

ATSAKYMAI Į RINKOS DALYVIŲ KLAUSIMUS

1

Eil. Nr.	Klausimas	Atsakymas	Perkančiosios organizacijos atsakymas
3.	Kokius reikalavimus papildomai siūlytumėte įtraukti į Techninę specifikaciją arba kurių reikėtų atsisakyti?	<p>Siūlome įsitraukti tokius reikalavimus:</p> <p>Duomenų centrui:</p> <p>1.1. Duomenų centro valdymas ir priežiūra turi atitikti ISO 27001:2013 arba lygiavėrio standarto reikalavimus (lygiavėriu standartu laikomas toks standartas, kurio reikalavimai visiškai atitinka arba viršija ISO 27001:2013 standarto reikalavimus).</p> <p>Sertifikatas užtikrina, kad paslaugas teikianti įmonė geba apsaugoti konfidencialią informaciją, sumažinti informacinių incidentų riziką, atitikti teisinius reikalavimus.</p> <p>1.2. Duomenų centro Tiekėjo informacinių technologijų paslaugų valdymo sistema turi atitikti ISO 20000 ar lygiavėrio standarto reikalavimus (lygiavėriu standartu laikomas toks standartas, kurio reikalavimai visiškai atitinka arba viršija ISO 20000 standarto reikalavimus).</p> <p>Sertifikatas užtikrina, kad paslaugas teikianti įmonė geba užtikrinti, kad paslaugos būtų kokybiškos ir patikimos, pagerinti IT veiklos efektyvumą.</p> <p>1.3 Duomenų centras neturi būti įrengtas požeminiame ar paskutiniame pastato aukšte. Jei duomenų centras įrengtas ne pagal nurodytą reikalavimą, tai Tiekėjas kartu su pasiūlymu turi pateikti nepriklausomos kompetentingos institucijos išduotą dokumentą, įrodantį, kad duomenų</p>	<p>Kadangi nesame įsidiegę šių standartų, į pasiūlymus 1.1 ir 1.2 neatsižvelgsime.</p> <p>Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje</p>

		<p>centras yra apsaugotas nuo vandens poveikio (užliejimo) įvykus stichinėms nelaimėms arba avarijoms šalia esančiuose inžineriniuose tinkluose.</p> <p>Reikalavimas sumažina fizinės grėsmės riziką ir garantuoja, kad bus išvengta paslaugų sutrikimų dėl aplinkos veiksnių.</p> <p>1.4. Tarnybinių stočių laikymo patalpoje turi būti įrengta tikslaus klimato kontrolės sistema, palaikanti pastovią temperatūrą 20-23 °C ir drėgnumą 40-60% ribose.</p> <p>Reikalavimas yra kritiškai svarbus IT infrastruktūros patikimumui ir yra tiesiogiai susijęs su tarnybinių stočių ilgaamžiškumu, stabilumu ir saugumu. Tai svarbu, nes tiekėjas užtikrina, kad tiekėjo įranga veiks patikimai visą sutarties laikotarpį, bus išvengta paslaugų sutrikimų dėl aplinkos veiksnių.</p> <p>2. Resursų nuomos paslaugai:</p> <p>2.1. Paslaugos pasiekiamumas - Ne blogiau kaip XX % per mėnesį.</p> <p>Šis reikalavimas užtikrina nepertraukiamą paslaugų veikimą, garantuoja paslaugos patikimumą ir nuolatinį pasiekiamumą.</p> <p>2.2. Našumo ir pajėgumo parametrai - Ne mažiau nei 5 (penkios) fizinės tarnybinės stotys, skirtos tarnybinių stočių virtualizavimo platformai. Jos turi būti apjungtos į aukšto patikimumo blokinį (angl. cluster).</p> <p>Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, procesorių našumas ne mažiau negu:</p> <p>SPEC2017_int_rate_base, skaičiuojant per CPU branduolį (SPEC2017_int_rate_base / # of Cores) ne mažiau 9,5;</p>	<p>Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje</p> <p>Į 2. ir 3. pasiūlymus atsižvelgsime ir papildysime techninėje specifikacijoje.</p>
--	--	---	--

	<p>SPEC2017_fp_rate_base, skaičiuojant per CPU branduolį (SPEC2017_fp_rate_base / # of Cores) ne mažiau 11,0.</p> <p>Pastaba: Našumo rezultatai turi būti išmatuoti su siūlomu procesoriumi bet kurioje aparatinėje platformoje. Našumo testų rezultatai turi būti viešai publikuoti www.spec.org puslapyje. Siūlomi procesoriai turi turėti ne mažiau nei 16 fizinių branduolių.</p> <p>Pasiūlyme būtina nurodyti fizinių tarnybinių stočių, kurios bus skiriamos tarnybinių stočių virtualizavimo platformai, procesorių skaičių, gamintoją ir modelį, dažnį, veikiančių branduolių skaičių, spartinančiosios atminties dydį, sisteminės magistralės dažnį.</p> <p>Suminis fizinių tarnybinių stočių operatyvinės atminties kiekis (RAM) ne mažesnis nei 2048 GB;</p> <p>Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, resursų (CPU ir RAM) panaudojimas neturi viršyti 70 %.</p> <p>Reikalavimas svarbus, nes užtikrina klientui reikiamą veikimo greitį, apsaugo nuo nekokybiškos įrangos, užtikrina SLA (paslaugų kokybės) reikalavimą.</p> <p>2.3. Duomenų centro saugumas - Duomenų centro infrastruktūra turi būti stebima su specializuota programine įranga informacinių sistemų žurnalinių įrašų saugojimo ir koreliacijos (angl. SIEM - Security Information and Event Management) funkcijoms atlikti. Pasiūlyme</p>	
--	---	--

		<p>nurodyti naudojamos programinės įrangos gamintoją, versiją ir pavadinimą.</p> <p>Programinė įranga turi rinkti žurnalinius įrašus (angl. logs) iš tinklo įrangos (maršrutizatorių, komutatorių, bevielių prieigos taškų), tinklo saugos įrenginių bei sistemų (ugniasienių, web aplikacijų ugniasienių, IPS/IDS, DHCP, DNS, Active Directory ir kt.), operacinių sistemų, duomenų bazių valdymo sistemų bei taikomosios programinės įrangos;</p> <p>Programinė įranga turi periodiškai atnaujinti ir įdiegti gamintojo pateikiamą saugumo grėsmių informaciją, pažeidžiamumų sąrašus, identifikuojančius komunikaciją su įtartinais ir kenksmingais šaltiniais (IP adresais) internete, kenksmingo kodo maišos sumas, žinomus blogus domenus ir kt.</p> <p>Programinė įranga privalo turėti įdiegtą naudotojų elgesio analizės (angl. User Behavior Analytics) komponentą, galintį: Analizuoti standartinę naudotojų veiklą ir aplikti joje anomalijas;</p> <p>Aptikti pavogtas, kompromituotas naudotojų paskyras;</p> <p>Integruotis ir perduoti informaciją į kitus sistemos saugumo komponentus, pavyzdžiui, koreliacijos variklį;</p> <p>Identifikuoti pasikeitimus naudotojų elgsenoje;</p> <p>Stebėti privilegijuotų naudotojų veiksmus;</p> <p>Gebėti naudoti grėsmių informaciją naudotojų stebėjime;</p> <p>Naudotojai turi turėti grėsmės įverčius, kurie kinta laike ir gali būti naudojami incidentams generuoti;</p>	
--	--	---	--

		<p>Tiekėjas privalo atlikti informavimą apie saugumo incidentus (incidentas apibūdinamas, kaip iš anksto nustatyta saugumo politikos pažeidimas arba saugumo įvykis, saugumo analitiko kvalifikuotą kaip teisingai-teigiamą (angl. true-positive)).</p> <p>Nustatęs teigiamą saugumo incidentą, tiekėjas turi pateikti: Incidento pirminių priežasčių (angl. root cause) nustatymas. Incidento atakos grandinės nustatymas. Incidento tyrimas, jo eigos atkūrimas. SIEM esančių incidento įrodymų surinkimas ir išsaugojimas. Saugos ir saugos valdymo procesų gerinimo rekomendacijų pateikimas, suvaldžius incidentą</p> <p>Reikalavimas yra tiesiogiai susijęs su kibernetiniu saugumu, incidentų prevencija ir atitikimu teisės aktams. Jis įrodo, kad tiekėjas apsaugo savo klientus nuo kibernetinių atakų grėsmių</p> <p>3. Virtualių tarnybinių stočių kopijavimo ir atstatymo paslaugos teikimui: Siūlome nusimatyti kokybės reikalavimus. Kokybės reikalavimai atsarginių kopijų darymui pirkime apsaugos nuo žemos kokybės paslaugos.</p>	
4.	Ar techninėje specifikacijoje nurodyti planuojamų įsigyti paslaugų techniniai aprašymai gali riboti kitų tiekėjų galimybes dalyvauti pirkime?	Neribojama	
5.	Ar vykdydami Techninėje specifikacijoje nurodytas paslaugas turėsite galimybę juos vykdyti laikantis aplinkos apsaugos vadybos	Taip	

	standartų reikalavimų ir pirkime pateikti tai įrodančius dokumentus?		
6.	Kokius kontrolės mechanizmus siūlote nustatyti viešojo pirkimo sutartyje atliekamų paslaugų kontrolei vykdyti?	Prašyti tiekėjo pateikti ataskaitas už ataskaitinį laikotarpį	Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje
7.	Prašome nurodyti preliminarią Techninėje specifikacijoje nurodytų paslaugų kainą EUR be PVM.	4000 Eur/mėn be PVM.	
8.	Prašome įvardyti kitą, Jūsų nuomone, reikšmingą informaciją tinkamam šių paslaugų įsigijimui.	<p>Siūlome įsitraukti kvalifikacinius reikalavimus, tokius kaip:</p> <p>1.1 Tiekėjas per paskutinius tris metus (arba per laikotarpį nuo Tiekėjo įregistravimo dienos, jeigu Tiekėjas vykdė veiklą trumpiau nei tris metus) turi būti pasirašęs ir įvykęs arba vykdo ne mažiau kaip vieną sutartį, kurios objektas informacinių sistemų resursų nuomos paslaugos, kurios vertė ne mažesnė kaip X 000 Eur (xxx) be PVM.</p> <p>Kvalifikaciją įrodantys dokumentai:</p> <p>Tiekėjo įvykdytų panašių sutarčių, susijusių su nurodytomis paslaugomis, sąrašas per paskutinius tris metus arba per laiką nuo tiekėjo įregistravimo dienos, jeigu tiekėjas vykdė veiklą mažiau nei 3 metus, nurodant paslaugų sumas, datas ir gavėju (5 priedas). Pateikiamos paslaugų gavėjų pažymos (skaitmeninės kopijos), įrodančios tinkamą paslaugų suteikimą.</p> <p><i>Pateikiamas dokumentas elektroninėje formoje*</i>. Tiekėjo įvykdytų panašių sutarčių, susijusių su nurodytomis paslaugomis, sąrašas per paskutinius tris metus arba per laiką nuo tiekėjo įregistravimo dienos, jeigu tiekėjas vykdė veiklą mažiau nei 3 metus, nurodant paslaugų sumas, datas ir gavėju (5 priedas). Pateikiamos paslaugų gavėjų</p>	Į pasiūlymą atsižvelgsime ir papildysime kvalifikaciniuose reikalavimuose

		<p>pažymos (skaitmeninės kopijos), įrodančios tinkamą paslaugų suteikimą. <i>Pateikiamas dokumentas elektroninėje formoje*</i>. Kvalifikacinis reikalavimas įrodo tiekėjo patirtį ir gebėjimą teikti pirkime numatytas paslaugas.</p> <p>1.2. Tiekėjas turi būti įdiegęs aplinkos apsaugos vadybos sistemą. Kvalifikaciją įrodantys dokumentai: ISO 14001 sertifikatas arba atitinkamo lygiavertis sertifikatas, išduotas įstaigų, atitinkančių ES teisės aktus ar atitinkamus. Europos arba tarptautinius sertifikavimo standartus, arba lygiaverčiai įrodymai. Sertifikatas užtikrina, kad paslaugas teikianti įmonė valdo neigiamą poveikį aplinkai, laikosi teisinių ir kitų su aplinkosauga susijusių reikalavimų</p> <p>1.3. Tiekėjas turi turėti įdiegęs IT paslaugų valdymo sistemą Kvalifikaciją įrodantys dokumentai: ISO 20000 sertifikatas arba kitas lygiavertis sertifikatas, išduotas įstaigų, atitinkančių ES teisės aktus ar atitinkamus Europos arba tarptautinius sertifikavimo standartus, arba lygiaverčiai įrodymai Sertifikatas užtikrina, kad paslaugas teikianti įmonė geba užtikrinti, kad paslaugos būtų kokybiškos ir patikimos, pagerinti IT veiklos efektyvumą.</p> <p>1.4. Tiekėjas turi būti įdiegęs informacijos saugumo valdymo sistemą. Kvalifikaciją įrodantys dokumentai: ISO 27001 sertifikatas arba kitas lygiavertis sertifikatas, išduotas įstaigų, atitinkančių ES teisės aktus ar atitinkamus Europos</p>	<p>Kadangi nesame įsidiegę šių standartų, į pasiūlymus 1.2, 1.3, 1.4 neatsižvelgsime.</p>
--	--	---	---

		<p>arba tarptautinius sertifikavimo standartus, arba lygiaverčiai įrodymai. Sertifikatas užtikrina, kad paslaugas teikianti įmonė geba apsaugoti konfidencialią informaciją, sumažinti informacinių incidentų riziką, atitikti teisinius reikalavimus.</p> <p>1.5. Kiekvienas specialistas turi gebėti gerai rašyti, skaityti, suprasti lietuvių kalbą (C1 lygis pagal „Europass“ kalbų pasą). Žemiau nurodyti reikalaujami specialistai ir reikalavimai jų kvalifikacijai:</p> <p>1.5.1. Ne mažiau kaip vienas duomenų centro valdymo specialistas: Turi turėti duomenų centro valdymo kvalifikaciją, patvirtintą Certified Data Centre Management Professional (CDCMP) arba lygiaverčiu sertifikatu</p> <p>1.5.2. Ne mažiau kaip vienas debesų kompiuterijos specialistas Turi turėti debesų kompiuterijos kvalifikaciją, patvirtintą CompTIA Cloud+, arba lygiaverčiu sertifikatu</p> <p>1.5.3. Ne mažiau kaip vienas kibernetinio saugumo specialistas: Turi turėti kibernetinio saugumo kvalifikaciją, patvirtintą CompTIA Advanced Security Practitioner (CASP+), arba lygiaverčiu sertifikatu</p> <p>1.5.4. Ne mažiau kaip vienas kibernetinių saugumo rizikų specialistas Turi turėti kibernetinių saugumo rizikų, patvirtintą pateiktas ISACA Certified in Risk and Information Systems Control, arba lygiaverčiu sertifikatu</p> <p>1.5.5. Ne mažiau kaip vienas IT paslaugų architektas</p>	<p>Į 1.5 pasiūlymą atsižvelgsime ir papildysime kvalifikaciniuose reikalavimuose</p>
--	--	--	--

		<p>Turi turėti IT paslaugų architekto kvalifikaciją, patvirtintą Togaf 9 arba lygiaverčiu sertifikatu</p> <p>Kvalifikaciją įrodantys dokumentai: Teikėjo specialistų sąrašas, kuriame turi būti nurodytas specialisto vardas, pavardė. Specialistų gyvenimo aprašymai (CV), nurodant išsilavinimą, darbo patirtį informacinių technologijų srityje. Specialistų kvalifikaciją patvirtinančių sertifikatų arba lygiaverčių dokumentų tinkamai patvirtintos kopijos (mokymo kursų išklausymo pažymėjimai nebus vertinami).</p> <p>Kiekvieno specialisto, kuris nėra Teikėjo darbuotojas, patvirtinimas raštu, kad jis dalyvaus vykdant Paslaugų teikimo sutartį. Pateikiamos skaitmeninės dokumentų kopijos*.</p> <p>Šis reikalavimas įrodo, kad paslaugas teikiantys specialistai yra kompetentingi, paslaugas teikiančių specialistų patirtį ir užtikrina, kad įmonė geba teikti numatytas paslaugas.</p>	
--	--	---	--

2

Eil. Nr.	Klausimas	Atsakymas	Perkančiosios organizacijos atsakymas
1.	Ar turite pastabų, klausimų techninei informacijai? Ar Pirkimo techninė specifikacija pakankamai išsami, konkreti ir aiški, ar joje yra visa informacija, reikalinga tinkamam pasiūlymo parengimui? Prašome pateikti argumentuotas pastabas/klausimus.	Pirkimo techninė specifikacija pakankamai išsami, konkreti ir aiški, ir joje yra visa informacija, reikalinga tinkamam pasiūlymo parengimui.	

2. -	Ar techninėje specifikacijoje, tiekėjų manymu, yra reikalavimų, kurie yra sunkiai įgyvendinami?	Techninėje specifikacijoje nėra reikalavimų, kurie yra sunkiai įgyvendinami.	
5	Ar vykdydami Techninėje specifikacijoje nurodytas paslaugas turėsite galimybę juos vykdyti laikantis aplinkos apsaugos vadybos standartų reikalavimų ir pirkime pateikti tai įrodančius dokumentus?	Taip, turėsime galimybę juos vykdyti laikantis aplinkos apsaugos vadybos standartų reikalavimų ir pirkime pateikti tai įrodančius dokumentus.	
7	Prašome nurodyti preliminarią Techninėje specifikacijoje nurodytų paslaugų kainą EUR be PVM.	7075.15 Eur be PVM	

3

Eil. Nr.	Klausimas	Atsakymas	Perkančiosios organizacijos atsakymas
1.	Ar turite pastabų, klausimų techninei informacijai? Ar Pirkimo techninė specifikacija pakankamai išsami, konkreti ir aiški, ar joje yra visa informacija, reikalinga tinkamam pasiūlymo parengimui? Prašome pateikti argumentuotas pastabas/klausimus.	TS 3.1. p. šeštoje eilutėje nedetalizuojate, kas apima informacinių sistemų konsultacijas	Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje
2.	Ar techninėje specifikacijoje, tiekėjų manymu, yra reikalavimų, kurie yra sunkiai įgyvendinami?	6.1. Šiame punkte nurodomas dešimties dienų terminas, riboja konkurenciją ir sudaro išskirtines sąlygas esamam tiekėjui. Rekomenduojame terminą ilginti iki dvidešimties dienų.	Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje
3.	Kokius reikalavimus papildomai siūlytumėte įtraukti į Techninę specifikaciją arba kurių reikėtų atsisakyti?	l. 40 p. siūlome išdėstyti taip: „Virtualių tarnybinių stočių duomenų atsarginės kopijos privalo būti laikomos ne mažiau kaip 10 km nutolusiame duomenų centre, nei yra fizinės tarnybinės stotys, kurių pagalba teikiamos aukščiau aprašytos paslaugos. „ didinti atstumą iki 10 km, taip užtikrinant,	Į pasiūlymą neatsižvelgsime, manome, kad tai riboja konkurenciją.

		<p>Turi būti galimybė pasinaudojant savitarnos portalu prisijungti prie virtualaus serverio, nenaudojant papildomų programinių įrankių. Virtualus serveris turi būti pasiekiamas ir tuo atveju, kai jai nėra prijungtas ar suteiktas virtualus tinklo adapteris ar IP adresas.</p> <ul style="list-style-type: none"> • Savitarnos portalo saugumas turi būti užtikrinantis naudojant dviejų veiksmų autentifikavimo metodu. • Turi būti suteikta galimybė valdyti atsarginių kopijų kūrimo tvarkaraščius pagal Pirkėjo poreikius, daryti kopijas virtualios aplikacijos (vApp) ir virtualaus serverio lygmeniu. • Turi būti suteikta galimybė atsargines kopijas atstatyti be paslaugų tiekėjo įsikišimo. • Turi būti užtikrinta galimybė be paslaugų tiekėjo įsikišimo kurti ir valdyti tinklą virtualaus duomenų centro (VDC) lygmenyje, kurti VPN, IPsec, valdyti tinklo ugniasienės taisykles per savitarnos portalą. • Leidžia naudotis VMware Marketplace arba lygiavertės aplinkos funkcionalumais IV. Paslaugų tiekėjas, teikdamas paslaugą, turi suteikti Pirkėjui galimybę savitarnos portale realiu laiku stebėti: <ul style="list-style-type: none"> -Virtulių serverių, virtualių aplikacijų (vApp), organizacijų ir Virtualaus duomenų centro (VDC) veikimą. -CPU, RAM, disko, tinklo srauto ir kt. utilizaciją. -Automatizuota įvykių ir problemų analizė. -Anomalijas, našumo degradavimą ir šuolius. <p>Stebėjimo duomenys turi būti saugomi 90 kalendorinių dienų.</p>	<p>Į pasiūlymą atsižvelgsime ir papildysime techninėje specifikacijoje</p>
--	--	---	--

		<p>Turi turėti galimybę Virtualaus duomenų centro (VDC) veiklos optimizavimui:</p> <ul style="list-style-type: none"> -Automatinės virtualių serverių naudojamų resursų optimizacijos rekomendacijos. -Automatinės resursų perskirstymo tarp virtualių serverių rekomendacijos (angl. rightsizing). -Automatinis nenaudojamų virtualių mašinų aptikimas (angl. ghost VM). -Automatinis resursų naudojimo ateities prognozės. <p>V. Siūlome nusimatyti saugumo sprendimą (vUTM) dėl saugaus prisijungimo prie nutolusių serverių, kad būtų užtikrintas saugus ir nepertraukiamas duomenų pasiekiamumas (Pvz. Dingus elektros energijos arba ryšio tiekimui jūsų padaliniuose). Rekomenduojamo sprendimo detalizacija pridedame atskiru failu.</p>	<p>Į pasiūlymą neatsižvelgsime, manome, kad tai perteklinis reikalavimas</p>
4.	Ar techninėje specifikacijoje nurodyti planuojamų įsigyti paslaugų techniniai aprašymai gali riboti kitų tiekėjų galimybes dalyvauti pirkime?	Nėra	
5.	Ar vykdydami Techninėje specifikacijoje nurodytas paslaugas turėsite galimybę juos vykdyti laikantis aplinkos apsaugos vadybos standartų reikalavimų ir pirkime pateikti tai įrodančius dokumentus?	Taip	
6.	Kokius kontrolės mechanizmus siūlote nustatyti viešojo pirkimo sutartyje atliekamų paslaugų kontrolei vykdyti?	Kontrolės mechanizmui siūlome nustatyti paslaugų pateikiamumą (angl. Availability) ne mažiau kaip 99,95 proc.	Į pasiūlymą atsižvelgsime ir pildysime techninėje specifikacijoje
7.	Prašome nurodyti preliminarią Techninėje specifikacijoje nurodytų paslaugų kainą EUR be PVM.	4800 EUR/mėn. be PVM	

Parametro pavadinimas	Reikalaujama parametro reikšmė	Perkančiosios organizacijos atsakymas
Paslaugos paskirtis	Apsaugoti interneto ryšio tinklą nuo interneto grėsmių, užtikrinti saugų duomenų perdavimo ryšį su kitais padaliniais. Suteikti galimybę prie įstaigos tinklo jungtis nuotoliniu būdu: keliaujantys ar namuose dirbantys įstaigos darbuotojai turi turėti galimybę saugiai ir patogiai jungtis prie įstaigos tinklo.	Į šiuos pasiūlymus neatsižvelgsime, nes šie reikalavimai pertekliniai šiam pirkimo objektui
Paslaugos tipas	<p>Paslauga turi būti teikiama naudojant specializuotus aparatinius-programinius įrenginius, su UTP saugumo paketu, skirtus užtikrinti perimetro kontrolę, VPN, įsibrovimų aptikimą ir prevenciją (įsibrovimų, pažeidžiamumų ir pan. aptikimas bei apsauga), srautų turinio kontrolę (apsauga nuo virusų, piktybinių kodų.). Siūloma paslauga turi naudoti programinį/aparatinį (angl. <i>appliance</i>) sprendimą, kurio visos sudedamosios dalys (priedai, procesoriai, atmintis, t. t.) yra sukomplektuoti fiziniuose įrenginiuose. Visa įrenginyje instaliuota programinė įranga yra specializuota programinė įranga numatytoms funkcijoms atlikti, užtikrinanti įrenginio veikimo patikimumą bei saugumą.</p> <p>Siūloma paslauga negali būti realizuota naudojant kompiuterinės debesijos virtualizacijos platformomis paremtais sprendimais.</p> <p>Kartu su pasiūlymu būtina pateikti naudojamos įrangos aprašymą, kuriame turi būti nurodyta - gamintojas, įrangos modeliai.</p>	
Aukšto patikimumo realizavimas	Aukštam patikimumui (angl. HA – <i>high availability</i>) realizuoti Paslaugos teikimui turi būti naudojama ne mažiau, kaip 2 vnt. ugniasienės fizinės įrangos.	
Virtualių ugniasienių palaikymas	Paslaugai naudojama įranga turi palaikyti virtualių ugniasienių funkcionalumą, kuomet fiziniai įrenginiai gali būti išskaidyti į kelias virtualias ugniasienes su atskiromis	

	<p>maršrutizavimo lentelėmis, ugniasienės taisyklėmis ir saugumo profiliais. Reikalingos licencijos pateikiamos kartu su įrenginiu. Perkančioji organizacija gali naudotis virtualia ugniasiene, kuri atitinka šioje specifikacijoje išvardintus techninius-kokybinius parametrus.</p>	
<p>Virtualių ugniasienių funkcionalumas</p>	<p>Kiekviena virtuali ugniasienė turi palaikyti tokį pat funkcionalumą kaip ir fizinė ugniasienė įskaitant, bet neapsiribojant:</p> <ul style="list-style-type: none"> • Ugniasienės funkcionalumas IPS/IDS; • Antivirusinė patikra; • Aplikacijų atpažinimas; • Srauto prioretizavimas (angl. QoS). Garantuoto srauto pralaidumo nustatymas aplikacijoms; • Adresų transliavimas įskaitant NAT64 ir NAT46; • Turi veikti kaip DHCP klientas; • Turi veikti kaip DHCP serveris; • VRRP protokolas; • URL filtravimas pagal kategorijas; • HTTPS dešifravimas ir patikra; • VPN IPsec. 	