymą turi užpildyti stulpelį Siūloma charakteristika, konkrečiais siūlomos įrangos ar paslaugų parametrais. Pažodinis reikalavimų kopijavimas ar konkrečių reikšmių neįrašymas yra laikytinas netinkamu pasiūlymo pateikimu ir gali tapti priežastimi pasiūlymui atmesti.

**Perkamų prekių/paslaugų sąrašas**

| Eil. Nr. | Prekių / paslaugų pavadinimas | Mato vnt. | Kiekis |
|---|---|---|---|
| 1. | Kompiuterinio tinklo perimetro ugniasienė | vnt. | 2 |
| 2. | Vienkartinių slaptažodžių raktų programinė įranga | vnt. | 1 |
| 3. | Žurnalinių įvykių valdymo platforma | vnt.. | 1 |
| 4. | Diegimo darbai | vnt. | 1 |

**TECHNINIAI REIKALAVIMAI**

1. **Kompiuterinio tinklo perimetro ugniasienė (2vnt.)**

Lentelė Nr. 1

| Eil. Nr. | Reikalaujama charakteristika | Siūloma charakteristika |
|---|---|---|
| 1.1. | Sprendimo architektūra ir sudedamosios dalys<br>Perimetro ugniasienių sprendimas turi būti sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t. y. kiekviena ugniasienė turi dirbti kaip nepriklausomas narys ir turi būti galima narius sujungti į aukšto patikimumo telkinį. Turi būti pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip ausšto patikimumo telkinio narius.<br>Žemiau pateikiami reikalavimai taikomi kiekvienam nariui atskirai, t. y. reikalavimus turi tenkinti kiekvienas iš telkinio narių. | Perimetro ugniasienių sprendimas yra sudarytas iš dviejų vienodų narių, skirtų užtikrinti perimetro kontrolę, įsibrovimų aptikimą ir prevenciją, URL filtravimą, srautų turinio kontrolę. Kiekvienas narys, t. y. kiekviena ugniasienė dirba kaip nepriklausomas narys ir galima narius sujungti į aukšto patikimumo telkinį. Yra pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip ausšto patikimumo telkinio narius.<br>Žemiau pateikiami reikalavimai taikomi kiekvienam nariui atskirai, t. y. reikalavimus tenkina kiekvienas iš telkinio narių. |
| 1.2. | Sprendimo narių įrangos gamintojas, modelis, modifikacija (jei yra).<br>Būtina išvardinti siūlomos įrangos komponentus, jų kiekius, modelius, gamintoją ir produktų kodus. Jeigu siūloma įranga licencijuojama, būtina pateikti licencijų kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia. | 2vnt. Fortinet FG-1101EBDL-950-60, kuriuos sudaro:<br>• 2vnt. FG-1101E<br>• 2vnt. 5 metų 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) licencija<br>• 2vnt. Rack mount sliding rails for FG-1100/1101E<br>• 12vnt. 10GE SFP+ transceiver module, short range<br>• 12vnt 3m (10ft) LC UPC to LC UPC Duplex OM4 Multimode PVC (OFNR) 2.0mm Fiber Optic Patch Cable |
| 1.3. | Surinkimo reikalavimai<br>Perimetro ugniasienių sprendimo nario įranga turi būti specializuotas aparatinis-programinis įrenginys arba modulinis įrenginys su vidiniais arba išoriniais moduliais komplektuojamas paties gamintojo. Ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) turi būti suderinti tarpusavyje, pagaminti vieno gamintojo arba kelių gamintojų, tačiau turi būti pateiktas ugniasienės gamintojo patvirtinimas dėl komponentų tarpusavio suderinamumo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais. | Perimetro ugniasienių sprendimo nario įranga yra specializuotas aparatinis-programinis įrenginys su vidiniais moduliais komplektuojamas paties gamintojo. Ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) yra suderinti tarpusavyje, pagaminti vieno gamintojo. Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtais sprendimais. |

| | | |
|---|---|---|
| 1.4. | Įrangos suderinamumas.<br>Siūloma perimetro ugniasienių sprendimo įranga turi būti pilnai suderinama su įsigyjama žurnalinių įvykių valdymo platforma. | Siūloma perimetro ugniasienių sprendimo įranga yra pilnai suderinama su įsigyjama žurnalinių įvykių valdymo platforma. |
| 1.5. | Siūloma perimetro ugniasienių sprendimo nario įranga turi būti pritaikyta montavimui į standartinę 19 colių įrangos montavimui skirtą spintą ir pateikiama su visais montavimui reikalingais priedais leidžiančiais ugniasienes montuoti ant ištraukiamų bėgių (įskaitant bet neapsiribojant tvirtinimo elementais). | Siūloma perimetro ugniasienių sprendimo nario įranga yra pritaikyta montavimui į standartinę 19 colių įrangos montavimui skirtą spintą ir pateikiama su visais montavimui reikalingais priedais leidžiančiais ugniasienes montuoti ant ištraukiamų bėgių (įskaitant bet neapsiribojant tvirtinimo elementais). |
| 1.6. | Maitinimo šaltiniai<br>Dubliuoti (du ar daugiau), karšto keitimo tipo, pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Ugniasienių sprendimo narys turi veikti sugedus vienam maitinimo šaltiniui. Pritaikyti 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklui. | Dubliuoti (du), karšto keitimo tipo, pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Ugniasienių sprendimo narys veikia sugedus vienam maitinimo šaltiniui. Pritaikyti 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklui. |
| 1.7. | Tinklo prievadų kiekis (ne mažiau kaip) ir tipas:<br>o 8 vnt. GE RJ45 prievadų;<br>o 4 vnt. GE SFP prievadų;<br>o 6 vnt. 10 GE SFP+ prievadų;<br>o 2 vnt. 25 GE SFP28 prievadų;<br>o 2 vnt. 40 GE QSFP+ prievadų. | Tinklo prievadų kiekis ir tipas:<br>o 16 vnt. GE RJ45 prievadų;<br>o 8 vnt. GE SFP prievadų;<br>o 4 vnt. 10 GE SFP+ prievadų;<br>o 4 vnt. 25 GE SFP28/ 10 GE SFP+ prievadų;<br>o 2 vnt. 40 GE QSFP+ prievadų. |
| 1.8. | Optiniai moduliai/kabeliai. Perimetro ugniasienių sprendimo nario įranga turi būti sukomplektuota su ne mažiau kaip:<br>o 8 vnt. 10G BASE-SR SFP+ 850 nm iki 300 m optiniais moduliais;<br>o 2 vnt. 1000 BASE-T SFP RJ-45 iki 100 m;<br>o 8 vnt. 3 m LC UPC į LC UPC Duplex OM4 multimodiniais PVC (OFNR) 2.0 mm optiniais kabeliais;<br>Optiniai moduliai privalo būti to paties gamintojo kaip ir perimetro ugniasienių sprendimo įrangos gamintojas. | Perimetro ugniasienių sprendimo nario įranga yra sukomplektuota su:<br>o 8 vnt. 10G BASE-SR SFP+ 850 nm iki 300 m optiniais moduliais;<br>o 2 vnt. 1000 BASE-T SFP RJ-45 iki 100 m;<br>o 8 vnt. 3 m LC UPC į LC UPC Duplex OM4 multimodiniais PVC (OFNR) 2.0 mm optiniais kabeliais;<br>Optiniai moduliai yra to paties gamintojo kaip ir perimetro ugniasienių sprendimo įrangos gamintojas. |
| 1.9. | Valdymo prievadai. Prievadų kiekis ir tipas:<br>o ne mažiau kaip vienas konsolės prievadas;<br>o ne mažiau kaip vienas valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę.<br>Šių prievadų skaičius turi būti papildomas, neturi būti įtrauktas į 1.7. punkte numatytą tinklo prievadų skaičių. | Prievadų kiekis ir tipas:<br>o 1vnt. konsolės prievadas;<br>o 1vnt. valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę.<br>Šių prievadų skaičius yra papildomas, nėra įtrauktas į 1.7. punkte numatytą tinklo prievadų skaičių. |
| 1.10 | Pajungimo į aukšto patikimumo telkinį prievadai.<br>Ne mažiau kaip 1 vnt.<br>Šių prievadų skaičius turi būti papildomas, neturi būti įtraukti į 1.7. punkte numatytą tinklo prievadų skaičių. | 1 vnt. pajungimo į aukšto patikimumo telkinį prievadas.<br>Šis skaičius yra papildomas, nėra įtrauktas į 1.7. punkte numatytą tinklo prievadų skaičių. |

| | | |
|---|---|---|
| 1.11 | Palaikomi standartai / protokolai. Perimetro ugniasienių sprendimo narys privalo palaikyti:<br>o kiekvienas tinklo duomenų srauto fizinis prievadas privalo palaikyti VLAN pagal 802.1Q arba lygiavertį standartą;<br>o LACP arba lygiavertį protokolą;<br>o bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą;<br>o 802.3ad arba lygiavertį standartą. Turi būti galima apjungti į vieną loginę tinklo sąsają ne mažiau kaip 4 fizines sąsajas. | Perimetro ugniasienių sprendimo narys palaiko:<br>o kiekvienas tinklo duomenų srauto fizinis prievadas palaiko VLAN pagal 802.1Q standartą;<br>o LACP protokolą;<br>o protokolus: Netflow, sFlow, IPFIX;<br>o 802.3ad. Galima apjungti į vieną loginę tinklo sąsają 4 fizines sąsajas. |
| 1.12 | VLAN palaikymas. Ne mažiau kaip 4000 VLAN žymių (angl. Vlan TAG) per įrenginį ir arba prievadą. | 4094 VLAN žymių (angl. Vlan TAG) per įrenginį/prievadą |
| 1.13 | Perimetro ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS), kenkėjiškų kodų, antivirusine patikra realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą. Ne mažiau kaip 7 Gbps. | Perimetro ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole, įsilaužimų prevencija (IPS), kenkėjiškų kodų, antivirusine patikra realiame duomenų sraute, bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą 7,1 Gbps. |
| 1.14 | IPsec VPN greitaveika Ne mažiau kaip 30 Gbps. | IPsec VPN greitaveika 48 Gbps. |
| 1.15 | IPsec tunelių skaičius naudojant vartotojų / klientų prisijungimą prie ugniasienės. Ne mažiau kaip 3000. | IPsec tunelių skaičius naudojant vartotojų / klientų prisijungimą prie ugniasienės 100000 |
| 1.16 | Maksimalus sesijų skaičius vienu metu: ne mažiau kaip 6,5 milijonų. | Maksimalus sesijų skaičius vienu metu 8 milijonai. |
| 1.17 | Maksimalus naujų sesijų skaičius per sekundę: ne mažiau kaip 350000. | Maksimalus naujų sesijų skaičius per sekundę 500000 |
| 1.18 | Suminis saugumo taisyklių skaičius per perimetro ugniasienių sprendimo narį: ne mažiau kaip 9000. | Suminis saugumo taisyklių skaičius per perimetro ugniasienių sprendimo narį 100000 |
| 1.19 | Aukšto patikimumo savybės. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą:<br>o nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais;<br>o turi būti galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys;<br>o automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių;<br>o automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių;<br>o turi būti galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą:<br>o nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais;<br>o galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys;<br>o automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių;<br>o automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių;<br>o galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema automatiškai persijungia jei nurodyti IP adresai tampa neaktyviais. |

| | | |
|---|---|---|
| 1.20 | Įrangos virtualizavimas. Turi būti funkcionalumas, leidžiantis perimetro ugniasienių sprendimo narį sudalinti į ne mažiau kaip 10 virtualų įrenginių. | Yra funkcionalumas, leidžiantis perimetro ugniasienių sprendimo narį sudalinti 10 virtualų įrenginių. |
| 1.21 | Perimetro ugniasienių sprendimo nario darbo režimai. Ne mažiau kaip :<br>o maršrutizavimo tarp skirtingų tinklų (OSI L3);<br>o skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);<br>o stebėjimo – pasyviai surenkant informaciją nuo tinklo įrangos, kuri sugeba atiduoti duomenų srauto kopiją. | Perimetro ugniasienių sprendimo nario darbo režimai:<br>o maršrutizavimo tarp skirtingų tinklų (OSI L3);<br>o skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);<br>o stebėjimo – pasyviai surenkant informaciją nuo tinklo įrangos, kuri sugeba atiduoti duomenų srauto kopiją. |
| 1.22 | Darbo režimai ir virtualizavimo funkcionalumas. Perimetro ugniasienių sprendimo narį dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema privalo veikti kiekvienu iš darbo režimų (maršrutizavimo, skaidrus, stebėjimo), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai turi būti galima nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos. | Perimetro ugniasienių sprendimo narį dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema veikia kiekvienu iš darbo režimų (maršrutizavimo, skaidrus, stebėjimo), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai galima nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos. |
| 1.23 | Maršrutizavimas. Perimetro ugniasienių sprendimo narys privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). | Perimetro ugniasienių sprendimo narys palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). |
| 1.24 | Maršrutizavimas. Perimetro ugniasienių sprendimo narys privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai. | Perimetro ugniasienių sprendimo narys palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai. |
| 1.25 | Perimetro ugniasienių sprendimo narys privalo palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą. | Perimetro ugniasienių sprendimo narys palaiko politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną sąsają, siuntėjo, gavėjo IP adresą. |
| 1.26 | Dinaminio maršrutizavimo protokolai. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus:<br>o BGP;<br>o OSFP v2 ir v3;<br>o RIP v2. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintus protokolus:<br>o BGP;<br>o OSFP v2 ir v3;<br>o RIP v2. |
| 1.27 | Perimetro ugniasienių sprendimo narys privalo turėti BGP perkrovimo (graceful restart) funkcionalumą. | Perimetro ugniasienių sprendimo narys turi BGP perkrovimo (graceful restart) funkcionalumą. |
| 1.28 | Perimetro ugniasienių sprendimo narys privalo palaikyti šiuos BGP protokolo gebėjimus:<br>o maksimalų išmokstamų maršrutų skaičiaus ribojimą per kaimyną;<br>o BGP kaimynų grupavimą; | Perimetro ugniasienių sprendimo narys palaiko šiuos BGP protokolo gebėjimus:<br>o maksimalų išmokstamų maršrutų skaičiaus ribojimą per kaimyną;<br>o BGP kaimynų grupavimą;<br>o filtravimą gaunamiems ir išsiunčiamiems maršrutams; |

| | | |
|---|---|---|
| | ○ filtravimą gaunamiems ir išsiunčiamiems maršrutams;<br>○ Local Preference;<br>○ MED;<br>○ AS prepend;<br>○ Route-reflector funkcionalumą<br>○ maršrutų stabilumo vertinimą (prefix dampening);<br>○ BGP BFD;<br>○ BGP community;<br>○ Next hop vertės keitimą;<br>○ Soft session reset. | ○ Local Preference;<br>○ MED;<br>○ AS prepend;<br>○ Route-reflector funkcionalumą<br>○ maršrutų stabilumo vertinimą (prefix dampening);<br>○ BGP BFD;<br>○ BGP community;<br>○ Next hop vertės keitimą;<br>○ Soft session reset. |
| 1.29 | Perimetro ugniasienių sprendimo narys privalo turėti grakštaus OSPF perkrovimo (graceful restart) funkcionalumą. | Perimetro ugniasienių sprendimo narys turi grakštaus OSPF perkrovimo (graceful restart) funkcionalumą. |
| 1.30 | Srauto balansavimas. Perimetro ugniasienių sprendimo narys privalo gebėti balansuoti serveriams skirtą srautą.<br>Turi būti palaikomi ne mažiau kaip Round robin ir Least session srauto balansavimo metodai. | Perimetro ugniasienių sprendimo narys geba balansuoti serveriams skirtą srautą.<br>Yra palaikomi Round robin ir Least session srauto balansavimo metodai. |
| 1.31 | Perimetro ugniasienių sprendimo narys privalo palaikyti BFD (bidirectional forwarding detection) protokolą. | Perimetro ugniasienių sprendimo narys palaiko BFD (bidirectional forwarding detection) protokolą. |
| 1.32 | Perimetro ugniasienių sprendimo narys privalo palaikyti IPv6 protokolą. | Perimetro ugniasienių sprendimo narys palaiko IPv6 protokolą. |
| 1.33 | Perimetro ugniasienių sprendimo narys turi palaikyti Jumbo paketus. | Perimetro ugniasienių sprendimo narys palaiko Jumbo paketus. |
| 1.34 | Adresų transliavimo funkcionalumas. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą:<br>○ NAT64;<br>○ Statinis adresų transliavimas;<br>○ Dinaminis adresų transliavimas keičiant prievadus (PAT). | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą:<br>○ NAT64;<br>○ Statinis adresų transliavimas;<br>○ Dinaminis adresų transliavimas keičiant prievadus (PAT). |
| 1.35 | Integracija su SNMP (Simple Network Management Protocol) įrenginio būsenos stebėjimui.<br>Privalo palaikyti SNMP protokolo 2 ir 3 versijas. | Integracija su SNMP (Simple Network Management Protocol) įrenginio būsenos stebėjimui.<br>Palaiko SNMP protokolo 2 ir 3 versijas. |
| 1.36 | Suderinamumas su Syslog. Perimetro ugniasienių sprendimo narys turi būti suderinamas su Syslog standartu. | Perimetro ugniasienių sprendimo narys yra suderinamas su Syslog standartu. |
| 1.37 | Žurnalinių įvykių (event log) palaikymas. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus žurnalinius įvykius:<br>○ sisteminiai;<br>○ administravimo;<br>○ VPN;<br>○ naudotojų autentifikavimo;<br>○ maršrutizavimo;<br>○ saugos incidentų įvykiai. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintus žurnalinius įvykius:<br>○ sisteminiai;<br>○ administravimo;<br>○ VPN;<br>○ naudotojų autentifikavimo;<br>○ maršrutizavimo;<br>○ saugos incidentų įvykiai. |
| 1.38 | Žurnalinių įvykių kaupimas. Perimetro ugniasienių sprendimo narys privalo leisti kaupti įvykių žurnalus įrenginio talpykloje ir | Perimetro ugniasienių sprendimo narys leidžia kaupti įvykių žurnalus įrenginio |

| | | |
|---|---|---|
| | siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.<br>Turi būti pilnai suderinama su perkama žurnalinių įvykių valdymo platforma. | talpykloje ir siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.<br>Yra pilnai suderinama su perkama žurnalinių įvykių valdymo platforma. |
| 1.39 | Diagnostikos priemonės. Privalomas srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu. | Yra srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu. |
| 1.40 | Nutolusių naudotojų duomenų bazių palaikymas.<br>Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes:<br>o LDAP;<br>o RADIUS;<br>o TACACS+;<br>o dviejų lygių (two-factor) autentifikaciją. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintas duomenų bazes:<br>o LDAP;<br>o RADIUS;<br>o TACACS+;<br>o dviejų lygių (two-factor) autentifikaciją. |
| 1.41 | Prieigos teisių valdymas. Perimetro ugniasienių sprendimo narys privalo:<br>o leisti suteikti prieigos teises tik naudotojams, kurių tapatybė yra patvirtinta;<br>o leisti suteikti prieigos teises naudotojams ir/arba naudotojų grupėms;<br>o leisti nustatyti naudotojų tapatybę, neprašydamas suvesti naudotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba programinės įrangos (agento) pagalba;<br>o leisti sukurti naudotoją – administratorių, kuris turėtų tik read-only teises (galimybė matyti visą konfigūraciją, bet keisti nieko negalima);<br>o leisti detaliai/individualiai apibrėžti kiekvieno fizinio ir/ar virtualaus naudotojo/administratoriaus teises:<br>• teisė keisti sisteminius įrenginio nustatymus;<br>• teisė kurti, keisti saugumo taisykles;<br>• teisė kurti, keisti taisyklių objektus;<br>• teisė konfigūruoti saugumo patikrų nustatymus;<br>• teisė peržiūrėti įvykių žurnalus;<br>• teisė peržiūrėti ataskaitas;<br>• teisė generuoti ataskaitas. | Perimetro ugniasienių sprendimo narys gali:<br>o leidžia suteikti prieigos teises tik naudotojams, kurių tapatybė yra patvirtinta;<br>o leidžia suteikti prieigos teises naudotojams ir/arba naudotojų grupėms;<br>o leidžia nustatyti naudotojų tapatybę, neprašydamas suvesti naudotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba programinės įrangos (agento) pagalba;<br>o leidžia sukurti naudotoją – administratorių, kuris turėtų tik read-only teises (galimybė matyti visą konfigūraciją, bet keisti nieko negalima);<br>o leidžia detaliai/individualiai apibrėžti kiekvieno fizinio ir/ar virtualaus naudotojo/administratoriaus teises:<br>• teisė keisti sisteminius įrenginio nustatymus;<br>• teisė kurti, keisti saugumo taisykles;<br>• teisė kurti, keisti taisyklių objektus;<br>• teisė konfigūruoti saugumo patikrų nustatymus;<br>• teisė peržiūrėti įvykių žurnalus;<br>• teisė peržiūrėti ataskaitas;<br>• teisė generuoti ataskaitas. |
| 1.42 | Autorizacijos integracija (single sign on)<br>Perimetro ugniasienių sprendimo narys privalo turėti integracijas su žemiau įvardintomis arba lygiavertėmis sistemomis:<br>o Windows AD;<br>o Microsoft Exchange server;<br>o Citrix Terminal Server Agent; | Perimetro ugniasienių sprendimo narys turi integracijas su žemiau įvardintomis sistemomis:<br>o Windows AD;<br>o Microsoft Exchange server;<br>o Citrix Terminal Server Agent;<br>o RADIUS; |

| | | |
|---|---|---|
| | ○ RADIUS;<br>○ 802.1x. | ○ 802.1x. |
| 1.43 | SSL šifruotas srautas. Perimetro ugniasienių sprendimo narys turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą.<br>Perimetro ugniasienių sprendimo narys privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus.<br>Privalo būti galima nurodyti kuris duomenų srautas turi būti dešifruojamas. | Perimetro ugniasienių sprendimo narys gali dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą.<br>Perimetro ugniasienių sprendimo narys palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus.<br>Galima nurodyti kuris duomenų srautas turi būti dešifruojamas. |
| 1.44 | DoS apsauga. Perimetro ugniasienių sprendimo narys privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui. | Perimetro ugniasienių sprendimo narys leidžia riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui. |
| 1.45 | Apsauga nuo grėsmių. Perimetro ugniasienių sprendimo narys turi saugoti nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdyti konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrinti perduodamą srautą nuo virusų. Virusų, kenkėjiškų kodų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip perimetro ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui. Turi būti galima naudoti gamintojo pateikiamus dinamiškai atnaujinamus kenksmingų IP adresų sąrašus. | Perimetro ugniasienių sprendimo narys saugo nuo atakų, piktybinių kodų (pvz. virusai, šnipinėjimo programos), stabdo konfidencialios informacijos perdavimą (pvz.: pagal raktinius žodžius, pagal IT politiką), tikrina perduodamą srautą nuo virusų. Virusų, kenkėjiškų kodų aprašai pateikiami nemokamai perimetro ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui. Galima naudoti gamintojo pateikiamus dinamiškai atnaujinamus kenksmingų IP adresų sąrašus. |
| 1.46 | IPS funkcionalumas. Perimetro ugniasienių sprendimo narys privalo turėti žemiau įvardintą funkcionalumą:<br>○ įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. Funkcionalumas nemokamai (turi būti įtraukta į pasiūlymo kainą) turi veikti ne trumpesniu nei įrangos garantinis laikotarpiu.<br>○ turi būti galima užblokuoti atakuojantį IP adresą.<br>○ leisti nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme. | Perimetro ugniasienių sprendimo narys turi žemiau įvardintą funkcionalumą:<br>○ įsilaužimų / pažeidžiamumų (IPS) aprašų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. Funkcionalumas nemokamai veikia įrangos garantiniu laikotarpiu.<br>○ galima užblokuoti atakuojantį IP adresą.<br>○ Leidžia nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme. |
| 1.47 | Protokolų anomalijos. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą:<br>○ protokolų anomalijų aptikimas;<br>○ protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą:<br>○ protokolų anomalijų aptikimas;<br>○ protokolų anomalijų, nuosavo „parašo“ susikūrimas ir įkėlimas į sistemą. |
| 1.48 | Aplikacijų valdymas. Perimetro ugniasienių sprendimo narys privalo palaikyti:<br>○ aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 3000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip | Perimetro ugniasienių sprendimo narys palaiko:<br>○ aplikacijų identifikavimą ir kontrolę. Identifikuoja \|daugiau nei 4000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip |

| | | |
|---|---|---|
| | viena programa). Aplikacijų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui;<br>o aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą. | viena programa). Aplikacijų aprašai pateikiami nemokamai ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiui; https://www.fortiguard.com/appcontrol<br>o aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą. |
| 1.49 | URL filtravimas. Perimetro ugniasienių sprendimo narys privalo palaikyti:<br>o prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). URL duomenų bazė pateikiama nemokamai (arba įskaičiuota į pasiūlymo kainą) netrumpesniam kaip ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiu;<br>o nuosavų draudžiamų URL sąrašų kūrimas;<br>o URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo. | Perimetro ugniasienių sprendimo narys palaiko:<br>o prieigos prie žiniatinklio resursų kontrolę naudojant gamintojo pateikiamą URL duomenų bazę (URL filtravimas). URL duomenų bazė pateikiama nemokamai ugniasienių sprendimo nario įrangos garantinio aptarnavimo laikotarpiu;<br>o nuosavų draudžiamų URL sąrašų kūrimas;<br>o URL, IP adresų, domenų vardų, kurie bus naudojami saugumo politikose, importavimas iš išorinio failo. |
| 1.50 | Sesijų laiko kontrolė. Turi būti galima kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma. | Galima kiekvienai aplikacijai nustatyti individualų laiką, po kurio neaktyvi sesija yra uždaroma. |
| 1.51 | Duomenų srautų kontrolės taisyklės. Kuriant duomenų srautų kontrolės taisyklės privalo būti galima nurodyti siuntėjo IP adresą ar potinklį, gavėją IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę.<br>Privalo būti galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones. | Kuriant duomenų srautų kontrolės taisyklės galima nurodyti siuntėjo IP adresą ar potinklį, gavėją IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę.<br>Galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones. |
| 1.52 | Duomenų srautų kontrolės taisyklių naudojimo stebėjimas.<br>Perimetro ugniasienių sprendimo narys privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count) | Perimetro ugniasienių sprendimo narys rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count) |
| 1.53 | VPN funkcionalumas. Perimetro ugniasienių sprendimo narys privalo turėti žemiau įvardintą VPN funkcionalumą:<br>o leisti redaguoti SSL VPN portalą;<br>o leisti naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento);<br>o nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais;<br>o nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) privalo būti to paties gamintojo kaip ir siūlomų perimetro | Perimetro ugniasienių sprendimo narys turi žemiau įvardintą VPN funkcionalumą:<br>o leidžia redaguoti SSL VPN portalą;<br>o leidžia naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento);<br>o nuotolinio prisijungimo naudotojo VPN klientas moka dirbti IPSec ir SSL protokolais;<br>o nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) yra to paties gamintojo kaip ir |

| | | |
|---|---|---|
| | ugniasienių sprendimo įrenginių gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. Jei siūlomas skirtingo gamintojo VPN klientas (programinė įranga) nei perimetro ugniasienių sprendimo įrenginių gamintojas, turi būti pateikti skirtingų gamintojų raštiški patvirtinimai, kad siūlomas sprendimas yra visiškai suderinamas bendram darbui su ugniasienių sprendimu;<br>o nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui. | siūlomų perimetro ugniasienių sprendimo įrenginių gamintojas.<br>o nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui. |
| 1.54 | IPSec kriptografijos algoritmai. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptografijos algoritmus:<br>o AES128;<br>o AES256. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec kriptografijos algoritmus:<br>o AES128;<br>o AES256. |
| 1.55 | IPSec maišos algoritmai. Perimetro ugniasienių sprendimo narys privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus:<br>o SHA-256;<br>o SHA-512. | Perimetro ugniasienių sprendimo narys palaiko žemiau įvardintus IPSec maišos algoritmus:<br>o SHA-256;<br>o SHA-512. |
| 1.56 | Srauto ribojimas. Perimetro ugniasienių sprendimo narys privalo leisti riboti srautą ir taikyti QoS per taisyklę (policy). | Perimetro ugniasienių sprendimo narys leidžia riboti srautą ir taikyti QoS per taisyklę (policy). |
| 1.57 | Valdymas. Ne mažiau kaip: grafinė vartotojo sąsaja (GUI) per naršyklę HTTPS protokolu, komandinė eilutė SSH protokolu.<br>Valdymui per grafinę vartotoją sąsaja (GUI) per HTTPS neturi būti naudojama speciali gamintojo pateikiama programinė įranga arba papildomi naršyklės įskiepiai.<br>Per valdymui skirtą grafinę vartotojo sąsają (GUI) per HTTPS turi būti galima atlikti ne mažiau kaip šiuos konfigūravimo, problemų paieškos ir analizės veiksmus:<br>o aukšto patikimumo funkcionalumo konfigūravimas;<br>o PBR funkcionalumo konfigūravimas;<br>o srauto balansavimo funkcionalumo konfigūravimas;<br>o prieigos politikų konfigūravimas;<br>o apsaugos nuo grėsmių funkcionalumo konfigūravimas;<br>o IPS funkcionalumo konfigūravimas;<br>o aplikacijų valdymo funkcionalumo konfigūravimas;<br>o URL filtravimo funkcionalumo konfigūravimas;<br>o VPN funkcionalumo konfigūravimas; | Grafinė vartotojo sąsaja (GUI) per naršyklę HTTPS protokolu, komandinė eilutė SSH protokolu.<br>Valdymui per grafinę vartotoją sąsaja (GUI) per HTTPS nėra naudojama speciali gamintojo pateikiama programinė įranga arba papildomi naršyklės įskiepiai.<br>Per valdymui skirtą grafinę vartotojo sąsają (GUI) per HTTPS galima atlikti šiuos konfigūravimo, problemų paieškos ir analizės veiksmus:<br>o aukšto patikimumo funkcionalumo konfigūravimas;<br>o PBR funkcionalumo konfigūravimas;<br>o srauto balansavimo funkcionalumo konfigūravimas;<br>o prieigos politikų konfigūravimas;<br>o apsaugos nuo grėsmių funkcionalumo konfigūravimas;<br>o IPS funkcionalumo konfigūravimas;<br>o aplikacijų valdymo funkcionalumo konfigūravimas;<br>o URL filtravimo funkcionalumo konfigūravimas;<br>o VPN funkcionalumo konfigūravimas; |

| | | |
|---|---|---|
| | ○ srauto įrašų peržiūra ir paieška, filtravimas;<br>○ sisteminių įrašų peržiūra ir paieška, filtravimas;<br>○ administravimo įrašų peržiūra ir paieška, filtravimas;<br>○ VPN įrašų peržiūra ir paieška, filtravimas;<br>○ maršrutizavimo įrašų peržiūra ir paieška, filtravimas;<br>○ saugos incidentų įvykių peržiūra ir paieška, filtravimas. | ○ srauto įrašų peržiūra ir paieška, filtravimas;<br>○ sisteminių įrašų peržiūra ir paieška, filtravimas;<br>○ administravimo įrašų peržiūra ir paieška, filtravimas;<br>○ VPN įrašų peržiūra ir paieška, filtravimas;<br>○ maršrutizavimo įrašų peržiūra ir paieška, filtravimas;<br>○ saugos incidentų įvykių peržiūra ir paieška, filtravimas. |
| 1.58 | Centralizuoto valdymo palaikymas. Privalo būti galimybė Ugniasienių sprendimo narį valdyti iš centrinio, valdymui dedikuoto, sprendimo. | Yra galimybė ugniasienių sprendimo narį valdyti iš centrinio, valdymui dedikuoto, sprendimo. |
| 1.59 | Aprašų, programinės įrangos atnaujinimas. Perimetro ugniasienių sprendimo narys privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų, pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL filtravimo duomenų bazę arba gauti informaciją realiu laiku iš gamintojo serverių / puslapio. | Perimetro ugniasienių sprendimo narys gali automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų, pažeidžiamumų, virusų, kenkėjiškų kodų aprašus, URL filtravimo duomenų bazę. |
| 1.60 | Garantiniai įsipareigojimai, techninis aptarnavimas.<br>Visiems techninės ir programinės įrangos komponentams, turi būti suteikta ne trumpesnė nei 60 mėn. gamintojo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos.<br>Gamintojo garantuojamas nemokamas garantinis aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės, virusų, piktybinių programų, pažeidžiamumų, įsilaužimo aprašų, URL filtravimo duomenų bazių ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus).<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis).<br>Gedimo atveju gamintojas turi užtikrinti išankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD)).<br>Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis. | Visiems techninės ir programinės įrangos komponentams, suteikta 60 mėn. gamintojo garantija, skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos.<br>Gamintojo garantuojamas nemokamas garantinis aptarnavimas bei visų atnaujinimų tiekimas garantiniu laikotarpiu (aplikacijų kontrolės, virusų, piktybinių programų, pažeidžiamumų, įsilaužimo aprašų, URL filtravimo duomenų bazių ir kt. pagal aukščiau techninėje specifikacijoje aprašytus reikalavimus).<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis).<br>Gedimo atveju gamintojas užtikrina išankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD)).<br>Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos anglų kalba. |

**2. Vienkartinių slaptažodžių raktų programinė įranga (1 vnt.)**

Lentelė Nr. 2

| Eil. Nr. | Reikalaujama charakteristika | Siūloma charakteristika |
|---|---|---|
| 2.1. | Įrangos gamintojas, modelis, modifikacija | Fortinet FTM-ELIC-2000 FortiToken One-Time Password Token for IOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users, Electronic license certificate. |
| 2.2. | Perkama licencija turi palaikyti ne mažiau 2000 vartotojų vienkartinių slaptažodžių raktų. | Perkama licencija palaiko 2000 vartotojų vienkartinių slaptažodžių raktų. |
| 2.3. | Sprendimo architektūra. Įsigyjami programiniai vienkartinių kodų generatoriai skirti antro faktoriaus naudotojų tapatybės nustatymui atlikti prisijungiant prie Perkančiosios organizacijos tinklo. | Įsigyjami programiniai vienkartinių kodų generatoriai skirti antro faktoriaus naudotojų tapatybės nustatymui atlikti prisijungiant prie Perkančiosios organizacijos tinklo. |
| 2.4. | Suderinamumas. Turi palaikyti integraciją su Perkančiosios organizacijos šiuo pirkimu įsigyjamomis kompiuterinio tinklo perimetro ugniasienėmis neribotą laiką ateityje. | Palaiko integraciją su Perkančiosios organizacijos šiuo pirkimu įsigyjamomis kompiuterinio tinklo perimetro ugniasienėmis neribotą laiką ateityje. |
| 2.5. | Saugumo algoritmas OATH-TOTP ar lygiavertis | Saugumo algoritmas OATH-TOTP |
| 2.6. | Saugumo funkcijos. Savaiminio ištrynimo apsauga nuo brutalios jėgos. | Savaiminio ištrynimo apsauga nuo brutalios jėgos. |
| 2.7. | Vieno palietimo patvirtinimo funkcija. Turi būti galima prisijungimą patvirtinti vienu prisilietimu. Naudotojui turi būti pateikiama prisijungimo informacija. | Galima prisijungimą patvirtinti vienu prisilietimu. Naudotojui yra pateikiama prisijungimo informacija. |
| 2.8. | Palaikoma programinė įranga. Turi būti galima įdiegti į ne mažiau kaip šių operacinių sistemų įrenginius:<br>o iOS;<br>o Android;<br>o Windows;<br>o Universal Windows Platform (UWP). | Galima įdiegti į šių operacinių sistemų įrenginius:<br>o iOS;<br>o Android;<br>o Windows;<br>o Universal Windows Platform (UWP). |
| 2.9. | Programinio vienkartinių kodų generatoriaus apsauga. Turi būti galima apsaugoti PIN kodu ir pirštų antspaudu. | Galima apsaugoti PIN kodu ir pirštų antspaudu. |
| 2.10. | Programinių vienkartinių kodų generatoriaus veikimo trukmė ne trumpesnė nei 60 mėn., skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos.<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas) ne trumpesnė nei 60 mėn.<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). | Programinių vienkartinių kodų generatoriaus veikimo trukmė 60 mėn., skaičiuojant nuo įrangos priėmimo-perdavimo akto pasirašymo dienos.<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas) 60 mėn.<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis). |

**3. Žurnalinių įvykių valdymo platforma (1 vnt.)**

Lentelė Nr. 3

| Eil. Nr. | Reikalaujama charakteristika | Siūloma charakteristika |
|---|---|---|
| 3.1. | Įrangos gamintojas, modelis, modifikacija (jei yra)<br>Būtina išvardinti siūlomos įrangos komponentus, jų kiekius, modelius, gamintoją ir produktų kodus. Jeigu siūloma įranga licencijuojama, būtina pateikti licencijų kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia. | 1vnt Fortinet FAZ-800G Centralized log&analysis appliance<br>• 1vnt. FC-10-L01KF-247-02-60 5 Yrs 24x7 FortiCare Contract<br>• 1vnt. SP-FAZ800G-PS AC power supply for FAZ-800G |
| 3.2. | Įrangos paskirtis. Įranga privalo centralizuotai, kaupti žurnalinę informaciją iš tinklo saugos įrenginių ir teikti ataskaitas apie esamą saugumo būseną ir tinklo naudojimo profilį. | Įranga centralizuotai kaupia žurnalinę informaciją iš tinklo saugos įrenginių ir teikia ataskaitas apie esamą saugumo būseną ir tinklo naudojimo profilį. |
| 3.3. | Suderinamumas. Siūlomas įrenginys turi būti pilnai suderinamas su siūlomomis perimetro ugniasienėmis. Turi būti galima perduodamų įrašų srautą šifruoti tarp įrašus saugančio ir įrašus siunčiančio įrenginio.<br>Įrenginys turi būti suderinamas su visais įrenginiais, galinčiais siųsti žurnalinius įvykius SYSLOG, CEF protokolais | Siūlomas įrenginys yra pilnai suderinamas su siūlomomis perimetro ugniasienėmis. Galima perduodamų įrašų srautą šifruoti tarp įrašus saugančio ir įrašus siunčiančio įrenginio.<br>Įrenginys yra suderinamas su visais įrenginiais, galinčiais siųsti žurnalinius įvykius SYSLOG, CEF protokolais |
| 3.4. | Aukštis ne daugiau nei 1U. Montuojamas į 19“ komutacinę spintą, turi būti pateikiamas su montavimui reikalingomis dalimis. | Aukštis 1U. Montuojamas į 19“ komutacinę spintą, pateikiamas su montavimui reikalingomis dalimis. |
| 3.5. | Maitinimo šaltiniai. Dubliuoti (du ar daugiau), pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Žurnalinių įvykių valdymo platformos įrenginys turi veikti sugedus vienam maitinimo šaltiniui. Pritaikyti prijungti prie 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklo. | Dubliuoti (du), pakankamos galios vidiniai maitinimo šaltiniai, kurie užtikrina aukštą patikimumą. Žurnalinių įvykių valdymo platformos įrenginys veikia sugedus vienam maitinimo šaltiniui. Pritaikyti prijungti prie 220 – 240 V, 50 – 60 Hz kintamos srovės elektros tinklo. |
| 3.6. | Įrangos tipas. Specializuota įranga, susidedanti iš techninės bei programinės įrangos.<br>Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais. | Specializuota įranga, susidedanti iš techninės bei programinės įrangos.<br>Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtais sprendimais. |
| 3.7. | Prievadų konfigūracija<br>Integruotų prievadų kiekis ir tipas:<br>o 1 GE RJ45 – ne mažiau 2 vnt.;<br>o 1 GE SFP – ne mažiau 2 vnt.;<br>o RJ45 konsolės prievadų – ne mažiau 1 vnt. | Integruotų prievadų kiekis ir tipas:<br>o 1 GE RJ45 – 4 vnt.;<br>o 1 GE SFP – 2 vnt.;<br>o RJ45 konsolės prievadų – 1 vnt. |
| 3.8. | Vidinė talpa: Ne mažiau nei 10 TB. | Vidinė talpa 16 TB |
| 3.9. | Turi palaikyti ne prasčiau nei šį įrenginio našumą:<br>o įranga turi gebėti per parą surinkti ne mažiau kaip 180 GB žurnalinių įvykių; | Palaiko šį įrenginio našumą:<br>o įranga geba per parą surinkti 200 GB žurnalinių įvykių;<br>o veikdama nepertraukiamu režimu, įranga geba analizuoti 4000 įrašų per sekundę; |

| | | |
|---|---|---|
| | ○ veikdama nepertraukiamu režimu, įranga turi gebėti analizuoti ne mažiau 3000 įrašų per sekundę;<br>○ piko metu įranga turi gebėti surinkti ne mažiau 5000 įrašų per sekundę;<br>○ įranga turi gebėti rinkti įrašus iš ne mažiau kaip 20 įrenginių. | ○ piko metu įranga geba surinkti 6000 įrašų per sekundę;<br>○ įranga geba rinkti įrašus iš 800 įrenginių. |
| 3.10. | Informacijos analizė. Turi palaikyti šias funkcijas:<br>○ įranga turi leisti peržiūrėti ir tvarkyti žurnalinę informaciją, bei suteikti paieškos priemones;<br>○ turi būti galima sukauptų įvykių istorijos peržiūra;<br>○ turi būti galima įvykių peržiūra realiame laike;<br>○ turi būti galima įvykių paieška, filtravimas pagal parametrus;<br>○ turi būti istorinis ir realaus laiko tinklo srauto stebėjimas;<br>○ turi būti galima stebėti vartotojų veiksmus remiantis vartotojo vardu, elektroninio pašto adresu, IP adresu;<br>○ įranga turi pateikti informaciją apie vartotojo naršytus tinklapius. | Palaiko šias funkcijas:<br>○ įranga leidžia peržiūrėti ir tvarkyti žurnalinę informaciją, bei suteikia paieškos priemones;<br>○ yra galima sukauptų įvykių istorijos peržiūra;<br>○ galima įvykių peržiūra realiame laike;<br>○ galima įvykių paieška, filtravimas pagal parametrus;<br>○ istorinis ir realaus laiko tinklo srauto stebėjimas;<br>○ galima stebėti vartotojų veiksmus remiantis vartotojo vardu, elektroninio pašto adresu, IP adresu;<br>○ įranga pateikia informaciją apie vartotojo naršytus tinklapius. |
| 3.11. | Ataskaitų formavimas. Įranga turi automatizuotai teikti šias ataskaitas (neapsiribojant pateiktu sąrašu):<br>○ kibernetinių atakų (pagal saugos įrenginį, per nustatytą laikotarpį, pagal atakos kategoriją, pagal atakos šaltinį);<br>○ kompiuteriniai virusai (dažniausiai pasitaikantys, virusai pagal perdavimo protokolą);<br>○ sistemos įvykiai (pagal saugos įrenginį, visi įvykiai, saugumo įvykiai, per nustatytą laikotarpį);<br>○ interneto naudojimas (didžiausi vartotojai, dažniausiai blokuojami tinklapiai);<br>○ srauto naudojimas (daugiausiai srauto naudojantys vartotojai, srauto naudojimas per nustatytą laikotarpį, srauto naudojimas pagal protokolą);<br>○ aplikacijų naudojimas (daugiausiai srauto sunaudojančios aplikacijos per nustatytą laikotarpį);<br>○ srauto naudojimas pagal šalis. | Įranga automatizuotai teikia šias ataskaitas (neapsiribojant pateiktu sąrašu):<br>○ kibernetinių atakų (pagal saugos įrenginį, per nustatytą laikotarpį, pagal atakos kategoriją, pagal atakos šaltinį);<br>○ kompiuteriniai virusai (dažniausiai pasitaikantys, virusai pagal perdavimo protokolą);<br>○ sistemos įvykiai (pagal saugos įrenginį, visi įvykiai, saugumo įvykiai, per nustatytą laikotarpį);<br>○ interneto naudojimas (didžiausi vartotojai, dažniausiai blokuojami tinklapiai);<br>○ srauto naudojimas (daugiausiai srauto naudojantys vartotojai, srauto naudojimas per nustatytą laikotarpį, srauto naudojimas pagal protokolą);<br>○ aplikacijų naudojimas (daugiausiai srauto sunaudojančios aplikacijos per nustatytą laikotarpį);<br>○ srauto naudojimas pagal šalis. |
| 3.12. | Valdymo galimybės. Turi būti šie įrangos valdymo būdai:<br>○ valdymas grafinėje aplinkoje iš standartinės interneto naršyklės;<br>○ ryšys tarp įrangos ir valdančiojo kompiuterio turi būti šifruojamas;<br>○ turi būti palaikomas SSH; | Yra šie įrangos valdymo būdai:<br>○ valdymas grafinėje aplinkoje iš standartinės interneto naršyklės;<br>○ ryšys tarp įrangos ir valdančiojo kompiuterio turi būti šifruojamas;<br>○ palaikomas SSH;<br>○ galima sukurti kelis sistemos administratorius; |

| | | |
|---|---|---|
| | ○ turi būti galima sukurti kelis sistemos administratorius;<br>○ turi būti galima sukurti kelis sistemos vartotojus turinčius ribotas prieigos teises. | ○ galima sukurti kelis sistemos vartotojus turinčius ribotas prieigos teises. |
| 3.13. | Saugumo pranešimai. Turi palaikyti šias funkcijas:<br>○ įranga privalo siųsti pranešimus, susijusius su saugumu, administratoriams el. paštu, SNMP arba Syslog protokolu.<br>○ turi būti galima saugumo pranešimams nustatyti skirtingus grėsmių lygius.<br>○ turi būti galima nurodyti, kada siųsti saugumo pranešimus: įvykus tam tikriems įvykiams, įvykus tam tikram skaičiui specifinių įvykių, atlikus tam tikrus veiksmus. | Palaiko šias funkcijas:<br>○ įranga siunčia pranešimus, susijusius su saugumu, administratoriams el. paštu, SNMP arba Syslog protokolu.<br>○ galima saugumo pranešimams nustatyti skirtingus grėsmių lygius.<br>○ galima nurodyti, kada siųsti saugumo pranešimus: įvykus tam tikriems įvykiams, įvykus tam tikram skaičiui specifinių įvykių, atlikus tam tikrus veiksmus. |
| 3.14. | Garantija. Gamintojo garantuojamas 60 mėn. nemokamas garantinis aptarnavimas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis).<br>Gedimo atveju gamintojas turi užtikrinti išankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD)).<br>Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. | Gamintojo garantuojamas 60 mėn. nemokamas garantinis aptarnavimas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Programinės įrangos palaikymas (teisė gauti klaidų pataisymus, taip pat naujesnes programinės įrangos versijas).<br>Teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) savaitės dienomis visą parą (paslaugos tipas 24x7) (telefonu ar kitomis elektroninėmis priemonėmis).<br>Gedimo atveju gamintojas užtikrina išankstinį įrangos pristatymą (angl. advanced hardware replacement (NBD)).<br>Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. |

**4. Diegimo darbai (1vnt.)**

Lentelė Nr. 4

| Eil. Nr. | Reikalaujama charakteristika | Siūloma charakteristika |
|---|---|---|
| 4.1. | Diegimo valdymas.<br>Tiekėjas yra atsakingas už Diegimo projekto valdymą ir būtinų kompetencijų pritraukimą sėkmingam įgyvendinimui.<br>Perkančioji organizacija pateiks turimą dokumentaciją ir prisijungimus. | Tiekėjas yra atsakingas už Diegimo projekto valdymą ir būtinų kompetencijų pritraukimą sėkmingam įgyvendinimui.<br>Perkančioji organizacija pateiks turimą dokumentaciją ir prisijungimus. |
| 4.2. | Projektavimas<br>• Turi būti parengta perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūra pateikiant fizines ir logines schemas. Vidinio tinklo segmentavimas turi būti įgyvendintas Perkančiosios | • Bus parengta perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūra pateikiant fizines ir logines schemas. Vidinio tinklo segmentavimas bus įgyvendintas Perkančiosios |

| | | |
|---|---|---|
| | organizacijos turimomis ugniasienėmis FortiGate 501E.<br>• Turi būti parengta Žurnalinių įvykių valdymo platformos prijungimo architektūra pateikiant fizines ir logines schemas.<br>• Turi būti paruošti ir suderinti migravimo ir testavimo planai | organizacijos turimomis ugniasienėmis FortiGate 501E.<br>• Bus parengta Žurnalinių įvykių valdymo platformos prijungimo architektūra pateikiant fizines ir logines schemas.<br>• Bus paruošti ir suderinti migravimo ir testavimo planai |
| 4.3. | Montavimas<br>Turi būti atlikta:<br>• perimetro ugniasienių sprendimo įrangos transportavimas, montavimas, sujungimas su tinklo;<br>• žurnalinių įvykių valdymo platformos transportavimas, montavimas, sujungimas su tinklo įranga;<br>• įranga turi būti sumontuota užsakovo patalpose adresu Eivenių g. 2 Kaunas. | Bus atlikta:<br>• perimetro ugniasienių sprendimo įrangos transportavimas, montavimas, sujungimas su tinklo;<br>• žurnalinių įvykių valdymo platformos transportavimas, montavimas, sujungimas su tinklo įranga;<br>• įranga bus sumontuota užsakovo patalpose adresu Eivenių g. 2 Kaunas. |
| 4.4. | Migravimas<br>Pagal paruoštą perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūrą Perimetro ugniasienėse atlikti šiuos migravimo/diegimo darbus:<br>o IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas;<br>o IP adresų/servisų objektų konfigūravimas;<br>o prieigos taisyklių konfigūravimas;<br>o saugumo profilių konfigūravimas;<br>o NAT konfigūravimas;<br>o Site-to-site IPsec VPN konfigūravimas;<br>o nuotolinės prieigos darbuotojams konfigūravimas;<br>o RADIUS, LDAP serverių IP konfigūravimas;<br>o lokalių administratorių paskyrų ir paskyrų profilių kūrimas;<br>o statinės ir dinaminės maršrutizacijos konfigūravimas;<br>o MLAG/LAG agreguotų sąsajų konfigūravimas;<br>o VLAN konfigūravimas;<br>o prievadų konfigūravimas;<br>o virtualių sistemų konfigūravimas;<br>o programinės įrangos atnaujinimas ir saugos aprašų duomenų bazių atnaujinimas iki naujausios gamintojo siūlomos versijos;<br>o aukšto patikimumo telkinio konfigūravimas.<br>Pagal paruoštą perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūrą Vidinio segmentavimo ugniasienėse atlikti šiuos migravimo /diegimo darbus: | Pagal paruoštą perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūrą Perimetro ugniasienėse bus atlikti šie migravimo/diegimo darbai:<br>o IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas;<br>o IP adresų/servisų objektų konfigūravimas;<br>o prieigos taisyklių konfigūravimas;<br>o saugumo profilių konfigūravimas;<br>o NAT konfigūravimas;<br>o Site-to-site IPsec VPN konfigūravimas;<br>o nuotolinės prieigos darbuotojams konfigūravimas;<br>o RADIUS, LDAP serverių IP konfigūravimas;<br>o lokalių administratorių paskyrų ir paskyrų profilių kūrimas;<br>o statinės ir dinaminės maršrutizacijos konfigūravimas;<br>o MLAG/LAG agreguotų sąsajų konfigūravimas;<br>o VLAN konfigūravimas;<br>o prievadų konfigūravimas;<br>o virtualių sistemų konfigūravimas;<br>o programinės įrangos atnaujinimas ir saugos aprašų duomenų bazių atnaujinimas iki naujausios gamintojo siūlomos versijos;<br>o aukšto patikimumo telkinio konfigūravimas.<br>Pagal paruoštą perimetro ir vidinio segmentavimo ugniasienių atskyrimo architektūrą Vidinio segmentavimo ugniasienėse bus atlikti šie migravimo /diegimo darbus: |

| | | |
|---|---|---|
| | ○ IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas;<br>○ IP adresų/servisų objektų konfigūravimas;<br>○ prieigos taisyklių konfigūravimas;<br>○ saugumo profilių konfigūravimas;<br>○ NAT konfigūravimas;<br>○ RADIUS, LDAP serverių IP konfigūravimas;<br>○ statinės ir dinaminės maršrutizacijos konfigūravimas;<br>○ MLAG/LAG agreguotų sąsajų konfigūravimas;<br>○ VLAN konfigūravimas;<br>○ prievadų konfigūravimas;<br>○ virtualių sistemų konfigūravimas;<br>○ programinės įrangos atnaujinimas ir saugos aprašų duomenų bazių atnaujinimas iki naujausios gamintojo siūlomos versijos;<br>○ aukšto patikimumo telkinio konfigūravimas.<br>Žurnalinių įvykių valdymo platformos diegimas:<br>○ žurnalinių įvykių valdymo platformos integravimas su perimetro ir vidinio segmentavimo ugniasienėmis;<br>○ žurnalinių įvykių valdymo platformoje ataskaitų konfigūravimas. | ○ IP adresų, SSH, SNMP, NTP, SYSLOG konfigūravimas;<br>○ IP adresų/servisų objektų konfigūravimas;<br>○ prieigos taisyklių konfigūravimas;<br>○ saugumo profilių konfigūravimas;<br>○ NAT konfigūravimas;<br>○ RADIUS, LDAP serverių IP konfigūravimas;<br>○ statinės ir dinaminės maršrutizacijos konfigūravimas;<br>○ MLAG/LAG agreguotų sąsajų konfigūravimas;<br>○ VLAN konfigūravimas;<br>○ prievadų konfigūravimas;<br>○ virtualių sistemų konfigūravimas;<br>○ programinės įrangos atnaujinimas ir saugos aprašų duomenų bazių atnaujinimas iki naujausios gamintojo siūlomos versijos;<br>○ aukšto patikimumo telkinio konfigūravimas.<br><br>Žurnalinių įvykių valdymo platformos diegimas:<br>○ žurnalinių įvykių valdymo platformos integravimas su perimetro ir vidinio segmentavimo ugniasienėmis;<br>○ žurnalinių įvykių valdymo platformoje ataskaitų konfigūravimas. |
| 4.5. | Testavimas<br>Turi būti atlikta:<br>○ ugniasienių aukšto patikimumo testavimas;<br>○ sistemų stebėjimas po migracijos ir problemų šalinimas. | Bus atlikta:<br>○ ugniasienių aukšto patikimumo testavimas;<br>○ sistemų stebėjimas po migracijos ir problemų šalinimas. |
| 4.6. | Mokymai<br>Tiekėjas turi apmokyti iki 3 Perkančiosios organizacijos darbuotojų, pateiktos įrangos administravimui ir priežiūrai. | Tiekėjas apmokys iki 3 Perkančiosios organizacijos darbuotojų, pateiktos įrangos administravimui ir priežiūrai. |
| 4.7. | Dokumentacija<br>Turi būti pateikta visa su projekto įgyvendinimu susijusi dokumentacija. | Bus pateikta visa su projekto įgyvendinimu susijusi dokumentacija. |