

Saugaus valstybinio duomenų perdavimo tinklo architektūra ir techniniai sprendimai



Projektą remia

Lietuvos Respublika



Projektą iš dalies finansuoja

Europos Sąjunga



INFOSTRUKTŪRA

SVDPT: paskirtis, kūrimo principai

- SVDPT – tai uždaras, saugus Lietuvos valstybės institucijų duomenų perdavimo tinklas, skirtas elektroninių duomenų mainams tarpusavyje ir su ES institucijomis.
- SVDPT kuriamas, vadovaujantis IDA programos principais, suderinimas su ES tinklo TESTA modeliu ir atitinka reikalavimus jungimams prie TESTA.



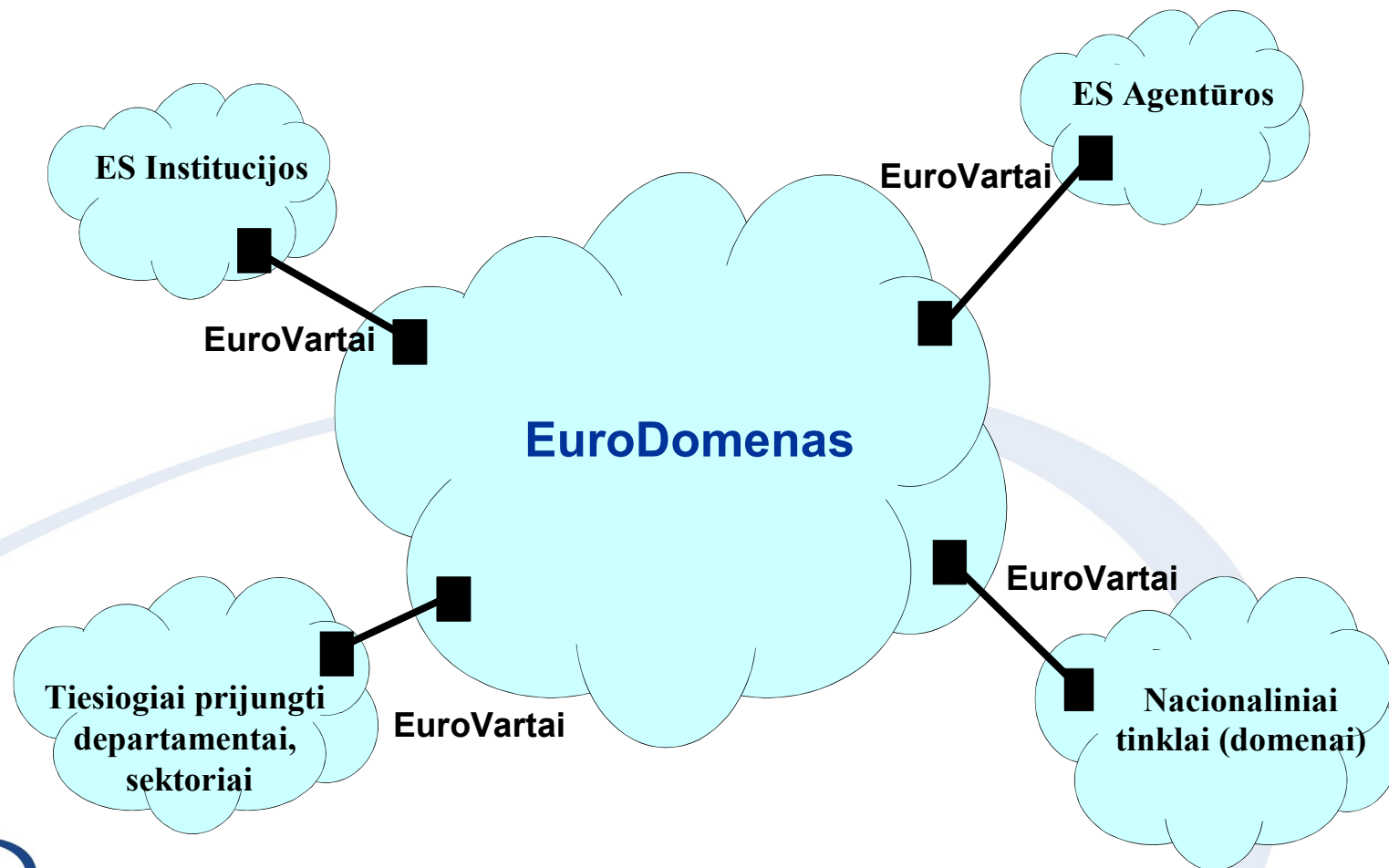
TESTA tinklas

TESTA (**T**rans **E**uropean **S**ervices for **T**elecommunications between **A**ministrations) – Europos Sąjungos administracijų telematikos tinklas, kurio naudojasi visos centrinės ES institucijos ir agentūros ir kuris sujungtas su ES valstybių-narių nacionaliniais tinklais:

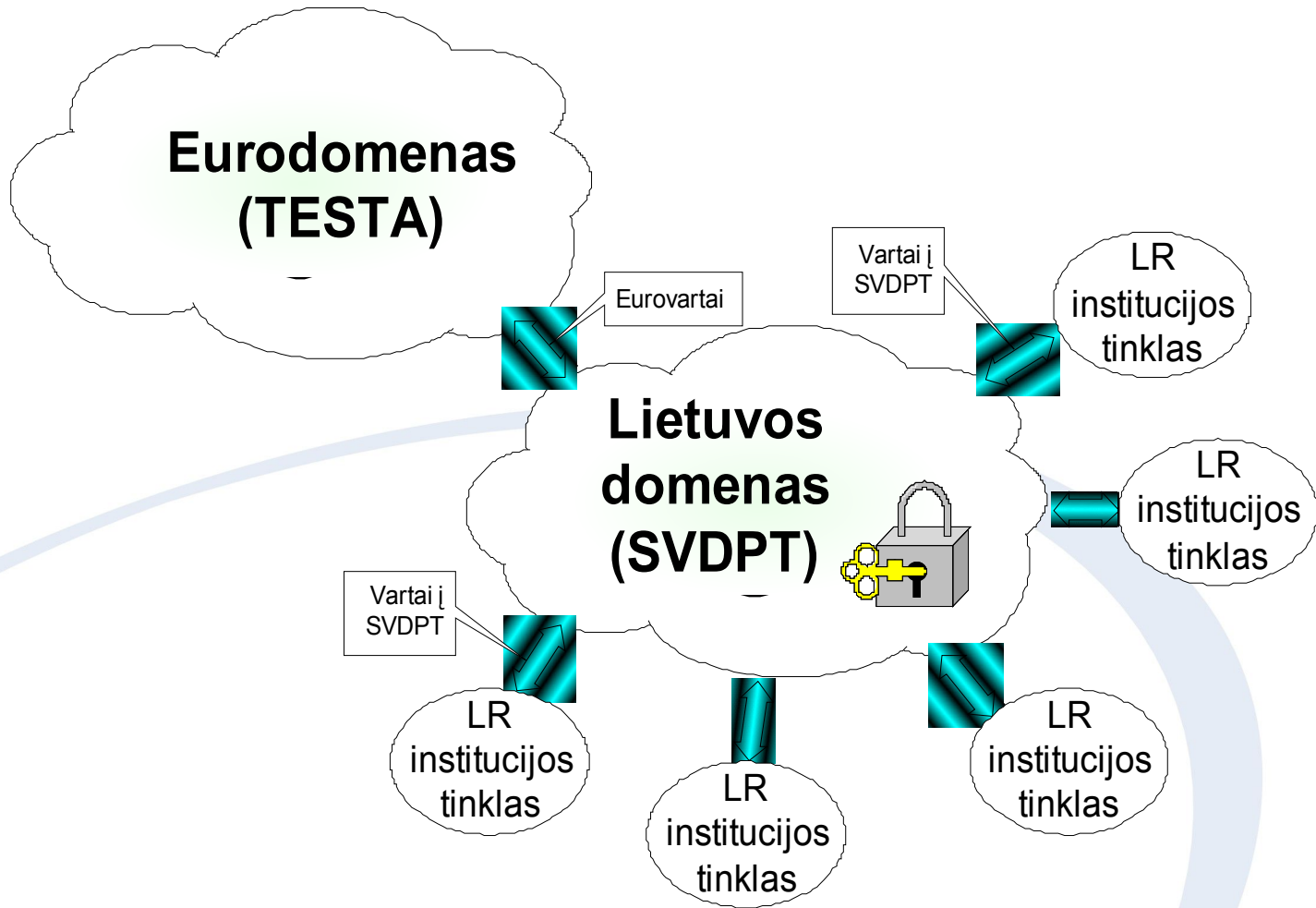
- Atskirtas nuo interneto;
- IP MPLS tinklo technologija;
- Naudojama nemaršrutizuojama internete IP adresų aibė
62.62.0.0 / 17;
- Lietuvos domeniui skirta adresų aibės:
62.62.105.0 / 8, 62.62.104.0 / 8;
- Domenų architektūra – Eurodomenas ir lokalūs domenai;
- Veikia bendrosios tinklo paslaugos – vardų sistema (DNS)
<vardas>.eu-admin.net, uždaras elektroninis paštas, uždaras tinklo portalas;
- Elektroninis parašas uždaroms vartotojų grupėms;
- Veikia informacinių sistemų servisai (pvz TachoNet, EuroDac ir kt.);
- Visi perduodami duomenys šifruojami.



TESTA: domenais besiremianti architektūra



Lietuvos Domenas



SVDPT teisinis pagrindas

2004- 2008 metų Vyriausybės programos priemonių planas, patvirtintas 2005 m. kovo 24 d. LR Vyriausybės nutarimu Nr. 315.

618 PRIEMONĖ: atsakingi vykdytojai - VRM, SM, ŽŪM, IVPK, apskričių viršininkai. Įvykdymo laikas - 2008 m. IV ketvirtis.

Plėtoti saugų valstybės ir savivaldybių institucijų ir įstaigų tinklą, sujungiant visus valstybės registrus ir informacines sistemas, užtikrinant saugų ir efektyvų duomenų teikimą Lietuvos Respublikos valstybės institucijoms bei įsijungimą į Europos Sąjungos ir šalių narių administracijų duomenų mainų tarp administracijų programos (IDA) telekomunikacijų tinklus, tame tarpe integruoti apskričių viršininkų administracijų, savivaldybių bei seniūnijų informacines sistemas į Saugų valstybinį duomenų perdavimo tinklą, užtikrinant perduodamų asmens duomenų saugumą.



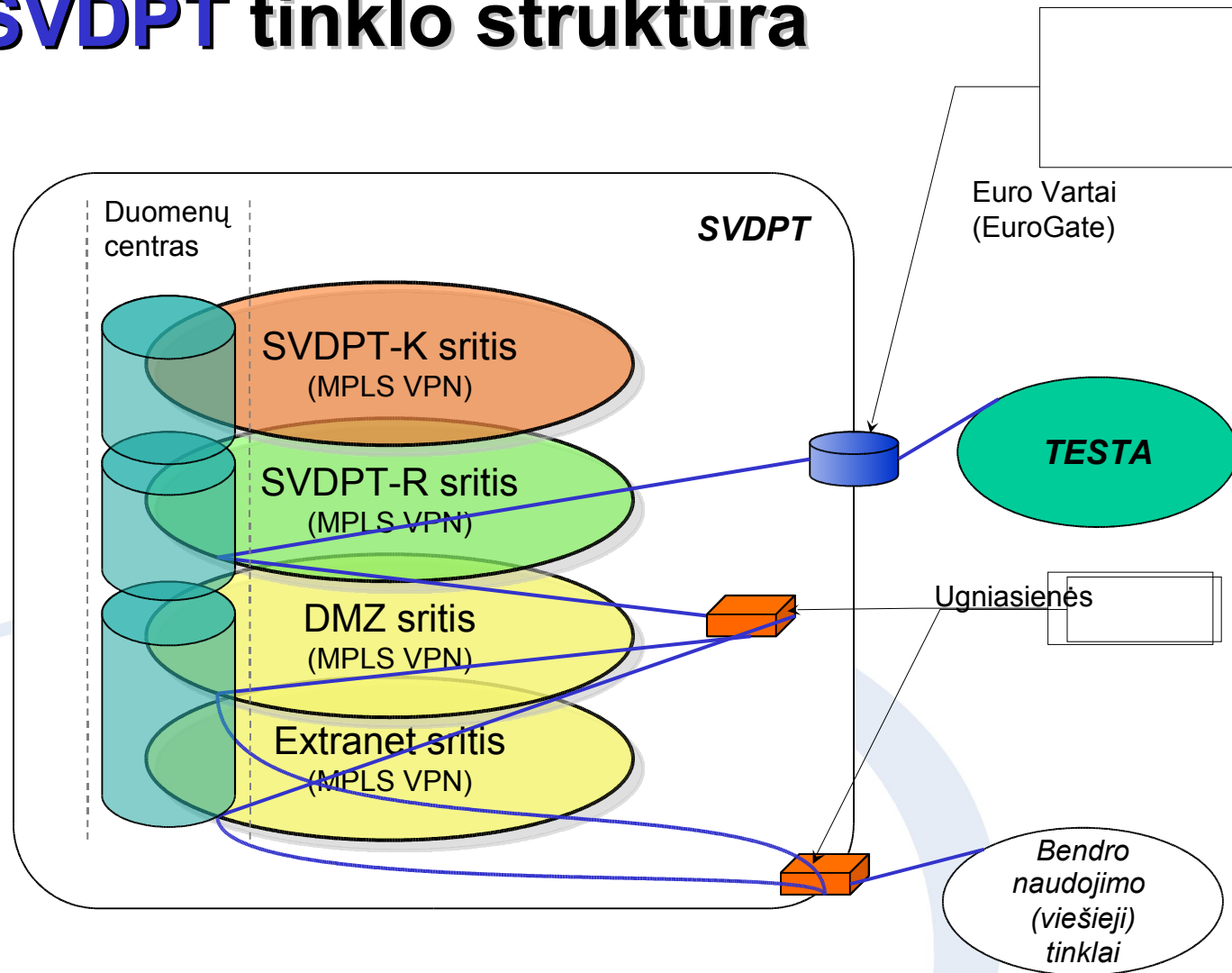
SVDPT (TESTA-Lietuva)

- Saugus valstybinis duomenų perdavimo tinklas kuriamas pagal TESTA tinklo principus:
 - Tinklo pagrindas - IP MPLS tinklas;
 - Uždara adresacijos schema;
 - Atskirtas nuo interneto;
 - visi perduodami SVDPT tinklu duomenys yra šifruojami;
 - Laikomasi domenu architektūros;
 - Veikia atskirtos nuo interneto bendrosios tinklo paslaugos – vardų sistema (DNS), uždaras elektroninis paštas, uždaras tinklo portalas, informacinių sistemų servisai (pvz Linessis, VBAMS ir kt.).



SVDPT tinklo struktūra

- ✓ Atitinka reikalavimus **konfidencialiai** informacijai perduoti
- ✓ Atitinka reikalavimus **riboto naudojimo** informacijai perduoti
- Apsaugota sritis ryšiui su viešaisiais tinklais
- Apsaugota sritis ryšiui su juridiniais asmenimis

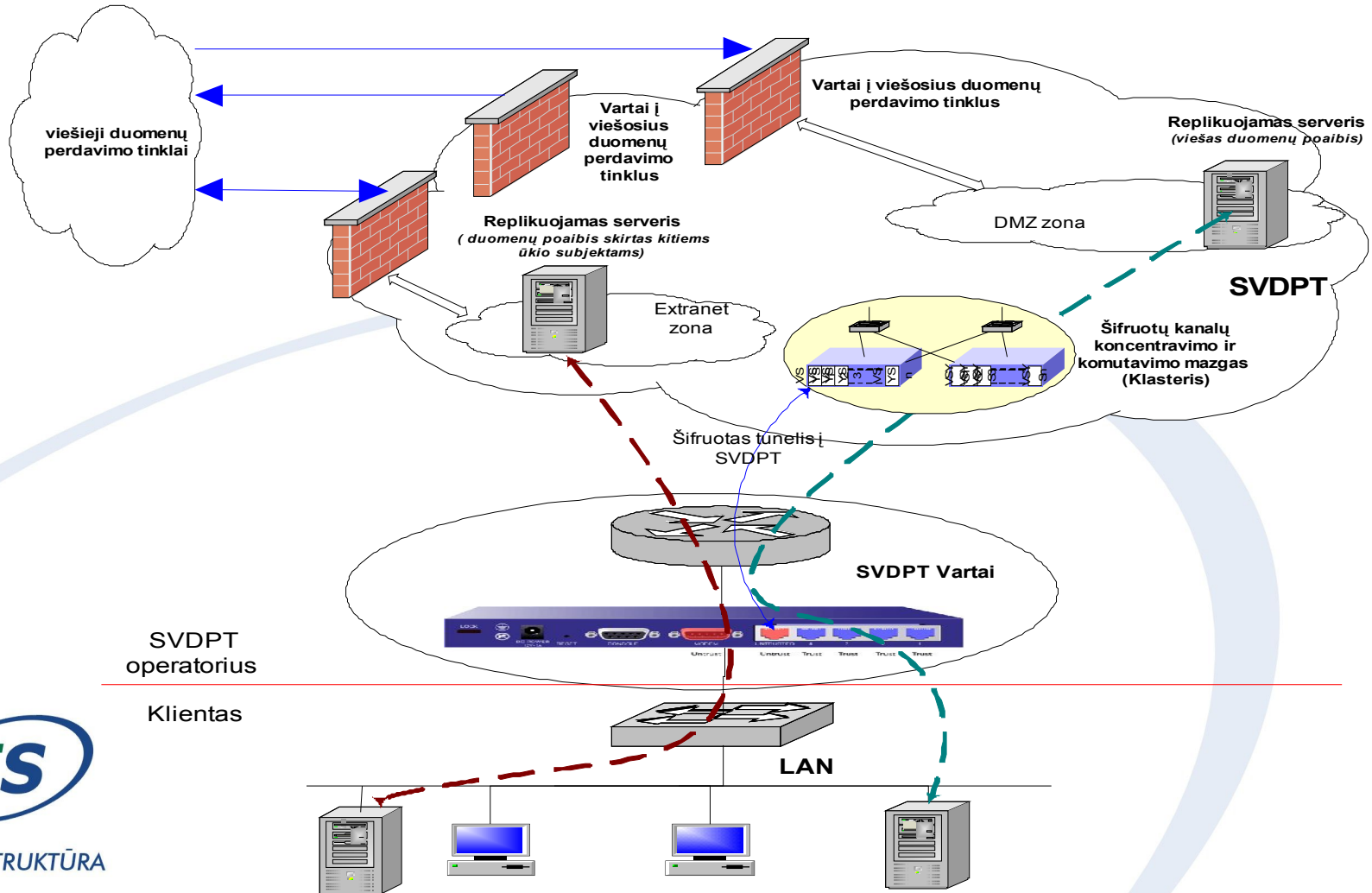


- SVDPT – K ir SVDPT R srityse pagal poreikį sukuriama keletas IPsec VPN zonų
- SVDPT gali būti sukurtos specialios zonos ir sritys žinybiniais institucijų tinklams

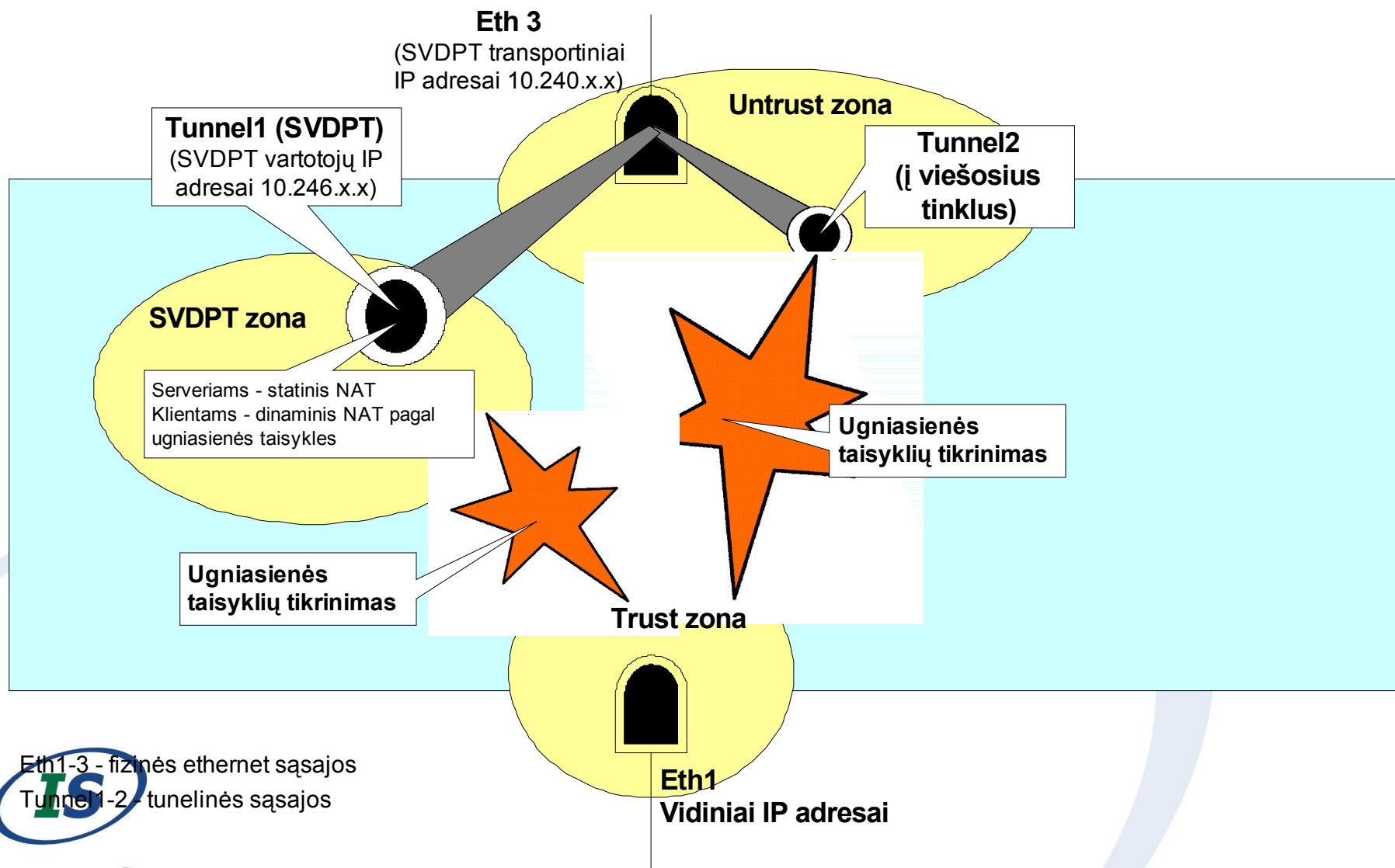


Prijungimo prie SVDPT schema

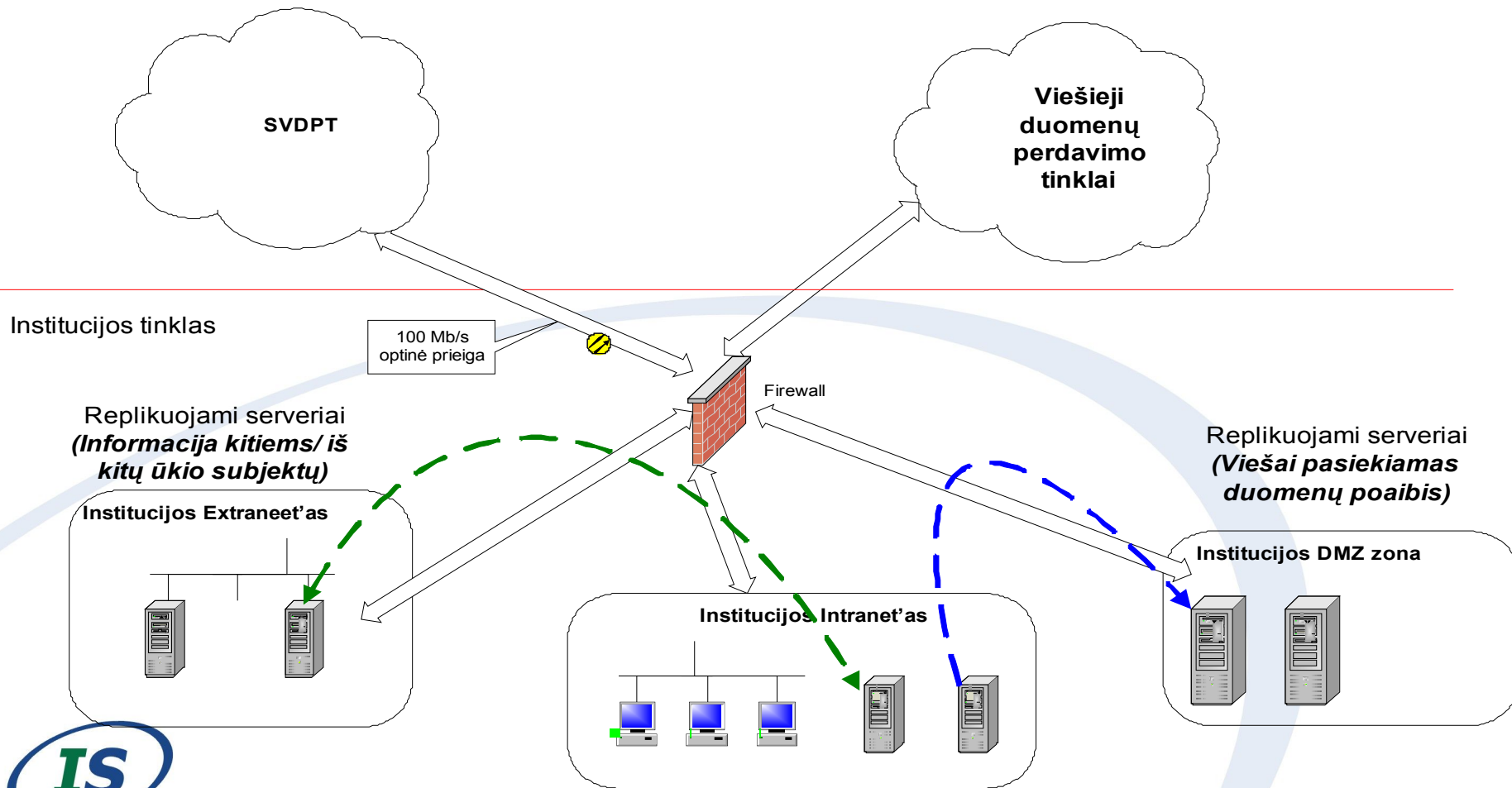
- Pagrindinis prijungimo prie SVDPT saugumo lygis.
- Teikiamos visos pagrindinės SVDPT paslaugos.



SVDPT vartų loginė schema



Institucijos tipiniai saugumo sprendimai



JAV nacionalinio standartizavimo institucijos parengtoje rekomendacijoje dėl informacinių sistemų saugumo principų (*“Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”*, *NIST Special Publication 800-27 Rev A*) kuriant ir eksploatuojant viešojo sektoriaus informacines sistemas siūloma:

- Izoliuoti viešai pasiekiamas sistemas nuo kritiškų veiklai resursų (duomenų bazių, programų ir procesų) [20-tas principas]. Tuo tikslu tinkluose naudojamos demilitarizuotos zonos (DMZ) ir kiti apsaugoti potinkliai (tinklo segmentai).
- Naudoti informacinių sistemų ir kompiuterinių tinklų išteklių skaidymą zonomis pagal tvarkomos informacijos pobūdį [21-as principas]. Duomenų mainai tarp zonų vykdomi per gerai kontroliuojamus taškus.
- Saugumo priemonės turi tenkinti daug persidengiančių informacinių domenų [31-as principas]. Informacinis domenas apima asmenis, procesus ir sistemas atliekančius tam tikrą veiklą. Efektyvi ir ekonomiška saugumo sistema turi leisti taikyti saugumo reglamentą (reglamentus) ne vienam, bet keliems informaciniams domenams, nekuriant atskiros fizinės infrastruktūros kiekvienam domeniui.



- SVDPT infrastruktūra yra sukurta tenkinti daugelio informacinių sistemų poreikius, taikant skirtingus tinklo saugumo reglamentus skirtingoms sistemoms.
- SVDPT tinkle skirtingus informacinius resursus galima talpinti skirtinguose segmentuose (zonose). Šiuo metu SVDPT apibrėžtos bendro naudojimo zonos tarpinstituciniams ryšiams, ryšiams su įmonėmis (“ekstranetas”) ir demilitarizuota zona ryšiui su viešais tinklais.
- Ryšiai tarp informacinių domenų (LR institucijų informacinių sistemų, įmonių informacinių sistemų ir paslaugų teikimo piliečiams ir įmonėms) vyksta per kontroliuojamus “vartus”. Ryšys su ES “TESTA” tinklu taip pat vyksta per “TESTA” tinklo vartus.
- SVDPT yra sukurtas ir vystomas pagal pripažintus šiuolaikinius duomenų perdavimo saugos principus ir atsižvelgiant į informacinių sistemų saugos užtikrinimo tendencijas.

