KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Mindaugas Mikučionis

Korporatyvinės įmonės informacinės saugos sistemos modeliavimas

Magistro darbas

Vadovas
doc. dr. A. Venčkauskas

KAUNAS, 2005

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
prof. E. Kazanavičius
2005-05-

Korporatyvinės įmonės informacinės saugos sistemos modeliavimas

Informatikos mokslo magistro baigiamasis darbas

Kalbos konsultantė
Lietuvių kalbos katedros lektorė
dr. J. Mikelionienė
2005-05-

Vadovas
doc. dr. A. Venčkauskas
2005-05-

Recenzentas
doc. dr. R. Butleris
2005-05-

Atliko
IFM 9/1 gr. stud.
M. Mikučionis
2005-05-

KAUNAS, 2005

SUMMARY

The purpose of this work is to create and analyze the information security models of large corporations. It's difficult and hard to deploy efficiently safe systems due to complex network environment and enterprise computer systems. It's important to analyze security system parameters before design process. The enterprise information security system modeling helps us to solve these problems. In this work I designed information security models with complex information security elements and safe data transferring between remote locations. These models will help designers to compare different systems and to find the most secure and effective. This thesis generalizes the information security modeling process and describes the factors influencing it.

TURINYS

ĮVADAS 8

1. BENDROJI DALIS 9

1.1. KORPORATYVINĖS ĮMONĖS KOMPIUTERINIS TINKLAS 9

1.1.1. Vietiniai tinklai 10

1.1.2. Globalieji tinklai 10

1.2. TINKLŲ ARCHITEKTŪROS ELEMENTAI 11

1.3. NUTOLUSIŲ VIETINIŲ TINKLŲ SUJUNGIMO ARCHITEKTŪROS 12

1.3.1. Skirtinės linijos 13

1.3.2. FR ir ATM 14

1.3.3. VPN 15

1.4. TINKLO SAUGOS ELEMENTAI 16

1.4.1. Antivirusinės sistemos 16

1.4.2. Ugniasienės 17

1.4.3. Tinko atakų aptikimo sistemos 18

1.4.4. VPN įrenginiai 18

1.5. KORPORATYVINĖS ĮMONĖS SAUGAUS TINKLO ARCHITEKTŪRA 19

1.5.1. Duomenų persiuntimo tarp įmonės nutolusių taškų saugumas 20

1.5.2. Tinklo perimetro saugumas 21

1.5.3. Vidinio tinklo saugumas 22

1.5.4. Vartotojo darbo vietos saugumas 22

1.6. INFORMACINĖS SAUGOS MODELIAVIMAS 23

1.6.1. Atakų grafo modelis 24

1.6.2. Markovo procesų modelis 27

1.6.3. Imitacinis GPSS modelis 30

2. TIRIAMOJI DALIS 33

2.1. ATAKŲ GRAFO MODELIS 33

2.2. MARKOVO PROCESŲ MODELIS 37

2.3. IMITACINIS GPSS MODELIS 40

2.3.1. Trust-Untrust architektūros modelis 41

2.3.2. Modeliavimo rezultatai 45

2.3.3. Trust-Untrust-Dmz architektūra 50

2.3.4. Modeliavimo rezultatai 53

IŠVADOS 60

LITERATŪRA 61

1 PRIEDAS. TRUST-UNTRUST ARCHITEKTŪROS APRAŠAS GPSS KALBA IR MODELIAVIMO REZULTATAI 63

2 PRIEDAS. TRUST-UNTRUST-DMZ ARCHITEKTŪROS APRAŠAS GPSS KALBA IR MODELIAVIMO REZULTATAI 69

3 PRIEDAS. STRAIPSNIS 75

Lentelių sąrašas

1.1 lentelė. Atakų medžio komponentai 25
2.1 lentelė. Pažeidžiamumų duomenys 34
2.2 lentelė. Pažeidžiami servisai 34
2.3 lentelė. Ryšių duomenys 35
2.4 lentelė. IDS duomenys 35
2.6 lentelė. Trust-Untrust ugniasienės taisyklės 42
2.7 lentelė. Trust-Untrust-Dmz ugniasienės taisyklės 51

Paveikslėlių sąrašas

1.1 pav. Skirtinės linijos 13
1.2 pav. FR ir ATM 14
1.3 pav. VPN 15
1.4 pav. Panda GateDefender įrenginys 16
1.5 pav. Ugniasinenė 17
1.6 pav. Tinklo skaidymas saugumo zonomis 18
1.7 pav. VPN įrenginiai 19
1.8 pav. Saugaus tinklo architektūra 20
1.9 pav. VPN loginė schema 21
1.10 pav. Korporatyvinės įmonės saugaus tinklo architektūra 23
1.11 pav. Atakų medžių projektavimas 25
1.12 pav. Tinklų sujungimo architektūra 27
1.13 pav. Būsenų grafas 29
1.14 pav. Laiko diagrama 30
1.15 pav. Imitacinis modelis 31
2.1 pav. Tinklo modelis 33
2.2 pav. Atakų grafas 37
2.3 pav. Tinklo architektūros pavyzdys 37
2.4 pav. Markovo modelio grafas 39
2.5 pav. Grafo fragmentas 40
2.6 pav. Trust-Untrust architektūra 41
2.7 pav. Trust-Untrust architektūros GPSS modelis 44

2.8 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms) 45
2.9 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms) 46
2.10 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms) 46
2.11 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje 47
2.12 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms) 48
2.13 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms) 48
2.14 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms) 49
2.15 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje 49
2.16 pav. Trust-Untrust-DMZ architektūra 50
2.17 pav. Trust-Untrust-DMZ architektūros GPSS modelis 53
2.18 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms) 54
2.19 pav. Paketo patikrinimo laiko pasiskirstymas VPN modulyje (ms) 55
2.20 pav. Paketo kodavimo laiko pasiskirstymas IDS modulyje (ms) 55
2.21 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje 56
2.22 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms) 57
2.23 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms) 57
2.24 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms) 58
2.25 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje 58
2.26 pav. Paketų eilių antiviruso modulyje palyginimas 59

ĮVADAS

Korporatyvinių įmonių kompiuterinių sistemų informacinės saugos užtikrinimas yra viena iš svarbiausių informacinių technologijų problemų. Augant ir plečiantis verslui iškyla nutolusių įmonės padalinių, partnerių, darbuotojų saugaus pasikeitimo duomenimis ir lokalių tinklų saugumo problema. Nuolatos auga informacinių technologijų vaidmuo verslo ir valdymo procesuose, didėja informacinių procesų sudėtingumas. Dėl šių priežasčių informacinės saugos pažeidimų kaina kompiuterinėse sistemose nuolatos auga.

Atsižvelgiant į informacinės saugos priemonių patikimumo ir našumo kriterijus, būtina šių sistemų veikimą ištirti prieš diegiant. Adekvačių sprendimų, užtikrinančių priimtiną informacinę saugą už atitinkamą kainą, priėmimas tampa vis sudėtingesniu uždaviniu. Korporatyvinės įmonės informacinės saugos modeliai leidžia išspręsti šias problemas bei gali būti taikomi informacinės saugos sistemoms projektuoti, parametrams parinkti ir diegti. Šiame darbe bus sudaromi ir nagrinėjami korporatyvinių įmonių informacinės saugos sistemų modeliai, aprašantys įvairias saugaus duomenų pasikeitimo ir informacinės saugos grėsmių neutralizavimo priemonių architektūras. Informacinės saugos realizavimo priemonės bus įvertintos atitinkamais parametrais. Modeliai leis palyginti įvairias informacinės saugos realizavimo architektūras ir parinkti efektyviausią.

1. BENDROJI DALIS

1.1. Korporatyvinės įmonės kompiuterinis tinklas

Kompiuterinis tinklas - tai tarpusavyje sujungtų autonominių kompiuterių rinkinys. Kompiuteriniai tinklai yra vienas iš svarbiausių faktorių, lemiančių įmonės darbo našumą. Visų kompiuterinių tinklų nepriklausomai nuo to, kokie sudėtingi jie būtų ir kaip jie skirtųsi nuo šitos paprastos sistemos, visų jų tikslas yra dalintis ir keistis informacija. Ši paprasta sistema pastūmėjo kurti laidais sujungtas kompiuterines sistemas. Kompiuteriniai tinklai padeda išvengti sudėtingo informacijos apsikeitimo tarp skirtingų verslo elementų.

Kompiuteriniai tinklai yra vienas iš svarbiausių faktorių, lemiančių įmonės darbo našumą. Pagrindinės priežastys dėl kurių sparčiai plinta kompiuteriniai tinklai [1]:

- Bendras resursų naudojimas. Toli vienas nuo kito esantys kompanijos kompiuteriai sujungti į tinklą. Informacija nuo vartotojo gali būti labai toli. Ją gali naudoti daug darbuotojų tuo pačiu metu.
- Didelis patikimumas. Duomenys turi po keletą kopijų skirtinguose kompiuteriuose. Kai vienas sugenda, galima naudotis kitais, neprarandant duomenų.
- Pinigų taupymas. Vienas didelis kompiuteris yra brangesnis už daug mažų, sujungtų į tinklą ir atliekančių tą patį darbą. Duomenys saugomi viename arba keliuose bendro naudojimo serveriuose.
- Galimybė nesunkiai plėsti tinklą, prijungiant naujus vartotojus ir naujus serverius pagal poreikius.
- Galinga toli esančių darbuotojų bendravimo priemonė, atliekant bendrą darbą.

Tinklai klasifikuojami pagal du svarbius požymiai:

- perdavimo technologija;
- dydis.

Pagal perdavimo technologiją tinklai skirstomi į du tipus:

- Transliacinio tipo tinklai;
- Taškas-taškas tipo tinklai.

Transliaciniai tinklai turi vieną ryšio kanalą, kurį bendrai naudoja visi tinklo kompiuteriai. Kai kurios sistemos palaiko perdavimą tik tam tikram kompiuterių poaibiui.

Taškas–taškas tinklai sudaryti iš daugelio sujungimų tarp individualių kompiuterių porų. Paketai pasiekia adresatą per keletą tarpinių stočių. Kadangi paketui yra skirtingo

ilgio keliai, tai reikalingi maršrutizacijos algoritmai, kurie yra labai svarbūs taškas - taškas tinkluose. Dažniausiai maži, geografiškai lokalizuoti tinklai yra transliaciniai, o dideli – taškas - taškas tipo.

Keleto tinklų sujungimas yra vadinamas tarptinkliniu. Atstumas labai svarbus klasifikacinis požymis, kadangi yra naudojama skirtinga technika tinklams realizuoti.

1.1.1. Vietiniai tinklai

Vietiniai tinklai dažniausiai įrengiami viename pastate. Ilgis – iki kelių kilometrų [3]. Plačiai naudojami asmeniniams kompiuteriams ir darbo stotims sujungti kompanijų, įstaigų kontorose bendram resursų naudojimui ir apsikeitimui informacija. Skiriasi nuo kitų tinklų dydžiu, perdavimo technologija, topologija.

Vietiniai tinklai riboto dydžio. Perdavimo laikas yra ribotas ir žinomas. Tai leidžia panaudoti tam tikrus metodus, kurie negalimi kitomis sąlygomis. Dažnai naudojamas vienas kabelis, prie kurio prijungti visi kompiuteriai.

Duomenų perdavimo sparta 10 - 1000 Mbps, mažas vėlinimas (dešimtys μs), nedaug klaidų. Tuo pačiu metu duomenis gali siųsti tik vienas kompiuteris. Reikalingas tam tikras konfliktus sprendžiantis mechanizmas, kai tuo pačiu metu duomenis nori siųsti keletas kompiuterių. Mechanizmas centralizuotas arba paskirstytas.

1.1.2. Globalieji tinklai

WAN užima didelę teritoriją (šalis, žemynas). Daugumoje WAN potinkliai susideda iš dviejų skirtingų komponenčių – perdavimo linijų ir komutacinių elementų. Komutaciniai elementai yra specializuoti kompiuteriai, naudojami sujungti keletą linijų. Jie vadinami: paketų komutacijos mazgai, tarpinės sistemos, maršrutizatoriai [2].

Kai paketas yra persiunčiamas iš vieno maršrutizatoriaus į kitą, jis gali praeiti per daugelį tarpinių maršrutizatorių. Kiekviename iš jų paketas priimamas ir saugomas, kol atsilaisvina reikalingas išėjimas. Potinklis, naudojantis šį principą, yra vadinamas taškas-taškas, išsaugoti ir persiųsti arba potinklis su paketų komutacija. Beveik visi WAN (išskyrus palydovinius) turi tokius potinklius. Kai paketai yra maži ir fiksuoto dydžio, jie dažnai vadinami ląstelėmis. Yra įvairios taškas-taškas potinklių organizavimo topologijos. Vietiniai tinklai paprastai turi simetrinę topologiją. Globalieji tinklai dažniausiai yra nereguliarios topologijos.

Dar yra palydoviniai tinklai ir antžeminės radijo sistemos. Kiekvienas maršrutizatorius turi anteną, per kurią priima ir perduoda. Visi arba tik kai kurie maršrutizatoriai gali priimti signalą iš palydovo.

1.2. Tinklų architektūros elementai

Tarptinkliniai ryšiai gali būti tokių tipų: LAN - LAN, LAN - WAN, WAN - WAN, LAN - WAN - LAN. Jiems realizuoti naudojami įrenginiai [4]:

- kartotuvai;
- tiltai (kanalinio lygio kadrų perdavimas tarp LAN);
- daugiaprotokoliai maršrutizatoriai.

Kartotuvas buvo sukurtas tam, kad būtų galima toliau perdavinėti signalą. Kartotuvas yra pats pigiausias būdas išplėsti kompiuterinį tinklą. Kartotuvas regeneruoja kompiuterinio tinklo signalą ir persiunčia jį toliau į kitą segmentą. Tiek vienas segmentas, tiek kitas segmentas turi naudoti tuos pačius protokolus, nes kartotuvas negali komunikuoti segmentų kur yra skirtingi protokolai. Kartotuvai gali jungti du skirtingus kabelių tipus, pavyzdžiui koaksialinį kabelį su optiniu kabeliu.

Tiltas, kaip ir kartotuvas, jungia du kompiuterinio tinklo segmentus. Tačiau tiltas be kartotuvo funkcijų atlieka ir izoliavimo funkciją. Tai yra tiltas gali izoliuoti duomenų judėjimą tarp dviejų tinklo segmentų. Tiltas gali būti naudojamas:

- išplėsti atstumą tarp tinklo segmentų ;
- pasiruošti kompiuterinio tinklo augimui;
- sumažinti duomenų susidūrimų ir nusimušimų tikimybę;
- sujungti skirtingus kabelius;
- sujungti skirtingų topologijų segmentus.

Kompiuteriniuose tinkluose, kur naudojami keli kompiuterinių tinklų segmentai su skirtingais protokolais ir architektūromis kartotuvas ir tiltas negalės sujungti tokių segmentų. Didesniems ir sudėtingesniems kompiuteriniams tinklams neužtenka žinoti kompiuterio adreso, reikia nustatyti ir geriausią kelią duomenų siuntimui. Duomenys siunčiami iš vieno segmento į kitą gali pereiti daug segmentų, kurie gali būti labai apkrauti ir todėl reikia rasti kelią kaip perduoti juos greičiau. Įrenginys atliekantis šią funkciją vadinamas maršrutizatorius. Maršrutizatorius gali perjunginėti ir maršrutizuoti paketus skirtinguose kompiuteriniuose tinkluose. Maršrutizatorius kaip ir tiltas gali filtruoti ir

izoliuoti duomenų judėjimą, sujungti skirtingus kompiuterinių tinklų segmentus. Maršrutizatoriai naudojami sudėtingesnėse sistemose todėl, kad jie užtikrina geresnį duomenų perdavimą ir nepraleidžia trukdžių. Maršrutizatoriai gali tarpusavyje dalintis informacija ir taip išvengti labiau apkrautų segmentų.

1.3. Nutolusių vietinių tinklų sujungimo architektūros

Augant ir plečiantis verslui iškyla įmonės padalinių, partnerių, nutolusių darbuotojų saugaus apsikeitimo duomenimis problema. Korporatyvinei įmonei yra nesvarbu kurioje geografinėje vietovėje yra atliekamas darbas. Svarbu kaip operatyviai apsikeisti informacija. Reikalingi atitinkami sprendimai saugiai sujungti šiuos korporatyvinės įmonės elementus:

- padalinius;
- verslo partnerius;
- klientus;
- nutolusius darbuotojus.

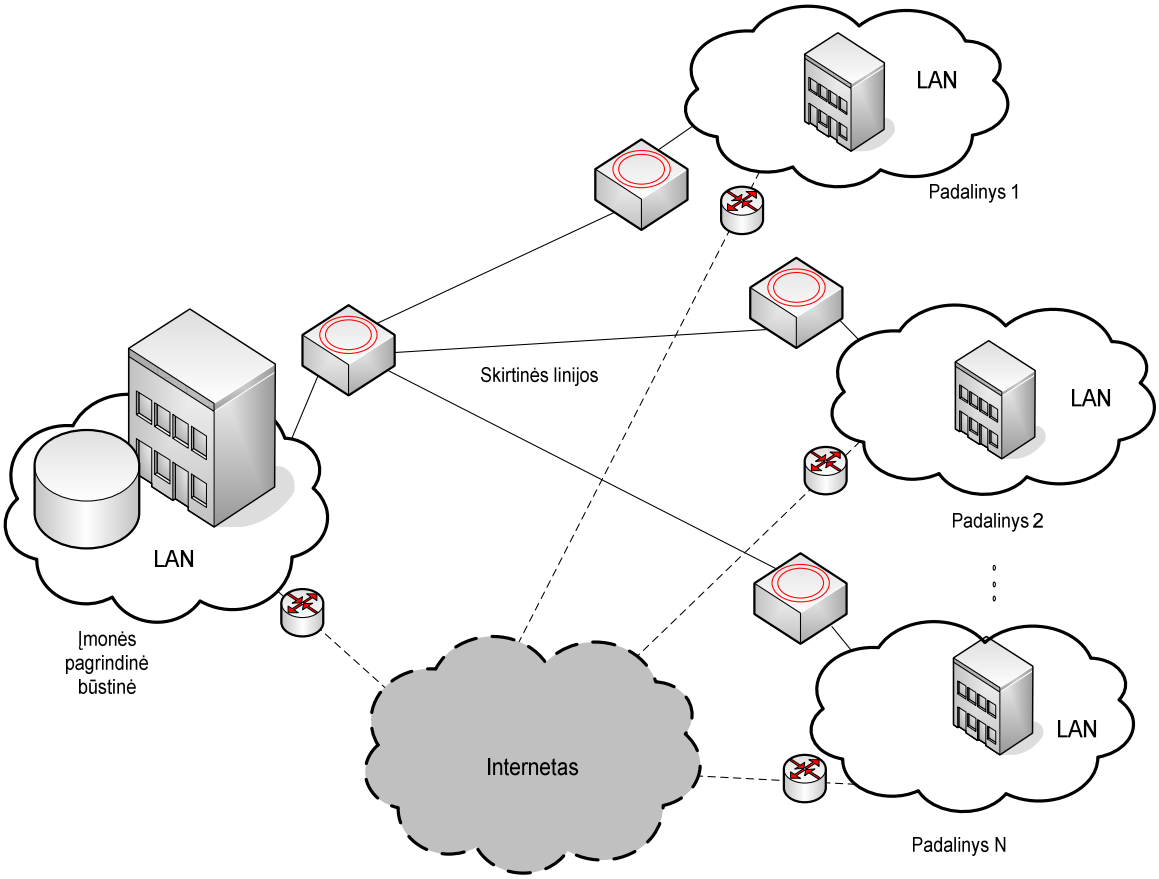
Kad pasiekti šiuos tikslus yra naudojamos įvairios tinklinės technologijos. Mažoms įmonėms svarbu nebrangaus ryšio užtikrinimas. Didelėms įmonėms reikia užtikrinti sudėtingą, įvairialypį, saugų tinklų sujungimą, užšifruojant informaciją ir kontroliuojant priėjimą prie jos.

Yra naudojamos įvairios architektūros korporatyvinės įmonės struktūrinių elementų sujungimui. Norint panagrinėti ir palyginti atskiras tinklo architektūras reikia apibrėžti kriterijus, kuriais remiantis jas vertinsime. Pagrindiniai kriterijai yra šie:

- saugumas;
- greitaveika;
- patikimumas;
- kaina.

Šie pagrindiniai kriterijai suformuoti remiantis tinklinių technologijų analize.

1.3.1. Skirtinės linijos



1.1 pav. Skirtinės linijos

Vienas iš seniausių ir saugiausių nutolusių filialų jungimo būdų yra skirtinėmis linijomis [5]. Du taškai yra sujungiami pastovaus pralaidumo fiksuota linija. T1 tipo kanalas palaiko 1.5Mbps linijos greitaveiką. Šia architektūra dažniausiai jungiami du geografiškai nutolę taškai. Taip pat gali būti naudojamos optinės linijos, ISDN. Išlaikyti tokį tinklą su skirtinėmis linijomis yra pakankamai brangu net ir didelėms kompanijoms.

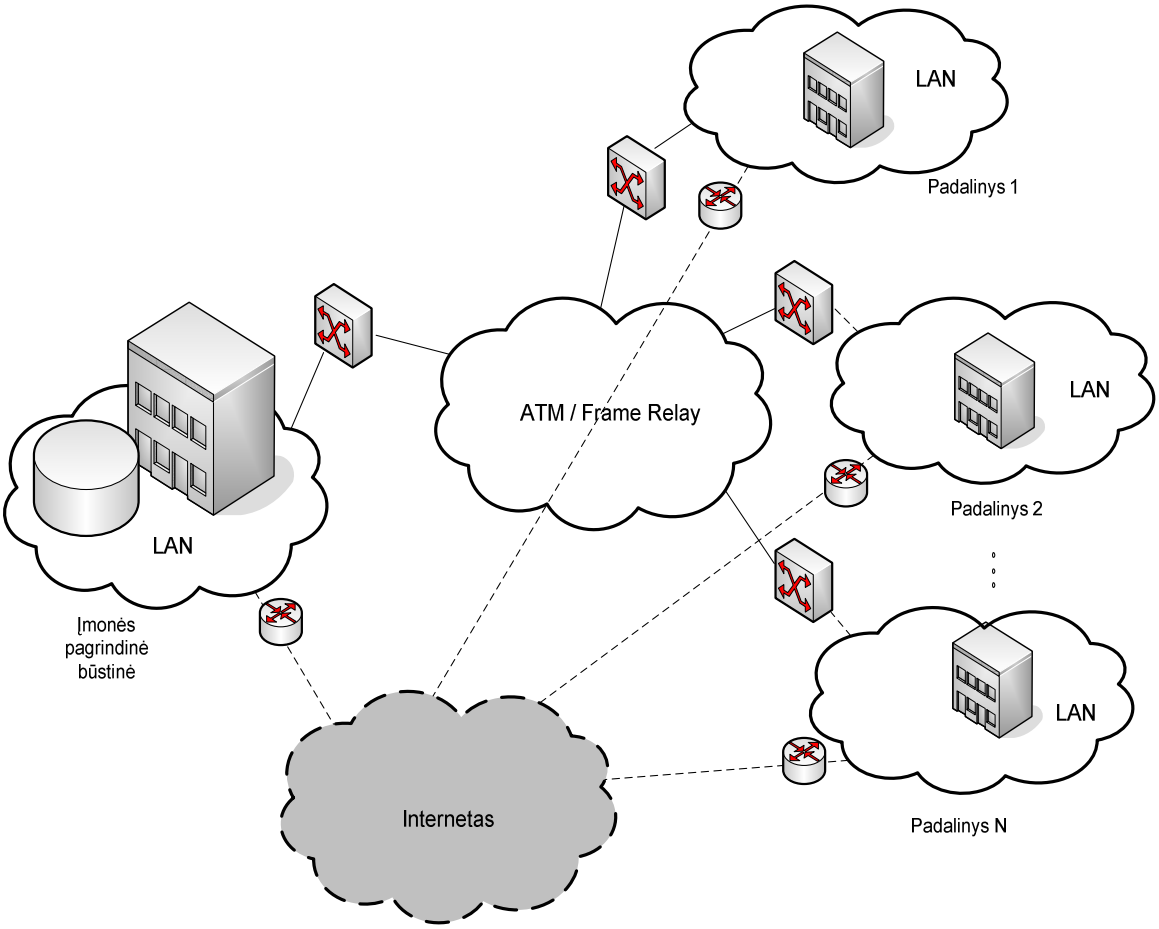
Skirtinių linijų privalumai:

- garantuotas saugumas (privačios linijos);
- užtikrinamas pastovus duomenų pralaidumas.

Skirtinių linijų trūkumai:

- didelė kaina;
- sudėtinga tinklo topologija;
- neįmanoma prijungti nutolusių vartotojų.

1.3.2. FR ir ATM



1.2 pav. FR ir ATM

FR ir ATM buvo sukurti, kad padidinti tinklų pralaidumą ir garantuoti ryšio kokybę [6]. Jie gali sujungti skirtingų tipų tinklus ir turi daug privalumų.

FR ir ATM privalumai:

- garantuoja informacijos perdavimą minimalia (nuo 200 bps iki 34 Mbps ir daugiau), su vartotoju suderinta perdavimo sparta (CIR);
- garantuotas saugumas (virtualūs kanalai).

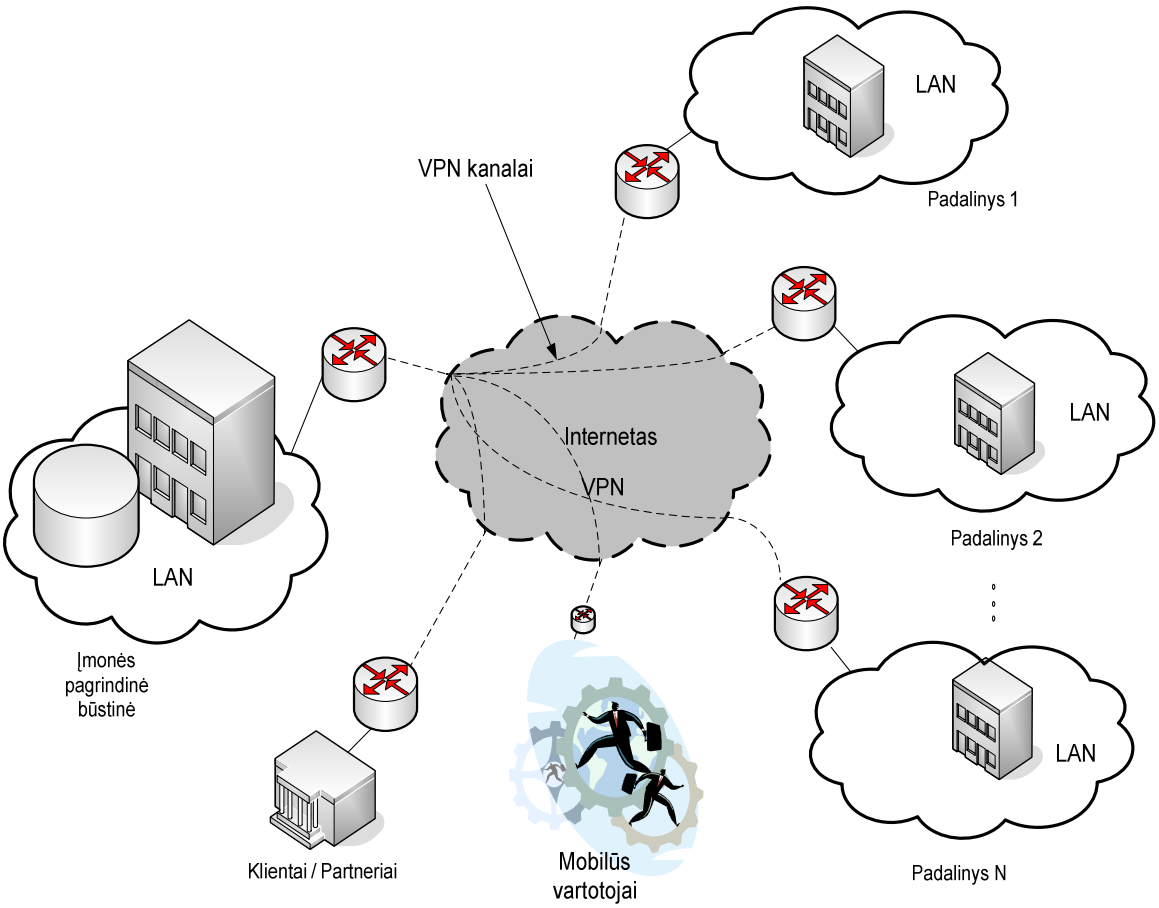
FR ir ATM trūkumai:

- nėra informacijos perdavimo prioritetų;
- didelė kaina;
- sudėtinga tinklo topologija;
- neįmanoma prijungti nutolusių vartotojų.

ATM tinklas yra transportinis tinklas. Jis kuriamas ATM komutatorių ir SDH transportinių sistemų pagrindu. Komutatoriai tarpusavyje jungiami per tinklo mazgo (NNI) sąsają. Mažos spartos terminalai į tinklą tiesiogiai nejungiami. Jie jungiami per prieigos

įrenginius (PBX, maršrutizatoriai). Yra galimybė tiesiogiai įjungti personalinį kompiuterį į ATM tinklą panaudojant adapterį.Minimali informacijos perdavimo sparta sąsajoje vartotojas-tinklas (UNI) 1,5 Mbps. Dabartiniu metu yra specifikuota UNI sparta iki 2,5 Gbps.

1.3.3. VPN



1.3 pav. VPN

VPN yra tinklas jungiantis korporatyvinės įmonės struktūrinius elementus panaudojant viešą interneto tinklą [7]. Čia nėra naudojamos saugios skirtinės linijos, todėl keliaujanti informacija turi būti koduojama. Viešame interneto tinkle sukuriami koduoti informacijos tuneliai tarp geografiškai išsibarsčiusių taškų.

VPN privalumai:

- saugus nutolusių vartotojų, filialų, klientų sujungimas;
- maža kaina (80% mažesnė nei skirtinių linijų);
- nesudėtinga tinklo topologija.

VPN trūkumai:

- greitaveikos sumažėjimas dėl informacijos kodavimo;
- neužtikrinamas duomenų srauto pastovus greitis.

Šiuo metu korporatyvinėms įmonėms sujungti dažniausiai naudojama VPN architektūra. Ji tapo populiari dėl palyginti nedidelės kainos, interneto tinklo plėtros, nesudėtingo valdymo ir lankstumo. Šiame darbe bus nagrinėjama VPN tinklo architektūra. Sudarant modeliu bus vertinami pagrindiniai VPN ir saugos priemonių kiekybiniai parametrai.

1.4. Tinklo saugos elementai

Kiekviena korporatyvinė įmonė prijungdama savo tinklus prie interneto susiduria su grėsmėmis. Šių grėsmių neutralizavimui yra naudojamos atitinkamos informacinės saugos priemonės.

1.4.1. Antivirusinės sistemos

Viena didžiausių grėsmių informacijos saugumui kyla dėl kompiuterių virusų. Virusų aptikimui ir neutralizavimui naudojamos antivirusinės priemonės. Turi būti naudojama kelių saugos lygių architektūra. Vartotojų darbo vietose turi būti programinės antivirusinės programos. Tačiau vartotojo darbo vietos dažnai yra nepatikimos (antivirusas gali būti išjungiamas), todėl aukščiausiame lygyje duomenų srautas turi būti tikrinamas prieš patenkant į įmonės privatų tinklą.Kaip pavyzdį galima paminėti Panda GateDefender įrenginį [8] (1.4 pav).

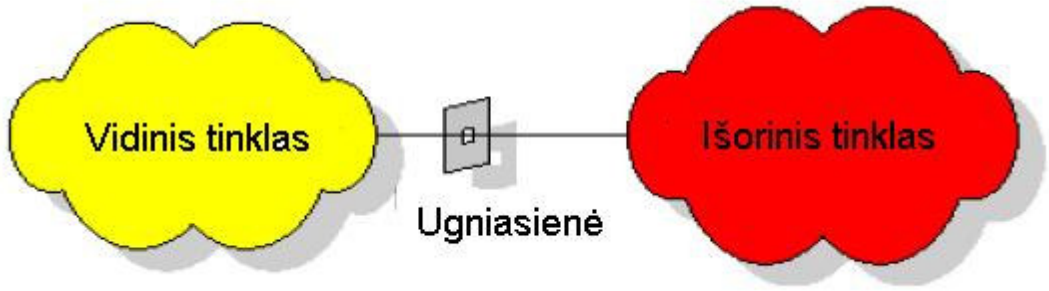
1.4 pav. Panda GateDefender įrenginys

Jis blokuoja virusus, nepageidaujamą elektroninį paštą ir nepageidaujamą turinį prieš jiems patenkant į kompaniją. Panda GateDefender turi automatišką atsinaujinimo sistemą, kuri

suteikia moderniausią apsaugą visam tinklui.. Panda GateDefender puikiausiai tinka visoms mažoms, vidutinėms ir didelėms įmonėms. Tokie aparatūriniai įrenginiai įterpiami tarp įmonės maršrutizatoriaus ir vidinio tinklo. Pagrindiniai parametrai yra maksimalus srauto tikrinimo greitis (5-30Mbps). Esant dideliam srautui susidaro duomenų kamščiai ir tinklas nefunkcionuoja. Esant kelioms tinklo saugumo zonoms tampa sudėtinga parinkti įrenginio darbo vietą, tam kad būtų patikrintas visas reikalingas srautas ir nebūtų bereikalingo srauto tikrinimo.

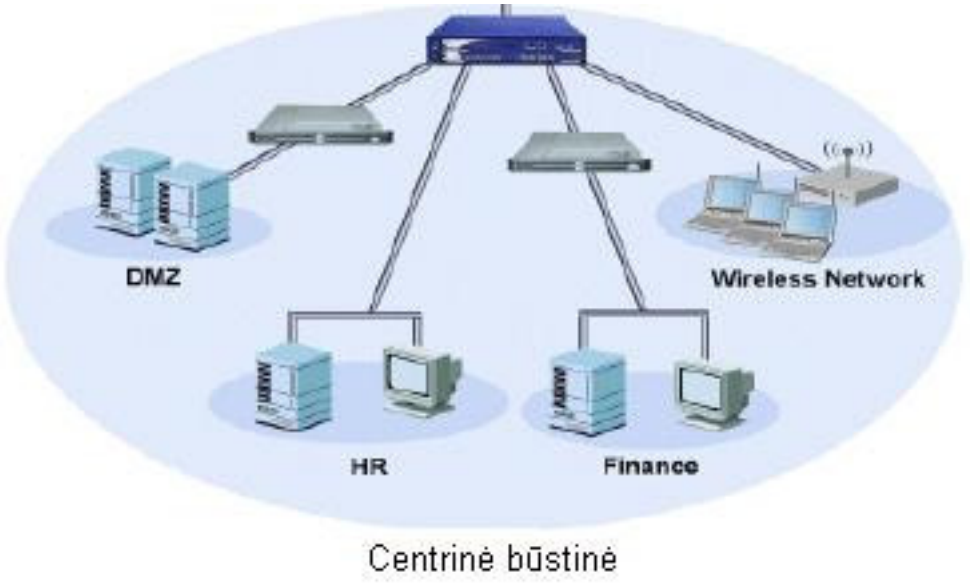
1.4.2. Ugniasienės

Ugniasienės yra pagrindiniai saugios korporatyvinės įmonės saugumo architektūros elementai. Ugniasienė kontroliuoja duomenų srautą į ir iš tinklo. Tam kad filtruoti paketus, reikia sudaryti aibę taisyklių, kurios nurodo protokolų tipus, kurie yra praleidžiami ir kurie nepraleidžiami priklausomai nuo gavėjo ir siuntėjo adresų. Yra dviejų tipų ugniasienės [9]: Filtravimo be atminties- kiekvieno paketo informacija lyginama su statiškai nustatytu taisyklių rinkiniu. Žiūrima tik į paketo antraščių informaciją (siuntėjo ir gavėjo IP, portus).



1.5 pav. Ugniasienė

Filtravimo su atmintimi - kai įvairių lentelių pagalba sekama paketų seka ir atitinkamos taisyklės taikomos priklausomai nuo esamos susijungimo būsenos. Ugniasienė tikrina ir paketo turinį, pagal kurį nustato esamo sujungimo būseną. Pirmas žingsnis norint sukurti saugią architektūrą – taisyklių projektavimas. Reikia numatyti kokių saugumo zonų reikia, kokie servisai bus teikiami, kam bus leidžiamas priėjimas prie atitinkamų resursų. Skirtingo lygio saugumo zonų sukūrimas žymiai padidina tinklo saugumą ir supaprastina saugumo taisyklių taikymą.



1.6 pav. Tinklo skaidymas saugumo zonomis

1.4.3. Tinko atakų aptikimo sistemos

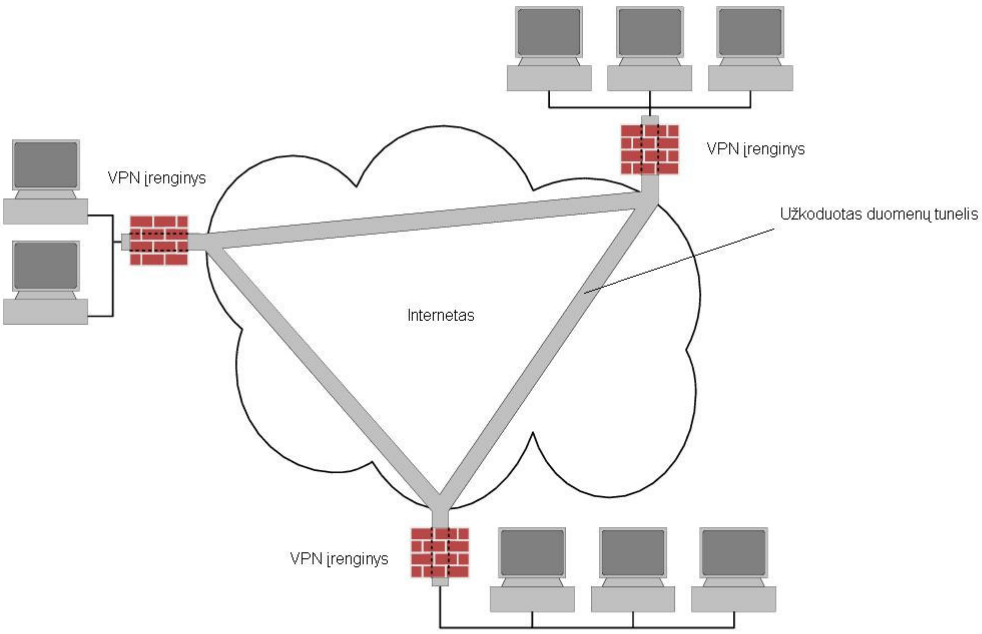
Įsilaužimų aptikimo sistema (IDS) stebi duomenų srautą ir aptikus įsilaužimo požymį generuoja pranešimą administratoriui [10]. Ugniasienės saugo tinklą nuo įsilaužimų, tuo tarpu IDS parodo ar tinklas atakuojamas. Yra du tipai IDS: tinklo ir lokalus. Kiekvienas tipas turi savo privalumo ir trūkumų.

Lokalus IDS esantis serveryje arba vartotojo darbo vietoje renka informaciją generuojamą lokalios sistemos. Šio tipo IDS sudėtinga administruoti didelės įmonės tinkluose.

Tinklinės IDS renka informaciją keliaujančią tinkle. Kiekvienas paketas yra sulyginamas su duomenų bazėje esančia informacija. Tinklines IDS yra lengviau paskirstyti ir administruoti. Tačiau yra ribotas maksimalus duomenų srautas, kurį gali apdoroti IDS.

1.4.4. VPN įrenginiai

VPN tinklo realizacijai naudojami specialūs įrenginiai, kurie užtikrina saugų ryšio kanalą tarp kelių nutolusių taškų. Saugiam ryšio tuneliui užtikrinti yra naudojamas IPSec protokolas [11].



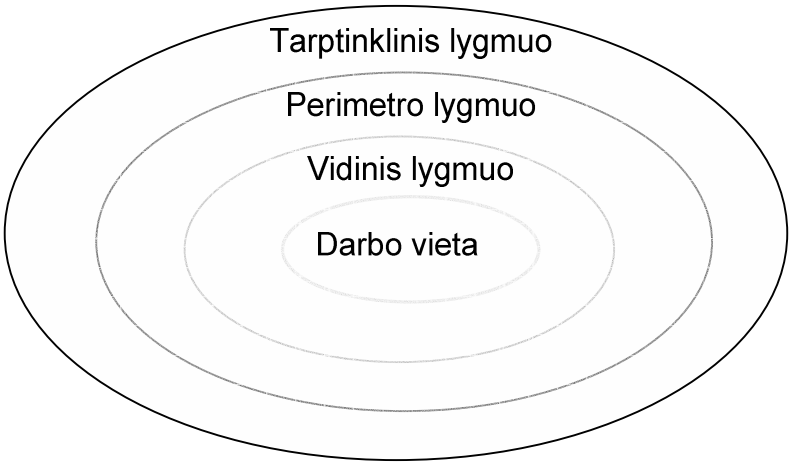
1.7 pav. VPN įrenginiai

VPN yra pagrįstas duomenų srauto tunelio idėja. Sukurtame virtualiame tunelyje užkoduoti duomenų paketai yra įvelkami į nešantįjį IP protokolą ir persiunčiami gavėjui. Gavėjas išpakuoja VPN paketą ir jį dekoduoja. Šie veiksmai sukuria ženklų vėlinimą.

1.5. Korporatyvinės įmonės saugaus tinklo architektūra

Korporatyvinės įmonės tinklo architektūra susideda iš keturių sluoksnių [12]:

- *Duomenų persiuntimo saugumas:* Apsaugo duomenų srautus tarp įmonės filialų, nutolusių vartotojų, verslo partnerių;
- *Tinklo perimetro saugumas:* Kontroliuoja ar duomenų srautas (HTTP, SMTP, POP3, FTP, VPN ir t. t.) gali įeiti arba išeiti į įmonės tinklą;
- *Vidinio tinklo saugumas:* Kontroliuoja vartotoju priėjimą prie įmonės servisų;
- *Vartotojo darbo vietos saugumas:* Galutinių vartotojų apsauga.



1.8 pav. Saugaus tinklo architektūra

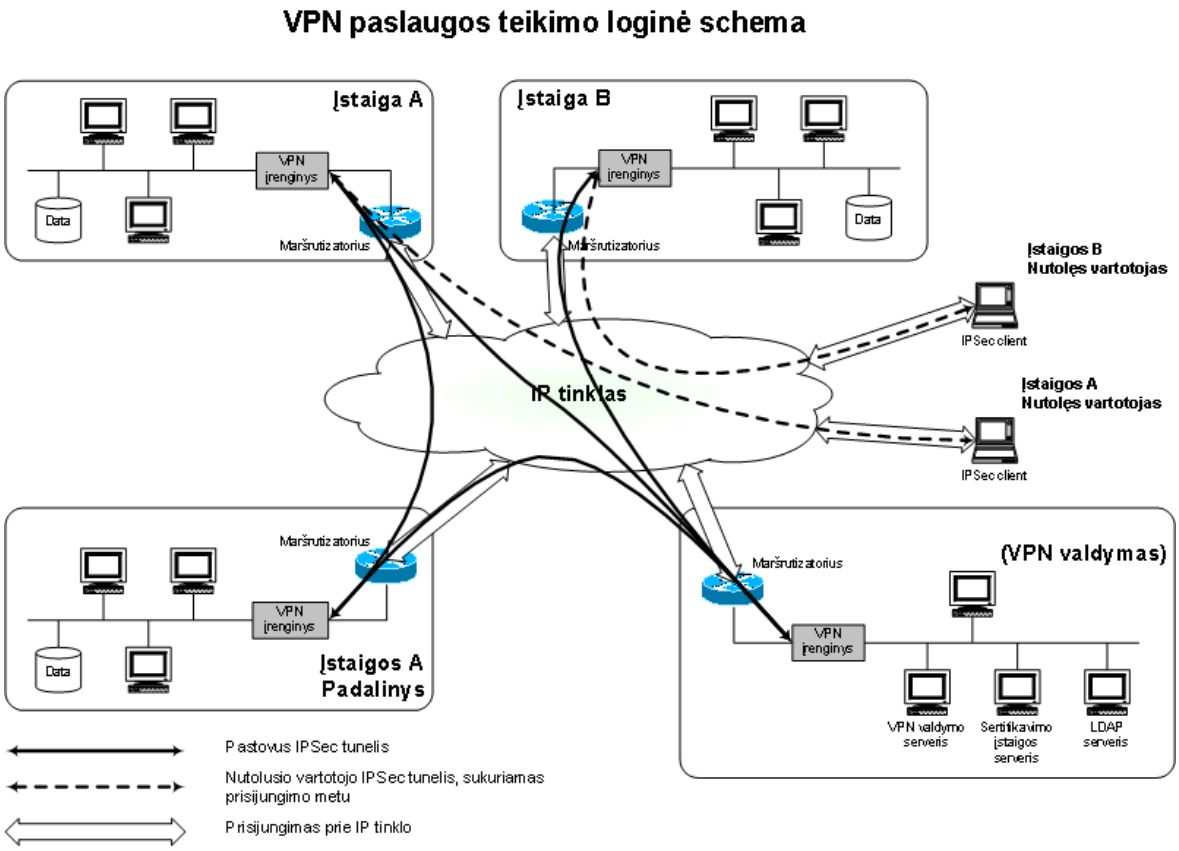
1.5.1. Duomenų persiuntimo tarp įmonės nutolusių taškų saugumas

Šis saugumo lygis reikalingas duomenims koduoti tarp nutolusių įmonės taškų. Virtualių tinklų technologija (VPN) užtikrina šio lygmens saugumą [11]. Užkoduotas duomenų srautas keliauja viešu interneto tinklu tarp geografiškai išsibarsčiusių įmonės taškų. Yra kelios skirtingos VPN technologijos. VPN ryšiui yra naudojamas IPSec protokolas. Šis protokolas užtikrina duomenų srautų atskyrimą, panaudojant duomenų srautų tunelius. Konfidencialumui užtikrinti naudojama autentifikacija.

VPN sprendimą galima realizuoti nepriklausomai nuo vartotojų prijungimo prie Interneto būdo, be to šios paslaugos diegimo neriboja geografiniai atstumai ar skirtingi Interneto paslaugų tiekėjai.

VPN sprendimus galima realizuoti:

- tarp vidinių ir nutolusių įmonės padalinių (Intranet VPN),
- tarp įmonės tinklo ir pavienių arba mobilių įmonės darbuotojų (Nuotolinio prisijungimo VPN),
- tarp įmonės ir jos partnerių, klientų bei tiekėjų .



1.9 pav. VPN loginė schema

1.5.2. Tinklo perimetro saugumas

Perimetrinio tinklo saugumas yra įmonės informacinės saugos branduolys, kurio pagrindinis elementas – ugniasienė [9]. Ugniasienės – komponentas ar aibė sudėtinių komponentų, kurie uždraudžia priėjimą prie apsaugoto tinklo ir interneto arba tarp kelių atskirų tinklų. Tam kad filtruoti duomenis, reikia sudaryti aibę taisyklių, kurios nurodo paketų tipus (iš kurio į kurį IP adresą, portą, aplikacijos tipą), kurie yra praleidžiami ir kurie tipai yra nepraleidžiami.Perimetrinis tinklas – tai tinklas, kuris yra įterptas tarp apsaugoti vidinio tinklo ir išorinio tinklo, tam kad užtikrinti papildomą tinklo apsaugos sluoksnį. Iš perimetrinio tinklo negalima prieiti prie vidinio tinklo resursų. Pagal nustatytas taisykles iš vidinio ir išorinio tinklų yra leidžiamas priėjimas prie tam tikrų resursų (WWW, POP3 ir t. t.).

Kartu su ugniasiene yra naudojama ir įsilaužimo aptikimo sistema (IDS). IDS analizuoja duomenų srautus keliaujančius per ugniasienę ir ieško iš anksto žinomų tinklinės atakos požymių. Aptikus kokią nors anomaliją (stipriai suintensyvėjęs duomenų srautas, paketų seka ir t. t.) IDS generuoja pranešimą sistemos administratoriui, arba nutraukia įtartiną duomenų srautą.

Įvairūs filtravimo ir skanavimo funkcijos taip pat įtrauktos į perimetrinio tinklo saugumo sluoksnį. WEB turinio, SPAM, antivirusinės skeneriai ankščiau buvę vidaus sluoksnio saugumo zonoje dabar vis plačiau naudojami perimetrinio sluoksnio zonoje. Jei grėsmė pasieka vartotojo darbo vietą, tai jau būna per vėlu. Grėsmė turi būti aptikta ir sustabdyta dar prieš jai patenkant į vidinio sluoksnio zoną.

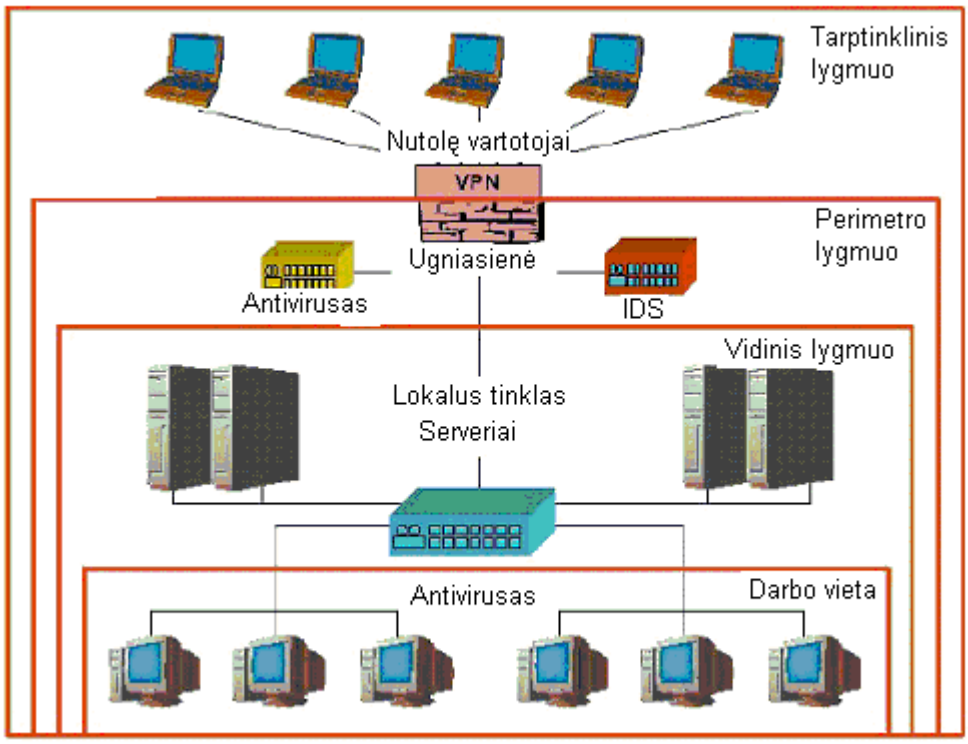
1.5.3. Vidinio tinklo saugumas

Vidinis tinklo lygmuo yra dažniausiai pamirštamas dėl viso dėmesio sukoncentravimo į išorinius lygius. Tačiau statistika rodo, kad tinklo atakos iš įmonės vidaus yra dažnesnės nei iš išorės. Apie 70% saugumo pažeidimų yra padaroma įmonės darbuotojų [13]. Šio lygmens saugumą yra sunkiausiai užtikrinti, nes įsilaužėliui yra žinoma vidinė struktūra ir jis jau turi tam tikras teises serveriuose. Atsaugant šį lygmenį yra naudojama šios saugos priemonės:

- tinklo segmentacija;
- vidinė IDS.

1.5.4. Vartotojo darbo vietos saugumas

Nors ir dauguma vartotojo darbo vietos saugos priemonių perkelta į perimetrinio sluoksnio lygmenį, tačiau kompiuteriuose turi būti antivirusinės priemonės [12]. Taip pat norint apsisaugoti nuo į vidinį tinklą patekusių internetinių kirminų būtina kompiuteriuose turėti asmenines ugniasienes.



1.10 pav. Korporatyvinės įmonės saugaus tinklo architektūra

1.6. Informacinės saugos modeliavimas

Kadangi įmonės saugumo infrastruktūros kūrimas yra sudėtingas procesas, todėl itin svarbu iš pradžių tiksliai suprojektuoti visą sistemą, nes po to bus sugaišta daug laiko (ir išleista pinigų) sistemos modifikacijai. Todėl projektavimo etape (tiek tinklo išdėstymo, tiek saugomo zonų pasiskirstymo, tiek papildomų saugumo priemonių) reiktų kartu pamodeliuoti kiek galima daugiau ir įvairesnių situacijų.

Informacinė sauga – tai sudėtinga ir persipynusi saugos priemonių visuma. Tos priemonės priklauso viena nuo kitos ir projektuojant reikia matyti bendrą vaizdą. Priklausomai nuo darbo vietų skaičiaus, įmonės geografinio išsidėstymo ir tinklo darbo intensyvumo priklausys informacinės saugos užtikrinimo priemonių parametrai ir duomenų srautai. Šios priemonės įtakoja duomenų srauto greitį. Šis apkrovimas taip pat priklausys nuo naudojamos tinklo architektūros ir saugos priemonių architektūros.

Modeliavimo metu reikėtų įvertinti:

- duomenų judėjimo tinkle greitį;
- tinklo architektūrą;
- įmonės struktūrą, t.y. geografinį išsidėstymą;
- VPN kodavimo vėlinimą;

- antiviruso vėlinimą;
- įsilaužimų aptikimo vėlinimą;
- protokolų pasiskirstymą duomenų sraute;
- įmonės servisus.

Panagrinėsime keletą informacinės saugos modeliavimo metodų ir apibrėšime jų privalumus ir trūkumus.

Atakų grafo – kiekviena sistema turi atakų grafų rinkinį Grafo mazgas reiškia sistemos pažeidimą. Grafas parodo kaip įsilaužėlis gali pakenkti įmonės kompiuterinėms sistemoms.

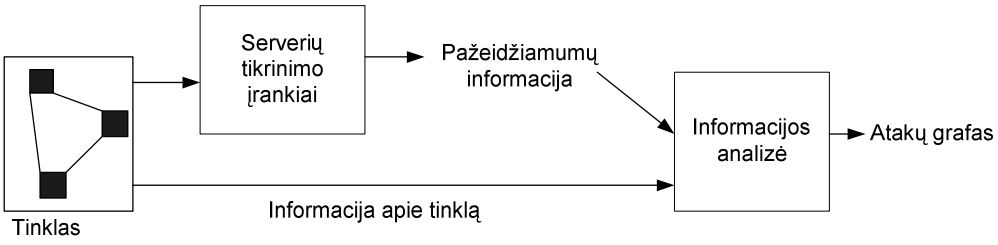
Markovo procesų modelis – korporatyvinės įmonės saugos sistema pavaizduojama grafu, kurio viršūnės yra atitinkami saugos elementai, o lanko svoris nurodo perėjimo į kitą būseną tikimybę.

Imitacinis modelis – GPSS modeliavimo kalba saugos sistema yra išskaidoma į blokus (procesus), kurie sujungiami ryšio kanalais. Blokais gali būti antivirusas, tinklo sąsajos, VPN modulis, IDS modulis, o ryšio kanalus atitinka informacijos duomenų srautai tarp tinklo segmentų.

Šio darbo tikslas yra sudaryti korporatyvinės įmonės saugaus komunikavimo architektūras, jų modelius ir jas įvertinti.

1.6.1. Atakų grafo modelis

Atakų grafas reprezentuoją visus galimus kelius, kurių tikslas yra modeliuojamas sistemos saugumo pažeidimas [14]. Didelių sistemų atakų medžių projektavimas yra ilgas ir sudėtingas procesas. Saugumo specialistai naudoja šiuos duomenis sistemos silpnų vietų aptikimui. Atakų grafo projektavimui reikia surinkti visus tinklo sistemos lokalius ir globalius pažeidžiamumus. Pažeidžiamumų duomenų bazės surinkimui naudojamos tinklo elementų, serverių saugumo tikrinimo priemonės. Sujungus ryšiais lokalius ir globalius pažeidimus gauname atakų grafą. Kiekvienas grafo lankas yra atitinkamą pažeidžiamumą išnaudojantis procesas, kuris perveda sistema į nestabilią būseną.



1.11 pav. Atakų medžių projektavimas

Atakos modelį galima apibrėžti taip sudėtingą sistemą ginančių ir atakuojančių agentų aibę. Atakų modelis yra $M = (S, \tau, s_0)$, kur S yra būsenų aibė. $\tau \in S \times S$ yra perėjimų tarp būsenų aibė, kur $s_0 \in S$ yra pradinė būsena. Būsena S apibrėžia trijų agentų rinkinį $\Phi = \{E, D, T\}$, kur T – Atakuojama sistema; E – grėsmė siekianti pažeisti sistemą; D – saugos priemonė. Būsenos perėjimus medyje inicijuoja įsilaužėlio veiksmai. Korporatyvinės įmonės tinklinės ir kompiuterinės sistemos susideda iš daugelio aparatūrinių ir programinių komponentų. Yra pasirinkti šeši komponentai konstruojant atakų medžių modelius M [15].

- H, serverių aibė;
- C, ryšių tarp serverių aibė (aprašo tinklo topologiją);
- T, ryšių tarp serverių aibė (aprašo autentifikaciją);
- I, įsilaužėlių aibė;
- A, veiksmų aibė (pažeidžiamumų išnaudojimas), kurią gali panaudoti įsilaužėliai;
- Ids, įsilaužimų aptikimo sistemų aibė;

Lentelėje pavaizduota kiekvieno agento *i* būsena S_i ir veiksmų aibė A_i.

1.1 lentelė. Atakų medžio komponentai

$i \in \Phi$	S_i	A_i
E	I	A
D	Ids	{aliarmas}
S	$H \times C \times T \times S$	$\otimes$

Kiekvienas būsenos perėjimas $(s_1, s_2) \in \tau$ generuoja arba įsilaužėlio veiksmą arba aliarmo signalą generuojamą Ids.

Serveris arba darbo vieta yra pagrindiniai įsilaužimų taikiniai, nes juose saugoma informacija ir teikiami servisai. Jie aprašomi tokiu informacijos (id, svcs, sw, vuls), čia:
id – serverio identifikatorius;

svcs – aibė aktyvių portų, kuriais serveris aptarnauja vartotojus;

sw – sąrašas programinės įrangos esančios serveryje;

vuls – sąrašas pažeidžiamumų esančių serveryje;

Ryšių tarp serverių aibė aprašoma $C(h_1, h_2, p)$. Kas reiškia, kad serveris h_2 yra pasiekiamas iš serverio h_1 per *p* portą.

Patikimo ryšio $T(h_1, h_2)$ nurodo, kad iš serverio h_2 galima prisijungti prie h_1 be autentifikacijos.

Ids gali gražinti dvi reikšmes priklausomai nuo to ar aptiko ar neaptiko įsilaužimą. $ids(h_1, h_2, a) = d$ - jei aptiko įsilaužimą *a* iš h_1 į h_2.

$ids(h_1, h_2, a) = s$ - jei neaptiko įsilaužimo *a* iš h_1 į h_2.

Jei $h_1 = h_2 = h$, tai Ids patalpinta serveryje h .

Kiekvienas veiksmas aprašomas (r, h_s, h_t), kur $h_s \in H$ iš kur vykdomas veiksmas ir $h_t \in H$ yra to veiksmo taikinys. *r* yra taisyklė kuri parodo kaip įsilaužėlis gali pakeisti sistemą arba sužinoti daugiau informacijos. Taisyklės turi keturis tipus: įsilaužimo pradinės sąlygos, tinklo pradinės sąlygos, įsilaužimo pasekmė, tinklo būsena po įsilaužimo. Įsilaužimo pradinėse sąlygose nurodoma būtinos pradinės žinios veiksmui atlikti. Tinklo pradinės sąlygos yra taikinio servisai, pažeidžiamumai, kurie turi būti išnaudoti įsilaužimui atlikti.

Įsilaužėlis turi pradinę informaciją apie tinklą ir serverius (adresai, pažeidžiamumai ir t. t.). $plvl : H \to \{none, user, root\}$ parodo kokias teisias įsilaužėlis turi sistemose.

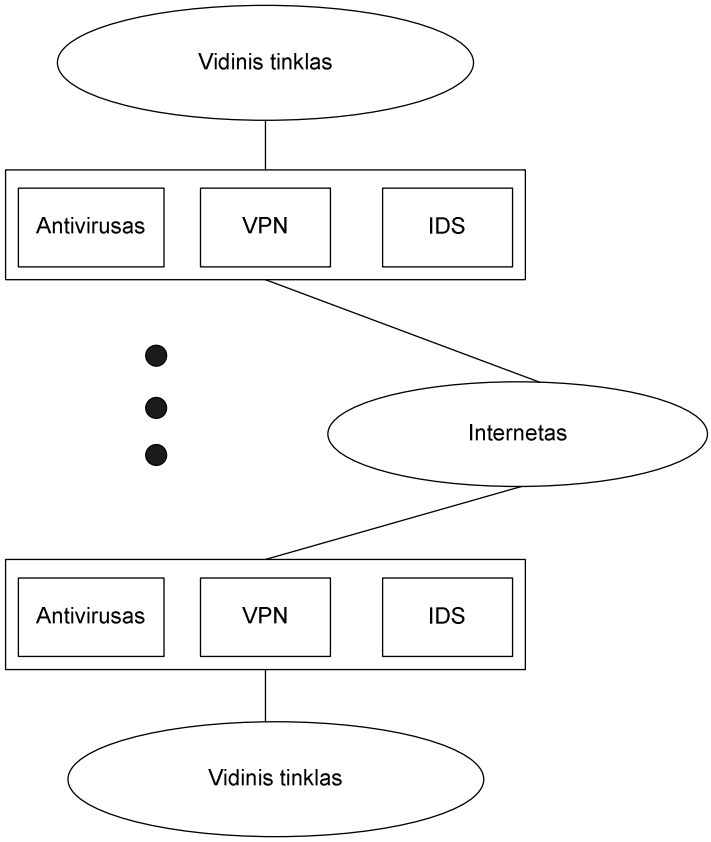
Atakų medžiai parodo:

- sėkmingas atakas, kurių neaptinka Ids ar kitos saugos priemonės;
- kur efektyviausiai išdėstyti saugos priemones;
- parinkti efektyvias programines ir aparatūrines saugos priemonių realizacijas;
- numatyti ateityje galimus incidentus;
- įvertinti skirtingų tinko topologijų efektyvumą;

Šiuo metodu galima labai smulkiai aprašyti įmonės sistemų atakų grafus. Tačiau tai labai sudėtingas darbas. Šiuo metu yra dirbama sudarinėjant atakų medžių automatinio generavimo metodus. Šiuo metodu negalime įvertinti kiekybinių saugos priemonių parametrų (antiviruso vėlinimas ir t. T.). Apibrėžiami tik pažeidžiamumai ir negalima modeliuoti saugos priemonių darbo.

1.6.2. Markovo procesų modelis

Kaip jau minėta, įmonės informacinės saugos efektyvumas priklauso nuo daugelio faktorių. Šiame darbe nagrinėsime architektūrą pavaizduotus paveiksle:



1.12 pav. Tinklų sujungimo architektūra

Pagrindiniai modeliuojami informacinės saugos elementai:

- Antivirusas
- VPN modulis
- IDS modulis

Kiekvieno iš šių modulių parinkimas tampriai siejasi su informacinės saugos sistemos kaina. Esant ribotai sistemos kainai projektuotojai turi rinktis kokius efektyvumą lemiančius kriterijus aukos vardan kitų. Informacinės saugos struktūros tobulinimas labiausiai įtakoja visos įmonės informacinių technologijų kokybę, kuri tiesiogiai veikia darbo našumą.

Panagrinėjus giliau šią schemą galima būtų išskirti pagrindinius informacinės saugos efektyvumą nusakančius kriterijus:

- sistemos elementų vėlinimas;
- protokolų santykinis pasiskirstymas duomenų sraute;
- paketų pasirodymo dažnis;
- duomenų maršrutizavimo taisyklės;
- sistemos elementų išdėstymas;

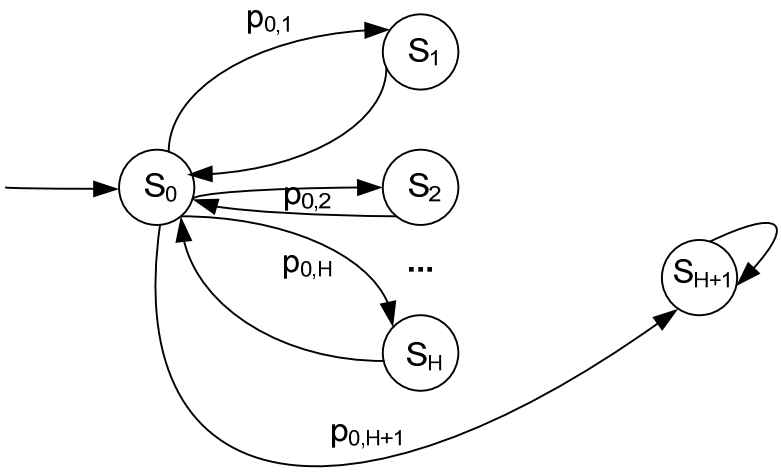
Modelis turi apibrėžti duomenų atsiradimo ir išėjimo taškus, įvertinti aukščiau išvardintus kriterijus. Šį modelį kuriame teigdami, kad sekanti duomenų apdorojimo būsena nepriklauso nuo ankstesnės. Šiuo atveju galime taikyti Markovo procesų modelį [16]. Apibrėšime būsenų modelį $\{ S_0,...,S_{H+1} \}$ ir perėjimų tikimybių matricą:

$$P=[p_{ij}]=\begin{array}{c|cccc} & S_0 & S_1 & \dots & S_{H+1} \\ S_0 & p_{0,0} & p_{0,1} & \dots & p_{0,H+1} \\ S_1 & p_{1,0} & p_{1,1} & \dots & p_{1,H+1} \\ \dots & & & \dots & \\ S_{H+1} & p_{H+1,0} & p_{H+1,1} & \dots & p_{H+1,H+1} \end{array}$$

Elementai p_{ij} matricoje P nurodo tikimybę perėjimo iš būsenos S_i į būseną S_j. Matrica P – stochastinė matrica. Jos atskirų eilučių suma $\sum_i p_{ij}=1$. Skaičiavimo procesas visada prasidės S_0 būsenoje. Po kiekvieno duomenų patekimo į būsena vykdomi atitinkami skaičiavimai. Iš būsenos S_0 duomenų paketas C pagal tikimybių matricą P pereina į būseną $S_1,...,S_{H+1}$, kurios apibrėžia sekančius sistemos saugos elementus arba pereina į paskutinę būseną, kuri žymi darbo pabaigą.

Siekiant modelį padaryti suprantamesniu matrica P vaizduojama grafu (1.13 pav.).

$$P=\begin{array}{c|cccccc} & S_0 & S_0 & S_2 & \dots & S_H & S_{H+1} \\ S_0 & 0 & p_{0,1} & p_{0,2} & \dots & p_{0,H} & p_{0,H+1} \\ S_0 & 1 & 0 & 0 & \dots & 0 & 0 \\ S_2 & 1 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ S_H & 1 & 0 & 0 & \dots & 0 & 0 \\ S_{H+1} & 0 & 0 & 0 & \dots & 0 & 1 \end{array}$$



1.13 pav. Būsenų grafas

Grafo lankas jungia dvi būsenas S_i ir S_j. Lanko svoris yra tikimybė, kuria įvyksta perėjimas iš S_i būsenos į S_j būseną. Tikimybės $p_{0,1},...,p_{0,H+1}$ priklauso nuo pasirinktų saugos modelio elementų, protokolų pasiskirstymo, maršrutizavimo taisyklių ir architektūros. Skaičiai $N_1,...,N_H$ parodo paketų skaičių tikrinamų įrenginyje $F_1,...,F_H$. Šiuo atveju vidutinis paketų skaičius pereinant iš S_0 į $S_1,...,S_{H+1}$ turi būti $(N_1+...+N_H)$..Vieną kartą paketas pereina iš būsenos S_0 į galutinę būseną S_{H+1}. Paketų skaičius išeinantis iš S_0 būsenos $N=\sum_{h=1}^{H} N_h+1$. Tikimybė $p_{0,h}$ parodo paketų pasirodymo tikimybę būsenoje S_h atžvilgiu visiems galimiems atvejams iš būsenos S_0 į $S_1,...,S_{H+1}$. Ši tikimybė būsenoje S_h lygi N_h/N, kur N_h- vidutinis paketų pasirodymo skaičius būsenoje S_h. Bendru atveju $p_{0,h}=N_h/N \quad (h=1,...,H)$;

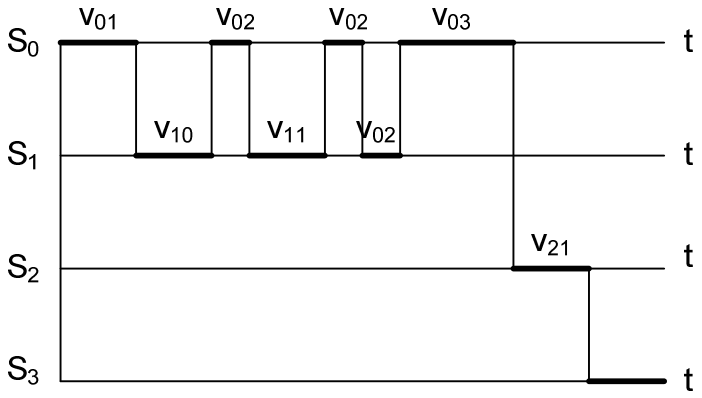
$$p_{0,H+1}=1/N$$

Kiekinį vėlinimo įvertinimą kiekvienoje būsenoje nusako parametrai $\sigma_1,...,\sigma_H$. σ nusako vidutinį vėlinimą atliktą su modeliuojamu paketų skaičiumi, tada $\sigma_1,...,\sigma_H$ parodo vidutinį vėlinimą atitinkamose $S_1,...,S_{H+1}$ būsenose. Vidutinis vienos būsenos vėlinimas: $\sigma_0=\sigma/N$, N – paketų kiekis.

Vėlinimas yra atsitiktinis dydis σ_i, kuris kinta tam tikrose nustatytose ribose.

Šiuo atveju sudarėme modelį su (H+2) būsenomis, pradine būsena S_0 ir tikimybių matrica P. Atsitiktinė būsenų kaita $S_0,...,S_{H+1}$, kurios kinta pagal tikimybių matrica P. Su

būsenomis $S_0,...,S_{H+1}$ susietas vėlinimas $\sigma_0,...,\sigma_H$. Šio modelio diagramos pavyzdys:



1.14 pav. Laiko diagrama

Sistemos našumas įvertinamas sekančiai: $n_i = \sum_{j=1}^{K} p_{ji} n_j \sigma_i \quad (i = 2,...,k), K = k + 1;$

k – grafo viršūnių skaičius; p_{ji} - tikimybė perėjimo iš viršūnės j į i, σ_i - i būsenos vėlinimas;

Konkrečios įmonės atveju pagal jos informacinės saugos sistemos elementų analizę apskaičiuojamos pagrindinės kiekybinės charakteristikos. Parinkus atitinkamus parametrus išrenkama optimali sistema pagal kainą ir duomenų apdorojimo trukmės kriterijus.

1.6.3. Imitacinis GPSS modelis

GPSS tinklo modelis sudarytas iš blokų [17]. Blokai turi savo paskirtį ir prasmę. Jais keliauja žymės (mūsų atveju tinklo paketai). Blokas GENERATE įveda į modelį naujus paketus atitinkamu laiko intervalu. Paketai juda laike iš vieno modelio bloko į kitą. Įeidamas į bloką paketas sužadina jo paprogramę, kuri apdoroja atitinkamą įvykį. Toliau paketas stengiasi pereiti į naują bloką. Ji keliauja tinklu kol nesutinka bloko, kuris atlieka tokias funkcijas:

- pašalina paketą iš modelio;
- laikinai sustabdo žymės judėjimą kol netenkinamos atitinkamos sąlygos;
- sustabdo atitinkamam laiko vienetui;

Toliau prasideda kito paketo judėjimas ir t. t. Vieno žingsnio metu peržiūrima ar yra procesų, kuriuos galima vykdyti. Modeliavimas baigiamas, kai visi paleisti paketai yra neaktyvūs.

Informacinė saugos sistema yra išskaidoma į blokus (procesus), kurie sujungiami ryšio kanalais. Blokais gali būti antivirusas, tinklo sąsajos, VPN modulis, IDS modulis, o ryšio kanalus atitinka informacijos duomenų srautai tarp tinklo segmentų. Fiziškai negalime įvertinti visų modeliuojamos sistemos parametrų, tačiau eilių teorija GPSS modelyje įvertinama pakankamai paprastai.

Naudodami matematinį aparatą aprašysime įmonės informacinės saugos modelį. Planuojamas modeliuoti informacinės saugos priemones (M_1, M_2 ...,M_{NM}) padaliname visoms tinklo sąsajoms I_0, I_2 ...,I_{NI}. Analogiškai tinklų generuojamus duomenis (S_1, S_2 ...,S_{NS}) paskirstome tinklo sąsajoms (I_1, I_2 ...,I_{NI}). Kol kas nesvarbu sąsajų saugomo lygiai.

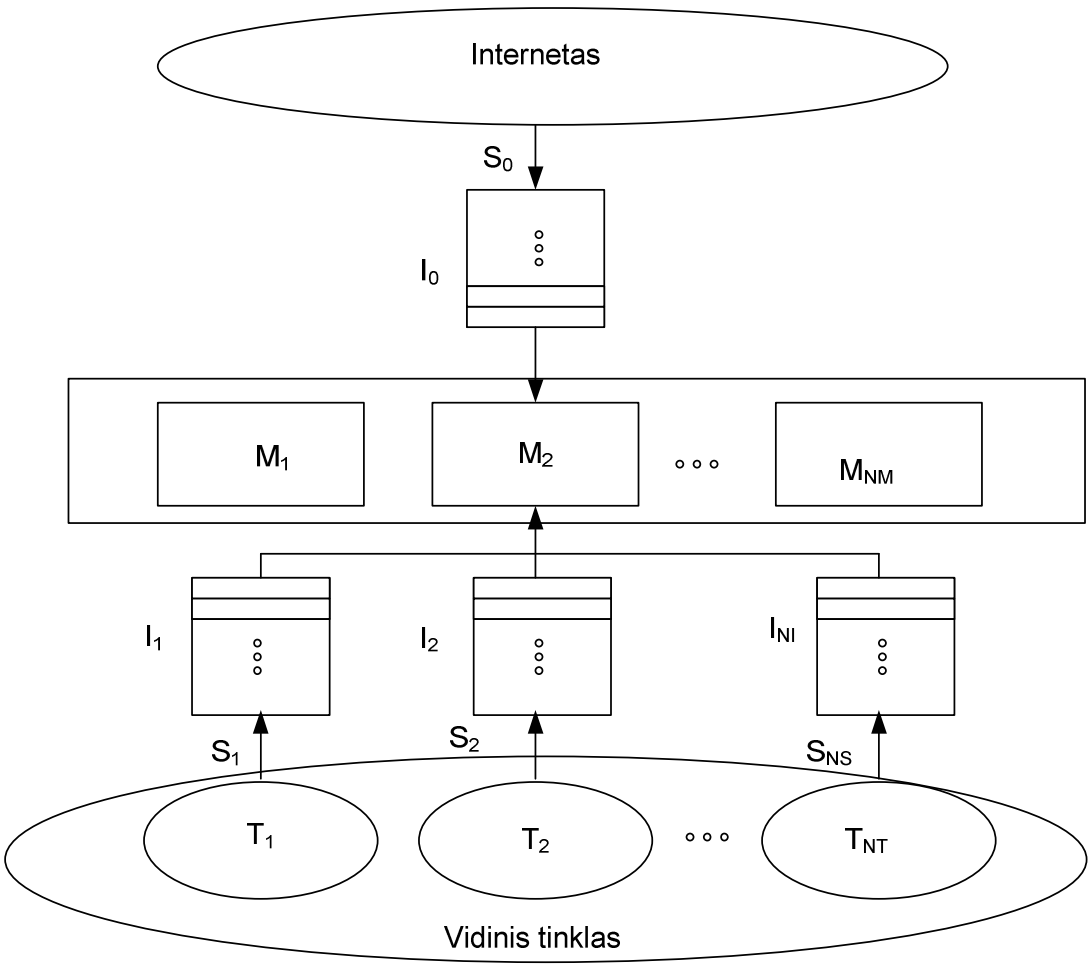
NM – saugumo priemonių kiekis sistemoje;

NI – tinklo sąsajų kiekis sistemoje;

NS – duomenų intensyvumas tinklo sąsajoje;

NT – tinklo segmentų kiekis sistemoje;

Bendru atveju modelio schema atrodys taip:



1.15 pav. Imitacinis modelis

Šiam modeliui reikalingi parametrai:

- Paketų pasirodymo dažnis sąsajose IS_0, IS_2 ...,$IS_{NI;}$
- Saugumo priemonių vėlinimas MD_1, MD_2 ...,$MD_{NM;}$
- Eilės prie tinklo sąsajų IQ_0, IQ_2 ...,$IQ_{NI;}$
- Eilės prie saugos modulių MQ_1, MQ_2 ...,$MQ_{NM;}$

Tinklo sąsajų apkrovimas aprašomas paketo pasirodymo dažniu (ms). Modelyje tariama, kad kiekvienas paketas yra 200 baitų dydžio. Jei norime aprašyti 2.5Mbps srautą, tada paketų pasirodymo dažnis bus 0.64ms.

Eilės susidaro prie tinklo sąsajų (kadangi reikalingas atitinkamas laiko tarpa duomenų siuntimui ir gavimui) ir prie saugos modulių (ribotas duomenų aptarnavimo kiekis ir laikas). Eilė prie sąsajų parodys tinklo pralaidumo resursų nepakankamumą, o eilė prie saugos modulių – jų resursų stygių (reiškia reikia kitaip dalinti duomenų srautus arba didinti modulių resursus).Pagal masinio aptarnavimo teoriją paraiškos į sistemą ateina Puasono srautu (pasiskirstę pagal eksponentinį dėsnį), kurio parametras – srauto intensyvumas – bus lygus ISi_I.

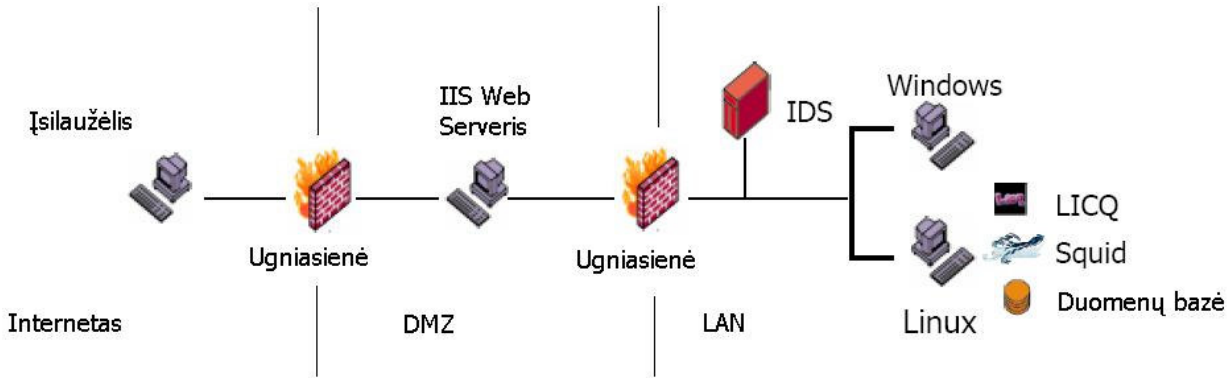
Šį modelį geriausia taikyti parenkant saugos priemonių parametrus, kiekius, duomenų srautų pasiskirstymą. Projektavimo pradžioje, trūkstant pradinių duomenų modeliavimui, naudojami tik tinklo sąsajų ir saugos modulių objektai, bei grubiai įvertinti duomenų srautai. Projektavimo eigoje aiškėjant procesams ir tikslėjant duomenų srautams įvedami nauji parametrai ir tikslinami ankstesni parametrai ir esant reikalui keičiama visa saugaus tinklo architektūra. Šiuo modeliu galima parinkti techninės įrangos kiekį ir charakteristikas. Jis neturi įtakos tinklo struktūros kokybei.

Šio darbo tikslas yra sudaryti korporatyvinės įmonės saugaus komunikavimo architektūras, modelius ir įvertinti jų efektyvumą.

2. TIRIAMOJI DALIS

2.1. Atakų grafo modelis

Turime korporatyvinės įmones dalie tinklo modelį kuriam konstruosime atakų grafą (2.1 pav.):



2.1 pav. Tinklo modelis

Kompiuterių aibė

H={Įsilaužėlis,II_ Serveris, Windows, Linux}.

Įsilaužėlių aibė

I={Įsilaužėlis_}.

Pažeidžiamumų aibė

A={ IIS_buffer_overflow, Squid_port_scan, LICQ_gain_user, Local_buffer_overflow}.

Linux serveris, esantis vidiniame tinkle teikia LICQ, Squid web proxy ir duomenų bazės paslaugas. DMZ zonoje patalpintas IIS web serveris. Tarkime, kad įsilaužėlio tikslas yra sunaikinti duomenų bazę. Šioje įmonės sistemoje yra penki pažeidžiamumai, kurias pasinaudojus galima pakenkti duomenų bazei.

2.1 lentelė. Pažeidžiamumų duomenys

Veiksmas	Pasekmė	CVE ID
IIS_buffer_overflow	Administratoriaus teisių gavimas (nuotoliniu būdu)	CAN-2002-0364
Squid_port_scan	Portų skanavimas	CVE-2001-1030
LICQ_gain_user	Vartotojo teisių gavimas (nuotoliniu būdu)	CVE-2001-0439
Local_buffer_overflow	Administratoriaus teisių gavimas (lokaliai)	CVE-2002-0004

Žinomų pažeidžiamumų sąrašą galima gauti CVE duomenų bazėje [18].

2.2 lentelė. Pažeidžiami servisai

w3svc	IIS web servisas
Squid	Squid kešavimo servisas
Licq	Licq servisas
Vul-at	*at* procesas pažeidžiamas buferio perpildymu

Ryšių tarp kompiuterių aibė

$C(h_1, h_2, p),\ h_1, h_2 \quad H,$

$C \quad H \times H \times P.$

Ryšius *C* tarp tinklo komponentų apibrėšime sekančiai: lentelės įrašas atitinka (h_1, h_2). IIS ir Squid servisai pasiekiami per 80 portą. LICQ klientas pasiekiamas per 5190 portą. Ryšys nusako kuris iš šių servisų gali būti pasiekiamas iš kito nutolusio kompiuterio. Įrašas susideda iš trijų loginių reikšmių. Pirma reikšmė „y“ jeigu h_1 ir h_2 yra sujungti tiesioginiu ryšiu. Antra reikšmė „y“ jeigu h_1 gali prisijungti prie h_2 per 80 portą. Trečia reikšmė „y“ jeigu h_1 gali prisijungti prie h_2 per 5190 portą.

2.3 lentelė. Ryšių duomenys

	Įsilaužėlis	IIS_Serveris	Windows	Linux
Įsilaužėlis	y,y,y	y,y,n	n,n,n	n,n,n
IIS_Serveris	y,n,n	y,y,y	y,y,y	y,y,y
Windows	n,n,n	y,y,n	y,y,y	y,y,y
Linux	n,n,n	y,y,n	y,y,y	y,y,y

2.3 lentelėje mes aprašome egzistuojančias ugniasienės taisykles ir fizinius tinklo ryšius. Pradinėje būsenoje įsilaužėlis gali pasiekti tik Web serverį per 80 portą.

IDS

Tinklinio tipo IDS stebi vidinio tinklo srautą. Ryšiai tarp Įsilaužėlis-IIS_serveris ir Linux-Windows nestebimi. Mūsų atveju IDS tikrina tik LICQ veiksmus. IDS apibrėšime kaip matricą. Matricos elemento reikšmė „y“ jeigu kelias tarp h_1 ir h_1 yra stebimas IDS.

2.4 lentelė. IDS duomenys

	Įsilaužėlis	IIS_Serveris	Windows	Linux
Įsilaužėlis	n	n	y	y
IIS_Serveris	n	n	y	y
Windows	y	y	n	n
Linux	y	y	n	n

Veiksmų aibė

Įsilaužėlis gauna administratoriaus teises atakuojamoje sistemoje.

veiksmas IIS_buffer_overflow **yra**
įsilaužėlio pradinė būsena
plvl(Įsilaužėlis) ≥ user *Vartotojo teisės* Įsilaužėlis *kompiuteryje*
plvl(IIS_Serveris) < root *Teisės* IIS_Serveris *serveryje*
tinklo pradinės būsena
$w3svc_{IIS\_Serveris}$ *Serveryje* IIS_Serveris *veikia pažeidžiamas IIS serveris*
C(Įsilaužėlis,Linux,80) *Serveris* IIS_Serveris *pasiekiamas iš* Įsilaužėlis *per 80 portą*
Įsilaužėlio būsena po veiksmo
plvl(T) := root *Administratoriaus lygio teisės serveryje* IIS_Serveris
tinklo būsena po veiksmo
$\neg w3svc_{IIS\_Serveris}$ *Serveryje* IIS_Serveris *sustabdytas IIS servisas*
pabaiga

Leidžia įsilaužėliui skanuoti kaimyninius tinklo kompiuterius.

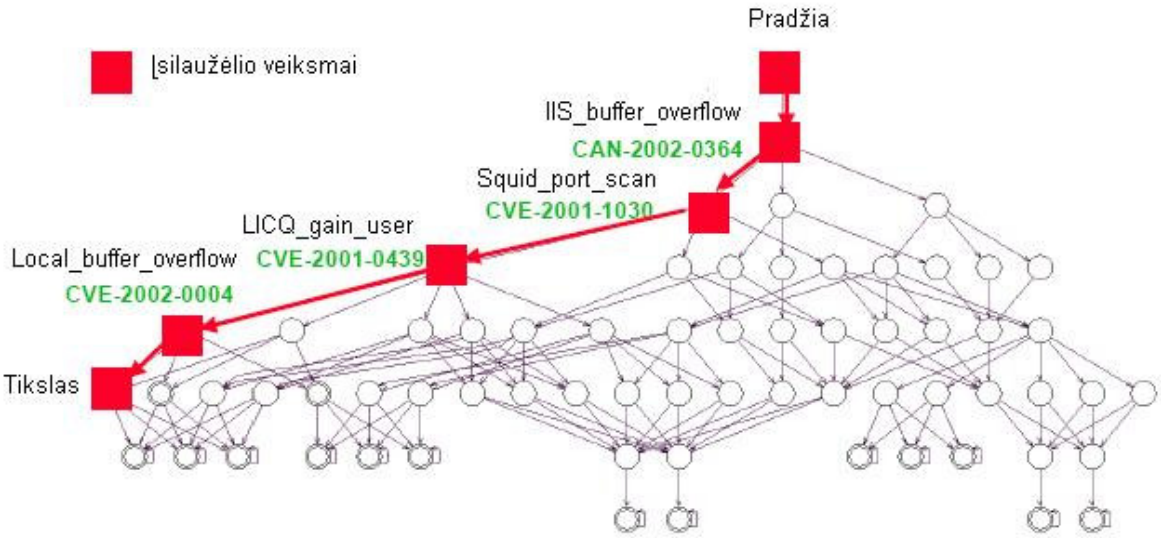
veiksmas squid_port_scan **yra**
įsilaužėlio pradinė būsena
plvl(IIS_Serveris) := root *Administratoriaus lygio teisės* IIS_Serveris *serveryje*
¬scan *Skanavimas dar neatliktas*
tinklo pradinės būsena
$squid_{Linux}$ S*erveryje* Linux *veikia pažeidžiamas Squid servisas*
R(IIS_Serveris, Linux, 80) S*erveris* Linux *pasiekiamas iš* IIS_Serveris *per 80 portą*
Įsilaužėlio būsena po veiksmo
scan *Skanavimas atliktas*
tinklo būsena po veiksmo
Tinklo būsena nepakito
pabaiga

Suteikia įsilaužėliui vartotojo lygio teises atakuojamoje sistemoje.

veiksmas LICQ_gain_user **yra**
įsilaužėlio pradinė būsena
plvl(IIS_Serveris) :=root *Administratoriaus lygio teisės* IIS_Serveris *serveryje*
plvl(Linux) = none *Jokių teisų T kompiuteryje*
scan *Skanavimas atliktas*
tinklo pradinės būsena
$licq_{Linux}$ S*erveryje Linux veikia pažeidžiamas LICQ servisas*
R(S, T, 5190) *Serveris Linux pasiekiamas iš* IIS_Serveris *per 5190 portą*
Įsilaužėlio būsena po veiksmo
plvl(Linux) := user *Vartotojo lygio teisės serveryje* Linux
tinklo būsena po veiksmo
Tinklo būsena nepakito
pabaiga

Suteikia įsilaužėliui administratoriaus teises atakuojamoje sistemoje.

veiksmas Local_buffer_overflow **yra**
įsilaužėlio pradinė būsena
plvl(Linux) = user *Vartotojo lygio teisės* S *kompiuteryje*
tinklo pradinės būsena
$vul\text{-}at_{Linux}$ *Serveryje* Linux *pažeidžiamas* at *procesas*
Įsilaužėlio būsena po veiksmo
plvl(Linux) := root *Administratoriaus lygio teisės serveryje T*
tinklo būsena po veiksmo
Tinklo būsena nepakito
pabaiga

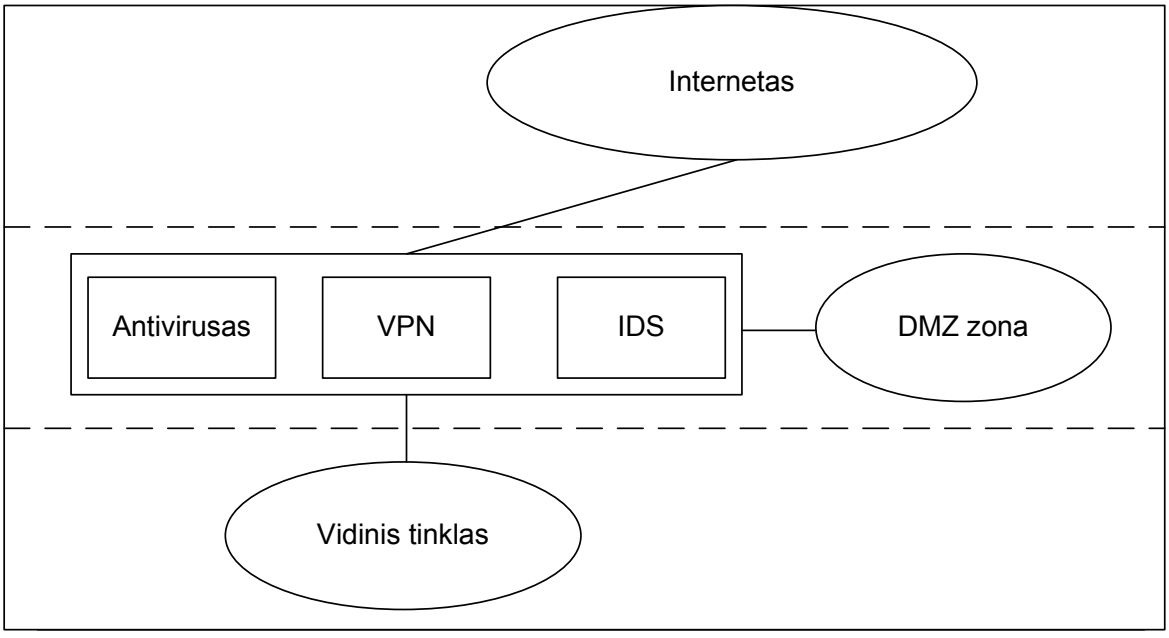


2.2 pav. Atakų medis

Realizavęs visus pažeidžiamumus įsilaužėlis gauna visas teises serveryje Linux. Remiantis šiuo grafu galime projektuoti apsaugos priemones ir tobulinti ugniasienės taisykles.

2.2. Markovo procesų modelis

Naudodamiesi šiuo modeliu aprašysime žemiau pateiktos korporatyvinės įmonės tinklo architektūros modelį.



2.3 pav. Tinklo architektūros pavyzdys

Sudarome modelio tikimybių matricą ir grafą.

	Trust	*Untrust*	*DMZ*	*VPN*	*Antivirusas*	*IDS*	*Pabaiga*
Trust	0	0	0	$p_{0,3}$	$p_{0,4}$	0	$p_{0,6}$
Untrust	0	0	0	$p_{1,3}$	0	$p_{1,5}$	0
DMZ	0	0	0	$p_{2,3}$	$p_{2,4}$	0	$p_{2,6}$
VPN	0	0	0	0	0	0	1
Antivirusas	0	0	0	0	0	0	1
IDS	0	0	0	0	$p_{5,4}$	0	$p_{5,6}$
Pabaiga	0	0	0	0	0	0	1

Būsenos = {Trust, Untrust, DMZ, VPN, Antivirusas, IDS, Pabaiga};

čia Trust – Maršrutizatoriaus sąsaja prie kurios prijungtas vidinis korporatyvinės įmonės tinklas

Untrust - Maršrutizatoriaus sąsaja prie kurios prijungtas išorinis tinklas (Internetas);

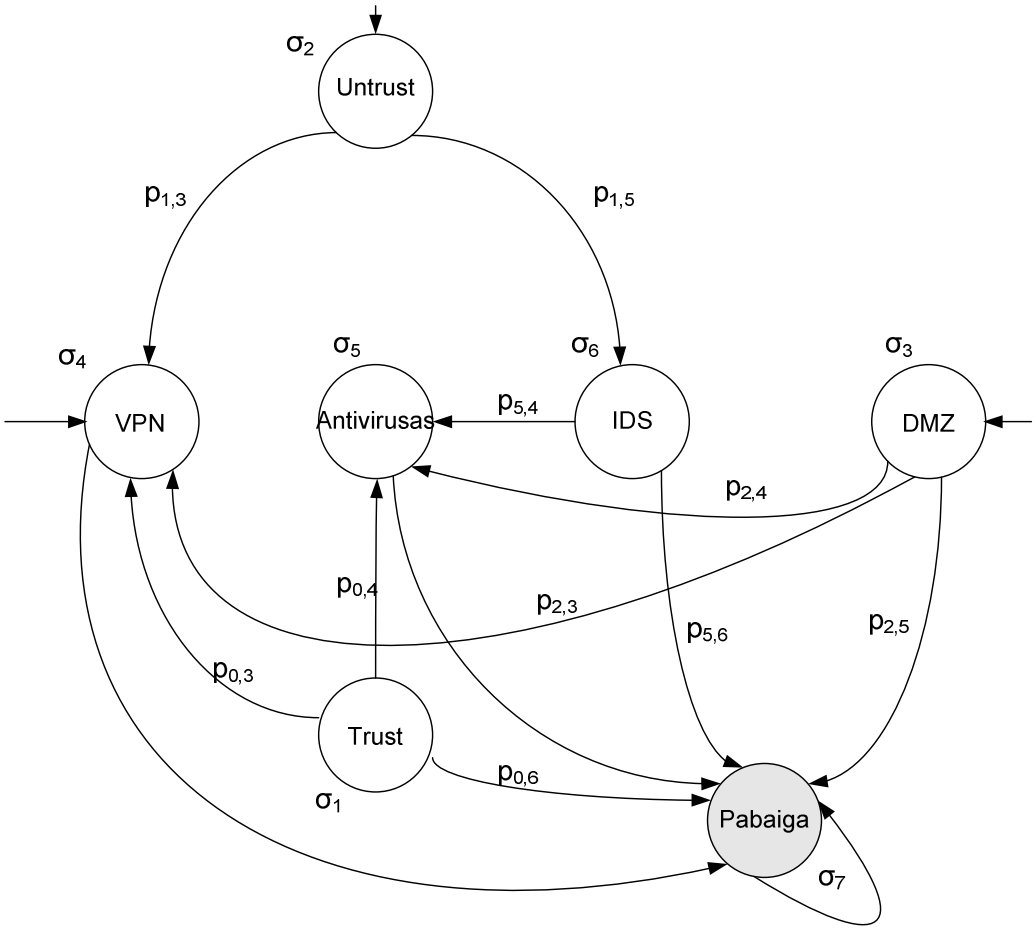
DMZ - Maršrutizatoriaus sąsaja prie kurios prijungtas perimetrinis korporatyvinės įmonės tinklas;

VPN –Virtualaus privataus tinklo duomenų kodavimo modulis;

Antivirusas – Antivirusinis modulis;

IDS – Įsilaužimų aptikimo modulis;

Pabaiga – Galutinė būsena.



2.4 pav. Markovo modelio grafas

Kiekvienos būsenos vėlinimai $\sigma = \{\sigma_1, ..., \sigma_7\}$;

čia σ_1 - Trust sąsajos vėlinimas siunčiant duomenų paketą;

σ_2 - Untrust sąsajos vėlinimas siunčiant duomenų paketą;

σ_3 - Dmz sąsajos vėlinimas siunčiant duomenų paketą;

σ_4 - VPN vėlinimas apdorojant duomenų paketą;

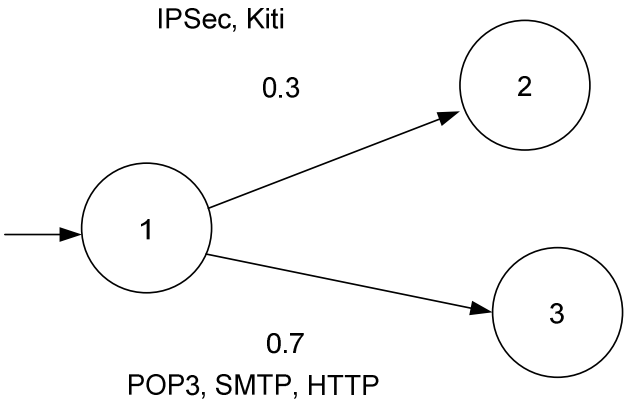
σ_5 - Antiviruso vėlinimas tikrinant duomenų paketą;

σ_6 - IDS vėlinimas tikrinant duomenų paketą;

σ_7 - Paskutinės būsenos vėlinimo dydis nesvarbus;

$p_{0,h} = N_h / N \quad (h = 1,...,H)$; čia N - Paketų skaičius išeinantis iš pradinės būsenos (Trust, Untrust arba DMZ); N_h - vidutinis paketų priklausančių nustatytai protokolų grupei pasirodymo skaičius būsenoje S_h

$p_{0,h}$ parodo tikimybę, kad paketas pereis į sekančią būseną. Modelyje sugrupuojame duomenų srautus pagal protokolus. Priklausomai nuo paketo priklausomybės tam tikram protokolui jis su tikimybe $p_{0,h}$ nukreipiamas į sekančią būseną. Pavyzdžiui:



2.5 pav. Grafo fragmentas

Tikimybė lygi 0.7, kad paketas priklausys (POP3,SMTP,HTTP) grupei. Atitinkamai tikimybė 0.3, kad paketas priklausys kitai grupei. Modeliuojant galima kaitalioti atitinkamas tikimybes ir būsenų vėlinimus, taip gaunant pageidaujamą rezultatą.

Apskaičiuojame sistemos (2.4 pav.) našumą. Pradinę būseną pasirenkame *Untrust*. Sunumeruojame būsenas: Untrust – 1; VPN – 2; IDS – 3; Antivirus – 4; Pabaiga – 5.

$n_1 = 1\sigma_2$;

$n_2 = p_{1,3} n_1 \sigma_4$;

$n_3 = p_{1,5} n_1 \sigma_6$;

$n_4 = p_{5,6} n_3 \sigma_5$

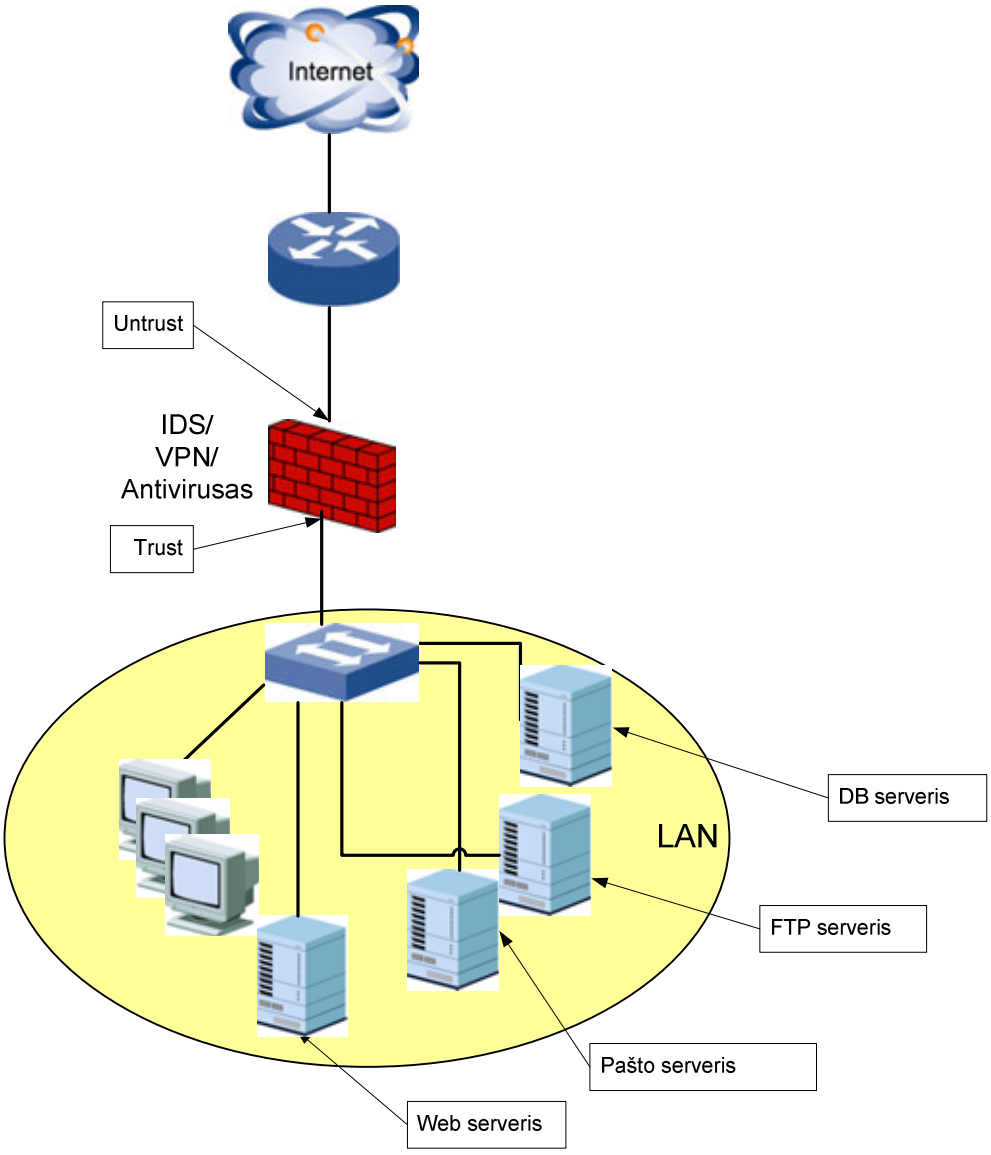
Sistemos našumas (pradinė būsena - *Untrust*) $= n_5 = 1n_4$

2.3. Imitacinis GPSS modelis

Modeliuojamos ir palyginamos dvi skirtingos architektūros. Duomenys parinkti remiantis AB „Snaige“ tinklo stebėjimo rezultatais.

2.3.1. Trust-Untrust architektūros modelis

Ši architektūra sudaryta remiantis maršrutizatoriumi, kuris turi mažiausiai dvi sąsajas. Jis jungia išorinį ir vidinį tinklus. Šiame maršrutizatoriuje yra integruotai antiviruso, IDS ir VPN moduliai. WEB, pašto, FTP serveriai išdėstyti vidiniame tinkle.



2.6 pav. Trust-Untrust architektūra

1. Saugumo priemonių kiekis

NM – 3;

M_1 – IDS; (Atakų aptikimas vykdomas Untrust sąsajoje)

M_2 – VPN;

M_3 – Antivirusas; (Tikrinami: HTTP, POP3, SMTP, FTP protokolai)

2. Tinklo sąsajų kiekis

NI – 2;

I_1 – Trust, čia Trust – sąsaja jungianti vidinį įmonės tinklą su maršrutizatoriumi.

I_2 – Untrust; čia Unrust – sąsaja jungianti interneto tinklą su įmonės maršrutizatoriumi.

3. Duomenų intensyvumas sąsajose I_1, I_2

S_1 – x, čia x – paketo pasirodymo dažnis (ms).

S_2 – y, čia y – paketo pasirodymo dažnis (ms).

4. Tinklo segmentai

T_1 – LAN, čia LAN – vidinis įmonės tinklas.

T_2 – Internetas; čia Internetas – viešas ir nesaugus tinklas, jungiantis korporatyvinės įmonės objektus.

4. Galimi duomenų judėjimo tarp tinklo keliai

2.6 lentelė. Trust-Untrust ugniasienės taisyklės

Iš	Į	Protokolai	Veiksmas
Trust	Untrust	Visi	Leisti
Untrust	Trust	HTTP, SMTP, SSH, FTP, IPSec (VPN)	Leisti

5. Protokolų pasiskirstymas duomenų srautuose ir judėjimo greitis

1 Variantas

Duomenų srautas į Trust sąsają juda 1.1Mbps greičiu (`GENERATE (Exponential(1,0,1.4))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 80% - HTTP;
- 5% - IPSEC (VPN);

- 5% - kiti.

Duomenų srautas į Untrust sąsają juda 2.5Mbps greičiu (`GENERATE (Exponential(1,0,0.64))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 55% - HTTP;
- 5% - FTP;
- 30% - SMTP;
- 10% - IPSEC (VPN).

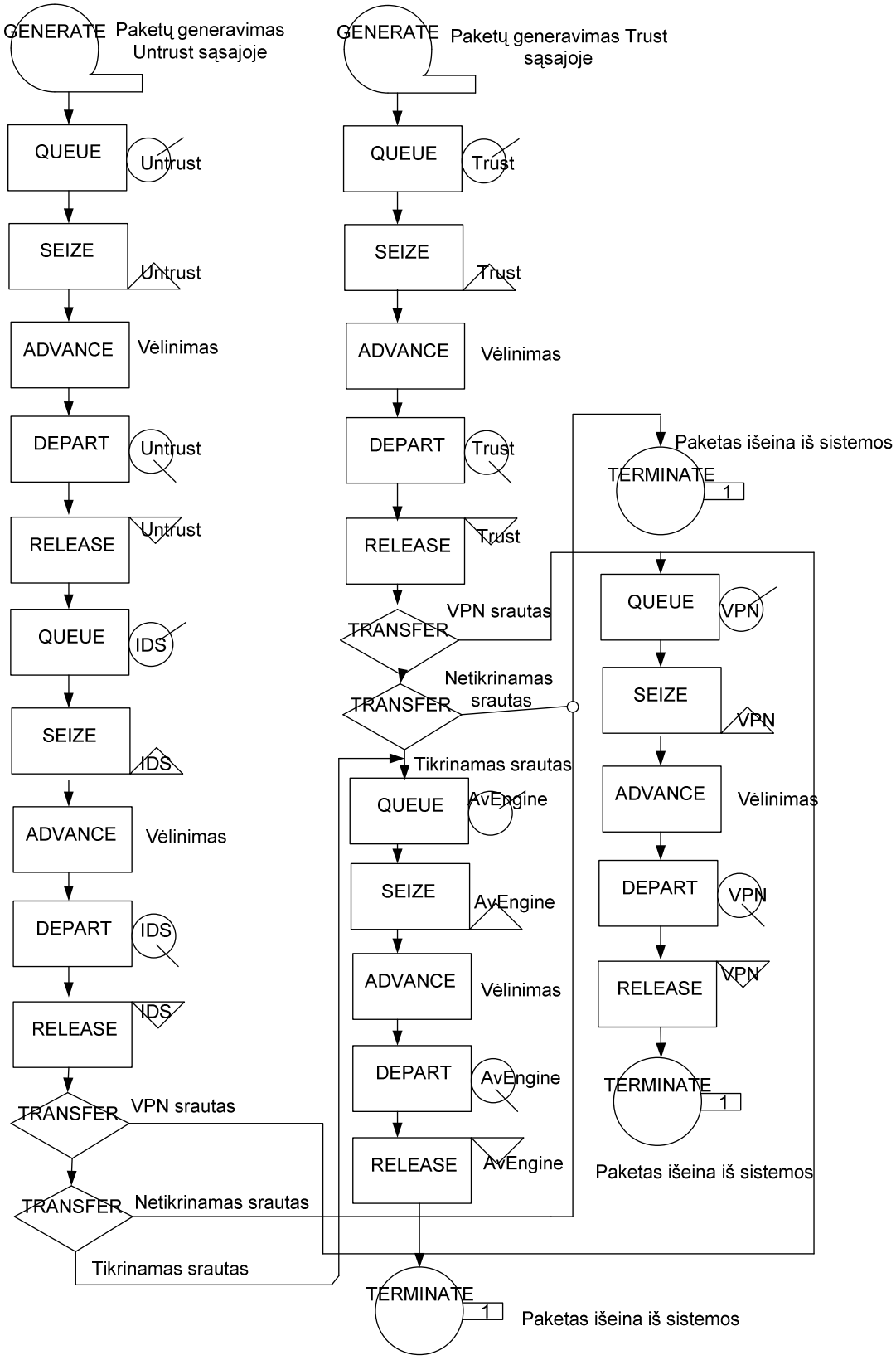
2 Variantas

Duomenų srautas į Trust sąsają juda 2.5Mbps greičiu (`GENERATE (Exponential(1,0,0.64))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 20% - HTTP;
- 50% - SMTP;
- 15% - IPSEC (VPN);
- 15% - kiti;

Duomenų srautas į Untrust sąsają juda 5Mbps greičiu (`GENERATE (Exponential(1,0,0.32))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 20% - HTTP;
- 55% - SMTP;
- 5% - FTP;
- 20% - IPSEC (VPN);



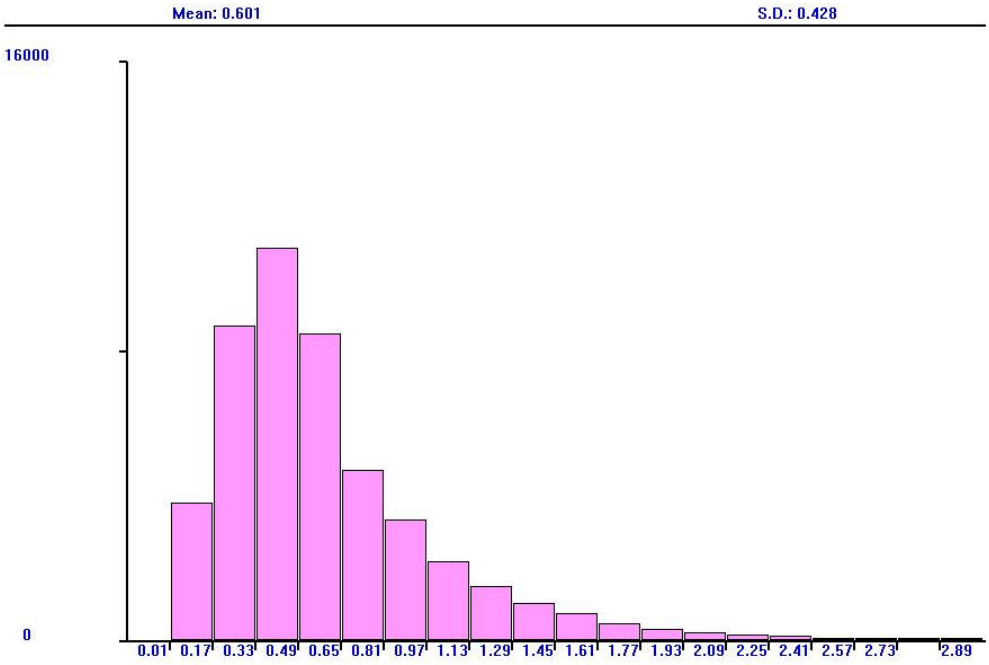
2.7 pav. Trust-Untrust architektūros GPSS modelis

2.3.2. Modeliavimo rezultatai

Šio modelio pavyzdys pateikiamas prieduose (modelis buvo aprašytas GPSS modeliavimo kalba).

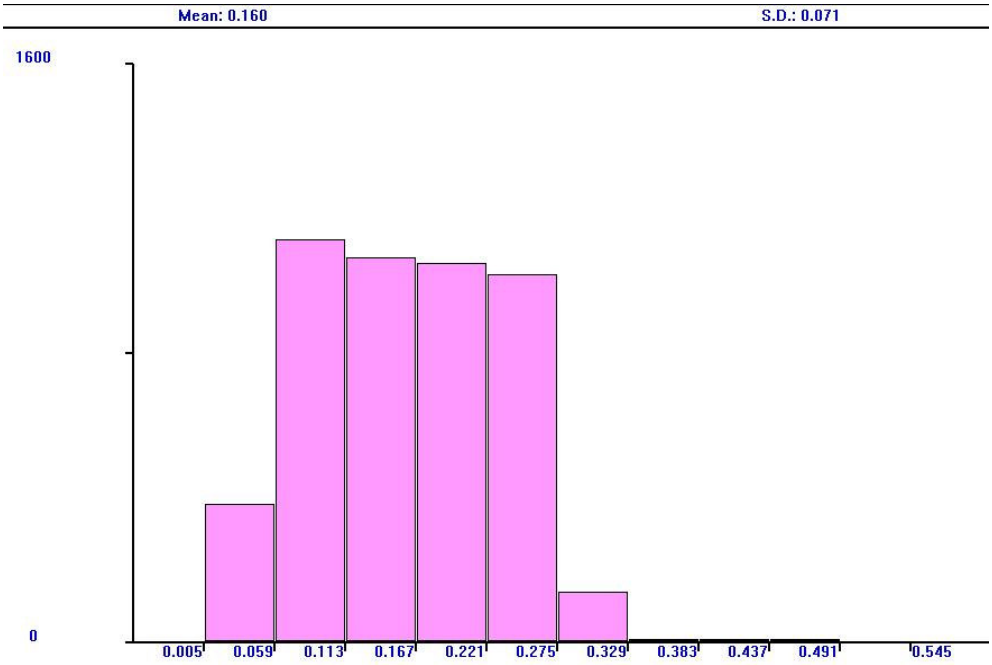
1 Variantas

Pateikti modeliavimo duomenys gauti modeliuojant 39140 paketų Untrust ir 17773 paketų Trust sąsajoje. Modelis parodė, jog esant šiai architektūrai ir duomenų srautams, antiviruso, IDS ir VPN pajėgumų užteks. (planuojamas vidutinis antiviruso apkrovimas 60%, IDS apkrovimas 25%, VPN apkrovimas 3%). Vidutinis paketo patikrinimo laikas antiviruso modulyje yra 0.6ms.



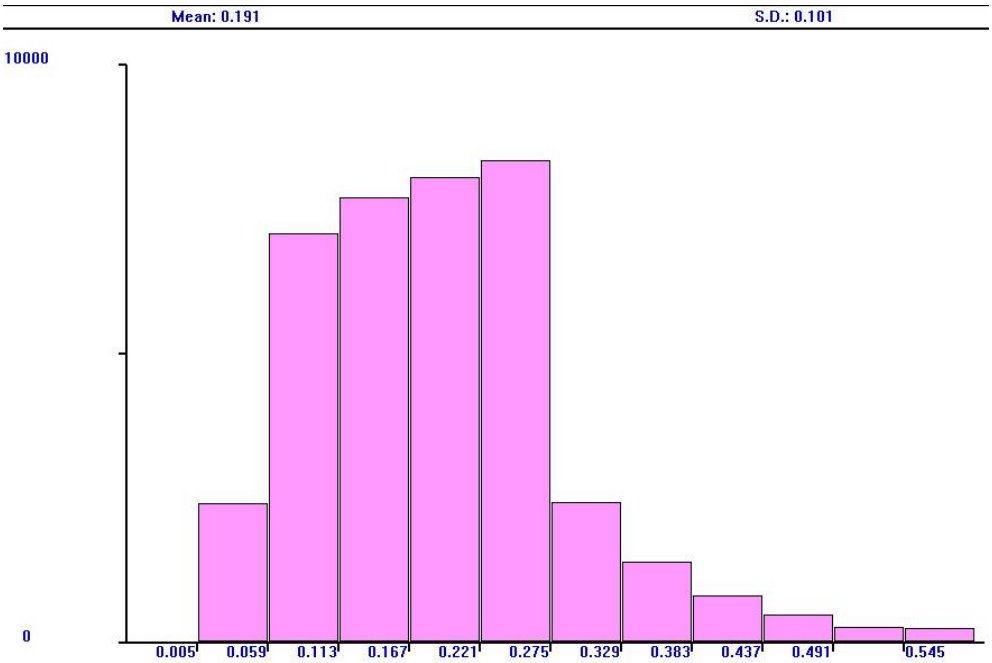
2.8 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms)

Vidutinis paketo kodavimo laikas VPN modulyje yra 0.16ms.



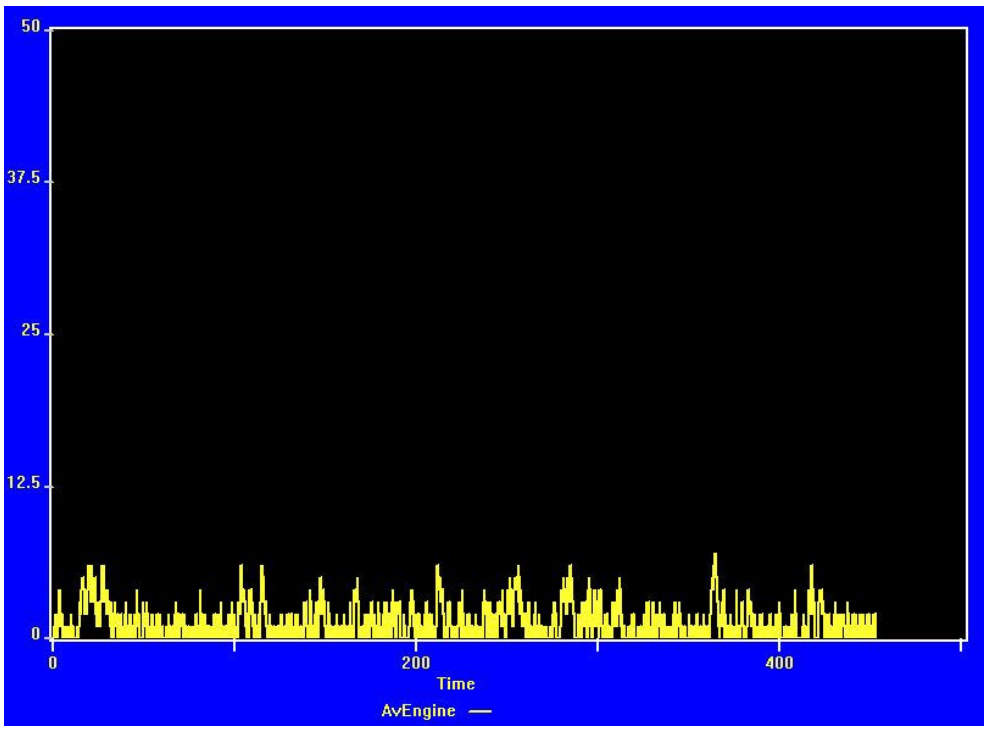
2.9 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms)

Vidutinis paketo tikrinimo laikas IDS modulyje yra 0.19ms.



2.10 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms)

Kaip matome grafike (2.11 pav.) nesusidaro paketų kamščiai antivirusiniame modulyje. Maksimalus, laukiančių patikrinimo, paketų kiekis 10.

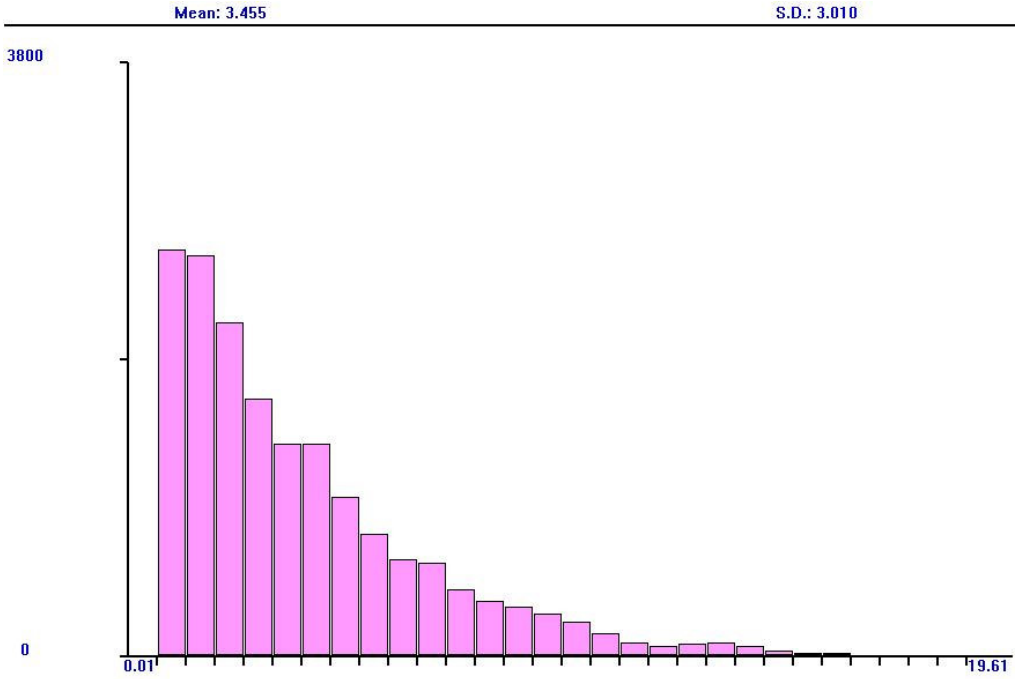


2.11 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje

Tokios konfigūracijos turi pakakti analizuojamiems duomenų srautams, tačiau ateityje atsirasiančius naujus duomenų srautus reiktų nukreipti į naujus antiviruso modulius arba padidinti esančio modulio galingumą.

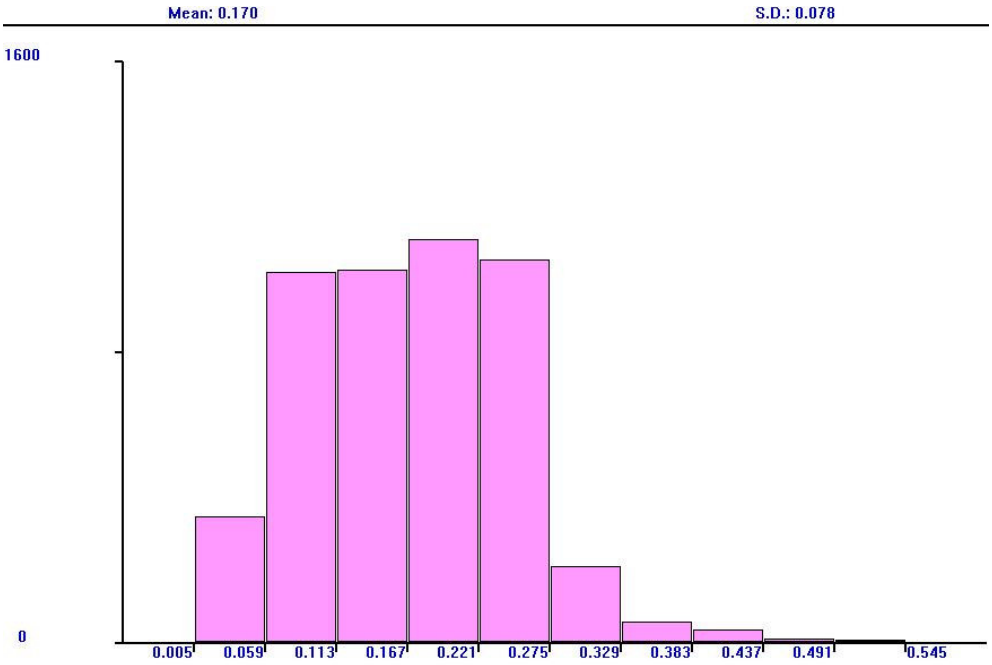
2 Variantas

Pateikti modeliavimo duomenys gauti modeliuojant 17858 paketų Untrust ir 8960 paketų Trust sąsajoje. Antivirusinis modulis apkraunamas 94%. Maksimalus antiviruso patikrinamas srautas 5Mbps. Kaip matome iš grafiko (2.12 pav) vidutinis paketo tikrinimo laikas 3.45ms.



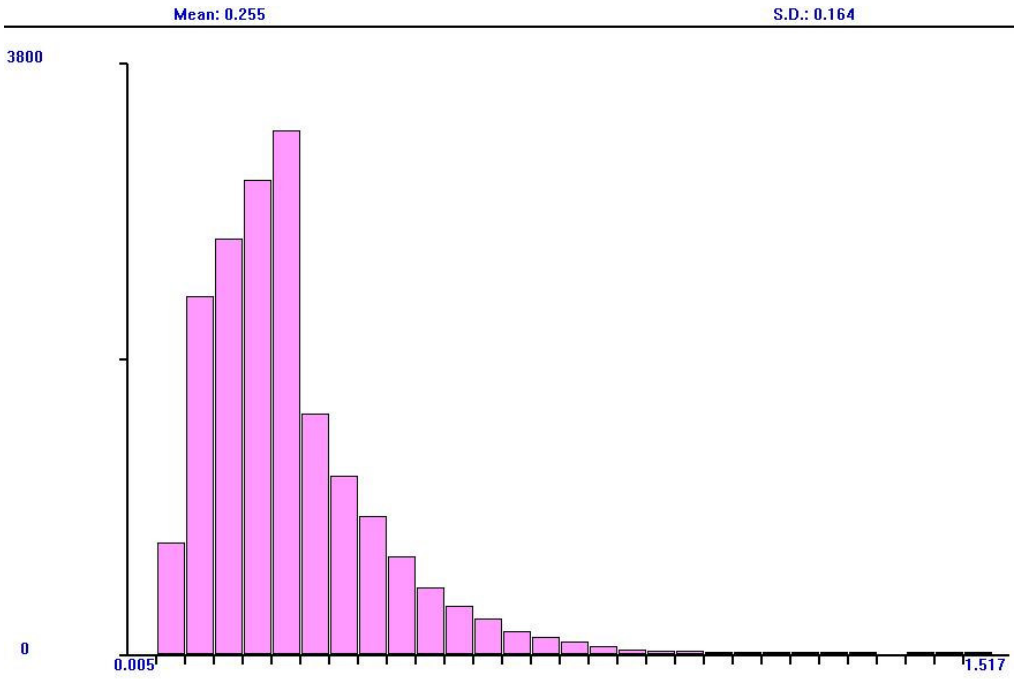
2.12 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms)

VPN duomenų srautai keliauja tarp įmonės padalinių ir yra nesudėtingai kontroliuojami, todėl nekyla VPN modulio apkrovimo problemų.



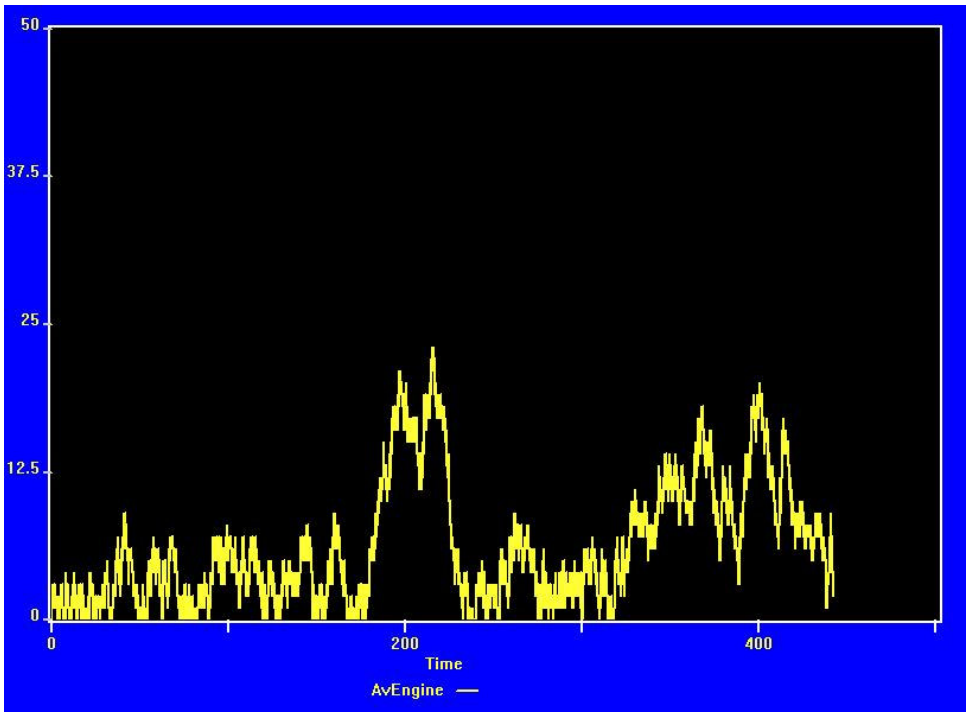
2.13 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms)

IDS modulio maksimalus pralaidumas 10Mbps. IDS tikrina duomenų srautą ateinantį iš išorės. Išorinis interneto greitis yra ribojamas interneto paslaugų tiekėjo, todėl jis neviršija 10Mbps.



2.14 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms)

Kaip matome grafike (2.15 pav.) nesusidaro paketų kamščiai antivirusiniame modulyje. Maksimalus, laukiančių patikrinimo, paketų kiekis 25.



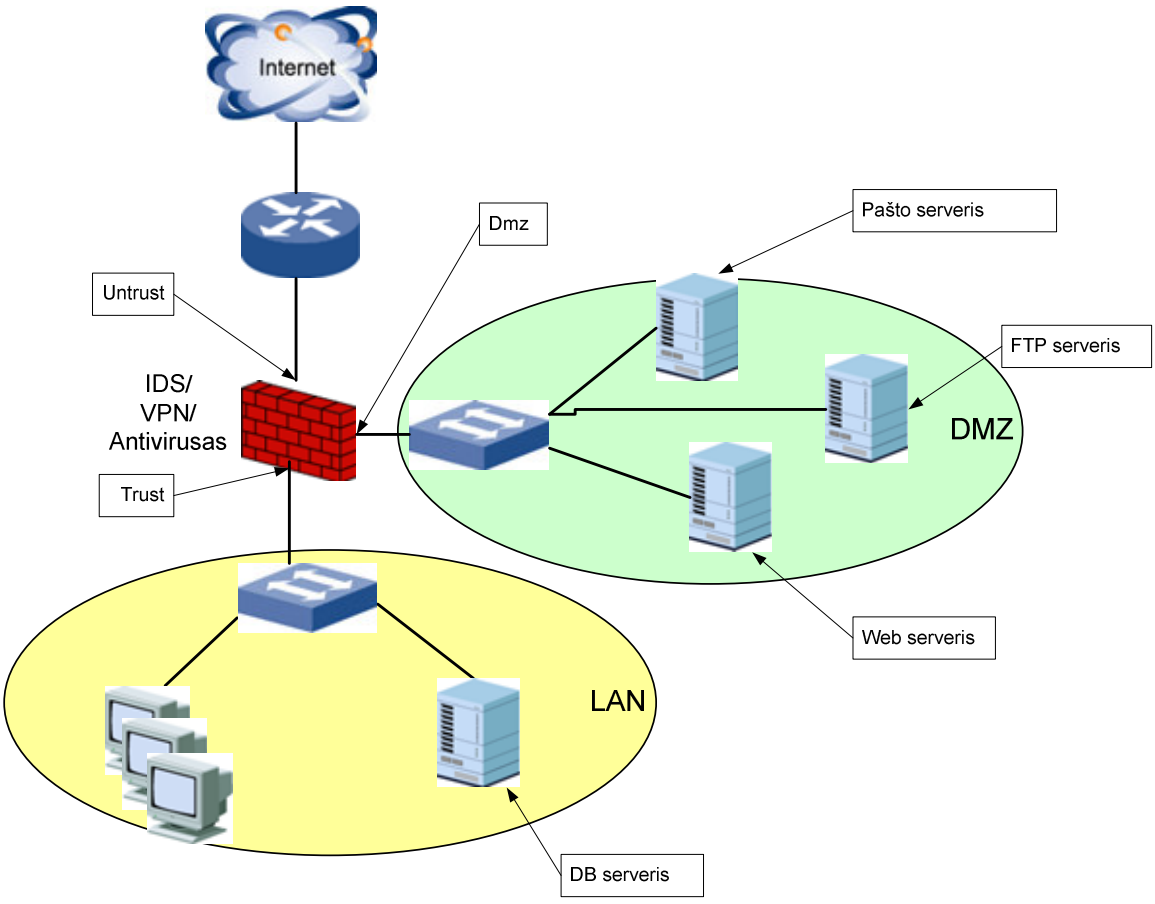
2.15 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje

Šiuo atveju matyti, kad antivirusinio modulio pajėgumai yra beveik maksimaliai išnaudojami. Norint nenutraukti duomenų srauto dėl antiviruso modulio nepakankamumo

reikėtų arba padidinti antiviruso galingumą arba keisti duomenų tikrinimo taisykles. Galima būtų netikrinti viso išeinančio srauto arba netikrinti HTTP protokolo srauto.

2.3.3. Trust-Untrust-Dmz architektūra

Šio tipo architektūra prideda vieną papildomą apsaugos sluoksnį, papildant ją DMZ tinklu, kuris izoliuoja vidinį tinklą nuo Interneto. DMZ zonoje patalpinami Web, FTP, Mail servisai. Jei įsilaužėlis patenka į DMZ zoną, šis sluoksnis užtikrina, kad nebus patekta į vidinį įmonės tinklą. Ši architektūra realizuojama panaudojant maršrutizatorių su integruotais antiviruso, IDS ir VPN modulius.



2.16 pav. Trust-Untrust-DMZ architektūra

1. Saugumo moduliai

NM - 3

M_1 – IDS; (Atakų aptikimas vykdomas Untrust sąsajoje)

M_2 – VPN;

M_3 – Antivirusas; (Tikrinami: HTTP, POP3, SMTP, FTP protokolai)

2. Tinklo sąsajų kiekis

NI – 3

I_1 – Trust, čia Trust – sąsaja jungianti vidinį įmonės tinklą su maršrutizatoriumi.
I_2 – Untrust, čia Unrust – sąsaja jungianti interneto tinklą su įmonės maršrutizatoriumi.
I_3 – DMZ;

3. Duomenų intensyvumas sąsajose I_1, I_2, I_3.

S_1 – x, čia x – paketo pasirodymo dažnis (ms).
S_2 – y, čia y – paketo pasirodymo dažnis (ms).
S_3 – z;, čia z – paketo pasirodymo dažnis (ms).

4. Tinklo segmentai

T_1 – LAN, čia LAN – vidinis įmonės tinklas.
T_2 – Internetas, čia Internetas – viešas ir nesaugus tinklas, jungiantis korporatyvinės įmonės objektus.
T_3 – DMZ, čia DMZ – perimetrinis tinklas.

5. Galimi duomenų judėjimo tarp tinklo keliai

2.7 lentelė. Trust-Untrust-Dmz ugniasienės taisyklės

Iš	Į	Protokolai	Veiksmas
Trust	Untrust	Visi	Leisti
Trust	DMZ	HTTP, POP3, SMTP, FTP, SSH	Leisti
DMZ	Trust	-	Leisti
DMZ	Untrust	SMTP, DNS	Leisti
Untrust	Trust	IPSec (VPN)	Leisti
Untrust	DMZ	HTTP, SMTP, IPSec (VPN)	Leisti

6. Protokolų pasiskirstymas duomenų srautuose ir judėjimo greitis

1. Variantas

Duomenų srautas į Trust sąsają juda 3.5Mbps greičiu (`GENERATE (Exponential(1,0,0.45))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 30% - HTTP;
- 30% - FTP;
- 15% - POP3 ir SMTP;
- 5% - IPSEC (VPN);
- 10% - kiti;

Duomenų srautas į Untrust sąsają juda 2.5Mbps greičiu (`GENERATE (Exponential(1,0,0.64))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 60% - HTTP;
- 30% - SMTP;
- 10% - IPSEC (VPN);

Duomenų srautas į DMZ sąsają juda 0.1Mbps greičiu (`GENERATE (Exponential(1,0,16))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 99% - SMTP;
- 1% - DNS;

2. Variantas

Duomenų srautas į Trust sąsają juda 2.5Mbps greičiu (`GENERATE (Exponential(1,0,0.64))`). Protokolai duomenų sraute pasiskirstę sekančiai:

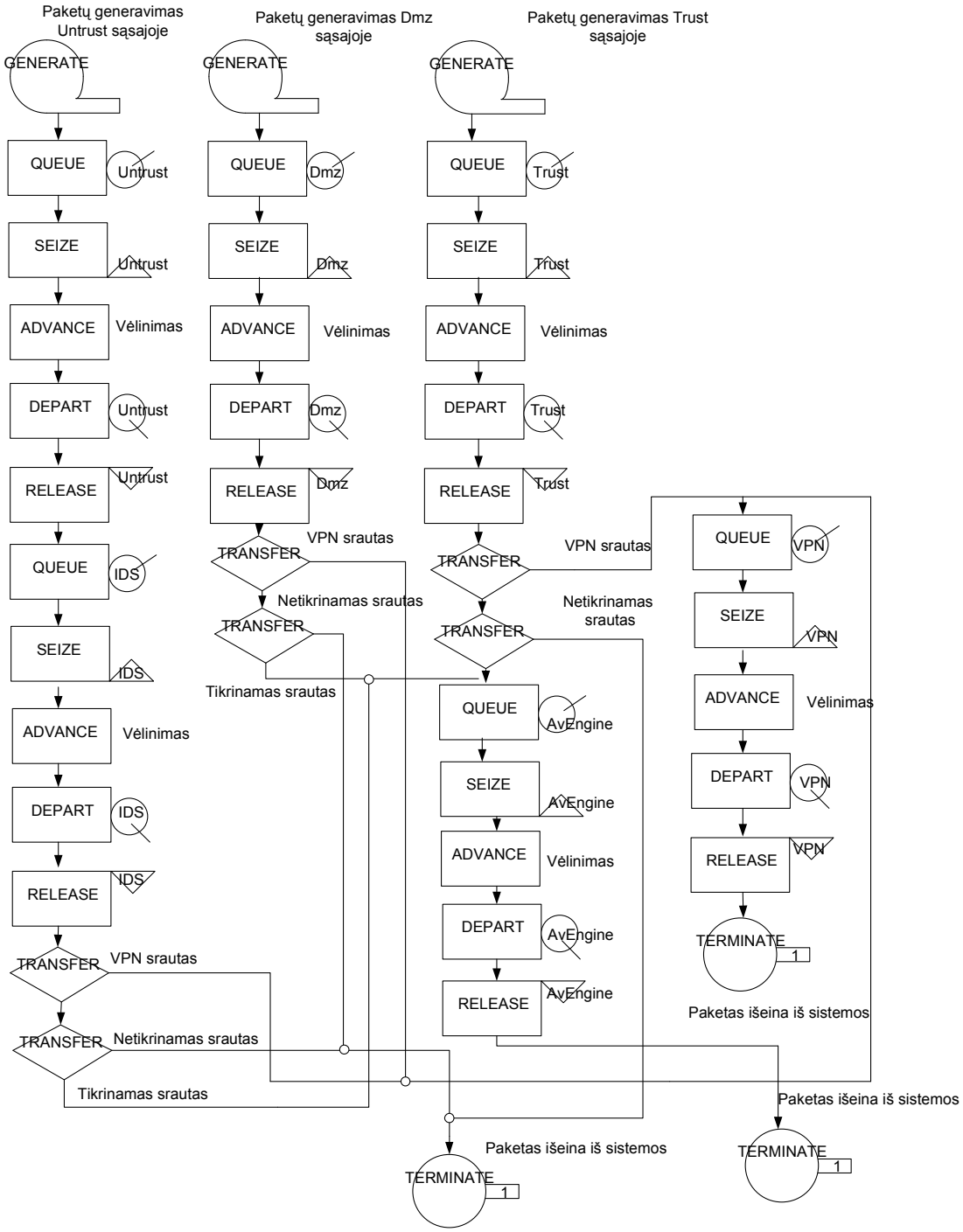
- 40% - HTTP;
- 40% - POP3 ir SMTP;
- 5% - IPSEC (VPN);
- 15% - kiti;

Duomenų srautas į Untrust sąsają juda 5Mbps greičiu (`GENERATE (Exponential(1,0,0.32))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 10% - HTTP;
- 85% - SMTP;
- 5% - IPSEC (VPN);

Duomenų srautas į DMZ sąsają juda 1Mbps greičiu (`GENERATE (Exponential(1,0,1.6))`). Protokolai duomenų sraute pasiskirstę sekančiai:

- 99% - SMTP;
- 1% - DNS;



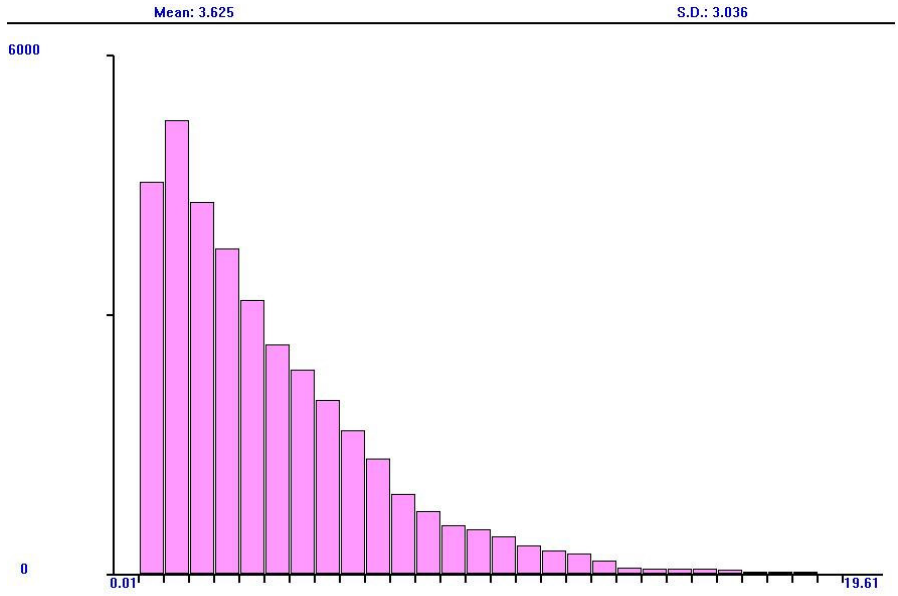
2.17 pav. Trust-Untrust-DMZ architektūros GPSS modelis

2.3.4. Modeliavimo rezultatai

Šio modelio pavyzdys pateikiamas prieduose (modelis buvo aprašytas GPSS modeliavimo kalba).

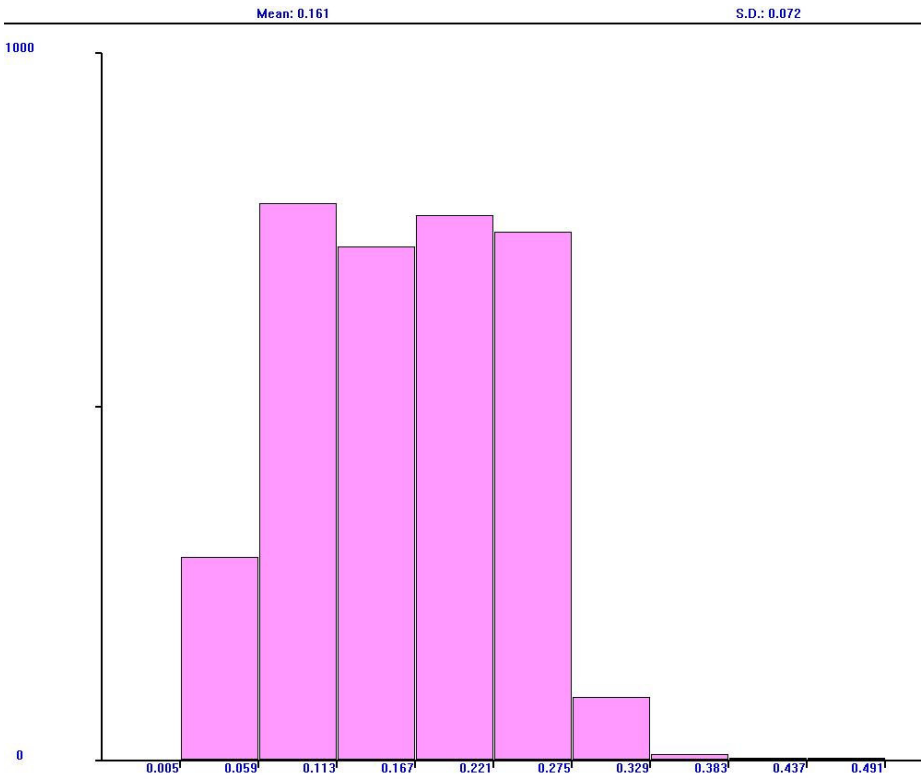
1 Variantas

Pateikti modeliavimo duomenys gauti modeliuojant 18706 paketų Untrust, 26139 paketų Trust sąsajoje ir 784 paketų Dmz sąsajoje. Modelis parodė, jog esant šiai architektūrai ir duomenų srautams, antiviruso, IDS ir VPN pajėgumų užteks. (planuojamas vidutinis antiviruso apkrovimas 95%, IDS apkrovimas 25%, VPN apkrovimas 2%). Vidutinis paketo patikrinimo laikas antiviruso modulyje yra 3.62ms.



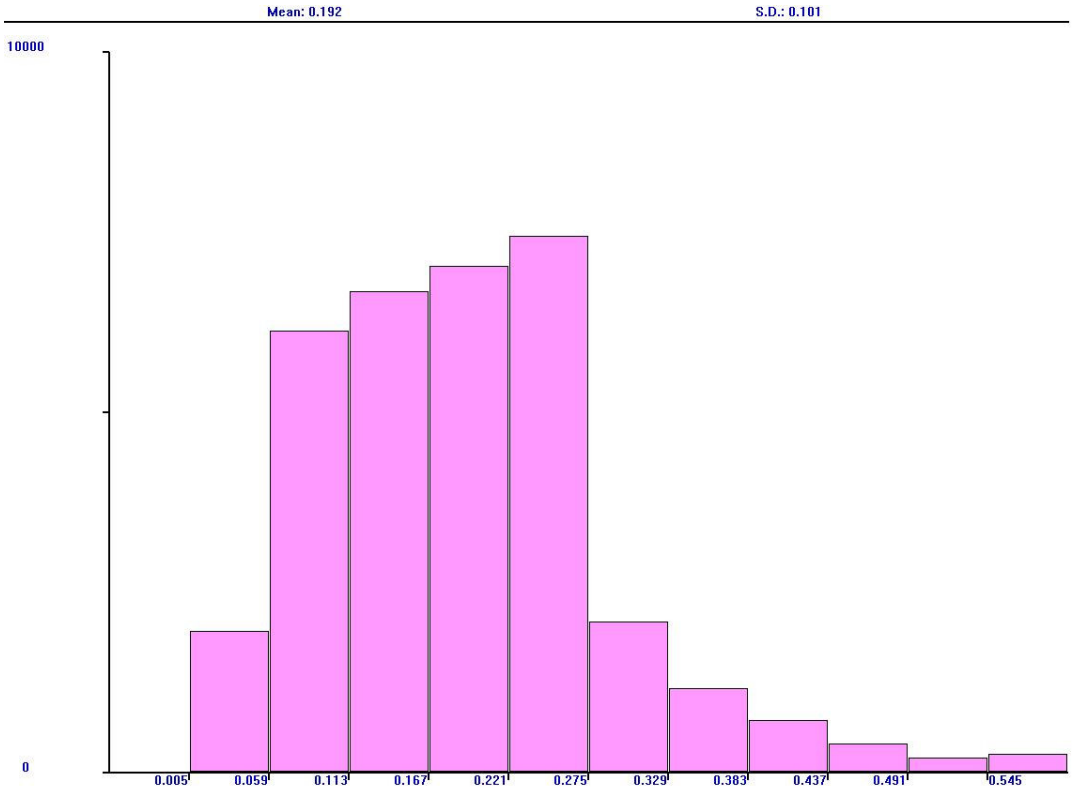
2.18 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms)

Vidutinis paketo kodavimo laikas VPN modulyje yra 0.192ms. Tas sudaro 2% įrenginio resursų panaudojimą.

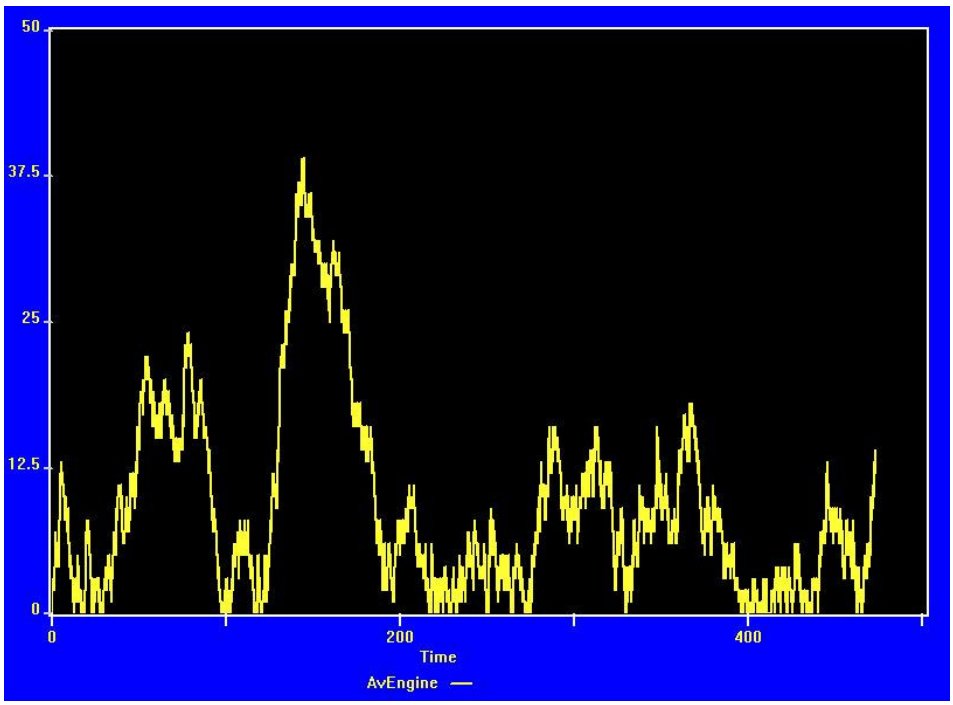


2.19 pav. Paketo patikrinimo laiko pasiskirstymas VPN modulyje (ms)

Duomenys į Untrust sąsają juda 2.5Mbps greičiu, todėl IDS modulio apkrovimas 24% (tikrinamas visas srautas patenkantis į Untrust sąsają).



2.20 pav. Paketo kodavimo laiko pasiskirstymas IDS modulyje (ms)

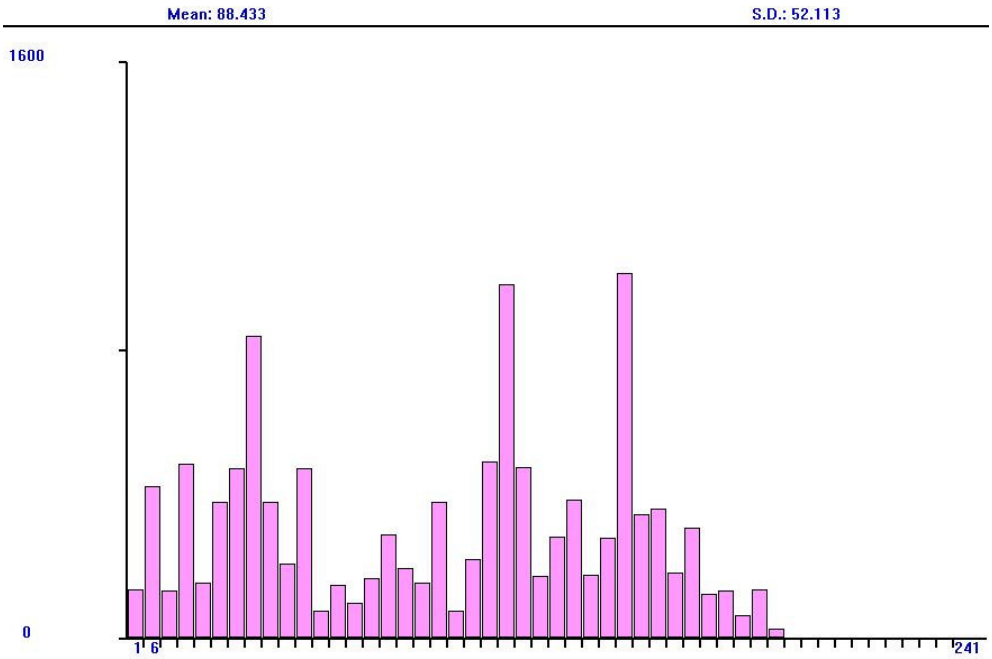


2.21 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje

Prie 95% antiviruso resursų išnaudojimo nesusidaro duomenų kamščiai. Maksimalus, laukiančių patikrinimo, paketų kiekis 38.

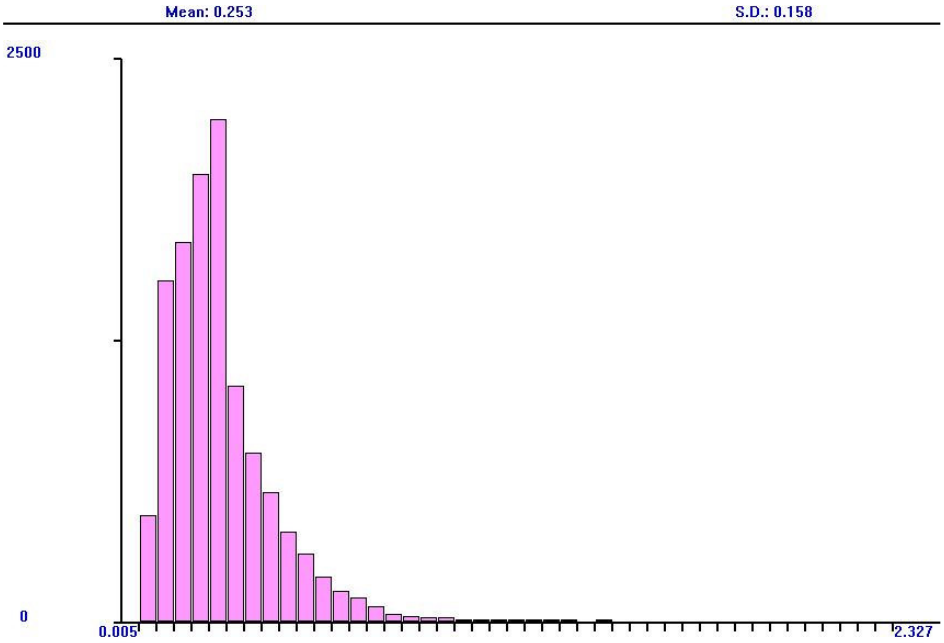
2 Variantas

Pateikti modeliavimo duomenys gauti modeliuojant 19620 paketų Untrust, 3929 paketų Trust sąsajoje ir 2633 paketų Dmz sąsajoje.. Antivirusinos modulis apkraunamas maksimaliai 100%. Tikrinamų duomenų srautas modelyje 10.11Mbps. Šiuo atveju nepakanka antiviruso resursų. Duomenų apdorojimo laikas tiesiškai auga.



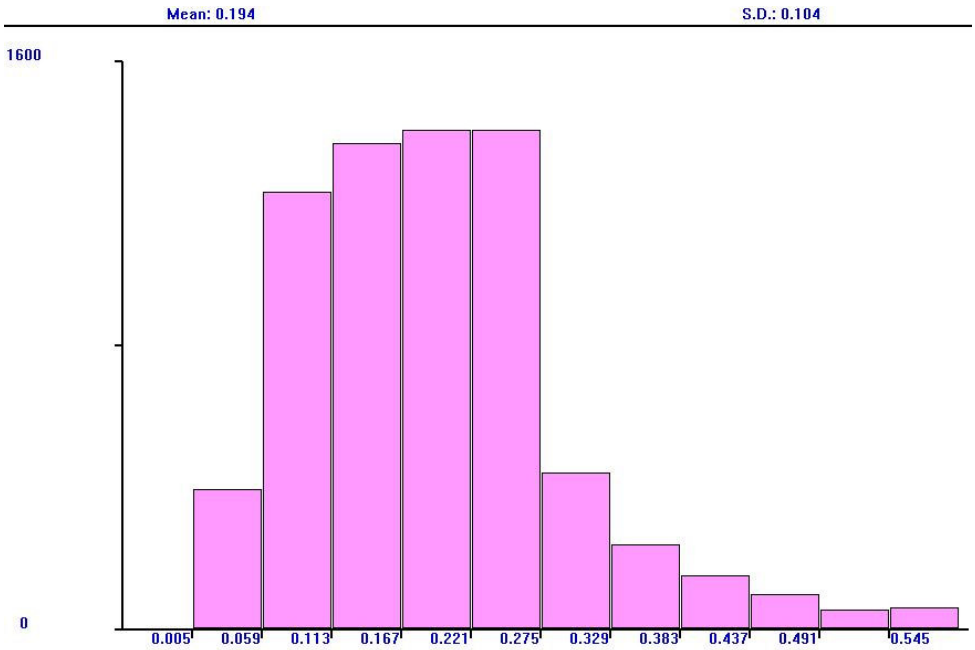
2.22 pav. Paketo patikrinimo laiko pasiskirstymas antiviruso modulyje (ms)

Duomenys į Untrust sąsają juda 7.5Mbps greičiu, todėl IDS modulio apkrovimas 76% (tikrinamas visas srautas patenkantis į Untrust sąsają).

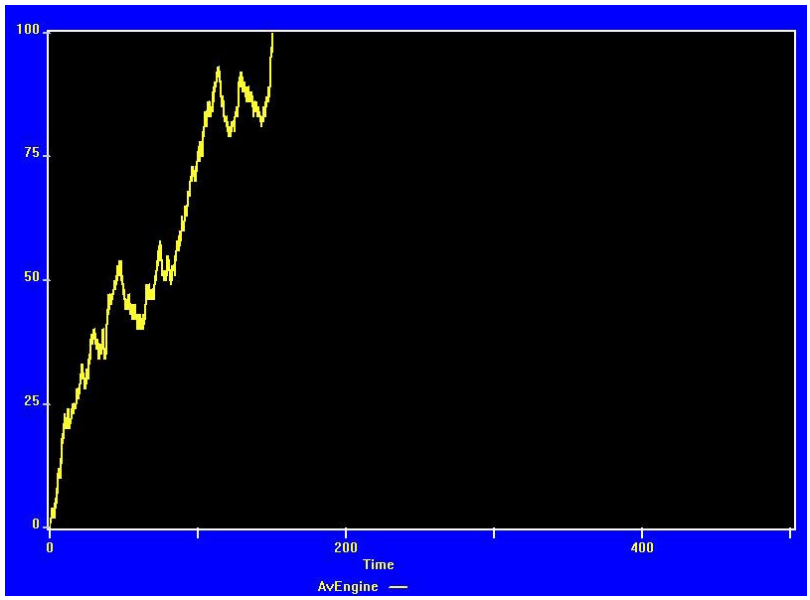


1.23 pav. Paketo patikrinimo laiko pasiskirstymas IDS modulyje (ms)

VPN modulis išnaudojamas 28%, todėl jo paketų apdorojimo laikas pasiskirstęs eksponentiškai.



2.24 pav. Paketo kodavimo laiko pasiskirstymas VPN modulyje (ms)

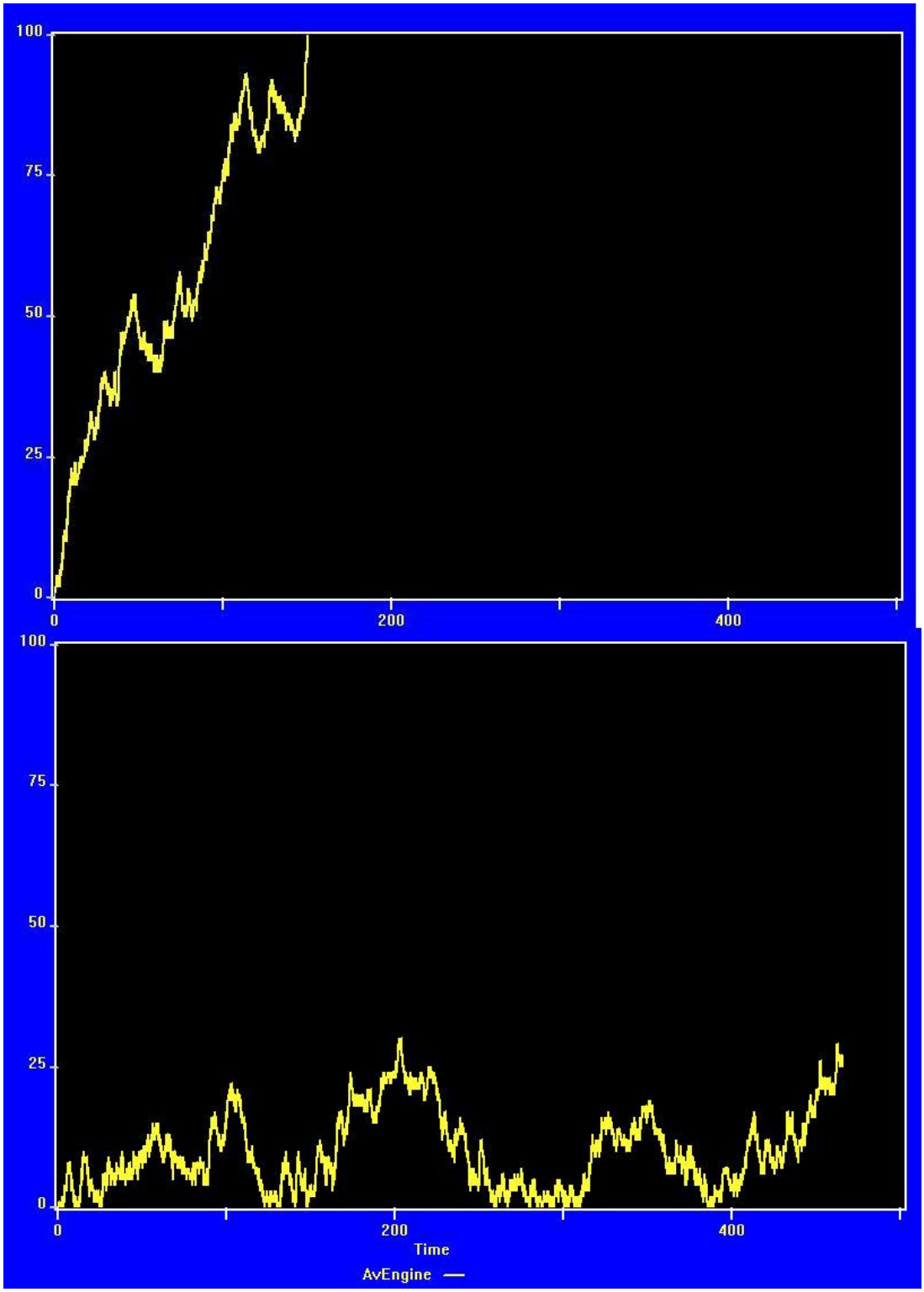


2.25 pav. Paketų eilė laukiančių patikrinimo antiviruso modulyje

Esant tokiems pradiniams duomenims matome, kad antiviruso modulis yra nepajėgus apdoroti modeliuojamų duomenų srautų. Šis antivirusinio modulio apkrovimas susidarė dėl duomenų tikrinimo tarp Trust ir Dmz zonų. Susidarė papildomas 3.5Mbps srautas kertantis Trust-Dmz saugumo zonas (2.4Mbps – FTP, 1Mbps – SMTP, 0.1Mbps – HTTP). Mūsų nagrinėjamu atvejų reikėtų iškelti FTP serverį į Trust zoną, nes serveris yra naudojamas tik įmonės privačiame tinkle ir gali būti pasiekiamas per VPN iš kitų padalinių.

Perkeliame FTP serverį į Trust zoną ir palyginame rezultatus su ankstesniu rezultatu (2.26 pav.). Matome, kad antiviruso darbas stabilizavosi ir nesusidaro augančios

eilės. Saugumo požiūriu saugesnė yra Trust-Untrust-Dmz architektūra nei Trust-Untrust, tačiau jai reikalingos ir našesnės informacinės saugos priemonės.



2.26 pav. Paketų eilių antiviruso modulyje palyginimas

IŠVADOS

Šiame darbe analizuota korporatyvinės įmonės tinklinio sujungimo būdai, informacinės saugos sistemos elementai. Buvo sudaromi ir nagrinėjami korporatyvinių įmonių informacinės saugos sistemų modeliai: atakų medžiai, Markovo grafas, imitacinis GPSS modelis.

- atakų medžių modelis leidžia aptikti modeliuojamos sistemos silpnas vietas, tačiau jo realizacija gana sudėtinga, nes sunku įvertinti visus korporatyvinėje įmonėje egzistuojančius pažeidžiamumus. Šiuo metodu negalime įvertinti kiekybinių saugos priemonių parametrų;
- Markovo procesų modelis leidžia kiekybiškai įvertinti nagrinėjamos architektūros informacinės saugos sistemos našumą. Parinkus grafo parametrus išrenkama optimali sistema pagal duomenų pasiskirstymą ir apdorojimo trukmės kriterijus;
- Imitacinis modelis naudingas tiek parenkant fizinius korporatyvinės įmonės saugos elementų parametrus, tiek modeliuojant duomenų srautus.

Įvertinus visa tai rekomenduojama:

- panaudojant atakų grafą nustatyti silpnas saugumo požiūriu korporatyvinės įmonės sistemas. Jų pagrindu suformuoti saugumo zonas su atitinkamomis duomenų srautų taisyklėmis ir parinkti informacinės saugos elementų išdėstymo vietas korporatyvinės įmonės tinklų topologijoje;
- informacinės saugos elementų parametrų nustatymui naudoti imitacinį GPSS modelį,. modeliuojant duomenų srautų judėjimą korporatyvinės įmonės tinkle.
- Išdėstyti serverius saugumo zonose taip, kad būtų kuo mažesni duomenų srautai tarp skirtingų zonų.

Paruoštas pranešimas „Dvyliktajai tarptautinei mokslinei kompiuterininkų konferencijai“, kuri vyks „Kompiuterininkų dienose – 2005“, 2005 m. rugsėjo 15–17 d. Klaipėdoje, Klaipėdos universitete ir straipsnis, kuris įteiktas specialiam žurnalo „Informacijos mokslai“ numeriui. Priedas Nr. 3.

LITERATŪRA

[1] Designing Network Architectures that Offer Competitive Advantages. [interaktyvus] 2004, liepa [žiūrėta 2005-05-07] Prieiga per internetą: http://www.synopsys.com/news/pubs/compiler/art1lead_dnetwork-sep03.html

[2] Network architectures, technologies and protocols. [interaktyvus] 2003, sausis [žiūrėta 2005-05-07] Prieiga per internetą: http://www.wtec.org/loyola/satcom2/04_04.htm

[3] IEEE 802.3 CSMA/CD (ETHERNET). [interaktyvus] 2005, gegužė [žiūrėta 2005-05-07] Prieiga per internetą: http://www.ieee802.org/3/

[4] Network interfaces, hubs, switches, bridges, routers, and firewalls. [interaktyvus] 1999, rugsėjis [žiūrėta 2005-05-05] Prieiga per internetą: http://www2.edc.org/cope/networkprimer/primch5.pdf

[5] Leased Lines and Private Networks. [interaktyvus] 2005, kovas [žiūrėta 2005-05-05] Prieiga per internetą: http://www.flexwork.eu.com/members/tech_brief/tb20.pdf

[6] Frame Relay and ATM WAN Technology. [interaktyvus] 2000, sausis [žiūrėta 2005-05-05] Prieiga per internetą: http://www.mcoecn.org/whitepapers/cisco-frame-relay-atm-technology.pdf

[7] VPN: The Basics. [interaktyvus] 1998, gruodis [žiūrėta 2005-05-05] Prieiga per internetą: http://www.internetweek.com/VPN/paper-4.htm

[8] Panda GateDefender. [interaktyvus] 2005, gegužė [žiūrėta 2005-05-05] Prieiga per internetą: http://enterprises.pandasoftware.com/products/gatedefender/

[9] Firewall Architecture. [interaktyvus] 2001, birželis [žiūrėta 2005-05-05] Prieiga per internetą: www.nextep.com.au/upload/Firewall_Architecture.pdf

[10] Priorities in The Deployment of Network Intrusion Detection Systems. [interaktyvus] 2002, kovas [žiūrėta 2005-05-05] Prieiga per internetą: www.tml.hut.fi/~tpv/opiskelijat/dobrucki.pdf

[11] Virtual Private Network Design. [interaktyvus] 2002, kovas [žiūrėta 2005-05-05] Prieiga per internetą: www.ins.com/downloads/whitepapers/ ins_white_paper_vpn_design_0301.pdf

[12] An Enterprise Network Security Framework [interaktyvus] 2004, gegužė [žiūrėta 2005-04-22] Prieiga per internetą: http://www1.avaya.com/enterprise/whitepapers/pc/lippiswp_052004.pdf

[13] Deepak K. Enterprise Network Design. Toronto: Sun Blueprints, 2003.

[14] The Formal Analyses of Attack graphs [interaktyvus] 2003 [žiūrėta 2005-04-22]. Prieiga per internetą: http://www.cs.wisc.edu/~jha/jha-papers/security/CSFW_2002_1.pdf

[15] Scenario Graphs and Attack Graphs. [interaktyvus] 2004, balandis [žiūrėta 2005-05-05]. Prieiga per internetą: http://reports-archive.adm.cs.cmu.edu/anon/2004/CMU-CS-04-122.pdf

[16] Markov chains and Markov processes. [interaktyvus] 2005, gegužė [žiūrėta 2005-05-05]. Prieiga per internetą: http://www.win.tue.nl/~iadan/sdp/h3.pdf

[17] GPSS World Reference Manual. [interaktyvus] 2001, vasaris [žiūrėta 2005-05-05]. Prieiga per internetą: http://www.minutemansoftware.com/reference/rpreface.htm

[18] Common Vulnerabilities and Exposures. [interaktyvus] 2005 [žiūrėta 2005-05-05]. Prieiga per internetą: http://www.cve.mitre.org

1 PRIEDAS. Trust-Untrust architektūros aprašas GPSS kalba ir modeliavimo rezultatai

Aprašas GPSS kalba

1 Variantas

```
*************************************************************************************
GENERATE (Exponential(1,0,0.64));Paketu pasirodymu daznis Untrust interfeise (ms) (max
2.5Mbps)
          QUEUE     Untrust      ;Eile Untrust interfeise
          SEIZE     Untrust      ;Untrust uzimtas
          ADVANCE   0.016,0.009 ;Untrust velinimas (pralaidumas) (max 100Mbps)
          DEPART    Untrust      ;Untrust laisvas
          RELEASE   Untrust      ;Siuntimas baigtas
          QUEUE     IDS          ;Eile prie IDS
          SEIZE     IDS          ;IDS uzimtas
          ADVANCE   0.16,0.12   ;IDS paketo tikrinimo laikas (ms) (max 10Mbps)
          DEPART    IDS          ;IDS laisvas
          RELEASE   IDS          ;IDS tikrinimas baigtas
*************************************************************************************
             TRANSFER  .1,,VPNTraffic      ;10% srauto VPN'as
             TRANSFER  .1,AvScan,NoAvScan   ;10% srauto netikrinama
          GENERATE  (Exponential(1,0,1.4));Paketu pasirodymu daznis Trust interfeise (ms)
(max 1.1Mbps)
          QUEUE     Trust               ;Eile Trust interfeise
          SEIZE     Trust               ;Trust uzimtas
          ADVANCE   0.016,0.009         ;Trust velavimas (pralaidumas) max 100Mbps
          DEPART    Trust               ;Trust laisvas
          RELEASE   Trust               ;Siuntimas baigtas
*************************************************************************************
             TRANSFER  .05,,VPNTraffic  ;5% srauto VPN'as
             TRANSFER  .1,,NoAvScan       ;10% srauto netikrinama
          AvScan QUEUE     AvEngine     ;Paketu eile laukianciu antiviruso patikrinimo
          SEIZE AvEngine                ;AvEngine uzimtas
          ADVANCE 0.32,0.24              ;Paketo tikrinimo laikas (ms) (max 5Mbps)
          DEPART AvEngine               ;AvEngine laisvas
          RELEASE AvEngine              ;Paketo patikrinimas baigtas
          TERMINATE                     ;Patikrintas paketas iseina i kita tinkla
          NoAvScan TERMINATE 1          ;Nepatikrintas paketas iseina i kita tinkla
          VPNTraffic QUEUE VPN          ;Eile VPN
          SEIZE     VPN                 ;VPN uzimtas
          ADVANCE  0.16,0.12             ;VPN velinimas (ms) (max 10Mbps)
          DEPART    VPN                 ;VPN laisvas
          RELEASE   VPN                 ;Paketo kodavimas baigtas
          TERMINATE 1                   ;VPNTraffic srautas
*************************************************************************************
WaitTrust QTABLE Trust,0.0001,0.0004,15       ;Apdorojimo laikas Trust interfeise
          WaitUntrust QTABLE Untrust,0.0001,0.0004,15   ;Apdorojimo laikas Untrust
interfeise
          WaitAvEngine QTABLE AvEngine,0.01,0.16,20     ;Apdorojimo laikas AvEngine
          WaitIDS QTABLE IDS,0.005,0.054,12             ;Apdorojimo laikas IDS
          WaitVPN QTABLE VPN,0.005,0.054,12             ;VPN kodavimas
```

2 Variantas

```
*************************************************************************************
GENERATE (Exponential(1,0,0.32));Paketu pasirodymu daznis Untrust interfeise (ms) (max
5Mbps)
          QUEUE     Untrust      ;Eile Untrust interfeise
          SEIZE     Untrust      ;Untrust uzimtas
          ADVANCE   0.016,0.009 ;Untrust velinimas (pralaidumas) (max 100Mbps)
          DEPART    Untrust      ;Untrust laisvas
          RELEASE   Untrust      ;Siuntimas baigtas
          QUEUE     IDS          ;Eile prie IDS
          SEIZE     IDS          ;IDS uzimtas
          ADVANCE   0.16,0.12   ;IDS paketo tikrinimo laikas (ms) (max 10Mbps)
          DEPART    IDS          ;IDS laisvas
          RELEASE   IDS          ;IDS tikrinimas baigtas
*************************************************************************************
             TRANSFER  .2,,VPNTraffic      ;20% srauto VPN'as
```

```
            TRANSFER  .2,AvScan,NoAvScan   ;20% srauto netikrinama
          GENERATE  (Exponential(1,0,0.64));Paketu pasirodymu daznis Trust interfeise (ms)
(max 2.5Mbps)
          QUEUE     Trust               ;Eile Trust interfeise
          SEIZE     Trust               ;Trust uzimtas
          ADVANCE   0.016,0.009         ;Trust velavimas (pralaidumas) max 100Mbps
          DEPART    Trust               ;Trust laisvas
          RELEASE   Trust               ;Siuntimas baigtas
*********************************************************************************
            TRANSFER  .15,,VPNTraffic    ;15% srauto VPN'as
            TRANSFER  .3,,NoAvScan       ;30% srauto netikrinama
          AvScan QUEUE     AvEngine     ;Paketu eile laukianciu antiviruso patikrinimo
          SEIZE AvEngine                ;AvEngine uzimtas
          ADVANCE 0.32,0.24              ;Paketo tikrinimo laikas (ms) (max 5Mbps)
          DEPART AvEngine               ;AvEngine laisvas
          RELEASE AvEngine              ;Paketo patikrinimas baigtas
          TERMINATE                     ;Patikrintas paketas iseina i kita tinkla
          NoAvScan TERMINATE 1          ;Nepatikrintas paketas iseina i kita tinkla
          VPNTraffic QUEUE VPN          ;Eile VPN
          SEIZE     VPN                 ;VPN uzimtas
          ADVANCE  0.16,0.12             ;VPN velinimas (ms) (max 10Mbps)
          DEPART    VPN                 ;VPN laisvas
          RELEASE   VPN                 ;Paketo kodavimas baigtas
          TERMINATE 1                   ;VPNTraffic srautas
*********************************************************************************
WaitTrust QTABLE Trust,0.0001,0.0004,15       ;Apdorojimo laikas Trust interfeise
          WaitUntrust QTABLE Untrust,0.0001,0.0004,15   ;Apdorojimo laikas Untrust
interfeise
          WaitAvEngine QTABLE AvEngine,1,20,50     ;Apdorojimo laikas AvEngine
          WaitIDS QTABLE IDS,0.005,0.054,45            ;Apdorojimo laikas IDS
          WaitVPN QTABLE VPN,0.005,0.054,12            ;VPN kodavimas
```

Modeliavimo rezultatai

1 Variantas

```
              GPSS World Simulation Report - gw11.26.26


                   Wednesday, May 04, 2005 23:49:52

           START TIME           END TIME  BLOCKS  FACILITIES  STORAGES
                0.000          25045.734    34        5          0


              NAME                      VALUE
          AVENGINE                    10005.000
          AVSCAN                         22.000
          IDS                         10007.000
          NOAVSCAN                       28.000
          TRUST                       10001.000
          UNTRUST                     10003.000
          VPN                         10009.000
          VPNTRAFFIC                     29.000
          WAITAVENGINE                10004.000
          WAITIDS                     10006.000
          WAITTRUST                   10000.000
          WAITUNTRUST                 10002.000
          WAITVPN                     10008.000


 LABEL              LOC  BLOCK TYPE     ENTRY COUNT CURRENT COUNT RETRY
                    1    GENERATE         39103             0       0
                    2    QUEUE            39103             0       0
                    3    SEIZE            39103             0       0
                    4    ADVANCE          39103             0       0
                    5    DEPART           39103             0       0
                    6    RELEASE          39103             0       0
                    7    QUEUE            39103             0       0
                    8    SEIZE            39103             0       0
                    9    ADVANCE          39103             0       0
                   10    DEPART           39103             0       0
                   11    RELEASE          39103             0       0
                   12    TRANSFER         39103             0       0
                   13    TRANSFER         35154             0       0
```

	14	GENERATE	17941	0	0
	15	QUEUE	17941	0	0
	16	SEIZE	17941	0	0
	17	ADVANCE	17941	0	0
	18	DEPART	17941	0	0
	19	RELEASE	17941	0	0
	20	TRANSFER	17941	0	0
	21	TRANSFER	17082	0	0
AVSCAN	22	QUEUE	46999	0	0
	23	SEIZE	46999	0	0
	24	ADVANCE	46999	0	0
	25	DEPART	46999	0	0
	26	RELEASE	46999	0	0
	27	TERMINATE	46999	0	0
NOAVSCAN	28	TERMINATE	5237	0	0
VPNTRAFFIC	29	QUEUE	4808	0	0
	30	SEIZE	4808	0	0
	31	ADVANCE	4808	0	0
	32	DEPART	4808	0	0
	33	RELEASE	4808	0	0
	34	TERMINATE	4808	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
TRUST	17941	0.011	0.016	1	0	0	0	0	0
UNTRUST	39103	0.025	0.016	1	0	0	0	0	0
AVENGINE	46999	0.601	0.320	1	0	0	0	0	0
IDS	39103	0.250	0.160	1	0	0	0	0	0
VPN	4808	0.031	0.159	1	0	0	0	0	0

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
TRUST	2	0	17941	0	0.012	0.016	0.016	0
UNTRUST	3	0	39103	0	0.025	0.016	0.016	0
AVENGINE	12	0	46999	0	1.128	0.601	0.601	0
IDS	9	0	39103	0	0.300	0.192	0.192	0
VPN	3	0	4808	0	0.031	0.161	0.161	0

TABLE	MEAN	STD.DEV.	RANGE			RETRY	FREQUENCY	CUM.%
WAITTRUST	0.016	0.005				0		
			0.005	-	_		17941	100.00
WAITUNTRUST	0.016	0.005				0		
			0.005	-	_		39103	100.00
WAITAVENGINE	0.601	0.427				0		
			0.010	-	0.170		3932	8.37
			0.170	-	0.330		8627	26.72
			0.330	-	0.490		10674	49.43
			0.490	-	0.650		8377	67.26
			0.650	-	0.810		4760	77.38
			0.810	-	0.970		3412	84.64
			0.970	-	1.130		2280	89.50
			1.130	-	1.290		1509	92.71
			1.290	-	1.450		1062	94.97
			1.450	-	1.610		742	96.54
			1.610	-	1.770		561	97.74
			1.770	-	1.930		345	98.47
			1.930	-	2.090		216	98.93
			2.090	-	2.250		156	99.26
			2.250	-	2.410		131	99.54
			2.410	-	2.570		71	99.69
			2.570	-	2.730		43	99.79
			2.730	-	2.890		34	99.86
			2.890	-	_		67	100.00
WAITIDS	0.192	0.103				0		
			0.005	-	0.059		2342	5.99
			0.059	-	0.113		7111	24.17
			0.113	-	0.167		7722	43.92
			0.167	-	0.221		7843	63.98
			0.221	-	0.275		8453	85.60
			0.275	-	0.329		2450	91.86
			0.329	-	0.383		1296	95.18
			0.383	-	0.437		879	97.42
			0.437	-	0.491		466	98.62
			0.491	-	0.545		236	99.22
			0.545	-	_		305	100.00
WAITVPN	0.161	0.071				0		
			0.005	-	0.059		376	7.82
			0.059	-	0.113		1034	29.33
			0.113	-	0.167		1129	52.81

0.167	-	0.221	1091	75.50
0.221	-	0.275	1046	97.25
0.275	-	0.329	107	99.48
0.329	-	0.383	15	99.79
0.383	-	0.437	7	99.94
0.437	-	0.491	3	100.00

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
57046	0	25046.638	57046	0	1		
57045	0	25047.394	57045	0	14		

2 Variantas

GPSS World Simulation Report - gw12.30.8

Wednesday, May 11, 2005 20:39:40

START TIME	END TIME	BLOCKS	FACILITIES	STORAGES
0.000	6141.844	34	5	0

NAME	VALUE
AVENGINE	10005.000
AVSCAN	22.000
IDS	10007.000
NOAVSCAN	28.000
TRUST	10001.000
UNTRUST	10003.000
VPN	10009.000
VPNTRAFFIC	29.000
WAITAVENGINE	10004.000
WAITIDS	10006.000
WAITTRUST	10000.000
WAITUNTRUST	10002.000
WAITVPN	10008.000

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	19556	0	0
	2	QUEUE	19556	0	0
	3	SEIZE	19556	0	0
	4	ADVANCE	19556	0	0
	5	DEPART	19556	0	0
	6	RELEASE	19556	0	0
	7	QUEUE	19556	0	0
	8	SEIZE	19556	0	0
	9	ADVANCE	19556	1	0
	10	DEPART	19555	0	0
	11	RELEASE	19555	0	0
	12	TRANSFER	19555	0	0
	13	TRANSFER	15627	0	0
	14	GENERATE	9574	0	0
	15	QUEUE	9574	0	0
	16	SEIZE	9574	0	0
	17	ADVANCE	9574	0	0
	18	DEPART	9574	0	0
	19	RELEASE	9574	0	0
	20	TRANSFER	9574	0	0
	21	TRANSFER	8133	0	0
AVSCAN	22	QUEUE	18129	11	0
	23	SEIZE	18118	0	0
	24	ADVANCE	18118	1	0
	25	DEPART	18117	0	0
	26	RELEASE	18117	0	0
	27	TERMINATE	18117	0	0
NOAVSCAN	28	TERMINATE	5631	0	0
VPNTRAFFIC	29	QUEUE	5369	0	0
	30	SEIZE	5369	0	0
	31	ADVANCE	5369	0	0
	32	DEPART	5369	0	0
	33	RELEASE	5369	0	0
	34	TERMINATE	5369	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
TRUST	9574	0.025	0.016	1	0	0	0	0	0

UNTRUST	19556	0.051	0.016	1	0	0	0	0	0
AVENGINE	18118	0.943	0.320	1	29115	0	0	0	11
IDS	19556	0.510	0.160	1	29131	0	0	0	0
VPN	5369	0.140	0.160	1	0	0	0	0	0

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
TRUST	3	0	9574	0	0.025	0.016	0.016	0
UNTRUST	3	0	19556	0	0.052	0.016	0.016	0
AVENGINE	46	12	18129	0	8.753	2.966	2.966	0
IDS	11	1	19556	0	0.834	0.262	0.262	0
VPN	5	0	5369	0	0.150	0.172	0.172	0

TABLE	MEAN	STD.DEV.	RANGE			RETRY	FREQUENCY	CUM.%
WAITTRUST	0.016	0.005				0		
			0.005	-	_		9574	100.00
WAITUNTRUST	0.016	0.006				0		
			0.005	-	_		19556	100.00
WAITAVENGINE	2.967	2.490				0		
			0.010	-	0.710		2847	15.71
			0.710	-	1.410		3275	33.79
			1.410	-	2.110		2531	47.76
			2.110	-	2.810		1942	58.48
			2.810	-	3.510		1455	66.51
			3.510	-	4.210		1500	74.79
			4.210	-	4.910		1137	81.07
			4.910	-	5.610		792	85.44
			5.610	-	6.310		715	89.39
			6.310	-	7.010		565	92.50
			7.010	-	7.710		401	94.72
			7.710	-	8.410		224	95.95
			8.410	-	9.110		205	97.09
			9.110	-	9.810		184	98.10
			9.810	-	10.510		126	98.80
			10.510	-	11.210		54	99.09
			11.210	-	11.910		28	99.25
			11.910	-	12.610		32	99.43
			12.610	-	13.310		48	99.69
			13.310	-	14.010		20	99.80
			14.010	-	14.710		14	99.88
			14.710	-	15.410		22	100.00
WAITIDS	0.262	0.178				0		
			0.005	-	0.059		769	3.93
			0.059	-	0.113		2494	16.69
			0.113	-	0.167		2919	31.61
			0.167	-	0.221		3231	48.14
			0.221	-	0.275		3636	66.73
			0.275	-	0.329		1727	75.56
			0.329	-	0.383		1197	81.68
			0.383	-	0.437		1007	86.83
			0.437	-	0.491		737	90.60
			0.491	-	0.545		508	93.20
			0.545	-	0.599		374	95.11
			0.599	-	0.653		243	96.35
			0.653	-	0.707		186	97.31
			0.707	-	0.761		140	98.02
			0.761	-	0.815		95	98.51
			0.815	-	0.869		72	98.87
			0.869	-	0.923		55	99.16
			0.923	-	0.977		43	99.38
			0.977	-	1.031		24	99.50
			1.031	-	1.085		10	99.55
			1.085	-	1.139		19	99.65
			1.139	-	1.193		12	99.71
			1.193	-	1.247		8	99.75
			1.247	-	1.301		6	99.78
			1.301	-	1.355		11	99.84
			1.355	-	1.409		6	99.87
			1.409	-	1.463		4	99.89
			1.463	-	1.517		5	99.91
			1.517	-	_		17	100.00
WAITVPN	0.172	0.082				0		
			0.005	-	0.059		396	7.38
			0.059	-	0.113		1098	27.83
			0.113	-	0.167		1160	49.43
			0.167	-	0.221		1134	70.55
			0.221	-	0.275		1206	93.02
			0.275	-	0.329		219	97.09
			0.329	-	0.383		76	98.51

0.383	-	0.437	46	99.37
0.437	-	0.491	24	99.81
0.491	-	0.545	2	99.85
0.545	-	_	8	100.00

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
29131	0	6141.903	29131	9	10		
29132	0	6141.990	29132	0	1		
29115	0	6142.052	29115	24	25		
29129	0	6142.158	29129	0	14		

2 PRIEDAS. Trust-Untrust-Dmz architektūros aprašas GPSS kalba ir modeliavimo rezultatai

Aprašas GPSS kalba

1. Variantas

```
************************************************************************          GENERATE
(Exponential(1,0,0.64));Paketu pasirodymu daznis Untrust interfeise (ms) (max 2.5Mbps)
          QUEUE     Untrust      ;Eile Untrust interfeise
          SEIZE     Untrust      ;Untrust uzimtas
          ADVANCE   0.016,0.009 ;Untrust velinimas (pralaidumas) (max 100Mbps)
          DEPART    Untrust      ;Untrust laisvas
          RELEASE   Untrust      ;Siuntimas baigtas
          QUEUE     IDS          ;Eile prie IDS
          SEIZE     IDS          ;IDS uzimtas
          ADVANCE   0.16,0.12   ;IDS paketo tikrinimo laikas (ms) (max 10Mbps)
          DEPART    IDS          ;IDS laisvas
          RELEASE   IDS          ;IDS tikrinimas baigtas
********************************************************************  TRANSFER
.1,,VPNTraffic      ;10% srauto VPN'as
            TRANSFER  .1,AvScan,NoAvScan  ;10% srauto neskanuojama
          GENERATE  (Exponential(1,0,0.45));Paketu pasirodymu daznis Trust interfeise (ms)
(max 3.5Mbps)
          QUEUE     Trust               ;Eile Trust interfeise
          SEIZE     Trust               ;Trust uzimtas
          ADVANCE   0.016,0.009         ;Trust velavimas (pralaidumas) (max 100Mbps)
          DEPART    Trust               ;Trust laisvas
          RELEASE   Trust               ;Siuntimas baigtas
********************************************************************  TRANSFER
.0,,VPNTraffic       ;0% srauto VPN'as
            TRANSFER  .25,AvScan,NoAvScan  ;25% srauto neskanuojama
          GENERATE  (Exponential(1,0,16));Paketu pasirodymu daznis Dmz interfeise (ms) (max
0.1Mbps)
          QUEUE     Dmz                 ;Eile Trust interfeise
          SEIZE     Dmz                 ;Trust uzimtas
          ADVANCE   0.016,0.009        ;Trust velavimas (pralaidumas) max 100Mbps
          DEPART    Dmz                 ;Trust laisvas
          RELEASE   Dmz                 ;Siuntimas baigtas
********************************************************************  TRANSFER
.0,,VPNTraffic       ;0% srauto VPN'as
            TRANSFER  .01,AvScan,NoAvScan  ;1% srauto neskanuojama
          AvScan QUEUE     AvEngine      ;Paketu eile laukianciu antiviruso patikrinimo
          SEIZE AvEngine                 ;AvEngine uzimtas
          ADVANCE 0.32,0.24              ;Paketo tikrinimo laikas (ms) (max 5Mbps)
          DEPART AvEngine                ;AvEngine laisvas
          RELEASE AvEngine               ;Paketo patikrinimas baigtas
          TERMINATE                      ;Patikrintas paketas iseina i kita tinkla
          NoAvScan TERMINATE 1           ;Nepatikrintas paketas iseina i kita tinkla
          VPNTraffic QUEUE VPN           ;Eile VPN
          SEIZE     VPN                  ;VPN uzimtas
          ADVANCE   0.16,0.12           ;VPN velinimas (ms) (max 10Mbps)
          DEPART    VPN                  ;VPN laisvas
          RELEASE   VPN                  ;Paketo kodavimas baigtas
          TERMINATE 1                    ;VPNTraffic srautas
************************************************************************
WaitTrust QTABLE Trust,0.0001,0.0004,15       ;Apdorojimo laikas Trust interfeise
          WaitUntrust QTABLE Untrust,0.0001,0.0004,15   ;Apdorojimo laikas Untrust
interfeise
          WaitAvEngine QTABLE AvEngine,0.01,0.16,20     ;Apdorojimo laikas AvEngine
          WaitDmz QTABLE Dmz,0.005,0.005,10          ;Apdorojimo laikas Dmz
          WaitIDS QTABLE IDS,0.005,0.054,12             ;Apdorojimo laikas IDS
          WaitVPN QTABLE VPN,0.005,0.054,12             ;VPN kodavimas
```

2 Variantas

```
************************************************************************************************
GENERATE  (Exponential(1,0,0.32));Paketu pasirodymu daznis Untrust interfeise (ms) (max
5Mbps)
          QUEUE     Untrust      ;Eile Untrust interfeise
          SEIZE     Untrust      ;Untrust uzimtas
          ADVANCE   0.016,0.009 ;Untrust velinimas (pralaidumas) (max 100Mbps)
          DEPART    Untrust      ;Untrust laisvas
          RELEASE   Untrust      ;Siuntimas baigtas
```

```
          QUEUE     IDS          ;Eile prie IDS
          SEIZE     IDS          ;IDS uzimtas
          ADVANCE   0.16,0.12   ;IDS paketo tikrinimo laikas (ms) (max 10Mbps)
          DEPART    IDS          ;IDS laisvas
          RELEASE   IDS          ;IDS tikrinimas baigtas
*******************************************************************************
            TRANSFER  .2,,VPNTraffic      ;20% srauto VPN'as
            TRANSFER  .2,AvScan,NoAvScan  ;y% srauto neskanuojama
          GENERATE  (Exponential(1,0,1.06));Paketu pasirodymu daznis Trust interfeise (ms)
(max 2.5Mbps)
          QUEUE     Trust               ;Eile Trust interfeise
          SEIZE     Trust               ;Trust uzimtas
          ADVANCE   0.016,0.009         ;Trust velavimas (pralaidumas) (max 100Mbps)
          DEPART    Trust               ;Trust laisvas
          RELEASE   Trust               ;Siuntimas baigtas
*******************************************************************************
            TRANSFER  .5,,VPNTraffic      ;x% srauto VPN'as
            TRANSFER  .3,AvScan,NoAvScan  ;y% srauto neskanuojama
          GENERATE  (Exponential(1,0,1.6));Paketu pasirodymu daznis Dmz interfeise (ms)
(max 1Mbps)
          QUEUE     Dmz                 ;Eile Trust interfeise
          SEIZE     Dmz                 ;Trust uzimtas
          ADVANCE   0.016,0.009         ;Trust velavimas (pralaidumas) max 100Mbps
          DEPART    Dmz                 ;Trust laisvas
          RELEASE   Dmz                 ;Siuntimas baigtas
*******************************************************************************
            TRANSFER  .10,,VPNTraffic      ;x% srauto VPN'as
            TRANSFER  .01,AvScan,NoAvScan  ;y% srauto neskanuojama
          AvScan QUEUE     AvEngine      ;Paketu eile laukianciu antiviruso patikrinimo
          SEIZE AvEngine                 ;AvEngine uzimtas
          ADVANCE 0.32,0.24              ;Paketo tikrinimo laikas (ms) (max 5Mbps)
          DEPART AvEngine                ;AvEngine laisvas
          RELEASE AvEngine               ;Paketo patikrinimas baigtas
          TERMINATE                      ;Patikrintas paketas iseina i kita tinkla
          NoAvScan TERMINATE 1           ;Nepatikrintas paketas iseina i kita tinkla
          VPNTraffic QUEUE VPN           ;Eile VPN
          SEIZE     VPN                  ;VPN uzimtas
          ADVANCE   0.16,0.12           ;VPN velinimas (ms) (max 10Mbps)
          DEPART    VPN                  ;VPN laisvas
          RELEASE   VPN                  ;Paketo kodavimas baigtas
          TERMINATE 1                    ;VPNTraffic srautas
*******************************************************************************
WaitTrust QTABLE Trust,0.0001,0.0004,15       ;Apdorojimo laikas Trust interfeise
          WaitUntrust QTABLE Untrust,0.0001,0.0004,15   ;Apdorojimo laikas Untrust
interfeise
          WaitAvEngine QTABLE AvEngine,1,20,50     ;Apdorojimo laikas AvEngine
          WaitDmz QTABLE Dmz,0.01,0.02,15          ;Apdorojimo laikas Dmz
          WaitIDS QTABLE IDS,0.005,0.054,45             ;Apdorojimo laikas IDS
          WaitVPN QTABLE VPN,0.005,0.054,12             ;VPN kodavimas
```

Modeliavimo rezultatai

1. Variantas

```
            GPSS World Simulation Report - gw21.11.19


                 Wednesday, May 11, 2005 19:40:02

          START TIME           END TIME  BLOCKS  FACILITIES  STORAGES
               0.000          11976.363    42        6          0


             NAME                       VALUE
          AVENGINE                   10005.000
          AVSCAN                        30.000
          DMZ                        10007.000
          IDS                        10009.000
          NOAVSCAN                      36.000
          TRUST                      10001.000
          UNTRUST                    10003.000
          VPN                        10011.000
          VPNTRAFFIC                    37.000
          WAITAVENGINE               10004.000
          WAITDMZ                    10006.000
```

WAITIDS	10008.000
WAITTRUST	10000.000
WAITUNTRUST	10002.000
WAITVPN	10010.000

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	18706	0	0
	2	QUEUE	18706	0	0
	3	SEIZE	18706	0	0
	4	ADVANCE	18706	0	0
	5	DEPART	18706	0	0
	6	RELEASE	18706	0	0
	7	QUEUE	18706	0	0
	8	SEIZE	18706	0	0
	9	ADVANCE	18706	0	0
	10	DEPART	18706	0	0
	11	RELEASE	18706	0	0
	12	TRANSFER	18706	0	0
	13	TRANSFER	16855	0	0
	14	GENERATE	26139	0	0
	15	QUEUE	26139	0	0
	16	SEIZE	26139	0	0
	17	ADVANCE	26139	0	0
	18	DEPART	26139	0	0
	19	RELEASE	26139	0	0
	20	TRANSFER	26139	0	0
	21	TRANSFER	26139	0	0
	22	GENERATE	784	0	0
	23	QUEUE	784	0	0
	24	SEIZE	784	0	0
	25	ADVANCE	784	0	0
	26	DEPART	784	0	0
	27	RELEASE	784	0	0
	28	TRANSFER	784	0	0
	29	TRANSFER	784	0	0
AVSCAN	30	QUEUE	35629	0	0
	31	SEIZE	35629	0	0
	32	ADVANCE	35629	0	0
	33	DEPART	35629	0	0
	34	RELEASE	35629	0	0
	35	TERMINATE	35629	0	0
NOAVSCAN	36	TERMINATE	8149	0	0
VPNTRAFFIC	37	QUEUE	1851	0	0
	38	SEIZE	1851	0	0
	39	ADVANCE	1851	0	0
	40	DEPART	1851	0	0
	41	RELEASE	1851	0	0
	42	TERMINATE	1851	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
TRUST	26139	0.035	0.016	1	0	0	0	0	0
UNTRUST	18706	0.025	0.016	1	0	0	0	0	0
AVENGINE	35629	0.954	0.321	1	0	0	0	0	0
DMZ	784	0.001	0.016	1	0	0	0	0	0
IDS	18706	0.251	0.161	1	0	0	0	0	0
VPN	1851	0.025	0.160	1	0	0	0	0	0

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
TRUST	4	0	26139	0	0.036	0.016	0.016	0
UNTRUST	3	0	18706	0	0.025	0.016	0.016	0
AVENGINE	58	0	35629	0	10.783	3.625	3.625	0
DMZ	1	0	784	0	0.001	0.016	0.016	0
IDS	7	0	18706	0	0.300	0.192	0.192	0
VPN	2	0	1851	0	0.025	0.161	0.161	0

TABLE	MEAN	STD.DEV.	RANGE			RETRY	FREQUENCY	CUM.%
WAITTRUST	0.016	0.006				0		
			0.005	-	_		26139	100.00
WAITUNTRUST	0.016	0.005				0		
			0.005	-	_		18706	100.00
WAITAVENGINE	3.625	3.036				0		
			0.010	-	0.710		4538	12.74
			0.710	-	1.410		5246	27.46
			1.410	-	2.110		4301	39.53
			2.110	-	2.810		3763	50.09
			2.810	-	3.510		3172	59.00

			3.510	-	4.210	2655	66.45
			4.210	-	4.910	2362	73.08
			4.910	-	5.610	2017	78.74
			5.610	-	6.310	1663	83.41
			6.310	-	7.010	1332	87.15
			7.010	-	7.710	933	89.76
			7.710	-	8.410	731	91.82
			8.410	-	9.110	569	93.41
			9.110	-	9.810	523	94.88
			9.810	-	10.510	443	96.12
			10.510	-	11.210	338	97.07
			11.210	-	11.910	279	97.86
			11.910	-	12.610	236	98.52
			12.610	-	13.310	153	98.95
			13.310	-	14.010	76	99.16
			14.010	-	14.710	69	99.35
			14.710	-	15.410	69	99.55
			15.410	-	16.110	62	99.72
			16.110	-	16.810	55	99.88
			16.810	-	17.510	14	99.92
			17.510	-	18.210	15	99.96
			18.210	-	18.910	15	100.00
WAITDMZ	0.016	0.005				0	
			0.005	-	0.010	134	17.09
			0.010	-	0.015	220	45.15
			0.015	-	0.020	213	72.32
			0.020	-	0.025	217	100.00
WAITIDS	0.192	0.100				0	
			0.005	-	0.059	1102	5.89
			0.059	-	0.113	3334	23.71
			0.113	-	0.167	3629	43.11
			0.167	-	0.221	3968	64.33
			0.221	-	0.275	4051	85.98
			0.275	-	0.329	1145	92.10
			0.329	-	0.383	633	95.49
			0.383	-	0.437	422	97.74
			0.437	-	0.491	207	98.85
			0.491	-	0.545	86	99.31
			0.545	- _		129	100.00
WAITVPN	0.161	0.071				0	
			0.005	-	0.059	130	7.02
			0.059	-	0.113	458	31.77
			0.113	-	0.167	388	52.73
			0.167	-	0.221	408	74.77
			0.221	-	0.275	413	97.08
			0.275	-	0.329	47	99.62
			0.329	-	0.383	5	99.89
			0.383	-	0.437	2	100.00

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
45632	0	11976.412	45632	0	14		
45629	0	11976.792	45629	0	1		
45593	0	11984.228	45593	0	22		

2. Variantas

GPSS World Simulation Report - gw22.17.3

Saturday, May 14, 2005 14:41:31

START TIME	END TIME	BLOCKS	FACILITIES	STORAGES
0.000	3108.058	42	6	0

NAME	VALUE
AVENGINE	10005.000
AVSCAN	30.000
DMZ	10007.000
IDS	10009.000
NOAVSCAN	36.000
TRUST	10001.000
UNTRUST	10003.000
VPN	10011.000
VPNTRAFFIC	37.000

WAITAVENGINE	10004.000
WAITDMZ	10006.000
WAITIDS	10008.000
WAITTRUST	10000.000
WAITUNTRUST	10002.000
WAITVPN	10010.000

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	9715	0	0
	2	QUEUE	9715	0	0
	3	SEIZE	9715	0	0
	4	ADVANCE	9715	0	0
	5	DEPART	9715	0	0
	6	RELEASE	9715	0	0
	7	QUEUE	9715	0	0
	8	SEIZE	9715	0	0
	9	ADVANCE	9715	0	0
	10	DEPART	9715	0	0
	11	RELEASE	9715	0	0
	12	TRANSFER	9715	0	0
	13	TRANSFER	7835	0	0
	14	GENERATE	9766	0	0
	15	QUEUE	9766	0	0
	16	SEIZE	9766	0	0
	17	ADVANCE	9766	0	0
	18	DEPART	9766	0	0
	19	RELEASE	9766	0	0
	20	TRANSFER	9766	0	0
	21	TRANSFER	4860	0	0
	22	GENERATE	1915	0	0
	23	QUEUE	1915	0	0
	24	SEIZE	1915	0	0
	25	ADVANCE	1915	0	0
	26	DEPART	1915	0	0
	27	RELEASE	1915	0	0
	28	TRANSFER	1915	0	0
	29	TRANSFER	1716	0	0
AVSCAN	30	QUEUE	11396	1736	0
	31	SEIZE	9660	0	0
	32	ADVANCE	9660	1	0
	33	DEPART	9659	0	0
	34	RELEASE	9659	0	0
	35	TERMINATE	9659	0	0
NOAVSCAN	36	TERMINATE	3015	0	0
VPNTRAFFIC	37	QUEUE	6985	0	0
	38	SEIZE	6985	0	0
	39	ADVANCE	6985	0	0
	40	DEPART	6985	0	0
	41	RELEASE	6985	0	0
	42	TERMINATE	6985	0	0

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
TRUST	9766	0.050	0.016	1	0	0	0	0	0
UNTRUST	9715	0.050	0.016	1	0	0	0	0	0
AVENGINE	9660	1.000	0.322	1	18140	0	0	0	1736
DMZ	1915	0.010	0.016	1	0	0	0	0	0
IDS	9715	0.498	0.159	1	0	0	0	0	0
VPN	6985	0.358	0.159	1	0	0	0	0	0

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
TRUST	3	0	9766	0	0.052	0.017	0.017	0
UNTRUST	3	0	9715	0	0.051	0.016	0.016	0
AVENGINE	1738	1737	11396	0	902.201	246.059	246.059	0
DMZ	2	0	1915	0	0.010	0.016	0.016	0
IDS	10	0	9715	0	0.819	0.262	0.262	0
VPN	6	0	6985	0	0.474	0.211	0.211	0

TABLE	MEAN	STD.DEV.	RANGE			RETRY	FREQUENCY	CUM.%
WAITTRUST	0.017	0.006				0		
			0.005	-	_		9766	100.00
WAITUNTRUST	0.016	0.006				0		
			0.005	-	_		9715	100.00
WAITAVENGINE	247.801	143.950				0		
			_	-	1.000		23	0.24
			1.000	-	21.000		392	4.30
			21.000	-	41.000		417	8.61

			41.000	-	61.000	335	12.08
			61.000	-	81.000	559	17.87
			81.000	-	101.000	385	21.86
			101.000	-	121.000	278	24.73
			121.000	-	141.000	501	29.92
			141.000	-	161.000	258	32.59
			161.000	-	181.000	531	38.09
			181.000	-	201.000	408	42.31
			201.000	-	221.000	233	44.73
			221.000	-	241.000	338	48.22
			241.000	-	261.000	299	51.32
			261.000	-	281.000	295	54.37
			281.000	-	301.000	288	57.36
			301.000	-	321.000	264	60.09
			321.000	-	341.000	715	67.49
			341.000	-	361.000	389	71.52
			361.000	-	381.000	414	75.80
			381.000	-	401.000	338	79.30
			401.000	-	421.000	523	84.72
			421.000	-	441.000	661	91.56
			441.000	-	461.000	399	95.69
			461.000	-	481.000	416	100.00
WAITDMZ	0.016	0.005				0	
			_	-	0.010	323	16.87
			0.010	-	0.030	1586	99.69
			0.030	-	0.050	6	100.00
WAITIDS	0.262	0.176				0	
			0.005	-	0.059	383	3.94
			0.059	-	0.113	1284	17.16
			0.113	-	0.167	1463	32.22
			0.167	-	0.221	1558	48.26
			0.221	-	0.275	1735	66.11
			0.275	-	0.329	874	75.11
			0.329	-	0.383	592	81.20
			0.383	-	0.437	498	86.33
			0.437	-	0.491	373	90.17
			0.491	-	0.545	280	93.05
			0.545	-	0.599	176	94.86
			0.599	-	0.653	157	96.48
			0.653	-	0.707	91	97.42
			0.707	-	0.761	60	98.03
			0.761	-	0.815	44	98.49
			0.815	-	0.869	30	98.80
			0.869	-	0.923	35	99.16
			0.923	-	0.977	17	99.33
			0.977	-	1.031	20	99.54
			1.031	-	1.085	13	99.67
			1.085	-	1.139	9	99.76
			1.139	-	1.193	5	99.81
			1.193	-	1.247	4	99.86
			1.247	-	1.301	4	99.90
			1.301	-	1.355	5	99.95
			1.355	-	1.409	2	99.97
			1.409	-	1.463	2	99.99
			1.463	-	1.517	1	100.00
WAITVPN	0.211	0.125				0	
			0.005	-	0.059	369	5.28
			0.059	-	0.113	1146	21.69
			0.113	-	0.167	1287	40.11
			0.167	-	0.221	1384	59.93
			0.221	-	0.275	1385	79.76
			0.275	-	0.329	513	87.10
			0.329	-	0.383	310	91.54
			0.383	-	0.437	208	94.52
			0.437	-	0.491	145	96.59
			0.491	-	0.545	95	97.95
			0.545	-	_	143	100.00

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
18140	0	3108.106	18140	32	33		
21396	0	3108.150	21396	0	14		
21399	0	3108.298	21399	0	1		
21398	0	3108.419	21398	0	22		

3 PRIEDAS. Straipsnis

Korporacinių įmonių informacinės saugos architektūrų modeliavimas

Mindaugas Mikučionis
Kauno technologijos universitetas
Kaunas University of Technology
Tel. (8 37) 30 03 89
El. paštas: mindaugas.mikucionis@ktu.lt

Algimantas Venčkauskas
Kauno technologijos universiteto docentas
Kaunas University of Technology, Assoc. Professor
Tel. (8 37) 30 03 89
El. paštas: algimantas.venckauskas@ktu.lt

Korporacinių įmonių kompiuterinių sistemų informacinės saugos užtikrinimas yra viena iš svarbiausių informacinių technologijų problemų. Augant ir plečiantis verslui iškyla nutolusių įmonės padalinių, partnerių, darbuotojų saugaus apsikeitimo duomenimis ir lokalių tinklų saugumo problema. Nuolatos auga informacinių technologijų vaidmuo verslo ir valdymo procesuose, didėja informacinių procesų sudėtingumas. Dėl šių priežasčių informacinės saugos pažeidimų kaina kompiuterinėse sistemose nuolatos auga.
Atsižvelgiant į informacinės saugos priemonių patikimumo ir našumo kriterijus, būtina šių sistemų veikimą ištirti prieš diegiant. Adekvačių sprendimų, užtikrinančių priimtiną informacinę saugą už atitinkamą kainą, priėmimas tampa vis sudėtingesniu uždaviniu. Korporacinės įmonės informacinės saugos modeliai leidžia išspręsti šias problemas bei gali būti taikomi informacinės saugos sistemų projektavimui, parametrų parinkimui ir diegimui. Šiame darbe sudaromos ir nagrinėjamos korporacinių įmonių informacinės saugos sistemų modeliai, aprašantys įvairias saugaus duomenų apsikeitimo ir informacinės saugos grėsmių neutralizavimo priemonių architektūras. Informacinės saugos realizavimo priemonės įvertintos atitinkamais parametrais. Modeliai leidžia palyginti įvairias informacinės saugos realizavimo architektūras ir parinkti efektyviausią.

Korporacinę įmonę sudaro geografiškai nutolę padaliniai. Dažniausiai padalinių lokalūs kompiuterių tinklai į bendrą korporacijos kompiuterių tinklą sujungiami internetinio ryšio priemonėmis. Kadangi internetas yra potencialiai pavojingas informacinė saugos požiūriu, reikia išspręsti šiuos pagrindinius korporacinės įmonės lokalių kompiuterių tinklų sujungimo uždavinius:
- saugus duomenų apsikeitimas tarp nutolusių padalinių lokalių tinklų kompiuterių,
- lokalių tinklų apsauga nuo galimų atakų ir įsilaužimų,
- antivirusinė apsauga.

Šie uždaviniai sprendžiami naudojant įvairias tinklines technologijas ir siekiant skirtingų tikslų. Mažoms įmonėms svarbu nebrangaus ryšio užtikrinimas. Didelėms įmonėms reikia užtikrinti sudėtingą, įvairialypį, saugų tinklų sujungimą, užšifruojant informaciją ir kontroliuojant priėjimą prie jos.
Saugus duomenų apsikeitimas tarp kompiuterių, esančių skirtinguose lokaliuose tinkluose, dažniausiai realizuojamas naudojant virtualius privačius tinklus (VPN) (Mitchell, 2005). VPN yra tinklas jungiantis korporacinės įmonės struktūrinius elementus panaudojant viešą interneto tinklą. Čia nėra naudojamos saugios skirtinės linijos, todėl perduodami duomenys turi būti koduojami. Viešame interneto tinkle sukuriami koduoti duomenų perdavimo tuneliai tarp geografiškai išdėstytų taškų. VPN privalumai yra saugus nutolusių kompiuterių sujungimas, maža kaina, nesudėtinga tinklo topologija. VPN trūkumai yra greitaveikos sumažėjimas dėl informacijos kodavimo, neužtikrinamas pastovus duomenų srauto perdavimo greitis. VPN gali būti realizuota naudojant specialią aparatinę programinę įrangą (Juniper Networks Firewall, 2005), operacinių sistemų VPN priemones (Microsoft Internet Security and Acceleration (ISA) Server, 2005), interneto paslaugų tiekėjų priemones (GPRS intranetas, Cisco VPN, 2005).
Lokalių tinklų apsaugai nuo galimų atakų ir įsilaužimų naudojamos ugniasienės ir tinklų atakų aptikimo priemonės (IDS). Ugniasienės yra pagrindiniai saugios korporacinės įmonės saugumo

architektūros elementai (Slemp, 2001). Ugniasienės kontroliuoja duomenų srautą į ir iš tinklo. Tam kad filtruoti paketus, reikia sudaryti aibę taisyklių, kurios nurodo protokolų tipus, kurie yra praleidžiami ir kurie nepraleidžiami priklausomai nuo gavėjo ir siuntėjo adresų. Yra dviejų tipų ugniasienės: filtravimo be atminties- kiekvieno paketo informacija lyginama su statiškai nustatytu taisyklių rinkiniu. Žiūrima tik į paketo antraščių informaciją (siuntėjo ir gavėjo IP, portus). Filtravimo su atmintimi - kai įvairių lentelių pagalba analizuojama paketų seka ir atitinkamos taisyklės taikomos priklausomai nuo esamos susijungimo būsenos. Ugniasienių pagalba, kompiuterių tinklas skaidomas į skirtingo lygio saugumo zonas, tai žymiai padidina tinklo saugumą ir palengvina saugumo taisyklių taikymą. Įsilaužimų aptikimo sistema (IDS) stebi duomenų srautą ir, aptikus įsilaužimo požymį, generuoja pranešimus (Dobrucki, 2002). Ugniasienės saugo tinklą nuo įsilaužimų, tuo tarpu IDS parodo ar tinklas atakuojamas. Yra du IDS tipai: tinklo ir lokalus. Kiekvienas tipas turi savo privalumo ir trūkumų. Lokalus IDS esantis serveryje arba vartotojo darbo vietoje renka informaciją generuojamą lokalios sistemos. Šio tipo IDS sudėtinga administruoti didelės įmonės tinkluose. Tinklinės IDS analizuoja duomenis perduodamus kompiuterių tinklu. Kiekvienas paketas yra sulyginamas su duomenų bazėje esančia informacija. Tinklines IDS yra lengviau paskirstyti ir administruoti. Tačiau yra ribotas maksimalus duomenų srautas, kurį gali apdoroti IDS.

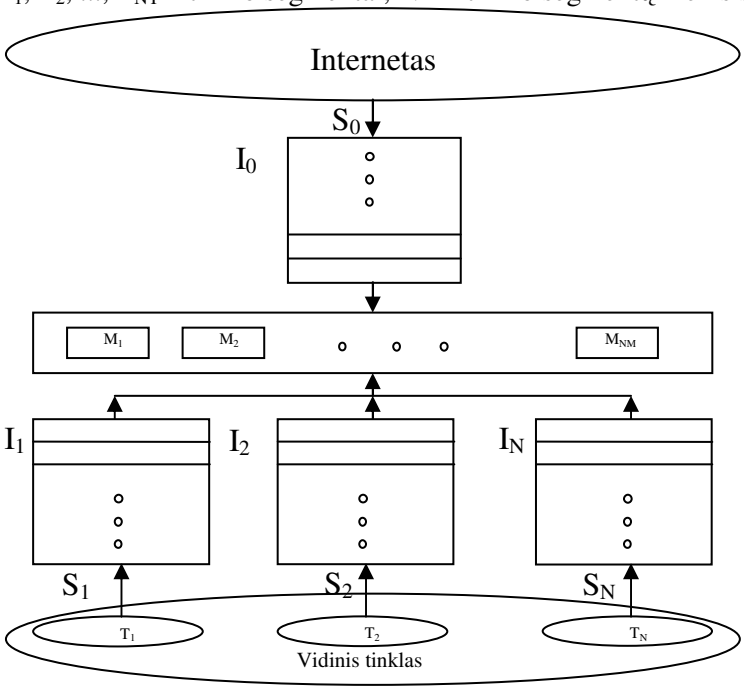
Viena didžiausių grėsmių informacijos saugumui kyla dėl kompiuterių virusų. Virusų aptikimui ir neutralizavimui naudojamos antivirusinės priemonės. Turi būti naudojama kelių saugos lygių architektūra. Vartotojų darbo vietose turi būti programinės antivirusinės (AV) programos. Tačiau vartotojo darbo vietos dažnai yra nepatikimos (antivirusas gali būti išjungiamas), todėl aukščiausiame lygyje duomenų srautas turi būti tikrinamas prieš patenkant į įmonės lokalų tinklą. Antivirusiniam duomenų srauto ateinančio arba išeinančio iš lokalaus tinklo skenavimui naudojamos programinės ir aparatinės priemonės. Pavyzdžiui galima paminėti Panda GateDefender įrenginį (Panda GateDefender, 2005). Jis blokuoja virusus, nepageidaujamą elektroninį paštą ir nepageidaujamą turinį prieš jiems patenkant į lokalų tinklą. Panda GateDefender turi automatišką atsinaujinimo sistemą, kuri suteikia moderniausią apsaugą visam tinklui.. Panda GateDefender puikiausiai tinka mažoms, vidutinėms ir didelėms įmonėms. Tokie aparatiniai įrenginiai įterpiami tarp įmonės maršrutizatoriaus ir vidinio tinklo. Pagrindiniai parametrai yra maksimalus srauto tikrinimo greitis (5-30Mbps). Esant dideliam srautui susidaro duomenų kamščiai ir tinklo funkcionavimas gali sutrikti. Esant kelioms tinklo saugumo zonoms tampa sudėtinga parinkti įrenginio darbo vietą, tam kad būtų patikrintas visas reikalingas srautas ir nebūtų bereikalingo srauto tikrinimo.

Įmonės saugumo infrastruktūros kūrimas yra sudėtingas procesas, todėl itin svarbu iš pradžių galimai tiksliau suprojektuoti visą sistemą, nes po to bus sugaišta daug laiko (ir išleista pinigų) sistemos modifikacijai. Todėl projektavimo etape (tiek tinklo išdėstymo, tiek saugomo zonų pasiskirstymo, tiek papildomų saugumo priemonių) reikia sumodeliuoti kiek galima daugiau ir įvairesnių situacijų. Informacinė sauga – tai sudėtinga ir persipynusi saugos priemonių visuma. Tos priemonės priklauso viena nuo kitos ir projektuojant reikia matyti bendrą vaizdą. Priklausomai nuo darbo vietų skaičiaus, įmonės geografinio išsidėstymo ir tinklo darbo intensyvumo priklausys informacinės saugos užtikrinimo priemonių parametrai ir duomenų srautai. Šios priemonės savo ruožtu įtakoja duomenų srauto greitį. Šis apkrovimas taip pat priklausys nuo naudojamos tinklo architektūros ir saugos priemonių architektūros.

Modeliavimo metu įvertinsime šias charakteristikas: duomenų judėjimo tinkle greitį; tinklo architektūrą; įmonės struktūrą, t.y. geografinį išsidėstymą; VPN kodavimo, antivirusinių ir įsilaužimų aptikimo priemonių įtaką; protokolų pasiskirstymą duomenų sraute; įmonės servisus. Panagrinėsime keletą informacinės saugos modeliavimo metodų ir apibrėšime jų privalumus ir trūkumus: atakų grafo metodą, apibendrinto kriterijaus metodas, markovo procesų modelį ir imitacinį GPSS modelį.

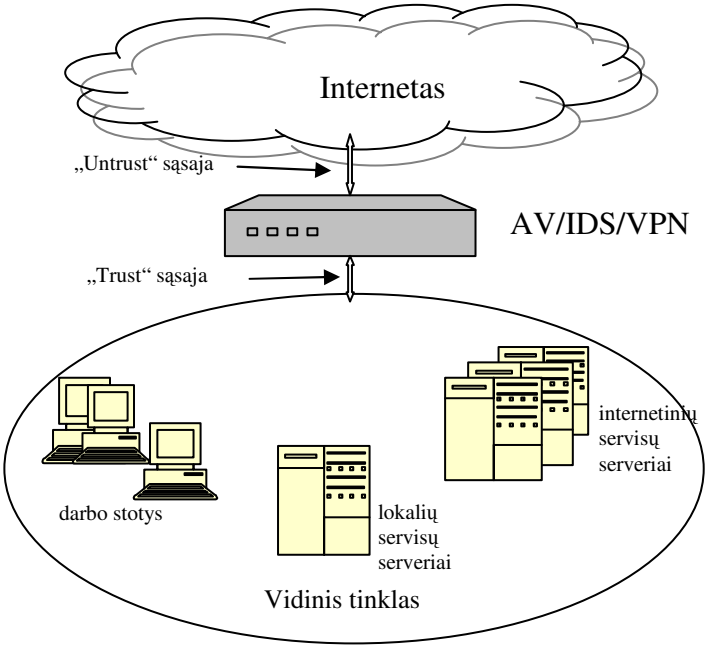
Atakų grafo metodas – kiekvienai sistemai galima aprašyti atakų grafų rinkinius (Jha ir kt., 2003; Sheyner, 2004). Grafo mazgas reiškia sistemos pažeidimą. Grafas parodo kaip įsilaužėlis gali pakenkti įmonės kompiuterinėms sistemoms. Atakų grafas reprezentuoją visus galimus kelius, kuriais galima pažeisti modeliuojamos sistemos saugumą. Didelių sistemų atakų medžių projektavimas yra ilgas ir sudėtingas procesas. Saugumo specialistai naudoja šiuos duomenis sistemos silpnų vietų aptikimui. Atakų grafo projektavimui reikia surinkti visus tinklo sistemos lokalius ir globalius pažeidžiamumus. Pažeidžiamumų duomenų bazės surinkimui naudojamos tinklo elementų, serverių saugumo tikrinimo priemonės. Sujungus ryšiais lokalius ir globalius

pažeidimus gauname atakų grafą. Kiekvienas grafo lankas yra atitinkamą pažeidžiamumą išnaudojantis procesas, kuris perveda sistema į nestabilią būseną. Atakų medžiai parodo: sėkmingas atakas, kurių neaptinka saugos priemonės; kur efektyviausiai išdėstyti saugos priemones; parinkti efektyvias programines ir aparatines saugos priemonių realizacijas; numatyti ateityje galimus incidentus; įvertinti skirtingų tinko topologijų efektyvumą. Tačiau atakų grafų sudarymas yra labai sudėtingas darbas. Šiuo metu kuriami atakų medžių automatinio generavimo metodui. Šiuo metodu negalime įvertinti kiekybinių saugos priemonių parametrų (saugos priemonių greitaveikos ir t.t.). Apibrėžiami tik pažeidžiamumai ir negalima modeliuoti saugos priemonių darbo greitaveikos.
Įmonės informacinės saugos efektyvumą galima vertinti apibendrintu kriterijumi (Venčkauskas ir kt., 2003). Santykinė šio kriterijaus reikšmė leidžia palyginti keletą informacinės saugos realizavimo variantų ir pasirinkti geriausią Šiuo metodu taip pat galima įvertinti įmonės informacinės saugos lygį pagal suformuluotus kriterijus ir vertinimo skalę, naudojant etaloninę informacinės saugos sistemą. Įmonės informacinės saugos efektyvumo vertinimo apibendrintu kriterijumi metodas yra informatyvus, nes sistemos sauga apibrėžiama vienu santykiniu dydžiu ir tai palengvina įvairių variantų analizę.
Markovo procesų modelis – korporacinės įmonės saugos sistema pavaizduojama grafu, kurio viršūnės yra atitinkamos saugos sistemos būsenos (elementai), o lankų svoriai nurodo perėjimo į kitą būseną tikimybę (16).
Grafo viršūnių įverčiai aprašo saugumo sistemos elementų (VPN, įsilaužimų aptikimo priemonių ir t.t.) darbo greitaveiką - vėlinimus duomenų perdavimui, kainą ir kitas kiekines charakteristikas, o lankų svoriai – duomenų srautų pasiskirstymą. Markovo procesų modeliai gerai tinka sistemos greitaveikos, kainos įvertinimui, tačiau neatspindi galimų pažeidimų įvairovės ir reagavimo į juos efektyvumo.
Sudėtingų techninių sistemų modeliavimui projektavimo metu plačiai naudojami imitaciniai metodai. Įmonės informacinės saugos sistemų architektūrų modeliavimui panaudosime GPSS sistemą (17). Modeliuojant GPSS metodu, saugos sistema yra išskaidoma į blokus (procesus), kurie sujungiami ryšio kanalais. Blokai – tai saugos sistemos realizavimo komponentai: VPN kodavimo, antivirusinių ir įsilaužimų aptikimo priemonės ir moduliai, tinklo sąsajos, o ryšio kanalai - tai duomenų srautai tarp tinklo komponentų ir segmentų. Bendra informacinės saugos sistemos imitacinio modelio schema pateikta 1pav. :
M_1, M_2 ...,M_{NM} - modeliuojamos informacinės saugos priemonės, NM – saugumo priemonių kiekis sistemoje;
I_0, I_2 ...,I_{NI} - tinklo sąsajos, NI – tinklo sąsajų kiekis sistemoje;
S_1, S_2 ...,S_{NS} - tinklų sąsajų generuojami duomenų srautai; NS – duomenų srautų kiekis;
T_1, T_2, ..., T_{NT} – tinklo segmentai, NT – tinklo segmentų kiekis sistemoje.



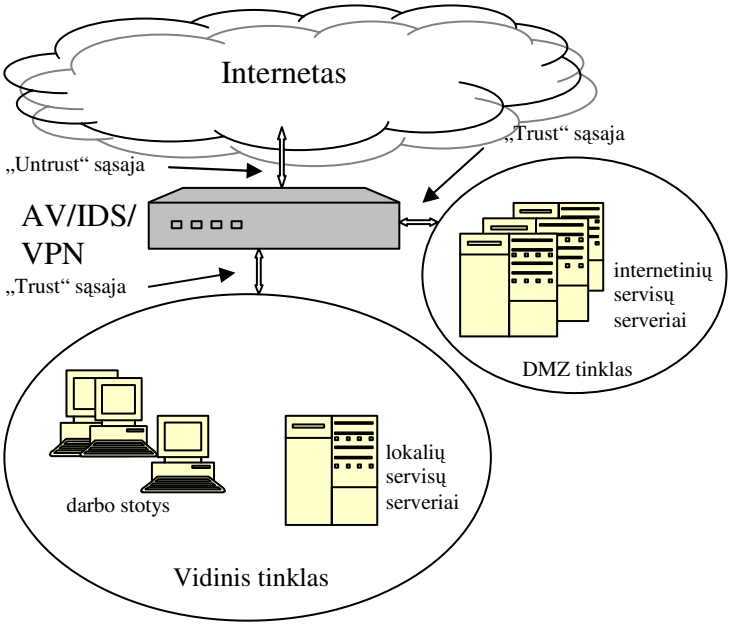
1 pav. Bendra informacinės saugos sistemos imitacinio modelio schema

Modeliuojant vertinsime šiuos parametrus: paketų pasirodymo dažnius sąsajose IS_i, saugumo priemonių vėlinimus (paketų apdorojimo laikus) MD_i, eiles prie tinklo sąsajų IQ_i, eiles prie saugos modulių MQ_i. Tinklo sąsajų apkrovimas aprašomas paketo pasirodymo dažniu (ms). Modelyje tariama, kad kiekvienas paketas yra 200 baitų dydžio. Jei norime aprašyti 2.5Mbps srautą, tada paketų pasirodymo dažnis bus 0.64ms.
Eilės susidaro prie tinklo sąsajų (kadangi reikalingas atitinkamas laiko tarpas duomenų siuntimui ir gavimui) ir prie saugos modulių (ribotas duomenų aptarnavimo kiekis ir laikas). Eilė prie sąsajų parodys tinklo pralaidumo resursų nepakankamumą, o eilė prie saugos modulių – jų resursų stygių (reiškia reikia kitaip dalinti duomenų srautus arba didinti modulių resursus). Pagal masinio aptarnavimo teoriją paraiškos į sistemą ateina Puasono srautu (pasiskirstę pagal eksponentinį dėsnį), kurio parametras – srauto intensyvumas – bus lygus IS_i.
Eksperimentinius GPSS modelius realizuosime dviems skirtingoms korporacinės įmonės informacinės saugos architektūroms, pateiktoms 2 pav. ir 3 pav.



2 pav. „Trust-Untrust“ architektūra

„Trust-Untrust“ architektūra sudaryta panaudojant maršrutizatorių, kuris turi mažiausiai dvi sąsajas. Jis jungia išorinį (nesaugų, „Untrust“) ir vidinį (saugų, „Trust“) kompiuterių tinklus. Šiame maršrutizatoriuje yra integruoti antivirusinis, IDS ir VPN moduliai. Visi įmonės serveriai: vidinių duomenų bazių, WEB, pašto, FTP serveriai išdėstyti vidiniame tinkle. Duomenų srautai tarp vidinio tinklo kompiuterių ir visų serverių, tame tarpe ir internetinių paslaugų WEB, pašto, FTP, perduodami be papildomo tikrinimo informacinės saugos priemonėmis.



3 pav. „Trust-Untrust-Dmz“ architektūra

„Trust-Untrust-Dmz“ architektūroje realizuotas papildomą apsaugos sluoksnis - DMZ tinklas, kuris izoliuoja vidinį tinklą nuo interneto paslaugų serverių. DMZ zonoje patalpinami Web, FTP ir pašto servisai, kurie yra labiausiai pažeidžiami. Ši architektūra realizuojama panaudojant maršrutizatorių su integruotais antivirusiniu, IDS ir VPN moduliais. Duomenų srautai tarp vidinio tinklo kompiuterių ir internetinių paslaugų WEB, pašto, FTP serverių perduodami papildomai tikrinant informacinės saugos priemonėmis. Tačiau, jei įsilaužėlis patenka į DMZ zoną, šis sluoksnis užtikrina, kad nebus patekta į vidinį įmonės tinklą.
Pagal įmonės saugumo politiką ir pasirinktą sistemos architektūrą apibrėžiama duomenų paketų judėjimo tarp sąsajų kryptys priklausomai nuo protokolo, saugumo modulių tipas ir skaičius. Modeliuojamoje sistemoje parinkti trys saugumo moduliai: VPN kodavimo, antivirusinės ir įsilaužimų aptikimo priemonės, kurios realizuotos Jenifer NetScreen įrenginyje (Juniper Networks Firewall, 2005). Modeliuojamas VPN modulis duomenų paketą koduoja 0.16 ms, antivirusinis modulis – tikrina 0.6 ms, įsilaužimų aptikimo modulis – 0.19 ms. Modeliuojamų sistemų architektūrų charakteristikos pateiktos 1 lentelėje.

1 lentelė

	"Trust-Untrust" architektūra		"Trust-Untrust-DMZ" architektūra		
	"Untrust" sąsaja	"Trust" sąsaja	"Untrust" sąsaja	"Trust" sąsaja	"DMZ" sąsaja
Saugumo modulių skaičius		3		3	3
Tinklo sąsajų kiekis	1	1	1	1	1
Leidžiami protokolai tarp sąsajų:					
Iš "Untrust" sąsajos		HTTP, SMTP, SSH, FTP, IPSec (VPN)		IPSec (VPN)	HTTP, SMTP, IPSec (VPN)
Iš "Trust" sąsajos	Visi		Visi		HTTP, POP3, SMTP, FTP, SSH
Iš "DMZ" sąsajos			SMTP, DNS		

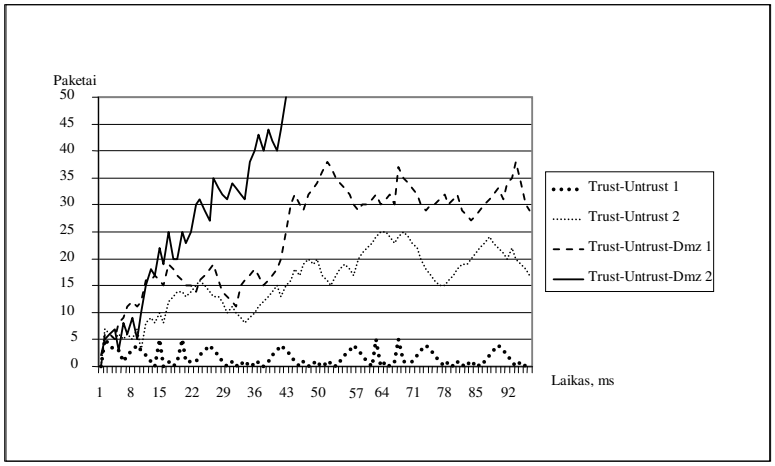
Duomenų srautų dydžiai, jų pasiskirstymas pagal protokolus priklauso nuo įmonės veiklos pobūdžio, naudojamų informacinių technologijų. Komercinėms įmonėms būdinga didesnis

interneto servisų naudojimas, gamybinėms įmonėms – didesnis lokalių servisų naudojimas. Srautų charakteristikos gali būti nustatomos eksperimentiniais matavimais arba ekspertiniais vertinimais. Duomenų paketai į modeliuojamą sistemą ateina Puasono srautu (pasiskirstę pagal eksponentinį dėsnį). Modeliuojami duomenų srautai ir jų pasiskirstymas pagal protokolus pateikti 2 lentelėje.

2 lentelė

	"Trust-Untrust" architektūra				"Trust-Untrust-DMZ" architektūra					
	I variantas		II variantas		I variantas			II variantas		
	"Untrust" sąsaja	"Trust" sąsaja	"Untrust" sąsaja	"Trust" sąsaja	"Untrust" sąsaja	"Trust" sąsaja	"DMZ" sąsaja	"Untrust" sąsaja	"Trust" sąsaja	"DMZ" sąsaja
Duomenų srauto dydis Mbps	2,50	1,10	5,00	2,50	2,50	3,50	0,10	5,00	2,50	1,00
Duomenų srautų pasiskirstymas pagal protokolus:										
HTTP	0,55	0,80	0,20	0,20	0,60	0,30		0,10	0,40	
FTP	0,05		0,05			0,30			0,40	
SMTP	0,30		0,55	0,50	0,30	0,15	0,99	0,85	0,05	0,99
IPsec (VPN)	0,10	0,05	0,20	0,15	0,10	0,05		0,05		
DNS							0,01			0,01
Kiti		0,05		0,15		0,10			0,15	

Modeliavimo metu gavome įvairius sistemos charakteristikų įvertinimus: saugos modulių darbo trukmes, jų apkrovimą, eilių prie saugumo modulių dydžius. Modeliuojamų architektūrų antivirusinio modulio gauti apkrovimai pateikti 4 pav.



4 pav. Antivirusinio modulio apkrovimas

Kaip matome iš gautų rezultatų, „Trust-Untrust-Dmz“ architektūroje, esant antrojo varianto duomenų srautams, antivirusinio modulio greitaveikos, planuojamam apkrautumui, nepakanka: reikia panaudoti dar vieną antivirusinį modulį, perskirstyti duomenų srautus: pvz. atskirti HTTP srautą ir jo antivirusiniu moduliu netikrinti.

Išvados

Šiame darbe analizuota korporacinės įmonės tinklinio sujungimo būdai, informacinės saugos sistemos elementai. Buvo sudaromi ir nagrinėjami korporacinių įmonių informacinės saugos sistemų modeliai: atakų medžiai, Markovo grafas, imitacinis GPSS modelis.
atakų medžių modelis leidžia aptikti modeliuojamos sistemos silpnas vietas, tačiau jo realizacija gana sudėtinga, nes sunku įvertinti visus korporacinėje įmonėje egzistuojančius pažeidžiamumus. Šiuo metodu negalime įvertinti kiekybinių saugos priemonių parametrų;

markovo procesų modelis leidžia kiekybiškai įvertinti nagrinėjamos architektūros informacinės saugos sistemos našumą. Parinkus grafo parametrus išrenkama optimali sistema pagal duomenų pasiskirstymą ir apdorojimo trukmės kriterijus;
Imitacinis modelis naudingas tiek parenkant fizinius korporacinės įmonės saugos elementų parametrus, tiek modeliuojant duomenų srautus.
Įvertinus visa tai rekomenduojama:
panaudojant atakų grafą nustatyti silpnas saugumo požiūriu korporacinės įmonės sistemas. Jų pagrindu suformuoti saugumo zonas su atitinkamomis duomenų srautų taisyklėmis ir parinkti informacinės saugos elementų išdėstymo vietas korporacinės įmonės tinklų topologijoje;
informacinės saugos elementų parametrų nustatymui naudoti imitacinį GPSS modelį,. modeliuojant duomenų srautų judėjimą korporacinės įmonės tinkle.
Išdėstyti serverius saugumo zonose taip, kad būtų kuo mažesni duomenų srautai tarp skirtingų zonų.

LITERATŪRA

- Mitchell B. An introduction to VPN software, VPN hardware and protocol solutions // http://compnetworking.about.com/od/vpn/l/aa010701a.htm, 2005-05-19
- Panda GateDefender (2005) // http://enterprises.pandasoftware.com/products/gatedefender/, 2005-05-19
- Slemp R. (2001) Firewall Architecture // www.nextep.com.au/upload/Firewall_Architecture.pdf, 2005-05-19
- Dobrucki M.(2002) Priorities in The Deployment of Network Intrusion Detection Systems // www.tml.hut.fi/~tpv/opiskelijat/dobrucki.pdf, 2005-05-19
- Jha S., Sheyner O., Wing J. (2003) The Formal Analyses of Attack graphs // http://www.cs.wisc.edu/~jha/jha-papers/security/CSFW_2002_1.pdf
- Sheyner O. (2004) Scenario Graphs and Attack Graphs // http://reports-archive.adm.cs.cmu.edu/anon/2004/CMU-CS-04-122.pdf, 2005-05-19
- (16)Markov chains and Markov processes (2005) // http://www.win.tue.nl/~iadan/sdp/h3.pdf, 2005-05-19
- (17)GPSS World Reference Manual (2001) // http://www.minutemansoftware.com/reference/rpreface.htm, 2005-05-19
- Venčkauskas A., Mikuckienė I., Mikuckas A. (2003) Įmonės informacinės saugos efektyvumo vertinimas. // Informacijos mokslai. Vilnius, T. 26, p. 90-93.
- Juniper Networks Firewall / IPSec VPN (2005) // http://www.juniper.net/products/integrated, 2005-05-19.
- Microsoft Internet Security and Acceleration (ISA) Server (2005) // http://www.microsoft.com/isaserver/evaluation/overview/default.mspx, 2005-05-19.
- GPRS intranetas, Cisco VPN (2005) // http://www.omnitel.lt/?m3_lt$206052_212539_212578_212932, 2005-05-19.