

PREKIŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

1.1. Pirkėjas – Uždaroji akcinė bendrovė „VILNIAUS VANDENYS“.

1.2. Pardavėjas - ūkio subjektas – fizinis asmuo, privatusis ar viešasis juridinis asmuo, kita organizacija ir (ar) jų padalinys įskaitant ūkio subjektus, kurių pajėgumais remiamasi, Subtiekėjus, darbuotojus ir kitus teisėtai pagrindais Prekių tiekimui pasitelktus asmenis.

1.3. Sutartis – Sutartis, sudaroma tarp Pardavėjo ir Pirkėjo dėl Pirkimo objekto.

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

1.5. Priėmimo-perdavimo aktas arba Aktas - perdavimo–priėmimo aktas arba kitas lygiavertis dokumentas, pasirašomas abiejų Sutarties Šalių, kuriame nurodomos Pardavėjo Pirkėjui faktiškai perduotos Prekės ir (ar) atlikti darbai ar suteiktos paslaugos, susiję su Prekių parengimu tinkamai naudoti. Aktas pasirašomas tais atvejais, kai Pardavėjo patiektos Prekės turi būti sumontuotos ar kitokiu būdu paruoštos tinkamam jų naudojimui.

1.6. Važtaraštis - teisės aktų reikalavimus atitinkantis dokumentas, pasirašomas abiejų Sutarties Šalių, kuriame nurodomos Pardavėjo Pirkėjui faktiškai perduotos Prekės ir kurį Pardavėjas Sutartyje nustatyta tvarka perduoda Pirkėjui kartu su Prekėmis. Važtaraštis pasirašomas tuo atveju, jeigu Pardavėjo patiektos Prekės nereikalauja sumontavimo ar kitokių papildomų veiksmų atlikimo, siekiant tinkamai naudoti įsigytas Prekes. Važtaraščio funkciją gali atlikti Prekes pristatiusio kurjerio elektroninėje laikmenoje Pirkėjo atstovo pasirašomas dokumentas.

2. PIRKIMO OBJEKTO PAVADINIMAS IR JO KIEKIAI/APIMTYS

2.1. Turimos saugumo sistemos Sophos atnaujinimas (toliau – Prekės).

2.2. Pirkimo objektas nėra skaidomas į pirkimo objekto dalis.

2.3. Perkamos Prekės ir jų kiekiai:

2.3.1. Ugniasienė (įrenginys) – 2 vnt.

2.3.2. Pagerintos palaikymo „plus“ paslaugos licencija – 1 vnt.

2.3.3. Elektroninio pašto apsaugos funkcionalumo licencija – 1 vnt.

2.3.4. WEB aplikacijų saugumo (WAF) funkcionalumo licencija – 1 vnt.

2.4. Kiekiai/APImtys: Perkamas Prekių kiekis yra konkretus.

2.5. Pardavėjas visas galimas išlaidas įskaičiuoja į Prekių įkainį ir (ar) kainą. Siūlomame įkainyje ir (ar) kainoje turi būti įskaičiuotos visos Pardavėjo išlaidos ir mokėtini mokesčiai, būtini tinkamam Sutarties įvykdymui.

2.6. Pardavėjas prisiima visą riziką dėl ne nuo Pirkėjo priklausančių aplinkybių, dėl kurių padidės su Sutarties vykdymu susijusios Pardavėjo išlaidos ir Pardavėjui Sutarties vykdymas taps sudėtingesnis (Pardavėjui padidės įsipareigojimų vykdymo kaina). Prekių kaina ir (ar) įkainiai jokiais atvejais nebus didinami, išskyrus Pirkimo sąlygose nustatytus kainos ir (ar) įkainių peržiūros procedūros atvejus.

2.7. Pirkimas laikomas žaliuoju, kadangi pirkimo objektui taikomi aplinkos apsaugos kriterijai, nustatyti Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 patvirtinto Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo 4.4.3 papunktyje (perkama prekė: programinės įrangos nuoma).

3. REIKALAVIMAI PIRKIMO OBJEKTUI

3.1. Pirkimo objekto aprašymas

3.1.1. Pirkėjas naudoja Sophos UTM aukšto patikimumo kompiuterinio tinklo apsaugos sistemą, kurios techninei įrangai baigiasi techninis palaikymas bei licencijų galiojimas. Įsigijamos prekės užtikrins patikimą kompiuterinio tinklo perimetro apsaugą nuo šios dienos kibernetinių grėsmių.

3.1.2. Licencijų galiojimas – ne mažiau nei 36 mėn.

- 3.1.3. Prekės turi būti naujos, kokybiškos ir nenaudotos, pateikiamos originalioje gamintojo pakuotėje, gamykliškai atnaujinti komponentai (ang. „Refurbished“) neleistini.
- 3.1.4. Pardavėjas turi užtikrinti, kad Prekių gamintojas nėra paskelbęs apie siūlomų Prekių gamybos arba tobulinimo nutraukimą (pvz. ang. „End of life time“ ar „Discontinued“).
- 3.1.5. Siūlomų Prekių gamintojas turi būti registruotas NATO arba ES priklausančioje valstybėje.
- 3.1.6. Techninėje specifikacijoje nurodyti konkretūs modeliai, tipai, sistemos, sertifikatai ir kt. gali būti pakeisti lygiavertėmis. Jei Pardavėjas siūlo lygiavertes medžiagas, standartus, metodus, tipus ar pan. – kartu su Pasiūlymu turi būti pateikiama ir pagrįsta informacija - pagrindimas – iš kurios Pirkėjas galėtų nustatyti, kad siūlomos medžiagos, standartai, metodai, tipai ar pan. yra lygiavertės reikalaujamoms.
- 3.1.7. Nurodytos Prekės (medžiagos, produktai, įranga), nekeičiant kainos, Pirkėjo sutikimu gali būti pakeistos kitomis, jeigu Prekės nebegaminamos ir Pardavėjas Pirkėjui pateikia tai pagrindžiančius dokumentus (pavyzdžiui, gamintojo raštą / patvirtinimą, kad Prekė nebegaminama). Pardavėjas taip pat privalo pateikti dokumentus, pagrindžiančius, jog naujos Prekės visiškai atitinka pirkimo dokumentuose nustatytą techninę specifikaciją ir (ar) Pardavėjo pasiūlyme nurodytas techninių rodiklių reikšmes, yra ne prastesnės, o lygiavertės ar geresnės kokybės. Toks Prekės (-ių) keitimas įforminamas raštu sudarant papildomą susitarimą prie Sutarties.
- 3.1.8. Prekėms turi būti taikoma **ne mažiau kaip 36 mėn.** nemokama kokybės garantija. Garantinis laikotarpis prasideda nuo Prekių perdavimo–priėmimo momento.
- 3.1.9. Pardavėjas garantuoja, kad Prekių garantiniu laikotarpiu gedimai, atsiradę dėl brokuotų medžiagų ar Prekių gamybos klaidų bus šalinami nemokamai arba pakeičiant nekokybiškas Prekes naujomis.
- 3.1.10. Prekės turi visiškai atitikti lentelėje Nr. 1 „Reikalavimai prekėms“ nurodytiems reikalavimams.

Lentelė Nr. 1 Reikalavimai prekėms

Eil. Nr.	Charakteristikos pavadinimas
Reikalavimai ugniasienėms	
1.	Reikalavimai fiziniams sąsajoms
1.1.	Ne mažiau kaip 4 vnt. 1G vario prievadų su LAN bypass funkcija.
1.2.	Ne mažiau kaip 4 vnt. 2,5G vario prievadų.
1.3.	Ne mažiau kaip 4 vnt. 10G SFP+ prievadų.
1.4.	Galimybė pajungti ne mažiau kaip 2 vnt. sąsajų išplėtimo modulius. Galimi praplėtimo moduliai: * 8 vnt. 1G variniai prievadai; * 8 vnt. 1G SFP prievadai; * 4 vnt. 10G SFP+ prievadai; * 4 vnt. 1G variniai su bypass prievadai; * 4 vnt. 1G variniai su PoE + 4 vnt. 1G variniai prievadai; * 2 vnt. 1G optiniai (LC) su bypass + 4 vnt. 1G SFP optiniai prievadai.
1.5.	Ne mažiau kaip 2 vnt. USB 3.0 jungčių

Eil. Nr.	Charakteristikos pavadinimas
1.6.	Ne mažiau kaip šios valdymui skirtos jungtys: * 1 vnt. micro USB; * 1 vnt. COM (RJ45); * 1 vnt. Ethernet (RJ45).
1.7.	Integruotas multifunkcinis LCD ekranas.
2.	Reikalavimai fiziniams išmatavimams bei aplinkai
2.1.	Įrenginys ne didesnis kaip 1 U bei pritaikytas montuoti į 19“ komutacinę spintą. Turi būti pateikiamas su visais montavimui reikalingais priedais (įskaitant bet neapsiribojant tvirtinimo elementais).
2.2.	Galimybė veikti esant 0 - 40°C temperatūrai.
2.3.	Galimybė veikti esant 10% - 90% drėgnumui (nekondensuojantis).
2.4.	Elektros suvartojimas ne didesnis kaip 155 W (be apkrovos), 270 W (pilna apkrova).
2.5.	Vidinis karšto keitimo maitinimo blokas 100-240 VAC, 50-60 Hz.
2.6.	Turi būti galimybė pajungti antrą (vidinį) maitinimo bloką.
3.	Reikalavimai tinklo srauto apdorojimo pajėgumams
3.1.	Integruotas dubliuotas (RAID1) SSD skirtas vietiniam karantinui, talpyklai (angl. cache) bei žurnalų įrašams (angl. log) ne mažesnės kaip 240 GB talpos.
3.2.	Ugniasienės pralaidumas ne mažesnis kaip 80 Gbps.
3.3.	Ugniasienės IMIX (Internet Mix) pralaidumas ne mažesnis kaip 37 Gbps.
3.4.	Ugniasienės vėlinimas (64 byte UDP) ne didesnis kaip 4 μs.
3.5.	Virtualaus privataus tinklo (IPsec) prieigos vartų pralaidumas ne mažesnis kaip 75 Gbps.
3.6.	Virtualaus privataus tinklo (SSL VPN) prieigos vartų palaikomų sujungimų skaičius ne mažesnis kaip 10000 vnt.
3.7.	Apsaugos nuo įsiveržimo (IPS) srauto pralaidumas ne mažesnis kaip 36 Gbps.
3.8.	Apsaugos nuo grėsmių (Threat Protection) srauto pralaidumas ne mažesnis kaip 31 Gbps.
3.9.	SSL / TLS dekodavimo pralaidumas ne mažesnis kaip 10 Gbps.
3.10.	SSL / TLS dekodavimo konkurentinių prisijungimų skaičius ne mažesnis kaip 276000 vnt.
3.11.	TCP konkurencinių prisijungimų skaičius ne mažesnis kaip 17000000 vnt.
3.12.	TCP naujų sesijų per sekundę skaičius ne mažesnis kaip 450000 vnt.

Eil. Nr.	Charakteristikos pavadinimas
4.	Reikalavimai įrangos palaikymui ir atnaujinimui
4.1.	Įrangai suteikiama ne trumpesnė kaip 36 mėn. gamintojo garantija.
4.2.	Turi būti užtikrintas 24/7 gamintojo techninis palaikymas (telefonu, el. paštu).
4.3.	Programinės įrangos, saugumo modulių (kurie turi būti periodiškai atnaujinami), virusų duomenų bazės atnaujinimai internetu turi būti galimi ne trumpiau kaip 36 mėn.
5.	Valdymo ir aukšto patikimumo reikalavimai
5.1.	Turi būti ugniasienės taisyklių grupavimas bei taisyklių sąrašė lengvai matomi indikatoriai kokios funkcijos įjungtos konkrečiai taisyklei.
5.2.	Turi būti palaikomas dviejų faktorių autentifikavimas: <ul style="list-style-type: none"> • administratoriaus bei vartotojo prisijungimui prie ugniasienės: • IPSEC bei SSL VPN prisijungimams.
5.3.	Turi būti tiesiai iš grafinės administravimo aplinkos prieinami trikdžių analizės bei šalinimo įrankiai (pvz.: paketų gaudyklė).
5.4.	Turi palaikyti aukšto dviejų įrenginių apjungimą į aukšto patikimumo grupę dirbant aktyvus - pasyvus arba aktyvus - aktyvus režimais.
5.5.	Turi būti tiesiai iš grafinės administravimo aplinkos prieinamas valdymas per komandinę eilutę (CLI).
5.6.	Ugniasienės administratoriams turi būti galima priskirti roles.
5.7.	Turi būti tiekiami ugniasienės programinės įrangos (angl. firmware) atnaujinimai, administratorius turi gauti pranešimus apie atsiradusį naują atnaujinimą. Turi būti galimybė lengvai grįžti į praeitą programinės įrangos bei konfigūracijos versiją neperdiegiant įrenginio operacinės sistemos.
5.8.	Turi būti galimybė kurti sisteminius objektus kuriuos vėliau galima naudoti konfigūracijoje. Objektai kuriami tinklams, prievadams, kompiuteriams, serveriams, vartotojams bei jų grupėms.
5.9.	Vartotojams turi būti prieinamas savitarnos portalas.
5.10.	Turi būti galimybė matyti ugniasienėje atliktų pakeitimų registrą.
5.11.	Turi būti galimybė lanksčiai valdyti prieigą prie ugniasienės valdymo konsolės pagal zonas.
5.12.	Turi būti palaikomi SNMP v3, sFlow (Sampled Flow) bei Netflow protokolai.
5.13.	Turi būti galimybė daryti ugniasienės konfigūracijos atsargines kopijas. Kopijos turi būti saugomos pačioje ugniasienėje su galimybe siųsti jas FTP protokolu ar el. paštu. Turi būti galimybė atsargines kopijas daryti rankiniu arba automatinio būdu pagal grafiką: kas dieną, kas savaitę, kas mėnesį.
5.14.	Turi būti palaikomas valdymas per API (angl. Application Programming Interface).
5.15.	Turi būti galimybė pervadinti ugniasienės tinklo prievadus.
5.16.	Turi būti galimybė įjungti saugią nuotolinę prieigą gamintojo IT priežiūros komandai.

Eil. Nr.	Charakteristikos pavadinimas
5.17.	Turi būti gamintojo portalas kuriame būtų galima valdyti licencijų naudojimą.
5.18.	Turi būti galimybė valdyti ugniasienę per debesija paremtą valdymo konsolę be papildomo mokesčio.
5.19.	Turi būti palaikomas automatinis Let's Encrypt sertifikatų diegimas.
6.	Reikalavimai debesija paremtai valdymo konsolei
6.1.	Turi būti galimybė valdyti kelias ugniasienes iš karto bei matyti kelių ugniasienių ataskaitas.
6.2.	Turi būti galimybė kurti ir valdyti objektus, nustatymus bei politikas kelioms ugniasienėms iš karto, o pakeitimai turi automatiškai sinchronizuotis su tomis ugniasienėmis.
6.3.	Turi būti galimybė matyti pakeitimų istoriją bei vykdomų pakeitimų statusą.
6.4.	Turi būti galimybė valdyti ugniasienių konfigūracijų atsargines kopijas bei programinės įrangos atnaujinimus.
6.5.	Turi būti galimybė, pasinaudojant USB atmintine, sukurtą konfigūraciją eksportuoti ir tuomet įdiegti į ugniasienę, ko pasekoje ugniasienė būtų automatiškai prijungta prie debesija paremtos valdymo konsolės.
7.	Reikalavimai paketų filtravimui ir maršrutizavimui
7.1.	Ugniasienė turi dirbti statefull režime bei gebėti atlikti gilią paketų analizę.
7.2.	Ugniasienė turi palaikyti TLS 1.3 nežemindama TLS versijos bei gebėti dešifruoti bet kokį TLS srautą vykstantį bet kokiais prievadais.
7.3.	Ugniasienėje turi būti srauto spartinimo funkcija kurią galima valdyti rankiniu būdu arba automatiškai.
7.4.	Turi būti galimybė ugniasienės taisykles kurti zonoms, tinklams, vartotojams, grupėms bei prievadams. Turi būti galimybė taisykles taikyti tik tam tikru laiku.
7.5.	Turi būti galimybė valdyti kuriuo laiku tam tikri vartotojai ar grupės turės prieigą prie tinklo resursų.
7.6.	Turi būti NAT (angl. Network Address Translation) valdymas su galimybe peradresuoti kelis prievadus vienoje taisyklėje. Turi būti NAT taisyklių kūrimo vedlys padedantis greitai sukurti sudėtingas taisykles.
7.7.	Turi būti apsauga nuo DoS, DDos atakų.
7.8.	Turi būti galimybė kontroliuoti prieigą pagal šalį (Geo-IP).
7.9.	Turi būti palaikomas statinis, dinaminis ir multicast maršrutizavimas. Palaikomi dinamio maršrutizavimo protokolai: RIP, BGP (įskaitant BGPv6), OSPF (įskaitant OSPFv3).
7.10.	Turi būti galimybė sukonfigūruoti HTTP(s) proxy serverį per kurį būtų pasiekiamas internetas (angl. Upstream proxy).
7.11.	Turi būti palaikomas prievadų apjungimas (angl. bridging) su STP bei ARP broadcast palaikymu.
7.12.	Turi būti palaikomi VLAN, galimybė kurti VLAN ant apjungtų (angl. bridged) prievadų. Taip pat turi būti palaikomas DHCP protokolas atskiriems VLAN.

Eil. Nr.	Charakteristikos pavadinimas
7.13.	Turi būti palaikomi keli interneto prievadai su galimybe: <ul style="list-style-type: none"> tikrinti jų veikimą; automatiškai naudoti kitą prievadą jei neveikia pirmasis; naudoti kelis prievadus iš karto srautą dalinant pagal „svorius“ (angl. Load balancing); valdyti kaip keli prievadai yra išnaudojami pagal įeinantį prievadą, pradžios tinklą, tikslo tinklą, servisą, aplikaciją, ar vartotoją.
7.14.	Turi būti palaikomi didelių dydžių paketai (angl. jumbo frame).
7.15.	Turi būti palaikomas 802.3ad tinklo prievadų apjungimas.
7.16.	Turi būti palaikomas dinaminis DNS.
7.17.	Turi būti galimybė konfigūruoti DNS, DHCP bei NTP servigus.
7.18.	Turi palaikyti IPv6 bei IPv6 tuneliavimą įskaitant: 6in4, 6to4, 4in6 bei IPv6 greitą diegimą (6rd) per IPSec.
8.	Srauto prioretizavimo ir valdymo reikalavimai
8.1.	Turi palaikyti DSCP žymėjimą ir VoIP srauto prioretizavimo galimybę.
8.2.	Turi būti galimybė nustatyti vienkartinės bei periodinės srauto kvotas vartotojams.
8.3.	Turi būti galimybė nustatyti srauto prioretizavimą vartotojams bei tinklams.
9.	Reikalavimai vartotojų autentifikavimui
9.1.	Turi būti palaikomas vartotojų autentifikavimas per: Active Directory, Entra ID (Azure AD), RADIUS, LDAP ir TACACS+.
9.2.	Turi būti palaikomas SSO (angl. Single Sign On) su: Active directory, Entra ID (Azure AD), RADIUS Accounting.
9.3.	Turi būti teikiama klientų autentifikavimo programinė įranga šioms OS: Windows, Mac OS X, Linux 32/64.
9.4.	Turi būti palaikoma naršyklės SSO: NTLM bei Kerberos.
9.5.	Turi būti galimybė sudiegti autentifikavimo sertifikatus iOS bei Android operacinėms sistemoms.
9.6.	Turi būti palaikomas Google Chromebook autentifikavimas naudojant Active Directory ir Google G Suite.
9.7.	Turi būti palaikomas API paremtas autentifikavimas.
10.	Reikalavimai vartotojų savitarnos portalui
10.1.	Turi būti galimybė parsisiųsti VPN agentą bei konfigūraciją.
10.2.	Turi būti galimybė parsisiųsti autentifikavimo agentą.
10.3.	Turi būti prieinama informacija apie Hotspot tipo bevielį tinklą.
10.4.	Turi būti galimybė pasikeisti savo slaptažodį.

Eil. Nr.	Charakteristikos pavadinimas
10.5.	Turi būti galimybė peržiūrėti savo interneto srauto naudojimą.
10.6.	Turi būti galimybė peržiūrėti el. pašto karantiną bei valdyti vartotojo blokavimų/leidimų sąrašą (tuomet kai naudojama el. pašto apsaugos licencija).
11.	Reikalavimai virtualaus privataus tinklo (VPN) technologijai
11.1.	Turi būti palaikomi Site-to-Site sujungimai naudojant SSL bei IPSEC VPN.
11.2.	Turi būti palaikomi 256bit AES-GCM, PFS, X.509 sertifikatai bei PSK (angl. pre-shared key) autentifikavimo / kodavimo algoritmai.
11.3.	Turi būti palaikomas SSO su Microsoft Entra ID.
11.4.	Turi būti palaikomas L2 pagal OSI modelį įrenginių apjungimo VPN tunelis.
11.5.	Turi būti palaikomas IKEv2.
11.6.	Turi būti palaikomi L2TP, PPTP, SSL bei IPSEC VPN vartotojų prisijungimams.
11.7.	Turi būti gamintojo teikiami VPN klientai (programinė įranga) Windows bei macOS operacinėms sistemoms.
11.8.	Teikiamas VPN klientas turi palaikyti srauto dalinimo funkciją (split tunneling), bei NAT traversal.
11.9.	VPN vartotojų skaičius nėra ribojamas įsigyjamose licencijose ir priklauso tik nuo aparatinės įrangos pajėgumų.
11.10.	VPN klientai teikiami nemokamai.
12.	Reikalavimai SD-WAN funkcijoms
12.1.	Galimybė prijungti keletą interneto prievadų su veikimo stebėjimu, apkrovos balansavimu, bei antrinės linijos aktyvavimu sugedus pirminei linijai.
12.2.	Galimybė lanksčiai kontroliuoti maršrutizavimą pagal naudojamą aplikaciją.
13.	Reikalavimai integruotoms saugumo sistemoje ataskaitoms bei registrui ir įspėjimo pranešimams
13.1.	<p>Turi būti integruotas ataskaitų įrankis rodantis:</p> <ul style="list-style-type: none"> • Tinklo srauto naudojimą; • Saugumo informaciją; • Rizikingu elgesiu internete pasižyminčius vartotojus; • Naudojamų aplikacijų informaciją; • Stebimų žodžių (keyword) pasitaikymą puslapiuose; • Tinklo grėsmių analizę; • VPN naudojimą; • El. pašto apsaugos naudojimą (tuomet kai naudojama el. pašto apsaugos licencija).

Eil. Nr.	Charakteristikos pavadinimas
13.2.	Turi būti galimybė peržiūrėti realaus laiko informaciją apie: <ul style="list-style-type: none"> • sistemos būseną; • prisijungusius vartotojus; • IPSec VPN sujungimus; • nutolusius vartotojus; • aktyvius sujungimus; • el. pašto karantiną (tuomet kai naudojama el. pašto apsaugos licencija).
13.3	Turi būti galimybė eksportuoti nuasmenintas ataskaitas.
13.4.	Turi būti galimybė siųsti ataskaitas pagal grafiką keliais adresais.
13.5.	Turi būti galimybė eksportuoti ataskaitas HTML, PDF, XLS formatais.
13.6.	Turi būti galimybė sukonfigūruoti kiek laiko bus saugoma ataskaitų informacija pagal ataskaitų kategoriją.
13.7.	Turi būti integruotas įrankis ugniasienės aktyvumo žurnalui peržvelgti su galimybe: <ul style="list-style-type: none"> • filtruoti sąrašą; • pakeisti sąrašo išvaizdą; • tiesiai iš sąrašo nueiti į susijusių ugniasienės taisyklę.
13.8.	Turi būti galimybė gauti operatyvius pranešimus apie vartotojus naršančius ribojamų kategorijų internetinėse svetainėse.
14.	Reikalavimai įsiveržimo aptikimo ir prevencijos sistemai
14.1.	Ugniasienė privalo turėti naujos kartos įsibrovimų prevencijos sistemą IPS (angl. intrusion prevention system), gebančią atlikti išsamų paketų patikrinimą DPI (angl. deep packet inspection).
14.2.	Ugniasienės administratorius turi galėti pasirinkti norimą IPS tikrinimo modelį ir jį priskirti norimai ugniasienės taisyklei.
14.3.	Ugniasienė privalo turėti gamintojo paruoštus ir reguliariai atnaujinamus IPS aprašus (angl. IPS signatures) su granuliariu kategorijų pasirinkimu.
14.4.	Turi būti galimybė pridėti savo IPS aprašus.
14.5.	Turi būti galimybė filtruoti IPS aprašus pasinaudojant lanksčiais filtrais, kurie būtų pritaikomi ir ateityje, kai gamintojas išleidžia atnaujintus aprašų sąrašus.
14.6.	Ugniasienė privalo aptikti ir blokuoti tinklo srautą, bandant susisiekti su komandų ir valdymo serveriais.
15.	Nutolusių taškų pajungimui skirtų įrenginių valdymas
15.1.	Ugniasiene turi gebėti valdyti visus SD-WAN įrenginius iš vienos konsolės, taip leidžiant administratoriams valdyti tinklą neprisijungs tiesiogiai prie galinių įrenginių.
15.2.	Šie prietaisai neturi reikalaui jokios išankstinės konfigūracijos ir turi prisijungti prie pagrindinės ugniasienės automatiškai pasinaudojant debesies pagrindu veikiančia teikimo paslauga, taip suteikiant galimybę siųsti įrenginius į nutolusius skyrius, kur reikės tik sujungti laidus be jokios papildomos konfigūracijos.

Eil. Nr.	Charakteristikos pavadinimas
15.3.	Turi naudoti apsaugotą ir užšifruotą tunelį naudojant skaitmeninius X.509 sertifikatus ir AES 256 bitų šifravimą.
15.4.	Turi veikti kaip virtualus „Ethernet“ tinklas, užtikrinantis patikimą viso srauto perdavimą tarp vietovių.
15.5.	Turi būti IP adresų valdymas su centralizuotai valdoma DHCP ir DNS serverių konfigūracija.
15.6.	Turi galėti automatiškai, nuotoliniu būdu panaikinti SD-WAN įrenginio autorizaciją po administratoriaus pasirinkto neveikimo laikotarpio.
15.7.	Turi būti galimybė suspausti tuneliu keliaujantį srautą.
15.8.	Įrenginiai turi gebėti sukurti L2 pagal OSI lygio tinklą bei palaikyti VLAN žymėjimą.
16.	Ugniasienės bei kompiuterinės darbo vietos apsaugos suderinamumas / sinchronizavimas
16.1.	Ugniasienė turi turėti galimybę keisti informaciją su to paties gamintojo antivirusine sistema (diegiama į kompiuterius ar serverius) ir taip suteikti galimybę iškart nustatyti pažeistus galinius taškus, įskaitant kompiuterį, vartotoją, procesą, įvykių skaičių ir įvykio laiką.
16.2.	Ugniasienė, reaguodama į to paties gamintojo antivirusinės sistemos (diegiamos į kompiuterius ar serverius) žinutes turi turėti galimybę apriboti prieigą prie tinklo išteklių arba visiškai izoliuoti pažeistas sistemas, kol jos bus išvalytos.
16.3.	Atlikus ugniasienės ir antivirusinės sistemos integraciją turi būti galimybė blokuoti visą komunikaciją tarp sveikų ir užkrėstų kompiuterinių darbo vietų. Visas srautas turi būti atmetamas, taip užkertant kelią grėsmių judėjimui tame pačiame transliacijos domene (angl. broadcast domain).
17.	VPN veikiantis per naršyklę
17.1.	Ugniasienė turi suteikti HTML5 standartu paremtą VPN portalą, kuris palaiko bent šiuos protokolus: RDP, HTTP, HTTPS, SSH, Telnet ir VNC.
18.	Reikalavimai interneto saugumo funkcionalumui
18.1.	Ugniasienė turi turėti visiškai skaidrų (angl. Fully transparent proxy) kenkėjiškų programų ir interneto filtravimą.
18.2.	Ugniasienė privalo turėti gamintojo paruoštą ir reguliariai atnaujinamą URL filtravimo kategorijų duomenų bazę.
18.3.	Ugniasienė privalo turėti galimybę nustatyti naršymo kvotos laiko politiką vienam arba grupei vartotojų.
18.4.	Administratorius turi galėti nustatyti vartotojo ar grupės prieigos laiko politiką.
18.5.	Ugniasienė turi mokėti aptikti kenkėjiškas programas ir blokuoti visas virusų formas, žiniatinklio kenkėjiškas programas, Trojos arklius ir šnipinėjimo programas keliaujančias HTTP (S), FTP ar žiniatinklio el. paštu.
18.6.	Ugniasienė turi turėti pažangią interneto kenkėjiškų programų apsaugą naudojant „JavaScript“ imitaciją.
18.7.	Ugniasienė turi turėti apsaugą realiuoju laiku ieškant naujausios informacijos apie grėsmes debesyje.
18.8.	Ugniasienė privalo turėti bent du skirtingus kenkėjiškų programų aptikimo variklius. Administratorius turi galėti pasirinkti naudoti viena iš jų ar abu iškart.
18.9.	Administratorius turi galėti pasirinkti skenavimą atlikti realiuoju laiku arba paketiniu režimu (angl. batch mode).
18.10.	Ugniasienė turi turėti farmingo (angl. pharming) apsaugą.

Eil. Nr.	Charakteristikos pavadinimas
18.11.	Ugniasienė turi gebėti atlikti HTTP (S) skenavimą bei kontrolę visuose pasirinktuose tinkluose ir pasirinktiems vartotojams ar jų grupėms su pilnai konfigūruojamomis taisyklėmis ir išimtimis.
18.12.	Ugniasienė turi gebėti aptikti SSL tunelius bei juos kontroliuoti.
18.13.	Ugniasienė turi gebėti tikrinti SSL sertifikatų galiojimą bei tikrumą.
18.14.	Ugniasienė turi atlikti failo filtravimą pagal „MIME“ tipą, plėtinį ar aktyvaus turinio tipą (pvz. „ActiveX“, programėlės, slapukai ir kt.).
18.15.	Ugniasienė turi turėti „Safe Search“ funkcionalumą (pagrįstą DNS) pagrindiniams paieškos varikliams pagal politiką (vartotojas / grupė).
18.16.	Ugniasienė privalo gebėti stebėti, registruoti, raportuoti ir blokuoti tinklo turinį atitinkantį raktinį žodį iš sąrašo su galimybe įkelti savo sukurtus sąrašus.
18.17.	Ugniasienė privalo blokuoti potencialiai nepageidaujamas programas.
18.18.	Ugniasienė privalo turėti pilnai konfigūruojamą funkcionalumą kiekvienam naudotojui atskirai, leidžiantį laikinai pasiekti blokuojamas žiniatinklio svetaines ar jų kategorijas.
18.19.	Atlikus ugniasienės ir Pirkėjo naudojamos antivirusinės programos integraciją turi veikti visų nežinomų „Windows“ ir „MacOS“ programų tinkle automatinis identifikavimas, klasifikavimas ir valdymas, dalijantis informacija tarp valdomų galinių taškų ir ugniasienės.
18.20.	Ugniasienė privalo turėti aprašais pagrįstą programų valdymą su bent tūkstančiu aprašų sąrašu.
18.21.	Ugniasienė privalo turėti debesijos programų matomumą ir valdymą.
18.22.	Ugniasienė privalo turėti programų valdymo išmaniuosius filtrus, kurie įgalina dinaminę politiką, kuri automatiškai atnaujinama, kai pridedami nauji programų aprašai.
18.23.	Ugniasienė turi gebėti atrasti ir valdyti mikro programas (angl. Micro app).
18.24.	Ugniasienė turi gebėti atlikti programų valdymą pagal kategorijas, charakteristikas (pvz. Pralaidumo ir našumo sąnaudas), technologijas (pvz., P2P) ir rizikos lygį.
18.25.	Ugniasienė turi valdyti srautą pagal žiniatinklio kategoriją ar programą, siekiant apriboti arba garantuoti įkeliamo ar atsisiunčiamo srauto prioritetą. Kvotas turi būti galima nustatyti kiekvienam naudotojui arba bendrai.
19.	Debesijos aplikacijų stebėjimo ir valdymo galimybės
19.1.	Ugniasienė turi pateikti informaciją apie duomenų kiekį įkeltą ir atsisiųstą naudojant debesijos programas. Turi būti galimybė skirstymas į kategorijas, kaip pav.: naujos, sankcionuojamos, nesankcionuojamos ir toleruojamos.
19.2.	Ugniasienės ataskaitose turi būti galima filtruoti debesijos programų naudojimą pagal kategoriją ar persiųstos informacijos kiekį.
Reikalavimai licencijoms	
20.	Reikalavimai elektroninio pašto apsaugos funkcionalumui
20.1.	Turi būti palaikomas el. pašto skenavimas naudojant SMTP, POP3 ir IMAP protokolus.
20.2.	Turi būti šlamšto (angl. spam) stebėjimas, kuris paremtas „Recurrent Pattern Detection“ technologija.
20.3.	Turi būti šlamšto ir kenkėjiškų programų blokavimas SMTP operacijos metu.

Eil. Nr.	Charakteristikos pavadinimas
20.4.	Turi būti DKIM ir BATV apsauga nuo šlamšto.
20.5.	Turi būti „Greylisting“ ir SPF apsaugos funkcijų palaikymas.
20.6.	Turi būti gavėjo patikrinimo dėl neteisingai įvestų el. pašto adresų palaikymas.
20.7.	Turi būti palaikomi du nepriklausomi apsaugos nuo kenksmingo kodo varikliai, bei galimybė pasirinkti naudoti vieną ar abu.
20.8.	Turi būti funkcija kuri realiuoju laiku (debesyje), patikrina ar skenuojamas failas yra saugus.
20.9.	Turi būti automatiniai aprašų ir šablonų atnaujinimai.
20.10.	Turi būti failo tipo nustatymo / blokavimo/ priedų nuskaitymo palaikymas.
20.11.	Turi būti funkcijų priimti, atmesti arba atmesti per didelius pranešimus, palaikymas.
20.12.	Turi aptikti fišingo nuorodas (angl. phishing URLs) el. laiškuose.
20.13.	Turi būti TLS šifravimo palaikymas SMTP, POP ir IMAP protokolams
20.14.	Turi gebėti pridėti parašą prie visų išeinančių laiškų automatiškai.
20.15.	Turi būti el. pašto archyvo palaikymas.
20.16.	Vartotojas, pasinaudodamas savitarnos portalu, turi galėti susikurti individualius blokuojamų ir leidžiamų siuntėjų sąrašus.
20.17.	Turi būti galimybė siųsti pranešimus apie į karantiną papuolusius laiškus.
20.18.	Turi būti kenkėjiškų pranešimų ir šlamšto susijusių su karantinu paieška, filtravimo galimybių pasirinkimai pagal datas, siuntėją, gavėją, temą, priežastį su galimybe ištrinti pranešimus.
20.19.	Turi būti vartotojų savitarnos portalo palaikymas, skirtas karantino pranešimams peržiūrėti ir išsiųsti.
20.20.	Turi būti integruota galimybė siųsti šifruotus el. laiškus be papildomos šifravimo programinės įrangos.
20.21.	Šifruoto laiško gavėjas turi galėti pats susikurti dešifravimo slaptažodį nenaudodamas jokios papildomos programinės įrangos išskyrus naršyklę.
20.22.	Šifruoto laiško gavėjas turi turėti galimybę saugiai atsakyti į laišką bei prie atsakymo galėti prisegti failus.
20.23.	Turi būti DLP funkcijos su automatiniu el. laiškų ir priedų skenavimu susijusių su jautriaisiais duomenimis palaikymas.
21.	Reikalavimai WEB aplikacijų saugumo (WAF) funkcionalumui
21.1.	Turi būti integruotas reverse proxy.
21.2.	Turi būti URL stiprinimo variklis su giliu nuorodų tikrinimu bei katalogų naršymo apsauga.
21.3.	Turi būti formų stiprinimo variklis.
21.4.	Turi būti apsauga nuo SQL injekcijų atakų.

Eil. Nr.	Charakteristikos pavadinimas
21.5.	Turi būti apsauga nuo cross-site scripting atakų.
21.6.	Turi būti palaikomas skenavimas su dviem nepriklausomais apsaugos nuo kenksmingo kodo varikliais su galimybe pasirinkti naudoti vieną ar abu kartu.
21.7.	Turi būti palaikomas HTTPS kodavimo nukrovimas.
21.8.	Turi būti slapukų pasirašymo funkcijos skaitmeniniais parašais palaikymas.
21.9.	Turi būti palaikomas maršrutizavimas pagal katalogą.
21.10.	Turi būti palaikomas Outlook Anywhere protokolas.
21.11.	Turi būti palaikomas autentifikavimo nukrovimas naudojant WEB formą arba bazinį naršyklės autentifikavimą.
21.12.	Turi būti palaikomas virtualaus ir fizinio serverio nukreipimas.
21.13.	Turi būti integruotas apkrovos balansavimo mechanizmas, kuris efektyviai paskirstytu vartotojų srautą keliuose serveriuose arba lygiavertė integruota funkcija.
21.14.	Turi būti galimybė kurti išimtis individualioms apsaugos funkcijoms.
21.15.	Turi būti gautų užklausų sutikrinimas iš tinklo šaltinių ar nurodytų atitinkamų URL adresų palaikymas.
21.16.	Turi būti suderinamumo palaikymas su įvairiomis konfigūracijomis ir nestandartiniais diegimais.
21.17.	Turi būti galimybė keisti WEB aplikacijų apsaugos sistemos našumo parametrus.
21.18.	Turi būti galimybė riboti skenuojamų failų dydžius.
21.19.	Turi būti galimybė leisti / blokuoti IP diapazonus.
21.20.	Turi būti „Wildcard“ palaikymas katalogams bei domeno vardams.
21.21.	Turi būti automatinio autentifikavimo žymų pridėjimo galimybė.
21.22.	Turi būti palaikomas SHA1, SHA256 ir SHA512 WEB aplikacijų saugumo dviejų faktorių autentifikavimas.
22.	Reikalavimai pagerinto palaikymo „plus“ paslaugai
22.1.	Visą palaikymo laikotarpį turi būti galimybė parsisiųsti ir įdiegti naujausius ugniasienės operacinės sistemos atnaujinimus.
22.2.	Turi būti numatyta galimybė automatiškai sudiegti naujausius saugumo atnaujinimus.
22.3.	Visą palaikymo laikotarpį turi būti sudaryta galimybė peržiūrėti, kurti, uždaryti ir administruoti techninės pagalbos užklausas bei gauti nuotolinę techninę pagalbą naudojantis SSH (angl. Secure Shell), Microsoft Terminal Services, LogMeIn Rescue arba TeamViewer.
22.4.	Nurodytam palaikymo laikotarpiui fizinės įrangos gedimo atveju turi būti suteikiama pakeitimo garantija.
22.5.	Esant gamintojo pripažintam garantiniam atvejui siuntimo išlaidos turi būti teikiamos gamintojo kaštais.
22.6.	Turi būti sudaryta galimybė gauti ne mažiau nei 8 valandas per metus nuotolinės gamintojo konsultacijos optimalaus ugniasienės konfigūravimo paslaugų ir gerųjų konfigūravimo praktikų įdiegimui.

Eil. Nr.	Charakteristikos pavadinimas
22.7.	Fizinės įrangos garantiją turi apimti ir papildomą įrenginį kuris dirba viename klasteryje (aktyvus – pasyvus režimu).

4. PREKIŲ PRISTATYMO VIETA, TERMINAI IR TVARKA

4.1. Prekių pristatymo vieta – Savanorių pr. 212, Vilniaus m. Prekės pristatomos Pirkėjo darbo laiku (I-V 7:30 – 16:00 val.).

4.2. Prekių tiekimo terminas – ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo Sutarties abipusių šalių pasirašymo. Prekių pristatymo terminas iškilus nenumatytoms aplinkybėms ir (ar) esant objektyvioms priežastims ir Sutarties šalims raštu (el. paštu) suderinus, gali būti pratęstas, bet ne ilgiau kaip **15 k. d.**

5. PREKIŲ KOKYBĖ IR TRŪKUMŲ ŠALINIMAS

5.1. Pardavėjas privalo garantuoti, kad pateiktos Prekės yra naujos, nenaudotos ir be defektų. Nekokybiškos ar Techninės specifikacijos neatitinkančios Prekės turi būti pakeistos nuo Pirkėjo rašytinio reikalavimo dėl trūkumų šalinimo pateikimo dienos ne vėliau kaip per 15 k. d.

6. SUTARTIES VYKDYMO METU PATEIKIAMA DOKUMENTACIJA

6.1. Kartu su pristatomomis Prekėmis pateikiama:

6.1.1. krovinio pristatymo Važtaraštis su nurodytais Prekių kiekiais;

6.1.2. garantiją patvirtinantys dokumentai.

7. PIRKĖJO IR PARDAVĖJO ĮSIPAREIGOJIMAI

7.1. Pirkėjo įsipareigojimai:

7.1.1. Bendradarbiauti su Pardavėju, teikiant reikalingą informaciją Sutarties vykdymo metu.

7.1.2. Priimti iš Pardavėjo jo pristatytas kokybiškas Prekes, atitinkančias Sutartyje numatytus reikalavimus, ir tinkamai bei laiku atsiskaityti su Pardavėju Sutartyje numatytomis sąlygomis.

7.1.3. Pastebėjęs trūkumus, Pirkėjas turi teisę nepriimti Prekių ir nepasirašyti Važtaraščio ir (ar) Akto.

7.2. Pardavėjo įsipareigojimai:

7.2.1. Pristatyti kokybiškas Prekes laiku, Sutartyje nustatyta tvarka, Lietuvos Respublikoje galiojančiais įstatymais ir kitais teisės aktais reglamentuojančiais Prekių tiekimą.

7.2.2. Pardavėjas, tiekdamas Prekes, privalo vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams valdantiems ypatingos svarbos informacinę infrastruktūrą, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (galiojančiomis aktualiomis redakcijomis).