



AB „PANEVĖŽIO ENERGIJA“
INFORMATIKOS IR RYŠIŲ TARNYBA

**FORTINET ĮRANGOS TECHNINIO BEI PROGRAMINIO PALAIKymo
PIRKIMO TECHNINĖ SPECIFIKACIJA**

2026 m. gegužės 4 d.
Panevėžys

1. Projekto tikslas

Pakeisti esamus tinklo saugumo įrenginius FortiGate 100E (2 vnt.) naujos kartos įrenginiais, kad palaikytų aukštą patikimumą 2 vnt. (angl. High Availability - HA).

2. Naujos įrangos reikalavimai

2.1. Aparatiniai reikalavimai

| Eil. Nr. | Aprašymas |
|----------|--|
| 1. | Specializuotas vieno gamintojo aparatinis – programinis sprendimas (angl. appliance). |
| 2. | Konstrukcija |
| 2.1. | Konstrukcija: Montuojamas į 19“ komutacinę spintą. Turi būti pateikiamas su visais reikalingais montavimui į 19 colių komutacinę spintą priedais |
| 2.2. | Įrangos elektros maitinimas tiekiamas iš AC 230V 50Hz tinklo. Privalo turėti du maitinimo šaltinius, užtikrinančius nepertraukiamą įrenginio veikimą sugedus vienam iš maitinimo šaltinių. |
| 2.3. | Nemažiau kaip 6 GE RJ-45 Ethernet prievadai. |
| 2.4. | Nemažiau kaip 1 10GE SFP+ Ethernet prievadas. |
| 2.5. | Ne mažiau kaip vienas RJ-45 prievadas įrangos valdymui per komandinę eilutę. |
| 2.6. | Ne mažiau kaip du RJ-45 prievadai įrangos jungimui į aukšto patikimumo sistemą. |

| | |
|-------|--|
| 2.7. | Įranga turi turėti galimybę dirbti Aktyvus/Pasyvus (angl. Active/Passive) ir Aktyvus/Aktyvus (angl. Active/Active) režimais. Sutrikus aktyvaus įrenginio veikimui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį. |
| 3. | Įrangos funkcijos |
| 3.1. | Turi būti ne mažiau kaip 100 IPsec VPN tunelių palaikymas; |
| 3.2. | Turi būti galimybė vienam iš HA įrenginių pakeisti HA statusą (padaryti aktyviu arba pasyviu klasterio elementu); |
| 3.3. | Turi būti galimybė atlikti programinės įrangos atnaujinimą, nesutrikdant ugniasienės, veikiančios HA režimu, duomenų perdavimo; |
| 3.4. | Turi palaikyti IPSec arba lygiaverčių standartų palaikymas; |
| 3.5. | Turi būti ne mažiau kaip 1000 IPsec vidinio tinklo vartotojų skaičius; |
| 3.6. | Turi būti ne mažiau kaip 1 000 000 sesijų vienu metu ir nemažiau kaip 100 000 naujų sesijų per sek. |
| 3.7. | Ugniasienės pralaidumas su IPS saugumo funkcionalumu turi būti ne mažesnis kaip 4 Gbps; |
| 3.8. | Ugniasienės pralaidumas su saugumo funkcionalumu (IPS, Antivirus, malware apsauga) vienu metu turi būti ne mažesnis kaip 2,5 Gbps; |
| 3.9. | Turi būti ne mažiau kaip 1 000 saugumo taisyklių (angl. Security policy); |
| 3.10. | Turi būti galima padalinti į ne mažiau kaip 3 virtualias sistemas (virtualios ugniasienės). Turi būti pateiktos visos reikalingos licencijos; |
| 3.11. | Turi palaikyti ne mažiau kaip 100 000 šifruoto srauto sesijų; |
| 3.12. | DES, 3DES, ir AES256 šifravimas; |
| 3.13. | Turi būti IKE sertifikato palaikymas (X.509); |
| 3.14. | Apsauga nuo DoS tipo atakų. (Turi būti apsauga nuo įsilaužimų, jų aptikimas ir prevencija (TCP Syn Flood, Land, Ping of Death, ir kt.); |
| 3.15. | Apsauga nuo Malware, Spyware ir bandymų įsilaužti ar kitaip išnaudoti sistemą (angl. IPS/IDS) bei Antivirusinė sistema; |
| 3.16. | <p>WEB puslapių kategorizavimas ir valdymas:</p> <ol style="list-style-type: none"> 1. Galimybė administratoriui aprašyti WEB filtravimą pagal URL 2. Turi būti galimybė URL filtravimui ir kategorizavimui pagal pilną URL, t.y. tikrinama URL host ir URI dalys. 3. Kategorizuotų WEB puslapių duomenų bazė 4. Galimybė laikinai suteikti naudotojui prieigą prie uždraustos WEB kategorijos |
| 3.17. | Turi palaikyti SSL šifruoto srauto inspekciją įrenginyje atitinkamai įkeliant reikiamus sertifikatus. |

| | |
|-------|--|
| 3.18. | Turi skenuoti HTTP/ SMTP/ POP3/ IMAP/ FTP ir tikrinti duomenų srautą nuo virusų. |
| 3.19. | Turi blokuoti bylas pagal bylos dydį ir tipą. |
| 3.20. | Turi atpažinti įvairias aplikacijas, įskaitant Youtube, Gmail, Twiter, Facebook, web paštus aplikacijų kontrolės funkcija (atpažinimas, blokavimas (angl. Application Control)). |
| 3.21. | Turi gebėti dirbti kaip DHCP klientas, DHCP serveris ir atlikti IP adreso pririšimus prie MAC; |
| 3.22. | Maršrutizavimas pagal taisykles (angl. Policy-Based Routing) (maršrutizavimas pagal sekančius kriterijus: protokolą, IP adresus, porto numerius); |
| 3.23. | Dinaminis maršrutizavimas (RIP v2, OSPF, BGP) kiekvienoje virtualioje ugniasienėje atskirai; |
| 3.24. | Turi būti srauto ribojimo funkcionalumas DSCP ir (angl. Traffic shaping), nurodant garantuotą bei maksimalų duomenų srauto dydį naudojant saugumo/srauto taisykles; |
| 3.25. | Turi būti įsibrovimų kaupimas ir raportavimas: Prekės laikinojoje atmintyje, SysLog serveryje, pranešimas el. paštu; |
| 3.26. | Įrenginys turi skaidriai nustatyti vartotojų tapatybę (naudojantis Microsoft AD); |
| 3.27. | Saugumo taisyklių kūrimas naudojant vartotojus (USER-ID) bei jų grupes, o ne tik IP adresus; |
| 3.28. | Turi gebėti dirbti skaidriame režime (angl. transparent) ir maršrutizavimo režime (angl. routed) skirtingose virtualiose ugniasienėse vienu metu; |
| 3.29. | Gebėti atlikti taisyklėmis paremtą adresų transliavimą (angl., „policy-based NAT“). |
| 3.30. | Turi būti IEEE 802.1Q VLAN palaikymas. |
| 3.31. | Vartotojų grupių autentifikavimas naudojant: - LDAP, RADIUS arba TACACS+ |
| 3.32. | Automatinis įsilaužimų aprašų (angl. signature) duomenų bazės atnaujinimas; |
| 3.33. | Įrenginys turi būti valdomas per komandinę eilutę ir grafinę sąsają; |
| 3.34. | Turi būti skirtingų lygių administravimo rolės. |
| 3.35. | Vidinis įvykių žurnalas. |
| 3.36. | Įvykių persiuntimas į nutolusį Syslog ar lygiavertį serverį. |
| 3.37. | Turi palaikyti SNMP v2c arba lygiavertį; |
| 3.38. | Turi būti galima stebėti, riboti, blokuoti aplikacijas; |
| 3.39. | Turi būti galimybė sukurti adresų objektų grupę kurioje esantys objektai negalėtų būti naudojami kitose grupėse. |

| | |
|------|---|
| 4. | Garantija |
| 4.1. | <p>Įrenginys turi būti pateikiamas su gamintojo garantija 36 mėnesių (nuo sistemos pateikimo priėmimo-perdavimo akto pasirašymo dienos) ir visom reikalingoms licencijoms šiam periodui. Turi būti gaunami reguliarūs virusų, įsilaužimo aprašai, WEB kategorijos ir jų atnaujinimai. Teikiamas gamintojo palaikymas nemažiau kaip 8x5 formatu.</p> <p>Garantiniu laikotarpiu turi būti teikiamas nemokamas programinės įrangos klaidų šalinimas. Programinės įrangos klaidų šalinimas turi būti vykdomas kaip įmanoma per trumpesnę laiko periodą nuo Pirkėjo pranešimo Pardavėjui išsiuntimo dienos. Turi būti programinės įrangos atnaujinimo galimybė garantiniu laikotarpiu. Programinės įrangos atsisivertinimas iš gamintojo puslapio;</p> |

3. Funkciniai reikalavimai

Nauja sistema turi užtikrinti:

- Pilną esamos konfigūracijos perkėlimą;
- Visi esami sprendimai turi veikti be funkcinių praradimų;
- Leidžiami tik tokie pakeitimai, kurie:
 - pagerina saugumą
 - optimizuoja veikimą

4. Migravimo darbai

4.1. Parengiamieji darbai

- Konfigūracijos įvertinimas
- Migravimo plano parengimas
- Darbų suderinimas su užsakovu

4.2. Diegimas ir migravimas

- Įrangos paruošimas
- Konfigūracijos perkėlimas konvertavus į naują įrenginį
- VPN atkūrimas (pakeitimas į IPsec VPN iš esamo SSL VPN)

4.3. Testavimas (užsakovas atlieka)

- Interneto veikimas
- Vidinių resursų prieiga
- VPN veikimas (perdaryto iš SSL VPN į IPsecVPN)
- Kritinių sistemų testavimas

5. Duomenų pateikimas tiekėjui

Užsakovas įsipareigoja:

- pateikti esamų įrenginių **serijinius numerius**
- prieš migraciją pateikti:
 - konfigūraciją arba
 - sudaryti galimybę su ja susipažinti

6. Priėmimo kriterijai

Projektas laikomas įgyvendintu, kai:

- visi funkcionalumai veikia
- nėra kritinių sutrikimų
- VPN ir tinklo paslaugos stabilios
- užsakovas patvirtina darbų rezultatus

7. Fizinių darbų atsakomybės

Fizinius darbus, susijusius su įrangos montavimu, įrenginių pastatymu bei tinklo kabelių pajungimu, gali atlikti užsakovas.

Tiekėjas privalo:

- pateikti aiškias pajungimo instrukcijas (port mapping, schemas),
- nurodyti techninius reikalavimus pajungimui,
- koordinuoti darbus su užsakovu migracijos metu,
- užtikrinti tinkamą įrangos paruošimą konfigūravimui.