KONKURSO DOKUMENTŲ
1 priedas
forma

PASIŪLYMAS KONKURSUI
SAUGOS KOMPIUTERINĖS ĮRANGOS VIEŠASIS PIRKIMAS
2024-07-12
(Data)
Vilnius
(Vieta)

Tiekėjo pavadinimas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai*/	UAB NBCS
Tiekėjo kodas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių kodai*/	301817848
Tiekėjo adresas /*Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai*/	Šeškinės Sodų g. 12-54, Vilnius
Telefono numeris	+370 5 2764563
El. pašto adresas	info@nbcs.lt
Bankas	Luminor Bank AS Lietuvos skyrius
Sąskaitos numeris	LT332140030003850923

Pastaba. Pildoma, jei Tiekėjas ketina pasitelkti, subtiekėją (-us) ir/ar specialistus ir ekspertus, kuriais bus remiamasi įrodinėjant Tiekėjo kvalifikaciją ir vykdant pirkimo sutartį, tačiau pasiūlymo pateikimo metu jie nėra Tiekėjo ar jo pasitelkiamo (ų) subtiekėjo(ų) darbuotojai, tačiau laimėjimo atveju bus įdarbinti.

Subtiekėjo (-ų) pavadinimas (-ai)	
Subtiekėjo (-ų) kodas (-ai)	
Subtiekėjo (-ų) adresas (-ai)	
Specialistai ir ekspertai, kuriais bus remiamasi įrodinėjant Tiekėjo kvalifikaciją ir vykdant pirkimo sutartį, tačiau jie nėra Tiekėjo ar Tiekėjo pasitelkiamo (ų) subtiekėjo (-ų) darbuotojai pasiūlymo pateikimo metu, bet laimėjimo atveju būtų įdarbinti	
Įsipareigojimų dalis (nurodant konkrečius pagal pirkimo sutartį prisiimamus įsipareigojimus), kuriai ketinama pasitelkti subtiekėją (-us)	

Bus remiamasi šių ūkio subjektų pajėgumais:

Eil. Nr.	Nurodomas ūkio subjekto pavadinimas ir kokiems reikalavimams pagrįsti remiamasi jų pajėgumais

Pastaba. Pildoma tuomet, jei bus remiamasi kitų ūkio subjektų pajėgumais.

Šiuo PASIŪLYMU Konkursui pažymime, kad sutinkame su visomis Konkurso sąlygomis, nustatytomis Konkurso dokumentuose.

Pareiškiame, kad esame suinteresuoti dalyvauti Konkurse ir sudaryti pirkimo sutartį pagal Konkurso dokumentuose nustatytus reikalavimus.

Pareiškiame, kad pasiūlymas yra parengtas nepasinaudojant ryšiais, informacija, sulygintais duomenimis arba susitarimu su kitais ūkiniais subjektais arba asmenimis.

Pastaba!

Pildomos tos Konkurso objekto dalies lentelės, atitinkamai, kuriai KONKURSO objekto daliai TIEKĖJAS teikia pasiūlymą.

Pranešame, kad rūpestingai išnagrinėję KONKURSO DOKUMENTUS, esame pasirengę atlikti Prekių teikimą **KONKURSO objekto 1 dalyje** pagal KONKURSO DOKUMENTŲ reikalavimus ir nurodome savo pasiūlymo kainą:

1 lentelė

	Pasiūlymo kaina **skaičiais**	Pasiūlymo kaina **žodžiais**
Pasiūlymo kaina **be PVM**		
Pasiūlymo kaina **su PVM**		

Detalizuojame pasiūlymo kainą KONKURSO objekto 1 dalyje – Kompiuterių tinklo apkrovos balansavimo įrenginiai su aplikacijų ugniasienės funkcija (WAF)**:**

Detalizuojame Konkurso pasiūlymo kainą:

2 lentelė.

Eil. Nr.	**Pavadinimas**	**Gamintojo PREKĖS pavadinimas, PREKĖS kodas**	**Kiekis, vnt. (a)**	**Vieneto kaina, EUR be PVM (b)**	**Suma, EUR be PVM (c=a*b)**
1.	Kompiuterių tinklo apkrovos balansavimo įrenginiai su aplikacijų ugniasienės funkcija (WAF).		2		
				Suma iš viso be PVM:	
				PVM suma:	
				Suma iš viso (EUR su PVM):	

Įranga bus diegiama ir instaliuojama adresais: Vasario 16-osios g. 14, Vilnius ir Europos pr. 105, Kaunas.

Tiekėjo siūlomų įrenginių parametro reikšmės (Tiekėjas pildo lentelės stulpelį: „Siūlomos parametrų reikšmės“):

3 lentelė.

Eil. Nr.	**Pavadinimas**	**Reikalavimai**	**Siūlomi parametrai**
1.	Gamintojas	Nurodyti.	
2.	Pavadinimas	Nurodyti tikslų siūlomo sprendimo pavadinimą.	
3.	Sprendimo tipas	Specializuotas aparatinis-programinis sprendimas, skirtas užtikrinti apkrovos balansavimą, interneto tinklapių saugumą, vartotojų prieigos prie aplikacijų valdymą. Įrenginys turi būti montuojamas į 19 colių komutacinę spintą. Montavimui reikalingos detalės turi būti pateiktos kartu su įranga.	
4.	Elektros maitinimas	Elektros maitinimas – kintamos srovės, 220V įtampos, naudojant dubliuotus maitinimo šaltinius.	
5.	Tinklo sąsajų tipas ir kiekis	Ne mažiau kaip 4 vnt. 10/100/1000 Base-T Ethernet prievadai. Ne mažiau kaip 2 vnt. 10G/25G SFP+/SFP28 optiniai prievadai. Atskiras 1000Base-T valdymo prievadas. USB ir *serial* prievadai valdymui.	
6.	Patikimumas	Įrenginiai turi palaikyti aukšto patikimumo funkcionalumą:	

		• Aukšto patikimumo sistema turi dirbti Aktyvus/Pasyvus (*angl. Active/Passive*) ir Aktyvus/Aktyvus (*angl. Active/Active*) režimais. • Sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį, užmegztos sesijos turi nenutrūkti.	
7.	Pralaidumas	Kiekvienas įrenginys turi užtikrinti ne mažesnį našumą: • Ne mažesnis negu 40 Gbps. Ne mažesnis negu 20 Gbps fiziškai dekriptuojant srautą. • Ne mažiau 1 300 000 L7 užklausių per sekundę. • Ne mažiau 500 000 L4 užklausų per sekundę. • Ne mažiau 2 500 000 L4 HTTP užklausų per sekundę. • Ne mažiau 38 000 000 konkurentinių L4 sesijų. • Ne mažiau 30 000 SSL kriptoraktų operacijų per sekundę naudojant 2Kb raktus. • Ne mažiau 14 000 kriptoraktų operacijų per sekundę naudojant ECDSA P256 arba RSA algoritmą su 2Kb raktais. Galimybė praplėsti įrenginio našumą su papildoma licencija: • Ne mažesnis negu 50 Gbps srauto apdorojimo našumas. Ne mažesnis negu 25 Gbps fiziškai dekriptuojant srautą. • Ne mažiau 1 800 000 L7 užklausių per sekundę. • Ne mažiau 750 000 L4 užklausų per sekundę. • Ne mažiau 3 500 000 L4 HTTP užklausų per sekundę. • Ne mažiau 45 000 SSL kriptoraktų operacijų per sekundę naudojant 2Kb raktus. • Ne mažiau 20 000 kriptoraktų operacijų per sekundę naudojant ECDSA P256 arba RSA algoritmą su 2Kb raktais.	
8.	Bendrosios funkcijos	• HTTP 1.0 / 1.1 / 2.0, HTTPS, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, FTP, SMTP protokolų palaikymas. • TLS SNI (Server Name Indication) palaikymas. • HSTS palaikymas. • SHA, SHA256, SHA384, SHA512 palaikymas.	
9.	Sprendimo funkcionalumas	Ugniasienės turi turėti licencijas šiam funkcionalumui: • Apkrovos balansavimo, aplikacijų stebėjimo, L7 srauto valdymo, protokolų optimizavimo. • WEB aplikacijų ugniasienės, apsaugos nuo nuo DDoS, XML ugniasienės. • Šifravimo funkcionalumas.	

		• Programavimo. • Prieigos valdymo, SSL proxy.	
10.	Apkrovos balansavimo funkcijos	• Aplikacijų srauto (HTTP, HTTP2, SSL, TLS) balansavimas. • Galimybė balansuoti srautą pagal serverių apkrovimą, aplikacijų veikimo patikros rezultatus aprašant kreipinius į aplikacijas. • Galimybė WEB aplikacijų SSL/TLS sesijas terminuoti įrenginyje, dekriptavimo apkrovą perkeliant sprendimui, arba kriptuoti srautą tarp sprendimo ir WEB serverių privačiais raktais. • Aplikacijų veikimo bei apkrovos stebėjimas, bei istorinių ataskaitų generavimo galimybė. • Galimybė saugoti dažnai prieinamą turinį įrenginio operatyvioje atmintyje, optimizuojant aplikacijos greitaveiką („cache“). • Galimybė aplikacijų telemetrinius duomenis perduoti į išorinius sprendimus analizei. • Integracija su Puppet, Chef, Terraform, Ansible automatizavimui.	
11.	WEB aplikacijų ugniasienės funkcijos	Ugniasienė turi apsaugoti nuo šių atakų tipų: • Protokolų anomalijų aptikimas (SYN, ICMP, ACK, UDP, TCP). • Apsaugą nuo taikomosios programinės įrangos lygio, L4, SSL, DNS DoS atakų. Įskaitant *Flood, Sweep* atakas. Srauto pavyzdžių įrašymas DOS atakos metu. DoS atakų, įskaitant L7 DoS atakas, „HASH DoS“, „Slowloris“, „floods“, „Keep-Dead“, „XML bomb“ atakas. • Galimybė blokuoti DoS atakas, analizuojant ir vertinant srauto anomalijas. • Apsauga nuo slaptažodžių spėliojimo („Brute force“) atakų. • Turinio nuskaitymo („Web scraping“) atakų. • OWASP TOP 10 atakų tipų. • Turinio injekcijų *(WEB injection)* atakų, sesijų perėmimo (*session hijacking*), HTTP parametrų manipuliavimo *HPP* atakų, buferio perpildymo (*buffer overflow*) ir *shellshock* tipo atakų. • Srauto blokavimas pagal GEO lokacijas. • Prisijungimo duomenų bandymo („Credential stuffing“) atakų. • BOT tinklų naudojimo atakoms identifikavimas ir susijusio srauto blokavimas. • WEBsocket srauto filtravimas. • Turi užmaskuoti bandymus nustatyti naudojamas operacines sistemas. • FTP komandų ilgių kontrolė, leistinų FTP komandų kontrolė, FTP apsauga nuo brutalių atakų (*angl. Brute force*). • Nepageidaujamų SMTP komandų blokavimas, DNS SPF įrašų tikrinimas,	

		Leistino laiškų per sekundę skaičiaus nustatymas (ribojimas). • Turi būti automatinio apsimokymo režimas (įranga surenka informaciją apie naudojamus failus, parametrus ir t. t.). • Galimybė integruoti įrenginį su tinklalapių pažeidžiamumų skanavimo įrangą. Turi būti galimybė pažeidžiamumų skanavimo įrangai tiesiogiai konfigūruoti interneto svetainių apsaugos įrenginį. • Galimybė veikti „reverse proxy“ režimu, dekriptuojant HTTPS srautą įrenginyje, bei užmezgant saugų ryšį su serveriais naudojant organizacijos sertifikatus. • Žalingų IP adresų sąrašo atnaujinimai iš gamintojo, galimybė blokuoti prieigą prie svetainių iš žinomų žalingų IP adresų. • Įsilaužimų prevencijos (IPS) funkcionalumas. • Grėsmių informacijos atnaujinimai iš gamintojo („threat intelligence“), galimybė naudoti aktyvių grėsmių informaciją apsaugant WEB svetaines. • ICAP palaikymas. • Su saugos funkcionalumo susijusių ataskaitų ir statistinės informacijos atvaizdavimo funkcionalumas.	
12.	Srauto šifravimo funkcionalumas	• Turi dešifruoti SSL srautą (įdiegus skaitmeninius sertifikatus su atitinkamais privačiais raktais). • Turi šifruoti HTTP srautą panaudojant skaitmeninį sertifikatą su privačiu raktu • Turi būti tarnybinės stoties tapatybės, naudojant skaitmeninius sertifikatus, nustatymo funkcionalumas. • Turi būti kliento tapatybės, naudojant skaitmeninius sertifikatus, nustatymo funkcionalumas. • Turi būti keisti SSL parametrus funkcionalumas: SSL šifravimo mechanizmą, SSL versija.	
13.	Prieigos valdymo funkcionalumas	• Galimybė autentifikuoti svetainių vartotojus, naudojant LDAP, RADIUS, SAML, REST API, OAuth, OIDC mechanizmus. • Vieningo prisijungimo (*single sign on, SSO*) ir prieigos federavimo palaikymas. • Reverse proxy funkcionalumas saugiai vartotojų prieigai prie aplikacijų. • Prieigos taisyklių vartotojams ir jų grupėms taikymas, leidžiant vartotojams tik reikalingas prieigas. • SSL VPN palaikymas.	
14.	Programavimo galimybė	Galimybė programuoti specializuotus algoritmus/scenarijus (angl. „script“), leidžiančius perimti, inspektuoti, keisti ir nukreipti bet kokį įeinanti ir išeinantį srautą pagal bet kokius parametrus.	

15.	Valdymo funkcionalumas	• Turi būti taisyklių kiekvienai žiniatinklio svetainei atskirai kūrimo funkcionalumas. • Turi būti atakų aprašų kūrimo pačiam vartotojui (*angl. custom*) funkcionalumas. • Turi būti skirtingų taisyklių versijų kūrimo funkcionalumas • Turi būti grįžimo prie anksčiau naudotų taisyklių funkcionalumas.	
16.	Kitos palaikomos funkcijos	• Prievadų loginis grupavimas pagal IEEE 802.3ad ar lygiavertį standartą; • VLAN palaikymas (IEEE 802.1Q); • IPv6 protokolo palaikymas; • Saugumo filtrai pagal OSI L3/L4 lygių informaciją (siuntėjo ir gavėjo IP adresą, siuntėjo ir gavėjo TCP/UDP porto numerį). Saugumo filtrai turi būti „stateful“. • BGP, RIP, OSPF, ISIS, BFD protokolų palaikymas. • VXLAN, NVGRE palaikymas. • GCM, ECC, Camellia, DSA, RSA kriptavimo algoritmų palaikymas. • HSM palaikymas raktų saugojimui. • sFlow palaikymas.	
17.	Valdymas	• Valdymas per WEB sąsają. • SNMP palaikymas. • REST API palaikymas.	
18.	Diegimo ir konfigūravimo darbai	Diegimo darbai turi apimti: • Naujai įsigyjamos fizinės įrangos fizinį montavimą ir pajungimą prie kompiuterinio tinklo. • Įrangos versijų atnaujinimą. • Naujai įsigyjamos įrangos konfigūravimą. • Esamo ugniasienių valdymo sprendimo konfigūravimą, naujos įrangos pajungimą. • Bazinės saugos politikos sukūrimą. Diegimo darbai neapima: • Esamo kompiuterinio tinklo įrenginių konfigūravimo. ▪ Susijusių IT infrastruktūros elementų konfigūravimo – vartotojų direktorijos, RADIUS serverių ir pan. Šiuos darbus atlikti turi Perkančioji organizacija, pagal su Tiekėju suderintą projektą.	
19.	Garantinis aptarnavimas	▪ 60 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu.	

		▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. ▪ Gedimo atveju pakaitinė įranga turi būti pristatyta ne vėliau kaip kitą darbo dieną.	

Pranešame, kad rūpestingai išnagrinėję KONKURSO DOKUMENTUS, esame pasirengę atlikti Prekių teikimą **KONKURSO objekto 2 dalyje** pagal KONKURSO DOKUMENTŲ reikalavimus ir nurodome savo pasiūlymo kainą:

4 lentelė

	Pasiūlymo kaina **skaičiais**	Pasiūlymo kaina **žodžiais**
Pasiūlymo kaina **be PVM**	412.900,00	Keturi šimtai dvylika tūkstančių devyni šimtai eurų 0 ct.
Pasiūlymo kaina **su PVM**	499.609,00	Keturi šimtai devyniasdešimt devyni tūkstančiai šeši šimtai devyni eurai 0 ct.

Detalizuojame pasiūlymo kainą KONKURSO objekto 2 dalyje – Kompiuterių tinklo ugniasienė**:**

Detalizuojame Konkurso pasiūlymo kainą:

5 lentelė.

Eil. Nr.	**Pavadinimas**	**Gamintojo PREKĖS pavadinimas, PREKĖS kodas**	**Kiekis, vnt. (a)**	**Vieneto kaina, EUR be PVM (b)**	**Suma, EUR be PVM (c=a*b)**
1.	Modulinis tinklo ugniasienių sprendimas	Quantum Maestro: CPAP-SG9300-PLUS-MHS-SNBT, CPSB-SNBT-9300-PLUS-2Y, CPAP-MHO-140, CPSB-MOB-U, CPAC-DAC-10G-3M, CPAC-DAC-25G-3M, CPES-SS-STANDARD, CPES-SS-STANDARD-ADD.	2	178.740,50	357.481,00
2.	Virtualios ugniasienės	CloudGuard Network virtual core for VMware ESXi, Hyper-V, KVM: CPSG-VSEC-VEN-BUN-NGTX-3Y.	10	2.477,40	24.774,00
3.	Check Point Security Management Server valdymo sprendimo plėtimas	Next Generation Security Management Software CPSM-NGSM25. SmartEvent, SmartReporter and Compliance blades: CPSB-EVS-COMP-25-2Y.	1	30.645,00	30.645,00
				Suma iš viso be PVM:	412.900,00
				PVM suma:	86.709,00
				Suma iš viso (EUR su PVM):	499.609,00

Tiekėjo siūlomų įrenginių parametro reikšmės (Tiekėjas pildo lentelės stulpelį: „Siūlomos parametrų reikšmės“):

6 lentelė.

Eil. Nr.	**Pavadinimas**	**Reikalavimai**	**Siūlomi parametrai**
1.	Pirkimo objektas	Tinklo ugniasienių sprendimas, skirtas:	Tinklo ugniasienių sprendimas, skirtas:

		• Apsaugoti Perkančiosios organizacijos vartotojų kompiuterinius tinklus. • Apsaugoti Perkančiosios organizacijos duomenų centrų kompiuterinius tinklus. • Įgyvendinti Perkančiosios organizacijos kompiuterinio tinklo segmentavimo poreikį, užtikrinti srauto tarp tinklo segmentų kontrolę bei kibernetinių incidentų prevenciją. • Užtikrinti lankstų plečiamumą, bei resursų perskirstymą esant poreikiui.	• Apsaugoti Perkančiosios organizacijos vartotojų kompiuterinius tinklus. • Apsaugoti Perkančiosios organizacijos duomenų centrų kompiuterinius tinklus. • Įgyvendinti Perkančiosios organizacijos kompiuterinio tinklo segmentavimo poreikį, užtikrinti srauto tarp tinklo segmentų kontrolę bei kibernetinių incidentų prevenciją. • Užtikrinti lankstų plečiamumą, bei resursų perskirstymą esant poreikiui.
2.	Gamintojas	Nurodyti.	Check Point Software Technologies
3.	Modelis	Nurodyti, įskaitant tikslius visų komplektuojančių dalių ir licencijų produktų kodus.	Quantum Maestro: CPAP-SG9300-PLUS-MHS-SNBT ,5 vnt. CPSB-SNBT-9300-PLUS-2Y ,5 vnt. CPAP-MHO-140 ,2 vnt. CPSB-MOB-U ,1 vnt. CPAC-DAC-10G-3M ,10 vnt. CPAC-DAC-25G-3M ,2 vnt. CPES-SS-STANDARD ,1 vnt. CPES-SS-STANDARD-ADD ,1 vnt.
Bendrieji reikalavimai			
4.	Sprendimo tipas	Modulinio ugniasienių sprendimo komplektas, sudarytas iš išorinių modulių, tarpusavyje sujungiamų naudojant tinklo prievadus. Visi sprendimo moduliai ir kiti komponentai turi būti vieno gamintojo.	Modulinio ugniasienių sprendimo komplektas, sudarytas iš išorinių modulių, tarpusavyje sujungiamų naudojant tinklo prievadus. Visi sprendimo moduliai ir kiti komponentai yra vieno gamintojo.
5.	Plečiamumas	Sprendimo komplektas turi būti plečiamas, pridedant, ne mažiau kaip 20 plėtimo modulių, galinčių proporcingai padidinti sprendimo našumą.	Sprendimo komplektas yra plečiamas, pridedant papildomus 47 plėtimo modulius, galinčių proporcingai padidinti sprendimo našumą.
6.	Moduliai	Sprendimo komplektas turi apimti: • Ne mažiau dviejų tinklo prievadų modulių, skirtų įgyvendinti tinklo funkcionalumą ir paskirstyti srautą ugniasienėms moduliams. • Ne mažiau penkių ugniasienės modulių.	Sprendimo komplektas apima: • Du tinklo prievadų modulius, skirtus įgyvendinti tinklo funkcionalumą ir paskirstyti srautą ugniasienėms moduliams. • Penkis ugniasienės modulius.
7.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Visos reikalingos montavimui dalys pateikiamos su įranga.
8.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V, 50 – 60 Hz

9.	Maitinimo šaltiniai	Visi sprendimo mazgai turi turėti dubliuotą maitinimą.	Visi sprendimo mazgai turi dubliuotą maitinimą.
10.	Virtualizavimo funkcionalumas	Ugniasienių modulių grupavimo funkcionalumo palaikymas, apimantis: • Ugniasienių modulių grupavimas, ugniasienių grupę valdant kaip atskirą ugniasienę, priskiriant konfigūraciją bei politiką. • Tinklo modulių prievadų priskyrimas ugniasienių moduliams. • Galimybė pridėti arba atimti, perskirstyti ugniasienių modulius atsižvelgiant į apkrovas bet kuriuo metu, be poveikio sprendimo veikimui. • Galimybė ugniasienių grupę padalinti į dvi virtualias ugniasienes, su galimybe plėsti virtualių ugniasienių kiekį papildoma licencija. • Ugniasienių grupės bei virtualios ugniasienės turi palaikyti visus funkcinius reikalavimus individualiai, t. y. taip kaip tai būtų taikoma fizinei įrangai.	Ugniasienių modulių grupavimo funkcionalumo palaikymas, apimantis: • Ugniasienių modulių grupavimas į saugos grupes. Ugniasienių grupės valdomos kaip atskira ugniasienė, priskiriant konfigūraciją bei politiką. • Tinklo modulių prievadų priskyrimas ugniasienių moduliams. • Galimybė pridėti arba atimti, perskirstyti ugniasienių modulius atsižvelgiant į apkrovas bet kuriuo metu, be poveikio sprendimo veikimui. • Galimybė ugniasienių grupę padalinti į dvi virtualias ugniasienes, su galimybe plėsti virtualių ugniasienių kiekį papildoma licencija. • Ugniasienių grupės bei virtualios ugniasienės palaiko visus funkcinius reikalavimus individualiai, t. y. taip kaip tai būtų taikoma fizinei įrangai.
11.	Aukšto patikimumo funkcionalumas	▪ Visi ugniasienės moduliai vienoje grupėje turi būti aktyvūs. ▪ Sugedus vienam moduliui/nariui, arba nutrūkus ryšiui su vienu iš modulių/narių, turi būti išlaikomos aktyvios sesijos. ▪ Du modulinių ugniasienių komplektai turi veikti aukšto patikimumo režimu, diegiant juos skirtinguose duomenų centruose. ▪ Ugniasienių grupė gali būti aktyvi viename komplekte ir pasyvi kitame aukšto patikimumo komplekte, su galimybe pakeisti statusą aktyvuojant grupę kitame komplekte rankiniu būdu, arba automatiškai įvykus gedimui. ▪ Konfigūracija tarp modulių/narių bei grupių atskiruose komplektuose	▪ Visi ugniasienės moduliai vienoje grupėje yra aktyvūs. ▪ Sugedus vienam moduliui/nariui, arba nutrūkus ryšiui su vienu iš modulių/narių, yra išlaikomos aktyvios sesijos. ▪ Du modulinių ugniasienių komplektai veikia aukšto patikimumo režimu, diegiant juos skirtinguose duomenų centruose. ▪ Ugniasienių grupė gali būti aktyvi viename komplekte ir pasyvi kitame aukšto patikimumo komplekte, su galimybe pakeisti statusą aktyvuojant grupę kitame komplekte rankiniu būdu, arba automatiškai įvykus gedimui.

		turi būti automatiškai sinchronizuojama.	▪ Konfigūracija tarp modulių/narių bei grupių atskiruose komplektuose yra automatiškai sinchronizuojama.
12.	Valdymo prievadai	▪ Ne mažiau vieno RJ-45 prievado skirto valdymui. ▪ Ne mažiau vieno USB prievado. ▪ Ne mažiau vieno „*console*“ tipo prievado.	Tinklo moduliai: • Vienas RJ-45 prievadas skirtas valdymui. • Vienas USB prievadas. • Vienas console tipo prievadas. Ugniasienių moduliai: • Vienas RJ-45 prievadas skirtas valdymui. • Du USB prievadai. • Vienas console tipo prievadas.
Reikalavimai tinklo prievadų moduliams			
13.	Prievadai	Kiekvienas tinklo modulis turi turėti: • Ne mažiau 48 vnt. 10 GE SFP+ lizdų SFP+ moduliams įrengti viename tinklo modulyje, viso komplekte ne mažiau 96 vnt. • Ne mažiau 8 vnt. 100 GE QSFP28 lizdų QSFP28 moduliams įrengti viename tinklo modulyje, viso komplekte ne mažiau 16 vnt. • Tinklo prievadai gali būti naudojami ugniasienės modulių pajungimui, naudojant nurodytą kiekį srautui apdoroti ir aukštam patikimumui užtikrinti.	Kiekvienas tinklo modulis turi: • 48 vnt. 10 GE SFP+ lizdų SFP+ moduliams įrengti viename tinklo modulyje, viso komplekte 96 vnt. • 8 vnt. 100 GE QSFP28 lizdų QSFP28 moduliams įrengti viename tinklo modulyje, viso 16 vnt. • Tinklo prievadai naudojami ugniasienės modulių pajungimui. Kiekvienas ugniasienės modulis jungiamas vienu prievadu į kiekvieną tinklo modulį.
14.	Optiniai moduliai	Su kiekvienu tinklo moduliu turi būti pateikti: • 8 vnt. SFP+ SR optinių modulių skirti duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula ne mažiau kaip 300 metrų atstumu. Optiniai moduliai turi būti to paties gamintojo kaip ir siūlomi ugniasienės moduliai. • Visi reikalingi optiniai moduliai ir optiniai kabeliai skirti bendram sprendimo funkcionalumui užtikrinti, pvz.: modulių tarpusavio apjungimui turi būti įtraukti į pasiūlymą.	Su kiekvienu tinklo moduliu yra pateikiami: • 8 vnt. SFP+ SR optinių modulių skirti duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula 300 metrų atstumu. Optiniai moduliai yra to paties gamintojo kaip ir siūlomi ugniasienės moduliai. • Visi reikalingi optiniai kabeliai skirti modulių tarpusavio apjungimui yra įtraukti į pasiūlymą (3 m ilgio DAC kabeliai).
Našumo reikalavimai			
15.	Bendrieji našumo reikalavimai	Našumas skaičiuojamas vienam sprendimo komplektui,	Našumas skaičiuojamas vienam sprendimo komplektui,

		visiems moduliams esant aktyvioje konfigūracijoje.	visiems moduliams esant aktyvioje konfigūracijoje.
16.	Ugniasienės našumas	Ne mažiau 315 Gbps su realiu tinklo srautu.	332 Gbps su realiu tinklo srautu.
17.	Apsaugos nuo įsilaužimų našumas (IPS)	Ne mažiau 175 Gbps su realiu tinklo srautu.	185 Gbps su realiu tinklo srautu.
18.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Ne mažiau 125 Gbps su realiu tinklo srautu.	133 Gbps su realiu tinklo srautu.
19.	Bendras ugniasienės, aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto filtravimo, bot'ų aptikimo našumas	Me mažiau 40 Gbps su realiu tinklo srautu.	42 Gbps su realiu tinklo srautu.
20.	Ipsec VPN pralaidumas	Ne mažiau 140 Gbps.	155 Gbps.
21.	Sesijų skaičius	Ne mažiau 18 Milijonų vienu metu.	18 Milijonų vienu metu.
22.	Naujų sesijų skaičius per sekundę	Ne mažiau 750 000.	750 000.
23.	Ugniasienės našumo skaičiavimo metodika ir vertinimas	• Ugniasienės našumas 16, 17, 18, 19 punktuose gali būti vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Realus srautas turi būti sudarytas iš įprastomis sąlygomis naudojamų HTTP, SMTP, HTTPS, DNS, FTP protokolų. Turi būti pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. • Ugniasienės našumo parametrai turi būti skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.	• Ugniasienės našumas 16, 17, 18, 19 punktuose vertinamas su realiu, įprastu vartotojų tinklams, srautu. Realus srautas yra sudarytas iš įprastomis sąlygomis naudojamų HTTP, SMTP, HTTPS, DNS, FTP protokolų. Nuoroda į gamintojo testavimo metodikos aprašymą: https://pages.checkpoint.com/enterprise-security-performance.html • Ugniasienės našumo parametrai yra skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.
Funkciniai reikalavimai			
24.	Darbo režimai	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;
25.	Tinklo funkcionalumas	▪ Ne mažiau 1024 VLAN palaikymas, ne mažiau 4096 VLAN naudojant virtualizaciją.	▪ 1024 VLAN palaikymas, 4096 VLAN naudojant virtualizaciją. ▪ 802.3ad ryšių apjungimo (angl. „*link*

		▪ 802.3ad ryšių apjungimo (angl. „*link aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas.	*aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas.
26.	Maršurizavimas	▪ OSPFv2 ir v3 protokolų palaikymas. ▪ BGP palaikymas, grakštaus BGP perkrovimo (angl. *graceful restart*) palaikymas. ▪ RIP palaikymas. ▪ Statinis maršrutizavimas, *multicast* maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). • PIM, IGMP v2 ir v3 protokolų palaikymas.	• OSPFv2 ir v3 protokolų palaikymas. • BGP palaikymas, grakštaus BGP perkrovimo (angl. *graceful restart*) palaikymas. • RIP palaikymas. • Statinis maršrutizavimas, *multicast* maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). • PIM, IGMP v2 ir v3 protokolų palaikymas.
27.	Tinklo adresų transliavimas (NAT)	Statinio NAT, PAT, NAT66 palaikymas.	Statinio NAT, PAT, NAT66 palaikymas.
28.	Valdymas	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Sprendimas turi būti valdomas iš perkančiosios organizacijos naudojamo Check Point Software Technologies centralizuoto valdymo Check Point Security Management serverio. Siūlant kito gamintojo sprendimą, turi būti pateikiamos siūlomo ugniasienės modulių gamintojo ir Check Point gamintojo pažymos apie sprendimų suderinamumą.	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Sprendimas yra valdomas iš perkančiosios organizacijos naudojamo Check Point Software Technologies centralizuoto valdymo Check Point Security Management serverio.
29.	Sertifikatų palaikymas	▪ Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12). ▪ Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas.	▪ Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12). ▪ Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas.
30.	Ugniasienės saugos funkcijos	▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS)	▪ Ugniasienė

		▪ Vartotojų atpažinimas ▪ Aplikacijų ir URL kontrolė ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Galimybė nežinomų grėsmių patikrai (angl. sandboxing) ▪ Virtualūs privatūs tinklai ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė	▪ Įsilaužimų prevencija (IPS) ▪ Vartotojų atpažinimas ▪ Aplikacijų ir URL kontrolė ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Galimybė nežinomų grėsmių patikrai (angl. sandboxing) ▪ Virtualūs privatūs tinklai ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė
31.	Ugniasienės funkcionalumas	▪ Ugniasienė turi atlikti srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė turi gebėti įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ Turi būti atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų. ▪ Ugniasienės taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. ▪ Galimybė ugniasienės taisykles taikyti tam tikru laiku (datos, laikas). ▪ HTTP/HTTPS proxy palaikymas. ▪ Galimybė aprašyti savo protokolus bei paslaugas.	▪ Ugniasienė atlieka srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė geba įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ Yra atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų. ▪ Ugniasienės taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. ▪ Galimybė ugniasienės taisykles taikyti tam tikru laiku (datos, laikas). ▪ HTTP/HTTPS proxy palaikymas. ▪ Galimybė aprašyti savo protokolus bei paslaugas.
32.	Įsilaužimų prevencijos (IPS) funkcionalumas	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai turi apimti: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas.	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai apima: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas.

		○ Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitąveiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neturi būti įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). ▪ Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.	○ Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitąveiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas nėra įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). ▪ Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.
33.	Vartotojų atpažinimo funkcionalumas	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. ▪ Galimybė atpažinti vartotojus virtualių darbo	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų

		vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.	grupių atpažinimas bei taisyklių grupėms pritaikymas. ▪ Galimybė atpažinti vartotojus virtualių darbo vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.
34.	Aplikacijų ir URL kontrolė	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos, URL naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas. ▪ Galimybė aprašyti savo aplikacijas. ▪ Ne mažiau 3000 aplikacijų atpažinimas. Ne mažiau	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos, URL naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo

		200 milijonų URL duomenų bazė.	naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas. ▪ Galimybė aprašyti savo aplikacijas. ▪ 3000 aplikacijų atpažinimas. 200 milijonų URL duomenų bazė.
35.	Virusų ir kompiuterių zombių tinklų (BotNet) prevencijos funkcionalumas	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. ▪ Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitaveiką.	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. ▪ Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitaveiką.
36.	Nežinomų grėsmių aptikimo (angl. sandboxing) funkcionalumas	▪ Turi būti nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto. ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios organizacijos duomenų centre. ▪ Turi būti galimybė analizuoti šiuos failų tipus: .xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy,	▪ Yra nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto. ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios organizacijos duomenų centre.

		.com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Turi būti galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office programine įranga (Office 2003, 2010, 2013, 2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis ne mažiau kaip 80 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.	▪ Yra galimybė analizuoti šiuos failų tipus: .xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Yra galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office programine įranga (Office 2003, 2010, 2013, 2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis 100 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.
37.	Virtualūs privatūs tinklai (VPN)	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas. ▪ DES, 3DES, AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų), o Group 2 (1024 bitų),	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas. ▪ DES, 3DES, AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų),

		○ Group 5 (1536 bitų), ○ Group 14 (2048 bitų), ○ Group 19, ○ Group 20. • Palaikoms virtualių privačių tinklų topologijos: ○ Tinklelis (visi taškai užmezga VPN tunelius su visais), ○ Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), • Galimybė nustatyti VPN tunelių būvį: ○ tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. ○ statiniai tuneliai, atnaujinami nustatytu periodiškumu.	○ Group 2 (1024 bitų), ○ Group 5 (1536 bitų), ○ Group 14 (2048 bitų), ○ Group 19, ○ Group 20. • Palaikoms virtualių privačių tinklų topologijos: ○ Tinklelis (visi taškai užmezga VPN tunelius su visais), ○ Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), • Galimybė nustatyti VPN tunelių būvį: ○ tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. statiniai tuneliai, atnaujinami nustatytu periodiškumu.
38.	Nuotolinio prisijungimo funkcionalumas	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos). ▪ Galimybė naudoti nuotoliniam prisijungimui perkančiosios organizacijos naudojamą Check Point Software Technologies Harmony Agent programinę įrangą. ▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: ○ Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. ○ SecureID. ○ RADIUS autentifikaciją. ○ CAPI slaptažodžių generatorius. ○ P12 sertifikatus. ▪ Galimybė nustatyti agentams automatinio	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos). ▪ Galimybė naudoti nuotoliniam prisijungimui perkančiosios organizacijos naudojamą Check Point Software Technologies Harmony Agent programinę įrangą. ▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: ○ Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. ○ SecureID. ○ RADIUS autentifikaciją. ○ CAPI slaptažodžių generatorius.

		tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. ▪ Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją. ▪ Turi būti įtrauktos licencijos užtikrinant neribotą nuotolinio prisijungimo vartotojų kiekį dviems ugniasienių moduliams viename komplekte.	o P12 sertifikatus. ▪ Galimybė nustatyti agentams automatinio tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. ▪ Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją. ▪ Yra įtrauktos licencijos užtikrinant neribotą nuotolinio prisijungimo vartotojų kiekį dviems ugniasienių moduliams viename komplekte.
39.	Valdymo tinklo (angl. Industrial Control Systems) protokolų valdymas	▪ Galimybė kurti taisykles naudojant kelias kategorijas ar protokolus ir jais siunčiamas komandas vienoje taisyklėje. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamiems protokolams, jų grupėms/kategorijoms ir protokolais siunčiamoms komandoms: o blokuoti,	▪ Galimybė kurti taisykles naudojant kelias kategorijas ar protokolus ir jais siunčiamas komandas vienoje taisyklėje. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamiems protokolams, jų grupėms/kategorijoms ir protokolais siunčiamoms komandoms:

		○ informuoti vartotojus apie nepageidaujamo protokolo naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų protokolų ir komandų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Protokolų ir siunčiamų komandų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis protokolų aprašų atnaujinimas. ▪ Galimybė aprašyti savo protokolus ir komandas. ▪ Komandų siunčiamų valdymo tinklo protokolais atpažinimas ir kontrolė. Pvz.: ugniasienė turi drausti MODBUS „read coils“ komandų siuntimą. ▪ Ugniasienė turi atpažinti ir kontroliuoti ne mažiau kaip 1200 valdymo tinklo protokolų ir jais siunčiamų komandų, įskaitant: BACNet, CIP, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, ModBus, OPC DA & UA, Profinet, Step7 (Siemens). • Turi būti galimybė kurti taisykles pagal iš kritinės infrastruktūros duomenų tinklo stebėjimo sistemos į ugniasienių valdymo serverį perduotus duomenis. Nurodant konkrečius įrenginius arba žymenis, pvz.: įrenginio gamintoją, tipą, turi būti galimybė drausti visiems pvz.: SIEMENS gamintojo įrenginiams komunikuoti su išoriniais potinkliais. ▪ Turi būti galimybė pagal kritinės infrastruktūros duomenų tinklo stebėjimo sistemos atrastus įrenginių pažeidžiamumus kurti įsilaužimo prevencijos taisykles.	○ blokuoti, ○ informuoti vartotojus apie nepageidaujamo protokolo naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų protokolų ir komandų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Protokolų ir siunčiamų komandų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis protokolų aprašų atnaujinimas. ▪ Galimybė aprašyti savo protokolus ir komandas. ▪ Komandų siunčiamų valdymo tinklo protokolais atpažinimas ir kontrolė. Pvz.: ugniasienė uždraudžia MODBUS „read coils“ komandų siuntimą. ▪ Ugniasienė atpažįsta ir kontroliuoja 1200 valdymo tinklo protokolų ir jais siunčiamų komandų, įskaitant: BACNet, CIP, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, ModBus, OPC DA & UA, Profinet, Step7 (Siemens). • Yra galimybė kurti taisykles pagal iš kritinės infrastruktūros duomenų tinklo stebėjimo sistemos į ugniasienių valdymo serverį perduotus duomenis. Nurodant konkrečius įrenginius arba žymenis, pvz.: įrenginio gamintoją, tipą, yra galimybė drausti visiems pvz.: SIEMENS gamintojo įrenginiams komunikuoti su išoriniais potinkliais. • Yra galimybė pagal kritinės infrastruktūros duomenų tinklo

			stebėjimo sistemos atrastus įrenginių pažeidžiamumus kurti įsilaužimo prevencijos taisykles.
40.	Šifruoto srauto (SSL/TLS) inspektavimas	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). ▪ Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas.	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). ▪ Šifruoto srauto patikra įgyvendina visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas.
41.	Failų perdavimo kontrolė	• HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. • Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. ▪ Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.	▪ HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. ▪ Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. ▪ Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.
42.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti generuojami žurnaliniai įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; • Žalingus failus; • BotNet veiklą; Turi būti galimybė nustatyti įvykio įrašymą konkrečiai ugniasienės taisyklei, nurodant	Įvykių žurnalai Yra kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Yra generuojami žurnaliniai įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; • Žalingus failus; • BotNet veiklą; Yra galimybė nustatyti įvykio įrašymą konkrečiai

		įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. Siūlomas sprendimas turi būti suderinamas su perkančiosios organizacijos naudojamu Check Point Software Technologies įvykių kaupimo ir analizės sprendimu Security Management Log Server. Siūlant kito gamintojo sprendimą, turi būti pateikiamos siūlomo ugniasienės modulių gamintojo ir Check Point gamintojo pažymos apie sprendimų suderinamumą.	ugniasienės taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. Siūlomas sprendimas yra suderinamas su perkančiosios organizacijos naudojamu Check Point Software Technologies įvykių kaupimo ir analizės sprendimu Security Management Log Server.
43.	Administratorių paskyros	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.	Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.
44.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio visu aptarnavimo laikotarpiu.	Yra nemokami garantinio visu aptarnavimo laikotarpiu.
45.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
46.	Diegimo ir konfigūravimo darbai	Diegimo darbai turi apimti: • Naujai įsigyjamos fizinės įrangos fizinį montavimą ir pajungimą prie kompiuterinio tinklo. • Įrangos versijų atnaujinimą. • Naujai įsigyjamos įrangos konfigūravimą. • Esamo ugniasienių valdymo sprendimo konfigūravimą, naujos įrangos pajungimą. • Bazinės saugos politikos sukūrimą. Diegimo darbai neapima: • Esamo kompiuterinio tinklo įrenginių konfigūravimo.	Diegimo darbai apima: • Naujai įsigyjamos fizinės įrangos fizinį montavimą ir pajungimą prie kompiuterinio tinklo. • Įrangos versijų atnaujinimą. • Naujai įsigyjamos įrangos konfigūravimą. • Esamo ugniasienių valdymo sprendimo konfigūravimą, naujos įrangos pajungimą. • Bazinės saugos politikos sukūrimą. Diegimo darbai neapima:

		▪ Susijusių IT infrastruktūros elementų konfigūravimo – vartotojų direktorijos, RADIUS serverių ir pan. Šiuos darbus atlikti turi Perkančioji organizacija, pagal su Tiekėju suderintą projektą.	▪ Esamo kompiuterinio tinklo įrenginių konfigūravimo. ▪ Susijusių IT infrastruktūros elementų konfigūravimo – vartotojų direktorijos, RADIUS serverių ir pan. Šiuos darbus atlikti turi Perkančioji organizacija, pagal su Tiekėju suderintą projektą.
47.	Administratorių mokymai	Su kiekvienu komplektu (įsigyjami du komplektai) turi būti pateikiami mokymai dviems administratoriams (viso 4 administratoriams). Mokymai turi būti ne trumpesnį negu 2 dienų, ir apimti praktiką bei teoriją diegiant ir aptarnaujant siūlomą ugniasienių sprendimą.	Su kiekvienu komplektu (įsigyjami du komplektai) yra pateikiami mokymai dviems administratoriams (viso 4 administratoriams). Mokymai yra ne trumpesnį negu 2 dienų, ir apimti praktiką bei teoriją diegiant ir aptarnaujant siūlomą ugniasienių sprendimą.
48.	Garantiniai įsipareigojimai	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. ▪ Gedimo atveju pakaitinė įranga turi būti pristatyta ne vėliau kaip kitą darbo dieną.	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. ▪ Gedimo atveju pakaitinė įranga pristatoma ne vėliau kaip kitą darbo dieną.

7 lentelė

Virtualios ugniasienės, 10 vnt.

Eil. Nr.	Pavadinimas	Reikalavimai	Siūlomi parametrai
1.	Pirkimo objektas	Virtualios ugniasienės diegiamos į virtualizacijos platformą vidinių duomenų centrų resursų apsaugai, tinklo srauto patikrai tarp vidinių duomenų centro segmentą. Sprendimas turi apimti virtualių ugniasienių licencijas sprendimui diegiamam į virtualizacjos platformą.	Virtualios ugniasienės diegiamos į virtualizacijos platformą vidinių duomenų centrų resursų apsaugai, tinklo srauto patikrai tarp vidinių duomenų centro segmentą. Sprendimas apima virtualių ugniasienių licencijas sprendimui diegiamam į virtualizacjos platformą.
2.	Gamintojas	Nurodyti.	Check Point Software Technologies
3.	Suderinamumas su virtualizacijos platformomis	Siūloma programinė įranga turi būti suderinama su žemiau nurodytomis arba lygiavertėmis virtualizacijos platformomis: • VMware ESXi 6.5, 6.7, 7, 8; • Microsoft Hyper-V Server 2012 R2, 2016, 2019; • KVM.	Siūloma programinė įranga yra suderinama su žemiau nurodytomis virtualizacijos platformomis: • VMware ESXi 6.5, 6.7, 7, 8; • Microsoft Hyper-V Server 2012 R2, 2016, 2019; • KVM.
Bendrieji reikalavimai			
4.	Licencijavimo tipas	• Virtualios ugniasienės turi būti licencijuojamos vienam procesoriaus branduoliui. • Turi būti lankstus licencijavimas, virtuali ugniasienė diegiama su norimu kiekiu branduolių (pradedant nuo 2 branduolių vienai ugniasienei). • Galimybė sumažinti arba padidinti virtualių branduolių kiekį ugniasienei be papildomo licencijavimo procedūrų arba pagalbos iš gamintojo. • Visos diegiamos virtualios ugniasienės valdomos iš to paties centrinio valdymo sprendimo turi būti licencijuojamos viena licencija, automatiškai priskiriant ugniasienei reikiamą branduolių licencijų kiekį (neviršijant suminio branduolių licencijų kiekio).	• Virtualios ugniasienės yra licencijuojamos vienam procesoriaus branduoliui. • Yra lankstus licencijavimas, virtuali ugniasienė diegiama su norimu kiekiu branduolių (pradedant nuo 2 branduolių vienai ugniasienei). • Galimybė sumažinti arba padidinti virtualių branduolių kiekį ugniasienei be papildomo licencijavimo procedūrų arba pagalbos iš gamintojo. • Visos diegiamos virtualios ugniasienės valdomos iš to paties centrinio valdymo sprendimo yra licencijuojamos viena licencija, automatiškai priskiriant ugniasienei reikiamą branduolių licencijų kiekį (neviršijant suminio branduolių licencijų kiekio).
5.	Aukšto patikimumo funkcionalumas	Virtualios ugniasienės turi palaikyti aukšto patikimumo funkcionalumą:	Virtualios ugniasienės palaiko aukšto patikimumo funkcionalumą:

		• Aukšto patikimumo sistema turi dirbti Aktyvus/Pasyvus (*angl. Active/Passive*) ir Aktyvus/Aktyvus (*angl. Active/Active*) režimais. ▪ Sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį, užmegztos sesijos turi nenutrūkti.	• Aukšto patikimumo sistema dirba Aktyvus/Pasyvus (*angl. Active/Passive*) ir Aktyvus/Aktyvus (*angl. Active/Active*) režimais. • Sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį, užmegztos sesijos nenutrūksta.
Našumo reikalavimai			
6.	Apsaugos nuo įsilaužimų našumas (IPS)	Dviejų branduolių ugniasienė: ne mažiau 6 Gbps. Keturių branduolių ugniasienei: ne mažiau 11 Gbps. Aštuonių branduolių ugniasienei: ne mažiau 16 Gbps. Našumas turi būti vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.	Dviejų branduolių ugniasienė: 6,1 Gbps. Keturių branduolių ugniasienei: 11,5 Gbps. Aštuonių branduolių ugniasienei: daugiau negu 16 Gbps. Našumas yra vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.
7.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Dviejų branduolių ugniasienė: ne mažiau 4 Gbps. Keturių branduolių ugniasienei: ne mažiau 7,5 Gbps. Aštuonių branduolių ugniasienei: ne mažiau 12 Gbps. Našumas turi būti vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.	Dviejų branduolių ugniasienė: 4,1 Gbps. Keturių branduolių ugniasienei: 7,9 Gbps. Aštuonių branduolių ugniasienei: 12,3 Gbps. Našumas yra vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.
8.	Bendras ugniasienės, aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto filtravimo, bot'ų aptikimo našumas	Dviejų branduolių ugniasienė: ne mažiau 1,5 Gbps. Keturių branduolių ugniasienei: ne mažiau 3 Gbps. Aštuonių branduolių ugniasienei: ne mažiau 6 Gbps. Našumas turi būti vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.	Dviejų branduolių ugniasienė: 1,7 Gbps. Keturių branduolių ugniasienei: 3,1 Gbps. Aštuonių branduolių ugniasienei: 6 Gbps. Našumas yra vertinamas su realiu tinklo srautu, VMWare ESXi platformoje.
9.	Naujų sesijų skaičius per sekundę	Dviejų branduolių ugniasienė: ne mažiau 55 tūkstančių. Keturių branduolių ugniasienei: ne mažiau 95 tūkstančių. Aštuonių branduolių ugniasienei: ne mažiau 165 tūkstančių.	Dviejų branduolių ugniasienė: 55 tūkstančiai. Keturių branduolių ugniasienei: 95 tūkstančiai. Aštuonių branduolių ugniasienei: 165 tūkstančiai.
10.	Ugniasienės našumo skaičiavimo metodika ir vertinimas	• Ugniasienės našumas 7, 8, 9 punktuose gali būti vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Realus srautas turi būti sudarytas iš įprastomis sąlygomis naudojamų HTTP, SMTP, HTTPS, DNS,	• Ugniasienės našumas 7, 8, 9 punktuose yra vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Realus srautas yra sudarytas iš įprastomis sąlygomis naudojamų HTTP, SMTP,

		FTP protokolų. Turi būti pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. • Ugniasienės našumo parametrai turi būti skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą. • Našumas turi būti vertinamas VMWare ESXi platformoje.	HTTPS, DNS, FTP protokolų. Pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą: https://pages.checkpoint.com/enterprise-security-performance.html • Ugniasienės našumo parametrai yra skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą. • Našumas yra vertinamas VMWare ESXi platformoje.
Funkciniai reikalavimai			
11.	Darbo režimai	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;
12.	Tinklo funkcionalumas	▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas.	▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas.
13.	Tinklo adresų transliavimas (NAT)	Statinio NAT, PAT, NAT66 palaikymas.	Statinio NAT, PAT, NAT66 palaikymas.
14.	Valdymas	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Sprendimas turi būti valdomas iš perkančiosios organizacijos naudojamo Check Point Software Technologies centralizuoto valdymo Check Point Security Management serverio. Siūlant kito gamintojo sprendimą, turi būti pateikiamos siūlomo ugniasienės modulių gamintojo ir Check Point gamintojo pažymos apie sprendimų suderinamumą.	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Sprendimas yra valdomas iš perkančiosios organizacijos naudojamo Check Point Software Technologies centralizuoto valdymo Check Point Security Management serverio.
15.	Sertifikatų palaikymas	▪ Pasirašytų sertifikatų importavimas ir	▪ Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų

		naudojamų sertifikatų eksportavimas (PKCS #12). ▪ Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas.	eksportavimas (PKCS #12). ▪ Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas.
16.	Ugniasienės saugos funkcijos	▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS) ▪ Vartotojų atpažinimas ▪ Aplikacijų ir URL kontrolė ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Galimybė nežinomų grėsmių patikrai (angl. sandboxing) ▪ Virtualūs privatūs tinklai ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė	▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS) ▪ Vartotojų atpažinimas ▪ Aplikacijų ir URL kontrolė ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Galimybė nežinomų grėsmių patikrai (angl. sandboxing) ▪ Virtualūs privatūs tinklai ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė
17.	Ugniasienės funkcionalumas	▪ Ugniasienė turi atlikti srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė turi gebėti įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ Turi būti atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų. ▪ Ugniasienės taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. ▪ Galimybė ugniasienės taisykles taikyti tam tikru laiku (datos, laikas). ▪ HTTP/HTTPS proxy palaikymas. ▪ Galimybė aprašyti savo protokolus bei paslaugas.	▪ Ugniasienė atlieka srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė geba įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ Yra atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų.
18.	Įsilaužimų prevencijos (IPS) funkcionalumas	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai turi apimti: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas.	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai apima: o Bandymų išnaudoti žinomus

		○ Protokolų anomalijų aptikimas. ○ Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitąveiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neturi būti įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). ▪ Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.	pažeidžiamumus aptikimas. ○ Protokolų anomalijų aptikimas. ○ Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitąveiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas nėra įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). ▪ Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.
19.	Vartotojų atpažinimo funkcionalumas	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui.	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas

		Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. ▪ Galimybė atpažinti vartotojus virtualių darbo vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.	vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. ▪ Galimybė atpažinti vartotojus virtualių darbo vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.
20.	Aplikacijų ir URL kontrolė	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos, URL naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas.	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos, URL naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas,

		▪ Galimybė aprašyti savo aplikacijas. ▪ Ne mažiau 3000 aplikacijų atpažinimas. Ne mažiau 200 milijonų URL duomenų bazė.	nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas. ▪ Galimybė aprašyti savo aplikacijas. ▪ 3000 aplikacijų atpažinimas. 200 milijonų URL duomenų bazė.
21.	Virusų ir kompiuterių zombių tinklų (BotNet) prevencijos funkcionalumas	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. ▪ Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitaveiką.	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. ▪ Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitaveiką.
22.	Nežinomų grėsmių aptikimo (angl. sandboxing) funkcionalumas	▪ Turi būti nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto bei el. laiškų (p. 36). ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios organizacijos duomenų centre. ▪ Turi būti galimybė analizuoti šiuos failų tipus:	▪ Yra nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto bei el. laiškų (p. 36). ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios

		.xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Turi būti galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office programine įranga (Office 2003, 2010, 2013, 2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis ne mažiau kaip 80 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.	organizacijos duomenų centre. ▪ Yra galimybė analizuoti šiuos failų tipus: .xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Yra galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office programine įranga (Office 2003, 2010, 2013, 2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis 100 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.
23.	Virtualūs privatūs tinklai (VPN)	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas. ▪ DES, 3DES, AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų),	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas. ▪ DES, 3DES, AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas:

		○ Group 2 (1024 bitų), ○ Group 5 (1536 bitų), ○ Group 14 (2048 bitų), ○ Group 19, ○ Group 20. • Palaikoms virtualių privačių tinklų topologijos: ○ Tinklelis (visi taškai užmezga VPN tunelius su visais), ○ Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), • Galimybė nustatyti VPN tunelių būvį: ○ tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. ○ statiniai tuneliai, atnaujinami nustatytu periodiškumu.	○ Group 1 (768 bitų), ○ Group 2 (1024 bitų), ○ Group 5 (1536 bitų), ○ Group 14 (2048 bitų), ○ Group 19, ○ Group 20. • Palaikoms virtualių privačių tinklų topologijos: ○ Tinklelis (visi taškai užmezga VPN tunelius su visais), ○ Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), • Galimybė nustatyti VPN tunelių būvį: ○ tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. statiniai tuneliai, atnaujinami nustatytu periodiškumu.
24.	Nuotolinio prisijungimo funkcionalumas	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos). ▪ Galimybė naudoti nuotoliniam prisijungimui perkančiosios organizacijos naudojamą Check Point Software Technologies Harmony Agent programinę įrangą. ▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: ○ Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. ○ SecureID. ○ RADIUS autentifikaciją. ○ CAPI slaptažodžių generatorius. ○ P12 sertifikatus.	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos). ▪ Galimybė naudoti nuotoliniam prisijungimui perkančiosios organizacijos naudojamą Check Point Software Technologies Harmony Agent programinę įrangą. ▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: ○ Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. ○ SecureID. ○ RADIUS autentifikaciją.

		▪ Galimybė nustatyti agentams automatinio tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. ▪ Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją.	o CAPI slaptažodžių generatorius. o P12 sertifikatus. ▪ Galimybė nustatyti agentams automatinio tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. o Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją.
25.	Valdymo tinklo (angl. Industrial Control Systems) protokolų valdymas	▪ Galimybė kurti taisykles naudojant kelias kategorijas ar protokolus ir jais siunčiamas komandas vienoje taisyklėje. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamiems	▪ Galimybė kurti taisykles naudojant kelias kategorijas ar protokolus ir jais siunčiamas komandas vienoje taisyklėje. ▪ Galimybė taikyti skirtingus veiksmus

		protokolams, jų grupėms/kategorijoms ir protokolais siunčiamoms komandoms: o blokuoti, o informuoti vartotojus apie nepageidaujamo protokolo naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų protokolų ir komandų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Protokolų ir siunčiamų komandų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis protokolų aprašų atnaujinimas. ▪ Galimybė aprašyti savo protokolus ir komandas. ▪ Komandų siunčiamų valdymo tinklo protokolais atpažinimas ir kontrolė. Pvz.: ugniasienė turi drausti MODBUS „read coils“ komandų siuntimą. ▪ Ugniasienė turi atpažinti ir kontroliuoti ne mažiau kaip 1200 valdymo tinklo protokolų ir jais siunčiamų komandų, įskaitant: BACNet, CIP, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, ModBus, OPC DA & UA, Profinet, Step7 (Siemens). • Turi būti galimybė kurti taisykles pagal iš kritinės infrastruktūros duomenų tinklo stebėjimo sistemos į ugniasienių valdymo serverį perduotus duomenis. Nurodant konkrečius įrenginius arba žymenis, pvz.: įrenginio gamintoją, tipą, turi būti galimybė drausti visiems pvz.: SIEMENS gamintojo įrenginiams komunikuoti su išoriniais potinkliais. ▪ Turi būti galimybė pagal kritinės infrastruktūros duomenų tinklo stebėjimo sistemos atrastus įrenginių	nepageidaujamiems protokolams, jų grupėms/kategorijoms ir protokolais siunčiamoms komandoms: o blokuoti, o informuoti vartotojus apie nepageidaujamo protokolo naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų protokolų ir komandų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Protokolų ir siunčiamų komandų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis protokolų aprašų atnaujinimas. ▪ Galimybė aprašyti savo protokolus ir komandas. ▪ Komandų siunčiamų valdymo tinklo protokolais atpažinimas ir kontrolė. Pvz.: ugniasienė uždraudžia MODBUS „read coils“ komandų siuntimą. ▪ Ugniasienė atpažįsta ir kontroliuoja 1200 valdymo tinklo protokolų ir jais siunčiamų komandų, įskaitant: BACNet, CIP, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, ModBus, OPC DA & UA, Profinet, Step7 (Siemens). • Yra galimybė kurti taisykles pagal iš kritinės infrastruktūros duomenų tinklo stebėjimo sistemos į ugniasienių valdymo serverį perduotus duomenis. Nurodant konkrečius įrenginius arba žymenis, pvz.: įrenginio gamintoją, tipą, yra galimybė drausti visiems pvz.: SIEMENS gamintojo

		pažeidžiamumus kurti įsilaužimo prevencijos taisykles.	įrenginiams komunikuoti su išoriniais potinkliais. • Yra galimybė pagal kritinės infrastruktūros duomenų tinklo stebėjimo sistemos atrastus įrenginių pažeidžiamumus kurti įsilaužimo prevencijos taisykles.
26.	Šifruoto srauto (SSL/TLS) inspektavimas	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). ▪ Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas.	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). ▪ Šifruoto srauto patikra įgyvendina visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas.
27.	Failų perdavimo kontrolė	• HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. • Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. ▪ Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.	▪ HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. ▪ Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. ▪ Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.
28.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti generuojami žurnaliniai įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.;	Įvykių žurnalai yra įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Yra generuojami žurnaliniai įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus;

		• Žalingus failus; • BotNet veiklą; Turi būti galimybė nustatyti įvykio įrašymą konkrečiai ugniasienės taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. Siūlomas sprendimas turi būti suderinamas su perkančiosios organizacijos naudojamu Check Point Software Technologies įvykių kaupimo ir analizės sprendimu Security Management Log Server. Siūlant kito gamintojo sprendimą, turi būti pateikiamos siūlomo ugniasienės modulių gamintojo ir Check Point gamintojo pažymos apie sprendimų suderinamumą.	• Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; • Žalingus failus; • BotNet veiklą; Yra galimybė nustatyti įvykio įrašymą konkrečiai ugniasienės taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. Siūlomas sprendimas yra suderinamas su perkančiosios organizacijos naudojamu Check Point Software Technologies įvykių kaupimo ir analizės sprendimu Security Management Log Server.
29.	Administratorių paskyros	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.	Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.
30.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio visu aptarnavimo laikotarpiu.	Yra. Nemokamai garantinio visu aptarnavimo laikotarpiu.
31.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
32.	Diegimo ir konfigūravimo darbai	Diegimo darbai turi apimti: • Naujai įsigyjamos programinės diegimą į virtualizacos platformą. • Naujai įsigyjamos programinės įrangos konfigūravimą. • Esamo ugniasienių valdymo sprendimo konfigūravimą, naujos įrangos pajungimą. • Bazinės saugos politikos sukūrimą.	Diegimo darbai apima: • Naujai įsigyjamos programinės diegimą į virtualizacos platformą. • Naujai įsigyjamos programinės įrangos konfigūravimą. • Esamo ugniasienių valdymo sprendimo konfigūravimą, naujos įrangos pajungimą. • Bazinės saugos politikos sukūrimą.

		Diegimo darbai neapima: • Esamo kompiuterinio tinklo įrenginių konfigūravimo. ▪ Susijusių IT infrastruktūros elementų konfigūravimo – vartotojų direktorijos, RADIUS serverių ir pan. Šiuos darbus atlikti turi Perkančioji organizacija, pagal su Tiekėju suderintą projektą.	Diegimo darbai neapima: • Esamo kompiuterinio tinklo įrenginių konfigūravimo. • Susijusių IT infrastruktūros elementų konfigūravimo – vartotojų direktorijos, RADIUS serverių ir pan. Šiuos darbus atlikti turi Perkančioji organizacija, pagal su Tiekėju suderintą projektą.
33.	Garantiniai įsipareigojimai	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.

8 lentelė

Management Server valdymo sprendimo plėtimas, 1 vnt.			
Eil. Nr.	**Pavadinimas**	**Reikalavimai**	**Siūlomi parametrai**
1.	Pirkimo objektas	Perkančiosios organizacijos turimo Check Point Security Management Server centrinio valdymo serverio licencijos plėtimas. Perkančiosios organizacijos Check Point paskyros Nr.: 5348141 Plečiamos licencijos produkto kodas: CPSM-NGSM5 Plečiamos licencijos numeris: E6C4F010281C	Perkančiosios organizacijos turimo Check Point Security Management Server centrinio valdymo serverio licencijos plėtimas. Perkančiosios organizacijos Check Point paskyros Nr.:

			5348141 Plečiamos licencijos produkto kodas: CPSM-NGSM5 Plečiamos licencijos numeris: E6C4F010281C
2.	Licencijos plėtimas	Licencija plečiama iki 25 įrenginių valdymo. Praplėtus licenciją turi būti išlaikomas turimas funkcionalumas, įskaitant šiuos plėtinius: • SmartEvent. • SmarReporter.	Licencija plečiama iki 25 įrenginių valdymo. Praplėtus licenciją išlaikomas turimas funkcionalumas, įskaitant šiuos plėtinius: • SmartEvent. SmarReporter.
3.	Diegimo ir konfigūravimo darbai	Diegimo darbai turi apimti: • Praplėstos licencijos paruošimą ir diegimą į valdymo serverį. • Papildomų resursų reikalingų praplėstam valdymo serveriui priskyrimą.	Diegimo darbai apima: • Praplėstos licencijos paruošimą ir diegimą į valdymo serverį. • Papildomų resursų reikalingų praplėstam valdymo serveriui priskyrimą.
4.	Garantiniai įsipareigojimai	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.	▪ 36 mėn. garantinis aptarnavimas. ▪ Garantinį aptarnavimą gali vykdyti įgaliotas gamintojo serviso centras, arba tiesiogiai gamintojas. ▪ Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu,

			elektroniniu paštu, faksu arba telefonu. ▪ Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.

Kartu su prekėmis turi būti pateikta visa, siūlomoms prekėms, gamintojo numatyta dokumentacija. Dokumentacija turi būti lietuvių arba anglų kalba.
Perkamos įrangos garantinį aptarnavimą atlieka gamintojo sertifikuotas techninis centras.

Į prekių kainą turi būti įtrauktos visos sutarties vykdymui būtinos išlaidos. TIEKĖJAS negali reikalauti iš UŽSAKOVO jokių papildomų (neįtrauktų į KONKURSO pasiūlyme nurodytą (nurodytas) prekių ir (ar) paslaugų dalies (dalių) kainą (kainas)) išlaidų.

TIEKĖJAS su savo pasiūlymu turi pateikti gamintojo (gamintojo atstovybės) patvirtinimą, kad visos prekės skirtos UŽSAKOVUI (Valstybinei mokesčių inspekcijai prie Lietuvos Respublikos finansų ministerijos) ir gamintojas prisiima visus garantinius įsipareigojimus susijusius su siūlomomis prekėmis.

TIEKĖJAS turi būti oficialus siūlomos įrangos gamintojo atstovas Lietuvoje, turintis teisę parduoti ir diegti siūlomą gamintojo įrangą atlikti jos garantinį remontą ir techninį aptarnavimą. TIEKĖJAS su pasiūlymu turi pateikti dokumentus, patvirtinančius atitikimą nurodytam reikalavimui, pvz.: (gamintojo patvirtinimas, įgaliojimas ar kt.) arba nuorodą į oficialų gamintojo tinklalapį, kuriame patvirtinami TIEKĖJO įgaliojimai (Konkurso dokumentų 2 priedo 7 punkto lentelės 1 punktas**).**

Kartu su pasiūlymu Konkurso objekto 1 daliai TIEKĖJAS turi pateikti dokumentus nurodytus Konkurso dokumentų 2 priedo 7 punkto lentelės 2-5 punktuose.

Ši pasiūlyme nurodyta informacija yra konfidenciali ir/arba neviešinama/ *Pirkėjas šios informacijos negali atskleisti tretiesiems asmenims*:

5 lentelė.

Eil.Nr.	Dokumentas	Paaiškinimas, kokia konkreti informacija dokumente yra konfidenciali
1	*2*	*3*
1.	D.Rynkevic igaliojimas	Visi dokumente pateikti asmens duomenys yra konfidencialūs
2.	UAB NBCS jungtinė RC pažyma	UAB NBCS vadovo asmens duomenys
3.	Gamintojo patvirtinimo rastas del oficialaus atstovo	CheckPoint atstovo asmens duomenys
4.	Gamintojo garantijos patvirtinimo rastas	CheckPoint atstovo asmens duomenys

Kartu su PASIŪLYMU Konkursui pateikiami šie dokumentai:

6 lentelė.

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento lapų skaičius
1.	KONKURSO_DOKUMENTŲ_6_priedas_Nacionalinio_saugumo_deklaracija NBCS	2
2.	KONKURSO_DOKUMENTŲ_7_priedas_Tiekėjo_deklaracija NBCS	1
3.	Gamintojo patvirtinimo rastas del oficialaus atstovo	1
4.	EBVPD NBCS	14
5.	D.Rynkevic igaliojimas	1
6.	Gamintojo garantijos patvirtinimo rastas	1
7.	UAB NBCS jungtinė RC pažyma	2

Tuo atveju, jeigu mūsų Konkurso pasiūlymas būtų priimtas, Pirkėjui pareikalavus įsipareigojame kuo greičiau pasirašyti pirkimo sutartį atitinkančią Konkurso dokumentų reikalavimus, ir pradėti Prekių tiekimą.

Mūsų pasiūlymas įsigalioja nuo Konkurso pasiūlymų pateikimo termino pabaigos, ir galioja 3 mėnesius nuo Konkurso pasiūlymų pateikimo termino pabaigos dienos.

Patvirtiname, kad nesudarėme jokių sutarčių, raštu ar žodžiu, su bet kokiomis trečiosiomis šalimis dėl Prekių tiekimo rezultato ar bet kokio jo elemento perleidimo ateityje, taip pat, kad Prekių tiekimo rezultato ar bet kokio jo elemento atžvilgiu nėra jokių neįvykdytų trečiųjų šalių teisių, įskaitant, bet neatsiribojant nuoma, panauda ir kt.

Patvirtiname, kad kol bus parengta ir sudaryta oficiali pirkimo sutartis, šis pasiūlymas su Pirkėjo raštu pateiktu pasiūlymo akceptavimu galioja kaip įpareigojanti sutartis.

Dariuš Rynkevič _____

(vardas, pavardė) (parašas)

Dokumentą elektroniniu parašu
pasirašė DARIUŠ,RYNKEVIČ
Data: 2024-07-12 14:09:13