**VALSTYBĖS ĮMONĖS TURTO BANKO**

# TECHNINIO STANDARTO

# PRIEDAS TechNet
# (Kibernetinio saugumo reikalavimai pastatams)

**2025 m.**

**KIBERNETINIO SAUGUMO REIKALAVIMAI PASTATŲ VALDYMO SISTEMOMS IR INŽINERINĖMS VALDYMO SISTEMOMS**

1. BENDROSIOS NUOSTATOS

1.1. Dokumento paskirtis

Šis dokumentas nustato privalomus kibernetinio saugumo reikalavimus, taikomus visoms pastatų valdymo sistemoms ir inžinerinėms valdymo sistemoms (toliau – OT), diegiamoms ar atnaujinamoms Turto banko valdomuose, projektuojamuose, prižiūrimuose objektuose. Dokumentas apibrėžia reikalavimus, kurių įgyvendinimą būtina užtikrinti visuose siūlomuose OT sprendimuose.

1.2. Taikymo sritis

Reikalavimai taikomi visiems rangovams, teikiantiems paslaugas ar įrangą, susijusią su:

- Pastatų valdymo sistemomis (toliau – PVS);
- ŠVOK (HVAC) sistemomis;
- Apšvietimo valdymo sistemomis;
- Gaisro aptikimo ir gesinimo sistemomis;
- Fizinės prieigos kontrolės sistemomis;
- Fizinio saugumo sistemomis;
- Energijos valdymo sistemomis;
- Kitomis inžinerinėmis sistemomis, kurios gali būti prijungtos prie tinklo.

1.3. Reikalavimų laikymasis:

1.3.1. Būtina pateikti išsamų dokumentą, aprašantį, kaip siūlomas sprendimas atitinka visus šiame dokumente nurodytus reikalavimus.

1.3.2. Bet kokie nukrypimai nuo reikalavimų turi būti aiškiai identifikuoti ir pateikti su pagrindimais bei alternatyviais kompensuojančiais kontrolės mechanizmais, kurių naudojimas turi būti suderintas su Užsakovo atsakingais asmenimis.

1.3.3. Visa reikalaujama dokumentacija turi būti pateikta lietuvių kalba.

2. TINKLO ARCHITEKTŪRA IR SEGMENTAVIMAS

2.1. Tinklo segmentavimas

2.1.1. Rengiamuose projektuose būtina įgyvendinti tinklo architektūrą, kurioje OT tinklai yra fiziškai arba logiškai atskirti nuo įmonės IT tinklo, naudojant pramoninės klasės ugniasienę su giluminės paketų analizės galimybėmis. Reikalavimus ugniasienei pateikia Turto bankas.

2.1.2. Rangovas turi pateikti išsamų tinklo architektūros brėžinį redaguojamu elektroniniu formatu (Microsoft Visio, Autocad), kuriame aiškiai pažymėti visi segmentai, ugniasienės, maršrutizatoriai ir kiti OT tinklo įrenginiai, nurodant kiekvieno komponento paskirtį bei ryšius tarp jų, loginio atskyrimo konfigūraciją.

2.1.3. Turto bankas pateikia OT tinklo loginio segmentavimo informaciją, kuri apima:

- VLAN pavadinimą ir ID;
- VLAN paskirtį;
- IP adresų diapazonus;
- Tinklo kaukes.

2.1.4. Kritinėms sistemoms (pvz., vaizdo, saugos sistemoms, gaisro aptikimo ir gesinimo sistemos, evakuacijos valdymo sistemos, fizinės prieigos kontrolės sistemos) turi būti naudojami fiziškai atskirti tinklo komutatoriai, užtikrinant, kad šių sistemų veikimas nepriklausytų nuo bendros OT tinklo infrastruktūros.

2.1.5. OT tinklo valdymui naudojamos įrangos reikalavimus pateikia Turto bankas.

2.2. Tinklo architektūros lygmenys

2.2.1. OT tinklo architektūra turi būti suskirstyta į bent tris lygmenis:

- Valdymo lygmenį (Management Level) - operatorių darbo vietos, serveriai;
- Automatizacijos lygmenį (Automation Level) - valdikliai, tinklo įrenginiai;

- Lauko įrenginių lygmenį (Field Level) - jutikliai, matuokliai.

2.2.2. Kiekvienas lygmuo turi būti atskirtas naudojant loginį atskyrimo būdą, kuris riboja duomenų srautus tarp skirtingų lygmenų.

2.2.3. Reikalaujama pateikti išsamią dokumentaciją, paaiškinančią kiekvieno lygmens paskirtį, veikimą ir saugumo kontrolės mechanizmus.

2.2.4. Turi būti įdiegti mechanizmai, užtikrinantys, kad kompromituotas vienas lygmuo negalėtų tiesiogiai paveikti kitų lygmenų saugumo.

2.3. Saugos sistemų atskyrimas

2.3.1. Būtina pateikti išsamią dokumentaciją, kaip užtikrinamas saugos sistemų atsparumas kibernetinėms grėsmėms, įskaitant:

- Tinklo architektūros aprašymą;
- Prieigos kontrolės mechanizmus;
- Autentifikacijos metodus;
- Šifravimo protokolus;
- Atsarginių kopijų strategijas.

2.3.2. Saugos sistemų kritinės funkcijos turi išlikti veikiančios net tuo atveju, jei kitos OT dalys yra pažeistos ar nepasiekiamos. Reikalaujama dokumentuoti, kaip užtikrinamas šis funkcionalumas.

2.3.3. Turi būti numatyti avariniai darbo režimai, leidžiantys valdyti saugos sistemas net visiško tinklo ryšio praradimo atveju.

2.3.4. Saugos sistemos turi turėti funkcionalumus tikrinančius sistemų pasiekiamumą ir veikimą.

2.4. Ugniasienės ir OT tinklo įrenginių konfigūracija

2.4.1. Ugniasienės turi būti sukonfigūruotos laikantis principo "uždrausti viską, išskyrus tai, kas būtina" visuose tinklo segmentuose. Turi būti dokumentuotas kiekvienas leidžiamas ryšys.

2.4.2. Būtina pateikti išsamų ugniasienės taisyklių sąrašą su aiškiu kiekvienos taisyklės pagrindimu. Sąrašas turi būti suderintas su Turto banko atsakingu asmeniu, kurio realizavimą atlieka Turto banko atsakingas asmuo. Sąraše turi būti nurodyta:

- Šaltinio IP adresas ar tinklas;
- Paskirties IP adresas ar tinklas;
- Protokolas ir prievadas;
- Veiksmas (leisti/drausti);
- Taisyklės paskirtis ir pagrindimas.

2.4.3. Ugniasienės taisyklės turi apriboti tiek įeinantį, tiek išeinantį ryšį tarp visų tinklo segmentų, užtikrinant mažiausių privilegijų principą.

2.4.4. Reikalaujama užtikrinti, kad ugniasienės taisyklės leidžia tik būtinus protokolus ir prievadus, reikalingus sistemų veikimui. Visi nenaudojami prievadai ir protokolai turi būti užblokuoti.

2.4.5. Ugniasienės konfigūracijos pakeitimai atliekami tik Turto banko atsakingų asmenų.

2.4.6. Ugniasienė turi palaikyti giluminę paketų analizę (Deep Packet Inspection) pramoniniams protokolams (Modbus, BACnet, KNX ir kt.), užtikrinant, kad per šiuos protokolus nėra perduodami kenkėjiški duomenys.

2.4.7. Būtina užtikrinti ugniasienių sinchronizaciją ir integruotą veikimą, jei architektūroje naudojamos kelios ugniasienės.

2.4.8. Komunikacija tarp skirtingų lygmenų turi būti įmanoma tik tarp gretimų lygmenų (pvz., valdymo lygmuo gali komunikuoti tik su automatizacijos lygmeniu, o ne tiesiogiai su lauko įrenginių lygmeniu).

2.4.9. OT tinkle turi būti realizuotas pajungiamų įrenginių autentifikavimas, kuris užtikrina tik autorizuotų įrenginių naudojimą. Neautorizuotų įrenginių naudojimas turi būti blokuojamas, užtikrinant jų izoliavimą nuo kitų OT tinklo įrenginių.

2.5. Integravimas su Turto banko saugumo sistemomis

2.5.1. Visi OT tinklo komponentai turi būti integruoti su Turto banko centralizuota žurnalinių įrašų kaupimo ir valdymo sistema, perduodant:

- OT sistemų įjungimas, išjungimas ar perkrovimas;
- Naudotojų ir administratorių autentifikavimo įvykiai, įskaitant prisijungimus prie sistemų valdymo sąsajų;
- Naudotojų, administratorių paskyrų sukūrimas, prieigų prie OT sistemų valdymo aplinkų pakeitimai;
- OT sistemų konfigūravimo parametrų pakeitimai;
- Saugasienių taisyklių pakeitimai;
- Žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas.

2.5.2. Reikalaujama užtikrinti, kad visi OT komponentų žurnaliniai įrašai yra perduodami į Turto banko centralizuoto žurnalų kaupimo sprendimą, laikantis šių reikalavimų:

- Žurnalinių įrašų perdavimui turi būti naudojamas Syslog protokolas (RFC 5424), kuris užtikrina standartizuotą formatą ir patikimą perdavimą;
- Perdavimui turi būti naudojamas šifruotas TLS transporto protokolas (Syslog over TLS, RFC 5425), užtikrinantis duomenų konfidencialumą ir vientisumą;
- Žurnalinių įrašų formatas turi atitikti Common Event Format (CEF) arba Structured Data formatą, kuris leidžia standartizuotai perduoti struktūrizuotus duomenis;
- Žurnalinių įrašų perdavimo mechanizmas turi palaikyti TCP protokolą, užtikrinantį patikimą duomenų perdavimą;
- Žurnalinių įrašų perdavimo mechanizmai turi būti sukonfigūruoti taip, kad būtų atsparūs tinklo ryšio sutrikimams, įskaitant lokalų įrašų kaupimą ryšio sutrikimo atveju ir automatinį perdavimą atkūrus ryšį.

2.6. Centralizuota nuotolinio prisijungimo architektūra

2.6.1. OT sprendimai su Turto banko tinklu integruojami naudojant site-to-site VPN sprendimą, kuris:

- Naudoja IPsec tunelinio režimo protokolą;
- Naudoja AES-256 ar stipresnį šifravimą;
- Naudoja SHA-256 ar stipresnį maišos algoritmą;
- Palaiko Perfect Forward Secrecy (PFS).

2.6.2. VPN sprendimo konfigūravimą atlieka Turto banko atsakingas asmuo.

2.6.3. VPN sprendimas turi užtikrinti pakankamą pralaidumą tiek operaciniams, tiek stebėsenos duomenims perduoti.

2.6.4. Visi Turto banko darbuotojai, išoriniai tiekėjai, rangovai, kuriems reikalinga nuotolinė prieiga prie OT, privalo naudoti Turto banko suteiktus sprendimus ir laikytis nustatytų prisijungimo sąlygų.

2.6.5. Visi prisijungimai prie nutolusių OT sprendimų turi būti stebimi atliekant:

- visų prisijungimo bandymų fiksavimą (fiksuojami sėkmingi ir nesėkmingi bandymai prisijungti);
- nuotolinės sesijos įrašymą.

2.6.6. Prieiga prie OT sistemų iš išorinių tinklų yra draudžiama.

## 3. PRIEIGOS VALDYMAS

3.1. OT sistemose turi būti realizuotas paskyrų sukūrimo ir valdymo funkcionalumas.

3.2. Prieigos prie OT sistemų turi būti grindžiamos rolėmis, užtikrinant mažiausių privilegijų principo įgyvendinimą.

3.3. OT sistemos automatizuotą paskyrų naudojimo, prieigos teisių keitimo žurnalizavimo mechanizmą, kuris naudojamas atliekantį auditus bei taikomas atitinkamų įvykių perdavimui į Turto banko centralizuotą žurnalinių įrašų kaupimo ir valdymo sistemą.

3.4. Nenaudojamos paskyros bus blokuojamos pagal Turto banko saugos taisyklėse nurodytus reikalavimus.

3.5. Būtina užtikrinti, kad OT sistemose būtų laikomasi slaptažodžių sudarymo reikalavimų, kurie numato:

3.5.1. Minimalų 16 simbolių slaptažodžio ilgį paskyroms.

3.5.2. Sudėtingumo reikalavimus (didžiosios ir mažosios raidės, skaičiai, specialūs simboliai), užtikrinant, kad slaptažodžiai būtų atsparūs žodyno atakoms.

3.5.3. Slaptažodžių galiojimo laiką (ne ilgiau kaip 90 dienų), užtikrinant reguliarų atnaujinimą.

3.5.4. Slaptažodžių istorijos saugojimą (bent 6 paskutinių slaptažodžių), neleidžiant pakartotinio naudojimo.

3.5.5. Draudimą naudoti lengvai atspėjamus slaptažodžius, įskaitant dažniausiai naudojamus ar pažeidžiamus slaptažodžius.

3.6. Reikalaujama pateikti dokumentaciją, kaip slaptažodžių politika yra įgyvendinta ir užtikrinama visuose OT komponentuose.

3.7. Visi gamykliniai slaptažodžiai turi būti pakeisti unikaliais slaptažodžiais prieš OT sistemų ir tinklo komponentų perdavimą eksploatacijai.

3.8. Slaptažodžių sudarymo reikalavimai gali būti netaikomi paskyroms, prie kurių prisijungimas galimas tik per Turto banko valdomą tarpinį prisijungimų serverį. Išimtys derinamos su Turto banko atsakingu asmeniu.

3.9. OT sistemose turi būti įdiegta rolėmis grįsta prieigos kontrolės sistema, kuri:

3.9.1. Leidžia apibrėžti ir valdyti roles, atitinkančias paskyros naudotojo funkcijas;

3.9.2. Palaiko minimalių privilegijų principą, suteikiant tik tas teises, kurios būtinos funkcijoms atlikti;

3.9.3. Rolių priskyrimo vartotojams auditavimą.

3.10. Turi būti pateikta išsami rolių valdymo dokumentacija, įskaitant:

3.10.1. Rolių hierarchijos aprašymą, nurodant pavaldumo ir paveldėjimo santykius;

3.10.2. Kiekvienos rolės teisių išsamų aprašymą.

3.11. Visi OT komponentai turi būti fiziškai apsaugoti nuo nesankcionuotos prieigos:
3.11.1. Serveriai ir tinklo įrenginiai turi būti laikomi užrakintose serverių spintose ar patalpose;
3.11.2. Valdikliai ir kita įranga turi būti laikoma užrakintuose skyduose ar spintose;
3.11.3. Lauko įrenginiai turi būti apsaugoti nuo neteisėtos prieigos ir vandalizmo;
3.12. Rangovas turi pateikti išsamią fizinės įrenginių apsaugos dokumentaciją, įskaitant:
3.12.1. Ryšio patalpų apsaugos aprašymą;
3.12.2. Spintų ir skydų apsaugos aprašymą;
3.12.3. Lauko įrenginių apsaugos aprašymą;
3.12.4. Kabelių apsaugos aprašymą.
3.13. Fizinė įrenginių apsauga turi atitikti Turto banko fizinės saugos standartus ir geriausias praktikas.
3.14. Fizinė įrenginių apsauga turi būti reguliariai tikrinama ir prižiūrima.

4. PROGRAMINĖS ĮRANGOS IR ĮRENGINIŲ SAUGUMO VALDYMAS

4.1. Programinės įrangos pataisų valdymas
4.1.1. Rangovas turi pateikti OT sistemų programinės įrangos pataisų diegimo dokumentaciją, įskaitant:
4.1.1.1. Pataisų šaltinių aprašymą;
4.1.1.2. Pataisų diegimo periodiškumą;
4.1.1.3. Pataisų diegimo ir atšaukimo procedūrą.
4.1.2. Kritinės saugumo spragos turi būti taisomos ne vėliau kaip per 60 dienų nuo jų paskelbimo, o ypač kritinės - per 14 dienų.
4.1.3. Jei negalima įdiegti pataisų, būtina pateikti kompensuojančių kontrolės priemonių aprašymą.
4.2. Programinės įrangos inventorizacija
4.2.1. Rangovas turi pateikti ir esant poreikiui atnaujinti visų OT sistemų, įrenginių programinės įrangos komponentų sąrašą, kuris apima:
4.2.1.1. Programinės įrangos pavadinimą ir versiją;
4.2.1.2. Gamintojo pavadinimą ir kontaktinę informaciją;
4.2.1.3. Licencijos informaciją ir galiojimo terminus;
4.2.1.4. Diegimo datą ir vietą;
4.2.1.5. Palaikymo informaciją ir galiojimo terminus
4.2.2. Programinės įrangos inventorizacija turi būti atnaujinama po kiekvieno pakeitimo.
4.3. OT įrenginių saugumo valdymas
4.3.1. Visų OT įrenginių konfigūravimas turi būti atliekamas taikant saugias nuostatas pagal gamintojų pateiktas kibernetinio saugumo rekomendacijas ir geriausias praktikas, įskaitant:
4.3.1.1. Nenaudojamų paslaugų išjungimą;
4.3.1.2. Nenaudojamų prievadų uždarymą;
4.3.1.3. Nenaudojamų protokolų išjungimą;
4.3.1.4. Nenaudojamų taikomųjų programų pašalinimą;
4.3.1.5. Operacinės sistemos saugos nuostatų taikymą.
4.3.2. Reikalaujama pateikti išsamią OT įrenginių nustatytų konfigūracijų dokumentaciją, įskaitant:
4.3.2.1. Standartinius nustatymus kiekvienam įrenginio tipui;
4.3.2.2. Nustatymų keitimo ir nustatymo procedūras.
4.3.3. OT įrenginių nuostatos turi būti nustatytos ir patikrintos prieš jų diegimą į eksploataciją.
4.4. OT įrenginių inventorizacija
4.4.1. Rangovas turi pateikti ir esant poreikiui atnaujinti visų OT įrenginių sąrašą, kuris apima:
4.4.1.1. Įrenginio tipą ir modelį
4.4.1.2. Gamintojo pavadinimą ir kontaktinę informaciją
4.4.1.3. Aparatinės įrangos ir programinės įrangos versijas
4.4.1.4. Tinklo informaciją (IP adresas, MAC adresas)
4.4.1.5. Fizinę vietą
4.4.1.6. Atsakingą asmenį
4.4.1.7. Palaikymo informaciją ir galiojimo terminus
4.4.2. OT įrenginių sąrašas turi būti atnaujinamas po kiekvieno pakeitimo.
4.5. Kenkėjiškos programinės įrangos apsauga

4.5.1. Visuose OT įrenginiuose, kurie palaiko tokias priemones, turi būti įdiegtos kenkėjiškos programinės įrangos apsaugos priemonės, kurias pateikia Turto bankas.

4.5.2. Jei OT įrenginiai negali palaikyti Turto banko pateiktų kenkėjiškos programinės įrangos apsaugos priemonių, būtina pateikti alternatyvių saugumo priemonių aprašymą.

4.6. Atsarginės kopijos ir atkūrimas

4.6.1. Tiekėjas turi pateikti atsarginių kopijų darymo bei sistemų veiklos atkūrimo aprašą, kuris aprašytų OT sistemų atsarginių kopijų darymą bei veiklos atkūrimo veiksmus.

4.6.2. Apraše, suderintame su atsakingu Turto banko darbuotoju, turi būti pateikta:

4.6.2.1. Atsarginių kopijų darymo grafikas

4.6.2.2. Atsarginių kopijų darymo procedūra

4.6.2.3. Atsarginių kopijų testavimo procedūra

4.6.2.4. Atkūrimo po incidentų prioritetus ir procedūrą

4.6.2.5. Atkūrimo laiko tikslus (RTO) ir atkūrimo taško tikslus (RPO)

4.6.2.6. Atkūrimo po incidentų testavimo procedūra

4.6.3. Atkūrimo po incidentų procesas turi apimti visus kritinius OT komponentus.

## 5. BAIGIAMOSIOS NUOSTATOS

5.1. Tiekėjų siūlomi sprendimai turi atitikti šiuos reglamentus:

5.1.1. Bendrąjį duomenų apsaugos reglamentą (BDAR);

5.1.2. Kibernetinio saugumo įstatymą;

5.1.3. Kitus taikytinus nacionalinius ir tarptautinius reglamentus.

5.2. Šie reikalavimai yra privalomi visiems tiekėjams, teikiantiems paslaugas ar įrangą, susijusią su Turto banko valdomuose objektuose projektuojamais, įrengiamais OT sprendimais.

5.3. Tiekėjai turi bendradarbiauti su Turto banko atsakingais asmenimis siekiant užtikrinti šių reikalavimų įgyvendinimą ir atitiktį.

5.4. Turto bankas pasilieka teisę keisti ir papildyti šiuos reikalavimus pagal poreikį.

**TECHNINIAI REIKALAVIMAI UGNIASIENEI**

**1. Bendroji informacija**

1.1. Valstybės įmonė Turto bankas (toliau – Turto bankas) numato, kad pastato valdymo technologinė įranga bus pasiekiama per BĮ Kertinio valstybės telekomunikacijų centro (toliau – KVTC) teikiamą tinklo paslaugą iš Turto banko būstinės Kęstučio g. 45, Vilniuje. Tuo tikslu pastate turi būti įrengtas tinklo įrenginys su ugniasienės funkcionalumu (toliau – ugniasienė), pilnai suderinamas su Turto banke naudojama ir centralizuotai valdoma Fortinet firmos įranga. Jeigu pastate nėra/nebus teikiamos KVTC tinklo paslaugos, ugniasienė, papildomai, turi turėti galimybę duomenis perduoti naudojant mobiliojo ryšio technologijas (SIM kortelę pateiks Turto bankas).

1.2. Ugniasienę konfigūruos ir valdys Turto bankas.

1.3. Ugniasienė turės būti registruota gamintojo sistemoje Turto banko vardu, pateikiant gamintojo arba įgalioto atstovo registravimo deklaraciją arba kitą tai patvirtinančią informaciją.

1.4. Ugniasienės įrangos gamintojas nėra paskelbęs apie siūlomos ugniasienės gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).

1.5. Ugniasienė privalo būti nauja ir nenaudota, gamykliškai atnaujinti komponentai („Refurbished“) neleistini.

1.6. Iki ugniasienės turi būti atvesti kompiuteriniai tinklai, atskiriant fiziškai arba logiškai (segmentuojant), šias pastato valdymo įrangas:

1.6.1. PVS (jei pastate bus centralizuota sistema)

1.6.2. Šildymo ir vėsinimo sistemų valdymo;

1.6.3. pastato apsaugos kontrolerio;

1.6.4. vaizdo stebėjimo sistemos;

1.6.5. elektroninės įeigos kontrolės (praėjimo kontrolės) sistemos(ų)

1.6.6. Kitos pastato valdymo sistemos.

## 2. Minimalūs techniniai reikalavimai ugniasienei:

| | |
|---|---|
| Produkto surinkimo reikalavimai | Ugniasienė turi būti specializuotas aparatinis-programinis įrenginys (angl. *Appliance*) komplektuojamas paties gamintojo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtus sprendimus. |
| Konstrukcija | Ne daugiau kaip 1U aukščio, montuojama į 19“ komutacinę spintą, pateikiama su montavimo komponentais ir/arba lentyna, skirtais siūlomą įrangą patalpinti komutacinėje spintoje. |
| Suderinamumas | Turi būti pilnai suderinama su Turto banke naudojamais ugniasienių centralizuoto valdymo sprendimais FortiManager ir FortiCloud, kurių pagalba centralizuotai ir efektyviai administruojama visa Turto banko tinklo saugumo infrastruktūra iš vienos vietos. |
| Vidinio tinklo prievadai (portai) | Ne mažiau kaip 5 vnt. 1G (RJ-45) , kiekvienas iš lizdų privalo palaikyti RJ-45 standarto jungtis. Parinkus tinkamas tinklų konfigūracijas ir suderinus su Turto banku prievadų kiekis gali būti mažinamas iki 4 vnt. Prievadų kiekis turi užtikrinti, kad būtų įgyvendintas šios techninės specifikacijos 1.6 punktas. |
| Išorinio tinklo (WAN) prievadai (portai) | Ne mažiau kaip 1 vnt. 1G (RJ-45), lizdas privalo palaikyti RJ-45 standarto jungtis. |
| Dedikuoti valdymo prievadai | • Ne mažiau kaip 1 vnt. konsolės prievadas RJ-45.<br>• Ne mažiau kaip 1 vnt. USB prievadas. |
| Belaidis duomenų perdavimas (taikoma jeigu pastate nėra KVTC teikiamo laidinio ryšio) | Integruotas 3G/4G/LTE/5G belaidžio WAN modulis su išorinėmis antenomis. Esant poreikiui užtikrinti stabilų ryšį papildomai pateikiami ir antenų prailginimo kabeliai. |
| Našumas (ne mažiau) | • Ugniasienės pralaidumas: 3 Gbps<br>• IPS pralaidumas: 2 Gbps<br>• NGFW (next-generation firewall) pralaidumas: 250 Mbps<br>• SSL VPN pralaidumas: 150 Mbps<br>• Palaikomas VPN vartotojų skaičius: iki 500 IPsec ir iki 100 SSL VPN naudotojų |
| Saugumo funkcijos | • Integruotas SD-WAN funkcionalumas arba lygiavertis<br>• Nulinio pasitikėjimo tinklo prieigos (Zero Trust Network Access) kontrolė |
| Valdymas | Ne mažiau nei: WEB naršyklė (HTTPS), SSH, konsolė RJ-45. |
| Galimi ugniasienės darbo režimai | L3 ir L2 pagal *OSI* modelį. |
| Ugniasienės funkcionalumas | Turi būti galimybė kurti taisykles pagal vartotojus |
| Maršrutizavimas | Turi palaikyti statinį, dinaminį ir maršrutizavimą pagal taisykles (angl. policy routing) arba lygiaverčius |
| Palaikomi NAT (Network Address Translation) tipai | Source NAT (SNAT), Destination NAT (DNAT), Virtual IP (VIP), One-to-One ANT, NAT Traversal, NAT-based Policy Routing arba lygiaverčius |
| Integruoti serveriai | Turi turėti šiuos integruotus serverius: DHCP Server (Dynamic Host Configuration Protocol), NTP Server (Network Time Protocol), DNS proxy server. |
| IPsec kriptavimo, maišos ir autentifikavimo algoritmai | Turi palaikyti:<br>• AES (Advanced Encryption Standard), 3DES (Triple DES) ir DES (Data Encryption Standard) IPsec kriptavimo algoritmus<br>• SHA (Secure Hash Algorithm) ir MD5 (Message Digest Algorithm 5) maišos (Hash) algoritmus<br>• Pre-shared Key (PSK), X.509 Certificates ir RSA (Rivest–Shamir– |

| | |
|---|---|
| | Adleman) autentifikavimo algoritmus<br>• IKEv2 (Internet Key Exchange version 2) VPN modulius. |
| VPN funkcionalumas | Turi būti šie funkcionalumai:<br>• Galimybė redaguoti SSL VPN portalą.<br>• Galimybė naudotis SSL VPN per naršyklę be papildomų agentų ar programinės įrangos.<br>• VPN klientasturi palaikyti tiek IPsec, tiek SSL protokolus.<br>• Kliento programinė įranga turi būti to paties gamintojo kaip ir įranga.<br>• Kliento programinė įranga turi palaikyti skaitmeninių sertifikatų naudojimą tapatybės nustatymui. |
| Įvykių žurnalo įrašai | Turi būti fiksuojami ir kaupiami šių kategorijų žurnalų įrašai: perduoto srauto sesijos, sesijos su pažeidimais, sistemos ir administratorių veiksmų įvykiai, maršrutizavimo ir VPN įvykių įrašai (ne mažiau). |
| Įvykių žurnalų (event log) įrašų saugojimo pasirinkimas | • Turi būti galimybė saugoti lokaliai<br>• Turi būti galimybė siųsti į Syslog/ SIEM serverius |
| Integravimas | Turi palaikyti SNMP (Simple Network Management Protocol):<br>• palaikyti SNMPv1, SNMPv2c, ir SNMPv3 protokolus<br>• palaikyti SNMP traps, Get ir Set užklausas<br>• turi būti galimybė naudoti SNMP OID duomenų gavimui ir valdymui |
| Galimybė užtikrinti aukšto patikimumo sprendimus | Ugniasienė turi turėti galimybę užtikrinti aukšto patikimumo sprendimus (palaikomi Active/Passive arba Clustering arba lygiaverčiai įrenginių sujungimo būdai). |
| Palaikymo paslaugos/įrangos garantijos | Turi būti pateiktas palaikymas apimantis techninį palaikymą, prietaiso garantiją, programinės įrangos atnaujinimus ir klaidų taisymą 5 metų laikotarpiui. |

Jeigu pastate diegiami sprendimai nepalaiko kokio nors funkcionalumo arba integracinių sprendimų, tiekėjas/rangovas gali pateikti lygiaverti sprendimą ir suderinęs jį su Turto banku, įgyvendinti. Turi būti užtikrintas pilnai veikiantis ugniasienes sprendimas, numatant visą techninę ir programinė įrangą.