Atviro konkurso sąlygų
3 priedas

TECHNINĖ SPECIFIKACIJA

I. BENDROJI DALIS

Bendrieji reikalavimai

1. **Kartu su pasiūlymu yra pateiktas** architektūros aprašymo dokumentas, kuriame detaliai aprašomas sprendimas:
    1.1. architektūrinė schema;
    1.2. detalūs siūlomų įrenginių kiekiai, gamintojai, modeliai ir pavadinimai (jei gamintojas suteikia – ir prekių kodai);
    1.3. integracija su turima įranga;
    1.4. esamų paslaugų nenutrūkstamo veikimo užtikrinimas.
2. **Kartu su pasiūlymu yra pateikta** siūlomos įrangos gamintojų techninė dokumentacija (angl. datasheets) arba nuorodos gamintojo puslapiuose, įrodančios visų techninių reikalavimų atitikimą.
3. Visi funkciniai ir našumo reikalavimai yra pagrįsti tiksliomis nuorodomis į gamintojo internetiniame puslapyje esančią informaciją arba gamintojo techninę dokumentaciją (angl. datasheets), nurodant dokumentą ir puslapio numerį (atsakymai „Atitinka“, „Yra“, „Tenkina“ ir pan. arba perkopijuoti reikalavimų formulavimai nebus laikomi pakankamu atitikimo įrodymu).
4. Į visų šioje specifikacijoje aprašytų prekių kainą yra įskaičiuota tinklo projektavimo, įrangos pristatymo, montavimo, markiravimo, konfigūravimo, dokumentavimo, garantijos, mokymų ir pilno paruošimo eksploatacijai kaina.
5. Visi techninėje specifikacijoje aprašomi komponentai yra pilnai suderinami tarpusavyje bei sudaro vientisą, pilnai paruoštą naudojimui sistemą. Visi siūlomi komponentai yra nauji ir nenaudoti.
6. Visas papildomas medžiagas, reikalingas tinkamam komponentų apjungimui į vientisą sistemą, pateiks tiekėjas savo sąskaita.
7. Visos prekės ir paslaugos tenkins atitinkamus Lietuvos Respublikoje ir Europos Sąjungoje galiojančius teisės aktus.
8. Jei tiekėjui bus poreikis įdiegti centralizuotą programinę įrangą siūlomos įrangos valdymui, perkančioji organizacija suteiks virtualų serverį VMware aplinkoje. Reikalingų operacinių sistemų ir kitos programinės įrangos licencijas pateiks tiekėjas.
9. Reikalavimai įrangos garantijai:
    9.1. Garantinio laikotarpio trukmė – 36 mėnesiai.
    9.2. Visų siūlomų įrenginių ir programinės įrangos garantija yra užtikrinama gamintojo garantijos paketais. Gamintojo garantijos paketai apima:
        9.2.1. Programinės įrangos palaikymą (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas);
        9.2.2. Teisę kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu;
        9.2.3. Visas reikiamas licencijas ir parašų prenumeratas (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui;

9.2.4. Sugedusios techninės įrangos keitimą.

9.3. Garantinis laikotarpis pradedamas skaičiuoti nuo atitinkamo priėmimo-perdavimo akto pasirašymo dienos.

9.4. Garantinis aptarnavimas atliekamas įrangos buvimo vietoje.

9.5. Garantinio laikotarpio metu Tiekėjas pašalins tinkamai eksploatuotos įrangos gedimus.

9.6. Garantiniu laikotarpiu galios nemokamas vidinės programinės įrangos (angl. firmware) atnaujinimų ir naujų versijų gavimas.

9.7. Teisė gauti klaidų pataisymus ir naujas versijas suprantama, kaip Perkančiajai organizacijai suteikiama teisė be papildomo mokesčio programinės įrangos palaikymo laikotarpiu gauti programinės įrangos gamintojo išleidžiamus klaidų pataisymus ir naujas programinės įrangos versijas.

10. Perkančiosios organizacijos rajonų centrų mazguose funkcionuoja centrinė duomenų srautų maršrutizavimo įranga. Naudojami Cisco 9500, HPE 10504, HPE 5800 ir Huawei XG-PON įrenginiai, kuriuos reikės integruoti su perkamu technologinio duomenų perdavimo tinklo specializuotu apsaugos ir kontrolės sprendimu. Dalis informacijos apie perkančiosios organizacijos turimą duomenų perdavimo tinklą negali būti viešai atskleista dėl galimų kibernetinių grėsmių. Dėl to detalūs tinklo įrangos sąrašai ir jų konfigūracija, tinklo topologijos schemos, konkretūs tinklo mazgų adresai, įrangos programinės įrangos versijos, **tinklo sujungimų techninė informacija bus pateikta <u>dalyviui CVP IS priemonėmis pateikus prašymą pateikti nurodytą informaciją</u>**, bei pateikus pasirašytą pasižadėjimą gautos informacijos neplatinti ir nenaudoti kitais tikslais, išskyrus pasiūlymo parengimą šiam pirkimui.

Tinklo projektavimo ir diegimo darbai, mokymai

1. Tinklo projektavimo ir diegimo darbai.

1.1. Tiekėjas suprojektuos technologiniame duomenų perdavimo tinkle naudojamų duomenų perdavimo įrenginių apsaugos, rizikos mažinimo ir prevencijos nuo galimų nesankcionuotų veiksmų sistemą ir paruoš detalų projekto planą apimantį žemiau išvardintas temas:

1.1.1. Fiziniai diegimo parametrai:

1.1.1.1. Adresai.

1.1.1.2. Vieta komutacinėse spintose.

1.1.1.3. Įrangos komplektacija.

1.1.1.4. Maitinimas, svoris, temperatūra.

1.1.1.5. Fizinis apjungimas su kita įranga.

1.1.2. Tinklo topologija:

1.1.2.1. IP adresacija.

1.1.2.2. OSI L2 protokolai.

1.1.2.3. Maršrutizavimo protokolai.

1.1.2.4. Prievadų agregavimas.

1.1.2.5. Rajonų centruose projektuojama dedikuota saugumo zona atskirta nuo likusio tinklo dedikuota specializuota tinklo apsaugos įranga.

1.1.3. Saugumas, valdymas ir stebėjimas:

1.1.3.1. Specializuotas tinklo apsaugos įrangos sujungimo žvaigždės topologija naudojant IPSec šifravimą.

1.1.3.2. Vieningas konfigūracijos valdymas naudojant specializuotą tinklo apsaugos įrenginių valdymo ir kontrolės sprendimą.

1.1.3.3. NetFlow, IPFIX arba sFlow eksportavimas iš esamų tinklo įrenginių.

1.1.4. Siūlomos įrangos stebėjimas naudojant esamą IBM Tivoli stebėjimo sistemą. Stebėjimas apimą:
1.1.4.1. Pasiekiamumo stebėjimas.
1.1.4.2. Aliarmų iš siūlomo valdymo sprendimo persiuntimas.
1.1.5. Įrangos palaikymas, kuriame būtų aprašyta:
1.1.5.1. Sugedusios įrangos keitimo procesas.
1.1.5.2. Incidentų fiksavimo procesas.
1.1.5.3. Klausimų pateikimo tiekėjui arba gamintojui procesas.
1.1.5.4. Incidentų eskalavimo procesas.

1.2. Remiantis sukurtu detaliuoju projekto planu Tiekėjas atliks šiuos darbus:
1.2.1. Diegiamus technologinio duomenų perdavimo tinklo apsaugos įrenginius pristatys į numatytas lokacijas.
1.2.2. Sumontuos įrangą remiantis aprašytais fiziniais parametrais ir gamintojų reikalavimais. Visi sumontuoti komponentai bus markiruoti unikaliais žymenimis. Žymuo bus gerai matomas. Kabeliai markiruojami abiejuose galuose. Markiravimo duomenys pateikiami Microsoft Excel formatu prieš įrangos priėmimo-perdavimo akto pasirašymą. Montavimo darbai bus atliekami vadovaujantis darbų saugos technikos taisyklėmis, EĮJT normomis, priešgaisrinės saugos reikalavimais ir kitais šiuos darbus reglamentuojančiais teisės aktais. Įrenginių markiravimas bus suderintas su perkančiąja organizacija.
1.2.3. Sukonfigūruos įrangą remiantis aprašytais tinklo topologijos parametrais.
1.2.4. Į naujai suprojektuotą dedikuotą saugumo zoną perjungiamas šios tinklo įrangos valdymas:
1.2.4.1. HPE 10500 centriniai maršrutizatoriai
1.2.4.2. HPE 5820 prieigos komutatoriai
1.2.4.3. Cisco Catalyst 9500 prieigos komutatoriai
1.2.4.4. Huawei XG-PON maršrutizatoriai
1.2.5. Sukonfigūruos esamą IBM Tivoli stebėjimo sistemą remiantis stebėjimo sistemos konfigūravimo plano parametrais.
1.2.6. Išbandys visus atliekamus darbus remiantis bandymo plano parametrais.
1.2.7. Sukonfigūruos specializuotą tinklo apsaugos įrangą remiantis tinklo apsaugos įrangos diegimo projekto planu.
1.2.8. Sukonfigūruos NetFlow, IPFIX ir sFlow surinktą iš šios tinklo įrangos:
1.2.8.1. HPE 10500 centriniai maršrutizatoriai
1.2.8.2. HPE 5820 prieigos komutatoriai
1.2.8.3. Cisco Catalyst 9500 prieigos komutatoriai

1.3. Tiekėjas parengs, pateiks ir suderins su perkančiąja organizacija išpildomosios dokumentacijos komplektą, kurį sudaro:
1.3.1. Kiekvieno diegiamo objekto išpildomoji dokumentacija, kuri apima įdiegto objekto fizinius diegimo parametrus aprašytus detaliame projekto plane, įskaitant sumontuotos įrangos sąrašą. Bus nurodyta įrangos gamintojas, modelis, serijinis numeris, sumontavimo vieta ir data, detalūs sumontuotos įrangos išdėstymo ir sujungimų brėžiniai.
1.3.2. Tinklo dokumentacija, kuri apima sumontuotos įrangos konfigūracijos išrašus, tinklo topologijos ir įrangos stebėjimo parametrus.
1.3.3. Visa dokumentacija bus pateikta popieriniu ir elektroniniu formatu:

1.3.3.1. Visi dokumentacijos brėžiniai ir schemos bus atlikti ir pateikti Microsoft Visio programinėje aplinkoje;

1.3.3.2. Visos dokumentacijoje pateikiamos lentelės bus pateiktos ir Microsoft Excel programinėje aplinkoje;

1.3.3.3. Pateikiamuose brėžiniuose naudojami primityvai bus iš anksto suderinti su perkančiąja organizacija.

2. Mokymai:
   2.1. Tiekėjas praves specializuotus siūlomos įrangos gamintojų mokymus ne mažiau kaip dviem grupėm po 2-4 asmenis. Mokymai atitiks šiuos reikalavimus:
      2.1.1. Į mokymų kursą bus įtraukti praktiniai užsiėmimai su laboratorine įranga, apimantys pagrindines siūlomos įrangos administravimo ir priežiūros sritis.
      2.1.2. Mokymai truks ne mažiau kaip 1 darbo dieną.
3. Įrangos diegimą, konfigūravimą, garantinį aptarnavimą atliekantys specialistai mokės lietuvių kalbą arba bus užtikrintos kokybiškos vertimo paslaugos.
4. Tiekėjas visiškai atsako už Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymo bei Lietuvos Respublikos įstatymų, reglamentuojančių darbų saugą, reikalavimų vykdymą.
5. Visi darbai ar medžiagos, kurie gali būti pagrįstai laikomi būtinais darbų užbaigimui ir tinkamam eksploatavimui, bus privalomai atlikti ir (ar) įrengiami nepriklausomai nuo to, ar jie yra apibūdinti šioje techninėje specifikacijoje, ar ne.
6. Jei šioje techninėje specifikacijoje numatytai įrangai yra keliamas reikalavimas atitikti standartus, tiekėjas turi teisę pasiūlyti įrangą, atitinkančią standartus, kurie yra lygiaverčiai techninėje specifikacijoje nurodytiems standartams.

II. SPECIALIOJI DALIS

PERKAMŲ PREKIŲ REIKALAUJAMOS TECHNINĖS SAVYBĖS

Eil. Nr.	**Pavadinimas**	**Reikalavimai**	**Atitikimas**
1.	Technologinio duomenų perdavimo tinklo specializuotas apsaugos ir kontrolės sprendimas		
1.1.	Sprendimo tikslas – technologiniame duomenų perdavimo tinkle naudojamų duomenų perdavimo įrenginių apsauga, rizikų mažinimas ir prevencija nuo galimų nesankcionuotų veiksmų.		
1.2.	Sprendimas komplektuojamas iš Specializuotų tinklo apsaugos įrenginių ir Valdymo ir kontrolės sprendimo		
1.3.	Specializuoti I ir II tipo tinklo apsaugos įrenginiai tarpusavyje bendrauja šifruotu kanalu.		
1.4.	I ir II tipo tinklo apsaugos įrenginiai yra pilnai valdomi Valdymo ir kontrolės sprendimo programinės įrangos		
1.5.	I ir II tipo tinklo apsaugos įrenginiai yra to pačio gamintojo, nauji ir nenaudoti.		
2.	**Specializuotas I tipo tinklo apsaugos įrenginys**		
2.1.	Pirkimo objektas	Specializuotas, programinis-aparatinis tinklo apsaugos įrenginys. Visa techninė ir programinė įranga turi būti to paties gamintojo. Diegiamas visuose perkančiosios organizacijos tinklo mazguose, kuriuose	Specializuotas, programinis-aparatinis tinklo apsaugos įrenginys. Visa techninė ir programinė įranga yra to paties gamintojo. Diegiamas visuose perkančiosios organizacijos tinklo mazguose, kuriuose funkcionuoja

		funkcionuoja centriniai srautų valdymo įrenginiai HPE 10500 ir Huawei XG-PON. Kiekviename mazge diegiamas aukštą patikimumą užtikrinantis įrenginių telkinys iš ne mažiau nei dviejų įrenginių.	centriniai srautų valdymo įrenginiai HPE 10500 ir Huawei XG-PON. Kiekviename mazge diegiamas aukštą patikimumą užtikrinantis įrenginių telkinys iš dviejų įrenginių.
2.2.	Gamintojas	Nurodyti.	CheckPoint Software Technologies Ltd
2.3.	Modelis	Nurodyti, įskaitant tikslius visų komplektuojančių dalių ir licencijų produktų kodus.	CPAP-SG1570-NGTP-CO-PREM – 1570 Appliance with NGTP subscription package and Collaborative Premium support; CPAC-1500/3600/3800-RM-DUAL - Rack Mount shelf for Single/Dual for 1500/ 3600/ 3800 desktop appliances.
Bendrieji reikalavimai			
2.4.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga. Siūlant stalinio (angl. *desktop*) tipo įrenginius, kartu su įrenginiais Tiekėjas privalo pateikti ir lentynas montavimui į 19 colių komutacinę spintą. Lentyna turi būti to paties gamintojo, į lentyną turi tilpti maitinimo šaltiniai. Turi būti siūloma viena lentyna kiekvienai specializuotų tinklo apsaugos įrenginių porai.	Visos reikalingos montavimui dalys yra pateiktos su įranga. Siūlomi stalinio (angl. *desktop*) tipo įrenginiai, kartu su įrenginiais Tiekėjas pateiks ir lentynas montavimui į 19 colių komutacinę spintą. Lentyna yra to paties gamintojo, į lentyną telpa maitinimo šaltiniai. Siūloma viena lentyna kiekvienai specializuotų tinklo apsaugos įrenginių porai. *1500-security-gateway-datasheet, 6 psl.* *CP_1500_3000_Universal_Rack_Mount_UserGuide, 13 psl.*
2.5.	Įrangos elektros maitinimas	220 V, 50 – 60 Hz	220 V, 50 – 60 Hz *1500-security-gateway-datasheet, 5 psl.*
2.6.	Elektros maitinimo šaltinis	Vidinis arba išorinis.	Išorinis. *1500-security-gateway-datasheet, 5 psl.*
2.7.	Aukšto patikimumo funkcionalumas	Viename mazge diegiami įrenginiai turi tenkinti aukšto patikimumo reikalavimus: • Įrenginiai turi veikti aktyvus/pasyvus režimais. • Aktyvus/pasyvus režimo atveju sugedus vienam	Viename mazge diegiami įrenginiai tenkina aukšto patikimumo reikalavimus: • Įrenginiai veikia aktyvus/pasyvus režimais. *CP_R80.40_ClusterXL_AdminGuide, 46 psl.*

		įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, turi būti išlaikomos aktyvios sesijos.	• Aktyvus/pasyvus režimo atveju sugedus vienam įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, yra išlaikomos aktyvios sesijos. *CP_R80.40_ClusterXL_AdminGuide, 46 psl.*
2.8.	Valdymo prievadai	• Ne mažiau vieno USB, USB-C arba analogiško „console“ prievado valdymui.	• Vienas USB-C „console“ prievadas valdymui. *1500-security-gateway-datasheet, 5 psl.*
Reikalavimai tinklo prievadams			
2.9.	Prievadai	• Ne mažiau 9 vnt. 1000BasetT RJ45 prievadų. • Ne mažiau vieno 1GE prievado, kuris gali veikti kaip 1GE RJ45 arba kaip 1000BaseT SFP prievadas.	• 9 vnt. 1000BasetT RJ45 prievadų. • Vienas 1GE prievadas, kuris gali veikti kaip 1GE RJ45 arba kaip 1000BaseT SFP prievadas. *1500-security-gateway-datasheet, 5 psl.*
Našumo reikalavimai			
2.10.	Sprendimo našumas	Ne mažiau 6 Gbps 1518 baitų dydžio UDP paketais.	6.4 Gbps 1518 baitų dydžio UDP paketais. *1500-security-gateway-datasheet, 5 psl.*
2.11.	Apsaugos nuo įsilaužimų našumas (IPS)	Ne mažiau 1 Gbps su realiu tinklo srautu.	1.05 Gbps su realiu tinklo srautu. *1500-security-gateway-datasheet, 5 psl.*
2.12.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Ne mažiau 950 Mbps su realiu tinklo srautu.	970 Mbps su realiu tinklo srautu. *1500-security-gateway-datasheet, 5 psl.*
2.13.	Bendras specializuoto tinklo apsaugos įrenginio, aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto filtravimo, bot‘ų aptikimo našumas	Ne mažiau 450 Mbps su realiu tinklo srautu.	500 Mbps su realiu tinklo srautu. *1500-security-gateway-datasheet, 5 psl.*

2.14.	IPSec VPN pralaidumas	Ne mažiau 1.5 Gbps.	1.95 Gbps. *1500-security-gateway-datasheet, 5 psl.*
2.15.	Konkurentinių sesijų skaičius	Ne mažiau 480 000 vienu metu.	500 000 vienu metu. *1500-security-gateway-datasheet, 5 psl.*
2.16.	Naujų sesijų skaičius per sekundę	Ne mažiau 15 000.	15 750. *1500-security-gateway-datasheet, 5 psl.*
2.17.	Specializuoto tinklo apsaugos įrenginio našumo skaičiavimo metodika ir vertinimas	• Specializuoto tinklo apsaugos įrenginio našumas 2.11, 2.12, 2.13 punktuose gali būti vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Turi būti pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. • Specializuoto tinklo apsaugos įrenginio našumo parametrai turi būti skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.	• Specializuoto tinklo apsaugos įrenginio našumas 2.11, 2.12, 2.13 punktuose yra vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Yra pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. *https://pages.checkpoint.com/enterprise-security-performance.html enterprise-testing-conditions-whitepaper, 3 psl.* • Specializuoto tinklo apsaugos įrenginio našumo parametrai yra skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą. *enterprise-testing-conditions-whitepaper, 2-3 psl.*
Funkciniai reikalavimai			
2.18.	Darbo režimai	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;	• Skaidrus (OSI L2); *CP_R80.40_NextGenSecurityGateway_Guide, 186 psl.* • Maršrutizavimo (OSI L3); *CP_R80.40_NextGenSecurityGateway_Guide, 182 psl.* • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos; *CP_R80.40_NextGenSecurityGateway_Guide, 184 psl.*
2.19.	Tinklo funkcionalumas	• Ne mažiau 48 VLAN palaikymas.	• 100 VLAN palaikymas.

		• 802.3ad ryšių apjungimo (angl. „link aggregation“) funkcionalumo palaikymas. • Layer 2 ir Layer 3 maršrutizavimo funkcionalumas.	*https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk164912* • 802.3ad ryšių apjungimo (angl. „link aggregation“) funkcionalumo palaikymas. *CP_R80.40_Gaia_AdminGuide, 99 psl.* • Layer 2 ir Layer 3 maršrutizavimo funkcionalumas. *1500-security-gateway-datasheet, 5 psl.*
2.20.	Maršrutizavimas	• OSPFv2 protokolų palaikymas. • BGP palaikymas. • RIP palaikymas. • Statinis maršrutizavimas, *multicast* maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). • PIM-SM, IGMP protokolų palaikymas.	• OSPFv2 protokolų palaikymas. • BGP palaikymas. • RIP palaikymas. *1500-security-gateway-datasheet, 5 psl.* • Statinis maršrutizavimas, *multicast* maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). *CP_R80.40_Gaia_Advanced_Routing_AdminGuide, 148, 462 psl.* • PIM-SM, IGMP protokolų palaikymas. *1500-security-gateway-datasheet, 5 psl.*
2.21.	Tinklo adresų transliavimas (NAT)	Statinio NAT, dinaminio NAT ir PAT palaikymas.	Statinio NAT, dinaminio NAT ir PAT palaikymas. *CP_R80.40_SecurityManagement_AdminGuide, 210 psl.*
2.22.	Valdymas	• WEB (HTTPS), SSH, konsolės prievadas. • SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. • Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). • IPFIX arba analogiškas protokolas gebantis eksportuoti statistinę tinklo srauto informaciją.	• WEB (HTTPS), SSH, konsolės prievadas. *CP_R80.40_Gaia_AdminGuide, 25, 330 psl.* • SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. *CP_R80.40_Gaia_AdminGuide, 206 psl.* • Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup).

		• Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu.	*CP_R80.40_Gaia_AdminGuide, 389 psl.* • IPFIX arba analogiškas Netflow protokolas gebantis eksportuoti statistinę tinklo srauto informaciją. *CP_R80.40_Gaia_AdminGuide, 179 psl.* • Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu. *CP_R80.40_SmartProvisioning_AdminGuide, 19 psl.*
2.23.	Sertifikatų palaikymas	• Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12 arba lygiavertis).	• Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12). *CP_R80.40_RemoteAccessVPN_AdminGuide, 45 psl.*
2.24.	Specializuoto tinklo apsaugos įrenginio saugos funkcijos	• Ugniasienė • Įsilaužimų prevencija (IPS) • Vartotojų atpažinimas • Aplikacijų kontrolė • Virtualūs privatūs tinklai • Šifruoto srauto (SSL/TLS) inspektavimas	• Ugniasienė • Įsilaužimų prevencija (IPS) • Vartotojų atpažinimas • Aplikacijų kontrolė • Virtualūs privatūs tinklai *1500-security-gateway-datasheet, 5 psl.* • Šifruoto srauto (SSL/TLS) inspektavimas *CP_R80.40_NextGenSecurityGateway_Guide, 28 psl.*
2.25.	Specializuoto tinklo apsaugos įrenginio funkcionalumas	• Specializuotas tinklo apsaugos įrenginys turi atlikti srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. stateful firewall). • Specializuotas tinklo apsaugos įrenginys turi gebėti įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms	• Specializuotas tinklo apsaugos įrenginys atlieka srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. stateful firewall). *CP_R80.40_NextGenSecurityGateway_Guide, 50 psl.* • Specializuotas tinklo apsaugos įrenginys geba įgyvendinti srauto, sesijų kiekio ribojimo funkcijas

		charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). • Specializuoto tinklo apsaugos įrenginio taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. • Galimybė tinklo apsaugos įrenginio taisykles taikyti tam tikru laiku (datos, laikas). • Proxy serverio palaikymas. • Galimybė aprašyti savo protokolus bei paslaugas.	taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). *CP_R80.40_SecurityManagement_AdminGuide, 178 psl.* *CP_R80.40_PerformanceTuning_AdminGuide.pdf, 36 psl.* • Specializuoto tinklo apsaugos įrenginio taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. *CP_R80.40_SecurityManagement_AdminGuide, 204 psl.* • Galimybė tinklo apsaugos įrenginio taisykles taikyti tam tikru laiku (datos, laikas). *CP_R80.40_SecurityManagement_AdminGuide, 178, 179 psl.* • Proxy serverio palaikymas. *CP_R80.40_Gaia_AdminGuide, 59 psl.* • Galimybė aprašyti savo protokolus bei paslaugas. *CP_R80.40_SecurityManagement_AdminGuide, 165 psl.*
2.26.	Įsilaužimų prevencijos (IPS) funkcionalumas	• Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai turi apimti: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. • Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant tinklo apsaugos įrenginio greitaveiką.	• Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai apima: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. *CP_R80.40_ThreatPrevention_AdminGuide, 29, 208 psl.* • Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant

		• Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas tinklo apsaugos įrenginio 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). • IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). • Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.	tinklo apsaugos įrenginio greitaveiką. *CP_R80.40_ThreatPrevention_AdminGuide, 46-47 psl.* • Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas tinklo apsaugos įrenginio apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neįjungtas pagal nutylėjimą. *CP_R80.40_ThreatPrevention_AdminGuide, 207 psl.* • Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). *CP_R80.40_ThreatPrevention_AdminGuide.pdf, 56, 215 psl.* • IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). *CP_R80.40_ThreatPrevention_AdminGuide, 193 psl.* • Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas. *CP_R80.40_NextGenSecurityGateway_Guide.pdf, 29 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 140 psl.*
2.27.	Vartotojų atpažinimo funkcionalumas	• Galimybė atpažinti bei autentifikuoti vartotojus. • Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. • Galimybė kurti vartotojų duomenų bazę specializuotame tinklo apsaugos įrenginyje.	• Galimybė atpažinti bei autentifikuoti vartotojus. *CP_R80.40_IdentityAwareness_AdminGuide, 46 psl.* • Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. *CP_R80.40_IdentityAwareness_AdminGuide, 31, 211, 220 psl.*

		• Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas.	• Galimybė kurti vartotojų duomenų bazę specializuotame tinklo apsaugos įrenginyje. *CP_R80.40_SecurityManagement_AdminGuide, 58 psl.* • Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. *CP_R80.40_IdentityAwareness_AdminGuide, 19, 32 psl.*
2.28.	Aplikacijų kontrolė	• Galimybė kurti aplikacijų taisykles naudojant kelias kategorijas vienoje taisyklėje. • Skirtingų aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. • Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. • Mechanizmas nepageidaujamų aplikacijų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. • Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ribojimą. • Aplikacijų atpažinimas bei ribojimas, nepriklausomai	• Galimybė kurti aplikacijų taisykles naudojant kelias kategorijas vienoje taisyklėje. *CP_R80.40_NextGenSecurityGateway_Guide, 412 psl.* • Skirtingų aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. *CP_R80.40_SecurityManagement_AdminGuide, 179, 259 psl.* • Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. *CP_R80.40_SecurityManagement_AdminGuide, 177 psl.* *CP_R80.40_ThreatPrevention_AdminGuide, 175-178 psl.* • Mechanizmas nepageidaujamų aplikacijų naudojimo ribojimui (pagal

		nuo naudojamų prievadų bei kitų tinklo parametrų. • Automatinis aplikacijų aprašų atnaujinimas. • Galimybė aprašyti savo aplikacijas. ▪ Ne mažiau 3000 aplikacijų atpažinimas.	laiką, datas), arba riboti jų greitaveiką. *CP_R80.40_SecurityManagement_AdminGuide, 178 psl.* • Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ribojimą. *CP_R80.40_ThreatPrevention_AdminGuide, 174 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 169 psl.* • Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. *CP_R80.40_SecurityManagement_AdminGuide, 163.* *CP_R80.40_PerformanceTuning_AdminGuide, 36 psl.* • Automatinis aplikacijų aprašų atnaujinimas. *CP_R80.40_NextGenSecurityGateway_Guide, 44 psl.* • Galimybė aprašyti savo aplikacijas. *CP_R80.40_SecurityManagement_AdminGuide, 165 psl.* • Virš 8000 aplikacijų atpažinimas. *https://appwiki.checkpoint.com/appwikisdb/public.htm*
2.29.	Virtualūs privatūs tinklai (VPN)	• Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. certificate authority). • IPSec protokolo palaikymas. • DES, 3DES, AES128, AES256 šifravimo standartų palaikymas. • MD5, SHA1, SHA256 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). *CP_R80.40_SecurityManagement_AdminGuide, 126 psl.* *CP_R80.40_ReleaseNotes, 19 psl.* • IPSec protokolo palaikymas. *CP_R80.40_RemoteAccessVPN_AdminGuide, 26 psl.* • DES, 3DES, AES128, AES256 šifravimo standartų palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 50 psl.*

		o Group 5 (1536 bitų), o Group 14 (2048 bitų), o Group 19, o Group 20. • Palaikomos virtualių privačių tinklų topologijos: o Tinklelis (visi taškai užmezga VPN tunelius su visais), o Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), • Galimybė nustatyti VPN tunelių būvį: o tuneliai užmezgami pagal poreikį, vykstant komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko; o statiniai tuneliai, atnaujinami nustatytu periodiškumu.	• MD5, SHA1, SHA256 duomenų vientisumo patikros algoritmų palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 50 psl.* • Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų), o Group 2 (1024 bitų), o Group 5 (1536 bitų), o Group 14 (2048 bitų), o Group 19, o Group 20. *CP_R80.40_SitetoSiteVPN_AdminGuide, 51 psl.* • Palaikomos virtualių privačių tinklų topologijos: o Tinklelis (visi taškai užmezga VPN tunelius su visais), o Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), *CP_R80.40_SitetoSiteVPN_AdminGuide, 41, 156 psl.* • Galimybė nustatyti VPN tunelių būvį: o tuneliai užmezgami pagal poreikį, vykstant komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko; o statiniai tuneliai, atnaujinami nustatytu periodiškumu. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 130 – 133 psl.* *CP_R80.40_SitetoSiteVPN_AdminGuide, 64 psl.*
2.30.	Vartotojų nuotolinio prisijungimo funkcionalumas	• Nuotolinis prisijungimas prie specializuotų tinklo apsaugos įrenginių naudojant IPSec VPN arba SSL VPN.	• Nuotolinis prisijungimas prie specializuotų tinklo apsaugos įrenginių naudojant IPSec VPN arba SSL VPN.

		• Ne mažiau negu 100 konkurentinių vartotojų prisijungimų vienu metu. • Galimybė suteikti programinės įrangos virtualiam tinklo prievadui IP adresą iš: o Specializuotame tinklo apsaugos įrenginyje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius.	*CP_R80.40_RemoteAccessVPN_AdminGuide, 26, 34 psl.* • 200 konkurentinių vartotojų prisijungimų vienu metu. *1500-security-gateway-datasheet, 5 psl.* • Galimybė suteikti programinės įrangos virtualiam tinklo prievadui IP adresą iš: o Specializuotame tinklo apsaugos įrenginyje numatyto IP adresų rėžio. *CP_R80.40_RemoteAccessVPN_AdminGuide, 77 psl.* o Naudojant DHCP relay. *CP_R80.40_RemoteAccessVPN_AdminGuide, 81 psl.* o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. *CP_R80.40_RemoteAccessVPN_AdminGuide.pdf, 72, 76-77 psl.*
2.31.	Šifruoto srauto (SSL/TLS) inspektavimas	• Šifruoto SSL ir TLS srauto dešifravimas ir patikra. • Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). • Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas saugos funkcijas prieš tai atlikus dešifravimą. • Perfect Forward Secrecy palaikymas.	• Šifruoto SSL ir TLS srauto dešifravimas ir patikra. *CP_R80.40_SecurityManagement_AdminGuide, 39, 274 psl.* • Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). *CP_R80.40_SecurityManagement_AdminGuide, 286 psl.* • Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas saugos funkcijas prieš tai atlikus dešifravimą. *CP_R80.40_SecurityManagement_AdminGuide.pdf, 281 psl.* • Perfect Forward Secrecy palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 52 psl.*

2.32.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti generuojami žurnaliniai įvykiai susiję su tinklo apsaugos įrenginio funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; Turi būti galimybė nustatyti įvykio įrašymą konkrečiai tinklo apsaugos įrenginio taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams.	Įvykių žurnalai yra kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Yra generuojami žurnaliniai įvykiai susiję su tinklo apsaugos įrenginio funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; *CP_R80.40_LoggingAndMonitoring_AdminGuide, 25, 80, 88, 111 psl.* Galimybė nustatyti įvykio įrašymą konkrečiai tinklo apsaugos įrenginio taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. *CP_R80.40_LoggingAndMonitoring_AdminGuide.pdf, 66, 68 psl.* *https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131064*
2.33.	Administratorių paskyros	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti galimybė smulkiai apibrėžti administratoriaus teises: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus;	Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. Yra galimybė smulkiai apibrėžti administratoriaus teises: • 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;	• teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas; *CP_R80.40_Gaia_AdminGuide, 269 psl.*
2.34.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Yra. Nemokamai garantinio aptarnavimo laikotarpiu *https://www.checkpoint.com/support-services/support-plans/*
2.35.	Atnaujinimai pagal nustatytą grafiką (Schedule)	Turi būti	Yra *CP_R80.40_Gaia_AdminGuide, 403 psl.* *CP_R80.20.05_1500_Appliance_Series_AdminGuide_Centrally_Managed, 104 psl.*
2.36.	Garantiniai įsipareigojimai	• Gamintojo garantuojamas nemokamas garantinis aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą turi būti įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui. • 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.	• Gamintojo garantuojamas nemokamas garantinis aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą yra įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. • Gedimo atveju pakaitinė įranga bus pristatyta ne vėliau kaip kitą darbo dieną. *https://www.checkpoint.com/support-services/support-plans/*
3.	**Specializuotas II tipo tinklo apsaugos įrenginys**		

5.1.	Pirkimo objektas	Specializuotas, programinis-aparatinis tinklo apsaugos įrenginys. Visa techninė ir programinė įranga turi būti to paties gamintojo. Atlieka IPsec tunelių terminavimo funkciją su specializuotais I tipo tinklo įrenginiais. Diegiamas centriniame mazge (1 vnt.). Diegiamas aukštą patikimumą užtikrinantis įrenginių telkinys iš ne mažiau nei dviejų įrenginių.	Specializuotas, programinis-aparatinis tinklo apsaugos įrenginys. Visa techninė ir programinė įranga yra to paties gamintojo. Atlieka IPsec tunelių terminavimo funkciją su specializuotais I tipo tinklo įrenginiais. Diegiamas centriniame mazge (1 vnt.). Diegiamas aukštą patikimumą užtikrinantis įrenginių telkinys iš dviejų įrenginių.
5.2.	Gamintojas	Nurodyti.	CheckPoint Software Technologies Ltd
5.3.	Modelis	Nurodyti, įskaitant tikslius visų komplektuojančių dalių ir licencijų produktų kodus.	CPAP-SG6400-PLUS-SNBT - 6400 Plus appliance with SandBlast subscription package; CPAC-4-10F-C-INSTALL - 4 Port 10GBase-F SFP+ interface card for 6000, 7000, 16000, 26000 and 28000 series. Requires an additional 10GBase SFP+ transceiver per interface port; CPAC-TR-10SR-C - SFP+ transceiver for 10G fiber Ports - short range (10GBase-SR) compatible with CPAC-4-10F-C only; CPAC-RAM16GB-6400-INSTALL - Memory Upgrade Kit from 16GB to 32GB for 6400 series appliances; CPSB-NGTP-6400-PLUS - Next Generation Threat Prevention for additional years for 6400 PLUS Appliance; CPSB-NGTP-6400-PLUS - Next Generation Threat Prevention for additional year for 6400 PLUS Appliance; CPCES-CO-PREMIUM-ADD - Premium Collaborative Enterprise Support.
Bendrieji reikalavimai			
5.4.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga.	Visos reikalingos montavimui dalys yra pateiktos su įranga.
5.5.	Įrangos elektros maitinimas	220 V, 50 – 60 Hz	220 V, 50 – 60 Hz

			6400-security-gateway-datasheet, 3 psl.
5.6.	Elektros maitinimo šaltiniai	Dubliuoti vidiniai maitinimo šaltiniai.	Dubliuoti vidiniai maitinimo šaltiniai. *6400-security-gateway-datasheet, 2 psl.*
5.7.	Aukšto patikimumo funkcionalumas	Centriniame mazge diegiami įrenginiai turi tenkinti aukšto patikimumo reikalavimus: • Įrenginiai turi veikti aktyvus/aktyvus arba aktyvus/pasyvus režimais. • Aktyvus/pasyvus režimo atveju sugedus vienam įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, turi būti išlaikomos aktyvios sesijos. • Aktyvus/aktyvus režimo atveju įrenginiai turi gebėti tolygiai paskirstyti tarpusavyje apkrovą. • VRRP palaikymas.	Centriniame mazge diegiami įrenginiai turi tenkina aukšto patikimumo reikalavimus: • Įrenginiai veikia aktyvus/aktyvus arba aktyvus/pasyvus režimais. • Aktyvus/pasyvus režimo atveju sugedus vienam įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, yra išlaikomos aktyvios sesijos. • Aktyvus/aktyvus režimo atveju įrenginiai geba tolygiai paskirstyti tarpusavyje apkrovą. *ClusterXL R80.40 Administration Guide, 46-47 psl.* • VRRP palaiko. *6400-security-gateway-datasheet, 3 psl.*
5.8.	Valdymo prievadai	• Ne mažiau vieno USB arba USB-C prievado valdymui. • Ne mažiau vieno „console“ tipo prievado. • Ne mažiau vieno 1000BaseT RJ45 prievadų sinchronizacijai tarp aukšto patikimumo sistemos narių. • Ne mažiau vieno specializuoto 1000BaseT RJ45 valdymo prievado.	• Vienas USB-C prievadas valdymui. • Vienas „console“ tipo prievadas. • Vienas 1000BaseT RJ45 prievadas sinchronizacijai tarp aukšto patikimumo sistemos narių. • Vienas specializuotas 1000BaseT RJ45 valdymo prievadas. *6400-security-gateway-datasheet, 2 psl.*
Reikalavimai tinklo prievadams			
5.9.	Prievadai	• Ne mažiau 8 vnt. 1000BasetT RJ45 prievadų. • Ne mažiau 4 vnt. 10GBase-F SFP+ prievadų SFP+ sąsajoms įdiegti.	• 8 vnt. 1000BasetT RJ45 prievadų. • 4 vnt. 10GBase-F SFP+ prievadų SFP+ sąsajoms įdiegti.

		• Visi tinklo prievadai turi būti atskiri fiziniai prievadai, su galimybe atlikti maršrutizavimą tarp tinklų nedarant įtakos bendrai tinklo apsaugos įrenginio greitaveikai. Nurodyti tinklo prievadai neturi būti sujungti į vidinį L2 komutatorių.	*Komplektuojama su papildomu moduliu CPAC-4-10F-C* *6400-security-gateway-datasheet, 2, 4 psl.* • Visi tinklo prievadai yra atskiri fiziniai prievadai, su galimybe atlikti maršrutizavimą tarp tinklų nedarant įtakos bendrai tinklo apsaugos įrenginio greitaveikai. Nurodyti tinklo prievadai nėra sujungti į vidinį L2 komutatorių. *6400-security-gateway-datasheet, 3 psl.*
5.10.	SFP sąsajos	Su specializuotu tinklo apsaugos įrenginiu turi būti pateikti 2 vnt. SFP+ SR optinių sąsajų skirtų duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula ne mažiau kaip 300 metrų atstumu. Sąsajos turi būti to paties gamintojo.	Su specializuotu tinklo apsaugos įrenginiu yra pateikti 2 vnt. SFP+ SR optinių sąsajų skirtų duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula ne mažiau kaip 300 metrų atstumu. Sąsajos yra to paties gamintojo. *CPAC-TR-10SR-C;* *6400-security-gateway-datasheet, 4 psl.*
Našumo reikalavimai			
5.11.	Sprendimo našumas	Ne mažiau 10 Gbps 1518 baitų dydžio UDP paketais.	12 Gbps 1518 baitų dydžio UDP paketais. *6400-security-gateway-datasheet, 3 psl.*
5.12.	Apsaugos nuo įsilaužimų našumas (IPS)	Ne mažiau 6 Gbps su realiu tinklo srautu.	6.5 Gbps su realiu tinklo srautu. *6400-security-gateway-datasheet, 3 psl.*
5.13.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Ne mažiau 5 Gbps su realiu tinklo srautu.	5.5 Gbps su realiu tinklo srautu. *6400-security-gateway-datasheet, 3 psl.*
5.14.	Bendras specializuoto tinklo apsaugos įrenginio, aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto	Ne mažiau 2 Gbps su realiu tinklo srautu.	2.5 Gbps su realiu tinklo srautu. *6400-security-gateway-datasheet, 3 psl.*

	filtravimo, bot'ų aptikimo našumas		
5.15.	IPSec VPN pralaidumas	Ne mažiau 2.5 Gbps.	2.73 Gbps. *6400-security-gateway-datasheet, 3 psl.*
5.16.	Konkurentinių sesijų skaičius	Ne mažiau 7.5 milijono vienu metu.	8 milijonai vienu metu. *6400-security-gateway-datasheet, 3 psl.*
5.17.	Naujų sesijų skaičius per sekundę	Ne mažiau 80 000.	90 000. *6400-security-gateway-datasheet, 3 psl.*
5.18.	Specializuoto tinklo apsaugos įrenginio našumo skaičiavimo metodika ir vertinimas	• Specializuoto tinklo apsaugos įrenginio našumas 3.11, 3.12, 3.13 punktuose gali būti vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Turi būti pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. • Specializuoto tinklo apsaugos įrenginio našumo parametrai turi būti skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.	• Specializuoto tinklo apsaugos įrenginio našumas 3.11, 3.12, 3.13 punktuose yra vertinamas tik su realiu, įprastu vartotojų tinklams, srautu. Yra pateikiama nuoroda į viešą gamintojo skaičiavimo metodikos aprašymą. *https://pages.checkpoint.com/enterprise-security-performance.html enterprise-testing-conditions-whitepaper, 3 psl.* • Specializuoto tinklo apsaugos įrenginio našumo parametrai yra skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą. *enterprise-testing-conditions-whitepaper, 3 psl.*
Funkciniai reikalavimai			
5.19.	Darbo režimai	• Skaidrus (OSI L2); • Maršrutizavimo (OSI L3); • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;	• Skaidrus (OSI L2); *CP_R80.40_NextGenSecurityGateway_Guide, 186 psl.* • Maršrutizavimo (OSI L3); *CP_R80.40_NextGenSecurityGateway_Guide, 182 psl.* • Stebėjimo (*monitoring*), surenkant ir pasyviai analizuojant informaciją iš tinklo įrangos;

			CP_R80.40_NextGenSecurityGateway_Guide, 184 psl.
5.20.	Sistemos virtualizavimas	• Turi būti galimybė praplėsti funkcionalumą padalinant įrenginį į 10 virtualių įrenginių. • Virtualūs įrenginiai turi užtikrinti pilną valdymo, politikų izoliavimą, bei galimybę riboti virtualaus įrenginio resursų išnaudojimą. • Funkcionalumas gali būti įgyvendinamas su atskira licencija, į pasiūlymą įtraukti nereikia.	• Yra galimybė praplėsti funkcionalumą padalinant įrenginį į 10 virtualių įrenginių. *6400-security-gateway-datasheet, 3 psl.* • Virtualūs įrenginiai užtikrina pilną valdymo, politikų izoliavimą, bei galimybę riboti virtualaus įrenginio resursų išnaudojimą. *CP_R80.40_VSX_AdminGuide, 28-30 psl.* • Funkcionalumas yra įgyvendinamas su atskira licencija, kuri į pasiūlymą neįtraukta. *6400-security-gateway-datasheet, 4 psl.*
5.21.	Tinklo funkcionalumas	• Ne mažiau 1024 VLAN palaikymas. Ne mažiau 4096 VLAN naudojant virtualizaciją. • 802.3ad ryšių apjungimo (angl. „link aggregation“) funkcionalumo palaikymas. • Layer 2 ir Layer 3 maršrutizavimo funkcionalumas.	• Ne mažiau 1024 VLAN palaikymas. Ne mažiau 4096 VLAN naudojant virtualizaciją. • 802.3ad ryšių apjungimo (angl. „link aggregation“) funkcionalumo palaikymas. • Layer 2 ir Layer 3 maršrutizavimo funkcionalumas. *6400-security-gateway-datasheet, 3 psl.*
5.22.	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-SM, IGMP v2 ir v3 protokolų palaikymas.	• OSPFv2 ir v3 protokolų palaikymas. *6400-security-gateway-datasheet, 3 psl.* • BGP palaikymas, grakštaus BGP perkrovimo (angl. graceful restart) palaikymas. *CP_R80.40_ClusterXL_AdminGuide, 174 psl.* • RIP palaikymas. • Statinis maršrutizavimas, multicast maršrutizavimas, maršrutizavimas pagal

			nustatytas taisykles (angl. „policy based“). • PIM-SM, IGMP v2 ir v3 protokolų palaikymas. *6400-security-gateway-datasheet, 3 psl.*
5.23.	IPv6 palaikymas	Siūlomas įrenginys privalo palaikyti IPv6.	Siūlomas įrenginys palaiko IPv6. *6400-security-gateway-datasheet, 3 psl.*
5.24.	Tinklo adresų transliavimas (NAT)	• Statinio NAT, NAT64 ir PAT palaikymas.	• Statinio NAT, NAT64 ir PAT palaikymas. *6400-security-gateway-datasheet, 3 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 210 psl.*
5.25.	Valdymas	• WEB (HTTPS), SSH, konsolė. • SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. • Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). • IPFIX arba analogiškas protokolas gebantis eksportuoti statistinę tinklo srauto informaciją. • Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu.	• WEB (HTTPS), SSH, konsolė. *CP_R80.40_Gaia_AdminGuide, 25, 330, 379 psl.* • SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. *CP_R80.40_Gaia_AdminGuide, 206 psl.* • Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). *CP_R80.40_Installation_and_Upgrade_Guide, 25 psl.* • IPFIX arba analogiškas Netflow protokolas gebantis eksportuoti statistinę tinklo srauto informaciją. *CP_R80.40_Gaia_AdminGuide, 179 psl.* • Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu. *CP_R80.40_SecurityManagement_AdminGuide, 121 psl.* *CP_R80.40_SmartProvisioning_AdminGuide, 19 psl.*
5.26.	Sertifikatų palaikymas	• Pasirašytų sertifikatų importavimas ir naudojamų	• Pasirašytų sertifikatų importavimas ir naudojamų

		sertifikatų eksportavimas (PKCS #12). • Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas.	sertifikatų eksportavimas (PKCS #12). • Centrinio valdymo sprendimo *Certificate authority* išduotų sertifikatų palaikymas. *CP_R80.40_RemoteAccessVPN_AdminGuide, 45 psl.*
5.27.	Specializuoto tinklo apsaugos įrenginio saugos funkcijos	• Ugniasienė • Įsilaužimų prevencija (IPS) • Vartotojų atpažinimas • Aplikacijų kontrolė • Virtualūs privatūs tinklai • Šifruoto srauto (SSL/TLS) inspektavimas	• Ugniasienė • Įsilaužimų prevencija (IPS) • Vartotojų atpažinimas • Aplikacijų kontrolė • Virtualūs privatūs tinklai *6400-security-gateway-datasheet, 3psl.* • Šifruoto srauto (SSL/TLS) inspektavimas *CP_R80.40_NextGenSecurityGateway_Guide, 28, psl.*
5.28.	Įsilaužimų prevencijos (IPS) funkcionalumas	• Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai turi apimti: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. • Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant tinklo apsaugos įrenginio greitaveiką. • Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas tinklo apsaugos įrenginio apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neturi būti įjungtas pagal nutylėjimą. • Darbo režimų taisyklių rinkiniams palaikymas:	• Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai apima: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. *CP_R80.40_ThreatPrevention_AdminGuide, 29 psl.* • Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant tinklo apsaugos įrenginio greitaveiką. *CP_R80.40_ThreatPrevention_AdminGuide, 46-47 psl.* • Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas tinklo apsaugos įrenginio apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties).

		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.	Nustatymas neįjungtas pagal nutylėjimą. *CP_R80.40_ThreatPrevention_AdminGuide, 207 psl.* • Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). *CP_R80.40_ThreatPrevention_AdminGuide.pdf, 56, 215 psl.* • Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. *CP_R80.40_ThreatPrevention_AdminGuide, 252 psl.* • IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). *CP_R80.40_ThreatPrevention_AdminGuide, 192 – 205 psl.* • Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas. *CP_R80.40_NextGenSecurityGateway_Guide.pdf, 29 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 140 psl.*
5.29.	Vartotojų atpažinimo funkcionalumas	• Galimybė atpažinti bei autentifikuoti vartotojus. • Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. • Galimybė kurti vartotojų duomenų bazę specializuotame tinklo apsaugos įrenginyje. • Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių	• Galimybė atpažinti bei autentifikuoti vartotojus. *CP_R80.40_IdentityAwareness_AdminGuide, 46 psl.* • Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP, dviejų faktorių autentifikaciją. *CP_R80.40_IdentityAwareness_AdminGuide, 31, 211, 220 psl.* • Galimybė kurti vartotojų duomenų bazę specializuotame tinklo apsaugos įrenginyje. *CP_R80.40_SecurityManagement_AdminGuide, 58 psl.*

		atpažinimas bei taisyklių grupėms pritaikymas.	• Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. *CP_R80.40_IdentityAwareness_AdminGuide, 19, 32 psl.*
5.30.	Aplikacijų kontrolė	• Galimybė kurti aplikacijų taisykles naudojant kelias kategorijas vienoje taisyklėje. • Skirtingų aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. • Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms arba jų grupėms/kategorijoms: • blokuoti, • informuoti vartotojus apie nepageidaujamos aplikacijos naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. • Mechanizmas nepageidaujamų aplikacijų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. • Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos 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.	• Galimybė kurti aplikacijų taisykles naudojant kelias kategorijas vienoje taisyklėje. *CP_R80.40_NextGenSecurityGateway_Guide, 412 psl.* • Skirtingų aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. *CP_R80.40_SecurityManagement_AdminGuide, 179, 259 psl.* • Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. *CP_R80.40_SecurityManagement_AdminGuide, 177 psl.* *CP_R80.40_ThreatPrevention_AdminGuide, 175-178 psl.* • Mechanizmas nepageidaujamų aplikacijų naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. *CP_R80.40_SecurityManagement_AdminGuide, 178 psl.*

			• Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ribojimą. *CP_R80.40_ThreatPrevention_AdminGuide, 174 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 169 psl.* • Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. *CP_R80.40_SecurityManagement_AdminGuide, 163 psl.* *CP_R80.40_PerformanceTuning_AdminGuide, 36 psl.* • Automatinis aplikacijų aprašų atnaujinimas. *CP_R80.40_NextGenSecurityGateway_Guide, 44 psl.* • Galimybė aprašyti savo aplikacijas. *CP_R80.40_SecurityManagement_AdminGuide, 165 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 176 – 181 psl.* • Virš 8000 aplikacijų atpažinimas. *https://appwiki.checkpoint.com/appwikisdb/public.htm*
5.31.	Virtualūs privatūs tinklai (VPN)	• Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. certificate authority). • IPSec protokolo palaikymas. • DES, 3DES, AES128, AES256 šifravimo 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), o Group 5 (1536 bitų), o Group 14 (2048 bitų),	• Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. certificate authority). *CP_R80.40_SitetoSiteVPN_AdminGuide, 26, 85-86 psl.* • IPSec protokolo palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 48 psl.* • DES, 3DES, AES128, AES256 šifravimo standartų palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 50 psl.* • MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas.

		○ Group 19, ○ Group 20. • Palaikomos 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.	*CP_R80.40_SitetoSiteVPN_AdminGuide, 50 psl.* • Diffie-Hellman grupių palaikymas: ○ Group 1 (768 bitų), ○ Group 2 (1024 bitų), ○ Group 5 (1536 bitų), ○ Group 14 (2048 bitų), ○ Group 19, ○ Group 20. *CP_R80.40_SitetoSiteVPN_AdminGuide, 50-51 psl.* • Palaikomos virtualių privačių tinklų topologijos: ○ Tinklelis (visi taškai užmezga VPN tunelius su visais), ○ Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais), *CP_R80.40_SitetoSiteVPN_AdminGuide, 41, 156 psl.* • Galimybė nustatyti VPN tunelių būvį: ○ tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. ○ statiniai tuneliai, atnaujinami nustatytu periodiškumu. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 130 – 133 psl.* *CP_R80.40_SitetoSiteVPN_AdminGuide, 64 psl.*
5.32.	Šifruoto srauto (SSL/TLS) inspektavimas	• Šifruoto SSL ir TLS srauto dešifravimas ir patikra. • Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI). • Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas	• Šifruoto SSL ir TLS srauto dešifravimas ir patikra. *CP_R80.40_SecurityManagement_AdminGuide, 39, 274 psl.* • Taisyklių pritaikymas šifruotam srautui bei dešifravimo, naudojant serverių vardų indikatorius (SNI).

		saugos funkcijas prieš tai atlikus dešifravimą. • Perfect Forward Secrecy palaikymas.	*CP_R80.40_ThreatPrevention_AdminGuide, 256 psl.* • Šifruoto srauto patikra įgyvendina visas reikalavimuose išvardintas saugos funkcijas prieš tai atlikus dešifravimą. *CP_R80.40_SecurityManagement_AdminGuide.pdf, 281 psl.* • Perfect Forward Secrecy palaikymas. *CP_R80.40_SitetoSiteVPN_AdminGuide, 52 psl.*
5.33.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti generuojami žurnaliniai įvykiai susiję su tinklo apsaugos įrenginio funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; Turi būti galimybė nustatyti įvykio įrašymą konkrečiai tinklo apsaugos įrenginio taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams.	Įvykių žurnalai yra kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Yra generuojami žurnaliniai įvykiai susiję su tinklo apsaugos įrenginio funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; *CP_R80.40_LoggingAndMonitoring_AdminGuide, 25, 80, 88, 111 psl.* Yra galimybė nustatyti įvykio įrašymą konkrečiai tinklo apsaugos įrenginio taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 66, 68 psl.* *https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131064* *CP_R80.40_ThreatPrevention_AdminGuide.pdf – 164 psl.*

5.34.	Administratorių paskyros	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti galimybė smulkiai apibrėžti administratoriaus teises: • 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: • 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; *CP_R80.40_Gaia_AdminGuide, 269 psl.*
5.35.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Yra. Nemokamai garantinio aptarnavimo laikotarpiu *https://www.checkpoint.com/support-services/support-plans/*
5.36.	Atnaujinimai pagal nustatyta grafiką (Schedule)	Turi būti	Yra *CP_R80.40_Gaia_AdminGuide, 403 psl.*
5.37.	Garantiniai įsipareigojimai	• Gamintojo garantuojamas nemokamas garantinis aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą turi būti įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam	• Gamintojo garantuojamas nemokamas garantinis aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą yra įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam funkcionalumui įgyvendinti

		funkcionalumui įgyvendinti visam garantiniam laikotarpiui. • 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.	visam garantiniam laikotarpiui. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. • Gedimo atveju pakaitinė įranga bus pristatyta ne vėliau kaip kitą darbo dieną. *https://www.checkpoint.com/support-services/support-plans/*
4.	**Valdymo ir kontrolės sprendimas**		
4.1.	Pirkimo objektas	Valdymo ir kontrolės sprendimas, skirtas valdyti siūlomus I ir II tipo specializuotus tinklo apsaugos įrenginius.	Valdymo ir kontrolės sprendimas, skirtas valdyti siūlomus I ir II tipo specializuotus tinklo apsaugos įrenginius.
4.2.	Gamintojas	Nurodyti.	CheckPoint Software Technologies Ltd., Cisco Systems ir iFlowScreen
4.3.	Modelis	Nurodyti, įskaitant tikslius produktų kodus.	CPSM-NGSM150 - Next Generation Security Management Software for 150 gateways (SmartEvent & Compliance); CPSB-EVS-150 - SmartEvent and SmartReporter blade for 150 gateways (Smart-1 & open server) subscription; CPSB-EVS-150 - SmartEvent and SmartReporter blade for 150 gateways (Smart-1 & open server) subscription; CPCES-CO-PREMIUM-ADD - Premium Collaborative Enterprise Support. ST-FR-BUN - Cisco Stealthwatch Flow Rate Bundle; L-ST-FR-S5 - Cisco Stealthwatch Flow Rate; L-ST-SMC-VE-K9 - Cisco Stealthwatch Management Console Virtual Edition; L-LC-TI-FC4K - Cisco Stealthwatch Threat Intelligence Service Subs FC4K; ST-FC4210-K9 - Cisco Stealthwatch Flow Collector 4210;

			CON-SNT-STFC4291 - SNTC-8X5XNBD Cisco Stealthwatch Flow Collector 4210. iFLOWSCREEN-BASE; iFLOWSCREEN-NF; iFLOWSCREEN-IF; iFLOWSCREEN-SF; iFLOWSCREEN-FPS.
4.4.	Tipas	• Programinė įranga, diegiama fiziniame arba virtualiame serveryje. Turi būti palaikomos VMware ESXi ir Microsoft HyperV virtualizacijos platformos. • Sprendimas gali būti įgyvendintas vienu arba kelių programinės įrangos serverių/sprendimo pagalba. • Sprendimas turi veikti kliento infrastruktūroje. • Siūlomai programinei įrangai, užsakovas savo turimoje VMware ESXi virtualizacijos platformoje gali skirti ne daugiau 200 GB RAM, 8 TB vietos diske, 20 vCPU. Jei reikalavimams įgyvendinti šių resursų neužtenka, tiekėjas turi pristatyti gamintojo patvirtintą reikalavimus tenkinančią fizinę įrangą.	• Programinė įranga, diegiama fiziniame arba virtualiame serveryje. Yra palaikomos VMware ESXi ir Microsoft HyperV virtualizacijos platformos. *CP_R80.40_ReleaseNotes, 25 psl.* • Sprendimas yra įgyvendintas CheckPoint ir Cisco programinės įrangos serverių/sprendimo pagalba. • Sprendimas veiks kliento infrastruktūroje. • Siūlomai programinei įrangai užteks užsakovo turimoje VMware ESXi virtualizacijos platformoje skiriamos 200 GB RAM, 8 TB vietos diske, 20 vCPU. Jei reikalavimams įgyvendinti šių resursų neužteks, tiekėjas pristatys gamintojo patvirtintą reikalavimus tenkinančią fizinę įrangą. *CP_R80.40_ReleaseNotes, 31 psl.* *SW_7_1_1_Installation_and_Configuration_Guide_DV_4_0, 17 psl.* *iFlowScreen datasheet en v1.0, 3 psl.* *SW_FC_4210_Spec_Sheet_DV_1_1, 4 psl.*
4.5.	Valdomi įrenginiai	• Siūlomas sprendimas turi gebėti pilnai valdyti siūlomus specializuotus tinklo apsaugos įrenginius ir turėti visas reikiamas tam licencijas.	• Siūlomas sprendimas geba pilnai valdyti siūlomus specializuotus tinklo apsaugos įrenginius ir turi visas reikiamas tam licencijas.

		• Sprendimas turi be papildomų licencijų leisti valdyti visą sprendimą apimančius specializuotus tinklo apsaugos įrenginius ir modulius. • Sprendimas turi būti pilnai suderinamas su siūlomais specializuotais tinklo apsaugos įrenginiais. Siūlant kito gamintojo sprendimą privaloma pateikti oficialų tinklo apsaugos įrenginio gamintojo patvirtinimą dėl pilno suderinamumo. Suderinamumas turi apimti ir bendrą garantinį aptarnavimą.	• Sprendimas be papildomų licencijų leidžia valdyti visą sprendimą apimančius specializuotus tinklo apsaugos įrenginius ir modulius. • Sprendimas yra pilnai suderinamas su siūlomais specializuotais tinklo apsaugos įrenginiais. Suderinamumas apima ir bendrą garantinį aptarnavimą. *security-management-suite-datasheet, 2-3 psl.* *CP_6000_7000_Appliances_GettingStartedGuide, 31-32 psl.*
4.6.	Valdymas	• Sprendimas turi būti valdomas per grafinę sąsają. • Turi būti galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. • Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. • Turi būti galimybė smulkiai apibrėžti administratoriaus teises: o teisė keisti sisteminius įrenginio nustatymus; o teisė kurti, keisti saugumo taisykles; o teisė kurti, keisti taisyklių objektus; o teisė konfigūruoti saugumo patikrų nustatymus; o teisė peržiūrėti įvykių žurnalus; o teisė peržiūrėti ataskaitas; o teisė generuoti ataskaitas.	• Sprendimas yra valdomas per grafinę sąsają. *CP_R80.40_SecurityManagement_AdminGuide 33 psl.* • Yra galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. *security-management-suite-datasheet, 2, 3 psl.* • Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. *CP_R80.40_Gaia_AdminGuide, 269 psl.* • Yra galimybė smulkiai apibrėžti administratoriaus teises: o teisė keisti sisteminius įrenginio nustatymus; o teisė kurti, keisti saugumo taisykles; o teisė kurti, keisti taisyklių objektus; o teisė konfigūruoti saugumo patikrų nustatymus; o teisė peržiūrėti įvykių žurnalus;

		• Turi būti galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams. • Turi veikti mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą. • Administratorių įgyvendinami pokyčiai turi būti detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus.	o teisė peržiūrėti ataskaitas; o teisė generuoti ataskaitas. *CP_R80.40_SecurityManagement_AdminGuide, 111-113 psl.* • Yra galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams. *security-management-suite-datasheet, 2psl.* • Veikia mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 113 psl.* • Administratorių įgyvendinami pokyčiai yra detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 25, 38 psl.*
4.7.	Centralizuotas valdymas	Centralizuoto valdymo funkcionalumas turi pilnai valdyti siūlomus specializuotus tinklo apsaugos įrenginius, įskaitant: • Specializuoto tinklo apsaugos įrenginio funkcijas. • IPS funkcijas. • Aplikacijų kontrolės funkcijas. • URL filtravimo funkcijas. • Bot aptikimo funkcijas. • Antivirusinio srauto filtravimo funkcijas. • Tinklo ir maršrutizavimo funkcijas. • Administratorių paskyras. Centralizuotam valdymui turi būti naudojama saugi, šifruota	Centralizuoto valdymo funkcionalumas pilnai valdys siūlomus specializuotus tinklo apsaugos įrenginius, įskaitant: • Specializuoto tinklo apsaugos įrenginio funkcijas. • IPS funkcijas. • Aplikacijų kontrolės funkcijas. • URL filtravimo funkcijas. • Bot aptikimo funkcijas. • Antivirusinio srauto filtravimo funkcijas. • Tinklo ir maršrutizavimo funkcijas. • Administratorių paskyras. *security-management-suite-datasheet, 1, 3 psl.* *CP_R80.40_SecurityManagement_AdminGuide, 35 psl.*

		komunikacija su specializuotais tinklo apsaugos įrenginiais.	Centralizuotam valdymui yra naudojama saugi, šifruota komunikacija su specializuotais tinklo apsaugos įrenginiais. *CP_R80.40_SecurityManagement_ AdminGuide, 123 psl.*
4.8.	Tinklo srautų statistinės informacijos ir žurnalinių įvykių surinkimas ir stebėjimas	• Sprendimas turi kaupti žurnalinius įvykius iš valdomų specializuotų tinklo apsaugos įrenginių. • Turi priimti iš trečių šalių įrenginių NetFlow, IPFIX ir sFlow formatų srautus. • Turi būti automatiškai aptinkami ir nufiltruojami tie NetFlow, IPFIX ir sFlow srautai, kurie kartojasi iš kelių įrenginių. • Turi būti ataskaitų funkcionalumas, leidžiantis ruošti ataskaitas pagal bet kokią su įrenginiu funkcionalumu susijusią sukauptą istorinę informaciją, vertinant bet kokius rėžius ir informaciją, įskaitant, bet neapsiribojant, vartotojus, jų grupes, įrenginius, aptiktas grėsmes, lankytas svetaines, incidentus ir pan.	• Sprendimas kaupia žurnalinius įvykius iš valdomų specializuotų tinklo apsaugos įrenginių. *CP_R80.40_LoggingAndMonitoring _AdminGuide 62 psl.* • Priima iš trečių šalių įrenginių NetFlow, IPFIX ir sFlow formatų srautus. *datasheet-ent-c78-739398, 5-6 psl.* • Automatiškai aptinka ir nufiltruoja tuos NetFlow, IPFIX ir sFlow srautus, kurie kartojasi iš kelių įrenginių. *datasheet-ent-c78-739398, 6 psl.* • Yra ataskaitų funkcionalumas, leidžiantis ruošti ataskaitas pagal bet kokią su įrenginiu funkcionalumu susijusią sukauptą istorinę informaciją, vertinant bet kokius rėžius ir informaciją, įskaitant, bet neapsiribojant, vartotojus, jų grupes, įrenginius, aptiktas grėsmes, lankytas svetaines, incidentus ir pan. *CP_R80.40_LoggingAndMonitoring _AdminGuide, 42 psl.*
4.9.	Našumas ir žurnalinių įvykių apimtis	• Sprendimas turi priimti ir apdoroti ne mažiau kaip 100 GB žurnalinių įvykių per dieną. • Siūlomų specializuotų tinklo apsaugos įrenginių kaupiamų ir saugomų žurnalinių įvykių apimtis ne mažiau 5 TB, plius kaupiamų NetFlow, IPFIX ir	• Sprendimas priima ir apdoroja ne mažiau kaip 100 GB žurnalinių įvykių per dieną. *https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk98767#Sizing* • Siūlomų specializuotų tinklo apsaugos įrenginių

		sFlow srautų kaupiamų ir saugomų įvykių apimtis ne mažiau 5 TB. • Surenkamam NetFlow, IPFIX ir sFlow srautui turi būti dedikuota ne mažiau 3 TB disko vietos. • NetFlow, IPFIX ir sFlow surinkimui siūlomos fizinės arba virtualios aparatinės įrangos našumas turi būti ne mažesnis nei 150000 srautų per sekundę (angl. flows per second). • Sprendimas turi priimti ne mažiau nei 50000 NetFlow, IPFIX ir sFlow srautų per sekundę (angl. flows per second). Užsakovo tinkle šį maksimalų srautų skaičių per sekundę sudaro aktualūs ir neaktualūs srautai. Aktualus srautas sudaro ne daugiau 20% viso srauto. • Įsigyjamo sprendimo tikslas - priimti 50000 NetFlow, IPFIX ir sFlow srautų per sekundę ir analizuoti tik aktualų srautą. Aktualų srautą nuo neaktualaus galima rūšiuoti pagal 3 parametrus vienu metu: siuntėjo/gavėjo IP adreso, MPLS žymos, įrenginio gavimo/siuntimo tinklo prievado.	kaupiamų ir saugomų žurnalinių įvykių apimtis 5 TB, plius kaupiamų NetFlow, IPFIX ir sFlow srautų kaupiamų ir saugomų įvykių apimtis 7,2 TB. *CP_R80.40_ReleaseNotes, 16 psl.* *SW_FC_4210_Spec_Sheet_DV_1_1, 4 psl.* • Surenkamam NetFlow, IPFIX ir sFlow srautui yra dedikuota 4 TB disko vietos. *SW_FC_4210_Spec_Sheet_DV_1_1, 4 psl.* • NetFlow, IPFIX ir sFlow surinkimui siūlomos fizinės arba virtualios aparatinės įrangos našumas yra 200000 srautų per sekundę (angl. flows per second). *SW_FC_4210_Spec_Sheet_DV_1_1, 3 psl.* • Sprendimas priima 50000 NetFlow, IPFIX ir sFlow srautų per sekundę (angl. flows per second). Užsakovo tinkle šį maksimalų srautų skaičių per sekundę sudaro aktualūs ir neaktualūs srautai. Aktualus srautas sudaro ne daugiau 20% viso srauto. *iFlowScreen datasheet en v1.0, 2, 3 psl.* • Sprendimas priima 50000 NetFlow, IPFIX ir sFlow srautų per sekundę ir analizuoja tik aktualų srautą. Aktualų srautą nuo neaktualaus filtruoja iFlowScreen pagal 3 parametrus vienu metu: siuntėjo/gavėjo IP adreso, MPLS žymos, įrenginio

			gavimo/siuntimo tinklo prievado. *SW_7_2_Stealthwatch_and_Cognitive_Analytics_Configuration_Guide_DV_1_0, 4 psl.* *iFlowScreen datasheet en v1.0, 2, 3 psl.*
4.10.	Centralizuoto konfigūravimo funkcionalumas	Administravimo veiklų planavimo ir automatizavimo funkcionalumas konfigūravimo skriptų paleidimui, konfigūracijų atsarginių kopijų darymui, įrenginių perkrovimui, atnaujinimui.	Administravimo veiklų planavimo ir automatizavimo funkcionalumas konfigūravimo skriptų paleidimui, konfigūracijų atsarginių kopijų darymui, įrenginių perkrovimui, atnaujinimui. *CP_R80.40_SecurityManagement_AdminGuide, 44 psl.*
4.11.	Stebėjimo funkcionalumas	• Turi būti centralizuoto įrenginių stebėjimo funkcionalumas. • Surenkamuose NetFlow, IPFIX ir sFlow srautuose turi būti galimybė matyti tokią informaciją: o IP įrenginiai ir jų grupės. o Tinklo įrenginiai ir informacija apie jų tinklo prievadus. o DSCP žymėmis pažymėtas srautas. o Įrenginiais keliaujantis srautas – aplikacijos, prievadų apkrautumas, aktyvios sesijos. • Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos stebėjimas, bei automatinis pranešimų administratoriams pateikimas.	• Yra centralizuoto įrenginių stebėjimo funkcionalumas. *CP_R80.40_SecurityManagement_AdminGuide, 121 psl.* • Surenkamuose NetFlow, IPFIX ir sFlow srautuose yra galimybė matyti tokią informaciją: o IP įrenginiai ir jų grupės. o Tinklo įrenginiai ir informacija apie jų tinklo prievadus. o DSCP žymėmis pažymėtas srautas. o Įrenginiais keliaujantis srautas – aplikacijos, prievadų apkrautumas, aktyvios sesijos. *SW_7_2_1_Stealthwatch_Desktop_Client_User_Guide_DV_2_0, 83, 59, 97, 145 psl.* • Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos stebėjimas, bei automatinis pranešimų administratoriams pateikimas. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 85, 107, 110 psl.*
4.12.	Grėsmių aptikimo ir	• Turi būti grėsmių aptikimo funkcionalumas.	• Yra grėsmių aptikimo funkcionalumas.

	analizės funkcionalumas	• Įvykių koreliavimo funkcionalumas aptinkant grėsmes ir incidentus, susiejant įvykius iš skirtingų įrenginių. • Surenkamuose NetFlow, IPFIX ir sFlow srautuose turi būti galimybė matyti tokius saugumo įvykius: o DDoS atakos. o Botnet tinklų aptikimas. o Duomenų nutekinimas. o SYN atakos. • Automatizuotas administratorių informavimas apie grėsmes ir incidentus. • Incidentų ir grėsmių analizės funkcionalumas, pateikiant išsamią informaciją apie įvykį, įgyvendinant konkrečių įvykių paiešką, bei įgalinant administratorių imtis veiksmų sulaikant grėsmes bei stabdant incidentus. • Turi būti naudojami AI giliojo mokymosi (angl. deep learning arba neural network) metodai. Informacija apie srautus turi būti pateikiama iš anksto apmokytam neuroniniam kompiuteriniam tinklui, kuris pagal įvesties duomenis turi gebėti aptikti tinklo anomalijas. • Informacijos iš valdomų tinklo apsaugos įrenginių, IPS, antivirusinės srauto kontrolės, bot aptikimo, URL filtravimo ir aplikacijų kontrolės modulių surinkimo funkcionalumas.	*CP_R80.40_ThreatPrevention_AdminGuide, 28 psl.* • Įvykių koreliavimo funkcionalumas aptinkant grėsmes ir incidentus, susiejant įvykius iš skirtingų įrenginių. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 81-82 psl.* • Surenkamuose NetFlow, IPFIX ir sFlow srautuose yra galimybė matyti tokius saugumo įvykius: o DDoS atakos. o Botnet tinklų aptikimas. o Duomenų nutekinimas. o SYN atakos. *SW_7_2_1_Stealthwatch_Desktop_Client_User_Guide_DV_2_0, 96, 190, 280, 278 psl.* • Automatizuotas administratorių informavimas apie grėsmes ir incidentus. *CP_R80.40_LoggingAndMonitoring_AdminGuide 85 psl.* • Incidentų ir grėsmių analizės funkcionalumas, pateikiant išsamią informaciją apie įvykį, įgyvendinant konkrečių įvykių paiešką, bei įgalinant administratorių imtis veiksmų sulaikant grėsmes bei stabdant incidentus. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 66 psl.* • Yra naudojami AI giliojo mokymosi (angl. deep learning arba neural network) metodai. Informacija apie srautus yra pateikiama iš anksto apmokytam neuroniniam kompiuteriniam tinklui, kuris pagal įvesties

			duomenis geba aptikti tinklo anomalijas. *white-paper-c11-740605, 4, 6 psl.* • Informacijos iš valdomų tinklo apsaugos įrenginių, IPS, antivirusinės srauto kontrolės, bot aptikimo, URL filtravimo ir aplikacijų kontrolės modulių surinkimo funkcionalumas. *CP_R80.40_LoggingAndMonitoring_AdminGuide, 75, 163, 129, 134 psl.*
4.13.	Automatizavimas	• Turi būti galimybė pagal nustatytą politiką, aptikus grėsmes, nustačius atakas, automatiškai riboti srautus, automatiškai diegti griežtos kontrolės politikas. • Turi būti galimybė integruoti valdymą su VMware vCenter, automatiniam vCenter objektų įkėlimui. Įkeliami objektai turi apimti virtualias ir fizines mašinas (*virtual machines, hosts*), virtualius duomenų diskus (*datastore*), tinklus (*networks*), vSphere vApp informaciją, resursų grupes (*resource pool*), aplankus (*folder*). Įkeliama informacija turi apimti objektų IP, pastabas ir kelius iki objekto (URI). • Informacija valdymo serveryje turi būti periodiškai sinchronizuojama su vCenter informacija. • Turi būti galimybė valdyti sprendimą per WEB API.	• Yra galimybė pagal nustatytą politiką, aptikus grėsmes, nustačius atakas, automatiškai riboti srautus, automatiškai diegti griežtos kontrolės politikas. *CP_R80.40_PerformanceTuning_AdminGuide, 36 psl.* • Yra galimybė integruoti valdymą su VMware vCenter, automatiniam vCenter objektų įkėlimui. Įkeliami objektai apima virtualias ir fizines mašinas (*virtual machines, hosts*), virtualius duomenų diskus (*datastore*), tinklus (*networks*), vSphere vApp informaciją, resursų grupes (*resource pool*), aplankus (*folder*). Įkeliama informacija apima objektų IP, pastabas ir kelius iki objekto (URI). *CP_R80.40_CloudGuard_Controller_AdminGuide, 35 psl.* • Informacija valdymo serveryje yra periodiškai sinchronizuojama su vCenter informacija. *CP_R80.40_CloudGuard_Controller_AdminGuide, 48 psl.* • Yra galimybė valdyti sprendimą per WEB API.

			CP_R80.40_CloudGuard_Controller_AdminGuide, 15 psl.
4.14.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu.	Yra. Nemokamai garantinio aptarnavimo laikotarpiu. *https://www.checkpoint.com/support-services/support-plans/*
4.15.	Atnaujinimai pagal nustatytą grafiką (Shedule)	Turi būti	Yra *CP_R80.40_Gaia_AdminGuide, 403 psl.*
4.16.	Garantiniai įsipareigojimai	• Gamintojo garantuojamas nemokamas aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą turi būti įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.	• Gamintojo garantuojamas nemokamas aptarnavimas. • Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu. • Į pasiūlymą yra įtrauktos visos reikiamos licencijos ir parašų prenumeratos (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. *https://www.checkpoint.com/support-services/support-plans/*
5.	**Technologinio tinklo specializuotas apsaugos ir kontrolės sprendimo garantijos ir palaikymo pratęsimas 12 mėn.**		
5.1.	Pirkimo objektas	Technologinio tinklo specializuoto apsaugos ir kontrolės sprendimo visos techninės ir programinės įrangos licencijų, gamintojų garantijos ir palaikymo pratęsimas sprendimo eksploatavimo 37-48 mėnesiais.	Technologinio tinklo specializuoto apsaugos ir kontrolės sprendimo visos techninės ir programinės įrangos licencijų, gamintojų garantijos ir palaikymo pratęsimas sprendimo eksploatavimo 37-48 mėnesiais.

5.2.	Apimtis	Visų siūlomų įrenginių ir programinės įrangos garantija turi būti užtikrina gamintojo garantijos paketais. Gamintojo garantijos paketai turi apimti: a) Programinės įrangos palaikymą (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas); b) Teisę kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu; c) Visas reikiamas licencijas ir parašų prenumeratas (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui; d) Sugedusios techninės įrangos keitimą.	Visų siūlomų įrenginių ir programinės įrangos garantija yra užtikrinama gamintojo garantijos paketais. Gamintojo garantijos paketai apima: a) Programinės įrangos palaikymą (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas); b) Teisę kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu; c) Visas reikiamas licencijas ir parašų prenumeratas (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui; d) Sugedusios techninės įrangos keitimą. *https://www.checkpoint.com/support-services/support-plans/*
6.	**Technologinio tinklo specializuotas apsaugos ir kontrolės sprendimo garantijos ir palaikymo pratęsimas papildomiems 12 mėn.**		
5.1.	Pirkimo objektas	Technologinio tinklo specializuoto apsaugos ir kontrolės sprendimo visos techninės ir programinės įrangos licencijų, gamintojų garantijos ir palaikymo pratęsimas sprendimo eksploatavimo 49-60 mėnesiais.	Technologinio tinklo specializuoto apsaugos ir kontrolės sprendimo visos techninės ir programinės įrangos licencijų, gamintojų garantijos ir palaikymo pratęsimas sprendimo eksploatavimo 49-60 mėnesiais.
5.2.	Apimtis	Visų siūlomų įrenginių ir programinės įrangos garantija turi būti užtikrina gamintojo garantijos paketais. Gamintojo garantijos paketai turi apimti: a) Programinės įrangos palaikymą (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas);	Visų siūlomų įrenginių ir programinės įrangos garantija yra užtikrinama gamintojo garantijos paketais. Gamintojo garantijos paketai apima: a) Programinės įrangos palaikymą (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas);

		b) Teisę kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu; c) Visas reikiamas licencijas ir parašų prenumeratas (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui; d) Sugedusios techninės įrangos keitimą.	b) Teisę kreiptis iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu arba telefonu; c) Visas reikiamas licencijas ir parašų prenumeratas (angl. subscriptions) išvardintam funkcionalumui įgyvendinti visam garantiniam laikotarpiui; d) Sugedusios techninės įrangos keitimą. *https://www.checkpoint.com/support-services/support-plans/*