[redacted]

KERTINIS VALSTYBĖS TELEKOMUNIKACIJŲ CENTRAS

Biudžetinė įstaiga. Gedimino pr. 40, LT-01110 Vilnius
Tel. (8 5) 239 17 08, faks. (8 5) 279 13 31, el. p.: info@kvtc.gov.lt, www.kvtc.gov.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 121738687

TVIRTINU
BĮ Kertinio valstybės
telekomunikacijų centro direktorius
Evaldas Serbenta

NUOTOLINIO PRISIJUNGIMO PLATFORMOS TECHNINĖ SPECIFIKACIJA

1 Įvadas

Kertinis valstybės telekomunikacijų centras įgyvendindamas savo tikslus ir misiją siekia teikti patikimas Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) paslaugas valstybinėms institucijoms, todėl inicijuoja naujų nuotolinės prieigos paslaugų sukūrimo projektą (toliau – projektas) ir tuo tikslu numato įsigyti nuotolinio prisijungimo platformos sprendimą, kuriuo bus teikiamos VPN (angl. *Virtual Private Network*) prieigos prie institucijos tinklo ir saugios trečių šalių prieigos paslaugos. Šiame dokumente pateikiami reikalavimai nuotolinio prisijungimo platformai, jos sudedamosioms dalims, įrangai, funkcionalumui, apibrėžiamos paslaugos, kurias numatoma teikti naudojantis nuotolinio prisijungimo platforma. Reikalavimai nuotolinio prisijungimo platformai ir joje numatomoms teikti paslaugoms pateikiami šiuose techninės specifikacijos skyriuose:

1. Paslaugų, kurias šiuo projektu siekiama sukurti ir teikti, aprašymas (skyrius Nr. 3);
2. Paslaugų teikimui reikalingo sprendimo architektūros, už kurios įgyvendinimą bus atsakingi tiekėjai, aprašymas (skyrius Nr. 4);
3. Sprendimo komponentų techninių reikalavimų aprašymas (skyrius Nr. 5);
4. Reikalavimai projekto apimtyje įsigyjamoms paslaugoms (skyrius Nr. 6).

2 Terminai

- Tiekėjas – įmonė, kuri bus atsakinga už šiame dokumente aprašytų paslaugų ir sprendimo įgyvendinimą, priežiūrą ir palaikymą.
- KVTC – Kertinis valstybės telekomunikacijų centras.
- Perkančioji organizacija – KVTC planuojanti įsigyti šiame dokumente apibrėžtas paslaugas.
- Prekė – numatomas įsigyti nuotolinio prisijungimo platformos sprendimas.
- Paslauga – objektas, kurį gali užsisakyti paslaugos gavėjas.

- Paslaugos atvejis – paslaugos gavėjo užsakyta ir jam teikiama paslauga. Pavyzdžiui, KVTC teikia VPN prieigos paslaugą, o konkrečiai institucijai teikiama VPN priežiūros paslauga yra paslaugos atvejis.
- Paslaugos tiekėjas – institucija, užtikrinanti paslaugos teikimą paslaugos gavėjui. Šiuo atveju visų paslaugų teikėjas yra KVTC.
- Paslaugos gavėjas – institucija, kuriai KVTC teikia užsakytą paslaugą.
- Paslaugos naudotojas – paslaugų gavėjo darbuotojas ar kitas asmuo, kuris naudojasi paslaugos teikiamu funkcionalumu. Pavyzdžiui, įstaigos darbuotojas naudojasi KVTC teikiama VPN prieigos paslauga.
- Paslaugos administratorius – paslaugų gavėjo darbuotojas atsakingas už paslaugos parametrų valdymą. Pavyzdžiui, įstaigos darbuotojas, kuris valdo VPN prieigos paslaugų naudotojų paskyras.
- Saugusis tinklas – KVTC teikiama Saugaus valstybinio duomenų perdavimo tinklo, uždaro nuo bendrojo naudojimo tinklų (angl. *Internet*), paslauga, teikiama kitoms valstybinėms institucijoms, įrašytoms į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą.
- IdP (angl. *identity provider*) – Tapatybių valdymo tarnyba leidžianti SAML/OIDC ir kitais protokolais identifikuoti ir autentifikuoti Saugiojo tinklo naudotojus (jų paskyras).
- KVTC administratorius – KVTC atstovas administruojantis teikiamas paslaugas ir jos teikimui naudojamus komponentus.
- IS – informacinė sistema.
- OTP – (angl. *one time password*) vienkartinis slaptažodis.
- PĮ – programinė įranga.

3 Paslaugų aprašymas

Žemiau yra pateikiamas paslaugų, kurias siekiama sukurti ir teikti nuotolinio valdymo platformoje šio projekto apimtyje, aprašymas. Tiekėjas turės sukurti sprendimą ir įgyvendinti šias paslaugas, bei užtikrinti šių paslaugų teikimo priežiūrą bei palaikymą.

3.1 VPN prieiga prie institucijos tinklo

Nr.	Savybė	Aprašymas
3.1.1.	Pavadinimas	VPN prieiga prie organizacijos tinklo.
3.1.2.	Aprašymas	Paslauga skirta institucijoms (paslaugų gavėjams) suteikti savo darbuotojams (paslaugų naudotojams) saugią nuotolinę prieigą prie jų turimų IS ir registrų bei kitų informacinių išteklių, būtinų darbuotojų funkcijoms atlikti.
3.1.3.	Paslaugos gavėjai	Saugųjį tinklą naudojanti viešo sektoriaus institucija, kuriai KVTC teikia paslaugą.
3.1.4.	Paslaugos naudotojai	Paslaugos gavėjo darbuotojai.
3.1.5.	Būtina sąlyga	Paslaugų gavėjas turi naudotis KVTC Saugiojo tinklo paslauga.
3.1.6.	Užsakymas	Paslauga užsakoma per KVTC pagalbos tarnybą.
3.1.7.	Savybės	Paslaugų naudotojų autentifikavimui paslaugos gavėjas gali pasirinkti vieną iš šių autentifikavimo mechanizmų: • Paslaugos gavėjo autentifikavimo priemonės, palaikančios SAML v2 ir OIDC autentifikavimo federavimo protokolus. LDAP protokolas paskyros naudotojo vardo ir slaptažodžio, valdomo paslaugos gavėjo priemonėmis, tikrinimui negali būti naudojamas.

		• KVTC autentifikavimo priemonės – naudotojo vardas, slaptažodis ir vienkartinis slaptažodis. Turi būti užtikrinta, kad prisijungimui naudojant VPN kliento PĮ, tarp paslaugos naudotojo įrenginio ir paslaugos gavėjo infrastruktūros nebūtų naudojamas adresų transliavimas (toliau – NAT), taip užtikrinant suderinamumą su paslaugų gavėjo infrastruktūroje veikiančiais informaciniais ištekliais. Paslaugos apimtyje yra valdoma tik paslaugos naudotojo teisė prisijungti prie paslaugos gavėjo tinklo. Detali tinklo lygio prieigos kontrolė (kuris paslaugos naudotojas kokius išteklius gali pasiekti) yra valdoma paslaugų gavėjo priemonėmis.
3.1.8.	Paslaugos naudotojo sąsaja	Paslaugos naudotojui turi būti suteikti du prisijungimo prie paslaugos gavėjo IT infrastruktūros būdai: • Naudojant VPN kliento PĮ, diegiamą paslaugos naudotojo kompiuteryje. VPN kliento PĮ yra suteikiama paslaugos apimtyje. VPN kliento PĮ turi būti suderinama su šiomis operacinėmis sistemomis: a. Microsoft Windows 10 (32-bit ir 64-bit); b. Microsoft Windows 11 (64-bit); c. macOS 10.15 ir naujesnėmis; d. iOS 15 ir naujesnėmis; e. Android 11 ir naujesnėmis. • Naudojant standartinę naršyklę be papildomai diegiamų įskiepių. Šis prisijungimo būdas turi palaikyti šias naršykles: a. Google Chrome, b. Firefox, c. Microsoft Edge. Naudojant naršyklę turi būti galimybė pasiekti paslaugų gavėjo informacinius išteklius mažiausiai šiais protokolais: • HTTP/HTTPS; Paslaugos apimtyje paslaugos naudotojui turi būti suteiktos savitarnos priemonės, veikiančios žiniatinklio technologijų pagrindu ir leidžiančios atlikti šiuos veiksmus su KVTC paskyra (negalioja paslaugos gavėjo valdomoms paskyroms): • pasikeisti KVTC paskyros slaptažodį; • susikonfigūruoti OTP.
3.1.9.	Paslaugos administratoriaus sąsaja	**Paskyrų valdymas.** Paslaugos gavėjo paslaugos administratoriui turi būti suteiktos šios KVTC paskyrų valdymo priemonės (netaikoma, jei naudojamos paslaugos gavėjo autentifikavimo priemonės): • Paslaugų administratoriaus grafinė vartotojo sąsaja veikianti žiniatinklio technologijomis, leidžianti: sukurti, ištrinti, užrakinti, atrakinti naudotojų paskyras bei pakeisti slaptažodį; • Automatinis paslaugos naudotojo paskyrų sinchronizavimas su paslaugos gavėjo LDAP (angl. Lightweight Directory Access Protocol) direktorija; • Automatinis paslaugų naudotojų paskyrų sinchronizavimas naudojant CSV, JSON, YAML formatų failus. Naudojant automatinį paskyrų sinchronizavimą gali būti valdomos tik paskyros ir naudotojų atributai, bet ne slaptažodžiai. Automatinio paskyrų valdymo atveju, turi būti naudojamas pirmo prisijungimo nuorodos, išsiųstos paslaugos naudotojo el. pašto adresu, su reikalavimu sukurti slaptažodį ir susikonfigūruoti OTP pirmo prisijungimo metu, mechanizmas. Gali būti naudojami ir kiti panašūs mechanizmai, suderinti su perkančiąja organizacija paslaugos įgyvendinimo metu.

		Žurnalai. Paslaugų naudotojų prisijungimų žurnalinus įrašus paslaugos administratorius galės gauti kreipęsis į KVTC pagalbos tarnybą.
3.1.10.	Našumas	Turi būti užtikrinti šie paslaugos našumo parametrai: • ne mažiau nei 20 000 unikalių paslaugos naudotojų, • ne mažiau nei 10 000 vienu metu prisijungusių paslaugų naudotojų, • nemažiau nei 500 paslaugų gavėjų, • nemažiau nei 16 Gb/s bendra visų prisijungusių paslaugos naudotojų duomenų srautą.
3.1.11.	Našumo plečiamumas	Ateityje turi būti galimybė, nekeičiant sprendimo architektūros ir esamų sprendimo komponentų, o tik įsigyjant ir įdiegiant papildomus techninės ar programinės įrangos komponentus, išplėsti paslaugos našumą taip, kad būtų užtikrinta: • ne mažiau nei 50 000 unikalių paslaugos naudotojų, • nemažiau nei 20 000 vienu metu prisijungusių paslaugų naudotojų, • nemažiau nei 800 paslaugų gavėjų, • nemažiau nei 32 Gb/s bendra visų prisijungusių paslaugos naudotojų duomenų srautą.
3.1.12.	Paslaugų kokybės reikalavimai (SLA)	Metinis paslaugos pasiekiamumas ne mažiau nei 99,7%

3.2 Saugi trečių šalių prieiga

Nr.	Pavadinimas	Aprašymas
3.2.1.	Pavadinimas	Saugi trečių šalių prieiga.
3.2.2.	Aprašymas	Paslauga yra skirta institucijoms (paslaugos gavėjams) suteikti saugią nuotolinę prieigą prie tam tikro informacinio ištekliaus (pvz. operacinės sistemos) trečių šalių specialistams, vykdantiems sistemų administravimo, priežiūros ir palaikymo darbus. Paslaugos apimtyje suteikiama prieiga prie vieno informacinio ištekliaus. Paslaugos gavėjas turi užsakyti paslaugą kiekvienam informaciniam ištekliui, prie kurio reikia suteikti prieigą trečios šalies specialistui.
3.2.3.	Paslaugos gavėjas	Saugųjį tinklą naudojanti viešo sektoriaus organizacija, kuriai KVTC teikia paslaugą.
3.2.4.	Paslaugos naudotojas	Paslaugos gavėjo IS, registrus ar kitus informacinius išteklius prižiūrinčių, diegiančių ar kitas informacinių technologijų paslaugas paslaugų gavėjui teikiančių trečių šalių darbuotojai.
3.2.5.	Būtinos sąlygos	Paslaugų gavėjas naudojasi KVTC Saugiojo tinklo paslauga.
3.2.6.	Savybės	Paslaugų naudotojų autentifikavimui paslaugos gavėjas gali pasirinkti vieną iš šių autentifikavimo mechanizmų: • Paslaugos naudotojo organizacijos (trečios šalies) autentifikavimo priemonės, palaikančios SAML v2 ir OIDC autentifikavimo federavimo protokolus. LDAP protokolas naudotojo paskyros vardo ir slaptažodžio, tikrinimui negali būti naudojamas. • KVTC autentifikavimo priemonės – naudotojo vardas, slaptažodis ir vienkartinis slaptažodis. • Paslaugos gavėjo autentifikavimo priemonės, palaikančios SAML v2 ir OIDC autentifikavimo federavimo protokolus. Šiuo atveju paslaugų gavėjas turėtų suteikti paslaugos naudotojui paskyrą ir autentifikavimo priemones. Paslaugų naudotojų autentifikavimui (naudotojo vardo ir slaptažodžio tikrinimui), kai paskyra yra valdoma paslaugų gavėjo ar paslaugų naudotojo

Nr.	Pavadinimas	Aprašymas
		organizacijos autentifikavimo priemonėmis, negali būti naudojamas LDAP protokolas. Prieiga prie apsaugotų informacinių ištekių turi būti realizuota taip, kad nebūtų atskleidžiama nei vidinė KVTC, nei paslaugų gavėjo tinklo infrastruktūra. Pavyzdžiui, naudojamas PROXY sujungimo būdas, kai paslaugos naudotojas jungiasi į tarpinę stotį, o tarpinė stotis inicijuoja tinklo sujungimą su apsaugotu IT ištekliumi. Paslaugos gavėjas gali pasirinkti iš žemiau pateiktų išteklių tipų: • Windows Server OS prisijungimas RDP protokolu; • Linux OS prisijungimas SSH protokolu; • prisijungimas prie įrenginių, palaikančių SSH, protokolą. Suteikiant prieigą prie apsaugoto ištekliaus, turi būti užtikrinama, kad: • prieigos sesija bus ribojama laike; • jeigu galutinio ištekliaus techninės galimybės leidžia, paslaugos naudotojas nežinos prisijungimo prie apsaugoto ištekliaus naudotojo slaptažodžio; • jei prisijungimas atliekamas RDP protokolu, bus įrašyta visa sujungimo sesija; • jei prisijungimas atliekamas SSH protokolu, bus įrašytos visos komandos vykdytos sesijos metu. Prieiga prie išteklių turi būti suteikta nenaudojant agentų ar kitos programinės įrangos. Paslaugų gavėjai turi būti suskirstyti į logines grupes, kad nematytų kitų paslaugos gavėjų.
3.2.7.	Paslaugos naudotojo sąsaja	Paslaugos naudotojui turi būti suteikta prisijungimo sesijų valdymo grafinė sąsaja veikianti žiniatinklio priemonėmis ir nereikalaujanti atskiro VPN sujungimo su KVTC infrastruktūra. Sąsaja turi leisti: • matyti apsaugotus išteklius, prie kurių paslaugos naudotojas gali prisijungti; • aktyvuoti prisijungimo sesiją; • deaktyvuoti prisijungimo sesiją; • prašyti\pratęsti leidimą prisijungti prie norimos sistemos; • peržiūrėti prašymo prisijungti prie sistemos būseną. Paslaugos apimtyje paslaugos naudotojui yra suteikiamos prisijungimo prie apsaugoto IT ištekliaus priemonės.
3.2.8.	Paslaugos administratoriaus sąsaja	**Paskyrų valdymas.** Paslaugos gavėjo paslaugos administratoriui turi būti suteiktos šios KVTC paskyrų valdymo priemonės (netaikoma, jei naudojamos paslaugos gavėjo ar paslaugos naudotojo organizacijos autentifikavimo priemonės): 1. Paslaugų administratoriaus grafinė vartotojo sąsaja veikianti žiniatinklio technologijomis, leidžianti: sukurti, ištrinti, užrakinti, atrakinti naudotojų paskyras bei pakeisti slaptažodį. 2. Automatinis paslaugos naudotojo paskyrų sinchronizavimas su paslaugos gavėjo LDAP direktorija. 3. Automatinis paslaugų naudotojų paskyrų sinchronizavimas naudojant CSV, JSON, YAML formatų failus. Naudojant automatinį paskyrų sinchronizavimą (2 ir 3 punktai) gali būti valdomos tik paskyros ir naudotojų atributai, bet ne slaptažodžiai. Automatinio paskyrų valdymo atveju, turi būti naudojamas pirmo prisijungimo nuorodos, išsiųstos paslaugos naudotojo el. pašto adresu, su reikalavimu sukurti slaptažodį ir susikonfigūruoti OTP priemones pirmo prisijungimo metu, mechanizmas. Gali būti naudojami ir kiti panašūs

Nr.	Pavadinimas	Aprašymas
		mechanizmai, suderinti su perkančiąja organizacija paslaugos įgyvendinimo metu. **Sesijų valdymas.** Paslaugos gavėjo paslaugos administratoriui turi būti suteiktos priemonės, veikiančios žiniatinklio pagrindu, atlikti šiuos veiksmus: • stebėti paslaugos naudotojo sesiją beveik realiu laiku (delsa iki 10 sek.). • nutraukti privilegijuotą sesiją iškarto arba po tam tikro laiko tarpo. • nusiųsti žinutę naudotojui, kuris naudojasi privilegijuota sesija. **Užklausos.** Šiuos veiksmus paslaugos administratorius galės atlikti registruodamas paslaugos užklausą (angl. service request) KVTC pagalbos tarnybai: • suteikti prieigą naujam paslaugos naudotojui. • panaikinti prieigą esamam paslaugos naudotojui. • panaikinti prieigą visai paslaugos gavėjo organizacijai. • užsakyti prisijungimų istorijos išklotinę. • užsakyti prisijungimo sesijos įrašą.
3.2.9.	Našumas	Turi būti užtikrinti šie paslaugos našumo parametrai: • nemažiau nei 50 vienu metu prie apsaugotų sistemų prisijungusių paslaugų naudotojų; • nemažiau nei 100 unikalių licencijuotų privilegijuotų paslaugų naudotojų; • nemažiau nei 100 paslaugų gavėjų; • nemažiau nei 5 000 paslaugos atvejų – apsaugotų paslaugų gavėjo IT išteklių (tarnybinių stočių, duomenų bazių ir vidinio organizacijos tinklo).
3.2.10.	Našumo plečiamumas	Ateityje turi būti galimybė, nekeičiant sprendimo architektūros ir esamų sprendimo komponentų, o tik įsigyjant ir įdiegiant papildomus techninės ar programinės įrangos komponentus, išplėsti paslaugos našumą taip, kad būtų užtikrinta: • nemažiau nei 100 vienu metu prie apsaugotų sistemų prisijungusių paslaugų naudotojų; • nemažiau nei 500 unikalių licencijuotų privilegijuotų paslaugų naudotojų; • nemažiau nei 500 paslaugų gavėjų; • nemažiau nei 10 000 paslaugos atvejų - apsaugotų paslaugų gavėjo IT išteklių (tarnybinių stočių, duomenų bazių ir vidinio organizacijos tinklo).
3.2.11.	Paslaugų kokybės reikalavimai (SLA)	Metinis paslaugos pasiekiamumas ne mažiau nei 99,7%

3.3 Paslaugų plėtra

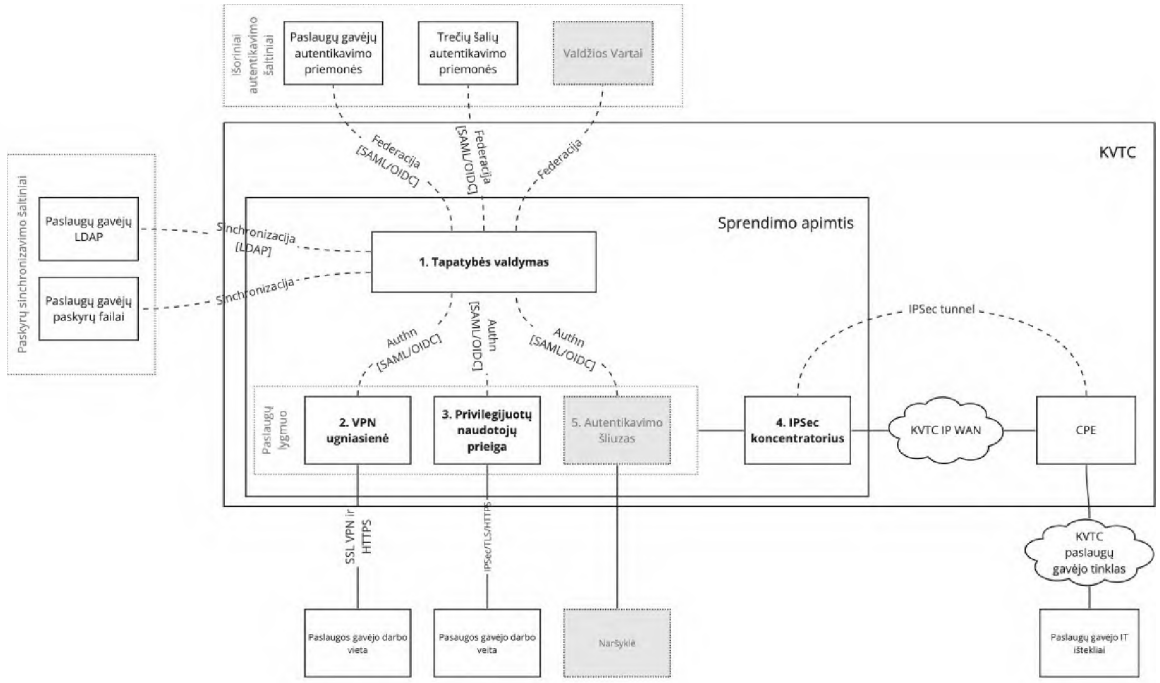
Ateityje yra planuojama kurti ir teikti daugiau paslaugų, skirtų valstybinėms institucijoms, bei toliau tobulinti šio projekto metu sukurtas paslaugas.
Planuojama **VPN prieigos prie institucijos tinklo** paslaugą patobulinti taip, kad paslaugos administratorius galėtų valdyti detalias paslaugų gavėjų tinklo lygio prieigas. Taip pat planuojama **Saugios trečių šalių prieigos** paslaugą papildyti naujais apsaugotų resursų tipais.
Viena naujų planuojamų paslaugų yra „**Saugi žiniatinklio prieiga**“ skirta valstybinėms institucijos saugiai publikuoti ir suteikti prieigą prie jų valdomų IS ar registrų viešojo sektoriaus darbuotojams, naudojant tik žiniatinklio priemones, bei „valdžios vartų“ autentifikavimo priemones. Nors šios

paslaugos įgyvendinimas nėra šio projekto apimtyje, tačiau siekiama, kad šio projekto apimtyje įdiegtus technologinius sprendinius būtų galima pernaudoti naujų paslaugų kūrimui ir teikimui.

4 Sprendimo architektūra

Paslaugų teikimui reikalingo sprendimo architektūra, apibrėžianti funkcinius komponentus ir sąryšius tarp jų, yra pateikiama pav. Pav. 1. Sprendimas sudarytas iš 4 atskirų funkcinių komponentų:

1. Tapatybės valdymo komponentas – užtikrina visų paslaugų naudotojų autentifikavimo logiką:
    a. Užtikrina KVTC paskyrų valdymą ir autentifikavimą.
    b. Užtikrina autentifikavimo federaciją su išorinėmis tapatybių valdymo sistemomis naudojant SAML v2 ir OIDC protokolus. Šio Projekto apimtyje yra numatyta autentifikavimo federacija su paslaugų gavėjų tapatybių valdymo sistemomis bei su saugios trečių šalių prieigos paslaugos paslaugų naudotojų institucijų tapatybių valdymo sistemomis. Ateityje numatomas poreikis realizuoti autentifikavimo federaciją su „Valdžios vartų“ autentifikavimo priemonėmis, kuriant paslaugą skirtą apsaugoti viešo sektoriaus darbuotojų prieigą prie valstybės IS ir registrų.
    c. Užtikrina automatizuotą paskyrų sinchronizavimą.
    d. Paslaugas realizuojantys komponentai deleguoja naudotojų autentifikavimą šiam komponentui, naudojant SAML v2 ir OIDC protokolus. Taip užtikrinama, kad tapatybės yra valdomos vienoje vietoje ir nėra dubliuojamas tapatybės valdymo logikos įgyvendinimas keliuose sprendimo komponentuose.
2. VPN koncentratorius – realizuoja VPN prieigą prie paslaugų gavėjo IT infrastruktūros. Šis komponentas deleguoja autentifikavimą tapatybės valdymo komponentui naudojant SAML v2 arba OIDC protokolus.
3. Privilegijuotų naudotojų prieiga – realizuoja saugios trečių šalių prieigą prie paslaugų gavėjų infrastruktūros.
4. IPSec koncentratorius – skirtas užtikrinti saugų duomenų perdavimą tarp paslaugų gavėjų ir KVTC paslaugų teikimo infrastruktūrų, bei užtikrinti paslaugų įgyvendinimui reikalingas bendras tinklo funkcijas (pvz., maršrutizavimą, paketų filtravimą).



Pav. 1 Sprendimo architektūra

Reikalavimai kiekvienam sprendimo komponentui yra aprašomi skyriuje Nr. 5.

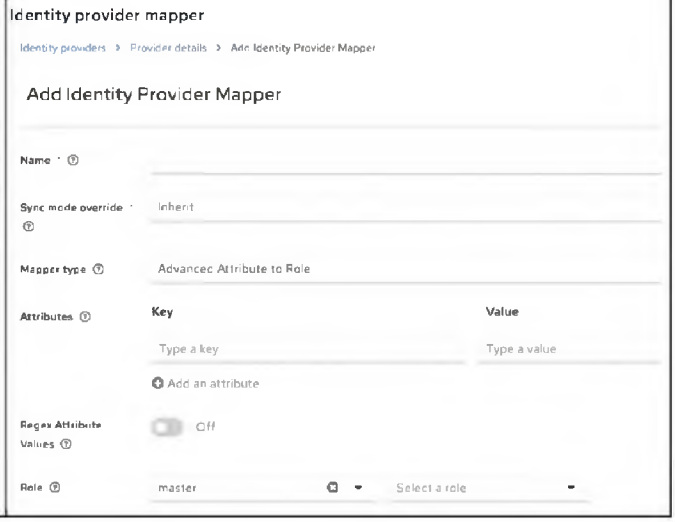
5 Reikalavimai sprendimo komponentams

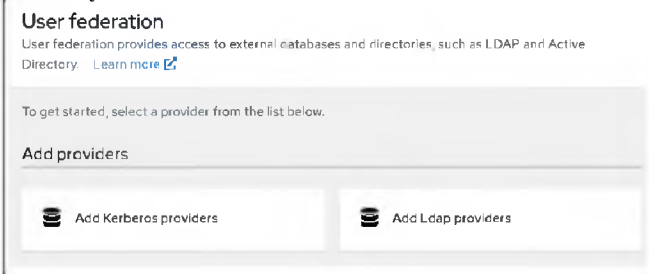
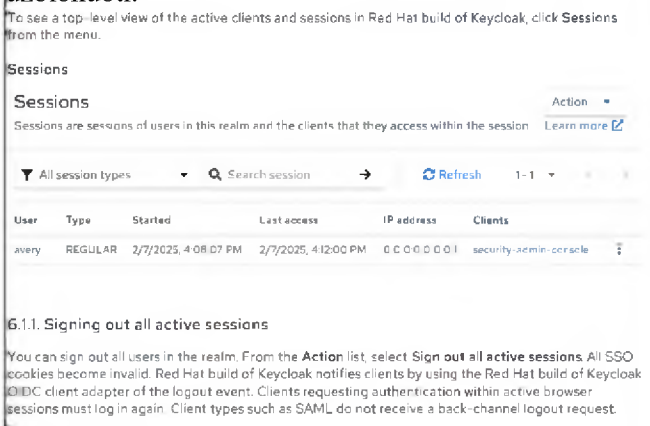
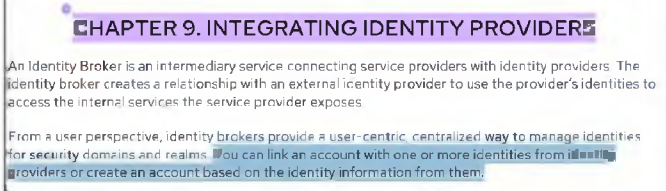
Tiekėjas turi užpildyti visus 5.1-5.5 punktų lentelių stulpelių „Atitikimas reikalavimams“ laukus, pagrįsdamas savo pasiūlyto sprendimo atitikimą nurodytiems techninės specifikacijos reikalavimams, priešingu atveju vertinimo komisija pasilieka teisę neužpildytus punktus traktuoti kaip neatitinkančius reikalavimų. Privaloma išsamiai aprašyti siūlomą parametrą.

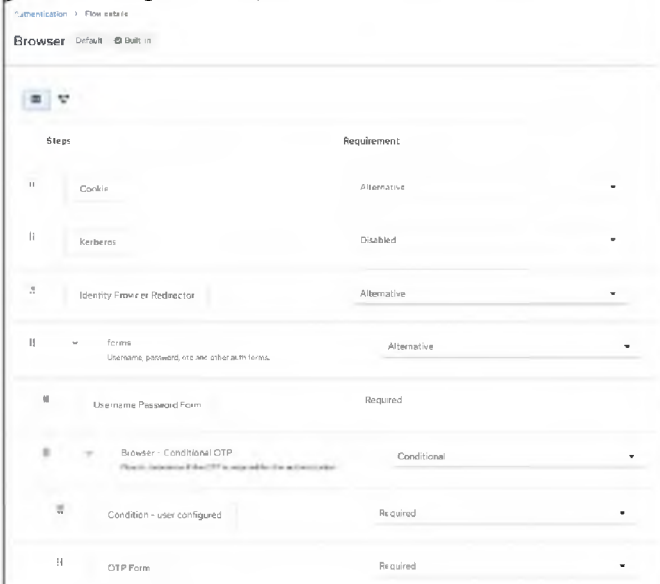
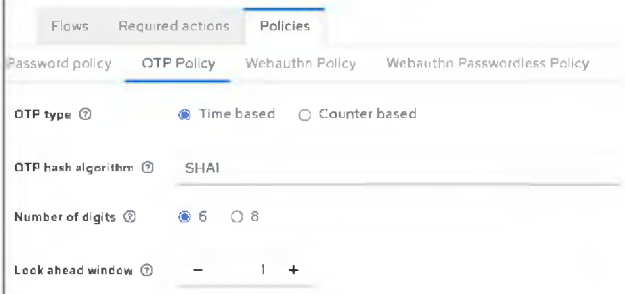
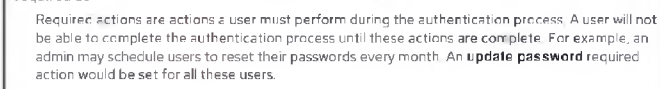
5.1. Tapatybės valdymo komponento reikalavimai

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
5.1.1.	Bendrieji reikalavimai Tapatybės valdymo komponentui (TVK)	Turi palaikyti naudotojų autentifikavimo delegavimą naudojant SAML v2 protokolą (SAML IdP rolė).	Palaiko naudotojų autentifikavimo delegavimą naudojant SAML v2 protokolą (SAML IdP rolė). Typically, Red Hat build of Keycloak bases identity providers on the following protocols: • SAML v2.0 • OpenID Connect v1.0 • OAuth v2.0 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 196psl.
		Turi palaikyti naudotojų autentifikavimo delegavimą naudojant OIDC protokolą (OIDC IdP rolė).	Palaiko naudotojų autentifikavimo delegavimą naudojant OIDC protokolą (OIDC IdP rolė).

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			Typically, Red Hat build of Keycloak bases identity providers on the following protocols: • SAML v2.0 • OpenID Connect v1.0 • OAuth v2.0 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 196psl.
		Turi turėti galimybę kiekvienam SAML SP (angl. service provider) ir OIDC klientui (angl. client) atskirai konfigūruoti gražinamus naudotojo atributus (angl. assertions, claims).	Yra galimybė kiekvienam SAML SP (angl. service provider) ir OIDC klientui (angl. client) atskirai konfigūruoti gražinamus naudotojo atributus (angl. assertions, claims). 13.4. OIDC TOKEN AND SAML ASSERTION MAPPINGS Applications receiving ID tokens, access tokens, or SAML assertions may require different roles and user metadata You can use Red Hat build of Keycloak to: • Hardcode roles, claims and custom attributes • Pull user metadata into a token or assertion. • Rename roles. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 327psl.
		Turi turėti galimybę kiekvienam OIDC klientui apibrėžti atskiras kliento roles (angl. client roles), prieigos teisių valdymui priskiriant jas naudotojų paskyroms.	Yra galimybė kiekvienam OIDC klientui apibrėžti atskiras kliento roles (angl. client roles), prieigos teisių valdymui priskiriant jas naudotojų paskyroms. 7.2. CLIENT ROLES 115 Red Hat build of Keycloak 26.2 Server Administration Guide Client roles are namespaces dedicated to clients. Each client gets its own namespace. Client roles are managed under the Roles tab for each client. You interact with this UI the same way you do for realm-level roles. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 115-120psl.
		Turi turėti galimybę kiekvienam OIDC klientui atskirai konfigūruoti autorizavimo logiką, t. y. neautentifikuoti naudotojo, jei jis neturi prieigos teisių prie kliento teikiamų paslaugų.	Yra galimybė kiekvienam OIDC klientui atskirai konfigūruoti autorizavimo logiką, t. y. neautentifikuoti naudotojo, jei jis neturi prieigos teisių prie kliento teikiamų paslaugų. my-resource-server OpenID Connect Authorization Settings Permissive Disabled Dokumentas: Red_Hat_build_of_Keycloak-26.2-Authorization_Services_Guide-en-US.pdf, 15-18psl.
		Turi palaikyti autentifikavimo federavimą su kitomis tapatybių valdymo sistemomis (angl. brokerage,	Palaiko autentifikavimo federavimą su kitomis tapatybių valdymo sistemomis (angl. brokerage, federation), veikiančioms SAML 2.0 protokolu.

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		federation), veikiančioms SAML 2.0 protokolu.	An Identity Broker is an intermediary service connecting service providers with identity providers. The identity broker creates a relationship with an external identity provider to use the provider's identities to access the internal services the service provider exposes. From a user perspective, identity brokers provide a user-centric, centralized way to manage identities for security domains and realms. You can link an account with one or more identities from identity providers or create an account based on the identity information from them. An identity provider derives from a specific protocol used to authenticate and send authentication and authorization information to users. It can be: • A social provider such as Facebook, Google, or Twitter. • A business partner whose users need to access your services. • A cloud-based identity service you want to integrate. Typically, Red Hat build of Keycloak bases identity providers on the following protocols: • SAML v2.0 • OpenID Connect v1.0 • OAuth v2.0 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 196psl.
		Turi palaikyti autentifikavimo federavimą su kitomis tapatybių valdymo sistemomis (angl. brokerage, federation), OIDC protokolu.	Palaiko autentifikavimo federavimą su kitomis tapatybių valdymo sistemomis (angl. brokerage, federation), veikiančioms OIDC protokolu. An Identity Broker is an intermediary service connecting service providers with identity providers. The identity broker creates a relationship with an external identity provider to use the provider's identities to access the internal services the service provider exposes. From a user perspective, identity brokers provide a user-centric, centralized way to manage identities for security domains and realms. You can link an account with one or more identities from identity providers or create an account based on the identity information from them. An identity provider derives from a specific protocol used to authenticate and send authentication and authorization information to users. It can be: • A social provider such as Facebook, Google, or Twitter. • A business partner whose users need to access your services. • A cloud-based identity service you want to integrate. Typically, Red Hat build of Keycloak bases identity providers on the following protocols: • SAML v2.0 • OpenID Connect v1.0 • OAuth v2.0 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 196psl.
		Turi turėti galimybę kiekvienai federuojamai tapatybių valdymo sistemai konfigūruoti federuojamos tapatybių valdymo sistemos gražinamų atributų susiejimą (angl. mapping) su KVTC tapatybės valdymo komponento naudotojo atributais.	Yra galimybė kiekvienai federuojamai tapatybių valdymo sistemai konfigūruoti federuojamos tapatybių valdymo sistemos gražinamų atributų susiejimą (angl. mapping) su KVTC tapatybės valdymo komponento naudotojo atributais. Identity provider mapper 

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 231-233psl.
		Turi turėti galimybę apjungti naudotojus iš kelių skirtingų šaltinių (keletas skirtingų LDAP saugyklų ar keletas skirtingų trečių šalių federuotų tapatybių valdymo sistemų.	Yra galimybė apjungti naudotojus iš kelių skirtingų šaltinių (keletas skirtingų LDAP saugyklų ar keleto skirtingų trečių šalių federuotų tapatybių valdymo sistemų.  Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 44psl.
		Turi turėti galimybę realiu laiku per grafinę ar API sąsają stebėti aktyvių naudotojų sesijas, jas nutraukti ar užblokuoti.	Yra galimybė realiu laiku per grafinę ar API sąsają stebėti aktyvių naudotojų sesijas, jas nutraukti ar užblokuoti.  Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 105psl.
		Tais atvejais, kai naudotojas yra susietas su keliais autentifikavimo šaltiniais, turi turėti galimybę leisti naudotojui autentifikavimo metu pasirinkti autentifikavimo šaltinį.	Tais atvejais, kai naudotojas yra susietas su keliais autentifikavimo šaltiniais, yra galimybė leisti naudotojui autentifikavimo metu pasirinkti autentifikavimo šaltinį.  Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 196psl.
		Turi palaikyti lanksčią ir derinamą naudotojo autentifikavimo proceso patirtį ir leisti konfigūruojant	Palaiko lanksčią ir derinamą naudotojo autentifikavimo proceso patirtį ir leidžia konfigūruojant keisti naudotojų autentifikavimo logiką (seką) įtraukiant skirtingus

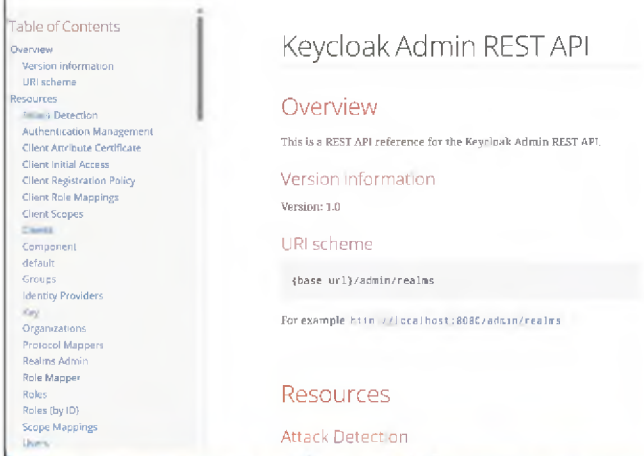
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		keisti naudotojų autentifikavimo logiką (seką) įtraukiant skirtingus autentifikavimo šaltinius, papildomas autentifikavimo priemones (pvz. OTP).	autentifikavimo šaltinius, papildomas autentifikavimo priemones (pvz. OTP).  Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 130-148psl.
		Turi turėti dviejų faktorių autentifikavimo funkcionalumą (pvz. OTP mobili programėlė).	Turi dviejų faktorių autentifikavimo funkcionalumą (pvz. OTP mobili programėlė).  Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 128-130psl.
		Turi turėti galimybę valdyti slaptažodžių politikas: reikalavimas pasikeisti slaptažodį pirmo prisijungimo metu, valdyti slaptažodžių sudėtingumą, galiojimą laiką.	Yra galimybė valdyti slaptažodžių politikas: reikalavimą pasikeisti slaptažodį pirmo prisijungimo metu, valdyti slaptažodžių sudėtingumą, galiojimą laiką. 

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			8.1.1.3. Digits The number of numerical digits required in the password string. 8.1.1.4. Lowercase characters The number of lower case letters required in the password string. 8.1.1.5. Uppercase characters The number of upper case letters required in the password string. 8.1.1.6. Special characters The number of special characters required in the password string. 8.1.1.7. Not username The password cannot be the same as the username. 8.1.1.8. Not email The password cannot be the same as the email address of the user. 8.1.1.9. Regular expression Password must match one or more defined Java regular expression patterns. See Java's regular expression documentation for the syntax of those expressions. 8.1.1.10. Expire password The number of days the password is valid. When the number of days has expired, the user must change their password. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 17, 124-127psl.
		Tapatybės valdymo komponentas turi palaikyti išplėstų slaptažodžių politikų taikymą (pvz. drausti naudoti el. paštą, paskyros vardą kaip slaptažodį, taikyti slaptažodžių istoriją, naudoti juoduosius sąrašus draudžiamiems slaptažodžiams).	Tapatybės valdymo komponentas palaiko išplėstų slaptažodžių politikų taikymą (pvz. draudžia naudoti el. paštą, paskyros vardą kaip slaptažodį, taiko slaptažodžių istoriją, naudoja juoduosius sąrašus draudžiamiems slaptažodžiams). 8.1.1.7. Not username The password cannot be the same as the username. 8.1.1.8. Not email The password cannot be the same as the email address of the user. 8.1.1.9. Regular expression Password must match one or more defined Java regular expression patterns. See Java's regular expression documentation for the syntax of those expressions. 8.1.1.10. Expire password The number of days the password is valid. When the number of days has expired, the user must change their password. 126 CHAPTER 8. CONFIGURING AUTHENTICATION 8.1.1.11. Not recently used Password cannot be already used by the user. Red Hat build of Keycloak stores a history of used passwords. The number of old passwords stored is configurable in Red Hat build of Keycloak. 8.1.1.12. Not recently used (In Days) Password cannot be reused within the configured time period (in days). If the new password was last set within this period, the user will be forced to provide a different one. 8.1.1.13. Password blacklist Password must not be in a blacklist file. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 126-127psl.
		TVK turi palaikyti:	TVK gamintojas neriboja paskyrų, federuotų tapatybių valdymo sistemų, loginių organizacijų objektų skaičiaus. Naudojantis šia rekomendacija:

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		• nemažiau kaip 20 000 unikalių naudotojų paskyrų; • nemažiau kaip 10 000 naudotojų autentifikavimų per minutę; • nemažiau kaip 500 federuotų tapatybių valdymo sistemų; • nemažiau kaip 500 loginių organizacijų (paslaugų gavėjų) tapatybės valdymą. Ateityje turi būti galimybė, nekeičiant TVK architektūros ir tik įsigyjant papildomas licencijas ir pridedant TVK elementus (horizontalus plečiamumas), išplėsti paslaugos našumą taip, kad būtų užtikrinta: • nemažiau kaip 50 000 unikalių naudotojų paskyrų; • nemažiau kaip 20 000 naudotojų autentifikavimų per minutę; • nemažiau kaip 500 federuotų tapatybių valdymo sistemų; • 500 loginių organizacijų (paslaugų gavėjų) tapatybės valdymą.	• For each 15 password-based user logins per second, allocate 1 vCPU to the cluster (tested with up to 300 per second). Red Hat build of Keycloak spends most of the CPU time hashing the password provided by the user, and it is proportional to the number of hash iterations. 10 000 naudotojų autentifikavimų per minutę yra 167 autentikavimų per sekundę. Rekomenduojama 1 vCPU skirti 15 slaptažodžio tipo autentikavimams, tai 167 yra 11 vCPU. Siūlome du Redhat build of Keycloak serverius po 16 vCPU. Tai vieno iš jų gedimo atveju bus padengtas poreikis 11 vCPU <16 vCPU. Ateityje planuojamas poreikis 20 000 naudotojų autentifikavimų per minutę (dvigubai didesnis už 10 000) tai vCPU poreikis yra 22 vCPU. Tokiu atveju rekomenduojama diegti papildomą trečią Redhat build of Keycloak serverį nes vieno iš jų gedimo atveju dirbtų du serveriai po 16 vCPU, 22 vCPU <32 vCPU. Dokumentas: Red_Hat_build_of_Keycloak-26.2-High_Availability_Guide-en-US.pdf, 17 psl. Papildomai pridedame gamintojo aiškinamąjį raštą, kuris bus pridėtas prie pasiūlymo dokumentų pavadinimu „Gamintojo Red Hat Aiškinamasis raštas“.
5.1.2.	Reikalavimai aukšto patikimumo diegimui per du duomenų centrus	Visi TVK komponentai (pvz., aplikacijos, duomenų bazių valdymo sistemos ir t.t.) turi palaikyti aukšto patikimumo diegimo būdą, diegiamą atliekant per du iki 20 km nutolusius duomenų centrus, turinčius 10Gbit/s L2 lygio tinklo sujungimo galimybę.	Visi TVK komponentai (pvz., aplikacijos, duomenų bazių valdymo sistemos ir t.t.) palaiko aukšto patikimumo diegimo būdą, diegiamą atliekant per du iki 20 km nutolusius duomenų centrus, turinčius 10Gbit/s L2 lygio tinklo sujungimo galimybę. Gamybinėje aplinkoje tinklo balansuotuvas, kuris nukreips klientų srautą į TVK aplikacijos serverius bus nustatytas su „Session affinity“ arba analogišku funkcionalumu kaip ir rekomenduojama: By relying on a distributable cache, cached user and client sessions are available to any node in the cluster so that users can be redirected to any node without the need to load session data from the database. However, production-ready deployments should always consider session affinity and favor redirecting users to the node where their sessions were initially created. By doing that, you are going to avoid unnecessary state transfer between nodes and improve CPU, memory, and network utilization. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Configuration_Guide-en-US.pdf, 66psl.

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			Duomenų bazių serveriai bus diegiami su dubliuotomis duomenų bazėmis, kurios bus replikuojamos sinchroniškai: *Synchronous-commit mode* emphasizes high availability over performance, at the cost of increased transaction latency. Under synchronous-commit mode, transactions wait to send the transaction confirmation to the client until the secondary replica has hardened the log to disk. When data synchronization begins on a secondary database, the secondary replica begins applying incoming log records from the corresponding primary database. As soon as every log record has been hardened, the secondary database enters the SYNCHRONIZED state. Thereafter, every new transaction is hardened by the secondary replica before the log record is written to the local log file. When all the secondary databases of a given secondary replica are synchronized, synchronous-commit mode supports manual failover and, optionally, automatic failover. Dokumentas: sql-sql-server-ver16.pdf, 874psl.(PDF) Gamintojų (Redhat ir Microsoft) dokumentacijoje nėra pateikta bendro tinklo pralaidumo tarp duomenų centrų reikalavimų. Laikoma, kad pateikti tinklo parametrai yra traktuojami kaip didelio tinklo greičio („High-speed“) ir žemos delsos („Low-latency“) ir yra tinkami sprendimo diegimui. Papildomai pridedame gamintojo aiškinamąjį raštą, kuris bus pridėtas prie pasiūlymo dokumentų pavadinimu „Gamintojo Red Hat Aiškinamasis raštas“.
		Turi užtikrinti keliamus našumo reikalavimus sutrikus vieno duomenų centro ir jame esančių TVK komponentų veiklai.	Užtikrins keliamus našumo reikalavimus sutrikus vieno duomenų centro ir jame esančių TVK komponentų veiklai. Naudojantis šia rekomendacija: • For each 15 password-based user logins per second, allocate 1 vCPU to the cluster (tested with up to 300 per second). Red Hat build of Keycloak spends most of the CPU time hashing the password provided by the user, and it is proportional to the number of hash iterations 10 000 naudotojų autentifikavimų per minutę yra 167 autentikavimų per sekundę. Rekomenduojama 1 vCPU skirti 15 slaptažodžio tipo autentikavimams, tai 167 yra 11 vCPU. Siūlome du Redhat build of Keycloak serverius po 16 vCPU diegiamus atskiruose duomenų centruose. Tai vieno iš jų gedimo atveju bus padengtas poreikis 11 vCPU <16 vCPU. Dokumentas: Red_Hat_build_of_Keycloak-26.2-High_Availability_Guide-en-US.pdf, 17 psl.
		Turi užtikrinti ne ilgesnį nei 60 sekundžių funkcionalumo sutrikimą vieno iš duomenų centro gedimo atveju.	Užtikrins ne ilgesnį nei 60 sekundžių funkcionalumo sutrikimą vieno iš duomenų centro gedimo atveju. Failure / Recovery / RPO[1] / RTO[2] Database node — If the writer instance fails, the database can promote a reader instance in the same or other site to be the new writer. — No data loss — Seconds to minutes (depending on the database) Red Hat build of Keycloak node — Multiple Red Hat build of Keycloak instances run on each site. If one instance fails some — No data loss — Less than 30 seconds Dokumentas: Red_Hat_build_of_Keycloak-26.2-High_Availability_Guide-en-US.pdf, 8 psl.

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		TVK turi užtikrinti automatinį veikimo atstatymą, atstačius vieno iš elemento veikimą po jo sutrikimo. Pavyzdžiui, atstačius TVK DBVS veikimą po sutrikimo, kiti TVK elementai (pvz. aplikacijos) pradeda veikti be žmogaus įsikišimo (pvz. rankinio perkrovimo).	TVK užtikrins automatinį veikimo atstatymą, atstačius vieno iš elemento veikimą po jo sutrikimo. Pavyzdžiui, atstačius TVK DBVS veikimą po sutrikimo, kiti TVK elementai (pvz. aplikacijos) pradeda veikti be žmogaus įsikišimo (pvz. rankinio perkrovimo). Keycloak naudos JDBC URL, kuriame nurodytas Availability Group Listener (AGL) (pvz., jdbc:sqlserver://tvk-listener.mydomain:1433), aplikacija automatiškai prisijungia prie aktyvaus SQL serverio. Synchronous-commit mode with automatic failover Automatic failover provides high availability by ensuring that the database is quickly made available again after the loss of the primary replica. To configure an availability group for automatic failover, you need to set both the current primary replica and at least one secondary replica to synchronous-commit mode with automatic failover. SQL Dokumentas: sql-sql-server-ver16.pdf, 880psl.(PDF)
		Turi turėti administravimo grafinę vartotojo sąsają (angl. „Graphical user interface“).	Turės administravimo grafinę vartotojo sąsają (angl. „Graphical user interface“). 3.1. USING THE ADMIN CONSOLE You configure realms and perform most administrative tasks in the Red Hat build of Keycloak Admin Console. Prerequisites To use the Admin Console, you need an administrator account. • If no administrators exist, see Creating the first administrator. • If other administrators exist, ask an administrator to provide an account with privileges to manage realms. Procedure 1. Go to the URL for the Admin Console. For example, for localhost, use this URL: http://localhost:8080/admin/ 2. Enter the username and password you created on the Welcome Page or through environment variables as described in Creating the initial admin user. Login page Sign in to your account Username or email avery Password •••••••• Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 20psl.
		Turi turėti atvirą ir dokumentuotą API, leidžiantį valdyti naudotojus, roles, grupes, grupių narystę, rolių priskyrimą, SAML ir OIDC klientus ir jų konfigūraciją ir kitus TVK administravimui būdingus veiksmus.	Turės atvirą ir dokumentuotą API, leidžiantį valdyti naudotojus, roles, grupes, grupių narystę, rolių priskyrimą, SAML ir OIDC klientus ir jų konfigūraciją ir kitus TVK administravimui būdingus veiksmus.

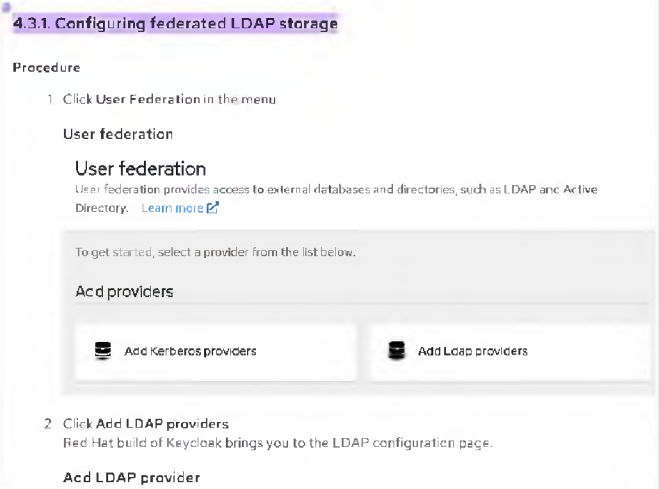
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			CHAPTER 1. RED HAT BUILD OF KEYCLOAK API DOCUMENTATION 1.1. JAVADOCS DOCUMENTATION JavaDocs Documentation 1.2. ADMIN REST API DOCUMENTATION Administration REST API  https://access.redhat.com/webassets/avalon/d/red_hat_build_of_keycloak-26.2/rest-api/ Dokumentas: Red_Hat_build_of_Keycloak-26.2-API_Documentation-en-US.pdf, 3psl.
		Įskiepių kūrimui turi būti programinės įrangos kūrimo įrankių rinkinys (angl. Software development kit arba SDK) bent vienai iš šių bendro naudojimo programavimo kalbų: Java, C#, GoLan, Python.	Įskiepių kūrimui yra programinės įrangos kūrimo įrankių rinkinys (angl. Software development kit arba SDK) Java programavimo kalbai:

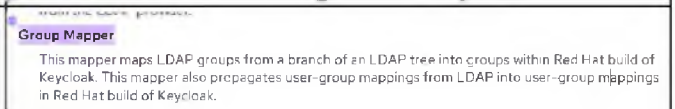
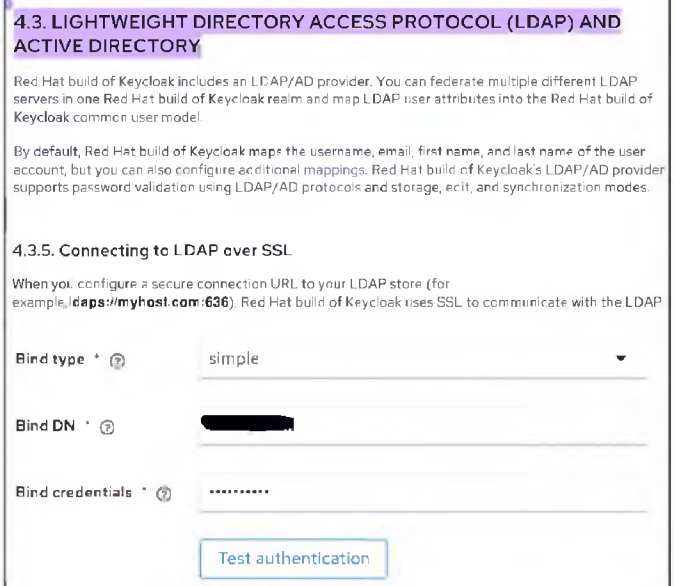
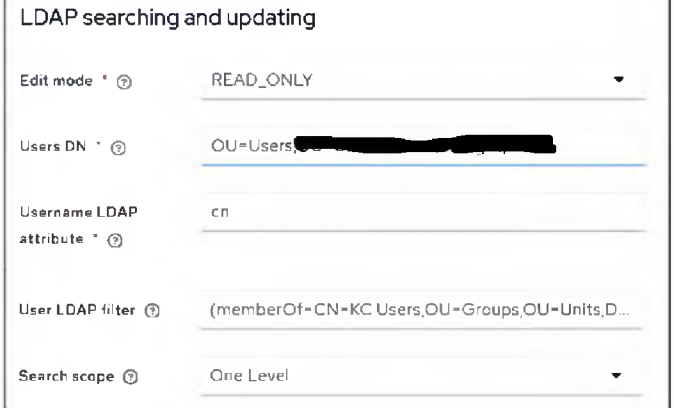
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))

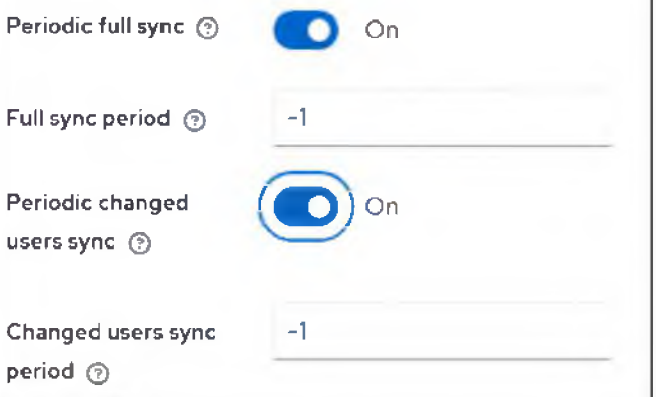
			CHAPTER 6. SERVICE PROVIDER INTERFACES (SPI)
			Red Hat build of Keycloak is designed to cover most use-cases without requiring custom code, but we also want it to be customizable. To achieve this Red Hat build of Keycloak has a number of Service Provider Interfaces (SPI) for which you can implement your own providers.
			6.1. IMPLEMENTING AN SPI
			To implement an SPI you need to implement its ProviderFactory and Provicer interfaces. You also need to create a service configuration file.
			For example, to implement the Theme Selector SPI you need to implement ThemeSelectorProviderFactory and ThemeSelectorProvicer and also provide the file **META-INF/services/org.keycloak.theme.ThemeSelectorProviderFactory**.
			Example ThemeSelectorProviderFactory:
			`package org.acme.provider;`
			`import ...`
			`public class MyThemeSelectorProviderFactory implements ThemeSelectorProviderFactory {`
			`@Override`
			`public ThemeSelectorProvider create(KeycloakSession session) {`
			`return new MyThemeSelectorProvider(session);`
			`}`
			`@Override`
			`public void init(Config.Scope config) {`
			`}`
			`@Override`
			`public void postInit(KeycloakSessionFactory factory) {`
			`}`
			`@Override`
			`public void close() {`
			`}`
			`@Override`
			`public String getId() {`
			`return "myThemeSelector";`
			`}`
			`}`
			Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Developer_Guide-en-US.pdf, 22psl.

		Turi būti galimybė standartinėmis HTML, CSS, JS priemonėmis kurti nuosavo dizaino naudotojo sąsajas, matomas naudotojo autentifikavimo metu.	Yra galimybė standartinėmis HTML, CSS, JS priemonėmis kurti nuosavo dizaino naudotojo sąsajas, matomas naudotojo autentifikavimo metu. 3.3. DEFAULT THEMES Red Hat build of Keycloak comes bundled with default themes in the JAR file **keycloak-themes-26.2.4.redhat-00001.jar** inside the server distribution. The server's root **themes** directory does not contain any themes by default, but it contains a README file with some additional details about the default themes. To simplify upgrading, do not edit the bundled themes directly. Instead create your own theme that extends one of the bundled themes. 3.4. CREATING A THEME A theme consists of: • HTML templates (Freemarker Templates) • Images • Message bundles • Stylesheets • Scripts • Theme properties Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Developer_Guide-en-US.pdf, 8psl.
		TVK turi turėti vieną iš šių sąsajų žurnalų eksportui į kitas perkančiosios organizacijos sistemas:	TVK turi šias sąsajas žurnalų eksportui į kitas perkančiosios organizacijos sistemas: • Žurnalinių įrašų siuntimas Syslog protokolu į nutolusį serverį;

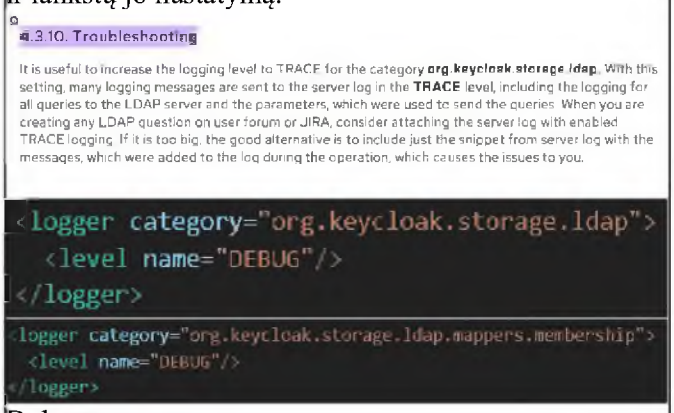
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		• Žurnalinių įrašų siuntimas Syslog protokolu į nutolusį serverį; • žurnalų įrašų rašymas į failus, leidžiantis agento pagalba failų turinį persiųsti į nutolusį serverį.	• žurnalų įrašų rašymas į failus, leidžiantis agento pagalba failų turinį persiųsti į nutolusį serverį. CHAPTER 16. CONFIGURING LOGGING Configure logging for Red Hat build of Keycloak. Red Hat build of Keycloak uses the JBoss Logging framework. The following is a high-level overview for the available log handlers with the common parent log handler root. • console • file • syslog Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Configuration_Guide-en-US.pdf, 96-111psl.
		Turi turėti galimybę prisijungusiam paskyros savininkui (paslaugos naudotojui) grafinėje sąsajoje valdyti savo paskyrą ir atlikti mažiausiai šiuos veiksmus: • keisti slaptažodį; • konfigūruoti naują OTP priemonę; • ištrinti egzistuojančią OTP priemonę.	Yra galimybė prisijungusiam paskyros savininkui (paslaugos naudotojui) grafinėje sąsajoje valdyti savo paskyrą ir atlikti mažiausiai šiuos veiksmus: • keisti slaptažodį; • konfigūruoti naują OTP priemonę; • ištrinti egzistuojančią OTP priemonę. The following are examples of required action types: Update Password 89 Red Hat build of Keycloak 26.2 Server Administration Guide The user must change their password. Configure OTP The user must configure a one-time password generator on their mobile device using either the Free OTP or Google Authenticator application. Verify Email The user must verify their email account. An email will be sent to the user with a validation link that they must click. Once this workflow is successfully completed, the user will be allowed to log in. Update Profile The user must update profile information, such as name, address, email, and phone number. 5.3.3. Creating an OTP If OTP is conditional in your realm, the user must navigate to Red Hat build of Keycloak Account Console to reconfigure a new OTP generator. If OTP is required, then the user must reconfigure a new OTP generator when logging in. 83 Red Hat build of Keycloak 26.2 Server Administration Guide Alternatively, you can send an email to the user that requests the user reset the OTP generator. The following procedure also applies if the user already has an OTP credential. Prerequisite • You are logged in to the appropriate realm. Procedure 1. Click Users in the main menu. The Users page is displayed. 2. Select a user. 3. Click the Credentials tab. 4. Click Credential Reset. 5. Set Reset Actions to Configure OTP. 6. Click Send Email. The sent email contains a link that directs the user to the OTP setup page. Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 83-84,89-90psl.
5.1.3.	Reikalavimai automatinio	Turi palaikyti tokius paskyrų sinchronizavimo šaltinius:	Bus palaikomi tokie paskyrų sinchronizavimo šaltiniai:

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
	naudotojų paskyrų be slaptažodžių sinchronizavimo funkcionalumui	• LDAP direktorija; • CSV failas; • YAML failas; • JSON failas.	• LDAP direktorija (adaptuotas esamas ir/arba programuojamas); • CSV failas (programuojamas); • YAML failas (programuojamas); • JSON failas (programuojamas).  4.3.1. Configuring federated LDAP storage Procedure 1. Click User Federation in the menu User federation User federation User federation provides access to external databases and directories, such as LDAP and Active Directory. Learn more To get started, select a provider from the list below. Add providers Add Kerberos providers Add Ldap providers 2. Click Add LDAP providers Red Hat build of Keycloak brings you to the LDAP configuration page. Add LDAP provider Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 44psl.
		Automatinė sinchronizacija turi užtikrinti: • naujų paskyrų sukūrimą; • senų paskyrų trynimą; • pasikeitusių paskyros atributų sinchronizavimą. Automatinės sinchronizacijos metu neturi būti sinchronizuojami slaptažodžiai. Turi būti naudojamas pirmo prisijungimo nuorodos, išsiųstos paslaugos naudotojo el. pašto adresu, su reikalavimu sukurti slaptažodį ir susikonfigūruoti OTP pirmo prisijungimo metu, mechanizmas, arba lygiavertis kitas būdas užtikrinantis saugų pirmo prisijungimo po paskyros sukūrimo būdą.	Automatinė programuojama sinchronizacija užtikrins: • naujų paskyrų sukūrimą; • senų paskyrų trynimą; • pasikeitusių paskyros atributų sinchronizavimą. Automatinės sinchronizacijos metu nebus sinchronizuojami slaptažodžiai. Bus naudojamos pirmo prisijungimo nuorodos, išsiųstos paslaugos naudotojo el. pašto adresu, su reikalavimu sukurti slaptažodį ir susikonfigūruoti OTP pirmo prisijungimo metu, mechanizmas, arba lygiavertis kitas būdas užtikrinantis saugų pirmo prisijungimo po paskyros sukūrimo būdą. Šie automatinio paskyrų sinchronizavimo reikalavimai bus įgyvendinami kaip suprogramuota integracija.
		LDAP sinchronizacija turi užtikrinta, kad TVK paskyros turi LDAP šaltinį atitinkančias grupes, kurios	LDAP sinchronizacija užtikrins, kad TVK paskyros turi LDAP šaltinį atitinkančias grupes, kurios yra konfigūruojamos (pavyzdžiui, institucijos "A" LDAP naudotojai turi "org-a" grupę).

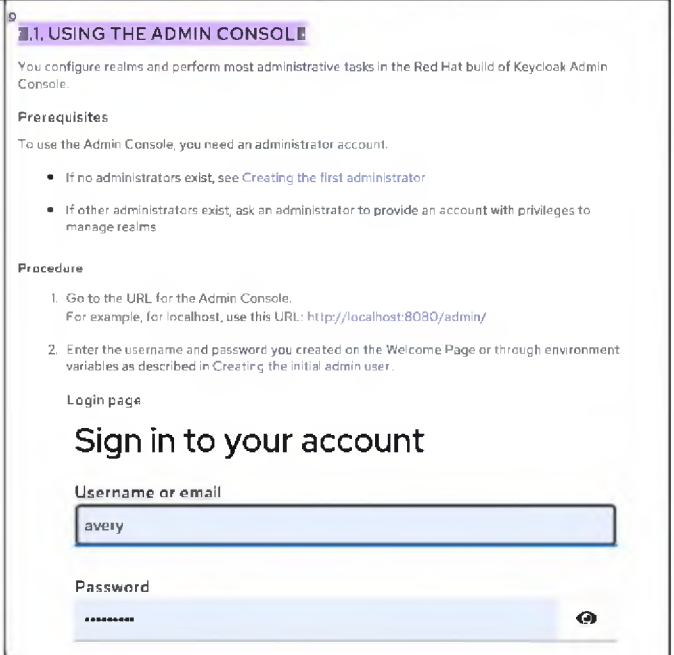
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		yra konfigūruojamos (pavyzdžiui, institucijos "A" LDAP naudotojai turi "org-a" grupę).	 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 49psl.
		Turi būti galimybė kiekvienam LDAP šaltiniui atskirai konfigūruoti tokius parametrus: • LDAP prisijungimo duomenys (adresas, prievadas, sertifikatai, naudotojas, slaptažodis ir k.t.); • LDAP užklausos filtras, kuris gražina tik reikiamus naudotojus (pavyzdžiui, visi naudotojai esantys tam tikrame organizaciniame vienete); • LDAP direktorijos atributų susiejimas su TVK paskyros atributais; • Priskiriamų grupių sąrašas; • Sinchronizavimo kalendorius (periodiškumas, dienos, laikas ir p.n.).	Bus galimybė kiekvienam LDAP šaltiniui atskirai konfigūruoti tokius parametrus: • LDAP prisijungimo duomenys (adresas, prievadas, sertifikatai, naudotojas, slaptažodis ir k.t.);  • LDAP užklausos filtras, kuris gražina tik reikiamus naudotojus (pavyzdžiui, visi naudotojai esantys tam tikrame organizaciniame vienete);  • LDAP direktorijos atributų susiejimas su TVK paskyros atributais;

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			4.3.7. LDAP mappers LDAP mappers are **listeners** triggered by the LDAP Provider. They provide another extension point to LDAP integration. LDAP mappers are triggered when: • Users log in by using LDAP. • Users initially register. • The Admin Console queries a user. When you create an LDAP Federation provider, Red Hat build of Keycloak automatically provides a set of **mappers** for this provider. This set is changeable by users, who can also develop mappers or update/delete existing ones. User Attribute Mapper This mapper specifies which LDAP attribute maps to the attribute of the Red Hat build of Keycloak user. For example, you can configure the **mail** LDAP attribute to the **email** attribute in the Red Hat build of Keycloak database. For this mapper implementation, a one-to-one mapping always exists. • Priskiriamų grupių sąrašas; Group Mapper This mapper maps LDAP groups from a branch of an LDAP tree into groups within Red Hat build of Keycloak. This mapper also propagates user-group mappings from LDAP into user-group mappings in Red Hat build of Keycloak. • Sinchronizavimo kalendorius (periodiškumas, dienos, laikas ir p.n.).  Cron darbas: `0 2 * * 1-5 curl -X POST \ -H "Authorization: Bearer $TOKEN" \ https://keycloak.example.com/auth/admin/realms/myrealm/user-storage/ldap-id/sync?action=triggerFullSync` Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 43-55psl. Papildomai pridedame gamintojo aiškinamąjį raštą, kuris bus pridėtas prie pasiūlymo dokumentų pavadinimu „Gamintojo Red Hat Aiškinamasis raštas“.
		Automatinė sinchronizacija turi palaikyti: • ne mažiau kaip bendrai 500 skirtingų šaltinių; • nemažiau kaip 20 000 naudotojų bendrai per visus šaltinius.	Automatinė sinchronizacija neribojama ir palaikys: • ne mažiau kaip bendrai 500 skirtingų šaltinių; nemažiau kaip 20 000 naudotojų bendrai per visus šaltinius. Papildomai pridedame gamintojo aiškinamąjį raštą, kuris bus pridėtas prie pasiūlymo dokumentų pavadinimu „Gamintojo Red Hat Aiškinamasis raštas“.
		Turi būti galimybė, nekeičiant architektūros, o tik pridedant papildomus komponentus (horizontalus	Yra galimybė, nekeičiant architektūros, o tik pridedant papildomus komponentus (horizontalus plečiamumas) užtikrinti automatinę sinchronizaciją: • nemažiau kaip 500 skirtingų šaltinių;

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
		plečiamumas) užtikrinti automatinę sinchronizaciją: • nemažiau kaip 500 skirtingų šaltinių; • nemažiau kaip 50 000 naudotojų bendrai per visus šaltinius.	nemažiau kaip 50 000 naudotojų bendrai per visus šaltinius. Papildomai pridedame gamintojo aiškinamąjį raštą, kuris bus pridėtas prie pasiūlymo dokumentų pavadinimu „Gamintojo Red Hat Aiškinamasis raštas“.

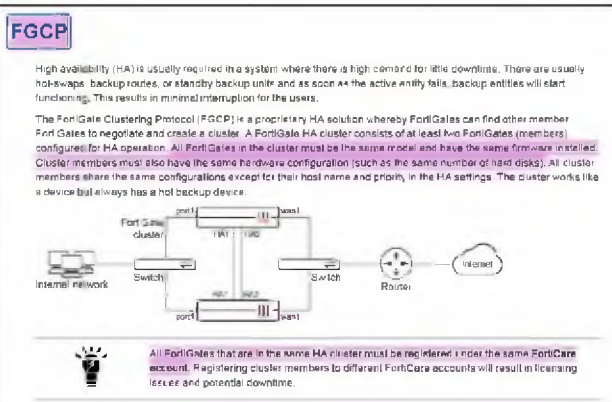
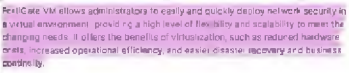
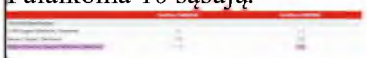
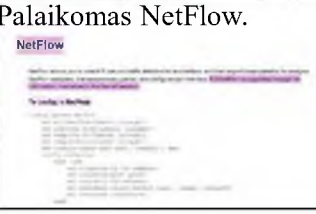
		TVK turi užtikrinti, automatinės sinchronizacijos metu atliekamų veiksmų su paskyromis (sukurtus, pakeistus, ištrintus naudotojus, priskirtas grupes ir panašiai) žurnalą.
		Visi TVK elementai (aplikacijos, DBVS, ar kiti technologiniai komponentai) turi būti diegiami perkančiosios organizacijos virtualizuotoje infrastruktūroje (žr. reikalavimus skyriuje Nr. 5.5)
			TVK užtikrins, automatinės sinchronizacijos metu atliekamų veiksmų su paskyromis (sukurtus, pakeistus, ištrintus naudotojus, priskirtas grupes ir panašiai) žurnalą ir lankstų jo nustatymą.
			 
			8.3.10. Troubleshooting
			It is useful to increase the logging level to TRACE for the category **org.keycloak.storage.ldap**. With this setting, many logging messages are sent to the server log in the **TRACE** level, including the logging for all queries to the LDAP server and the parameters, which were used to send the queries. When you are creating any LDAP question on user forum or JIRA, consider attaching the server log with enabled TRACE logging. If it is too big, the good alternative is to include just the snippet from server log with the messages, which were added to the log during the operation, which causes the issues to you.
			
			`<logger category="org.keycloak.storage.ldap">`
			`  <level name="DEBUG"/>`
			`</logger>`
			
			`<logger category="org.keycloak.storage.ldap.mappers.membership">`
			`  <level name="DEBUG"/>`
			`</logger>`
			
			Dokumentas:
			Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 51 psl.
			Visi TVK elementai (aplikacijos, DBVS, ar kiti technologiniai komponentai) bus diegiami perkančiosios organizacijos virtualizuotoje infrastruktūroje.

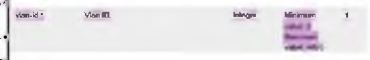
		Visi TVK, išskyrus automatinio paskyrų sinchronizavimo, reikalavimai turi būti realizuojami egzistuojančiomis technologijomis, turinčiomis gamintojo palaikymą. Automatinio paskyrų sinchronizavimo reikalavimai gali būti įgyvendinami kaip suprogramuota integracija.	Visi TVK, išskyrus automatinio paskyrų sinchronizavimo, reikalavimai bus realizuojami egzistuojančiomis technologijomis, turinčiomis gamintojo palaikymą. Automatinio paskyrų sinchronizavimo reikalavimai bus įgyvendinti kaip suprogramuota integracija.
5.1.4.	Sprendimo valdymo sąsajos reikalavimai	Turi turėti intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galėtų kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.	Turės intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galės kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.

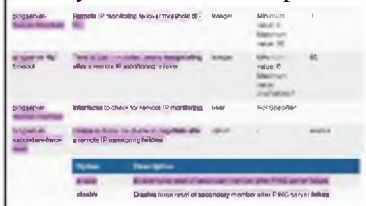
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
			 Dokumentas: Red_Hat_build_of_Keycloak-26.2-Server_Administration_Guide-en-US.pdf, 20psl.

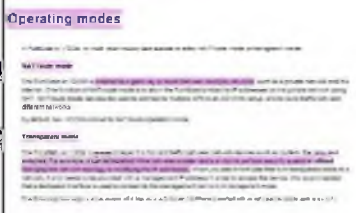
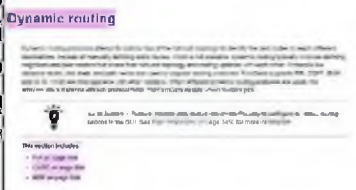
5.2. VPN ugniasienės komponento reikalavimai

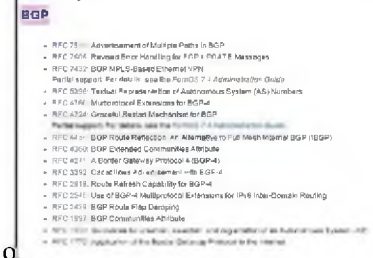
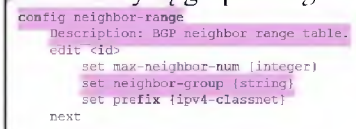
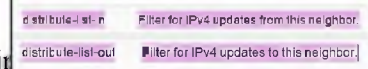
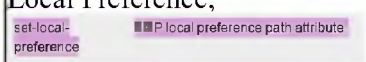
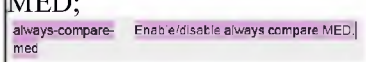
Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
5.2.1.	Sprendimo architektūra ir sudedamosios dalys	VPN ugniasienių sprendimas turi būti sudarytas iš aštuonių vienodų narių. Kiekvienas narys, t. y. kiekviena ugniasienė turi gebėti dirbti kaip nepriklausomas narys ir turi būti galima narius sujungti į aukšto patikimumo telkinį. Turi būti pateikta visa programinė įranga ir licencijos leidžiančios VPN ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aušto patikimumo telkinio narius.	VPN ugniasienių sprendimas yra sudarytas iš aštuonių vienodų narių. Kiekvienas narys, t. y. kiekviena ugniasienė geba dirbti kaip nepriklausomas narys ir yra galima narius sujungti į aukšto patikimumo telkinį. Pateikiama programinė įranga leidžianti VPN ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aukšto patikimumo telkinio narius. Aukšto patikimumo funkcionalumas nelicencijuojamas ir yra įskaičiuotas į programinės įrangos komplektaciją. Dokumentas: RST250615SVL1-01 produktu kodai_KONFIDENCIALU.pdf

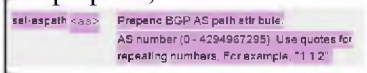
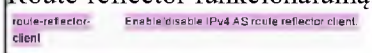
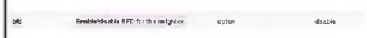
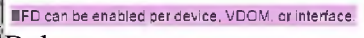
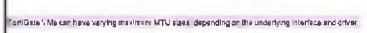
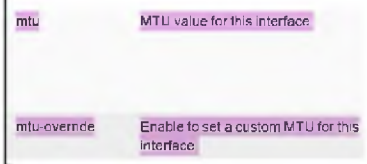
			 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3206 psl.
		Siūloma įranga turi būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais.	Siūloma įranga yra realizuota naudojant virtualizacijos platformomis paremtais sprendimais.  Dokumentas: FortiGate_VM_ESXi.pdf, 1 psl.
		Žemiau pateikiami reikalavimai taikomi kiekvienam nariui atskirai, t. y. reikalavimus turi tenkinti kiekvienas iš telkinio narių.	Žemiau pateikiami reikalavimai tenkinami kiekvieno nario atskirai, t. y. reikalavimus tenkina kiekvienas iš telkinio narių.
5.2.2.	Suderinamumas su virtualizacijos platformomis	Privalo būti suderinama su VMware ESXi 7.0 ar aukštesne versija arba lygiavertėmis virtualizacijos platformomis.	Suderinama su VMware ESXi 7.0.  Dokumentas: fortigate-vm.pdf, 7 psl.
5.2.3.	Procesorių branduolių skaičius (vCPU)	Ne mažiau 8.	Palaikomi 8 vCPU.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.4.	Palaikomos virtualios tinklo sąsajos	Ne mažiau 4.	Palaikoma 10 sąsajų.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.5.	Palaikomas pastoviosios atminties (angl. storage) kiekis	Ne mažiau 256 GB.	Palaikoma 2 TB.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.6.	Palaikomos vidinės atminties (RAM) kiekis	Ne mažiau 2 GB.	Palaikoma ne mažiau 2 GB.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.7.	Palaikomi standartai / protokolai	VPN ugniasienių sprendimo narys turi palaikyti bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą;	Palaikomas NetFlow. 

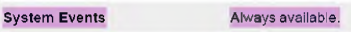
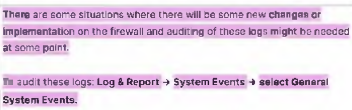
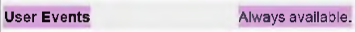
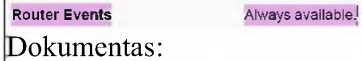
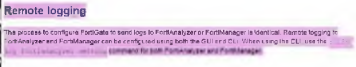
			Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 674 psl. Palaikomas sFlow.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 706 psl.
5.2.8.	VLAN palaikymas	VLAN palaikymas. Ne mažiau kaip 4000 VLAN žymių (angl. Vlan TAG) per įrenginį ir arba prievadą.	Palaikoma 4095.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1519 psl.
5.2.9.	Ugniasienės greitaveika	VPN ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas įrašymų į įvykių žurnalą – ne mažiau kaip 9 Gbps.	Ugniasienės greitaveika 9,1 Gbps  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.10.	IPsec VPN greitaveika	Ne mažiau kaip 4 Gbps.	4 Gbps.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.11.	SSL VPN greitaveika	Ne mažiau kaip 8 Gbps.	Greitaveika 8,1 Gbps.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.12.	Maksimalus sesijų skaičius vienu metu	Ne mažiau kaip 2 milijonų.	Maksimalus sesijų skaičius vienu metu 13 milijonų.  Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.13.	Maksimalus naujų sesijų skaičius per sekundę	Ne mažiau kaip 200 tūkstančių.	Maksimalus naujų sesijų skaičius per sekundę 392 tūkstančiai. 

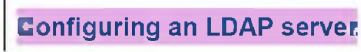
			Dokumentas: FortiGate_VM_ESXi.pdf, 7 psl.
5.2.14.	Aukšto patikimumo savybės	VPN ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; turi būti galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; turi būti galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.	VPN ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; HA active-passive cluster setup An HA Active-Passive (A-P) cluster can be set up using the GUI or CLI. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3220 psl. HA active-active cluster setup An HA Active-Active [illegible] cluster can be set [illegible] the GUI or CLI. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3226 psl. yra galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1452 psl. automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; Synchronizing the configuration Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3207 psl. automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3308 psl. yra galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema gali automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1453 psl.

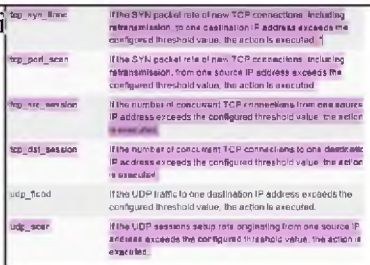
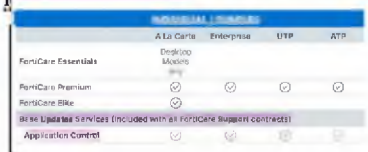
5.2.15.	Ugniasienės darbo režimai	Ne mažiau kaip : maršrutizavimo tarp skirtingų tinklų (OSI L3); skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);	Palaikomas maršrutizavimo tarp skirtingų tinklų (OSI L3) bei skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2);  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3058 psl.
5.2.16.	Maršrutizavimas	VPN ugniasienė privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing).	Palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing).  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 462 psl.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 488 psl.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 475 psl.
5.2.17.	Maršrutizavimas	VPN ugniasienė privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.	Palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1088 psl.
5.2.18.	PBR funkcionalumas	VPN ugniasienė privalo palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.	Palaiko politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą. 

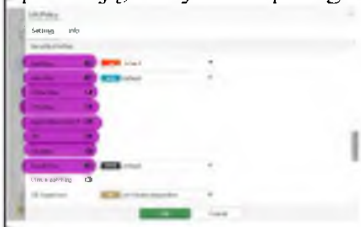
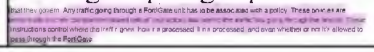
			Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 476 psl.
5.2.19.	Dinaminio maršrutizavimo protokolai	VPN ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: BGP; OSFP v2 ir v3;	Palaiko žemiau įvardintus protokolus: BGP;  Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 6 psl. OSFP v2 ir v3;  Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 12 psl.
5.2.20.	BGP funkcionalumas	VPN ugniasienė privalo turėti BGP perkrovimo (angl. graceful restart) funkcionalumą.	Turi BGP perkrovimo (angl. graceful restart) funkcionalumą. Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 971 psl.
5.2.21.	BGP konfigūracijos palaikymas	VPN ugniasienė privalo palaikyti šiuos BGP protokolo gebėjimus: BGP kaimynų grupavimą; filtravimą gaunamiems ir išsiunčiamiems maršrutams; Local Preference; MED; AS prepend; Route-reflector funkcionalumą BGP BFD;	Palaiko šiuos BGP protokolo gebėjimus: BGP kaimynų grupavimą;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 965 psl. filtravimą gaunamiems ir išsiunčiamiems maršrutams;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 982 ir 983 psl. Local Preference;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1084 psl. MED;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 968 psl.

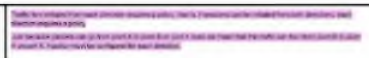
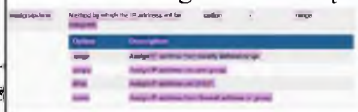
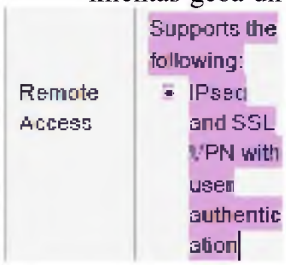
			AS prepend;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1083 psl. Route-reflector funkcionalumą;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 990 psl. BGP BFD;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 980 psl.
5.2.22.	OSPF funkcionalumas	VPN ugniasienė privalo turėti grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.	Turi grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1032-1033 psl.
5.2.23.	BFD palaikymas	VPN ugniasienė privalo palaikyti BFD (angl. bidirectional forwarding detection) protokolą.	Palaiko BFD (angl. bidirectional forwarding detection) protokolą.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 582 psl.
5.2.24.	Jumbo paketai	VPN ugniasienė turi palaikyti Jumbo paketus.	Palaiko Jumbo paketus. MTU konfigūruojamas priklausomai nuo virtualizacijos infrastruktūros galimybių.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 191 psl.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1502 psl.
5.2.25.	Adresų transliavimo funkcionalumas	VPN ugniasienė privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: NAT64; Statinis adresų transliavimas; Dinaminis adresų transliavimas keičiant prievadus (PAT).	Palaiko žemiau įvardintą funkcionalumą: NAT64;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 747 psl. Statinis adresų transliavimas;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1576 psl.

			Dinaminis adresų transliavimas keičiant prievadus (PAT).  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1578 psl.
5.2.26.	Integracija su SNMP (angl. Simple Network Management Protocol) įrenginio būsenos stebėjimui	Privalo palaikyti SNMP protokolo 2 ir 3 versijas.	Palaiko SNMP v1/v2c ir v3 versijas. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3358 psl.
5.2.27.	Suderinamumas su Syslog	VPN ugniasienių sprendimo narys turi būti suderinamas su Syslog standartu.	Yra suderinamas su Syslog standartu. • RFC 5424: The Syslog Protocol Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 16 psl.
5.2.28.	Žurnalinių įvykių (event log) palaikymas	VPN ugniasienė privalo palaikyti žemiau įvardintus žurnalinius įvykius: Sisteminiai/ administravimo; VPN; naudotojų autentifikavimo; maršrutizavimo;	Palaiko žemiau įvardintus žurnalinius įvykius: Sisteminiai/ administravimo;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl.  Dokumentas: Administration_logs.pdf, 2 psl. VPN; Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl. naudotojų autentifikavimo;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl. maršrutizavimo;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl.
5.2.29.	Žurnalinių įvykių kaupimas	VPN ugniasienė privalo gebėti įvykių žurnalinius įrašus siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.	Geba įvykių žurnalinius įrašus siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3988 psl.
5.2.30.	Diagnostikos priemonės	Privalomas srauto / paketų nuo konkretaus interfeiso	Palaikomas srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (angl. packet capture) diagnostikos

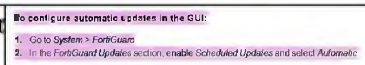
		„įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 854 psl.
5.2.31.	Nutolusių naudotojų duomenų bazių palaikymas	VPN ugniasienė privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: LDAP; RADIUS; TACACS+; SAML;	Palaiko žemiau įvardintas duomenų bazes: LDAP;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2895 psl. RADIUS;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2913 psl. TACACS+;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2983 psl. SAML;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2957 psl.
5.2.32.	SSL šifruotas srautas	VPN ugniasienė turi gebėti dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. VPN ugniasienė privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Privalo būti galima nurodyti kuris duomenų srautas turi būti dešifruojamas.	Gebėti dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2255 psl. Palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2255 psl. Yra galima nurodyti kuris duomenų srautas turi būti dešifruojamas.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2256 psl.
5.2.33.	DoS apsauga	VPN ugniasienė privalo leisti riboti sesijų arba paketų per	Leidžia riboti sesijų ir paketų per sekundę skaičius jų šaltiniui arba adresatui.

		sekundę skaičius jų šaltiniui arba adresatui.	 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1566 psl.
5.2.34.	Aplikacijų valdymas	VPN ugniasienė privalo palaikyti: aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 2000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienės garantinio aptarnavimo laikotarpiui; aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.	Palaiko: aplikacijų identifikavimą ir kontrolę. **Application control** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2013 psl. Identifikuoja daugiau nei 2000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa).  uoroda internete: https://www.fortiguard.com/appcontrol Aplikacijų aprašai įskaičiuoti į pasiūlymo kainą ugniasienės garantinio aptarnavimo laikotarpiui; **FORTICARE SUPPORT SERVICES AND INCLUDED SERVICES**  Dokumentas: og-fortiguard.pdf, 3 psl. aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą. Creating IPS and application control sign Dokumentas: Custom_IPS_and_Application_Control_Signature-7.6-Syntax_Guide.pdf, 6 psl.
5.2.35.	Sesijų laiko kontrolė	Turi būti galimybė nustatyti VPN sesijos laiką, po kurio neaktyvi sesija yra uždaroma.	Yra galima nustatyti VPN sesijos laiką, po kurio neaktyvi sesija yra uždaroma. idle-timeout Agentless VPN disconnects if idle for specified time in seconds Dokumentas:

			FortiOS-7.6.3-CLI_Reference.pdf, 2154 psl.
5.2.36.	Duomenų srautų kontrolės taisyklės	Kuriant duomenų srautų kontrolės taisyklės privalo būti galima nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį, servisą/prievadą, prievadų zoną, aplikaciją, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Privalo būti galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.	Kuriant duomenų srautų kontrolės taisyklės yra galima nurodyti: siuntėjo IP adresą ar potinklį; **Source address(es)** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1509 psl. gavėjo IP adresą ar potinklį; **Destination address** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. siuntėjo šalį panaudojant Geography tipo objektą; **Geography** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1687 psl. gavėjo šalį panaudojant Geography tipo objektą; **Geography** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1687 psl. servisą/prievadą; **Service** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. prievadų zoną;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 240 psl. aplikaciją, taikytinas apsaugos priemones;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1517 psl. vartotoją, vartotojų grupę. **User/group** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. Yra galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones. 

			 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1508-1509 psl.
5.2.37.	Duomenų srautų kontrolės taisyklių naudojimo stebėjimas	VPN ugniasienė privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).	Rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count). Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1535 psl.
5.2.38.	VPN funkcionalumas	VPN ugniasienė privalo turėti žemiau įvardintą VPN funkcionalumą: • leisti redaguoti SSL VPN portalą; • leisti skirtingoms vartotojų grupėms priskirti skirtingus IP adresų rėžius; • leisti naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); • nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais; • nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) privalo būti to paties gamintojo kaip ir siūlomos ugniasienės gamintojas arba skirtingų gamintojų, suderinamas bendram darbui. Jei siūlomas skirtingo gamintojo VPN klientas (programinė įranga) nei ugniasienės gamintojas, turi būti pateikti skirtingų gamintojų raštiški patvirtinimai, kad siūlomas sprendimas yra visiškai suderinamas bendram darbui su ugniasiene; • nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti skaitmeninius	Turėi žemiau įvardintą VPN funkcionalumą: • leidžia redaguoti SSL VPN portalą;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2748 psl. • leidžia skirtingoms vartotojų grupėms priskirti skirtingus IP adresų rėžius;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 2057 psl. • leidžia naudotis SSL VPN WEB naršyklės pagalba (be papildomos aplikacijos / agento); Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2764 psl. • nuotolinio prisijungimo naudotojo VPN klientas geba dirbti IPSec ir SSL protokolais;  Dokumentas: FortiClient_7.4.3_Administration_Guide.pdf, 10 psl. • nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) yra to paties gamintojo kaip ir siūlomos ugniasienės;  Dokumentas: FortiClient_7.4.3_Administration_Guide.pdf, 6-7 psl.

		sertifikatus tapatybės nustatymui; • nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti funkcionalumą, leidžiantį naudoti naršyklę naudotojo autentifikacijai SAML protokolu; • IKev1 ir IKEv2 palaikymas.	• nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti skaitmeninius sertifikatus tapatybės nustatymui; • Certificate authentic Dokumentas: FortiClient_7.4.3_Administration_Guide.pdf, 11 psl. • nuotolinio prisijungimo naudotojo VPN klientas palaiko funkcionalumą, leidžiantį naudoti naršyklę naudotojo autentifikacijai SAML protokolu; SAML support for SSL VPN Dokumentas: FortiClient_7.4.3_Administration_Guide.pdf, 69 psl. • IKev1 ir IKEv2 palaikymas. IKE Version Either 1 or 2. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2316 psl.
5.2.39.	IPSec kriptografijos algoritmai	VPN ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptografijos algoritmus: • AES128; • AES256.	Palaiko žemiau įvardintus IPSec kriptografijos algoritmus: • AES128; • AES128: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl. • AES256. • AES256: a 128-bit block algorithm that uses a 256-bit key Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl.
5.2.40.	IPSec maišos algoritmai	VPN ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus: • SHA-256; • SHA-512.	Palaiko žemiau įvardintus IPSec maišos algoritmus: • SHA-256; • SHA256: a 256-bit message digest. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl. • SHA-512. • SHA512: a 512-bit message digest. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl.
5.2.41.	Srauto ribojimas	VPN ugniasienė privalo leisti riboti srautą ir taikyti QoS (angl. Quality of Service) per taisyklę.	VPN ugniasienė leidžia riboti srautą ir taikyti QoS (angl. Quality of Service) per taisyklę. Traffic shaping policy Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1738 psl.
5.2.42.	Aprašų, atnaujinimas	VPN ugniasienė privalo galėti automatiškai, reguliariai,	VPN ugniasienė geba automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.

		nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.	 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3422 psl.
5.2.43.	Sprendimo valdymo sąsajos reikalavimai	Turi turėti intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galėtų kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.	Turi intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galėtų kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 41 psl.

5.3. Privilegijuotos prieigos valdymo komponento reikalavimai

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
5.3.1.	Sprendimas	Specializuotas privilegijuotos prieigos valdymo sprendimas su integruota slaptažodžių spinta ir nuotoliniu slaptažodžių valdymu (angl. PAM).	Bus teikiamas specializuotas privilegijuotis prieigos valdymo sprendimas su integruota slaptažodžių spinta ir nuotoliniu slaptažodžių valdymu (angl.PAM). **Introduction** 5.3.1 Delinea Secret Serveris an enterprise-grade password management solution designed to help organizations securely store, manage, and control access to privileged credentials. It aims to improve the security of sensitive data, reduce the risk of data breaches, and streamline the password management process. Dokumentas: delinea-secret-server 11.8.x.pdf 1 iš 88 psl.
5.3.2.	Sprendimo lokacija	Sprendimas turi būti įdiegtas Perkančiosios organizacijos infrastruktūroje (angl. on-premise) arba Perkančiosios organizacijos infrastruktūroje (angl. on-premise) su galimybe naudotis hibridinės viešosios debesijos (angl. cloud) pagrindu veikiančiais komponentais, tačiau paskyros ir slaptažodžiai turi būti saugomi lokalioje (angl. on-premise) infrastruktūroje.	Sprendimas bus įdiegtas perkančiosios organizacijos infrastruktūroje (angl. on-premise) su galimybe naudotis hibridinės viešosios debesijos (angl. cloud) pagrindu veikiančiais komponentais, tačiau paskyros ir slaptažodžiai bus saugomi lokalioje (angl. on-premise) infrastruktūroje. 5.3.2 **Secret Server Vault** / **Delinea Essentials** / **Secret Server Professional** / **Delinea Standard*** / **Secret Server Platinum** Deployment: On-premises / Cloud / On-premises / Cloud / On-premises Dokumentas: delinea-secret-server 11.8.x.pdf 1 iš 88 psl. Naudojamas cloud componentas yra privileged remote access. 5.3.2 Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through Remote Desktop Protocol (RDP) and Secure Socket Shell (SSH), with no need for a Virtual Private Network (VPN). Dokumentas: Delinea-Platform.pdf 8 iš 782 psl. Integracija apribota tik nuotolinei prieigai, paslaptys saugomi slaptažodžių saugykloje. **Manually Integrate Secret Server On Premise** 5.3.2 The integration of Secret Server On Premise (SSOP) with the Delinea Platform is limited to the Remote Access use case only. To use this integration, you must launch a Remote Access session from a vaulted secret stored in Secret Server On Premise. No secret server capabilities, such as lifecycle management, can be managed from the platform interface at this time.

<table>
<tr><td></td><td></td><td></td><td>Dokumentas: Delinea-Platform.pdf 737-738 iš 782 psl.</td></tr>
<tr><td>5.3.3.</td><td>Sprendimo naudotojų kiekis</td><td>Ne mažiau nei 100. Įsigyjant papildomas licencijas turi būti galimybė plėsti iki 500.
Ne mažiau nei 50 vienu metu prie apsaugotų sistemų prisijungusių paslaugų naudotojų. Įsigyjant papildomas licencijas turi būti galimybė plėsti iki 100.</td><td>Bus suteikta 100 vnt. naudotojų licencijų. Naudotojai licencijuojami per vieną naudotoją (vardiniai). Yra galimybė plėsti neribotai įsigyjant papildomas licencijas.
Taip pat bus suteikta 50 bendrinių (concurrent), nuotolinio prisijungimo, hibridinio PRA sprendimo licencijų, kurias taip pat galima plėsti įsigyjant papildomas licencijas.
<table><tr><th>Delinea Standard*</th><th>Secret Server Platinum</th><th>Delinea Enterprise</th></tr><tr><td>Cloud</td><td>On-premises</td><td>Cloud</td></tr><tr><td>15 included</td><td>Licensed by User</td><td>30 included</td></tr></table>Dokumentas: Delinea Platform and Secret Server onprem feature comparizon 2024-2025.pdf 1 pls.

5.3.3 PRA concurrent user licenses entitle users on that tenant to connect to remote systems using PRA . Each concurrent user license is consumed by one user when they start their first remote connection. Each user is entitled to a maximum of 4 concurrent remote sessions. The license continues to be in use by that user for the total duration of all their concurrent remote sessions until their last remote session ends. At this time the license is released for use by other users.
Dokumentas: Delinea Platform.pdf 307 iš 782 pls.

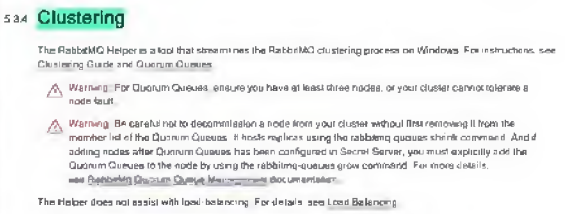
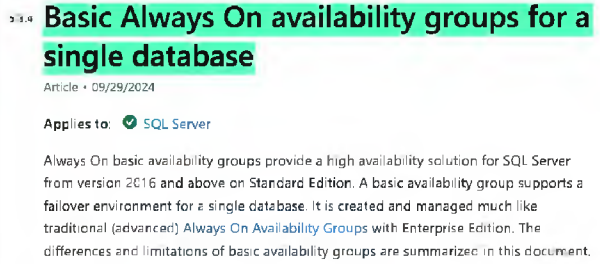
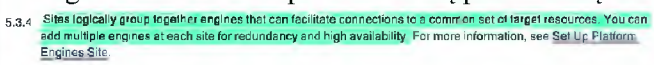
Leidžia vienu metu dirbti 50 naudotojų.
<table><tr><th>Session Type</th><th># of PRA Workloads</th><th># of Concurrent Sessions</th></tr><tr><td>SSH</td><td>1</td><td>200</td></tr><tr><td>RDP</td><td>1</td><td>100</td></tr></table>Dokumentas: Delinea-Platform.pdf 218 iš 782 psl.</td></tr>
<tr><td>5.3.4.</td><td>Architektūra</td><td>Sprendimas turi palaikyti diegimą tiek fizinėje, tiek virtualioje aplinkoje arba būti hibridinė debesijos paslauga. Visi sprendimo komponentai turi būti sukonstruoti, kad sprendimas atitiktų aukštą patikimumą (angl. High Availability).</td><td>Sprendimas palaiko diegimą on-premises:
<table><tr><th>Platinum</th></tr><tr><td>On-Premises</td></tr><tr><td>No Limits</td></tr><tr><td>Licensed by User</td></tr></table>Dokumentas: delinea-secret-server 11.8.x.pdf 8 iš 2009 psl.

Siūlomą sprendimą galima diegti į virtualias ir fizines mašinas:

upgrading.
5.3.4 ▪ System Requirements apply to both physical and virtual machines.
Dokumentas: delinea-secret-server 11.8.x.pdf 89 iš 2009 psl.

Siūloma hibridinė dalis nuotolinei prieigai yra Privileged remote access

5.3.4 Delinea PRA runs on the Delinea Platform and seamlessly integrates with Delinea Secret Server vault, deployed from the cloud or from within your private network. PRA automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity without exposing sensitive parts of credentials to the end user. PRA usage is completely integrated into the Delinea Platform UI.
Dokumentas: Delinea-Platform.pdf 244 iš 782 psl.</td></tr>
</table>

			Sprendimas Palaiko aukšto patikimumo konfigūraciją. <table><tr><th>Feature</th><th>Vault</th><th>Professional</th><th>Platinum</th></tr><tr><td>Resilient Secrets (DR)</td><td></td><td>add-on</td><td>add-on</td></tr><tr><td>Unlimited Admin Mode for Emergencies ("break the glass")</td><td>•</td><td>•</td><td>•</td></tr><tr><td>High Availability / Clustering</td><td></td><td>add-on</td><td>•</td></tr></table> Dokumentas: delinea-secret-server 11.8.x.pdf 11 iš 2009 psl. Sprendimo komponentai palaiko aukštą patikimumą  5.3.4 Clustering The RabbitMQ Helper is a tool that streamlines the RabbitMQ clustering process on Windows. For instructions, see Clustering Guide and Quorum Queues. Warning: For Quorum Queues, ensure you have at least three nodes, or your cluster cannot tolerate a node fault. Warning: Be careful not to decommission a node from your cluster without first removing it from the member list of the Quorum Queues. If node replicas using the rabbitmq-queues shrink command. And if adding nodes after Quorum Queues has been configured in Secret Server, you must explicitly add the Quorum Queues to the node by using the rabbitmq-queues grow command. For more details, see RabbitMQ Quorum Queue Management documentation. The Helper does not assist with load balancing. For details, see Load Balancing. Dokumentas: delinea-rabbitmq-helper.pdf xlix i 108 psl. SQL komponentui naudojamas SQL alwaysOn sprendimas.  5.3.4 Basic Always On availability groups for a single database Article • 09/29/2024 Applies to: SQL Server Always On basic availability groups provide a high availability solution for SQL Server from version 2016 and above on Standard Edition. A basic availability group supports a failover environment for a single database. It is created and managed much like traditional (advanced) Always On Availability Groups with Enterprise Edition. The differences and limitations of basic availability groups are summarized in this document. Dokumentas: sql-sql-server-ver16.pdf 1296 pdf psl. Privileged remote access palaiko aukštą patikimumą  5.3.4 Sites logically group together engines that can facilitate connections to a common set of target resources. You can add multiple engines at each site for redundancy and high availability. For more information, see Set Up Platform Engines Site. Dokumentas: delinea-platform.pdf 245 iš 782 psl.
		Jei sprendimo aukšto patikimumo veikimui naudojamas srauto balansavimas (angl. load balancer), Tiekėjas pateiks reikalingų parametrų srauto balansavimo sprendimą.	Sprendimo aukšto patikimumo veikimui bus naudojamas srauto balansavimas (angl. load balancer), Tiekėjas pateiks srauto balansavimo komponentus: FAD-VM04 Application Delivery Controller - virtual appliance for all supported platforms. Supports up to 4 x vCPU cores. 2 vnt. FC-10-AVM04-248-02-36 FortiCare Premium Support 2 vnt. FAD-VM01 Application Delivery Controller - virtual appliance for all supported platforms. Supports up to 1 x vCPU cores. 1 vnt. FC-10-AVM01-248-02-36 FortiCare Premium Support 1 vnt.

		Jei riboto pasiekiamumo tinklo lokacijų valdymui sprendimas naudoja papildomus komponentus, šie komponentai turi gebėti veikti aukšto patikimumo režimu. Sprendimo nuotoliniu būdu valdomoje įrangoje ar sistemose neturi būti diegiami agentai ar kita su sprendimu susijusi programinė įranga.	Privileged remote access HA 5.3.4 Sites logically group together engines that can facilitate connections to a common set of target resources. You can add multiple engines at each site for redundancy and high availability. For more information, see Set Up Platform Engines Site. Dokumentas: delinea-platform.pdf 245 iš 782 psl. 5.3.4 ▪ Delinea recommends installing a minimum of two Platform Engines per site with PRA capabilities Note: This setup will support remote session balancing in order to ensure high availability for remote sessions. PRA efficiently distributes the sessions across workloads on multiple engines, irrespective of the host operating systems. Dokumentas: delinea-platform.pdf 255 iš 782 psl. Sprendimas gali veikti agentless režimu, nereikia į valdomus serverius diegti papildomos programinės įrangos. Next-Gen Privileged Remote Access 5.3.4 ▪ Launch secure VPN-less browser-based SSH and RDP sessions with a single click ▪ Agentless deployment – no additional software is required on target hosts ▪ No end-user clients required – based on a modern HTML5-based web client ▪ Zero impact on customer security posture – no inbound firewall rules to open ▪ Agentless session recording to meet customers' audit and compliance requirements Dokumentas: delinea-platform.pdf 772 iš 782 psl.
		Sprendimas turi gebėti saugiai suteikti prieigą prie valdomos infrastruktūros RDP ir SSH protokolais, be VPN, agentų ar kitos į kliento kompiuterį diegiamos programinės įrangos.	VPN'less RDP ir SSH 5.3.4 Privileged Remote Access Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through RDP (Remote Desktop Protocol) and SSH (Secure Socket Shell), without the need for a VPN (Virtual Private Network). Delinea PRA runs on the Delinea Platform and seamlessly integrates with Delinea Secret Server vault, deployed from the cloud or from within your private network. PRA automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity without exposing sensitive parts of credentials to the end user. PRA usage is completely integrated into the Delinea Platform UI. Delinea PRA displays RDP and SSH sessions in the user's web browser, freeing users from the need to install and maintain additional remote access or VPN software. This architecture also makes PRA extremely portable. Dokumentas: delinea-platform.pdf 244-245 iš 782 psl. Sprendimas gali veikti agentless režimu, nereikia į valdomus serverius diegti papildomos programinės įrangos. Next-Gen Privileged Remote Access 5.3.4 ▪ Launch secure VPN-less browser-based SSH and RDP sessions with a single click ▪ Agentless deployment – no additional software is required on target hosts ▪ No end-user clients required – based on a modern HTML5-based web client ▪ Zero impact on customer security posture – no inbound firewall rules to open ▪ Agentless session recording to meet customers' audit and compliance requirements Dokumentas: delinea-platform.pdf 772 iš 782 psl.
5.3.5.	Avarinio atstatymo veikimas	Sprendimas turi gebėti sinchronizuoti privilegijuotas paskyras į kitame duomenų centre esantį privilegijuotos prieigos sprendimą.	Sprendimas gali sinchronizuoti privilegijuotas paskyras į kitą duomenų centrą. 5.3.5 Disaster Recovery and Resilient Secrets Resilient Secrets Coverage Overview The Resilient Secrets (RS) feature is tailored to replicate data from a primary data source to a secondary data replica. The features and specific data replicated do not constitute the entirety of an instance of Secret Server. Instead, replicates the prioritized vital data and functionality needed so that, in the event of an outage of the primary data source, the most important information and functionality can be accessed on the secondary data replica to aid restoring the primary data source while keeping minimal operations running. Dokumentas: delinea-secret-server 11.8.x.pdf 448 iš 2009 psl.
		Sprendimas turi veikti skaitymo rėžimu (angl. Read Only). Esant poreikiui turi būti galimybė perjungti sistemų valdymą iš pagrindinio privilegijuotos prieigos	Sprendimas gali veikti skaitymo režimu: Best Practices 5.3.5 ▪ Read-Only Mode. Replicas should be in read-only mode during operation because there can only be one source of truth - the Source instance. Dokumentas: delinea-platform.pdf 743 iš 782 psl. Galimybė perjungti sistemų valdymą iš avarinės prieigos replikos.

		sprendimo į avarinės prieigos sprendimą.	5.3.5 Resilient Secrets Coverage Overview The Resilient Secrets (RS) feature is tailored to replicate data from a primary data source to a secondary data replica. The features and specific data replicated do not constitute the entirety of an instance of Secret Server. Instead, replicates the prioritized vital data and functionality needed so that, in the event of an outage of the primary data source, the most important information and functionality can be accessed on the secondary data replica to aid restoring the primary data source while keeping minimal operations running. Dokumentas: delinea-secret-server 11.8.x.pdf 448 iš 2009 psl.
		Avarinio atstatymo sprendimas turi palaikyti šias funkcijas: • turi būti replikuojamos integracijos su katalogų tarnybomis (angl. Active Directory); • turi leisti autentifikuoti naudotojus su katalogų tarnybomis; • turi leisti naudoti kvantiniams kompiuteriams atsparų šifravimą; • turi leisti replikuoti pagrindiniame privilegijuotos prieigos sprendime naudojamus SSH šifravimo algoritmus. • turi būti replikuojama katalogų struktūra iš pagrindinio privilegijuotos prieigos sprendimo. • turi būti replikuojamos katalogų struktūros teisės, įskaitant paveldimas ir nepaveldimas teises; • turi gebėti replikuoti asmeninius katalogus ir jų naudotojus; • turi gebėti replikuoti paslapčių šablonų apribojimus sukonfigūruotus katalogų struktūroje. • turi būti replikuojamos paslaptys, jų šablonai, pavadinimai, aktyvavimo būsena, katalogas kur paslaptis yra. • turi būti replikuojami šie paslapčių nustatymai: ▪ 2FA autentifikavimo nustatymas;	Avarinio atstatymo sprendimas palaiko šias funkcijas: Replikuojama: • Yra replikuojamos replikuojamos integracijos su katalogų tarnybomis (angl. Active Directory); The only global configuration settings replicated are: ▪ Enable directory service integration. Dokumentas: delinea-secret-server 11.8.x.pdf 449 iš 2009 psl. • leidžia autentifikuoti naudotojus su katalogų tarnybomis; ▪ Allow authentication against directory services. Dokumentas: delinea-secret-server 11.8.x.pdf 449 iš 2009 psl. • Leidžia naudoti kvantiniams kompiuteriams atsparų šifravimą; ▪ Allow quantum state encryption Dokumentas: delinea-secret-server 11.8.x.pdf 449 iš 2009 psl. • leidžia replikuoti pagrindiniame privilegijuotos prieigos sprendime naudojamus SSH šifravimo algoritmus. The SSH cipher suite configuration is replicated. Dokumentas: delinea-secret-server 11.8.x.pdf 449 iš 2009 psl. • yra replikuojama katalogų struktūra iš pagrindinio privilegijuotos prieigos sprendimo. Folders are replicated, along with extended values associated with their function: ▪ Subfolders and the entire tree structure, as specified by the RS configuration. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • yra replikuojamos katalogų struktūros teisės, įskaitant paveldimas ir nepaveldimas teises; ▪ Any permissions associated with the folder, including whether or not to inherit them from its parent folder. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • geba replikuoti asmeninius katalogus ir jų naudotojus;

		▪ laikinas paslapties užrakinimas vienam naudotojui; ▪ reikalavimas palikti komentarą; ▪ SSH sesijos paleidimo per tarpinį serverį reikalavimas; ▪ slaptažodžio slėpimo nustatymas. • jeigu paslapčių laukuose saugomi failai, kaip SSH raktai, sertifikatai ar kt. šie laukai taip pat turi būti replikuojami; • turi būti replikuojama paslapties laukų istorija; • turi būti replikuojami paslapčių paleidikliai ir su jais susijusi informacija: ▪ paleidiklių laukai; ▪ paleidiklių sujungimai su paslapčių šablonais ir jų konfigūracija; ▪ paleidiklių asociacijos su privilegijuotomis paskyromis. • turi būti replikuojami sąrašai su šią informacija: ▪ kategorijos; ▪ kategorijų narių įrašai; ▪ sąrašų priskyrimai komandoms; ▪ sujungimai su paslaptimis. • turi būti replikuojami paslapčių ir katalogų struktūros metaduomenys; • turi būti replikuojamos	▪ For personal folders, the associated user. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • geba replikuoti paslapčių šablonų apribojimus sukonfigūruotus katalogų struktūroje. ▪ Secret template restrictions placed on folders. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • yra replikuojamos paslaptys, jų šablonai, pavadinimai, aktyvavimo būsena, katalogas kur paslaptis yra. Secrets are replicated along with essential information relating to them: ▪ The template, active status, name, and the folder the secret is in. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • yra replikuojami šie paslapčių nustatymai: ▪ 2FA autentifikavimo nustatymas; ▪ Several secret settings, including: • Multi-factor authentication required Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. ▪ laikinas paslapties užrakinimas vienam naudotojui; • Check out enabled or RPC interval Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. ▪ reikalavimas palikti komentarą; • Require comment Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. ▪ SSH sesijos paleidimo per tarpinį serverį reikalavimas; • SSH proxy enabled Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. ▪ slaptažodžio slėpimo nustatymas. • Hide launcher password Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • jeigu paslapčių laukuose saugomi failai, kaip SSH raktai, sertifikatai ar kt. šie laukai taip pat yra replikuojami; ▪ The secret field, item value, and whether or not it is a file attachment. If it is a file attachment, its contents are replicated as well Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl. • yra replikuojama paslapties laukų istorija; ▪ Audits are not replicated, but, for data integrity, secret item history, including the history of file attachments, is replicated. Dokumentas: delinea-secret-server 11.8.x.pdf 450 iš 2009 psl.

		sukonfigūruotos rolės ir teisės, bei jų priskyrimai naudotojams ar grupėms; • turi būti replikuojami šie paslapčių šablonų parametrai: • nustatymai, teisės, laukai; • slaptažodžių reikalavimai, taisyklės ir slaptažodžių simbolių rinkiniai; • turi būti replikuojamos lokacijos (angl. sites); • turi būti replikuojamos komandos ir jų parametrai, priskyrimai lokacijoms, bei grupėms. (angl. Teams); • turi būti replikuojami naudotojai ir grupės. Replikuoti naudotojai turi būti išjungti. • turi būti išsaugomas surišimas su naudotojų ir grupių katalogų tarnybomis.	• yra replikuojami paslapčių paleidikliai ir su jais susijusi informacija: ▪ paleidiklių laukai; All launchers are replicated, along with: ▪ Their fields. Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. ▪ paleidiklių sujungimai su paslapčių šablonais ir jų konfigūracija; ▪ Mappings to secret templates. Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. ▪ paleidiklių asociacijos su privilegijuotomis paskyromis. ▪ Any default associated and privileged secrets. Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. • yra replikuojami sąrašai su šią informacija: ▪ kategorijos; All list information is replicated, including: ▪ Categories Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. ▪ kategorijų narių įrašai; ▪ Item values Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. ▪ sąrašų priskyrimai komandoms; ▪ Team restrictions Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. ▪ sujungimai su paslaptimis. ▪ Secret item mappings Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. • yra replikuojami paslapčių ir katalogų struktūros metaduomenys; All metadata on secrets and folders that are configured for replication are replicated. All Metadata on users and groups will be replicated. This includes: Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. • yra replikuojamos sukonfigūruotos rolės ir teisės, bei jų priskyrimai naudotojams ar grupėms; ***Roles and Permissions*** Roles and permissions are replicated, as are their assignments to users and groups. Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl. • yra replikuojami šie paslapčių šablonų parametrai: • nustatymai, teisės, laukai; ▪ Secret templates, their settings, permissions, and secret fields are replicated.

<table>
<tr><td></td><td></td><td></td><td>Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl.

• slaptažodžių reikalavimai, taisyklės ir slaptažodžių simbolių rinkiniai;
▪ Password requirements, associated rules, and their character sets are replicated.
Dokumentas: delinea-secret-server 11.8.x.pdf 451 iš 2009 psl.

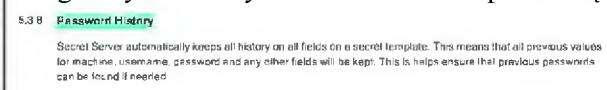
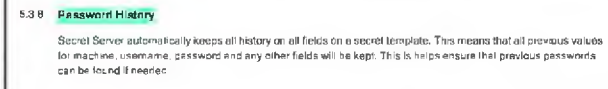
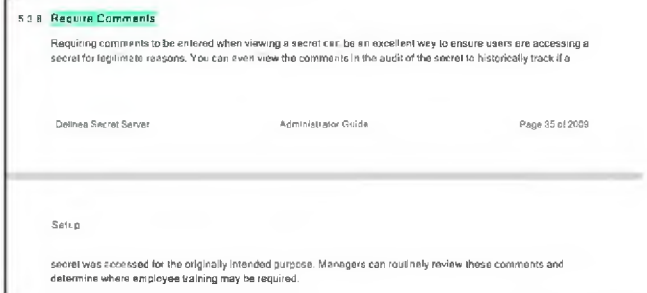
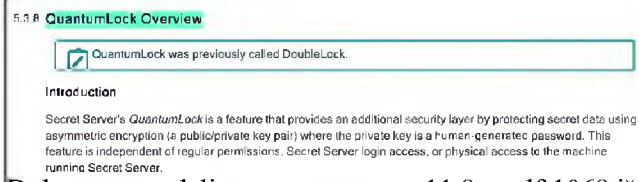
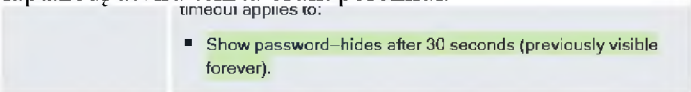
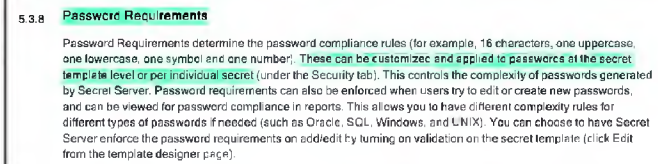
• yra replikuojamos lokacijos (angl. sites);
5.3.5 Sites
Covered Features
All sites are replicated.
Dokumentas: delinea-secret-server 11.8.x.pdf 452 iš 2009 psl.

• yra replikuojamos komandos ir jų parametrai, priskyrimai lokacijoms, bei grupėms. (angl. Teams);
5.3.5 Teams
All teams are replicated, along with their group and site mappings.
Dokumentas: delinea-secret-server 11.8.x.pdf 452 iš 2009 psl.

• yra replikuojami naudotojai ir grupės. Replikuoti naudotojai turi būti išjungti.
All users and groups in the system are replicated and, for licensing purposes, we recommend the RS configuration be set to having users inactive by default and only enable the ones needed for vital access. User accessibility is maintained between source and replica. Group memberships are replicated and any associated roles and permissions mapped to them will come across as well.
Dokumentas: delinea-secret-server 11.8.x.pdf 452 iš 2009 psl.

• yra išsaugomas surišimas su naudotojų ir grupių katalogų tarnybomis.
Any directory services on the source is replicated to the data replica, and all users and groups mapped to these services retain system accessibility, provided the data replica is on a network that can reach the service endpoint.
Dokumentas: delinea-secret-server 11.8.x.pdf 452 iš 2009 psl.</td></tr>
<tr><td>5.3.6.</td><td>Saugomų objektų ir kredencialų kiekis slaptažodžių spintoje</td><td>Nemažiau kaip 10000.</td><td>Saugomi kredencialai ir objektai siūlomame sprendime vadinami secrets.
5.3.6
5.3.7
<table><tr><th></th><th>Secret Server Vault</th><th>Delinea Essentials</th><th>Secret Server Professional</th><th>Delinea Standard*</th><th>Secret Server Platinum</th><th>Delinea Enterprise</th></tr><tr><td>Deployment</td><td>On-premises</td><td>Cloud</td><td>On-premises</td><td>Cloud</td><td>On-premises</td><td>Cloud</td></tr><tr><td>User Limit</td><td>25 Users Included</td><td>15 included</td><td>Licensed by User</td><td>15 included</td><td>Licensed by User</td><td>30 included.</td></tr><tr><td>Secrets</td><td>Unlimited for on-prem</td><td>10,000 Secrets Max</td><td>Unlimited for on-prem</td><td>No Limits</td><td>Unlimited for on-prem</td><td>No Limits</td></tr></table>Dokumentas: Delinea Platform and Secret Server onprem feature comparizon 2024-2025.pdf 1 pls.</td></tr>
<tr><td>5.3.7.</td><td>Sprendimo palaikomų sistemų (serverių, darbo vietų, tinklo, saugumo ir kitos nuotoliniu</td><td>Nemažiau kaip 10000.</td><td>Saugomi kredencialai ir objektai siūlomame sprendime vadinami secrets.
5.3.6
5.3.7
<table><tr><th></th><th>Secret Server Vault</th><th>Delinea Essentials</th><th>Secret Server Professional</th><th>Delinea Standard*</th><th>Secret Server Platinum</th><th>Delinea Enterprise</th></tr><tr><td>Deployment</td><td>On-premises</td><td>Cloud</td><td>On-premises</td><td>Cloud</td><td>On-premises</td><td>Cloud</td></tr><tr><td>User Limit</td><td>25 Users Included</td><td>15 included</td><td>Licensed by User</td><td>15 included</td><td>Licensed by User</td><td>30 included.</td></tr><tr><td>Secrets</td><td>Unlimited for on-prem</td><td>10,000 Secrets Max</td><td>Unlimited for on-prem</td><td>No Limits</td><td>Unlimited for on-prem</td><td>No Limits</td></tr></table></td></tr>
</table>

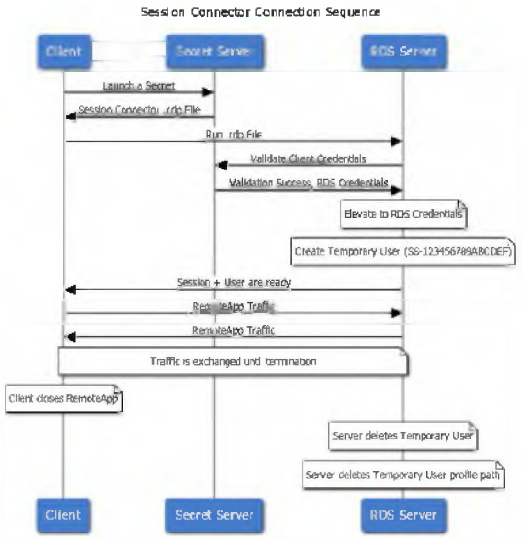
	būdu valdomos įrangos) kiekis		Dokumentas: Delinea Platform and Secret Server onprem feature comparizon 2024-2025.pdf 1 pls.
5.3.8.	Slaptažodžių spinta	Turi leisti saugoti šią jautrią informaciją: • slaptažodžiai; • SSH privataus/viešo rakto poros; • sertifikatai su privačiais raktais; • API raktai; • PIN kodai; • bylos; • programinės įrangos licencijų raktai.	Leidžia saugoti išvardintą informaciją naudojantis gamintojo iš anksto paruoštais šablonais: 5.3.8 ▪ Password ▪ Pin 5.3.8 ▪ SSH Key 5.3.8 ▪ Product License Key Dokumentas: delinea-secret-server 11.8.x.pdf 1146-1147 iš 2009 psl. Kita reikalaujamą informaciją: Bylos, API raktai, sertifikatai su privačiu raktu, gali būti saugomi prie šablonų pridedant reikiamus laukus. 5.3.8 ▪ File: File attachment link. File attachments are stored in the Microsoft SQL Server database. 5.3.8 ▪ Password: Password type text-entry field. Dokumentas: delinea-secret-server 11.8.x.pdf 1164 iš 2009 psl.
		Kiekvienas slaptažodis turi būti šifruotas individualiu šifravimo raktu.	Kiekvienas slaptažodis yra šifruotas individualiu šifravimo raktu Secret Key Rotation Overview 5.3.8 Secret key rotation is a somewhat similar process to RPC by which the encryption key, used for securing secret data, is changed and that secret data is re-encrypted. Each secret receives a new, unique AES-256 key. Secret key rotation can be used to meet compliance requirements that mandate encryption keys be changed on a regular basis. Dokumentas: delinea-secret-server 11.8.x.pdf 1441 iš 2009 psl.
		Turi būti realizuotas slaptažodžio maskavimas (nerodymas). Slaptažodžio rodymas/nerodymas turi būti laisvai konfigūruojamas.	Yra realizuotas slaptažodžio maskavimas. 5.3.8 Feature | Vault | Professional | Platinum Password Hiding | • | • | • Dokumentas: delinea-secret-server 11.8.x.pdf 8 iš 2009 psl. Slaptažodios slėpimas nuo naudotojo paleidžiant sesijas. 5.3.8 Hide Launcher Password Many times, giving an employee access to a resource through Secret Server does not require that he or she have access to the actual password for the account used. As long as the application a user needs can be started by the launcher, there is no reason the user needs to copy/paste or type the password. The hide launcher password setting implements the following: ▪ Users with access to the secret will see only asterisks (****) in the password field ▪ There will be no copy-to-clipboard, field history, or unmask icons next to the field Delinea Secret Server Administrator Guide Page 34 of 2009 Setup Users with edit permissions to a secret with "hide launcher password" enabled can still view the password when editing the secret. To prevent all possible access to the password, limit users to view permission only. This can be an important way to reduce exposure of your privileged account passwords. Hiding launcher passwords can be enabled for secrets under the Security tab of a secret or by applying a secret policy. You can also remove the ability for a user to see the password for any secret with a launcher by removing the "view launcher password" permission from their role.

			Dokumentas: delinea-secret-server 11.8.x.pdf 34-35 iš 2009 psl.
		Turi būti galimybė nustatyti ir kontroliuoti slaptažodžio istorijos įrašų kiekį.	Yra galimybė nustatyti ir kontroliuoti slaptažodžių istoriją:  5.3.8 Password History Secret Server automatically keeps all history on all fields on a secret template. This means that all previous values for machine, username, password and any other fields will be kept. This is helps ensure that previous passwords can be found if needed. Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009psl.
		Turi būti funkcionalumas, leidžiantis pasižiūrėti, kokie slaptažodžiai buvo naudoti praeityje (ne mažiau 10 paskutinių).	Yra funkcionalumas, leidžiantis pasižiūrėti slaptažodžių istorija:  5.3.8 Password History Secret Server automatically keeps all history on all fields on a secret template. This means that all previous values for machine, username, password and any other fields will be kept. This is helps ensure that previous passwords can be found if needed. Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009 psl.
		Turi leisti reikalauti įrašyti komentarą, kodėl peržiūrimas slaptažodis ar prašoma suteikti privilegijuotą prieigą.	Yra funkcionalumas leidžiantis įjungti reikalavimą įrašyti komentarą, kodėl peržiūrimas slaptažodis ar prašoma suteikti privilegijuotą prieigą. Komentaro reikalavimas:  5.3.8 Require Comments Requiring comments to be entered when viewing a secret can be an excellent way to ensure users are accessing a secret for legitimate reasons. You can even view the comments in the audit of the secret to historically track if a Delinea Secret Server Administrator Guide Page 35 of 2009 Setup secret was accessed for the originally intended purpose. Managers can routinely review these comments and determine where employee training may be required. Dokumentas: delinea-secret-server 11.8.x.pdf 35-36 iš 2009 psl.
		Turi leisti naudotojui uždėti papildomą slaptažodį privilegijuotos paskyros apsaugai, kuris negali būti atstatomas ar apeinamas sprendimo administratoriams.	Yra galimybė naudotojui uždėti papildomą slaptažodį privilegijuotos paskyros apsaugai, kuris negali būti atstatomas ar apeinamas sprendimo administratoriams. Naudojamas Quantum lock mechanizmas:  5.3.8 QuantumLock Overview QuantumLock was previously called DoubleLock. Introduction Secret Server's *QuantumLock* is a feature that provides an additional security layer by protecting secret data using asymmetric encryption (a public/private key pair) where the private key is a human-generated password. This feature is independent of regular permissions, Secret Server login access, or physical access to the machine running Secret Server. Dokumentas: delinea-secret-server 11.8.x.pdf 1068 iš 2009 psl.
		Turi parodyti slaptažodį atviru tekstu ten kur nėra galimybės automatizuoti privilegijuotą prisijungimą.	Rodo slaptažodį atviru tekstu esant poreikiui.  timeout applies to: 5.3.3 ▪ Show password–hides after 30 seconds (previously visible forever). Dokumentas: delinea-secret-server 11.8.x.pdf 1703 iš 2009 psl.
5.3.9.	Slaptažodžių politikos	Sprendimas turi leisti kurti laisvai modifikuojamas (angl. custom) slaptažodžių politikas.	Leidžia laisvai kurti modifikuojamas slaptažodžių politikas  5.3.8 Password Requirements Password Requirements determine the password compliance rules (for example, 16 characters, one uppercase, one lowercase, one symbol and one number). These can be customized and applied to passwords at the secret template level or per individual secret (under the Security tab). This controls the complexity of passwords generated by Secret Server. Password requirements can also be enforced when users try to edit or create new passwords, and can be viewed for password compliance in reports. This allows you to have different complexity rules for different types of passwords if needed (such as Oracle, SQL, Windows, and UNIX). You can choose to have Secret Server enforce the password requirements on add/edit by turning on validation on the secret template (click Edit from the template designer page). Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009 psl.
		Sprendimas turi leisti taikyti skirtingas slaptažodžių	Galima taikyti skirtingas slaptažodžių politikas privilegijuotų paskyrų slaptažodžiams.

		politikas privilegijuotų paskyrų slaptažodžiams.	5.3.8 **Password Requirements** Password Requirements determine the password compliance rules (for example, 16 characters, one uppercase, one lowercase, one symbol and one number). These can be customized and applied to passwords at the secret template level or per individual secret (under the Security tab). [redacted] controls the complexity of passwords generated [redacted] Secret Server. Password requirements can also be enforced when users try to edit or create new passwords. Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009 psl.
		Sprendimas turi leisti generuoti atsitiktinius slaptažodžius atitinkančius nustatytą politiką.	Leidžia generuoti atsitiktinius slaptažodžius atitinkančius nustatytą politiką: 5.3.8 **Password Requirements** Password Requirements determine the password compliance rules (for example, 16 characters, one uppercase, one lowercase, one symbol and one number). These can be customized and applied to passwords at the secret template level or per individual secret (under the Security tab). This controls the complexity of passwords generated by Secret Server. Password requirements can also be enforced when users try to edit or create new passwords, and can be viewed for password compliance in reports. This allows you to have different complexity rules for different types of passwords if needed (such as Oracle, SQL, Windows, and UNIX). You can choose to have Secret Server enforce the password requirements on add/edit by turning on validation on the secret template (click Edit from the template designer page). Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009 psl.
		Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžio politiką jo išsaugojimo, keitimo slaptažodžių spintoje metu. Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžių politiką, slaptažodžio keitimo nuotoliniu būdu metu.	Leidžia pasirinktinai kontroliuoti\nekontroliuoti slaptažodžio politiką jo išsaugojimo, keitimo slaptažodžių spintoje metu: 5.3.8 **Password Requirements** Password Requirements determine the password compliance rules (for example, 16 characters, one uppercase, one lowercase, one symbol and one number). These can be customized and applied to passwords at the secret template level or per individual secret (under the Security tab). This controls the complexity of passwords generated by Secret Server. Password requirements can also be enforced when users try to edit or create new passwords, and can be viewed for password compliance in reports. This allows you to have different complexity rules for different types of passwords if needed (such as Oracle, SQL, Windows, and UNIX). You can choose to have Secret Server enforce the password requirements on add/edit by turning on validation on the secret template (click Edit from the template designer page). Dokumentas: delinea-secret-server 11.8.x.pdf 38 iš 2009 psl. Sprendimas leidžia pasirinktinai kontroliuoti/nekontroliuoti slaptažodžių politiką, slaptažodžio keitimo nuotoliniu būdu metu: 5.3.9 **Configuring Password Policy for Secret Templates** When creating and rotating passwords for secrets inside of Secret Server, it is important to uphold strong requirements and to use Secret Server to manage changing requirements effectively. For example, Secret Server allows administrators to set the minimum password length to 6 characters, observe that a 7-character password and a 16-character password are both accepted, then change the minimum length to 8, observe that a 7-character password is then rejected but that a 16-character password is accepted. In Secret Server password requirements can be set and applied *at the Secret Template level*. To adjust requirements: Dokumentas: delinea-secret-server 11.8.x.pdf 1331 iš 2009 psl.
5.3.10.	Privilegijuotų sesijų paleidikliai	Turi leisti inicijuoti RDP ir SSH privilegijuotas sesijas į sprendimo valdomas sistemas, neatskleidžiant tikrųjų sistemos kredencialų.	Leidžia inicijuoti RDP ir SSH privilegijuotas sesijas į sprendimo valdomas sistemas, neatskleidžiant tikrųjų sistemos kredencialų. RDP proxy su laikinais kredencialais: 5.3.10 **SSH Proxy Configuration** The Secret Server proxy routes SSH and RDP sessions and helps protect the endpoint credentials. There are two configuration options for proxying: ▪ Proxy through the Secret Server Web application ▪ Proxy through a distributed engine Dokumentas: delinea-secret-server 11.8.x.pdf 811 iš 2009 psl.
		Turi būti gamintojo paruošti privilegijuotų sesijų paleidikliai.	Yra gamintojo paruošti privilegijuotų sesijų paleidikliai: 5.3.10 **Built-In Launcher Types** Secret Server launchers, supported by protocol handlers, come in three primary types: ▪ **Remote Desktop:** Launches a Windows Remote Desktop session and automatically authenticates the user to the machine. ▪ **PuTTY:** Opens a PuTTY session and authenticates the user to a Unix system. ▪ **Web Password Filler:** Uses a Chrome extension to automatically log the user into a website with secret credentials. ▪ **Web Launcher:** An alternative method to automatically log on websites. See "Web Launchers" on page 686. Dokumentas: delinea-secret-server 11.8.x.pdf 637 iš 2009 psl.
		Turi leisti kurti laisvai modifikuojamus (angl. custom) sesijų paleidiklius ir	Leidžia laisvai kurti nestandartinius paleidiklius:

		įrašyti jų naudojimo vaizdo įrašą, kai sesija užmezgama ne per įgaliotąjį serverį (angl. proxy/jumphost).	5.3.10 **Custom Launchers** Custom launchers extend the functionality of Secret Server by allowing integration with any application that can be started via the command line. They pass values from the secret text fields to the command-line of the application being launched, enabling users to initiate processes or connect to services directly from the Secret Server interface without manually entering credentials. Dokumentas: delinea-secret-server 11.8.x.pdf 637 iš 2009 psl. Galima įrašinėti nestandartinių paleidiklių sesijas: 5.3.10 **Extending Session Recording with Custom Launchers** You can configure Secret Server with custom launchers to run arbitrary programs, which can then be recorded by session recording. To do so: Dokumentas: delinea-secret-server 11.8.x.pdf 1223 iš 2009 psl.
		Turi leisti kurti paleidiklius iš Windows proceso. Turi leisti kurti paleidiklius iš kelių Windows procesų.	Leidžia kurti paleidiklius Windows proceso; 5.3.10 ▪ **Process**: use this type if you want to use secret credentials to connect directly to the remote host. This choice launches the process on the user's machine and replaces $ parameters with values from the secret and its associated secret. Dokumentas: delinea-secret-server 11.8.x.pdf 650 iš 2009 psl. Leidžia kurti paleidiklius iš keleto Windows procesų: 5.3.10 ▪ **Batch File**: Not used for this task. Launches the indicated batch file on the user's machine. Allows the script to launch multiple processes using information from the server. Recommended only for advanced users Dokumentas: delinea-secret-server 11.8.x.pdf 650 iš 2009 psl.
		Paleidikliai turi veikti naudotojo kompiuteryje (ne web serveryje). Turi būti įskiepis į interneto naršyklę web aplikacijų formų kredencialų automatiniam užpildymui arba lygiavertis funkcionalumas.	Paleidikliai veikia naudotojo kompiuteryje: 5.3.10 **Protocol Handlers** A protocol handler is an application installed on an end-user's machine that facilitates communication between Secret Server and the client machine. It also provides the necessary files for the launchers to function. When a user initiates a launcher, the protocol handler Dokumentas: delinea-secret-server 11.8.x.pdf 636 iš 2009 psl. Yra įskiepis interneto naršyklei web aplikacijų formų kredencialų automatiniam pildymui. **5.3.10 Using Secrets on Websites (Web Password Filler)** Please set up Web Password Filler (WPF) in the following order: 1. Ensure you can log in to Secret Server the conventional way. 2. If necessary, create a folder in Secret Server where the WPF secrets will reside. 3. Install the WPF browser extension. Dokumentas: delinea-secret-server 11.8.x.pdf 77 iš 88 psl.
5.3.11.	Paskyrų aptikimo automatizuoti skanavimai	Turi skanuoti ir automatizuotai aptikti šių tipų paskyras: • Windows lokalias; • Unix/Linux lokalias; • Active Directory; • VMware ESXi lokalias. Turi leisti aprašyti taisykles, kaip automatiškai įtraukti aptiktas paskyras į sprendimą pagal iš anksto apibrėžtus kriterijus.	Skanuoja ir automatizuotai aptinka šių tipų paskyras: • Windows lokalias; • Unix/Linux lokalias; • Active Directory; • VMware ESXi lokalias. **Step 8: Discovery** 5.3.11 Secret Server has a discovery feature that can automatically find local Windows accounts, Active Directory service, Unix, VMware ESXi/ESXi, and Active Directory domain accounts. Account and dependency types not supported out-of-the-box in Secret Server can still be discovered by writing PowerShell scripts that can be run as custom scanners. This allows administrators to quickly import accounts found by Secret Server on specified domains or IP addresses. Dokumentas: delinea-secret-server 11.8.x.pdf 83 iš 88 psl. Leidžia kurti taisykles ir automatiškai importuoti aptiktas paskyras į sprendimą pagal iš anksto apibrėžtus kriterijus:

			Introduction 5.3.11 Secret Server discovery roles in play a pivotal role in automating the process of finding, importing, and managing passwords, API keys, and other credentials throughout the IT environment. Dokumentas: delinea-secret-server 11.8.x.pdf 531 iš 2009 psl.
5.3.12.	Šifravimas	Visa slaptažodžių spintoje saugoma jautri informacija turi būti šifruota AES-256 arba lygiaverčiu algoritmu.	Visa slaptažodžių spintoje saugoma jautri informacija yra šifruojama AES-265 algoritimu: 5.3.12 Feature | Vault | Professional | Platinum Active Directory Integration | • | • | • AES 256 Encryption | • | • | • Dokumentas: delinea-secret-server 11.8.x.pdf 13 iš 2009 psl.
5.3.13.	„Keturios akys“	Siūlomo sprendimo administravimas turi turėti aiškiai išskirtas teises, kurios leistų realizuoti „keturių akių“ administravimo principą - vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja. Teikėjas jomis negali pasinaudoti, gavėjas negali jų sau suteikti.	Siūlomo sprendimo administravimas turi aiškiai išskirtas teises, kurios leidžia realizuoti „keturių akių“ administravimo principą - vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja. Teikėjas jomis negali pasinaudoti, gavėjas negali jų sau suteikti: 5.3.13 A user with the "Unlimited Administrator" role permission can view and edit all secrets in the system, regardless of permissions--if and only if the unlimited administration mode is enabled in the configuration settings--but the Unlimited Administrator role does not have permission to enable the mode. To enable unlimited administration mode, the Administer Configuration Unlimited Admin role permission is required. This provides dual control, ensuring no single user can enable unlimited administration mode. Of course, you can bypass this safeguard by simply assigning both roles to the same user. Dokumentas: delinea-secret-server 11.8.x.pdf 264 iš 2009 psl.
5.3.14.	Autentifikavimas	Turi palaikyti ne mažiau, kaip šiuos autentifikavimo protokolus: • Radius; • Kerberos. Turi palaikyti lokalių naudotojų ir Microsoft Active Directory naudotojų prisijungimus į web portalą. Autentifikavimo procesas į sprendimo valdomus įrenginius ar sistemas turi būti apsaugotas nuo tikrųjų kredencialų (tiek atviro teksto, tiek koduotame formate) paviešinimo prisijungimo šaltinyje (sprendimo naudotojo kompiuteryje).	Leidžia naudotojų autentifikavimui naudoti Kerberos: 5.3.14 ▪ User accounts from an Azure Active Directory tenant ▪ User accounts from another OLDAP source (Basic/Kerberos). Dokumentas: delinea-secret-server 11.8.x.pdf 25 iš 2009 psl. 5.3.14 ▪ Security. By using Kerberos or NTLM (Windows challenge/response) protocols, IWA provides robust security. Kerberos is preferred due to its stronger encryption and mutual authentication capabilities, but NTLM is used for compatibility with older systems. Dokumentas: delinea-secret-server 11.8.x.pdf 372 iš 2009 psl. 5.3.14 8. Click the **Authentication** dropdown list to select either the **Basic**, **Anonymous**, or **Kerberos** authentication method. Dokumentas: delinea-secret-server 11.8.x.pdf 510 iš 2009 psl. Sprendimas leidžia naudotojų autentifikavimui naudoti RADIUS: 5.3.14 RADIUS User Authentication Secret Server allows the use of *Remote Authentication Dial-In User Service* (RADIUS) two factor authentication on top of the normal authentication process for additional security needs. Secret Server acts as a RADIUS client that can communicate with any server implementing the RADIUS protocol. Dokumentas: delinea-secret-server 11.8.x.pdf 429 iš 2009 psl. Sprendimas leidžia naudotojus autentifikuoti AD paskyromis į web portalą. 5.3.14 Directory Services Secret Server provides a multitude of authentication options through directory services. It can sync users into the application from various LDAP sources. It is important to use an outside authentication source to automate user provisioning. The User Account Options setting in the directory services configuration provides these options: Dokumentas: delinea-secret-server 11.8.x.pdf 29 iš 2009 psl.

			Sprendimas gali apsaugoti tikruosius prisijungimo duomenis nuo paviešinimo naudotojo kompiuteryje naudojant laikinus /vienkartinius prisijungimo duomenis. **RDP Proxy** The RDP Proxy feature in Secret Server enhances security by routing Remote Desktop Protocol (RDP) connections through Secret Server, ensuring that secret credentials are protected during remote access sessions. This proxying mechanism can be configured in two ways: the recommended method, which uses temporary credentials to Dokumentas: delinea-secret-server 11.8.x.pdf 796 iš 2009 psl. 5.3.14 Figure: Session Connector Connection Sequences for an RDS Server  5.3.14 Dokumentas: delinea-secret-server 11.8.x.pdf 664-665 iš 2009 psl.
5.3.15.	Palaikomi paskyrų tipai	Sprendimas turi palaikyti šių tipų paskyras: • tinklo įrenginių paskyros; • saugumo įrenginių paskyros; • duomenų bazių paskyros; • Web svetainių paskyros; • debesų kompiuterijos administracinės paskyros; • Windows lokalios privilegijuotos paskyros; • Linux/Unix lokalios privilegijuotos paskyros; • AD privilegijuotos paskyros; • AD tarnybų paskyros (angl. service account);	Palaiko norimus paskyrų tipus: • tinklo įrenginių paskyros; ▪ Cisco Account (SSH) ▪ Cisco Account (Telnet) 5.3.15 ▪ Cisco Enable Secret (SSH) ▪ Cisco Enable Secret (Telnet) ▪ Cisco VPN Connection Dokumentas: delinea-secret-server 11.8.x.pdf 1146 iš 2009 psl. 5.3.15 ▪ SonicWall NSA Web Admin Account ▪ SonicWall NSA Web Local User Account Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • saugumo įrenginių paskyros; 5.3.15 ▪ Security Alarm Code Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • duomenų bazių paskyros; 5.3.15 ▪ SQL Server Account Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl.

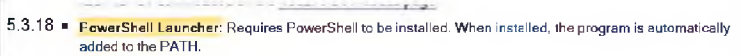
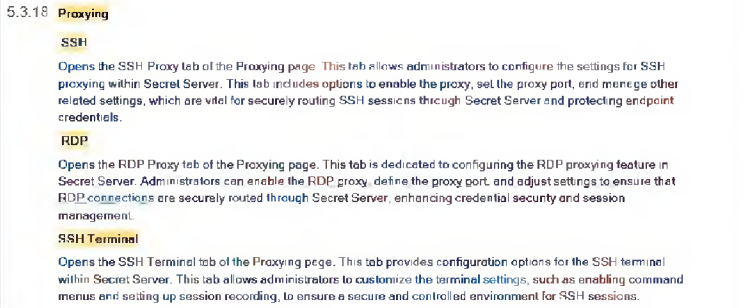
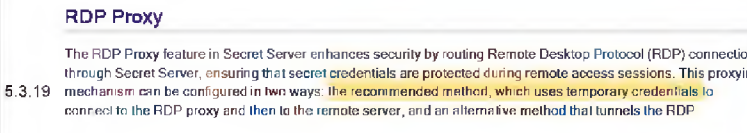
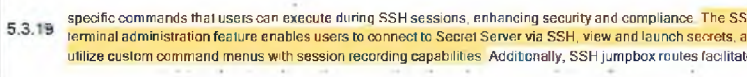
		• serverių OOB valdymo sąsajų paskyros (iLO, iDRAC ir kitos).	• Web svetainių paskyros; 5.3.15 ▪ Web Password Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • debesų kompiuterijos administracinės paskyros; 5.3.15 ▪ Azure AD Account Dokumentas: delinea-secret-server 11.8.x.pdf 1146 iš 2009 psl. • Windows lokalios privilegijuotos paskyros; 5.3.15 ▪ Windows Account Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • Linux/Unix lokalios privilegijuotos paskyros; 5.3.15 ▪ Unix Account (Privileged Account SSH Key Rotation - No Password) ▪ Unix Account (Privileged Account SSH Key Rotation) ▪ Unix Account (SSH Key Rotation - No Password) ▪ Unix Account (SSH Key Rotation) ▪ Unix Account (SSH) ▪ Unix Account (Telnet) ▪ Unix Root Account (SSH) Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • AD privilegijuotos paskyros; 5.3.15 ▪ Active Directory Account Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. • AD tarnybų paskyros (angl. service account); 5.3.15 ▪ Active Directory Account Dokumentas: delinea-secret-server 11.8.x.pdf 1147 iš 2009 psl. Priklausomybės (dependencies) keičia slaptažodžius tarnybose kur naudojamas AD service naudotojas. 5.3.15 Secret Dependencies for RPC *Secret dependencies* are items that rely on the username, password, or SSH private key stored in the secret. By adding them to the Dependencies tab, they are automatically updated when the secret's password is changed, ensuring they are up to date with the account on which they depend. Dokumentas: delinea-secret-server 11.8.x.pdf 914 iš 2009 psl. • serverių OOB valdymo sąsajų paskyros (iLO, iDRAC ir kitos). 5.3.15 ▪ HP iLO Account (SSH) 5.3.15 ▪ z/OS Mainframe 5.3.15 ▪ IBM iSeries Mainframe Dokumentas: delinea-secret-server 11.8.x.pdf 1146-1147 iš 2009 psl.
5.3.16.	Kelių faktorių autentifikavimas (angl. MFA)	Turi būti funkcionalumas, leidžiantis sprendimą integruoti su trečių šalių MFA sprendimais, kurie veikia naudodami nuo laiko	Yra funkcionalumas, leidžiantis sprendimą integruoti su trečių šalių MFA sprendimais, kurie veikia naudodami nuo laiko priklausomus vienkartinius slaptažodžius (angl. time based onetime password). Palaiko Cisco DUO tiesiogine integracija:

		priklausomus vienkartinius slaptažodžius (angl. time based onetime password).	5.3.16 Secret Server supports using Duo Security as a second factor of authentication. See below for setup instructions. Dokumentas: delinea-secret-server 11.8.x.pdf 424 iš 2009 psl.

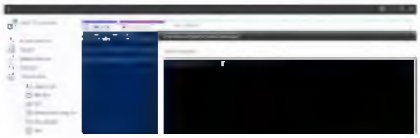
		Turi būti naudojama hibridinė dalis, turi būti konfigūruojami autentifikavimo reikalavimų profiliai, kurie numato leidžiamus autentifikavimo metodus IP adresai.
		Turi būti galimybė skirtingus profilius priskirti skirtingiems naudotojams.
			Bus naudojama hibridinė iš interneto dalis, kuri turi lanksčias, lengvai konfigūruojamas, prieigos teisių politikas apimančias filtravimą pagal IP, skirtingus MFA metodus ir skirtingų metodų taikymą pagal situaciją. Bus galimybė skirtingus profilius priskirti skirtingiems naudotojams.
			5.3.16 **About MFA**
			Platform MFA has two components: Creating Authentication Profiles and Creating Identity Policies.
			▪ An authentication *profile* determines which MFA challenges are presented to a user (see Creating Authentication Profiles).
			▪ An identity *policy* determines whether and when a user is presented with the challenges in their assigned MFA profile (see Creating Identity Polices).
			For more information about MFA on the Delinea Platform, see the following sections:
			▪ Creating Identity Policies. Enabling MFA on the platform requires setting up identity policies and assigning them to users. An identity policy determines whether and when a user is presented with the challenges specified in the associated MFA profile.
			▪ Creating Authentication Profiles. Enabling MFA on the platform requires setting up authentication profiles. An authentication profile specifies the authentication challenges required to log in to the platform, and the length of time that must elapse before a user is re-prompted for authentication.
			▪ Using MFA Providers. Configuring MFA providers provides an additional layer of security to ensure proper authentication for users accessing the Delinea Platform.
			▪ Using MFA for Secrets. Multi-factor authentication (MFA) for secrets gives platform administrators the option to add one or more security requirements to access defined secrets.
			▪ Configuring IWA. The Delinea Platform can accept an Integrated Windows Authentication (IWA) connection as sufficient authentication for users with Active Directory accounts to log in to the platform.
			▪ Using Corporate IP Range. The Corporate IP Range function is used to define IP ranges for both internal and external networks and to define authentication requirements, such as the locations or IP ranges from which users can log in to the Delinea Platform.
			▪ Login Flow for the Delinea Platform Portal (MFA). The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. Also see Delinea Mobile Log in Process.
			▪ MFA Providers: Configuring MFA providers adds an additional layer of security to ensure that users accessing the Delinea Platform are properly authenticated.
			  ▪ Duo Authentication
			  ▪ RADIUS Authentication
			Dokumentas: delinea-platform.pdf 422 iš 782 psl.

		Turi būti funkcionalumas, leidžiantis naudoti aparatines autentifikavimo žymes FIDO2.	Yra funkcionalumas, leidžiantis naudoti aparatines autentifikavimo žymes FIDO2: 5.3.16 **FIDO2 (YubiKey) Two-Factor Authentication Configuration** **Overview** FIDO2 FIDO2 (Fast Identity Online, second edition) is an open authentication standard that uses physical devices for authentication. Delinea uses this standard for two-factor authentication (2FA) with FIDO2 providing the second authentication after a normal password entry. Any FIDO2-enabled user attempting access to a Secret Server account must have a FIDO2 device in hand. The device eliminates many password-related issues, such as phishing and man-in-the-middle attacks. It also speeds up the login process over callback or texting 2FA. Dokumentas: delinea-secret-server 11.8.x.pdf 426 iš 2009 psl. 5.3.16 ▪ **FIDO2 authenticator**: FIDO2 is an authentication standard hosted by FIDO Alliance. FIDO2 includes the Web Authentication ("WebAuthn") API specification, written by the World Wide Web Consortium (W3C) and FIDO, with participation from third parties. The WebAuthn API is backward compatible with Universal 2nd Factor (U2F) keys. Delinea leverages the WebAuthn API to enable authentication to the platform without passwords, using either on-device authenticators or external authenticators. On-device authenticators are biometric authenticators integrated into the device hardware. Popular examples are Mac Touch ID, Windows Hello, and fingerprint scanners. External authenticators are security keys that you plug into the device's USB port, such as a YubiKey. Dokumentas: delinea-platform.pdf 425 iš 782 psl.
		Turi palaikyti šias autentifikavimo mobiliąsias programėles: • Google Authenticator; • Microsoft Autenticator.	Palaiko Google Authenticator ir Microsoft Authenticator mobiliąsias programėles. **TOTP** Secret Server supports using any type of soft token or mobile application authentication using the *Time-Based One-Time Password* (TOTP) RFC6238 algorithm. TOTPs are typically generated and authenticated by a mobile application using an algorithm that incorporates the current time to ensure that each one-time password (OTP) is 5.3.16 unique. TOTP applications include Authy, Google Authenticator, and Microsoft Authenticator. Dokumentas: delinea-secret-server 11.8.x.pdf 432 iš 2009 psl.

5.3.17.	Sesijos neaktyvumas	Sprendimas turi panaikinti naudotojo sesiją į web portalą po nustatyto neaktyvumo laiko.	Sprendimas gali panaikinti naudotojo sesiją į web portalą.: 5.3.17 ▪ **Force Inactivity Timeout**: This setting is the time limit on idle Secret Server sessions. Once a session expires, the user must login again with their username and password. Dokumentas: delinea-secret-server 11.8.x.pdf 1268 iš 2009 psl.
5.3.18.	Privilegijuoti prisijungimai	Naudotojui turi būti galimybė prisijungti prie sprendimo valdomų sistemų RDP ar SSH protokolais, neatskleidžiant tikrųjų sistemos kredencialų, bent dviem skirtingais būdais: • tiesiogiai iš naudotojo kompiuterio į sprendimo valdomą sistemą; • iš naudotojo kompiuterio per įgaliotąjį serverį (angl. proxy/jumphost) į sprendimo valdomą sistemą; • iš naudotojo kompiuterio per naršyklę į RDP ir SSH sesijas. Turi leisti pasirinkti prisijungimo būdą kiekvienai privilegijuotai paskyrai. Pats sprendimas turi galėti jungtis prie įrenginių ar sistemų šiais būdais: • SSH; • RDP; • Powershell.	Naudotojui bus galimybė prisijungti prie sprendimo valdomų sistemų RDP ar SSH protokolais neatskleidžiant tikrųjų sistemos kredencialų. Kredencialų apsaugai naudojamas RDP ir SSH proxy mechanizmas, bei SSH terminalas. 5.3.18 **Proxying** **SSH** Opens the SSH Proxy tab of the Proxying page. This tab allows administrators to configure the settings for SSH proxying within Secret Server. This tab includes options to enable the proxy, set the proxy port, and manage other related settings, which are vital for securely routing SSH sessions through Secret Server and protecting endpoint credentials. **RDP** Opens the RDP Proxy tab of the Proxying page. This tab is dedicated to configuring the RDP proxying feature in Secret Server. Administrators can enable the RDP proxy, define the proxy port, and adjust settings to ensure that RDP connections are securely routed through Secret Server, enhancing credential security and session management. **SSH Terminal** Opens the SSH Terminal tab of the Proxying page. This tab provides configuration options for the SSH terminal within Secret Server. This tab allows administrators to customize the terminal settings, such as enabling command menus and setting up session recording, to ensure a secure and controlled environment for SSH sessions. Dokumentas: delinea-secret-server 11.8.x.pdf 162 iš 2009 psl. • tiesiogiai iš naudotojo kompiuterio į sprendimo valdomą sistemą; 5.3.18 **Protocol Handler** — An application on an end-user's machine. It enables communication between Secret Server and that client machine. It also provides the files needed by launchers. Dokumentas: delinea-secret-server 11.8.x.pdf 48 iš 88 psl. • iš naudotojo kompiuterio per įgaliotąjį serverį (angl. proxy/jumphost) į sprendimo valdomą sistemą; 5.3.18 With Secret Server Session Connector (SSSC) installed on a Remote Desktop Services (RDS) server, anyone who can download and launch a standard Remote Desktop Protocol (RDP) shortcut file can have the same experience. The RDS server itself runs a special SSPH for RDS–SSPH (RDS) as a remote app to record the sessions, so end-users do not need to install any additional software. Dokumentas: delinea-secret-server 11.8.x.pdf 663 iš 2009 psl. 5.3.18 **SSH Jumpbox Routes** An *SSH jumpbox route*, is a series of regular Linux servers, accessible from the Internet, that is a gateway to other Linux machines on a private network using the SSH protocol. This topic and its subtopics address discuss using jumpbox routes Dokumentas: delinea-secret-server 11.8.x.pdf 843 iš 2009 psl. • iš naudotojo kompiuterio per naršyklę į RDP ir SSH sesijas. **Privileged Remote Access (formerly RAS)** ▪ Launch secure VPN-less browser-based SSH and RDP sessions with a single click. Dokumentas: delinea-platform.pdf 2 iš 782 psl. Leidžia pasirinkti prisijungimo būdą per paleidiklį jungiantis į sesiją: 5.3.18 ▪ Quick Launch: Secrets that display a rocket icon have secret launchers associated with them. Click the icon and a Select Launcher page appears. Click on the desired launcher from the list.

			Dokumentas: delinea-platform.pdf 151 iš 782 psl. Sprendimas gali jungtis prie sistemų per: Powershell:  5.3.18 ▪ PowerShell Launcher: Requires PowerShell to be installed. When installed, the program is automatically added to the PATH. Dokumentas: delinea-platform.pdf 652 iš 782 psl. RDP iš SSH:  5.3.18 Session Launcher The Launcher can be configured on the secret template to allow any tool to be launched using the secret such as Remote Desktop, PuTTY, Web launcher or a custom launcher you configure for a particular executable file, for Dokumentas: delinea-platform.pdf 38 iš 782 psl.
5.3.19.	SSH ir RDP prieiga	Turi leisti jungtis prie sprendimo valdomų sistemų per SSH įgaliotąjį serverį (angl. proxy/jumphost) naudojant atsitiktinai automatiškai sugeneruotus vienkartinius naudotojų vardus ir vienkartinius slaptažodžius, neatskleidžiant tikrųjų sistemos kredencialų.	Leidžia jungtis prie sprendimo valdomų sistemų per SSH įgaliotąjį serverį (angl. proxy/jumphost) naudojant atsitiktinai automatiškai sugeneruotus vienkartinius naudotojų vardus ir vienkartinius slaptažodžius, neatskleidžiant tikrųjų sistemos kredencialų. Kredencialų apsaugai naudojamas RDP ir SSH proxy mechanizmas, bei SSH terminalas.  5.3.18 Proxying SSH Opens the SSH Proxy tab of the Proxying page. This tab allows administrators to configure the settings for SSH proxying within Secret Server. This tab includes options to enable the proxy, set the proxy port, and manage other related settings, which are vital for securely routing SSH sessions through Secret Server and protecting endpoint credentials. RDP Opens the RDP Proxy tab of the Proxying page. This tab is dedicated to configuring the RDP proxying feature in Secret Server. Administrators can enable the RDP proxy, define the proxy port, and adjust settings to ensure that RDP connections are securely routed through Secret Server, enhancing credential security and session management. SSH Terminal Opens the SSH Terminal tab of the Proxying page. This tab provides configuration options for the SSH terminal within Secret Server. This tab allows administrators to customize the terminal settings, such as enabling command menus and setting up session recording, to ensure a secure and controlled environment for SSH sessions. Dokumentas: delinea-secret-server 11.8.x.pdf 162 iš 2009 psl.  RDP Proxy 5.3.19 The RDP Proxy feature in Secret Server enhances security by routing Remote Desktop Protocol (RDP) connections through Secret Server, ensuring that secret credentials are protected during remote access sessions. This proxying mechanism can be configured in two ways: the recommended method, which uses temporary credentials to connect to the RDP proxy and then to the remote server, and an alternative method that tunnels the RDP Dokumentas: delinea-secret-server 11.8.x.pdf 796 iš 2009 psl.  SSH Proxy Configuration 5.3.19 The Secret Server proxy routes SSH and RDP sessions and helps protect the endpoint credentials. There are two configuration options for proxying: Dokumentas: delinea-secret-server 11.8.x.pdf 811 iš 2009 psl.
		Turi leisti naudotis slaptažodžių spinta ir privilegijuotomis SSH sesijomis jungimuisi į sprendimo valdomas sistemas iš komandinės eilutės, nenaudojant interneto naršyklės ir neatskleidžiant tikrųjų sistemos kredencialų.	Leidžia naudotis slaptažodžių spinta ir privilegijuotomis SSH sesijomis jungimuisi į sprendimo valdomas sistemas iš komandinės eilutės, nenaudojant interneto naršyklės ir neatskleidžiant tikrųjų sistemos kredencialų. Naudoja SSH terminalą, kuris naudoja proxy mechanizmą.  5.3.19 specific commands that users can execute during SSH sessions, enhancing security and compliance. The SSH terminal administration feature enables users to connect to Secret Server via SSH, view and launch secrets, and utilize custom command menus with session recording capabilities. Additionally, SSH jumpbox routes facilitate Dokumentas: delinea-secret-server 11.8.x.pdf 811 iš 2009 psl. Proxy naudojimas SSH terminalo sesijai.

			• Cat command to display secret details of with specified secret ID 5.3.19 • Launch command to begin a Proxy launch session with specified secret ID ▪ Use up and down keystrokes for command history Dokumentas: delinea-secret-server 11.8.x.pdf 815 iš 2009 psl.
		Turi leisti jungtis prie sprendimo valdomų sistemų per RDP įgaliotąjį serverį (angl. proxy/jumphost), naudojant atsitiktinai automatiškai sugeneruotus vienkartinius domeno vardus, vienkartinius naudotojų vardus ir vienkartinius slaptažodžius, neatskleidžiant tikrųjų sistemos kredencialų.	Leidžia jungtis per RDP įgaliotąjį serverį (angl. proxy/jumphost), naudojant atsitiktinai automatiškai sugeneruotus vienkartinius domeno vardus, vienkartinius naudotojų vardus ir vienkartinius slaptažodžius, neatskleidžiant tikrųjų sistemos kredencialų. : 5.3.18 With Secret Server Session Connector (SSSC) installed on a Remote Desktop Services (RDS) server, anyone who 5.3.19 can download and launch a standard Remote Desktop Protocol (RDP) shortcut file can have the same experience. The RDS server itself runs a special SSPH for RDS–SSPH (RDS) as a remote app to record the sessions, so end-users do not need to install any additional software. Dokumentas: delinea-secret-server 11.8.x.pdf 663 iš 2009 psl. Kuria laikinus naudotojus: 5.3.19 ▪ Each RDS server needs to have a credential available to manage temporary users. This credential should be able to create and delete local users and add users to the Remote Desktop Users group. If you plan to use one Dokumentas: delinea-secret-server 11.8.x.pdf 667 iš 2009 psl.
		Turi leisti jungties prie sprendimo valdomų RDP ir SSH sistemų per interneto naršyklę (Google Chrome, MS Edge, FireFox, Safari) iš išorinio tinklo be VPN.	Leidžia jungtis prie sprendimo valdomų RDP ir SSH sistemų per naršyklėje (Google Chrome, MS Edge, FireFox, Safari) enkapsuliuotose RDP ir SSH sesijose, iš išorinio tinklo be VPN. **Privileged Remote Access (formerly RAS)** 5.3.18 ▪ Launch secure VPN-less browser-based SSH and RDP sessions with a single click. 5.3.19 ▪ Agentless deployment - no additional software is required on your target hosts Dokumentas: delinea-platform.pdf 2 iš 782 psl. Palaikomos visos naršyklės kurios dirba su HTML5 standartu, o tai yra visos šiuolaikinės naršyklės (įskaitant, google chrome, MS Edge, FireFox, Safari). 5.3.19 ▪ No end-user clients required: all based on a modern HTML5-based web client. Dokumentas: delinea-platform.pdf 2 iš 782 psl. 5.3.19 **Knowing the Supported Browsers** The Delinea Platform can accommodate most major browsers available today. We encourage users to use the latest version of a supported browser for the best experience and security on the Delinea Platform. We support the last two stable versions of the browsers listed below: ▪ Google Chrome ▪ Mozilla Firefox ▪ Apple Safari ▪ Microsoft Edge Dokumentas: delinea-platform.pdf 24 iš 782 psl.
		Turi leisti sudaryti leistinų SSH komandų sąrašus. Turi leisti sudaryti draudžiamų SSH komandų sąrašus.	Leidžia sudaryti leistinų SSH komandų sąrašus. 5.3.19 **SSH Command Restrictions** SSH command restrictions in Secret Server enhance security by allowing administrators to define and enforce specific commands that users can execute during SSH sessions. This feature, part of the privilege management Dokumentas: delinea-secret-server 11.8.x.pdf 832 iš 2009 psl.

			Leidžia sudaryti draudžiamų SSH komandų sąrašus. 5.3.19 With SSH blocked command lists, you can define disallowed commands when connecting as a privileged account. The blocked command list is defined by a series of regular expressions Dokumentas: delinea-secret-server 11.8.x.pdf 833 iš 2009 psl.
5.3.20.	Unifikuota naudotojo sąsaja	Turi leisti dirbti su keliomis skirtingomis privilegijuotomis RDP ir SSH sesijomis vienu metu iš bendros sąsajos, kurioje sesijų langai būtų organizuoti kortelių (angl. tabs) principu, analogišku interneto naršyklėms (angl. internet browser tabs). Darbas su sesija turi vykti tik pasirinkus atitinkamą kortelę (angl. tab). Turi leisti keisti privilegijuotos sesijos lango rezoliuciją.	Leidžia dirbti su keliomis skirtingomis privilegijuotomis RDP ir SSH sesijomis vienu metu iš bendros sąsajos, kurioje sesijų langai būtų organizuoti kortelių (angl. tabs) principu, analogišku interneto naršyklėms (angl. internet browser tabs). Sesijų langai organizuojami lentelių principu. 5.3.20 **Work Area** The work area consists mostly of tabs representing open connections. The first tab corresponds to one of the selected options in the navigation tree which includes Dokumentas: delinea-connection-manager.pdf 33 iš 192 psl. Leidžia keisti lango rezoliuciją: 5.3.20 **Screen Resolution for New Session Window Views** When you maximize an active RDP session window or you drag it as a standalone window to a second monitor, the session automatically disconnects and reconnects so it can use the highest supported screen resolution for the new window view. When you do the same with an active RDP *Proxy* session window, the session cannot automatically reconnect because RDP Proxy sessions launch with a one-time password (OTP) that cannot be regenerated. Therefore an RDP Proxy session cannot use the highest supported screen resolution for a new window view. Note 5.3.20 no RDP session of any kind can use the highest supported screen resolution for a new window view if the default setting for Desktop Size has been changed from Auto to a fixed size under RDP Global Settings Dokumentas: delinea-connection-manager.pdf 116-117 iš 192 psl. Darbas vyksta pasirinkus norimą lentelę, bei galima lentelės atkabinti bei perkelti kur reikia. 5.3.20 **Moving and Reorganizing Session Tabs and Windows** You can undock, move, and redock session tabs and windows in Connection Manager. To undock a session window, click the session tab and drag it out of the tab dock area. The tab becomes a standalone session window, which you can drag to another monitor or to another location on your desktop. To redock a session window, click and drag it toward the row of docked tabs in the main Connection Manager window. As you drag the window close to the tab dock, a blue line appears around the dock.  Dokumentas: delinea-connection-manager.pdf 117 iš 192 psl.
5.3.21.	Prieigos patvirtinimai	Turi palaikyti vieno asmens patvirtinimą. Turi technologiškai palaikyti daugiasluoksnį prieigos patvirtinimą, kuomet prieigai patvirtinti reikalingi keli skirtingi asmenys. Turi leisti ne mažiau kaip 3 asmenims patvirtinti prieigą. Jei nors vienas iš jų nepatvirtina, prieiga turi būti nesuteikiama.	Palaiko vieno asmens patvirtinimą: **Require Approval** The "requires approval for access" setting is typically employed in the following cases: 5.3.21 Simple approval workflows: ▪ When a user should be required to request access to a secret for a certain time period ▪ When an administrator would like to approve a user's access to a secret in advance for a time in the future (such as a maintenance period outside normal business hours) ▪ When a group of administrators would not like anyone to access a secret without the approval of another administrator Dokumentas: delinea-secret-server 11.8.x.pdf 35 iš 2009 psl. Leidžia kurti prieigos patvirtinimo mechanizmus keletui asmenų, iki 15 žingsnių. 5.3.21 ▪ Require multiple workflow steps, each with different reviewers and number of required approvers, if desired. 5.3.21 **Multi-Level Workflow** The original access requests are one level or step-required. Workflows allow up to 15 approval steps

			Dokumentas: delinea-secret-server 11.8.x.pdf 1077 iš 2009 psl. Technologiškai palaiko daugiasluoksnį prieigos patvirtinimą, kuomet prieigai patvirtinti reikalingi keli skirtingi asmenys. 5.3.21 Advanced approval workflows ▪ When requiring a multi-tier approval process that involves having more than one individual approve access to a secret ▪ When requiring multiple workflow steps, each with different reviewers and a varied number of required approvers Dokumentas: delinea-secret-server 11.8.x.pdf 35 iš 2009 psl. Nors vienam nepatvirtinus prieigos, prieiga nesuteikiama: 5.3.21 **Multi-Level Workflow** The original access requests are one level or step--anyone approving approves the request--no other input is required. Workflows allow up to 15 approval steps where approval by reviews in step 1 moves the request to step 2, approval at step 2 moves it to step 3 and so forth. Denial at any step denies the request. Dokumentas: delinea-secret-server 11.8.x.pdf 1077 iš 2009 psl.
		Turi būti galimybė prieigos užklausų patvirtinimus siųsti el. paštu.	Yra galimybė prieigos užklausų patvirtinimus siųsti el. paštu. : 5.3.21 ▪ An email is sent to everyone in the approval groups, notifying them of the request. Dokumentas: delinea-secret-server 11.8.x.pdf 1061 iš 2009 psl. Leidžia patvirtinti užklausą per laišką. ***Allow Approval for Access from Email*** Recommendation: Off 5.3.21 Allow Approval For Access from Email is a convenience option that allows users to approve or deny a secret access request by clicking a link in the request email sent by Secret Server. Allow Approval From Email does not require a Dokumentas: delinea-secret-server 11.8.x.pdf 1392 iš 2009 psl.
		Turi būti galimybė prieigos užklausas patvirtinti web portale.	Yra galimybė patvirtinti prieiga web portale: 5.3.21 **Inbox Drawer** **Secret Access Requests** Opens to Inbox > Secret Access Requests. The secret access requests feature in Secret Server allows a secret to require approval before access is granted. When a user requests access to a secret, an email is sent to the approval group(s), notifying them of the request. Members of the approval groups can approve or deny the request, and access can be granted for a set time period. This feature establishes a workflow model where users must request access, and approvals can be managed through the Secret Server interface or via email if configured. Dokumentas: delinea-secret-server 11.8.x.pdf 160 iš 2009 psl.
		Patvirtinant turi leisti nustatyti prieigos laiko ribotą trukmę.	Patvirtinant leidžia nustatyti prieigos laiko ribotą trukmę: 5.3.21 **Inbox Drawer** **Secret Access Requests** Opens to Inbox > Secret Access Requests. The secret access requests feature in Secret Server allows a secret to require approval before access is granted. When a user requests access to a secret, an email is sent to the approval group(s), notifying them of the request. Members of the approval groups can approve or deny the request, and access can be granted for a set time period. This feature establishes a workflow model where users must request access, and approvals can be managed through the Secret Server interface or via email if configured. Dokumentas: delinea-secret-server 11.8.x.pdf 160 iš 2009 psl.
		Turi būti galimybė vykdyti komandines sekas prieš ir po privilegijuotos sesijos rezervacijos.	Yra galimybė vykdyti komandines sekas prieš ir po privilegijuotos sesijos rezervacijos (check out) naudotjant Event pipelines. 5.3.21 *Event pipelines* (EPs) are a named group of triggers, filters, and tasks to manage events and responses to them. Event pipelines themselves can be grouped into EP policies. The Secret Server EP system is essentially a flexible instruction set builder and manager for controlling events and responses. Dokumentas: delinea-secret-server 11.8.x.pdf 275 iš 2009 psl.

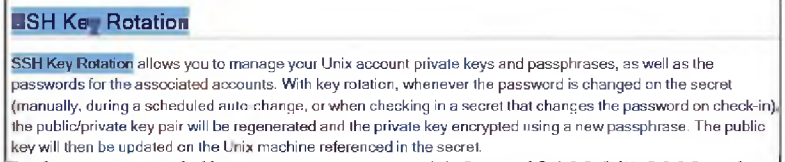
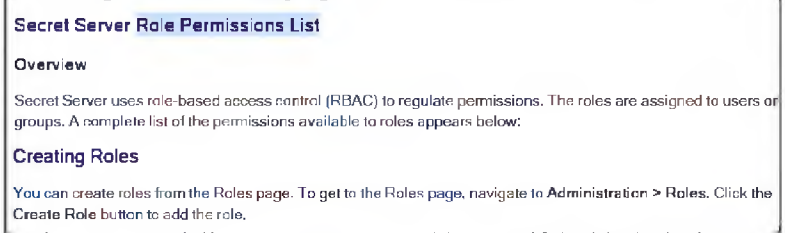
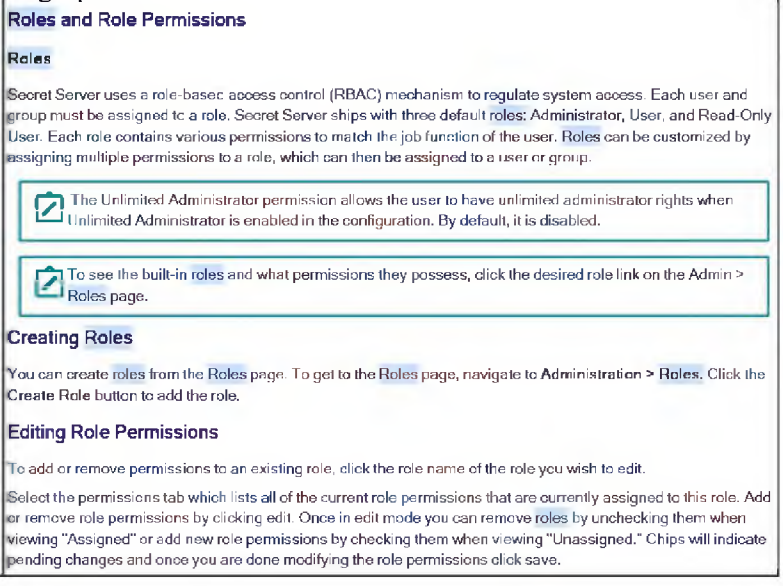
			Galimi event pipeline trigeriai: 5.3.21 ▪ Pre-Check Out 5.3.21 ▪ Pre-Check In Dokumentas: delinea-secret-server 11.8.x.pdf 283 iš 2009 psl. Event pipeline task leisti komandų seką (script): 5.3.21 ▪ Run Script Dokumentas: delinea-secret-server 11.8.x.pdf 279 iš 2009 psl.
5.3.22.	Naudotojų komandos	Turi leisti virtualiai skirstyti naudotojus ir grupes, apjungiant juos į komandas, kurios būtų izoliuotos viena nuo kitos (vienos komandos nariai nematytų kitos komandos narių ir objektų).	Leidžia virtualiai skirstyti naudotojus ir grupes, apjungiant juos į komandas, kurios yra izoliuotos viena nuo kitos (vienos komandos nariai nematytų kitos komandos narių ir objektų): 5.3.22 **User Teams** User teams in Secret Server are special groups created to restrict what users can see. A team bundles users and groups to assign them the same rules regarding visibility of other users and sites. This is particularly useful for managed service providers or large companies that need to isolate users by department or customer. Dokumentas: delinea-secret-server 11.8.x.pdf 1238 iš 2009 psl.
5.3.23.	Informacinių sistemų administravimo veiksmų (sesijų) vaizdo įrašymas	Turi būti galimybė daryti informacinių sistemų administravimo veiksmų (sesijų) vaizdo įrašymą neribotam kiekiui privilegijuotų paskyrų. Kokybiškai įrašyta valandos trukmės RDP sesija turi užimti ne daugiau nei 70 MB vietos. Privilegijuota RDP ir SSH sesija turi būti įrašoma net ir kuomet jungiamasi tiesiogiai į sprendimo valdomą sistemą (ne per įgaliotąjį serverį (angl. proxy/jumphost)).	Yra galimybė daryti informacinių sistemų administravimo veiksmų (sesijų) vaizdo įrašymą neribotam kiekiui privilegijuotų paskyrų. Sesijų įrašymas neribojamas. 5.3.2.3 Session Monitoring & Control / Vault / Essentials / Professional / Standard / Platinum / Enterprise Proxying RDP & SSH / N/A / x / x / x / x / x Session Recording / N/A / x / 50 secrets / x / x / x Dokumentas: Delinea Platform and Secret Server onprem feature comparizon 2024-2025.pdf 4 PDF psl. Kokybiškai įrašyta valandos trukmės RDP sesija neviršija 70MB. 5.3.23 Our documented standard for session recording storage sizing is around This equals around 6.7GB for around 100 hours of recorded sessions. If a 450 hours or per day per node, this means that you could expect a maxin Dokumentas: Secret Server - Sizing Guide 2021 Public Release.pdf 8 psl. Privilegijuota RDP ir SSH sesija įrašoma net ir kuomet jungiamasi tiesiogiai į sprendimo valdomą sistemą (ne per įgaliotąjį serverį (angl. proxy/jumphost). 5.3.23 Session recording allows you to record an RDP or PuTTY session, with optional metadata, and play it back in Secret Server. The Windows protocol handler encodes your session in WebM format in real time and sends the recording to Secret Server. There is an "Enable On-Demand Video Processing" option in Secret Server which leaves the recordings in Dokumentas: delinea-secret-server 11.8.x.pdf 1221 iš 2009 psl.
		Turi būti galimybė fiksuoti RDP ir SSH sesijų klavišų paspaudimus (angl. keyloging) neribotam kiekiui privilegijuotų paskyrų.	Yra galimybė fiksuoti RDP ir SSH sesijų klavišų paspaudimus (angl. keyloging) neribotam kiekiui privilegijuotų paskyrų. Nėra apribojimo.

			5.3.2.3 / 5.3.23 Session Monitoring & Control | Vault | Essentials | Professional | Standard | Platinum Proxying RDP & SSH | N/A | x | x | x | x Session Recording | N/A | x | 50 secrets | x | x Session Monitoring | N/A | x | Add on | x | x Keystroke Logging | N/A | x | 50 secrets | x | x Dokumentas: Delinea Platform and Secret Server onprem feature comparizon 2024-2025.pdf 4 PDF psl.
		Turi leisti atlikti paiešką vaizdo įraše pagal tekstą iš fiksuojamų klavišų paspaudimų.	Leidžia atlikti paiešką vaizdo įraše pagal tekstą iš fiksuojamų klavišų paspaudimų. 5.3.23 Basic session recording supports logging keystroke metadata for RDP and SSH sessions without requiring an agent across both Windows and Mac environments. Users can search for keystrokes, and the session playback interface displays this additional activity information. Dokumentas: delinea-secret-server 11.8.x.pdf 1213 iš 2009 psl.
		Turi saugoti vaizdo įrašus šifruotame formate, tam kad nebūtų galima jų peržiūrėti neturint reikalingų teisių sprendime.	Yra saugomi vaizdo įrašai šifruotame formate, tam kad nebūtų galima jų peržiūrėti neturint reikalingų teisių sprendime. . 5.3.23 Encrypt Archive on Disk This setting encrypts the session videos when stored on disk. Videos stored on disk are played back through the Secret Server UI but cannot be viewed directly from the file system. Dokumentas: delinea-secret-server 11.8.x.pdf 1227 iš 2009 psl.
5.3.24.	Privilegijuotos sesijos valdymas	Turi leisti matyti privilegijuotos RDP ir SSH sesijos vaizdą beveik realiu laiku.	Leidžia stebėti RDP ir SSH sesijas beveik realiu laiku. 5.3.24 Session monitoring allows administrators with the Session Monitoring permission to view all active launcher sessions within Secret Server. If session recording is enabled on the secret, an administrator can watch the user's session in real time. Dokumentas: delinea-secret-server 11.8.x.pdf 1214 iš 2009 psl.
		Turi leisti nutraukti privilegijuotą sesiją neįspėjus naudotojo rankiniu būdu.	Leidžia nutraukti sesiją neįspėjus naudotojo. ▪ Terminate: Sends a message to the business user or terminates their session. T Dokumentas: delinea-secret-server 11.8.x.pdf 1214 iš 2009 psl.
		Turi leisti nutraukti privilegijuotą sesiją įspėjus naudotoją rankiniu būdu.	Leidžia nutraukti privilegijuotą sesiją įspėjus naudotoją rankiniu būdu. 5.3.24 ▪ Terminate: Sends a message to the business user or terminates their session. The business user sees an alert dialog pop up on their machine with the message. Session Recording does not need to be enabled for this to Dokumentas: delinea-secret-server 11.8.x.pdf 1214 iš 2009 psl.
		Turi leisti nutraukti sesiją suteikiant ne daugiau 5 min. laiko vykdomo darbo pabaigimui.	Leidžia nutraukti sesiją suteikiant ne daugiau 5 min. laiko vykdomo darbo pabaigimui: 5.3.24 ▪ Improvement: Terminate, limit to 5 minutes, and message only have been added to live viewing in the new session monitoring Dokumentas: delinea-secret-server 11.8.x.pdf 1645 iš 2009 psl.
5.3.25.	Bendras privilegijuotas valdymas	Turi leisti valdyti bendro administravimo privilegijuotas paskyras tokias, kaip „root“, „administrator“ ir pan. Turi būti atsekamumas, kas jomis naudojosi. Turi leisti rezervuoti tokią paskyrą vienam naudotojui	Leidžia valdyti bendro administravimo privilegijuotas paskyras tokias, kaip „root“, „administrator“ ir pan.:

		vienu metu tam, kad kiti naudotojai negalėtų ja pasinaudoti.	5.3.25 Typical account passwords and sensitive data being stored in Secret Server ▪ Active Directory domain administrator accounts ▪ Active Directory service accounts ▪ Application passwords (such as SAP and, custom apps) ▪ Cloud Administrative or Privileged Accounts ▪ Database accounts (such as MS SQL, Oracle, or MySQL) ▪ Network equipment passwords (such as router, switches, firewalls, phones, and appliances) ▪ Sensitive files (such as private key files, SSL certificates, and network documentation info) ▪ Software license keys, serial numbers, personnel data, and Wi-Fi passwords ▪ UNIX, Linux, Mac root and local user accounts ▪ Website passwords (cloud services, DNS, Amazon AWS, vendors) ▪ Windows local administrator accounts Dokumentas: delinea-secret-server 11.8.x.pdf 22 iš 2009 psl. Yra atsekamumas kas jomis naudojosi: 5.3.25 **Secret Audit Log** The audit log for a secret can be accessed by clicking the **View Audit** button on the **Secret View** page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret. Dokumentas: delinea-secret-server 11.8.x.pdf 274 iš 2009 psl. Leidžia rezervuoti paskyrą vienam naudotojui vienu metu, kiti naudotojai negali naudotis šia paskyra: **Checkout Overview** **Introduction** 5.3.25 The Secret Server *checkout* feature forces accountability on secrets by granting exclusive access to a single user. If Dokumentas: delinea-secret-server 11.8.x.pdf 1064 iš 2009 psl.
5.3.26.	Nuotolinis slaptažodžių keitimas	Turi būti gamintojo paruošti nuotoliniai slaptažodžių keitikliai. Turi leisti kurti laisvai konfigūruojamus (angl. custom) nuotolinius slaptažodžių keitiklius.	Yra gamintojo paruošti nuotoliniai salptažodžių keitikliai: 5.3.26 We have a large number of out-of-the-box RPC changers, which are expandable by writing your own SSH, SQL or PowerShell scripts to do RPC, which can get information from the secret. See "Secret Dependencies for RPC" on page 914 and the "Password Changer List" on page 889. Dokumentas: delinea-secret-server 11.8.x.pdf 884 iš 2009 psl. Galima kurti laisvai konfigūruojamus (angl. custom) nuotolinius slaptažodžių keitiklius: 5.3.26 **Custom Password Changers** The Password Changers Configuration page can be accessed by navigating to **Admin > Remote Password Changing > Configure Password Changers**. There are a few password changing types that allow the user to enter in specific commands that are sent to the computer where the password is changing. This enables the system to accommodate for differences in the standard password change procedure. For example: The Unix system that is being changed prompts for the current password twice instead of only once before asking for the new password. Dokumentas: delinea-secret-server 11.8.x.pdf 884-885 iš 2009 psl.
		Turi leisti pasirinkti kokie simboliai traktuojami, kaip eilutės pabaiga SSH tipo nuotolinio slaptažodžio keitiklio konfigūracijoje.	Leidžia pasirinkti kokie simboliai bus traktuojami kaip eilutės pabaiga SSH tipo nuotolinio slaptažodžio keitiklio konfigūracijoje: 5.3.26 **Changing Ports and Line Endings** To change the port or line ending used on a password changer, click the password changer on the **Configure Password Changers** page and then click **Edit**. There, you can choose the line ending and port used by the device. By default, line endings are set to New Line (\n), however some devices and applications (such as HP iLO) use a different line ending system. The port defaults to 22 for SSH connections and 23 for Telnet connections. Dokumentas: delinea-secret-server 11.8.x.pdf 900 iš 2009 psl.
		Turi periodiškai automatiškai tikrinti ar sprendime saugomas slaptažodis teisingas ir juo gali būti	Periodiškai automatiškai tikrina ar sprendime saugomas slaptažodis teisingas ir juo gali būti prisijungta prie sprendimo valdomos sistemos:

		prisijungta prie sprendimo valdomos sistemos.	5.3.26 **Heartbeat Overview** *Heartbeat* which can be integrated with RPC, allows Secret Server to verify if the credentials stored in a secret can successfully authenticate with the target system. This ensures that the credentials are still valid and have not been changed outside of Secret Server Dokumentas: delinea-secret-server 11.8.x.pdf 1030 iš 2009 psl.
		Turi nuotoliniu būdu keisti lokalių paskyrų slaptažodžius Windows tipo operacinėms sistemoms.	Nuotoliniu būdu keičia lokalių paskyrų slaptažodžius Windows tipo operacinėms sistemoms: 5.3.26 ▪ Windows Account Dokumentas: delinea-secret-server 11.8.x.pdf 892 iš 2009 psl.
		Turi nuotoliniu būdu keisti Microsoft Active Directory paskyrų slaptažodžius. Turi nuotoliniu būdu keisti Active Directory tarnybų paskyrų (angl. service accounts) slaptažodžius.	Nuotolinu būdu keičia Microsoft Active Directory paskyrų slaptažodžius: 5.3.26 ▪ Active Directory LDS Dokumentas: delinea-secret-server 11.8.x.pdf 890 iš 2009 psl. Nuotoliniu būdų keičia Active Directory tarnybų paskyrų (angl. service accounts) slaptažodžius: 5.3.26 **RPC for Service Accounts** RPC can be performed on service accounts where the dependent services is automatically updated and restarted as the service account password is changed. Administrators are notified if a dependency fails to restart. The Dokumentas: delinea-secret-server 11.8.x.pdf 1012 iš 2009 psl.
		Turi nuotoliniu būdu keisti Windows suplanuotų užduočių (angl. scheduled tasks) slaptažodžius.	Nuotoliniu būdu keičia Windows suplanuotų užduočių (angl. scheduled tasks) slaptažodžius. 5.3.26 **RPC for Service Accounts** RPC can be performed on service accounts where the dependent services is automatically updated and restarted as the service account password is changed. Administrators are notified if a dependency fails to restart. The supported dependency types are IIS application pools, IIS application pool recycle, scheduled tasks, windows Dokumentas: delinea-secret-server 11.8.x.pdf 1012 iš 2009 psl.
		Turi mokėti perleisti iš naujo Windows tarnybas (angl. services) po tarnybos paskyros slaptažodžio pakeitimo. Turi mokėti perleisti iš naujo Windows suplanuotas užduotis (angl. scheduled tasks) po užduoties paskyros slaptažodžio pakeitimo.	Moka iš naujo paleisti Windows tarnybas (angl. services) po tarnybos slaptažodžio pakeitimo. Moka paleisto iš naujo Windows suplanuotas užduotis (angl. scheduled tasks) po užduoties paskyros slaptažodžio pakeitimo. 5.3.26 **RPC for Service Accounts** RPC can be performed on service accounts where the dependent services is automatically updated and restarted as the service account password is changed. Administrators are notified if a dependency fails to restart. The supported dependency types are IIS application pools, IIS application pool recycle, scheduled tasks, windows services, passwords embedded in .ini, .config, and other text files. Custom dependencies can be created using SSH, PowerShell, or SQL scripts. The application pool recycle only recycles the specified application pool, it does not update the password of the service account running the application pool. Secret Server attempts to unlock the service account should the account become locked during the dependency password change if there is a privileged account assigned to the secret. Dokumentas: delinea-secret-server 11.8.x.pdf 1012S iš 2009 psl.
		Turi nuotoliniu būdu keisti šiuos UNIX/Linux tipo slaptažodžius: • Unix standartinė paskyra; • Unix „root“ paskyra.	Nuotoliniu būdu keičia šiuos UNIX/Linux tipo slaptažodžius: • Unix standartinė paskyra; • Unix „root“ paskyra.

		Nuotolinis slaptažodžio keitimas turi būti galimas: • pagal pareikalavimą; • periodiškai; • pasibaigus nustatytam slaptažodžio galiojimo laikui.	Unix Account (SSH) Secret Template for RPC Overview This document briefly discusses using Secret Server Remote Password Changing (RPC) for Unix Account (SSH) accounts. With Remote Password Changing (RPC), secrets can automatically change remote account passwords when a secret expires, either immediately or on a defined schedule. In addition, the new passwords' strengths and other qualities are completely configurable. See the "Password Changer List" on page 889 for a complete list of available password changers. Unix Root Account (SSH) Secret Template for RPC Overview This document briefly discusses using Secret Server Remote Password Changing (RPC) for the Unix Root Account (SSH). With Remote Password Changing (RPC), secrets can automatically change remote account passwords when a secret expires, either immediately or on a defined schedule. In addition, the new passwords' strengths and other qualities are completely configurable. See the "Password Changer List" on page 889 for a complete list of available password changers. Dokumentas: delinea-secret-server 11.8.x.pdf 970, 972 iš 2009 psl Nuotolinis slaptažodžio keitimas bus galimas: • pagal pareikalavimą; • periodiškai; • pasibaigus nustatytam slaptažodžio galiojimo laikui. Verification To monitor heartbeat status, go to Settings > Heartbeat Log. To change the password immediately, select Change password now. Dokumentas: delinea-secret-server 11.8.x.pdf 1027 iš 2009 psl
5.3.27.	SSH privataus/viešo rakto poros rotavimas	Turi automatiškai rotuoti ir išsaugoti SSH privataus/viešo rakto porą privilegijuotos prieigos sprendime ir jo valdomose sistemose. Kiekvienai sistemai turi valdyti individualią ir unikalią privataus/viešo raktų porą. Raktų poros generavimas turi būti galimas: • pagal pareikalavimą; • periodiškai; • pasibaigus nustatytam raktų poros galiojimo laikui. Turi leisti rezervuoti raktų porą vienam naudotojui vienu metu tam, kad kiti naudotojai negalėtų ja pasinaudoti. Turi automatiškai rotuoti ir išsaugoti slaptažodį, saugantį SSH privataus/viešo rakto porą.	Gali automatiškai rotuoti ir išsaugoti SSH privataus/viešo rakto porą privilegijuotos prieigos sprendime ir jo valdomose sistemose. Kiekvienai sistemai bus valdoma individuali ir unikali privataus/viešo raktų pora. Configuring Remote Password Changing for SSH Key Rotation *Security Overview for SSH Key Rotation and PuTTY Launcher* SSH Key Rotation allows you to manage your Unix account private keys and passphrases as well as their passwords. The public/private key pair is regenerated and the private key is encrypted with a new passphrase any time a secret's password changes, either manually or automatically. The public key is then updated on the Unix machine referenced on the secret. Dokumentas: delinea-secret-server 11.8.x.pdf 1333 iš 2009 psl Raktų poros generavimas yra galimas: • pagal pareikalavimą; • periodiškai; • pasibaigus nustatytam raktų poros galiojimo laikui. ***Rotate SSH Key Remotely*** 1. Navigate back to the SSH Key Rotation Secret's **View** screen. 2. At the bottom of the screen, click the **Change Password Remotely** button. *Resetting an Expired Secret* To reset an expired Secret, you will need to change the field that has expired and is required to change. For example, if the field set to expire is the Password field and the current Password is "asdf", then a change to "jklh" will reset the expiration interval and thus remove the expiration text on the Secret View page. If you do not know which field is set to expire, you will need to go to the Secret template that the Secret was created from. Navigate to **Administration	Secret Template** and select the template. Click the Edit button and then on the next page, click the "Change" link. In the "Change Required On" textbox you will see the field that is set to expire. *AutoChanging an Expired Secret* Remote Password Changing (RPC) is enabled under the Administration, Remote Password Changing page. Click Edit to enable Remote Password Changing, Secret Heartbeat, and Secret Checkout. Once enabled, all Secret templates with RPC configured will be available to use RPC. Dokumentas: delinea-secret-server 11.8.x.pdf 1336, 1338 iš 2009 psl Leis rezervuoti raktų porą vienam naudotojui vienu metu tam, kad kiti naudotojai negalėtų ja pasinaudoti.

			The Secret Server checkout feature forces accountability on secrets by granting exclusive access to a single user. If a secret is configured for check out, a user can then access it. If Change Password on Check In is turned on, after check in, Secret Server automatically forces a password change on the remote machine. No other user can access a secret while it is checked out, except unlimited administrators. This guarantees that if the remote machine is accessed using the secret, the user who had it checked out was the only one with proper credentials at that time. Dokumentas: delinea-secret-server 11.8.x.pdf 53 iš 88 psl automatiškai rotuos ir išsaugos slaptažodį, saugantį SSH privataus/viešo rakto porą.  SSH Key Rotation SSH Key Rotation allows you to manage your Unix account private keys and passphrases, as well as the passwords for the associated accounts. With key rotation, whenever the password is changed on the secret (manually, during a scheduled auto change, or when checking in a secret that changes the password on check-in), the public/private key pair will be regenerated and the private key encrypted using a new passphrase. The public key will then be updated on the Unix machine referenced in the secret. Dokumentas: delinea-secret-server 11.8.x.pdf 1036 iš 2009 psl
5.3.28.	Teisės	Visas sprendime realizuotas funkcionalumas turi turėti individualias teises. Sprendimas turi leisti grupuoti teises į roles.	Visas sprendime realizuotas funkcionalumas turės individualias teises. Sprendimas leis grupuoti teises į roles.  Secret Server Role Permissions List Overview Secret Server uses role-based access control (RBAC) to regulate permissions. The roles are assigned to users or groups. A complete list of the permissions available to roles appears below: Creating Roles You can create roles from the Roles page. To get to the Roles page, navigate to Administration > Roles. Click the Create Role button to add the role. Dokumentas: delinea-secret-server 11.8.x.pdf 1244, 1243 iš 2009 psl
5.3.29.	Rolės	Turi būti gamintojo iš anksto paruoštos rolės. Turi leisti kurti laisvai modifikuojamas (angl. custom) roles ir leisti joms priskirti reikiamas teises. Turi leisti taikyti roles naudotojams ir grupėms.	Bus gamintojo iš anksto paruoštos rolės. Bus leidžiama kurti laisvai modifikuojamas (angl. custom) roles ir leisti joms priskirti reikiamas teises. Bus leidžiama taikyti roles naudotojams ir grupėms.  Roles and Role Permissions Roles Secret Server uses a role-based access control (RBAC) mechanism to regulate system access. Each user and group must be assigned to a role. Secret Server ships with three default roles: Administrator, User, and Read-Only User. Each role contains various permissions to match the job function of the user. Roles can be customized by assigning multiple permissions to a role, which can then be assigned to a user or group. The Unlimited Administrator permission allows the user to have unlimited administrator rights when Unlimited Administrator is enabled in the configuration. By default, it is disabled. To see the built-in roles and what permissions they possess, click the desired role link on the Admin > Roles page. Creating Roles You can create roles from the Roles page. To get to the Roles page, navigate to Administration > Roles. Click the Create Role button to add the role. Editing Role Permissions To add or remove permissions to an existing role, click the role name of the role you wish to edit. Select the permissions tab which lists all of the current role permissions that are currently assigned to this role. Add or remove role permissions by clicking edit. Once in edit mode you can remove roles by unchecking them when viewing "Assigned" or add new role permissions by checking them when viewing "Unassigned." Chips will indicate pending changes and once you are done modifying the role permissions click save.

			Dokumentas: delinea-secret-server 11.8.x.pdf 1259, 1243 iš 2009 psl
5.3.30.	Privilegijuotų paskyrų grupavimas	Privilegijuotos paskyros turi būti grupuojamos į katalogus, į kuriuos suteikiama prieiga kontroliuojant teises tiek į visą katalogą, tiek į konkrečią privilegijuotą paskyrą.	Privilegijuotos paskyros bus grupuojamos į katalogus, į kuriuos suteikiama prieiga kontroliuojant teises tiek į visą katalogą, tiek į konkrečią privilegijuotą paskyrą. **Secrets** Secrets in Secret Server are individually named sets of sensitive information, such as passwords, API keys, SSH keys, and other authentication credentials. These secrets are created using secret templates, which define the fields, launchers, and remote password changers for different types of secrets. Secret Server ensures that all secret data is securely encrypted before being stored in the database, and it maintains a detailed audit trail for access and history. Secrets can be centrally managed through sharing settings and folder structures, allowing for inheritance of permissions from parent folders. This robust management system helps organizations securely store, manage, and control access to privileged credentials, reducing the risk of data breaches and ensuring compliance with security policies. **Folders** Folders in Secret Server allow you to organize your secrets into logical groups and control access through permissions assigned to the folders. Secret folders allow you to create containers of secrets based on your needs. They help organize your customers, computers, regions, and branch offices, to name a few. Folders can be nested within other folders to create sub-categories for each set of classifications. You can assign secrets to these folders and sub-folders. Folders allow you to customize permissions at the folder level, and all secrets within can inherit the folder's permissions. Setting permissions at the folder level ensures future secrets placed in that folder have the same permissions, simplifying management across users and groups. Thoughtfully organizing your secrets into folders and setting granular permissions helps ensure the right people have access to the credentials they need while maintaining security. You can "favorite" a folder in the main menu by right clicking it. **Folder Permissions** If the new folder is a subfolder, it can use the sharing settings of its parent folder if you enable the **Inherit permissions from parent** setting for the folder. Folders can apply one of the following permissions to users or groups in the folder's **Permissions** table: You can access a folder's permissions table by accessing the folder, clicking on the three horizontal dots by its name and selecting **Edit Folder** from the dropdown options. ▪ **View**: Allows the user to see the folder and the secrets in that folder which inherit its permissions. Users need to have this permission for the parent folder to be able to see any subfolders available. Permissions granted to the root/parent folder will be inherited by subfolders. ▪ **Edit**: Allows the user to create new folders in the root/parent folder, which forces the **Inherit Permissions from Parent** setting on the new folder. This permission also allows for creating new and moving secrets into that folder, as well as renaming the folder. ▪ **Add Secret**: Allows the user to add a secret into a folder, but does NOT grant access to the added secret. Dokumentas: delinea-secret-server 11.8.x.pdf 1046 iš 2009 psl
5.3.31.	Pranešimai	Turi leisti kurti laisvai modifikuojamus pranešimus apie įvykius vykstančius sprendime, kurie siunčiami elektroniniu paštu. Turi leisti kurti pranešimus apie įvykius vykstančius sprendime, susijusius su realizuotu įvairiu funkcionalumu. Turi leisti siųsti pranešimus el. pašto adresams, kurie nėra susieti su sprendimo naudotojų paskyromis.	Leidžia kurti laisvai modifikuojamus pranešimus apie įvykius vykstančius sprendime, kurie siunčiami elektroniniu paštu. Leidžia kurti pranešimus apie įvykius vykstančius sprendime, susijusius su realizuotu įvairiu funkcionalumu. **Creating Event Subscriptions** Event subscriptions trigger notifications of defined events within the system. These notifications are sent to the inbox, which may send them externally via email or Slack, depending on your configuration. These notifications are an alert of specific events and not intended to be used for archived reporting. To add an event subscription: **Task 1: Creating an Event Subscription** 1. Navigate to **Admin > Event Subscriptions**. 2. Click the **Create Event Subscription** button. The Create Event Subscription page appears. 3. In the **Name** text box, enter a name for this new event subscription. 4. Click to select the **Send Email** check box if you want to send an email via an inbox notification. 5. Click to select the **Send Slack** check box if you want to send an Slack message via an inbox notification. Dokumentas: delinea-secret-server 11.8.x.pdf 300-333 iš 2009 psl. leidžia siųsti pranešimus el. pašto adresams, kurie nėra susieti su sprendimo naudotojų paskyromis.

			▪ Backup Configuration - Backup Failure ▪ Configuration - Edit ▪ Encryption - Key Management Disabled ▪ Role ▪ Role Permission ▪ Site - Engine Offline These alerts can be sent to different people or can even be sent to users that do not have a Secret Server account. Dokumentas: delinea-secret-server 11.8.x.pdf 39-40 iš 2009 psl
5.3.32.	Komandinės sekos (angl. scripts)	Turi palaikyti SSH komandines sekas. Turi palaikyti SQL komandines sekas. Turi palaikyti Powershell komandines sekas.	Palaiko SSH, SQL ir Powershell komandines sekas. **Creating and Using SSH Scripts** SSH scripts can be used in Secret Server to automate specific tasks. An SSH script can be configured as a dependency of a secret and run after the password is successfully changed on the secret. **Creating and Using SQL Scripts** You can use SQL scripts in Secret Server to automate specific tasks. You can configure a SQL script as a dependency of a secret and run after the password is successfully changed on the secret. **Creating and Using PowerShell Scripts** **Overview** You can use PowerShell scripts in Secret Server to automate specific tasks. These scripts are useful in several places in Secret Server, such as in creating custom remote password changers, custom dependency changers, discovery scanners, and custom ticket system integration. Dokumentas: delinea-secret-server 11.8.x.pdf 1474, 1471, 1462 iš 2009 psl.
5.3.33.	Sistemos ir naudotojų įrašai (angl. logs)	Prie skirtingo sprendimo funkcionalumo konfigūravimo turi būti atvaizduojami tik su tuo funkcionalumu susiję automatiškai atrinkti įrašai (angl. logs). Kada nors sprendime sukurti objektai (naudotojai, rolės, katalogai, paslaptys, paskyros, šablonai ir kiti) turi likti net ir po jų ištrynimo, audito, įrodymų ir veiksmų atsekamumo tikslais. Visas naudotojo aktyvumas sprendime turi būti fiksuojamas įvykių žurnale (angl. logs). Turi būti naudotojų veiksmų atsekamumas pagal įrašus.	Prie skirtingo sprendimo funkcionalumo konfigūravimo bus atvaizduojami tik su tuo funkcionalumu susiję automatiškai atrinkti įrašai (angl. logs). **Secret Audit Log** The audit log for a secret can be accessed by clicking the **View Audit** button on the **Secret View** page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret. 1. From the **Reports** page, click the **User Audit** tab. 2. From the dialog on the tab, select a user and a date range to view. 3. Click **Search History** to view the user's audit trail. Dokumentas: delinea-secret-server 11.8.x.pdf 274-275 iš 2009 psl Sprendime sukurti objektai (naudotojai, rolės, katalogai, paslaptys, paskyros, šablonai ir kiti) liks net ir po jų ištrynimo, audito, įrodymų ir veiksmų atsekamumo tikslais. **Deactivating and Reactivating Secrets** Secrets are not removed forever in Secret Server. Instead, they are *deactivated*. This maintains an audit trail for secrets, even ones that are no longer used. Administrators or users with specific permissions can view or even reactivate deactivated secrets. **Activating and Deactivating Templates** If a template is no longer relevant or outdated, it can be inactivated. This can be done from the specific template's Secret Template Edit page. Dokumentas: delinea-secret-server 11.8.x.pdf 1120, 1148, iš 2009 psl Visas naudotojo aktyvumas sprendime bus fiksuojamas įvykių žurnale (angl. logs). Bus naudotojų veiksmų atsekamumas pagal įrašus. **User Audit** Opens the Reports page to the User Audit tab. The user audit report feature in Secret Server displays every password or secret accessed by a user within a specified period. This report is essential for assessing and controlling vulnerability risk when someone leaves the organization and for complying with regulatory requirements. **Secret Audit Log** The audit log for a secret can be accessed by clicking the **View Audit** button on the **Secret View** page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret. Dokumentas: delinea-secret-server 11.8.x.pdf 159, 274 iš 2009 psl

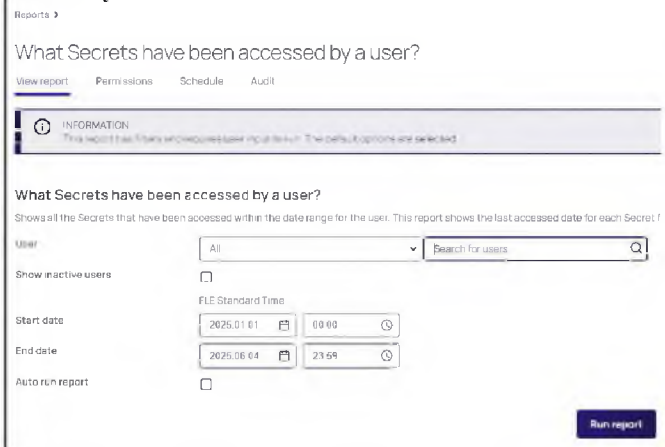
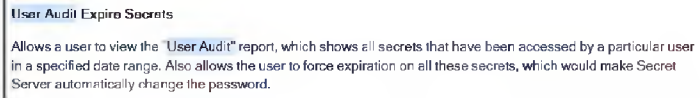
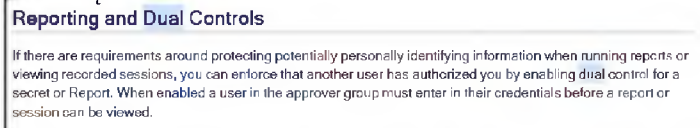
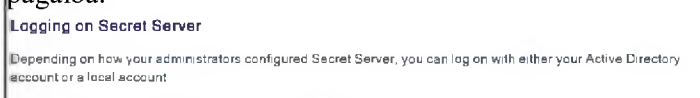
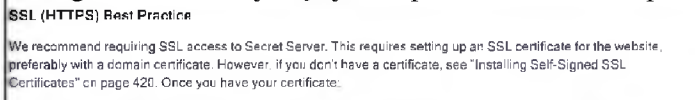
5.3.34.	Eksportavimas ir importavimas	Sprendimas turi leisti importuoti paskyras ir kredencialus masiniu būdu iš tekstinės bylos CSV ir XML formatu. Atstatymo ir migravimo tikslais turi leisti eksportuoti kredencialus ir paskyras XML ir CSV formatu. Eksportavimo teisė turi būti išskirta ir konfigūruojama pasirinktinai.	Sprendimas leis importuoti paskyras ir kredencialus masiniu būdu iš tekstinės bylos CSV ir XML formatu. Atstatymo ir migravimo tikslais leis eksportuoti kredencialus ir paskyras XML ir CSV formatu. Eksportavimo teisė gali būti išskirta ir konfigūruojama pasirinktinai. **Secret Import and Export Overview** **Introduction** Secrets are imported or exported as a comma-separated-value (CSV) file or as XML: ▪ The CSV file is easily read and edited in Excel or other spreadsheet application. The file is grouped by secret template and each cluster of secrets has a header row that contains the template text-entry field names followed by all exported secrets based on that template. ▪ The XML file is useful for migrating data from one Secret Server installation to another or even from a third-party application to Secret Server. **Permissions** The following permissions relate to automatic secret export: ▪ **Administer Automatic Export**: The user can do everything the other permissions allow *and* edit the automatic export configuration. ▪ **Download Automatic Export**: The user can view all of the automatic export tabs *and* download exports from cloud storage (cloud customers only). ▪ **Run Automatic Export**: The user can view all of the automatic export tabs *and* run the export manually by clicking the Run Export button. ▪ **View Automatic Export**: The user can view all of the automatic export tabs. Dokumentas: delinea-secret-server 11.8.x.pdf 1088-1091 iš 2009 psl
5.3.35.	Atsarginės kopijos	Avarinio atstatymo ar on premises diegimas sprendimas turi automatiškai daryti tiek web aplikacijos, tiek duomenų bazės atsargines kopijas nurodytu dažnumu į šias lokacijas: • lokalus diskas; • tinklo katalogas. Sprendimas turi būti suderinamas su kliento naudojama Veeam atsarginių kopijų sistema.	Avarinio atstatymo ar on premises diegiamas sprendimas automatiškai darys tiek web aplikacijos, tiek duomenų bazės atsargines kopijas nurodytu dažnumu į šias lokacijas: • lokalus diskas; • tinklo katalogas. **Backing up Secret Server to a Network Share** This topic only applies to Secret Server On-Premises. Secret Server can be configured to backup to a network share instead of a local folder on the server. For example, you may want to do this such as when the Secret Server database (SQL) is located on a different server than the web application server (IIS). Dokumentas: delinea-secret-server 11.8.x.pdf 442 iš 2009 psl Sprendimas bus suderinamas su kliento naudojama Veeam atsarginių kopijų sistema. Veeam darys backup virtualaus vmware serverio lygmeniu.
5.3.36.	Atnaujinimai	Sprendimas ir jo komponentai turi gebėti automatiškai pasitikrinti internete ar nėra naujos programinės įrangos versijos. Sprendimas ir jo komponentai turi leisti parsisiųsti ir įdiegti programinės įrangos naują versiją web grafinės sąsajos pagalba. Sprendimas ir jo komponentai turi leisti atnaujinti programinę įrangą rankiniu būdu (offline).	Sprendimas ir jo komponentai gebės automatiškai pasitikrinti internete ar nėra naujos programinės įrangos versijos. Sprendimas ir jo komponentai leis parsisiųsti ir įdiegti programinės įrangos naują versiją web grafinės sąsajos pagalba. Sprendimas ir jo komponentai leis atnaujinti programinę įrangą rankiniu būdu (offline). **How Standard Upgrades Work** Secret Server periodically polls the update server to detect new updates. If the "Allow Automatic Checks for Software Updates" option is enabled in the Admin > Configuration menu, you will see the "An update is available (xx.x.xxxxxx)" link after logging in with an administrator account. **How to Upgrade** 1. From a computer that has outbound network access, go to **Settings** > All Settings and click the **Upgrade Secret Server** link in the **Content** section. Admin > Upgrade. The Upgrade Secret Server page appears. 2. Ensure your install is backed up: All your data is encrypted using the `encryption.config` file in your Secret Server application folder. **Your data cannot be decrypted without it**. Thus, it is critical that you backup the application folder and its contents before proceeding. a. Click the **Backup** button. The Admin > Backup tab appears. Here you can configure and then run a backup of the SQL Server database and the web application. You can save backups to local folders or network folders through configuration. The AppPool running Secret Server must be configured to not shut down. The

			Upgrading Secret Server Without Outbound Access This topic only applies to Secret Server On-Premises. Dokumentas: delinea-secret-server 11.8.x.pdf 117-144 iš 2009 psl
5.3.37.	Integracijos	Sprendimas turi turėti SOAP arba REST API. API turi būti apsaugotas SSL/TLS. API turi palaikyti pagrindines programavimo kalbas .NET, JAVA arba lygiavertes. API turi leisti ieškoti slaptažodžių, išsaugoti slaptažodžius, leisti autentifikuotis.	Sprendimas turi SOAP ir REST API. **Web Services API** Secret Server's web services API includes both SOAP and RESTful interfaces, making it accessible to a wide range of programming languages and platforms. Developers can use these APIs to automate tasks such as creating, retrieving, and managing secrets, as well as configuring folders and permissions. This level of integration is crucial for maintaining a secure and efficient environment where privileged credentials are centrally managed and protected. Dokumentas: delinea-secret-server 11.8.x.pdf 1453 iš 2009 psl API bus apsaugotas SSL/TLS. **SSL and Secret Server** Secret Server employs SSL (Secure Sockets Layer) to ensure that all communication between the user's web browser and the Secret Server application is encrypted, providing a secure channel for data transmission. By using SSL, Secret Server protects sensitive information such as passwords, secrets, and user credentials from being intercepted by unauthorized parties during transit. SSL also helps in verifying the identity of the server, mitigating the risk of man-in-the-middle attacks. Administrators can enforce SSL by enabling the "Force HTTPS/SSL" option in the Secret Server configuration, ensuring that all access to the application is conducted over HTTPS. Additionally, Secret Server supports HTTP Strict Transport Security (HSTS) to further enhance security by instructing browsers to only interact with the server over secure connections. Dokumentas: delinea-secret-server 11.8.x.pdf 420 iš 2009 psl API palaiko pagrindines programavimo kalbas .NET, JAVA ir kitas **REST API Overview** The REST API for Secret Server provides a robust and flexible way to programmatically interact with the Secret Server platform, enabling seamless integration with other IT systems and automation of critical security processes. The API supports both SOAP and RESTful interfaces, making it accessible to a wide range of programming languages and platforms, including .NET, Java, Python, Ruby, and PowerShell. Dokumentas: delinea-secret-server 11.8.x.pdf 1481 iš 2009 psl API leidžia ieškoti slaptažodžių, išsaugoti slaptažodžius, leisti autentifikuotis. **Key Functions** ■ Authenticating to Secret Server ■ Creating and managing secrets ■ Configuring folders and permissions ■ Searching for secrets Dokumentas: delinea-secret-server 11.8.x.pdf 1482 iš 2009 psl
		Turi būti integruojamas su automatizuotomis DevOps aplinkoms skirtomis slaptažodžių spintomis.	Gali būti integruojamas su automatizuotomis DevOps aplinkoms skirtomis slaptažodžių spintomis. **Syncing with DevOps Secrets Vault** **Overview** Secret Server can push its secrets to DevOps Secrets Vault by creating a secret based on the "DevOps Secret Vault Client Credentials" template, which holds the client credentials for a DevOps Secrets Vault tenant. Using the REST API, you can then register a DevOps Secrets Vault tenant in Secret Server. That tenant references that secret to push secrets to DevOps Secrets Vault at a set sync interval. Dokumentas: delinea-secret-server 11.8.x.pdf 1550 iš 2009 psl
		Turi būti integruojamas su RPA (angl. robotic process automation) aplinkomis ir įrankiais.	Gali būti integruojamas su RPA (angl. robotic process automation) aplinkomis ir įrankiais. **Integrating UiPath Orchestrator with Secret Server** UiPath Orchestrator is a web application that enables you to deploy, schedule, monitor and manage Robots and processes through centralized work queues. For more information visit UiPath's website. Robotic Process Automation software uses "robot" agents on Windows endpoints to follow scripted actions and solve problems the way a person would by looking at the screen, reading pages, and copying text into fields. These robots need credentials to run, and in the course of their duties may also need to use passwords for other systems. The integration between Secret Server and UiPath ensures that: ■ Passwords are securely vaulted in Secret Server ■ UiPath bots can request passwords whenever they are needed ■ Role-based access controls limit which passwords each bot can use ■ All access by bots is captured in the Secret Server Audit Trail Dokumentas: delinea-integrations.pdf 634 iš 921 psl.

		Turi būti integruojamas su SSO (angl. single sign on) sistemomis.	Bus integruojamas su su SSO (angl. single sign on) sistemomis. **SAML** If your organization is already using SAML for SSO across your organization, it might be a good option for Secret Server authentication too. SAML uses browser-based communication, between the service provider (Secret Server) and the identity provider (SSO providers) to broker authentication. For more information on configuring SAML with Secret Server, please see the . The major benefits SAML provides are: ▪ A consistent MFA strategy across all applications in your environment. ▪ Simplified authentication communication: The browser handles the process. For SSC, if the authentication strategy is to authenticate against the domain, that communication must flow from Secret Server Cloud to the distribute engine and finally to the domain controller and back for authentication. SAML shortcuts this by having the browser communicate to the service provider and identity providers, reducing authentication latency. ▪ Easy to configure, manage, and add new users. ▪ Supports multiple MFA options based on conditional access. For example, a user may only need to verify with one factor for accessing less critical apps, but Secret Server uses two-factor authentication. Dokumentas: delinea-secret-server 11.8.x.pdf 29 iš 2009 psl
		Turi būti integruojamas su SAML ir OIDC sistemomis. Turi veikti SAML 2.0 Service Provider (SP) rolėje.	Bus integruojamas su SAML ir OIDC sistemomis. Veiks SAML 2.0 Service Provider (SP) rolėje **SAML** If your organization is already using SAML for SSO across your organization, it might be a good option for Secret Server authentication too. SAML uses browser-based communication, between the service provider (Secret Server) and the identity provider (SSO providers) to broker authentication. For more information on configuring SAML with Secret Server, please see the . The major benefits SAML provides are: ▪ A consistent MFA strategy across all applications in your environment. ▪ Simplified authentication communication: The browser handles the process. For SSC, if the authentication strategy is to authenticate against the domain, that communication must flow from Secret Server Cloud to the distribute engine and finally to the domain controller and back for authentication. SAML shortcuts this by having the browser communicate to the service provider and identity providers, reducing authentication latency. ▪ Easy to configure, manage, and add new users. ▪ Supports multiple MFA options based on conditional access. For example, a user may only need to verify with one factor for accessing less critical apps, but Secret Server uses two-factor authentication. Dokumentas: delinea-secret-server 11.8.x.pdf 29 iš 2009 psl **OpenID Connect** OpenID Connect (OIDC) in Secret Server is an identity protocol built on top of the OAuth 2.0 framework, designed to facilitate secure and streamlined authentication processes. By integrating with external OpenID Connect providers such as Azure AD, ADFS, Auth0, or Okta, Secret Server enables single sign-on (SSO) capabilities, allowing users to authenticate using their existing credentials from these providers. This integration not only enhances security by leveraging robust authentication mechanisms but also simplifies user management and access control. Administrators can configure Secret Server to delegate authentication to these external providers, ensuring a seamless and secure login experience for users across various applications and services. Dokumentas: delinea-secret-server 11.8.x.pdf 390 iš 2009 psl
		Turi integruotis su keliais Active Directory domenais. Integracijai su Active Directory neturi būti naudojama domeno administratoriaus ar kita aukštų privilegijų Active Directory paskyra.	Gali integruotis su keliais Active Directory domenais. Integracijai su Active Directory nebus naudojama domeno administratoriaus ar kita aukštų privilegijų Active Directory paskyra. **Step 2: Adding a Domain** 1. Select **Admin > Directory Services**. The Domains tab of the Directory Services page appears. 2. Click the **Add Domain** button and select **Active Directory Domain** from the dropdown. The Active Directory popup appears. 3. Type the Fully Qualified Domain Name and Friendly Name in their text boxes. Dokumentas: delinea-secret-server 11.8.x.pdf 439 iš 2009 psl **Active Directory Rights for Synchronization Account** Below is a listing of the Active Directory permissions required by the account used for synchronization. See "Configuring Active Directory" on page 493 for more on selecting this account. The locations discussed below are part of the Active Directory Administrative Center (ADAC). See Advanced AD DS Management Using Active Directory Administrative Center for information on using the ADAC. **Recommended Permissions** **Object Tab** This object and all descendant objects: ▪ List contents ▪ Read all properties Dokumentas: delinea-secret-server 11.8.x.pdf 484-485 iš 2009 psl
		Turi integruotis su HSM (angl. hardware security	Bus galimybė integruoti su HSM (angl. hardware security module) aparatiniais šifravimo raktų saugumo moduliais.

		module) aparatiniais šifravimo raktų saugumo moduliais.	Secret Server integrates with hardware security modules (HSMs). When Secret Server is configured to use an HSM, the Secret Server encryption key is protected by that HSM. Dokumentas: delinea-secret-server 11.8.x.pdf 1426 iš 2009 psl
		Turi integruotis su pažeidžiamumų valdymo sistemomis. Turi leisti pažeidžiamumų valdymo sistemoms tikrinti mašinas su individualiais tos mašinos kredencialais, saugomais privilegijuotos prieigos valdymo sistemoje.	Gali integruotis su pažeidžiamumų valdymo sistemomis. Gali leisti pažeidžiamumų valdymo sistemoms tikrinti mašinas su individualiais tos mašinos kredencialais, saugomais privilegijuotos prieigos valdymo sistemoje. **Integrating Tenable Security Center with Secret Server** Third-party vendors create and maintain this integration. Delinea does not guarantee that the integration will work properly or that it respects Delinea product limitations. Delinea has not reviewed this integration and Delinea Support staff can only assist with the Delinea side of setup. Integrating Tenable Security Center (Tenable.sc) with Delinea Secret Server enables secure management and automated retrieval of credentials for vulnerability scans. This integration ensures the protection of sensitive information while promoting efficient and compliant security operations. Dokumentas: delinea-integrations.pdf 864 iš 921 psl.
		Turi integruotis su sisteminių ir saugumo įvykių valdymo sistemomis (angl. SIEM), siunčiant Syslog pranešimus CEF formatu. Bent trys populiariausi SIEM gamintojai turi turėti paruoštas pranešimų apdorojimo (angl. parsing rules) taisykles (nurodyti SIEM gamintojus). Turi palaikyti integruotą Windows autentifikavimą (angl. IWA) arba lygiavertį.	Yra galimybė integruotis su sisteminių ir saugumo įvykių valdymo sistemomis (angl. SIEM), siunčiant Syslog pranešimus CEF formatu. **Configuring an External Audit Server** 1. Navigate to Admin > Application. The Application page appears. 2. Click the Edit button at the top right of the page. 3. Click to select the **Enable Syslog/CEF Log Output** check box. A syslog/CEF section expands below. Note: syslog/CEF may require an additional license key. To install licenses, navigate to **Admin > Licenses > Install New License**. Once installed, the license requires activation. Contact your Delinea Sales Representative with any questions. 4. Type IP address or name for the IIS server hosting the syslog/CEF server in the **Syslog/CEF Server** text box. You can add multiple entries, separating each with a semicolon. Dokumentas: delinea-secret-server 11.8.x.pdf 361 iš 2009 psl. Palaiko integruotą Windows autentifikavimą (angl. IWA) 8. If necessary, click to select the following check boxes: ▪ **Enable Directory Services** ▪ **Enable Integrated Windows Authentication.** Dokumentas: delinea-secret-server 11.8.x.pdf 374 iš 2009 psl. Palaiko integraciją su populiariais SIEM ir turi parsing taisykles: 1. IBM Qradar **Integrating QRadar DSM with Secret Server** Leveraging Secret Server event data with IBM's QRadar Security Intelligence Platform can give organizations deep insight into the use of privileged accounts (such as Windows local administrator, service or application accounts, UNIX root accounts, Cisco enabled passwords, and more). Used together, these tools provide a secure access for privileged accounts and a greater visibility to meet compliance mandates and detect internal network threats. **QID Mappings** The QID or QRadar Identifier is what QRadar uses to give events their name, high-level category, and lowlevel category.

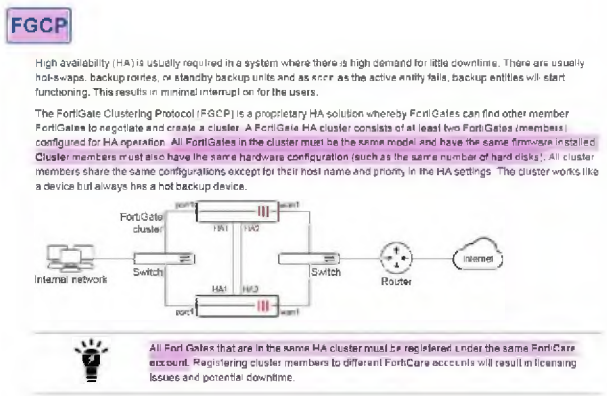
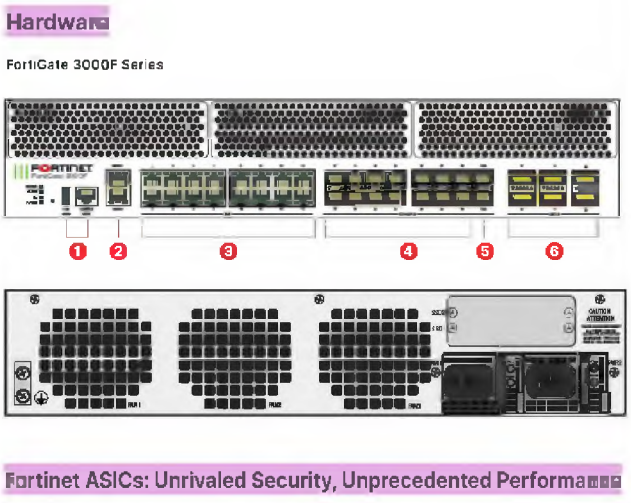
			Event List CONFIGURATION - EDIT | The main Delinea Secret Server configuration has been edited | 10 | 19001 FOLDER - CREATE | A Folder has been created | 2 | 19001 FOLDER - DELETE | A Folder has been deleted | 5 | 19001 FOLDER - EDIT PERMISSIONS | The configuration has been edited | 10 | 19001 FOLDER - SECRET POLICY CHANGE | The policy assigned to a folder has been changed | 6 | 19001 FOLDER - SECRET POLICY CHANGE | The Secret policy assigned to a folder has been changed | 8 | 19001 GROUP - OWNERS MODIFIED | The owners of a group have been modified | 5 | 19001 LICENSE - EXPIRES 30 DAYS | Secret Servers license will expire in 30 days | 1 | 19001 POWERSHELL SCRIPT - CREATE | A PowerShell script has been created | 5 | 19001 Dokumentas: delinea-integrations.pdf 144,151,152,153,154,155 iš 921 psl. 2. Splunk (Cisco) palaiko integracija ir turi parsing taisykles **Integrating Splunk Enterprise with Secret Server** Integrating Secret Server event data with Splunk SIEM solutions can give organizations deep insight into privileged account usage (such as Windows local administrator, service or application accounts, UNIX root accounts, Cisco enable passwords, and more). Together, these tools provide secure access to privileged accounts and greater visibility to meet compliance requirements and detect internal network threats. Splunk Enterprise software enables you to search, analyze, and visualize the data gathered by your Secret Server instance. By using the data in Splunk, you can perform real-time event analysis and gain visibility into the use of privileged account data in Secret Server. After the data source is defined, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search. Dokumentas: delinea-integrations.pdf 614 iš 921 psl. 3. Palo Alto XSIAM turi sukūrę savo integraciją su Delinea Secret server. Palo Alto Networks' integration between XSOAR and Secret Server supports the XSOAR and XSIAM automation platforms. Users can configure XSOAR automation within the platform, while the engineering team at Palo Alto Networks exclusively develops XSIAM data collection (SIEM) integrations using a different mechanism. In response to a customer request, the team created a custom XSIAM collector integration for Delinea, now part of a broader content pack, explaining the reference to XSIAM content within the pack. If you need assistance with the XSIAM collector integration, please reach out to Palo Alto Networks support, as they develop and maintain that content. Dokumentas: delinea-integrations.pdf 304 iš 921 psl.
5.3.38.	Sistemos saugumo stiprinimas	Turi būti realizuoti gamintojo automatizuoti testai, kurie parodo kiek esama konfigūracija atitinka gerąsias praktikas. Turi pateikti rekomendacijas, kaip sutvarkyti esamos konfigūracijos neatitikimus gerosioms praktikoms.	Yra realizuoti gamintojo automatizuoti testai, kurie parodo kiek esama konfigūracija atitinka gerąsias praktikas. Bus pateiktos rekomendacijos, kaip sutvarkyti esamos konfigūracijos neatitikimus gerosioms praktikoms. **Security Hardening** Opens the Reports page to the Security Hardening tab. The security hardening report checks aspects of Secret Server to ensure security best practices are being implemented. It identifies potential security issues within an installation and provides recommendations for hardening the security posture of the Secret Server environment. Dokumentas: delinea-secret-server 11.8.x.pdf 159 iš 2009 psl
5.3.39.	Ataskaitos	Turi būti gamintojo iš anksto paruoštos ataskaitos. Turi leisti kurti laisvai modifikuojamas (angl. custom) ataskaitas. Turi būti paruošta ataskaita apie laisvai pasirenkamą	Bus iš anksto paruoštos gamintojo ataskaitos. **Built-in Reports** Secret Server includes many pre-configured reports that you can run or use as templates for creating custom reports. Below are the reports shipped with current release of Secret Server: Dokumentas: delinea-secret-server 11.8.x.pdf 863 iš 2009 psl. Bus leidžiama kurti laisvai modifikuojamas (angl. custom) ataskaitas.

		konkretų privilegijuotą sprendimo naudotoją, kuri leistų nustatyti, kokiais slaptažodžiais naudotojas pasinaudojo per nurodytą laiko intervalą. Nustačius konkretaus naudotojo per nurodytą laiko intervalą naudotus slaptažodžius, turi juos pakeisti nuotoliniu būdu vienu paspaudimu (išėjusio iš darbo privilegijuoto naudotojo scenarijus). Siekiant apsaugoti asmens ir kitus jautrius duomenis, prieigai prie ataskaitų ir sesijų įrašų turi leisti nustatyti dviejų asmenų prieigos kontrolę.	 Dokumentas: delinea-secret-server 11.8.x.pdf 867 iš 2009 psl. Bus paruošta ataskaita apie laisvai pasirenkamą konkretų privilegijuotą sprendimo naudotoją, kuri leistų nustatyti, kokiais slaptažodžiais naudotojas pasinaudojo per nurodytą laiko intervalą.  Nustačius konkretaus naudotojo per nurodytą laiko intervalą naudotus slaptažodžius, galima juos pakeisti nuotoliniu būdu vienu paspaudimu (išėjusio iš darbo privilegijuoto naudotojo scenarijus).  Dokumentas: delinea-secret-server 11.8.x.pdf 1253 iš 2009 psl. Siekiant apsaugoti asmens ir kitus jautrius duomenis, prieigai prie ataskaitų ir sesijų įrašų bus leista nustatyti dviejų asmenų prieigos kontrolę.  Dokumentas: delinea-secret-server 11.8.x.pdf 874 iš 2009 psl.
5.3.40.	Sprendimo valdymo sąsajos reikalavimai	Turi būti web grafinė naudotojo sąsaja valdoma interneto naršyklės pagalba.	Web grafinė naudotojo sąsaja bus valdoma interneto naršyklės pagalba.  Dokumentas: delinea-secret-server 11.8.x.pdf 76 iš 88 psl.
		Web grafinė naudotojo sąsaja turi būti pasiekiama HTTPS protokolu.	Web grafinė naudotojo sąsaja bus pasiekiama HTTPS protokolu.  Dokumentas: delinea-secret-server 11.8.x.pdf 81 iš 88 psl.

		Turi būti laisvai modifikuojami (angl. custom) darbalaukiai.	Bus laisvai modifikuojami (angl. custom) darbalaukiai. Customized Tabs *Tab Management* The following operations are available for creating custom tabs: ▪ **Create:** Click the + icon to the right of the tabs to create a new empty tab. ▪ **Delete:** Click **Remove tab** page on a tab and select **Confirm remove tab** to delete a tab. You can cancel changes by clicking **Cancel**. A confirmation pop up page appears. ▪ **Rename:** Click **Rename** on a tab to change the tab name. You can cancel changes by clicking the Cancel button. ▪ **Sort:** Click **Sort**: on a tab, the Sort menu will appear. Drag the tab names up and down inside the Sort menu to change the sort order of the tabs. When done, click **Save tab order**. Dokumentas: delinea-secret-server 11.8.x.pdf 153 iš 2009 psl.
		Turi būti paskutinių naudotų kredencialų atvaizdavimas vienoje vietoje.	Bus atvaizdavimas paskutinių naudotų kredencialų vienoje vietoje. Overview Tab The Overview tab provides several fixed widgets for getting a quick understanding of your Secret Server installation: ▪ **Approvals:** Your current in-process approvals. See "Access Request Overview" on page 1061. ▪ **Engine Status:** A scrollable list of distributed engine connections and activation statuses. ▪ **Heartbeat Status:** A graphic of the current status of your heartbeats: success, pending, or failed. When you click on one of the statuses, you are brought to a report page for that status. For example, **Reports > Secrets Failing Heartbeat**. When you click the **Heartbeat Status by Day** link , you are brought to the **Reports > Heartbeat Status by Day** page. See "Heartbeat Overview" on page 1030. ▪ **Most Used Secrets:** A table of the most recently accessed secrets, listed by date and folder. ▪ **Password Rotation:** The state of your current password rotations. When you click the **RPC by Day for today** link you are brought to the **Reports > RPC by Day** report page. See "RPC Overview" on page 884. Dokumentas: delinea-secret-server 11.8.x.pdf 153 iš 2009 psl.
		Turi leisti reikalingus kredencialus pažymėti kaip mėgstamus ir juos atvaizduoti vienoje vietoje.	Bus leidžiama reikalingus kredencialus pažymėti kaip mėgstamus ir juos atvaizduoti vienoje vietoje. Dashboard Components Secret Panel Click the **Open Secret Panel** button in the top right to view the Secret panel. The panel contains: ▪ **Favorites:** A list of your favorite secrets, which you manually tagged by clicking the star icon on the All Secrets page. Dokumentas: delinea-secret-server 11.8.x.pdf 153 iš 2009 psl.
		Turi būti SSH nuotolinio administravimo terminalinė sąsaja.	Bus SSH nuotolinio administravimo terminalinė sąsaja. **SSH and Secret Server** Secret Server provides robust SSH management capabilities, including SSH proxy, command restrictions, terminal administration, and jumpbox routes. The SSH proxy feature routes SSH sessions through Secret Server, ensuring secure and monitored access to endpoints. Command restrictions allow administrators to define and enforce specific commands that users can execute during SSH sessions, enhancing security and compliance. The SSH terminal administration feature enables users to connect to Secret Server via SSH, view and launch secrets, and utilize custom command menus with session recording capabilities. Additionally, SSH jumpbox routes facilitate secure access to internal systems by routing connections through one or more intermediary servers, known as jumpboxes or bastion hosts, which are hardened and monitored to reduce security risks. Dokumentas: delinea-secret-server 11.8.x.pdf 811 iš 2009 psl.
		Turi leisti nustatyti IP adresų sąrašus, iš kurių leistini prisijungimai sprendimo administravimui.	Bus leista nustatyti IP adresų sąrašus, iš kurių leistini prisijungimai sprendimo administravimui. IP address restrictions Opens the Overview tab of the IP Address Management page. IP address restrictions in Secret Server allow administrators to control the locations and networks from which users can gain access. This feature enables limiting access to Secret Server to users who are "on network" and not accessing through VPN or other external networks. Dokumentas: delinea-secret-server 11.8.x.pdf 160 iš 2009 psl.

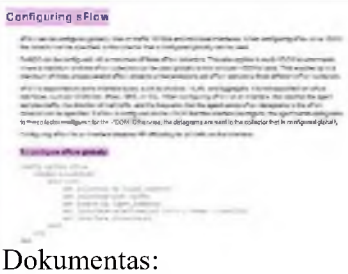
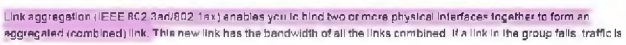
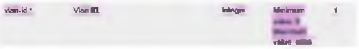
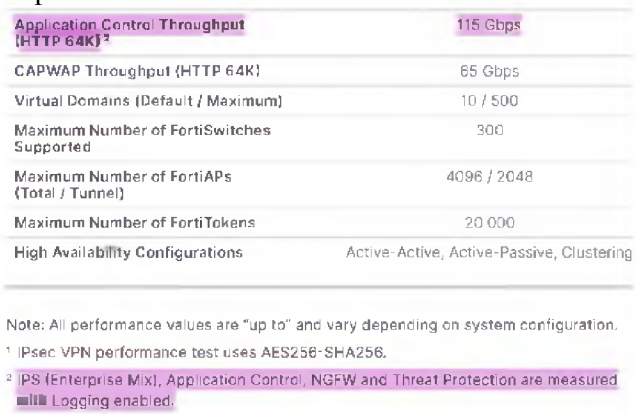
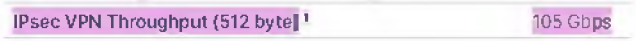
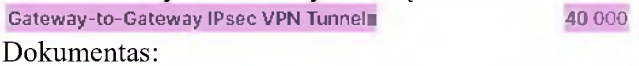
5.4. IPsec koncentratoriaus komponento reikalavimai

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
5.4.1.	Sprendimo architektūra ir sudedamosios dalys	IPsec koncentravimo ugniasienių sprendimas turi būti sudarytas iš dviejų vienodų narių. Kiekvienas narys, t. y. kiekviena ugniasienė turi dirbti kaip nepriklausomas narys ir turi	IPsec koncentravimo ugniasienių sprendimas yra sudarytas iš dviejų vienodų narių. Kiekvienas narys, t. y. kiekviena ugniasienė geba dirbti kaip nepriklausomas narys ir yra galima narius sujungti į aukšto patikimumo telkinį. Pateikiama aparatinė-programinė įranga leidžianti IPsec koncentravimo ugniasienių sprendimo narius

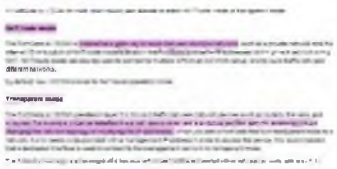
		būti galima narius sujungti į aukšto patikimumo telkinį. Turi būti pateikta visa aparatinė-programinė įranga ir licencijos leidžiančios IPsec koncentravimo ugniasienių sprendimo narius diegti kaip nepriklausomus narius ir kaip aušto patikimumo telkinio narius.	diegti kaip nepriklausomus narius ir kaip aušto patikimumo telkinio narius. Aukšto patikimumo funkcionalumas nelicencijuojamas ir yra įskaičiuotas į aparatinės-programinės įrangos komplektaciją. Dokumentas: RST250615SVL1-01 produktu kodai_KONFIDENCIALU.pdf  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3206 psl.
5.4.2.	Surinkimo reikalavimai	IPsec koncentravimo ugniasienių sprendimo nario įranga turi būti specializuotas aparatinis-programinis įrenginys arba modulinis įrenginys su vidiniais arba išoriniais moduliais komplektuojamas paties gamintojo. IPsec koncentravimo ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) turi būti suderinti tarpusavyje, pagaminti vieno gamintojo arba kelių gamintojų, tačiau turi būti pateiktas ugniasienės gamintojo patvirtinimas dėl komponentų tarpusavio suderinamumo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtais sprendimais.	IPsec koncentravimo ugniasienių sprendimo nario įranga yra specializuotas aparatinis-programinis įrenginys komplektuojamas paties gamintojo. IPsec koncentravimo ugniasienių sprendimo narį sudarantys aparatiniai komponentai (procesoriai, atmintis ir kt.) yra suderinti tarpusavyje, pagaminti vieno gamintojo. Siūloma įranga nėra realizuota naudojant virtualizacijos platformomis paremtus sprendimus.  Dokumentas: fortigate-3000f-series.pdf, 5, 7psl.
5.4.3.	Tinklo prievadai	Tinklo prievadų kiekis (ne mažiau kaip) ir tipas:	Tinklo prievadų kiekis ir tipas:

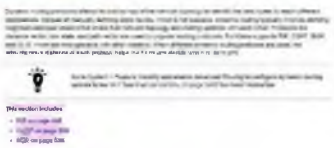
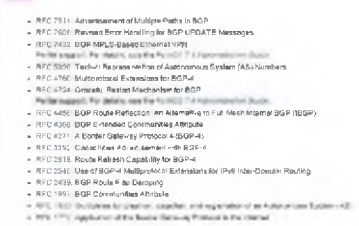
		• 12 vnt. 10 GE SFP+ prievadų; • 4 vnt. 40 GE QSFP+/ 100 GE QSFP28 prievadų.	• 14 vnt. 25GE SFP28/10 GE SFP+/1G SFP prievadų; 4. 14 × 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots Dokumentas: fortigate-3000f-series.pdf, 7psl. • 6 vnt. 40 GE QSFP+/ 100 GE QSFP28 prievadų. 6. 6 × 100 GE QSFP28 / 40 GE QSFP+ Slots Dokumentas: fortigate-3000f-series.pdf, 7psl.
5.4.4.	Optiniai moduliai/kabeliai	IPsec koncentravimo ugniasienių sprendimo nario įrenginys turi būti sukomplektuotas su ne mažiau kaip: • 8 vnt. 10G BASE-SR SFP+ 850 nm iki 300 m optiniais moduliais; • 4 vnt. 100G BASE-SR4 QSFP28 850 nm iki 100 m optiniais moduliais; Optiniai moduliai privalo būti to paties gamintojo kaip ir ugniasienių sprendimo įrangos gamintojas.	IPsec koncentravimo ugniasienių sprendimo nario įrenginys yra sukomplektuotas su: • 8 vnt. 10G BASE-SR SFP+ 850 nm iki 300 m optiniais moduliais; • 4 vnt. 100G BASE-SR4 QSFP28 850 nm iki 100 m optiniais moduliais; Optiniai moduliai yra to paties gamintojo kaip ir ugniasienių sprendimo įrangos gamintojas. Dokumentas: RST250615SVL1-01 produktu kodai_KONFIDENCIALU.pdf
5.4.5.	Valdymo prievadai	Prievadų kiekis ir tipas: • ne mažiau kaip vienas konsolės prievadas; • ne mažiau kaip vienas valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę. Šių prievadų skaičius turi būti papildomas, neturi būti įtrauktas į 5.4.3 punkte	Prievadų kiekis ir tipas: • vienas konsolės prievadas; 1. 1 x USB and 1 x Console Port Dokumentas: fortigate-3000f-series.pdf, 7psl. • vienas valdymo prievadas skirtas įrenginio valdymui per grafinę sąsają bei komandinę eilutę.

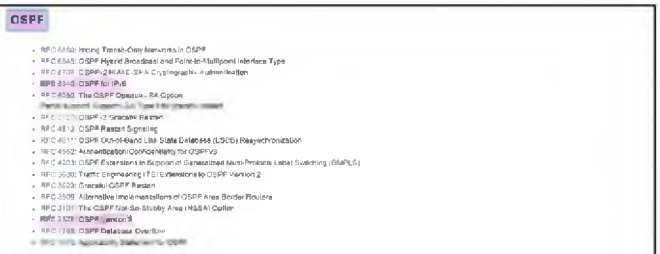
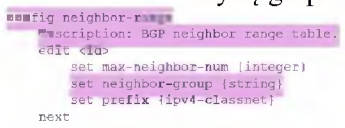
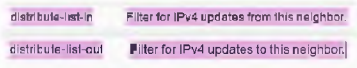
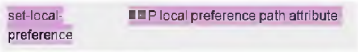
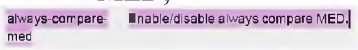
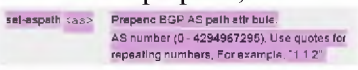
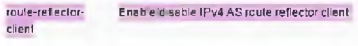
		numatytą tinklo prievadų skaičių.	2. 2 × 10 GE / GE RJ45 Management Ports Dokumentas: fortigate-3000f-series.pdf, 7psl. Šių prievadų skaičius yra papildomas, nėra įtrauktas į 5.4.3 punkte numatytą tinklo prievadų skaičių.
5.4.6.	Pajungimo į aukšto patikimumo telkinį prievadai	Ne mažiau kaip 2 vnt. Šių prievadų skaičius turi būti papildomas, neturi būti įtrauktas į 5.4.3 punkte numatytą tinklo prievadų skaičių.	2 vnt. 5. 2 × 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots Dokumentas: fortigate-3000f-series.pdf, 7psl. Šių prievadų skaičius yra papildomas, nėra įtrauktas į 5.4.3 punkte numatytą tinklo prievadų skaičių.
5.4.7.	Palaikomi standartai / protokolai	IPsec koncentravimo ugniasienių sprendimo narys turi palaikyti: • kiekvienas tinklo duomenų srauto fizinis prievadas privalo palaikyti VLAN pagal 802.1Q arba lygiavertį standartą; • LACP arba lygiavertį protokolą; • bent vieną iš protokolų: Netflow, sFlow, IPFIX arba kitą lygiavertį protokolą; • 802.3ad arba lygiavertį standartą. • Turi būti galima apjungti į vieną loginę tinklo sąsają ne mažiau kaip 4 fizines sąsajas.	IPsec koncentravimo ugniasienių sprendimas palaiko: • kiekvienas tinklo duomenų srauto fizinis prievadas palaiko VLAN pagal 802.1Q; In NAT mode, the FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switches or routers You can define VLAN subinterfaces on all FortiGate physical interfaces Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 208 psl. • LACP; physical interfaces to increase throughput and to provide redundancy. FortiOS supports a link aggregation (LAG) interface using the Link Aggregation Control Protocol (LACP) based on IEEE 802.3ad/802.1ax. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 176 psl. • NetFlow.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 674 psl. • sFlow.

			 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 706 psl. • 802.3ad;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 222 psl. • Yra galima apjungti į vieną loginę tinklo sąsają ne mažiau kaip 8 fizines sąsajas.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 222 psl.
5.4.8.	VLAN palaikymas	VLAN palaikymas. Ne mažiau kaip 4000 VLAN žymių (angl. Vlan TAG) per įrenginį ir arba prievadą.	Palaikoma 4095.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1519 psl.
5.4.9.	Ugniasienės greitaveika	IPsec koncentravimo ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą – ne mažiau kaip 100 Gbps.	IPsec koncentravimo ugniasienių sprendimo nario greitaveika atliekant duomenų srautų kontrolę su aplikacijų atpažinimu ir kontrole bei informacijos apie sujungimų sesijas rašymų į įvykių žurnalą - 115 Gbps.  Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.10.	IPsec VPN greitaveika	Ne mažiau kaip 80 Gbps.	IPsec VPN greitaveika 105 Gbps.  Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.11.	IPsec Gateway-to-Gateway	Ne mažiau kaip 4000.	IPsec Gateway-to-Gateway tunelių skaičius 40 000.  Dokumentas: fortigate-3000f-series.pdf, 8psl.

	tunelių skaičius		
5.4.12.	Maksimalus sesijų skaičius vienu metu	Ne mažiau kaip 30 milijonų.	Maksimalus sesijų skaičius vienu metu 70 milijonų. Concurrent Sessions (TCP) 70 Million Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.13.	Maksimalus naujų sesijų skaičius per sekundę	Ne mažiau kaip 800 tūkstančių.	Maksimalus naujų sesijų skaičius per sekundę 870 000. New Sessions/Second (TCP) 870 000 Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.14.	Suminis saugumo taisyklių skaičius per ugniasienę	Ne mažiau kaip 60000.	Suminis saugumo taisyklių skaičius per ugniasienę 200 000. Firewall Policies 200 000 Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.15.	Aukšto patikimumo savybės	IPsec koncentravimo ugniasienių sprendimo narys privalo palaikyti žemiau įvardintą funkcionalumą: • nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; • turi būti galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; • automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; • automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; • turi būti galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai	IPsec koncentravimo ugniasienių sprendimo narys palaiko žemiau įvardintą funkcionalumą: • nario pajungimas į aukšto patikimumo telkinį, kuris gali dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; HA active-passive cluster setup An HA Active-Passive (A-P) cluster can be set up using the GUI or CLI. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3220 psl. HA active-active cluster setup An HA Active-Active (A-A) cluster can be set up using the GUI or CLI. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3226 psl. • yra galima nurodyti, kad veikiantis ir aukštesnį prioritetą turintis narys visada būtų aktyvus telkinio narys; Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1452 psl. • automatinis konfigūracijos sinchronizavimas tarp aukšto patikimumo telkinio narių; Synchronizing the configuration Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3207 psl. • automatinis aktyvių sesijų sinchronizavimas tarp aukšto patikimumo telkinio narių; Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3308 psl.

		persijungti jei nurodyti IP adresai tampa neaktyviais.	• yra galima iš telkinio nario stebėti ar aktyvūs nurodyti IP adresai. Sistema gali automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1453 psl.
5.4.16.	Įrangos virtualizavimas	Turi būti funkcionalumas, leidžiantis IPsec koncentravimo ugniasienių sprendimo narį sudalinti į ne mažiau kaip 10 virtualius įrenginius.	Yra funkcionalumas, leidžiantis IPsec koncentravimo ugniasienių sprendimo narį sudalinti į 10 virtualių įrenginių. Virtual Domains (Default / Maximum) 10 / 500 Dokumentas: fortigate-3000f-series.pdf, 8psl.
5.4.17.	Ugniasienės darbo režimai	Ne mažiau kaip : • maršrutizavimo tarp skirtingų tinklų (OSI L3); • skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2).	Palaikomas maršrutizavimo tarp skirtingų tinklų (OSI L3), bei skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2); Operating modes  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3058 psl.
5.4.18.	Darbo režimai ir virtualizavimo funkcionalumas	IPsec koncentravimo ugniasienę dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema privalo veikti kiekvienu iš darbo režimų (maršrutizavimo, skaidrus), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai turi būti galima nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos.	IPsec koncentravimo ugniasienę dalinant į virtualias sistemas tos pačios fizinės sistemos apimtyje, kiekviena virtuali sistema geba veikti kiekvienu iš darbo režimų (maršrutizavimo, skaidrus), tai nustatant konfigūracijoje pasirinktinai. Kiekvienai virtualiai sistemai yra galima nustatyti darbo režimą nepriklausomai nuo to, kokiu režimu dirba kitos virtualios sistemos. In multi-VDOM mode, the FortiGate can have multiple VDOMs that function as independent units. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3164 psl. opmode Firewall operation mode (NAT or Transparent) option - nat Option Description nat Change to NAT mode. transparent Change to transparent mode. Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1833 psl.
5.4.19.	Maršrutizavimas	IPsec koncentravimo ugniasienė privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing).	Palaiko statinius bei dinaminius maršrutizavimo protokolus bei politika pagrįstą maršrutizavimą (angl. policy based routing). Adding or editing a static route Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 462 psl.

			Dynamic routing  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 488 psl. Configuring a policy route Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 475 psl.
5.4.20.	Maršrutizavimas	IPsec koncentravimo ugniasienė privalo palaikyti statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.	Palaiko statinių maršrutų tikrinimo mechanizmą, kuomet maršrutas panaikinamas iš maršrutizavimo lentelės, jeigu nepasiekiami vienas ar keli aprašyti IP adresai.  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1088 psl.
5.4.21.	PBR funkcionalumas	IPsec koncentravimo ugniasienė privalo palaikyti politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.	Palaiko politika pagrįstą maršrutizavimą (angl. Policy based routing) atsižvelgiant į šaltinio/paskirties zoną arba sąsają, siuntėjo, gavėjo IP adresą.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 476 psl.
5.4.22.	Dinaminio maršrutizavimo protokolai	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: • BGP; • OSFP v2 ir v3;	Palaiko žemiau įvardintus protokolus: BGP; BGP  Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 6 psl. OSFP v2 ir v3;

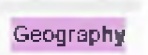
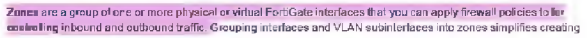
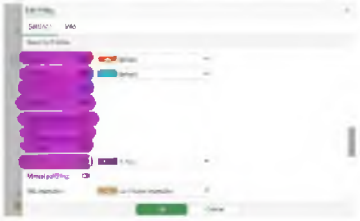
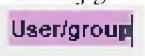
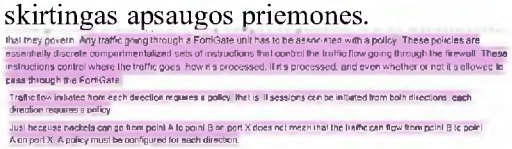
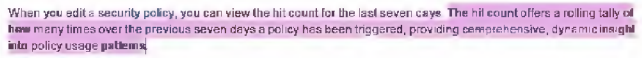
			 Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 12 psl.
5.4.23.	BGP funkcionalumas	IPsec koncentravimo ugniasienė privalo turėti BGP perkrovimo (graceful restart) funkcionalumą.	Turi BGP perkrovimo (angl. graceful restart) funkcionalumą. Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 971 psl.
5.4.24.	BGP konfigūracijos palaikymas	IPsec koncentravimo ugniasienė privalo palaikyti šiuos BGP protokolo gebėjimus: • BGP kaimynų grupavimą; • filtravimą gaunamiems ir išsiunčiamiems maršrutams; • Local Preference; • MED; • AS prepend; • Route-reflector funkcionalumą • BGP BFD;	IPsec koncentravimo ugniasienė palaiko šiuos BGP protokolo gebėjimus: • BGP kaimynų grupavimą;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 965 psl. • filtravimą gaunamiems ir išsiunčiamiems maršrutams;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 982 ir 983 psl. • Local Preference;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1084 psl. • MED;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 968 psl. • AS prepend;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1083 psl. • Route-reflector funkcionalumą;  Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 990 psl. • BGP BFD;

			Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 980 psl.
5.4.25.	OSPF funkcionalumas	IPsec koncentravimo ugniasienė privalo turėti grakštaus OSPF perkrovimo (graceful restart) funkcionalumą.	Turi grakštaus OSPF perkrovimo (angl. graceful restart) funkcionalumą. restart-mode OSPF restart mode (graceful or LLS) *graceful-restart* Graceful Restart Mode. Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1032-1033 psl.
5.4.26.	BFD palaikymas	IPsec koncentravimo ugniasienė privalo palaikyti BFD (bidirectional forwarding detection) protokolą.	Palaiko BFD (angl. bidirectional forwarding detection) protokolą. BFD can be enabled per device, VDOM, or interface. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 582 psl.
5.4.27.	Jumbo paketai	IPsec koncentravimo ugniasienė turi palaikyti Jumbo paketus.	Palaiko Jumbo paketus (MTU up to 9216 bytes). - ASIC accelerated FortiGate interfaces, such as NP6, NP7, and SOC4 (np6xlite), support MTU sizes up to 9216 bytes Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 191 psl. FortiGate 3000F FG-3000F Dokumentas: fortigate-3000f-series.pdf, 10 psl.
5.4.28.	Adresų transliavimo funkcionalumas	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: • NAT64; • Statinis adresų transliavimas; • Dinaminis adresų transliavimas keičiant prievadus (PAT).	Palaiko žemiau įvardintą funkcionalumą: • NAT64; NAT64 policy and DNS64 (DNS proxy) Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 747 psl. • Statinis adresų transliavimas; Static SNAT Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1576 psl. • Dinaminis adresų transliavimas keičiant prievadus (PAT). IP pool types Overload Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1578 psl.
5.4.29.	Integracija su SNMP (Simple Network Management Protocol) įrenginio būsenos stebėjimui	Privalo palaikyti SNMP protokolo 2 ir 3 versijas.	Palaiko SNMP v1/v2c ir v3 versijas. The FortiGate SNMP implementation is read-only. SNMP v1/v2c and v3 compliant SNMP managers have read-only access to FortiGate system information through queries, and can receive trap messages from the FortiGate unit. See Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3358 psl.
5.4.30.	Suderinamumas su Syslog	IPsec koncentravimo ugniasienių sprendimo narys turi būti suderinamas su Syslog standartu.	Yra suderinamas su Syslog standartu. • RFC 5424: The Syslog Protocol Dokumentas: FortiOS-7.6-Supported_RFCs.pdf, 16 psl.

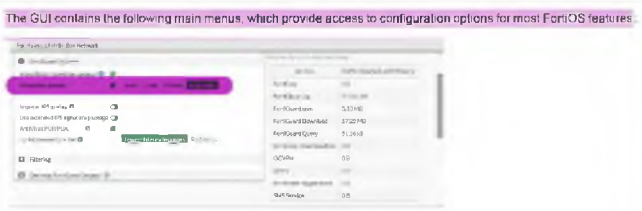
5.4.31.	Žurnalinių įvykių (event log) palaikymas	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintus žurnalinius įvykius: • sisteminiai; • administravimo; • VPN; • maršrutizavimo;	IPsec koncentravimo ugniasienė palaiko žemiau įvardintus žurnalinius įvykius: • sisteminiai; System Events Always available. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl. • administravimo; There are some situations where there will be some new charges or implementation on the firewall and auditing of these logs might be needed at some point. To audit these logs: Log & Report → System Events → select General System Events. Dokumentas: Administration_logs.pdf, 2 psl. • VPN; VPN Events Available when VPN is enabled in System > Feature Visibility. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl. • maršrutizavimo; Router Events Always available. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3791 psl.
5.4.32.	Žurnalinių įvykių kaupimas	IPsec koncentravimo ugniasienė privalo gebėti įvykių žurnalus siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą.	IPsec koncentravimo ugniasienė geba įvykių žurnalinius įrašus siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą sprendimą. Remote logging Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3988 psl.
5.4.33.	Diagnostikos priemonės	Privalomas srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	Palaikomas srauto / paketų nuo konkretaus interfeiso „įsirašymas“ (angl. packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 854 psl.
5.4.34.	Nutolusių naudotojų duomenų bazių palaikymas	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: • LDAP; • RADIUS; • TACACS+;	IPsec koncentravimo ugniasienė palaiko žemiau įvardintas duomenų bazes: • LDAP; Configuring an LDAP server Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2895 psl. • RADIUS; Configuring a RADIUS server

			Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2913 psl. • TACACS+; **TACACS+ servers** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2983 psl.
5.4.35.	SSL šifruotas srautas	IPsec koncentravimo ugniasienė turi dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. IPsec koncentravimo ugniasienė privalo palaikyti SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. Privalo būti galima nurodyti kuris duomenų srautas turi būti dešifruojamas.	Geba dešifruoti ir tikrinti įeinantį ir išeinantį SSL duomenų srautą. When you use deep inspection, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2255 psl. Palaiko SSL šifruoto srauto inspektavimą į narį įkeliant reikiamus sertifikatus. When the FortiGate re-encrypts the content, it uses a stored certificate, such as *Fortinet_CA_SSL*, *Fortinet_CA_Untrusted*, or your own CA certificate that you uploaded. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2255 psl. Yra galima nurodyti kuris duomenų srautas turi būti dešifruojamas. If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2256 psl.
5.4.36.	DoS apsauga	IPsec koncentravimo ugniasienė privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.	Leidžia riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui. tcp_syn_flood — If the SYN packet rate of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed. tcp_port_scan — If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed. tcp_src_session — If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed. tcp_dst_session — If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed. udp_flood — If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed. udp_scan — If the UDP sessions sent packets originating from one source IP address exceeds the configured threshold value, the action is executed. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1566 psl.
5.4.37.	Aplikacijų valdymas	IPsec koncentravimo ugniasienė privalo palaikyti: • aplikacijų identifikavimą ir kontrolę. Turi identifikuoti ne mažiau kaip 2000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa). Aplikacijų aprašai pateikiami nemokamai (arba	IPsec koncentravimo ugniasienė palaiko: • aplikacijų identifikavimą ir kontrolę. **Application control** Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2013 psl. Identifikuoja daugiau nei 2000 aplikacijų (Tos pačios programos skirtingos versijos skaičiuojamos kaip viena programa).

		įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip ugniasienės garantinio aptarnavimo laikotarpiui; • aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą.	 Nuoroda internete: https://www.fortiguard.com/appcontrol Aplikacijų aprašai įskaičiuoti į pasiūlymo kainą ugniasienės garantinio aptarnavimo laikotarpiui; FORTICARE SUPPORT SERVICES AND INCLUDED SERVICES  Dokumentas: og-fortiguard.pdf, 3 psl. • aplikacijų atpažinimo nuosavo aprašo susikūrimą ir įkėlimą į sistemą. Creating IPS and application control sign Dokumentas: Custom_IPS_and_Application_Control_Signature-7.6-Syntax_Guide.pdf, 6 psl.
5.4.38.	Sesijų laiko kontrolė	Turi būti galimybė nustatyti VPN sesijos laiką, po kurio neaktyvi sesija yra uždaroma.	Yra galima nustatyti VPN sesijos laiką, po kurio neaktyvi sesija yra uždaroma. idle-timeout Agentless VPN disconnects if idle for specified time in seconds Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 2154 psl.
5.4.39.	Duomenų srautų kontrolės taisyklės	Kuriant duomenų srautų kontrolės taisyklės privalo būti galima nurodyti siuntėjo IP adresą ar potinklį, gavėjo IP adresą ar potinklį, siuntėjo šalį, gavėjo šalį servisą/prievadą, programą, taikytinas apsaugos priemones, vartotoją, vartotojų grupę. Privalo būti galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.	Kuriant duomenų srautų kontrolės taisyklės yra galima nurodyti: siuntėjo IP adresą ar potinklį; Source address(es) Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1509 psl. gavėjo IP adresą ar potinklį; Destination address Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. siuntėjo šalį panaudojant Geography tipo objektą; Geography Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1687 psl.

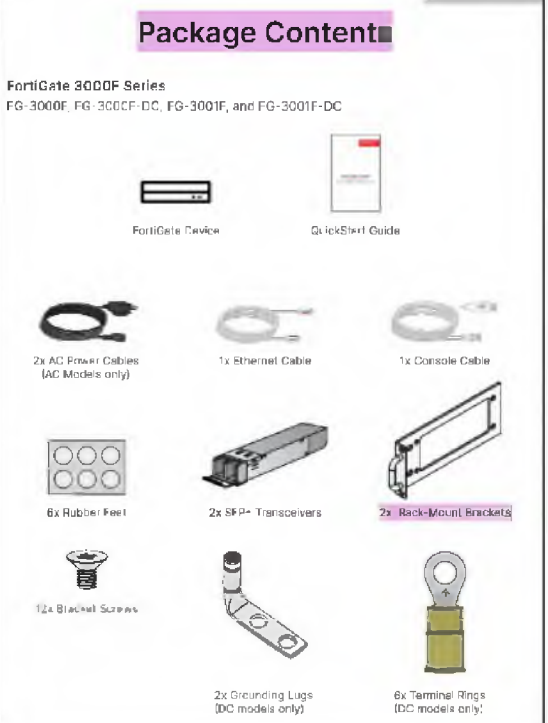
			gavėjo šalį panaudojant Geography tipo objektą;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1687 psl. servisą/prievadą;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. prievadų zoną;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 240 psl. aplikaciją, taikytinas apsaugos priemones;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1517 psl. vartotoją, vartotojų grupę.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1510 psl. Yra galima skirtingiems duomenų srautams naudoti skirtingas apsaugos priemones.  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1508-1509 psl.
5.4.40.	Duomenų srautų kontrolės taisyklių naudojimo stebėjimas	IPsec koncentravimo ugniasienė privalo rodyti taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).	Rodo taisyklių žymas: taisyklės panaudojimo skaičius (angl. hit count).  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1535 psl.
5.4.41.	VPN funkcionalumas	IPsec koncentravimo ugniasienė privalo turėti žemiau įvardintą VPN funkcionalumą: • IKev1 ir IKEv2 palaikymas;	IPsec koncentravimo ugniasienė turi žemiau įvardintą VPN funkcionalumą: • IKev1 ir IKEv2 palaikymas;  Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2316 psl.

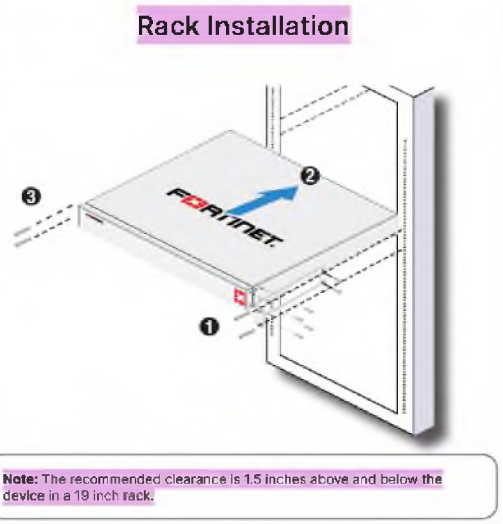
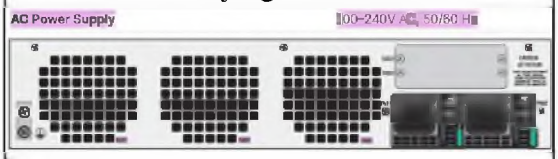
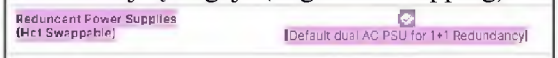
		• Autentifikacija sertifikatu; • Autentifiakcija prie-shared raktu; • Galimybė keisti IKE prievadą;	• Autentifikacija sertifikatu; Certificate Name The server certificate that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. See Digital certificates. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2316 psl. • Autentifiakcija prie-shared raktu; Pre-shared Key The pre-shared key that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. The same key must be defined at the remote peer or client. See Pre-shared key. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2316 psl. • Galimybė keisti IKE prievadą; ike-port UDP port for IKE/IPsec traffic (default 500). Dokumentas: FortiOS-7.6.3-CLI_Reference.pdf, 1829 psl.
5.4.42.	IPSec kriptografijos algoritmai	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptografijos algoritmus: • AES128; • AES256.	Palaiko žemiau įvardintus IPSec kriptografijos algoritmus: • AES128; • AES128: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl. • AES256. • AES256: a 128-bit block algorithm that uses a 256-bit key. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl.
5.4.43.	IPSec maišos algoritmai	IPsec koncentravimo ugniasienė privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec maišos algoritmus: • SHA-256; • SHA-512.	Palaiko žemiau įvardintus IPSec maišos algoritmus: 4. SHA-256; • SHA256: a 256-bit message digest. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl. 5. SHA-512. • SHA512: a 512-bit message digest. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 2317 psl.
5.4.44.	Srauto ribojimas	IPsec koncentravimo ugniasienė privalo leisti riboti srautą ir taikyti QoS per taisyklę (policy).	Leidžia riboti srautą ir taikyti QoS (angl. Quality of Service) per taisyklę. Traffic shaping policy Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 1738 psl.
5.4.45.	Aprašų, atnaujinimas	IPsec koncentravimo ugniasienė privalo galėti automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus.	Geba automatiškai, reguliariai, nustatytu laiku atsisiųsti ir aktyvuoti aplikacijų aprašus. To configure automatic updates in the GUI: 1. Go to System > FortiGuard. 2. In the FortiGuard Updates section, enable Scheduled Updates and select Automatic. Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 3422 psl.
5.4.46.	Sprendimo valdymo sąsajos reikalavimai	Turi turėti intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galėtų	Turi intuityvią, lengvai naudojamą grafinę valdymo sąsają, kurioje administratoriai galėtų kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.

		kurti, keisti, trinti ar kitaip valdyti sprendimo konfigūraciją.	 Dokumentas: FortiOS-7.6.3-Administration_Guide.pdf, 41 psl.

5.5. Bendri reikalavimai visiems komponentams

Nr.	Pavadinimas	Aprašymas	Atitikimas reikalavimams (Nurodomos siūlomos prekės charakteristikos (pildo Tiekėjas))
5.5.1.	Reikalavimai sprendime naudojamai programinei ir techninei įrangai	Turi būti pateikta 36 mėn. prenumeratos tipo (angl. subscription) arba nuolatinio galiojimo (angl. perpetual) įranga su ne mažiau kaip 36 mėn. gamintojo teikiamu įrangos palaikymu. Gamintojo garantijos teikimo terminas arba Gamintojo prenumeratos tipo (angl. subscription) licencijų teikimo terminas skaičiuojamas nuo Įrangos užregistravimo ir/ar užsakymo pas gamintoją dienos. Perkančiajai organizacijai turi būti suteikta prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos lietuvių arba anglų kalbomis. Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos programinės ir techninės įrangos gamybos arba tobulinimo nutraukimą (angl. „End of Lifetime“ arba „Discontinued“). Techninės Įrangos dokumentai turi būti lietuvių arba anglų kalba. Užrašai ant įrenginio ir jo dalių turi būti anglų arba lietuvių kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama anglų arba lietuvių kalba. Techninę ir programinę įrangą Tiekėjas privalo užregistruoti Perkančiosios organizacijos vardu gamintojų nustatyta	Bus pateikta 36 mėn. prenumeratos tipo (angl. subscription) įranga su 36 mėn. gamintojo teikiamu įrangos palaikymu, išskyrus MS SQL server ir MS Windows server nuolatinio galiojimo (angl. perpetual). Gamintojo garantijos teikimo terminas skaičiuojamas nuo Įrangos užregistravimo ar užsakymo pas gamintoją dienos. Perkančiajai organizacijai bus suteikta prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos anglų kalbomis. Tiekėjas užtikrina, kad visi gamintojai nėra paskelbę žinios apie siūlomos programinės ir techninės įrangos gamybos arba tobulinimo nutraukimą (angl. „End of Lifetime“ arba „Discontinued“). Gamintojo skelbiamame oficialiame nustotų gaminti gaminių sąraše siūlomos įrangos nėra. Pateikiamas gamintojo Fortinet išduotas oficialus dokumentas patvirtinantis, kad siūloma įranga nėra paskelbta apie gamybos arba tobulinimo nutraukimą (angl. „End of Lifetime“ arba „Discontinued“). Rašto pavadinimas: EOL raštas KVTC sign.pdf Žiūrėti pridedamą raštą RST250615SVL1-01 produktu kodai_KONFIDENCIALU Delinea, RH, MS https://learn.microsoft.com/en-us/lifecycle/products/sql-server-2022 https://access.redhat.com/support/policy/updates/red_hat_build_of_keycloak_notes https://access.redhat.com/support/policy/updates/errata

		tvarka garantinių paslaugų teikimui ir palaikymui, o registracijos duomenis perduoti Perkančiajai organizacijai.	https://support.delinea.com/s/product-lifecycle Techninės Įrangos dokumentai yra pateikiama anglų kalba. Užrašai ant įrenginio ir jo dalių yra anglų kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama anglų kalba. Techninę ir programinę įrangą Tiekėjas užregistruos Perkančiosios organizacijos vardu gamintojų nustatyta tvarka garantinių paslaugų teikimui ir palaikymui, o registracijos duomenis perduos Perkančiajai organizacijai.
5.5.2.	Reikalavimai sprendime naudojamai techninei įrangai	Įrangos gedimo atveju iš instaliacijos vietos remontui išvežamą pas tiekėją (jo atstovą) sugedusią įrangą pirkėjas pateikia be joje sumontuotų standžiųjų ar puslaidininkinių diskų (angl. HDD/SSD) ar kitų atminties laikmenų.	Įrangos gedimo atveju iš instaliacijos vietos remontui išvežamą pas tiekėją (jo atstovą) sugedusią įrangą pirkėjas pateikia be joje sumontuotų standžiųjų ar puslaidininkinių diskų (angl. HDD/SSD) ar kitų atminties laikmenų.
		Įranga turi būti montuojama į 19“ komutacinę spintą. Turi būti pateikiamas su visais montavimui reikalingais priedais (įskaitant bet neapsiribojant tvirtinimo elementais).	Visa sprendime naudojama techninė įranga yra montuojama į 19“ komutacinę spintą. Pateikiamas su visais montavimui reikalingais priedais (įskaitant bet neapsiribojant tvirtinimo elementais). 

			 Dokumentas: FG-3000-QSG.pdf, 5, 8 psl.
		Techninės įrangos maitinimo įtampa turi būti 230V 50Hz su jungtimi IEC14 arba IEC16 arba IEC20.	Techninės įrangos maitinimo įtampa yra 100-240V 50/60Hz su jungtimi IEC14.  Dokumentas: fortigate-3000f-series.pdf, 7, 8 psl.
		Visa techninė įranga turi ne mažiau kaip du maitinimo šaltinius. Vienam iš jų sugedus, įranga turi veikti toliau. Turi būti galimybė pakeisti maitinimo šaltinį veikiančioje įrangoje (angl. hot-swapping).	Visa techninė įranga turi du maitinimo šaltinius. Vienam iš jų sugedus, įranga veiks toliau. Yra galimybė pakeisti maitinimo šaltinį veikiančioje įrangoje (angl. hot-swapping).  Dokumentas: fortigate-3000f-series.pdf, 8 psl.
		Visi siūlomo sprendimo įrangos optiniai keitikliai turi būti to paties gamintojo kaip ir siūloma Įranga arba skirtingų gamintojų suderinami bendram darbui, ir būti visiškai su jais suderinami. Jei siūlomi skirtingų gamintojų optiniai keitikliai, turi būti pateiktas siūlomos įrangos gamintojo raštiškas patvirtinimas, kad siūlomi optiniai keitikliai yra visiškai suderinami bendram darbui, bei kad visą įrangos	Visi siūlomo sprendimo įrangos optiniai keitikliai yra to paties gamintojo kaip ir siūloma Įranga. Nurodyti gamintojo kodai atskirai pateikiamame dokumente „RST250615SVL1-01 produktu kodai_KONFIDENCIALU“.

		eksploatacijos laikotarpį atnaujinus programinę įrangą atpažins pasiūlytus optinius keitiklius, korektiškai rodys jų serijinius numerius, gamintoją ir kitus parametrus bei bus teikiama gamintojo garantija be apribojimų.	
5.5.3.	Reikalavimai sprendime naudojamiems virtualiems įrenginiams	Jei sprendimui bus naudojami virtualūs įrenginiai (angl. virtual appliance), tiekėjas turi pateikti kokie virtualūs resursai reikalingi. Suderinus projekto įgyvendinimo plane numatytą datą, Perkančioji organizacija pateiks reikalingų techninių parametrų virtualias mašinas. Tokiu atveju virtualūs įrenginiai privalo būti suderinami su VMware ESXi 7.0 arba naujesne. Esant poreikiui Perkančioji organizacija suteiks tiekėjui reikalingų parametrų virtualias mašinas testavimo aplinkai.	VPN ugniasienės komponentui reikalingi virtualūs resursai (visiems 8 VPN nariams kartu sudėjus reikia): 64 vCPU 512 GB RAM 800 GB DISK Testinės aplinkos VPN ugniasienės komponentui reikalingi virtualūs resursai: 1 vCPU 16 GB RAM 100 GB DISK Privilegijuotos prieigos valdymo komponento sprendimo aukšto patikimumo veikimui naudojamiems srauto balansavimo įrenginiams reikalingi virtualūs resursai (visiems 2 įrenginiams kartu sudėjus reikia): 8 vCPU 64 GB RAM 200 GB DISK Testavimo aplinkos Privilegijuotos prieigos valdymo komponento sprendimo aukšto patikimumo veikimui naudojamiems srauto balansavimo įrenginiams reikalingi virtualūs resursai: 1 vCPU 16 GB RAM 100 GB DISK Virtualūs įrenginiai yra suderinami su VMware ESXi 7.0.  Dokumentas: fortigate-vm.pdf, 7 psl. **System requirements** VM environment | Tested Versions VMware | ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 7.0, 8.0 Dokumentas: fortiadc-7.6.1-vm-installation-vmware-vmsphere.pdf, 7 psl.

5.5.4.	Reikalavimai sprendime naudojamai programinei įrangai	Sprendimo PĮ turi būti diegiama virtualiose tarnybinėse stotyse ir turi būti suderinama su VMware ESXi 7.0 arba naujesne virtualizavimo platforma. Perkančioji organizacija pateiks reikalingų techninių parametrų virtualias mašinas. Tiekėjas turi nurodyti kokių virtualių serverių išteklių (VM skaičius, CPU skaičius, RAM dydis, Disko talpa) reikės sprendimo diegimui perkančiosios organizacijos virtualizavimo infrastruktūroje. Jeigu siūlomo sprendimo veikimui naudojama Microsoft SQL duomenų bazė ar Microsoft Remote Desktop Services tarnyba, Tiekėjas pateiks reikalingas Microsoft SQL Standard, Microsoft Windows Server ir Microsoft RDS CAL licencijas. Jeigu siūlomo sprendimo veikimui naudojama kita programinė įranga (pvz. kitokia DBVS ar operacinė sistema), Tiekėjas turi įtraukti reikiamų licencijų įsigijimą kartu su visu sprendimu.	Sprendimo PĮ bus diegiama virtualiose tarnybinėse stotyse ir yra suderinama su VMware ESXi 7.0 arba naujesne virtualizavimo platforma. **Red Hat Enterprise Linux 9** **x86(64-bit)-Bit Guest OS Support** **Release** — **Supported Releases** Red Hat Enterprise Linux 9.x — ESXi 8.0 [1,2,3,4], 8.0 U3 [1,2,3,4], 8.0 U2 [1,2,4], 8.0 U1 [1,2,4], 8.0 [1,2,4], 7.0 U3 [1,2,5,4], 7.0 U2 [1,2,4], 7.0 U1 [1,2,4,6], 7.0 [1,2,4]; VMware Cloud on AWS7.0 [1] Windows Server 2025 Standard Edition — WS17.6; Fusion13.6; ESXi8.0 [1,2,3,4,5,6,7], 8.0 U3 [1,3,4,5,6,7], 8.0 U2 [3,4,5,6,7], 8.0 U1 [3,4,5,6,7], 8.0 [3,4,5,6,7], 7.0 U3 [3,4,5,6,7]; VMware Cloud on AWS7.0 U3 [1,3,4,5,6,7] Windows Server 2025 Datacenter Edition — WS17.6; Fusion13.6; ESXi8.0 [1,2,3,4,5,6,7], 8.0 U3 [1,3,4,5,6,7], 8.0 U2 [3,4,5,6,7], 8.0 U1 [3,4,5,6,7], 8.0 [3,4,5,6,7], 7.0 U3 [3,4,5,6,7]; VMware Cloud on AWS7.0 U3 [1,3,4,5,6,7] Dokumentas: VMware_GOS_Compatibility_Guide.pdf, 83, 67 psl. TVK komponentui reikalingi virtualūs resursai (visiems 7 TVK nariams kartu sudėjus reikia): 48 vCPU 304 GB RAM 3895 GB DISK PAM komponentui reikalingi virtualūs resursai (visiems 8 PAM nariams kartu sudėjus reikia): 40 vCPU 112 GB RAM 1100 GB DISK TVK komponentui Testavimo aplinkai reikalingi virtualūs resursai (visiems 3 TVK nariams kartu sudėjus reikia): 10 vCPU 36 GB RAM 915 GB DISK PAM Testavimo aplinkos diegimui reikalingi resursai (visiems 3 PAM nariams kartu sudėjus reikia) : 12 vCPU 24 GB RAM 360 GB DISK Kad užtikrinti sprendimo veikimą bus naudojamos Microsoft SQL duomenų bazė, Tiekėjas pateiks reikalingas Microsoft SQL Standard, Microsoft Windows Server, Windows Server CAL licencijos, Windows Server 2022 External Connector, Red Hat Enterprise Linux for Virtual Datacenters, Red Hat Runtimes ir tiekėjas pateiks visas reikalingas licencijas.

5.5.5.	Sprendime naudojamos integracijos	Būtina nurodyti kurie TVK reikalavimai bus įgyvendinti kuriant integracijas ir nenaudojant egzistuojančių produktų.	„5.1.3 Reikalavimai automatinio naudotojų paskyrų be slaptažodžių sinchronizavimo funkcionalumui“ bus įgyvendinti kuriant programuojamą integraciją.

6. Reikalavimai sprendimo paslaugoms

6.1. Organizaciniai projekto įgyvendinimo reikalavimai:

Nr.	Pavadinimas	Aprašymas
6.1.1.	Planavimo etapas	Projekto įgyvendinimo plano parengimas ir suderinimas su Perkančiąja organizacija (ne vėliau kaip per 30 kalendorinių dienų nuo Sutarties įsigaliojimo dienos). Projekto įgyvendinimo planą sudaro: • projekto įgyvendinimo planas/tvarkaraštis; • projekto koordinavimo planas; • dalijimosi informacija priemonių sąrašas; • projekto teikimo darbo grupės sudėtis; • projekto tarpinių ir galutinių rezultatų pateikimo ir pristatymo tvarka; • projekto teikimo rizikų planas; • kassavaitinių ir mėnesinių atliktų projekto veiklų priėmimo - perdavimo ataskaitų formos.
6.1.2.		1. Tiekėjas koordinuoja ir užtikrina suderinto darbų grafiko sekimą, teikia projekto veiklų priėmimo - perdavimo ataskaitas apie atliktus Perkančiosios organizacijos nuotolinės prisijungimo platformos diegimo darbus; 2. Nedelsiant telefonu ir el. paštu informuoja (atsakingus asmenis) apie kylančias rizikas dėl nesavalaikio veiklų įgyvendinimo; 3. Teikia siūlymus dėl rizikų mažinimo. 4. Tiekėjas teikia suderinimui projekto veiklų priėmimo - perdavimo ataskaitas apie atliktus Perkančiosios organizacijos objektų informacijos surinkimo darbus: • Kassavaitinė projekto veiklų priėmimo - perdavimo ataskaita už praėjusią savaitę parengiama ir pateikiama suderinimui el. paštu kiekvieną pirmadienį iki 11 val.; • Mėnesinė atliktų projekto veiklų priėmimo-perdavimo ataskaita už praėjusį mėnesį parengiama ir pateikiama suderinimui el. paštu iki einamojo mėn. 5 dienos.

a. Sprendimo projektavimas ir diegimas

Nr.	Pavadinimas	Aprašymas
6.2.1.	Bendrieji reikalavimai siūlomo sprendimo diegimui ir įrangos montavimui	Pagal Perkančiosios organizacijos poreikį įrangos tiekėjas turės suteikti ne mažiau kaip žemiau išvardintas paslaugas: • Sprendimui reikalingos įrangos montavimą – kai sprendimui pasiūlyta techninė įranga, ji turi būti sumontuota Perkančiosios organizacijos nurodytose patalpose; • Sprendimui reikalingos įrangos sujungimą – kai sprendimui pasiūlyta techninė įranga, ji turi būti prijungta prie elektros tinklo. Turi būti atliktas būtinas įrangos kabeliavimas, kabelių žymėjimas bei parengta techninė dokumentacija;

		• Sprendimui reikalingos įrangos mikrokodo (angl. firmware) atnaujinimą – kai sprendimui pasiūlyta techninė įranga, turi būti atliktas vidinės programinės įrangos mikrokodo (angl. firmware) atnaujinimas ir įrangos parengimas eksploatacijai. • Įrangos sujungimą – visa siūloma įranga turi būti sujungta su kitais pasiūlytais sprendimo komponentais. • Sprendimo testavimą – pabaigus diegimo darbus tiekėjas, kartu su Perkančiosios organizacijos atstovais, pagal iš anksto suderintus testavimo scenarijus, turės atlikti pateikto sprendimo testavimus (nuotolinį prisijungimą visais pateiktais būdais, aukšto patikimumą, našumo savybes ir pan.) ir pateikti testų rezultatus bei elektroniniu formatu.
6.2.2.	Bendrieji reikalavimai sprendimo diegimui, konfigūravimui, testavimui	Tiekėjas turi užtikrinti visų sprendimo komponentų diegimą, konfigūravimą ir testavimą.
		Sprendimo komponentai turi būti sukonfigūruoti tiek, kad būtų galima atlikti paslaugų suteikimą.
		Turi būti paruošti testavimo scenarijai, atliktas testavimas ir pateikta testavimo ataskaita.
		Turi būti sukonfigūruotas rezervinis duomenų kopijavimas.
		Visi darbai turi būti atliekami netrikdant sistemų ir neįtakojant naudotojų darbingumo su jomis. Esant numatomam ar galimam sistemų darbo sutrikdymui, tai turi būti iš anksto aptarta ir suderinta su Perkančiosios organizacijos atstovais.
6.2.3.	Specialieji reikalavimai tapatybės valdymo komponento diegimui ir konfigūravimui	Sprendimas turi būti suprojektuotas taip, kad būtų užtikrintas nepertraukiamas sistemos veikimas esant vieno iš tapatybės valdymo programinės įrangos (TVPĮ) komponento gedimo atvejui. Analizės ir projektavimo etapo metu turi būti atlikta: • Įvertinti TVPĮ sistemai keliami pasiekiamumo ir patikimumo reikalavimai. • TVPĮ sistema turi būti suprojektuota diegimui nenaudojant papildomos aparatinės įrangos ir turi būti diegiama į Perkančiosios organizacijos naudojamą virtualizacijos platformą. • Sprendimo architektūra turi turėti plėtimo galimybę esant du kartus didesniam duomenų kiekiui. • Projektavimo rezultatas turi būti suderintas su Perkančiosios organizacijos atstovais. Perkančiosios organizacijos atstovams turi būti pateikti reikalavimai infrastruktūros paruošimui, kurie bus susiję su šiuo TVPĮ sprendimu. Turi būti atliktas sprendimo diegimas pagal projektavimo etape numatytą architektūrą, bei šiam TVPĮ sprendimui keliamus reikalavimus.
6.2.4.	Specialieji reikalavimai VPN ugniasienės diegimui ir konfigūravimui	Turi būti atlikti sprendimo analizės darbai: • perkančiosios organizacijos infrastruktūros ir tinklo analizė; Turi būti atlikti sprendimo projektavimo darbai: • sprendimo architektūros projektavimas; • sprendimo srautų balansavimo projektavimas; • sprendimo išsidėstymo Perkančiosios organizacijos tinkle projektavimas; Turi būti atlikti sprendimo diegimo ir konfigūravimo darbai, apimantys: • sprendimo programinės įrangos diegimas; • sprendimo integracija su TVPĮ; • sprendimo integracija su IPsec koncentratoriumi;

		• standartinės paslaugos konfigūracijos šablono paruošimas; • standartinės paslaugos konfigūravimo instrukcijos sprendimo administratoriui paruošimas; • standartinės paslaugos instrukcijos sprendimo naudotojui paruošimas;
6.2.5.	Specialieji reikalavimai privilegijuotos prieigos valdymo komponento diegimui ir konfigūravimui	Turi būti atlikti sprendimo analizės darbai: • perkančiosios organizacijos infrastruktūros ir tinklo analizė; • privilegijuotų paskyrų analizė. Turi būti atlikti sprendimo projektavimo darbai: • sprendimo architektūros projektavimas; • sprendimo išsidėstymo Perkančiosios organizacijos tinkle projektavimas; • sprendimo prieigų ir teisių projektavimas. Turi būti atlikti sprendimo diegimo ir konfigūravimo darbai: • sprendimo programinės įrangos diegimas; • sprendimo avarinio atstatymo konfigūravimas; • sprendimo saugumo nustatymų sustiprinimas (angl. security hardening); • sprendimo integracija su TVPĮ; • sprendimo katalogų struktūros konfigūravimas; • sprendimo naudotojų, komandų, grupių ir rolių konfigūravimas; • el. pašto pranešimų konfigūravimas; • SSH ir RDP įgaliotųjų serverių (angl. proxy/jumphost) konfigūravimas; • sesijų vaizdo įrašymo konfigūravimas; • saugaus nuotolinio prisijungimo konfigūravimas.
6.2.6.	Specialieji reikalavimai IPsec koncentratoriaus komponento diegimui ir konfigūravimui	Turi būti atlikti sprendimo analizės darbai: • perkančiosios organizacijos infrastruktūros ir tinklo analizė; Turi būti atlikti sprendimo projektavimo darbai: • sprendimo architektūros projektavimas; • sprendimo išsidėstymo Perkančiosios organizacijos tinkle projektavimas; Turi būti atlikti sprendimo diegimo ir konfigūravimo darbai: • sprendimo integracija su VPN ugniasienėmis; • sprendimo integracija su privilegijuotos prieigos valdymo komponento elementais; • sprendimo integracija su kliento organizacijos ugniasienėmis; • standartinės paslaugos konfigūracijos šablono paruošimas; • standartinės paslaugos konfigūravimo instrukcijos sprendimo administratoriui paruošimas.
6.2.7.	Reikalavimai mokymams	Turi būti atlikti 4 (keturių) perkančiosios organizacijos darbuotojų siūlomo Sprendimo administravimo ir naudojimo, ne trumpesni nei 4 dienų (32 akademinės valandos), mokymai apimantys: • Darbuotojų apmokymą administruoti sprendimo techninius komponentus; • Darbuotojų apmokymą naujų paslaugų gavėjų ir jų paslaugų konfigūravimui. Mokymai turi vykti tiekėjo nurodytose patalpose arba nuotoliniu būdu. Jei mokymai vyksta ne nuotoliniu būdu, į pasiūlymo kainą turi būti įtrauktos visos su mokymais susijusios išlaidos, tame tarpe transportavimo, patalpų nuoma ir kt.

6.2.8.	Reikalavimai dokumentacijai	Turi būti pateikta įdiegtos programinės ir fizinės įrangos atliktų darbų techninė dokumentacija, apimanti programinės ir techninės įrangos diegimo aprašymus, sprendimo loginių sujungimo schemas bei kitus duomenis, reikalingus tolimesniam įrangos konfigūravimui ir eksploatavimui (IP adresai, valdymo programų vardai, prisijungimų vardai, slaptažodžiai ir pan.) Dokumentacija turi būti parengta lietuvių kalba ir pateikta elektroniniu formatu. Turi būti paruoštos visų paslaugų aktyvavimo (angl. onboarding) galutiniams klientams instrukcijos tinkančios paslaugų tiekėjui. Turi būti paruoštos instrukcijos paslaugų užsakymui ir/ar konfigūravimui, tinkančios paslaugų galutiniam naudotojui (pvz. VPN kliento sukonfigūravimas).

b. Pilotinis paslaugų diegimas ir testavimas

Nr.	Pavadinimas	Aprašymas
6.3.1.	Bendrieji reikalavimai	Siekiant užtikrinti sprendimo funkcionalumą ir dokumentacijos kokybę, tiekėjas projekto apimtyje kartu su perkančiosios organizacijos atstovais pagal paslaugų suteikimo dokumentaciją turi atlikti pilotinį paslaugų diegimą ir testavimą. Tiekėjas kartu su perkančiosios organizacijos atstovais turės sukonfigūruoti IPSec tunelius visiems paslaugų gavėjams, kurie pateks į pilotinių paslaugų apimtį. Pilotinių paslaugų suteikimo metu tiekėjas bus atsakingas už: • aptiktų standartinės konfigūracijos problemų tvarkymą; • paslaugų suteikimo dokumentacijos atnaujinimą; • aptiktų paslaugos gavėjo instrukcijų klaidų taisymą; • aptiktų paslaugos naudotojo instrukcijos klaidų taisymą; • nustatytų paslaugų įgyvendinimo trūkumų šalinimą. Pilotinių paslaugų diegimui ir testavimui perkančioji organizacija užtikrins: • pilotinio paslaugų gavėjų sąrašo pateikimą bei darbų koordinavimą su paslaugų gavėju ir paslaugų naudotojais; • aktyvų dalyvavimą pilotinių paslaugų diegime, testavime bei problemų identifikavime.
6.3.2.	Apimties reikalavimai	VPN prieigos prie institucijos tinklo paslaugos pilotinis diegimas ir testavimas turi apimanti: • nemažiau nei **10** paslaugų gavėjus (institucijas); • nemažiau nei **150** paslaugos naudotojų bendrai per visus pilotiniame diegime dalyvaujančius paslaugų gavėjus. Saugios trečių šalių prieigos paslaugos pilotinis diegimas ir testavimas, turi apimti: • nemažiau nei **5** paslaugų gavėjus (institucijas); • nemažiau nei **10** paslaugų naudotojų bendrai per visus pilotiniame diegime dalyvaujančius paslaugos gavėjus.

c. Konsultacijų paslauga

Nr.	Pavadinimas	Aprašymas
6.4.1.	Bendrieji reikalavimai	Pagal Perkančiosios organizacijos poreikį tiekėjas turi teikti konsultacijas apimančias: • paslaugų ir sprendimo keitimus pagal kintančius ar naujus reikalavimus;

Nr.	Pavadinimas	Aprašymas
		• pakeitimų susijusių su naujų PĮ versijų suderinamumu įgyvendinimą; • KVTC darbuotojų, atsakingų už paslaugų teikimą, konsultacijas. Konsultacijos turi būti teikiamos darbo dienomis nuo 8:00 val. iki 17:00 val. nuotoliniu būdu telefonu, el. paštu arba per vaizdo konferencijų platformą (pvz. Microsoft Teams).
6.4.2.	Apimties reikalavimai	Konsultacijos turi būti teikiamos 36 mėn. nuo sprendimo įgyvendinimo dienos. Tiekėjas turi suteikti iki 600 val. konsultacijų, kurios turi būti įskaičiuotos į sprendimo kainą.

d. Sprendimo priežiūra ir palaikymas

Nr.	Pavadinimas	Aprašymas
6.5.1.	Bendrieji reikalavimai	Sprendimo priežiūra ir palaikymas turi apimti: • kasdienį viso sprendimo ar atskirų jo komponentų stebėjimą (monitoringas), incidentų aptikimą ir sprendimą, įrangos bendrinės konfigūracijos pakeitimų, išskyrus naujų ar keičiamų paslaugų konfigūravimą, atlikimą; • sprendimo komponentų atnaujinimo planavimą, diegimą ir testavimą, išskrus tuos atvejus, kai dėl naujų versijų funkcionalumo pasikeitimo atsiranda komponentų tarpusavio suderinamumo problemos; • projekto metu apibrėžtų reikalavimų ar konsultacijų metų padarytų pakeitimų apimtyje, aptiktų klaidų taisymą, veikimo problemų sprendimą. Sprendimo priežiūra ir palaikymas neturi apimti: • dėl gamintojų atliktų PĮ versijų pakeitimų atsiradus sprendimo komponentų tarpusavio suderinamumo, pasikeitus atskirų komponentų PĮ versijoms ar sąsajoms, kurios reikalauja esminių komponentų konfigūracijų ar sukurtų integracijų pakeitimų, problemų sprendimo; • sprendimo ir paslaugų tobulinimo pasikeitus esamiems ar atsiradus naujiems reikalavimams; • Naujų paslaugų gavėjų prijungimo, bei susijusių konfigūracijų pakeitimų; • Paslaugų gavėjų, paslaugų administratorių, paslaugų naudotojų kreipinių valdymo. Visos paslaugų gavėjų, paslaugų administratorių, paslaugų naudotojų užklausos bus valdomos Perkančiosios organizacijos pagalbos tarnybos. Užklausos Tiekėjui bus perduodamos tik Perkančiosios organizacijos pagalbos tarnybos ar kitų Perkančiosios organizacijos atsakingų darbuotojų.
6.5.2.	Apimties reikalavimai	Sprendimo priežiūra ir palaikymas turi būti teikiamas 36 mėn. nuo sprendimo įgyvendinimo dienos. Sprendimo priežiūra ir palaikymas turi būti vykdomas darbo dienomis nuo 08:00 iki 17:00, o Tapatybės valdymo komponentui vykdoma priežiūra 24 val. per parą, 7 dienas per savaitę.
6.5.3.	Paslaugų kokybės reikalavimai (SLA)	Priežiūros ir palaikymo paslaugos turi atitikti žemiau pateiktą paslaugų teikimo lygį (SLA) per 1 mėn. (minutėmis): • viso sprendimo neveikimas kuris įtakoja visas paslaugas, darbo dienomis, nuo 08:00 iki 17:00:

		• reakcijos laikas – 60 min.; • gedimų šalinimo laikas – 180 min. • viso sprendimo neveikimas kuris įtakoja visas paslaugas darbo dienomis nuo 17:00 iki 08:00 ir nedarbo dienomis: • reakcijos laikas – 60 min.; • gedimų šalinimo laikas – 360 min. • VPN prieigos prie organizacijos tinklo paslaugos visiškas neveikimas, darbo dienomis, nuo 08:00 iki 17:00: • reakcijos laikas – 60 min.; • gedimų šalinimo laikas – 240 min. • Trečiųjų šalių prieigos paslaugos visiškas neveikimas, darbo dienomis, nuo 08:00 iki 17:00: • reakcijos laikas – 60 min.; • gedimų šalinimo laikas – 360 min.
6.5.4.	Pagalbos tarnyba	Tiekėjo pagalbos tarnyba turi suteikti galimybes registruoti kreipinius įvairiais nurodytais kanalais: elektroniniu paštu; fiksuoto ir mobilaus ryšio telefonu; naudojant WEB sąsają. Tiekėjas turi būti įdiegęs veikiančius ir aprašytus incidentų bei keitimų valdymo procesus, atitinkančius IT paslaugų valdymo (ITIL ar lygiavertės metodikos) gerųjų praktikų rekomendacijas bei veikiantį internetinį portalą kreipiniams registruoti bei peržiūrėti. Tiekėjo pagalbos tarnyba turi užtikrinti operatyvų atgalinį ryšį ir informacijos apie incidentus realiu laiku (angl. On-line) teikimą interneto tinklalapyje, veikiančiame HTTPS protokolu. Pagalbos tarnyba turi informuoti apie užregistruotų incidentų būklę, planuojamą incidentų išsprendimo datą ir laiką bei incidentų išsprendimą. Tiekėjas turi būti įsidiegęs sprendimą, kurio pagalba visi nuotoliniai prisijungimai būtų įrašomi, o esant Perkančiosios organizacijos poreikiui, Tiekėjas turi suteikti Perkančiajai organizacijai įrašytą sesiją. Sesijos turi būti saugomos ne trumpiau kaip 6 mėn.

7. Bendrieji reikalavimai paslaugoms

7.1. Perkančioji organizacija, vadovaudamasi Viešųjų pirkimų įstatymo (toliau – Įstatymas) 37 straipsnio 8 ir 9 dalies 1 papunkčiu, laikys, kad prekės kelia grėsmę nacionaliniam saugumui, kai prekių gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.

7.2. Perkančioji organizacija, vadovaudamasi Įstatymo 47 straipsnio 8 ir 9 dalimi, laikys, kad prekės kelia grėsmę nacionaliniam saugumui, kai tiekėjas turi interesų, galinčių kelti grėsmę nacionaliniam saugumui, ir draudžia pirkime dalyvauti tiekėjams, jų subtiekėjams ar ūkio subjektams, kurių pajėgumais remiamasi, kurie patys ar juos kontroliuojantys asmenys yra registruoti (jeigu tiekėjas, jo subtiekėjas, ūkio subjektas, kurio pajėgumais remiamasi, ar kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.

7.3. Į bendrą pasiūlymo kainą turi būti įtrauktos visos gamintojo licencijos, reikalingos perkamo spendimo nuotolio prisijungimo sprendimo reikalaujamoms funkcijoms vykdyti ir palaikyti.

7.4. Kartu su Pasiūlymu Tiekėjas laisva forma turi pateikti tikslias siūlomos įrangos konfigūracijas, kuriose būtų pateikti tikslūs Nuotolinio prisijungimo sprendimo komponentų modeliai,

prekių kodai, kiekiai, pavadinimai ir kita standartiškai gamintojų konfigūratoriuose pateikiama informacija.

7.5. *Kartu su pasiūlymu tiekėjas **turi pateikti** dokumentus, (gamintojų dokumentaciją, nuorodas į gamintojų svetaines, gamintojų raštus, Tiekėjo deklaraciją ar kitus dokumentus), įrodančius siūlomų prekių atitikimą kokybės ir techniniams reikalavimams, nurodytiems pirkimo dokumentų techninėje specifikacijoje: tiekėjas turi pateikti gamintojo parengtus katalogus ir/ar siūlomos įrangos (šiuo metu gaminamų, išbandytų, sertifikuotų ir paruoštų tiekimui) techninių charakteristikų aprašymus (jei gamintojo kataloge neišsamiai atsispindi siūlomų prekių atitikimas techninės specifikacijos reikalavimams) (pdf formatu). **Šiuose dokumentuose tiekėjas turi grafiškai nurodyti (t. y. pastebimai pažymėti – spalvotai žymėti ir/ar nurodyti rodyklėmis, ir/ar pabraukti) konkrečias teikiamų dokumentų vietas, kur aprašomos reikalaujamų techninių charakteristikų reikšmės, bei įrašyti, kurį techninių reikalavimų punktą jos atitinka**. Jei gamintojo išleistame kataloge nėra Perkančiosios organizacijos reikalaujamos prekės parametro atitiktį patvirtinančios informacijos, Tiekėjas gali pateikti atitiktį patvirtinančią prekių gamintojo deklaraciją.*

7.6. Įrangos diegimą, konfigūravimą, garantinį aptarnavimą atliekantys specialistai privalo mokėti lietuvių kalbą arba turi būti užtikrintos kokybiškos vertimo paslaugos.