KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGA

TOMAS KAZAKEVIČIUS

DDoS ATAKŲ APTIKIMO METODŲ TAIKYMAS DIFERENCIJUOTŲ PASLAUGŲ ARCHITEKTŪROS TINKLUOSE

Magistro baigiamasis darbas

Darbo vadovas
doc. I. Lagzdinytė-Budnikė

KAUNAS, 2013

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGA

TOMAS KAZAKEVIČIUS

DDOS ATAKŲ APTIKIMO METODŲ TAIKYMAS DIFERENCIJUOTŲ PASLAUGŲ ARCHITEKTŪROS TINKLUOSE

Magistro baigiamasis darbas

Recenzentas
doc. dr. T. Adomkus
2013-05-25

Darbo vadovas
doc. I. Lagzdinytė-Budnikė
2013-05-25

Darbą atliko:
Tomas Kazakevičius
2013-05-25

KAUNAS, 2013

AUTORIŲ GARANTINIS RAŠTAS
DĖL PATEIKIAMO KŪRINIO

2013 - gegužės - 25 d.
Kaunas

Autoriai, _____ Tomas Kazakevičius**_____**
(vardas, pavardė)

_____,

patvirtina, kad Kauno technologijos universitetui pateiktas baigiamasis bakalauro (magistro) darbas (toliau vadinama – Kūrinys) DDoS ATAKŲ APTIKIMO METODŲ TAIKYMAS DIFERENCIJUOTŲ PASLAUGŲ ARCHITEKTŪROS TINKLUOSE
(kūrinio pavadinimas)

pagal Lietuvos Respublikos autorių ir gretutinių teisių įstatymą yra originalus ir užtikrina, kad

1) jį sukūrė ir parašė Kūrinyje įvardyti autoriai;
2) Kūrinys nėra ir nebus įteiktas kitoms institucijoms (universitetams) (tiek lietuvių, tiek užsienio kalba);
3) Kūrinyje nėra teiginių, neatitinkančių tikrovės, ar medžiagos, kuri galėtų pažeisti kito fizinio ar juridinio asmens intelektinės nuosavybės teises, leidėjų bei finansuotojų reikalavimus ir sąlygas;
4) visi Kūrinyje naudojami šaltiniai yra cituojami (su nuoroda į pirminį šaltinį ir autorių);
5) neprieštarauja dėl Kūrinio platinimo visomis oficialiomis sklaidos priemonėmis.
6) atlygins Kauno technologijos universitetui ir tretiesiems asmenims žalą ir nuostolius, atsiradusius dėl pažeidimų, susijusių su aukščiau išvardintų Autorių garantijų nesilaikymu;
7) Autoriai už šiame rašte pateiktos informacijos teisingumą atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Autoriai

Tomas Kazakevičius_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)

SANTRAUKA

Viena iš svarbiausių šiandien keliamų problemų yra įvairių sistemų, veikiančių internete, saugumo užtikrinimas. Viena iš plačiai naudojamų sistemų yra diferencijuotų paslaugų architektūros tinklai. Šia architektūra siekiama užtikrinti tam tikrų paslaugų kokybinius parametrus. Tačiau šio tipo architektūros tinklai yra pažeidžiami paskirstytomis paslaugų nutrauko atakomis (DDoS). Šio tipo atakos gali ženkliai įtakoti diferencijuotų paslaugų architektūros tinklo veikimą ir paslaugų užtikrinimą. Siekiant išvengti tinklo darbo sutrikdymo, atsiranda poreikis sukurti apsaugos nuo DDoS atakų sistemą.

Darbo rezultate pasiūlytas ir sukurtas apsaugos modulis, kuriame panaudotos įvairios srauto filtravimo taisyklės. Šiomis taisyklėmis siekiama aptikti atakos srautą pagal tam tikrus požymius ir jį atmesti. Taip pat atliekamas dinaminis taisyklių sudarymas blokuojant IP adresus.

Pasiūlyto atakų aptikimo/apsaugos modulio naudojimas diferencijuotų paslaugų architektūros tinkluose leidžia pasiekti didesnį saugumo lygį juose užtikrinant, kad neteisėtas srautas yra blokuojamas ir apdorojamas tik teisėtas srautas.

SUMMARY

One of the most important challenges of today are assure security of different types systems that are connected to Internet. One of the most widely used systems are differentiated service architecture networks. This architecture has to ensure certain quality of services parameters. However, this type of architecture networks are vulnerable to distributed denial of service attacks. This type of attacks can significantly influence the differentiated services architecture network operation and service assurance. In order to avoid network disruption, there is a need to build protection against DDoS attacks.

The result of this work is proposed and developed a security module, which uses various traffic filtering rules. These rules are intended to detect attack traffic according to certain attributes and reject it.

The proposed attack detection / protection module used in differentiated service architecture networks allows to achieve higher level of security in them to ensure that the illegal flow is blocked and treated only legitimate traffic.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

DSCP – **Differentiated Services Code Point.** Žymė naudojama nusakyti į kurią klasę perduoti paketą. Šiai žymei sudaryti naudojami šeši bitai ir ji įrašoma į ToS.

TCP – **Transmission Control Protocol.** Tai vienas iš pagrindinių protokolų, esančių Internetinių protokolų rinkinyje. TCP yra tarpinis lygis tarp IP ir aplikacijos bei priklauso transportavimo lygmeniui, pagal OSI kompiuterinių tinklų modelį. Naudodamos šį protokolą, aplikacijos gali sukurti jungtis tarp viena kitos ir dalintis duomenimis. Šis protokolas užtikrina patikimą duomenų perdavimą tarp dviejų tinklo taškų.

UDP – **User Datagram Protocol.** Šis protokolas nėra patikimas, neatlieka duomenų tėkmės kontrolės ir neturi klaidų atitaisymo mechanizmų. Daugeliu atvejų šitos funkcijas atliekamos aukštesniame pagal OSI lygmenyje, o **UDP** naudojamas tik persiųsti duomenis.

TCP/IP – **Transmission control protocol/Internet Protocol.** Standartinis duomenų perdavimo protokolų rinkinys, kurio pagrindu veikia Internetas bei daugelis privačių komercinių tinklų. Svarbiausi šio protokolo komponentai – TCP ir IP protokolai.

WRR – **Weighted round robin**. Tai eilių aptarnavimo disciplina.

AF – **Assure Forwarding PHB**. Užtikrinto perdavimo klasė. Skirta užtikrinti, kad paketai pasieks gavėją su didele tikimybę, tol kol neviršys nustatyto duomenų kiekio. Sudaryta iš keturių klasių.

EF – **Expedited Forwarding PHB.** Paspartinto perdavimo klasė. Užtikrina mažas paketų vėlinimo, praradimo ir vėlinimo skirtumų charakteristikas. Naudojamas balso, video ir kitoms realaus laiko paslaugoms.

BE – **Best-Effort Forwarding PHB.** Geriausių pastangų klasė. Taikoma paprastiems duomenų perdavimams, pvz. failų atsisiuntimui.

PHB – **Per-hop behavior**. Nusako taisykles tam tikrai taikomai paslaugos klasei.

ĮVADAS

Šiame XXI amžiuje, informacinių technologijų naudojimas yra kasdienybė. Informacinės technologijos sparčiai vystomos, kuriant naujas ar patobulinant senas. Informacinių technologijų dėka galime naudotis elektroninio pašto paslaugomis, perduoti duomenų kitiems kompiuteriams ar pasinaudoti kitomis paslaugomis. Tačiau, naudojantis šiomis technologijomis, susiduriama ne tik su privalumais, bet taip pat ir su tam tikrais pavojais. Tai įvairūs nusikaltimai elektroninėje erdvėje, kuriuos įvykdžius, dažnai organizacijoje išbalansuojami kasdieniai procesai, prarandama svarbi ir konfidenciali informacija, nukenčia organizacijos reputacija. Sukurti gerą IT sistemų apsaugą tampa nelengvu uždaviniu.

Virtualioje erdvėje naudojama daug priemonių, kurios gali sutrikdyti įprastą IT sistemos darbą. Tai gali būti įvairūs virusai, atakos nukreiptos į neapsaugotas sistemas.

Šiomis dienomis susiduriama su dar viena populiaria atakų rūšimi – paslaugų nutraukimo arba paskirstytomis paslaugų nutraukimo atakomis. Šių atakų tikslas – išnaudoti pavienių įrenginių ar tam tikrų sistemų turimus resursus, pvz.: tinklo srauto užtvindymas suklastotais paketais ar tam tikrais atsakymais į pateiktą klaidingą užklausą. Įvykdžius tokią ataką, įrenginys negalės tam tikrą laiką funkcionuoti, kadangi bus išnaudoti jo resursai. Tokios atakos yra trumpalaikės, kadangi įrenginys po tam tikro laiko vėl gali veikti, tačiau padarančios ypač daug žalos, ypatingai sistemoms, kurios teikia nepertraukiamas, svarbias paslaugas plačiam vartotojų ratui.

Problema

Dauguma interneto tiekėjų savo tinklo infrastruktūroje yra įdiegę eilę duomenų srautų kokybę užtikrinančių mechanizmų ir priemonių. Diferencijuotų paslaugų architektūros tinklai – vienas iš būdų kaip būtų galima užtikrinti duomenų srautų, o tuo pačiu ir paslaugų, kokybę. Ši tinklo architektūra leidžia užtikrinti realaus laiko paslaugoms - greitą duomenų perdavimą su mažais paketų praradimais ir vėlinimais, kitoms paslaugoms - tam tikrus jų specifinius reikalavimus duomenų srauto perdavimui. Deja ir šios sistemos yra pažeidžiamos paslaugų nutraukimo atakomis. Įvykus tokiam incidentui sistema nebegali kokybiškai perduoti paslaugų su joms skirtais kokybės reikalavimais, o vartotojas nebegali gauti kokybiškų paslaugų.

Šiuo metu ieškoma įvairių būdų kaip užkirsti kelią šioms atakoms ir apsaugoti diferencijuotų paslaugų architektūros tinklus nuo jų resursų eikvojimo.

Darbo tikslas ir uždaviniai

Pagrindinis šio darbo tikslas - ištirti egzistuojančių DDoS atakų aptikimo būdų pritaikymo diferencijuotų paslaugų architektūros tinklams galimybes bei pasiūlyti DDoS atakų aptikimo diferencijuotų paslaugų architektūros tinkluose modelį.

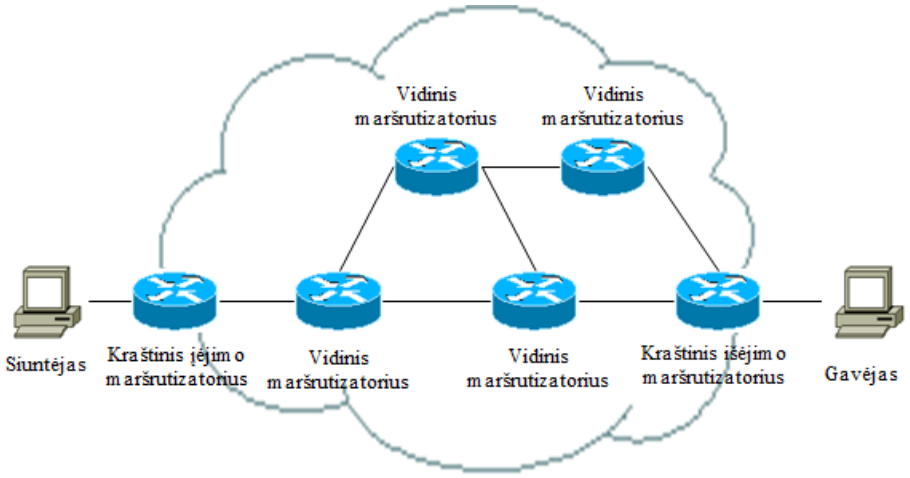
Uždaviniai:

1. Išanalizuoti diferencijuotų paslaugų architektūros tinklų savybes ir identifikuoti labiausiai pažeidžiamus tokių tinklų segmentus;
2. Išanalizuoti DoS ir DDoS atakas, identifikuoti jų tipus, požymius bei aptikimo būdus;
3. Ištirti egzistuojančių DDoS atakų aptikimo būdų pritaikymo diferencijuotų paslaugų architektūros tinklams galimybes;
4. Pasiūlyti DDoS atakų aptikimo diferencijuotų paslaugų architektūros tinkluose modelį;
5. Suprojektuoti ir realizuoti sistemą, naudojančią vieną ar kelis diferencijuotų paslaugų architektūros tinklams adaptuotus DDoS atakų aptikimo ir sustabdymo būdus;
6. Atlikti sukurtos DDoS aptikimo sistemos eksperimentinį įvertinimą.

1 DIFERENCIJUOTŲ PASLAUGŲ ACHITEKTŪROS TINKLAI

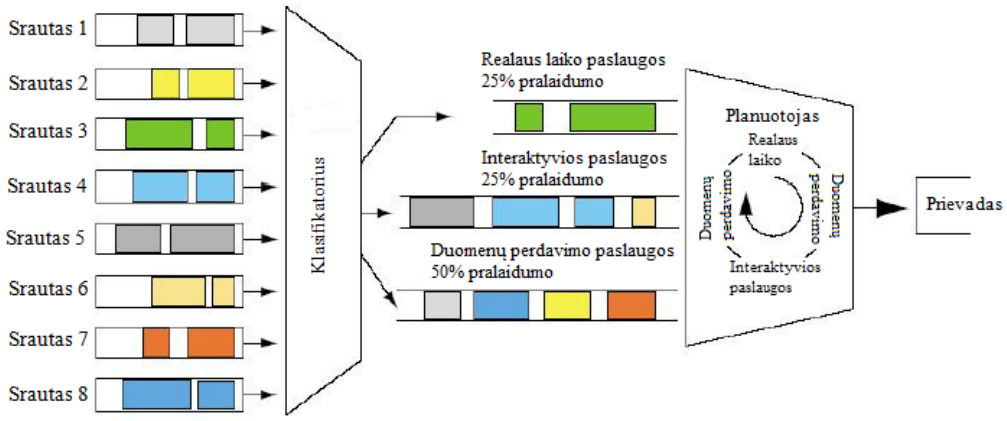
1.1 Diferencijuotų paslaugų domenas

Diferencijuotų paslaugų architektūra įgyvendinama realizuojant diferencijuotų paslaugų domeną, kurio ribose yra taikomos architektūroje apibrėžtos taisyklės ir reikalavimai. Diferencijuotų paslaugų domeną remiantis dokumentu [1] sudaro vidiniai ir kraštiniai maršrutizatoriai (žr. 1 pav.). Kraštiniame įėjimo maršrutizatoriuje atliekamas paketų klasifikavimas ir žymėjimas. Vidiniuose maršrutizatoriuose realizuojamos paspartinto perdavimo klasė [2], garantuoto perdavimo klasė [3], ir geriausių pastangų klasė [4]. Kraštiniame išėjimo maršrutizatoriuje atliekamas srauto matavimas, paketų vėlinimas ar atmetimas. Paketai atėję iš kraštinio maršrutizatoriaus yra nukreipiami į tam tikrą klasę pagal atitinkamą žymę.



1 pav. Diferencijuotų paslaugų architektūra

2 pav. pavaizduota, kaip atliekamas paketų klasifikavimas į klases: ateinantis srautas pirmiausia patenka į kraštinį maršrutizatorių, kur yra klasifikuojamas ir pažymimas.



2 pav. WRR eilių aptarnavimo disciplina [5]

Paketas gali būti klasifikuojamas pagal siuntėją, TCP ar UDP protokolus ir prievadus ar DSCP reikšmę. Žymėjimas vyksta į paketo ToS antraštę įrašant DSCP žymę. Tokiu būdu paketai yra skirstomi į tam tikras paslaugos klases ir išdėstomi į eilę. Tada kiekviena eilė yra aptarnaujama sukimosi principu pagal tam tikrus eilių aptarnavimo algoritmus. Šitaip paketai yra perduodami į kitą maršrutizatorių. Vėliau vyksta paketų apribojimas arba atmetimas pagal tam tikras taisykles.

PHB (Per-hop behavior) – nusako paketų apdorojimo taisykles taikomas tam tikrai paslaugos klasei. Yra keletas tipų tokių taisyklių rinkinių:

- Geriausių pastangų – taikoma paprastiems duomenų perdavimams, pvz. failų atsisiuntimui.
- Paspartinto perdavimo – užtikrina mažas paketų vėlinimo, praradimo ir vėlinimo skirtumų charakteristikas. Naudojamas balso, video ir kitoms realaus laiko paslaugoms.
- Užtikrinto perdavimo – skirta užtikrinti, kad paketai pasieks gavėją su didele tikimybę, tol kol neviršys nustatyto duomenų kiekio.

Kraštiniame įėjimo maršrutizatoriuje siekiant tinkamai pažymėti ateinančius paketus, pirmiausia reikia juo išanalizuoti pagal tam tikrus požymius, pvz., jei gaunami duomenų paketai, kurių dydis yra 100-200 baitų ir naudojamas UDP protokolas, galima teigti, kad naudojamasi realaus laiko paslaugomis ir šiems paketams turi būti uždėta atitinkama žymė, pagal kurią jie apdorojami toliau, t.y. turi patenka į paspartinto perdavimo klasę, kurioje užtikrinami maži paketų praradimai ir vėlinimai. Vidiniuose maršrutizatoriuose paketai pagal savo žymę patenka į tam tikrą klasę, kuri turi užtikrinti kokybinius reikalavimus (paketų vėlinimai, praradimai ir pan). Taip pat atitinkamai paketai gali būti pažymimi žymėmis, kurios užtikrins jų perdavimą į garantuoto bei geriausių pastangų klases ir atitinkamą tose klasėse nustatytą paketų apdorojimą.

Kadangi kraštiniame įėjimo maršrutizatoriuje atliekamas paketų analizavimas pagal tam tikrus požymius ir jų žymėjimas bei klasifikavimas, todėl labai svarbu užtikrinti šio maršturizatoriaus korektišką veikimą. Atakos atveju, į šį maršrutizatorių gali būti siunčiami labai dideli duomenų kiekiai, kuriuos jis turės aptarnauti. Tokiu atveju maršrutizatorius gali nebespėti apdoroti šių duomenų kiekių (pagal savo turimas technines charakteristikas - CPU, atmintis ir pan) ir teisėtas srautas taip pat bus neapdorojamas.

Todėl reikia sukurti apsaugos priemonę, kuri padėtų apsisaugoti nuo atakų, pvz., atakos srautas būtų blokuojamas ir neapdorojamas šio maršrutizatoriaus.

1.2 Diferencijuotų paslaugų domeno sauga

Diferencijuotų paslaugų domeno tinkle egzistuoja kelios pasitikėjimo erdvės [6], kurios yra būtinos geram diferencijuotų paslaugų domeno veikimui. Šias pasitikėjimo erdves sudaro:

- Pasitikėjimas tarp kraštinio maršrutizatoriaus ir siuntėjo;
- Pasitikėjimas tarp vidinio ir kraštinio maršrutizatoriaus;
- Pasitikėjimas paslaugų tiekėjais.

1.2.1 Pasitikėjimas tarp kraštinio maršrutizatoriaus ir siuntėjo

Ateinantys paketai iš siuntėjo pirmiausia yra kontroliuojami kraštiniame įėjimo maršrutizatoriuje. Norint teisingai kontroliuoti ar pažymėti paketą siuntėjas turi atitikti tam tikrus reikalavimus nustatytus kraštiniame maršrutizatoriuje. Šie maršrutizatoriai pasitiki, kad šaltinis atitinka reikalavimus, norint tinkamai valdyti paketus.

1.2.2 Pasitikėjimas tarp vidinio ir kraštinio maršrutizatoriaus

Pagrindinis diferencijuotų paslaugų architektūros tikslas yra supaprastinti vidinių maršrutizatorių veikimą, kad galėtų sparčiai perduoti paketus į atitinkamą srauto klasę. Vidiniai maršrutizatoriai pasitiki kraštiniais maršrutizatoriais, kad jie atliko teisingą paketų žymėjimą ir kontroliavimą.

1.2.3 Pasitikėjimas paslaugų tiekėjais

Korektiškas paspartinto ir garantuoto perdavimo klasių veikimas priklauso nuo interneto paslaugų tiekėjų nustatymų. Jei šios klasės yra perkrautos labai dideliu srautu, šių klasių veikimas gali žymiai sumažėti. Todėl maršrutizatoriai turi būti gerai sukonfigūruoti, kad nekiltų problemų užtikrinti klasių našumą.

1.2.4 Grėsmės diferencijuotų paslaugų domeno tinklo saugumui

Pasitikėjimo erdvės, kurios egzistuoja diferencijuotų paslaugų domeno architektūroje gali sukelti keletą rimtų saugumo grėsmių: paslaugų nutraukimo atakos ir išteklių išnaudojimas.

Išteklių išnaudojimas

Išteklių išnaudojimas gali atsirasti keliose domeno vietose. Šį išnaudojimą galima traktuoti kaip tinklo pralaidumo sumažinimą siunčiant papildomus suklastotus paketus. Tinklo pralaidumo išnaudojimas gali būti įvykdytas kraštiniuose ir vidiniuose maršrutizatoriuose. Dalis pralaidumo

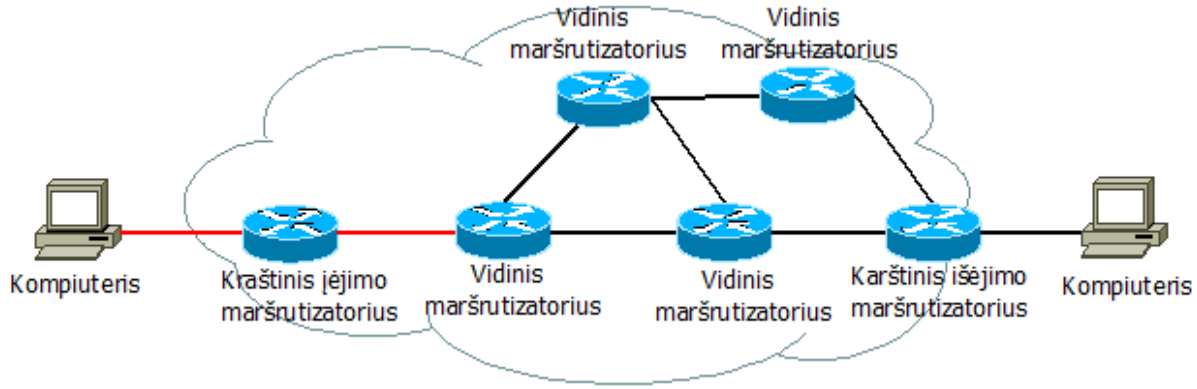
kraštiniuose maršrutizatoriuose išnaudojama bereikalingai, jei paketai yra klastojami. Vidiniuose maršrutizatoriuose pralaidumas išnaudojamas tada, kai kraštiniai maršrutizatoriai perduoda paketus į vidinius maršrutizatorius jų neapdorodami.

Paslaugų nutraukimo ataka

Viena iš pagrindinių problemų su kuria susiduria diferencijuotų paslaugų domenas yra paslaugų nutraukimo ataka. Ši ataka gali pasireikšti kraštiniame maršrutizatoriuje. Kadangi šis maršrutizatorius kontroliuoja srautus, tai paprasčiausias būdas atlikti paslaugų nutraukimo ataką yra siųsti duomenis su suklastotu šaltinio adresu, siekiant užkirsti legalaus srauto patekimui i domeną.

Paslaugų nutraukimo ataką galima įvykdyti ir domeno kraštiniame išėjimo maršrutizatoriuje, kuris jungiasi su kitais interneto tiekėjų maršrutizatoriais. Tokiu būdu apkraunamas esamo domeno kraštinis išėjimo maršrutizatorius arba kito domeno kraštinis įėjimo maršrutizatorius bandant apriboti srautą. Šis atakos tipas reikalauja, kad atakuotojas bandantis atlikti šią ataką žinotų tinklo topologiją.

Atakos tikslas taip pat gali būti ir vidinių maršrutizatorių pažeidimas. Kadangi šiuose maršrutizatoriuose realizuotos paslaugų perdavimo klasės, jas apkraunant nereikalingu srautu, gali suprastėti šių klasių našumas, t.y. paketai, kurie turi būti perduodami su tam tikrais paslaugų kokybės reikalavimais, nebus tinkamai perduoti.



3 pav. Domeno pažeidžiamos vietos

Remiantis 1.1.1 – 1.1.3 skyriuose aptarta informacija, 3 pav. raudona spalva pažymėtos pažeidžiamos diferencijuotų paslaugų domeno vietos. Pirmoji pažeidžiama vieta yra tinklo segmentas tarp vartotojo (arba paslaugos gavėjo) kompiuterio ir kraštinio įėjimo maršrutizatoriaus. Antroji pažeidžiama vieta yra tinklo segmentas tarp kraštinio įėjimo ir vidinio maršrutizatorių.

Labai svarbu yra užtikrinti pirmojo tinklo segmento saugą (ryšys tarp kompiuterio ir kraštinio įėjimo maršrutizatoriaus), nes neapsaugojus kraštinio įėjimo maršrutizatoriaus, šis praleis į domeno vidų tiek teisėtus, tiek neteisėtus srautus, tokiu būdu pakenkdamas viso domeno kokybiškam funkcionavimui.

Apsaugojus šį mazgą, galima daryti prielaidą, kad neteisėti srautai į domeno vidų nepraleidžiami, todėl grėsmės vidiniams domeno maršrutizatoriams ir domeno viduje esantiems duomenų srautams išnyksta.

Šio darbo metu siekiama sukurti apsaugos sprendimą kraštiniams diferencijuotų paslaugų domeno maršrutizatoriams.

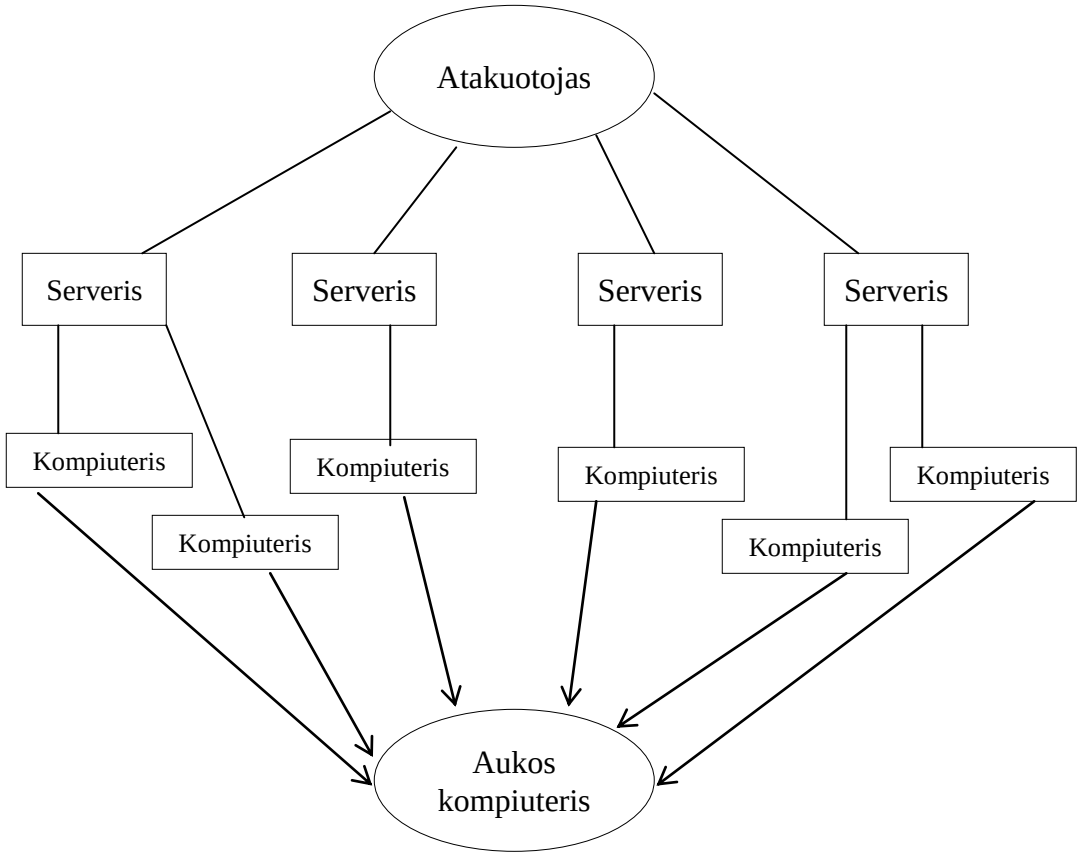
1.3 Skyriaus išvados

Diferencijuotų paslaugų domeno tinklai naudojami perduoti duomenų srautą, atitinkantį tam tikrus kokybinius rodiklius, nuo siuntėjo iki gavėjo. Šį domeną sudaro kraštiniai ir vidiniai maršrutizatoriai. Šiuose maršrutizatoriuose atliekami paketų žymėjimai ir skirstymas į tam tikras klases, kurios turi užtikrinti perduodamų duomenų kokybės parametrus. Tačiau šie domenai yra pažeidžiami DDoS atakų. Šios atakos nukreiptos į diferencijuotų paslaugų domeno tinklus, gali sutrikdyti įprastą jų veikimą, pvz., išeikvoti tinklo pralaidumą ar maršrutizatoriaus resursus. Įvykus šios atakoms, diferencijuotų paslaugų domeno tinkluose sumažės perduodamų duomenų kokybė, gali atsirasti paketų praradimai, vėlinimai ir pan.

Atsižvelgiant, kad diferencijuotų paslaugų architektūros tinklai yra pažeidžiami reikalingos tam tikros apsaugos priemonės, galinčios aptikti ar bent iš dalies sustabdyti DDoS atakas. Diferencijuotų paslaugų architektūros tinkluose labiausiai pažeidžiamos vietos yra tarp siuntėjo ir kraštinio maršrutizatoriaus, bei kraštinio ir vidinio maršrutizatoriaus. Todėl labai svarbu užtikrinti kraštinio maršrutizatoriaus pastovų veikimą ir apsaugą nuo atakų. Neapsaugojus šio maršrutizatoriaus nuo atakų, sutrikdomas viso domeno veikimas, neužtikrinama reikiama paslaugų kokybė.

2 DOS IR DDOS ATAKŲ TIPAI, JŲ APTIKIMAS

Šiomis dienomis interneto vartotojai gali susidurti su daug pavojų keliančiais veiksniais, pvz.: virusinė programa veikianti vartotojo kompiuteryje, prisijungimo duomenų pavogimas ir pan. Taip pat viena iš populiaresnių grėsmių yra DoS – Denial of Service [7] arba DDoS – Distributed Denial of Service [8] atakos. Šios atakos vadinamos paslaugų nutraukimo atakomis arba paskirstytomis paslaugų nutraukimo atakomis. Tipinė paskirstyta paslaugų nutraukimo ataka parodyta 4 pav.



4 pav. Paskirstyta paslaugų nutraukimo ataka

Šiomis atakomis siekiama sukliudyti vartotojui naudotis internetinėmis paslaugomis, kadangi į aukos kompiuterį siunčiami maži duomenų paketai, kuriuose inicijuojamas sujungimas su kitais kompiuteriais. Tokiu būdu išnaudojami visi aukos kompiuterio resursai ir jis nebegalės pasinaudoti internetinėmis paslaugomis. Taip pat šios atakos gali būti panaudotos ir prieš internete veikiančias paslaugas, pvz.: serverius, teikiančius specifines paslaugas kaip svetainės saugojimas juose, arba panaudojamos kompiuterių tinklų funkcionavimo sutrikdymui.

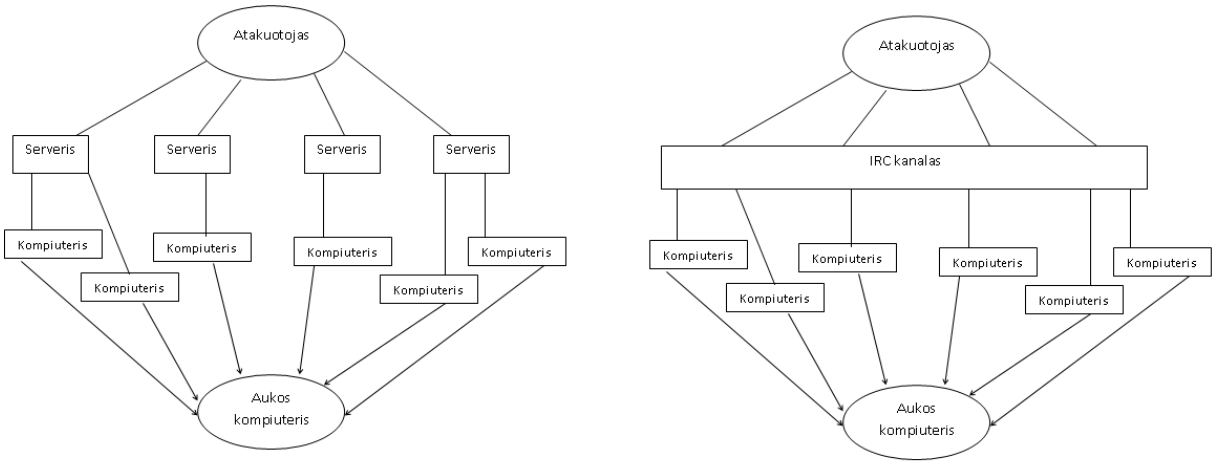
Šios atakos gali būti atliekamos įvairiais būdais:

1. Kompiuterio resursų išnaudojimas: kietojo disko talpa, procesoriaus išnaudojimas, tinklo srautas.

2. Maršrutų lentelių sugadinimas.
3. Ryšio tarp dviejų bendraujančių vartotojų nutraukimas.

2.1 DDoS atakų architektūros

DDoS atakų architektūros yra dviejų tipų: serverių („valdytojų“) ir „zombių“ kompiuterių (Agent-Handler) [9] modelis ir Internet Relay Chat (IRC) [9] modelis. „Agent-Handler“ modelis sudarytas iš atakuotojų, serverių ir „zombių“ kompiuterių, kurie prijungti prie serverio. Atakuotojas naudoja serverius, kad nustatytų kurie kompiuteriai yra aktyvūs, tam kad galėtų įvykdyti ataką (žr. 5 pav. (a)).



(a) (b)

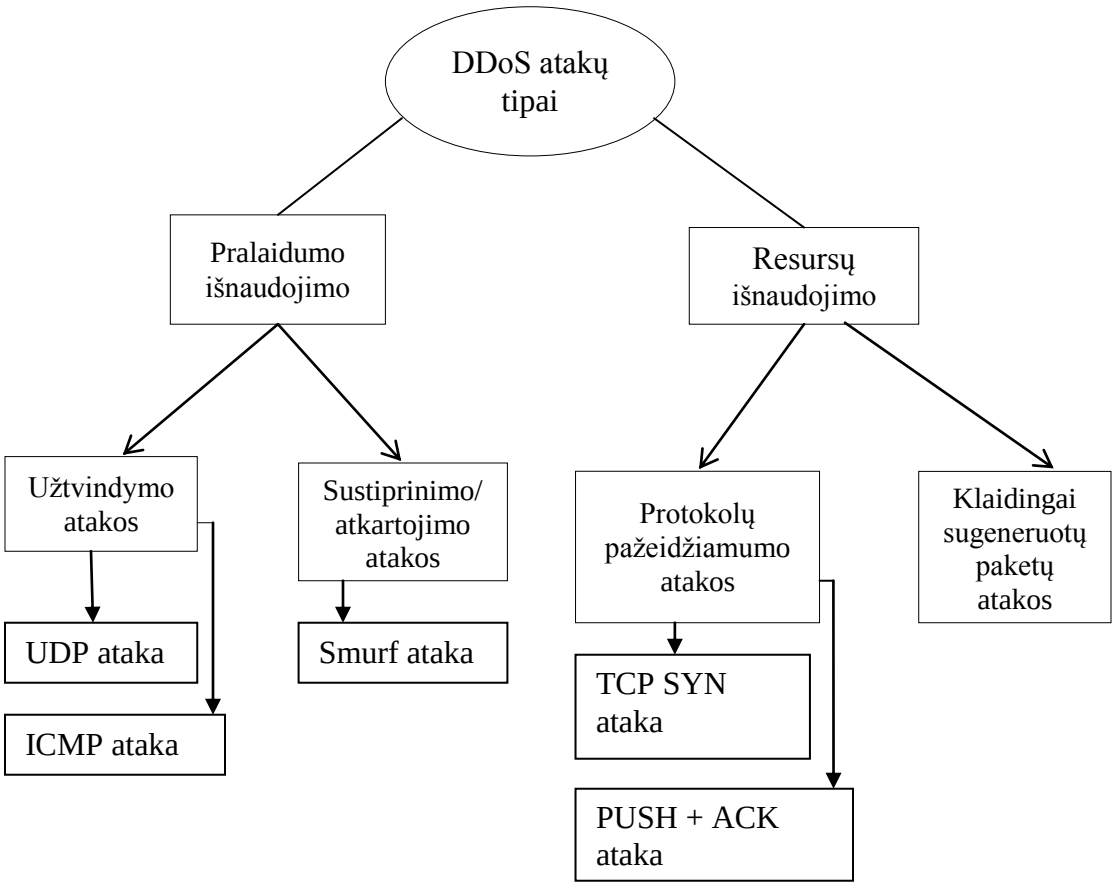
5 pav. DDoS atakų architektūros: (a) Agent-Handler modelis, (b) Internet Relay Chat modelis

IRC pagrindu veikianti DDoS atakų architektūra panaši į prieš tai minėtą, tačiau atakuotojas naudoja IRC kanalą tam, kad galėtų tiesiogiai valdyti „kompiuterinių zombių“ tinklą. Modelio iliustracija pateikta 5 paveiksliuke.

2.2 DDoS atakų tipai

Yra dvi pagrindinės DDoS atakų klasės: pralaidumo išnaudojimo ir resursų išnaudojimo. Pralaidumo išnaudojimo atakos paremtos tuo, kad naudojamos užtvindyti aukos naudojamą tinklą nepageidaujamu srautu, užkertant kelią teisėtam srautui pasiekti gavėją.

Resursų išnaudojimo atakos naudojamos išeikvoti visus aukos kompiuterio resursus taip sutrikdant kompiuterio darbą.

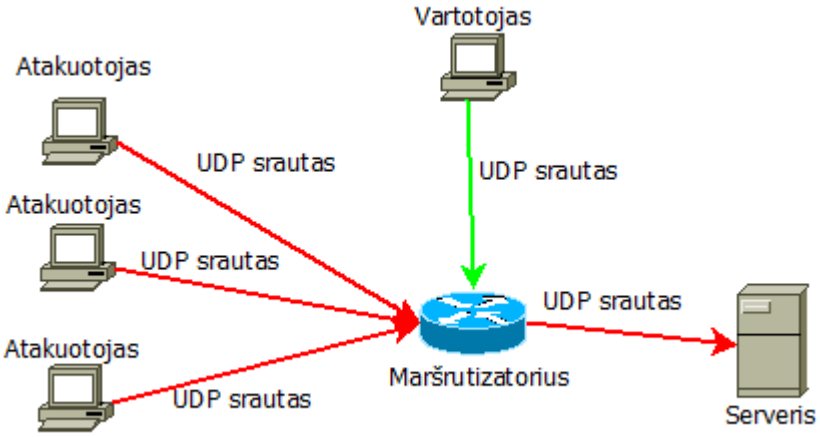


6 pav. DDoS atakų tipų klasifikacija

Pralaidumo išeikvojimo atakos gali būti apibūdinamos kaip užtvindymo arba atkartojimo (stiprinimo) atakos. Užtvindymo atakos atliekamos naudojant „zombių“ kompiuterius, kurie siunčia didelius kiekius srauto į aukos kompiuterį. Tokiu atveju kompiuteris gali sulėtėti ar būti neveiksnus. Šio tipo atakoms atlikti naudojamas UDP ir ICMP protokolai.

2.2.1 UDP protokolo užtvindymo ataka

UDP protokolo užtvindymo atakos metu yra siunčiami dideli kiekiai šio protokolo paketų į aukos kompiuterį pasirenkant atsitiktinius ar tikslius prievadus. Tokiu atveju aukos kompiuteris stengsis apdoroti gautus paketus siekiant nustatyti kokioms programoms šie paketai yra siunčiami.

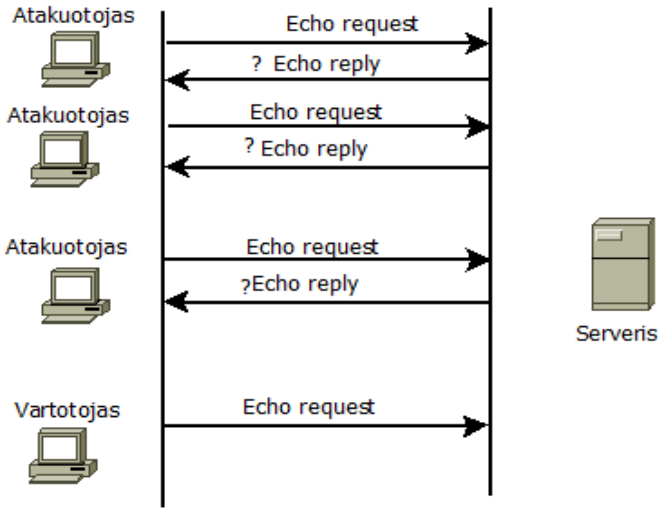


7 pav. UDP protokolo užtvindymo ataka

7 pav. Pavaizduota, kad atakuotojai siunčia didelius UDP protokolo paketus į serverį ir taip išnaudoja maksimalų prisijungimų skaičių prie serverio. Viršijus šį limitą vartotojai negalės pasiekti serverio.

2.2.2 ICMP protokolo užtvindymo ataka

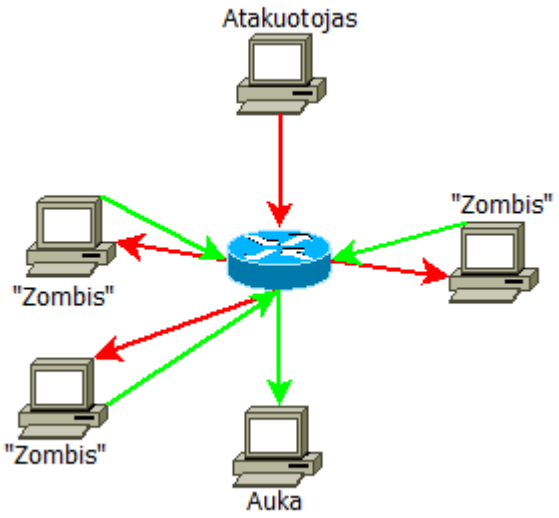
ICMP protokolo užtvindymo atakos atliekamos tada, kai atakuotojai siunčia didelius kiekius „ping“ paketų su suklastotu siuntėjo IP adresu į aukos kompiuterį. Tada aukos kompiuteris bando atsakyti į užklausą ICMP ECHO REPLY paketu (žr. 8 pav.). Šiuo būdu taip pat išnaudojamas tinklo pralaidumas.



8 pav. ICMP protokolo užtvindymo ataka

2.2.3 ICMP srautu pasižyminčios atakos

Šiame sraute naudojama „smurf“ [10] tipo ataka, kuri yra tinkamiausia norint atlikti paslaugų nutraukimo ataką viešame internete. Ši ataka naudojama blogai sukonfigūruotose tinklo įrenginiuose, kurie gali transliacijos būdu siųsti paketus visiems kompiuteriams esantiems tam tikrame tinkle. Tada atakuotojas siunčia daug IP paketų su suklastotu šaltinio adresu. Tokiu būdu greitai išnaudojamas tinklo srautas ir kompiuteriai negali tinkamai veikti.

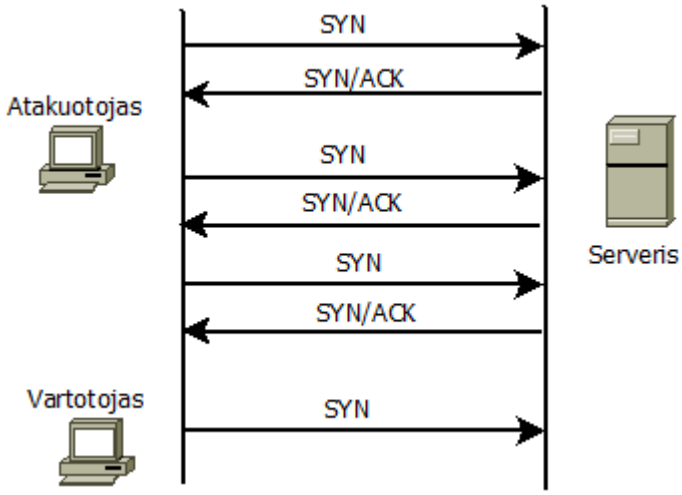


9 pav. Smurf ataka

9 paveiksliuke pateikta „smurf“ tipo ataka, kai atakuotojas siunčia paketus su suklastotu siuntėjo IP adresu transliacijos būdu tinkle esantiems įrenginiams. Atakuotojo siunčiamų duomenų kryptis pažymėta raudona linija. Tuo tarpu visi tinkle esantys kompiuteriai atsako į užklausas siuntėjui, t.y. aukai. Atsakymo kryptis pažymėta žalia linija.

2.2.4 TCP SYN paketų srautas

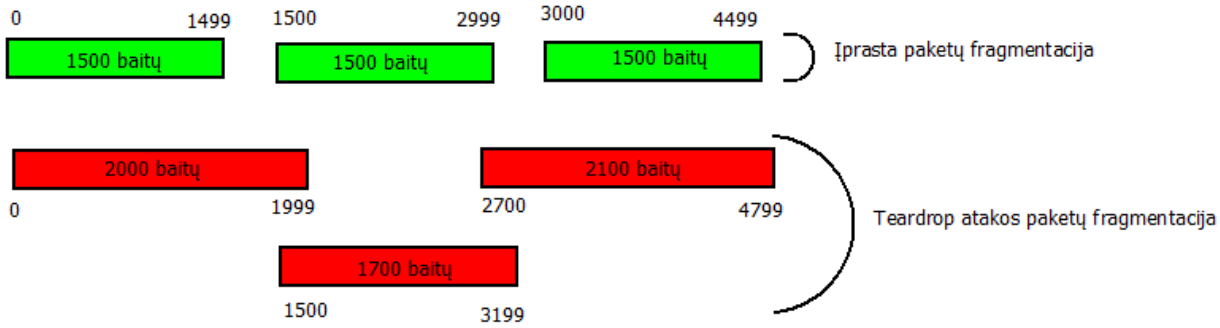
Šios atakos metu (žr. 10 pav) atakuotojas siunčia „TCP/SYN“ paketų srautą [9] su suklastotu siuntėjo adresu. Šie paketai inicijuoja susijungimą, todėl įrenginys atsako į šiuos susijungimus „TCP/SYN-ACK“ paketais ir laukia atsako iš siuntėjo. Kadangi siuntėjo adresas yra suklastotas, todėl įrenginys negaus jokio atsako iš siuntėjo. Tokiu būdu įrenginyje lieka daugybė pradėtų susijungimų, kurie naudoja įrenginio resursus ir tokiu būdu įrenginys negali priimti naujų susijungimų.



10 pav. TCP SYN ataka

2.2.5 Teardrop ataka

Teardrop ataka [11] pasižymi tuo, kad siunčiami suklastoti IP paketų fragmentai į aukos kompiuterį. Įprastai dideli paketai yra skaidomi į mažesnius paketus, kurių maksimalus dydis yra 1500 baitų. Tačiau atakos metu, yra klastojamas paketų fragmentacijos dydis ir tokiu būdu galimas kompiuterio sisteminės įrangos „nulūžimas“.

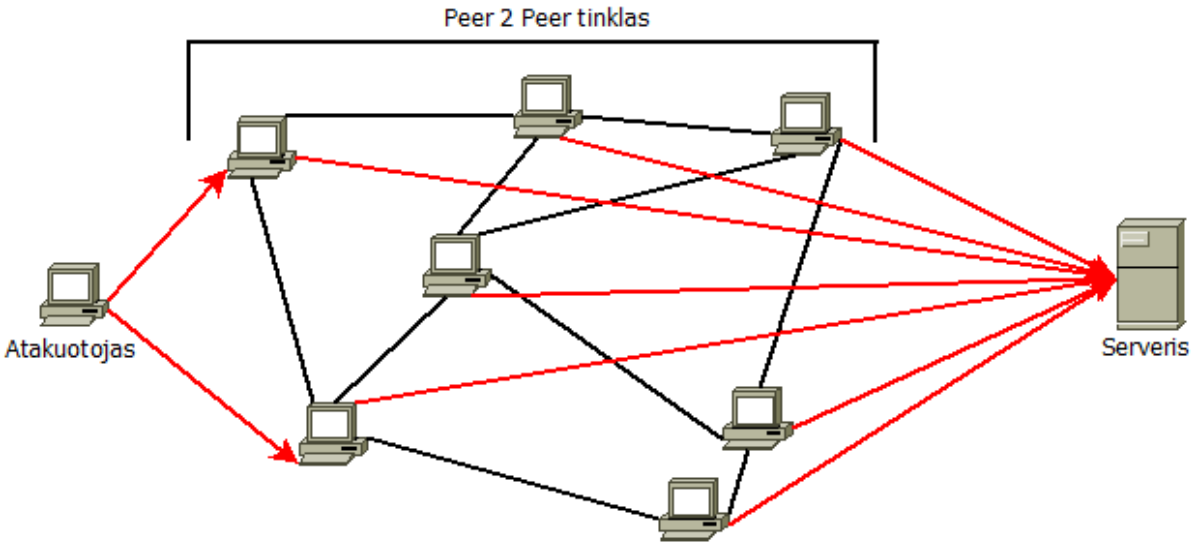


11 pav. Teardrop ataka

2.2.6 Taškas į tašką ataka

Atakuotojai surado būdą kaip pasinaudoti spragomis taškas į tašką tinkle siekiant atlikti paskirstytą paslaugų nutraukimą. Viena iš agresyviausių taškas į tašką paskirstytų paslaugų nutraukimo atakų gali būti atliekama pasinaudojant duomenų dalijimosi programa. Taškas į tašką ataka [12] (žr. 12 pav) skiriasi nuo įprastos kompiuterinių „zombių“ atakos. Atakuotojas atlieka „lėlių marionetės“ vaidmenį, kuris nurodo dideliam taškas į tašką failų dalijimosi klientų tinklui atsijungti nuo esamo tinklo ir jungtis prie aukos internetinio puslapio. Tokiu būdu daugybė kompiuterių bandys agresyviai jungtis prie internetinės svetainės. Dauguma internete esančių serverių gali užtikrinti tik kelis šimtus

susijungimų per sekundę, todėl esant keliems tūkstančiams ir daugiau susijungimų per sekundę, serveriai pradeda nebeveikti.



12 pav. Peer 2 Peer ataka

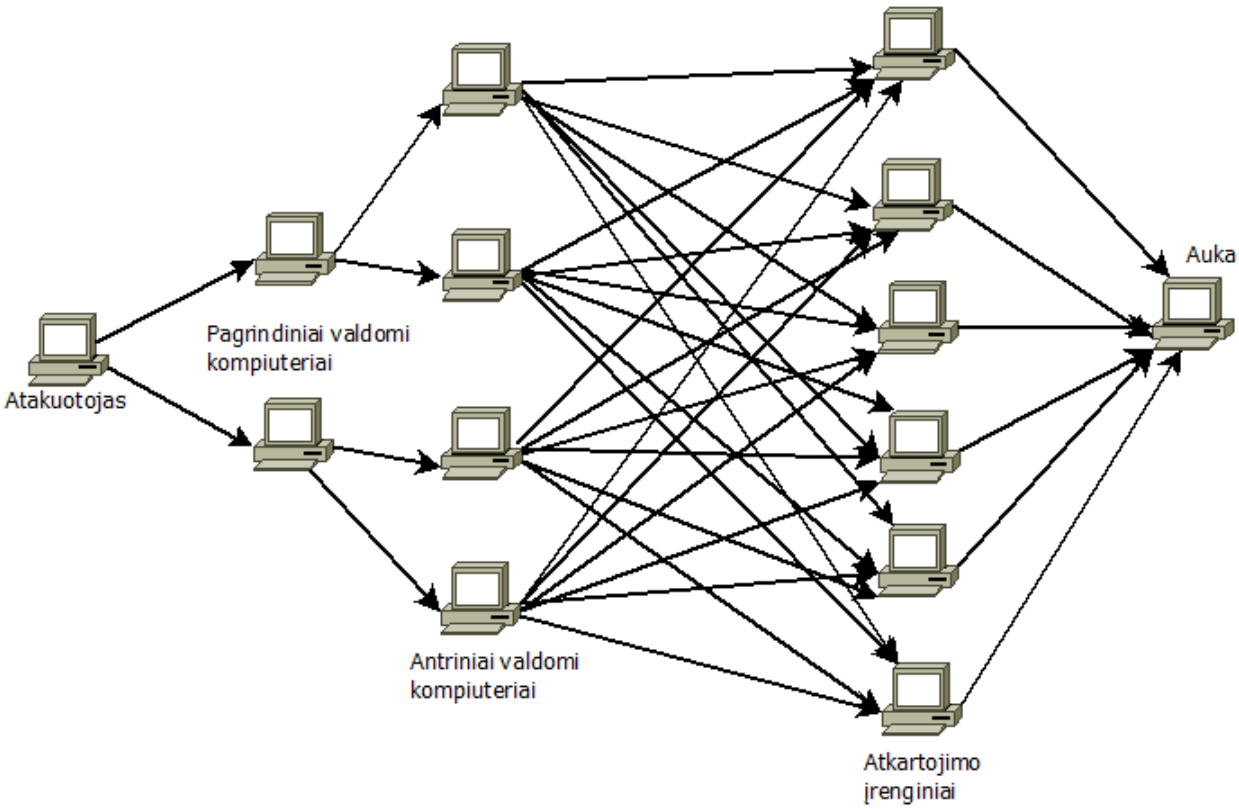
2.2.7 Ilgalaikė paslaugų nutraukimo ataka

Įvykdžius ilgalaikę paslaugų nutraukimo ataką [13] (PDoS – permanent denial of service) galima sugadinti sistemą ar įrenginį taip sunkiai, kad gali tekti pakeisti techninę įrangą. Ši ataka pasižymi saugumo pažeidžiamumais, kuriuos atakuotojas suradęs gali prisijungti prie nutolusio įrenginio, kaip maršrutų parinktuvo, spausdintuvo ar prie kitos įrangos esančios tinkle. Atakuotojas naudoja šiuos pažeidžiamumus pakeičiant įrenginio esamą mikroprogramine įrangą į modifikuotą ar sugadintą, tokiu būdu išvedant įrenginį iš įprasto veikimo. Toks įrenginys nebegalės atlikti įprastų veiksmų, kol nebus sutaisytas ar pakeistas.

Šis atakos tipas yra naudojamas pažeisti įrenginių techninę įrangą ir taip pat yra paprastesnis bei reikia mažiau resursų nei atliekant DDoS atakas.

2.2.8 Atkartota ataka

Paskirstyta atkartota paslaugų nutraukimo ataka (DRDoS – Distributed Reflected Denial of Service) [14] siunčia suklastotas tam tikro tipo užklausas dideliam kiekiui kompiuterių, kurie atsako į užklausą. Atliekant IP adresų klastojimą, nurodomas aukos IP adresas kaip siuntėjo IP adresas į kurį ateina atsakymai į užklausas iš kitų kompiuterių.



13 pav. Atkartota ataka

2.3 DDoS atakų palyginimas

1 lentelėje pateiktas aptartų DDoS atakų palyginimas pagal atakoje naudojamą protokolą bei atakos tikslą.

1 lentelė. Atakų palyginimai

Atakos pavadinimas	Naudojamas protokolas	Paskirtis
UDP užtvindymo ataka	UDP	Išeikvoti tinklo srautą, siunčiant didelius kiekius UDP protokolo paketus į pasirinktus prievadus
ICMP užtvindymo ataka	ICMP ECHO	Išeikvoti tinklo srautą, siunčiant didelius kiekius „ping“ paketų į aukos kompiuterį.
Smurf ataka	ICMP ECHO REQUEST	Išnaudoti tinklo srautą, kad kompiuteriai negalėtų tinkamai komunikuoti tarpusavyje
TCP SYN flood ataka	TCP	Užkimšti serverį ar paprastą kompiuterį inicijuotais susijungimais, kurie nėra iki galo patvirtinami
Teardrop ataka	UDP	Sugadinti operacinę sistemą, siunčiant suklastotus IP fragmentus su dideliais apkrovos kiekiais, kurių sistemą negali apdproti
Taškas į tašką ataka	TCP	Nutraukti esamus susijungimus tarp vartotojų kompiuterių, o naujus susijungimus nukreipti į atakuojamąjį serverį.
Ilgalaikė paslaugų nutraukimo ataka	-	Sugadinti įrenginio programinę įrangą, kad jis negalėtų tinkamai funkcionuoti, kol nebus ištaisytos atsiradusios programinės įrangos klaidos
Atkartojimo ataka	TCP, ICMP	Užtvindyti aukos kompiuterį atsakymų pranešimais iš serverių į kuriuos atakuotojas pasiuntė užklausas.

Palyginimo rezultatai rodo, kad dauguma atakų yra atliekamos naudojant TCP protokolą. Šis protokolas naudingas tuo, kad dauguma atakų remiasi suklastotais susijungimais ar užklausomis į kuriuos reikia atsakyti. Tokiu būdu yra išnaudojami tinklo ar kompiuterio esami resursai užkertant galimybę tinkamai naudotis paslaugomis.

Nors šios atakos šiek tiek skiriasi viena nuo kitos, tačiau pagrindinis jų tikslas yra išnaudoti esamus resursus, sutrikdant įprastą tinklo įrenginių veikimą.

Atsižvelgiant į atakos pobūdį, joje naudojamus parametrus, tokius kaip protokolas, paketų dydžiai ir kitą informaciją, galima sukurti ugniasienės taisykles, kurios galėtų filtruoti paketus pagal šiuos parametrus. Tokiu atveju būtų galima sumažinti kenkėjiškų paketų patekimą į diferencijuotų paslaugų domeno vidinius maršrutizatorius.

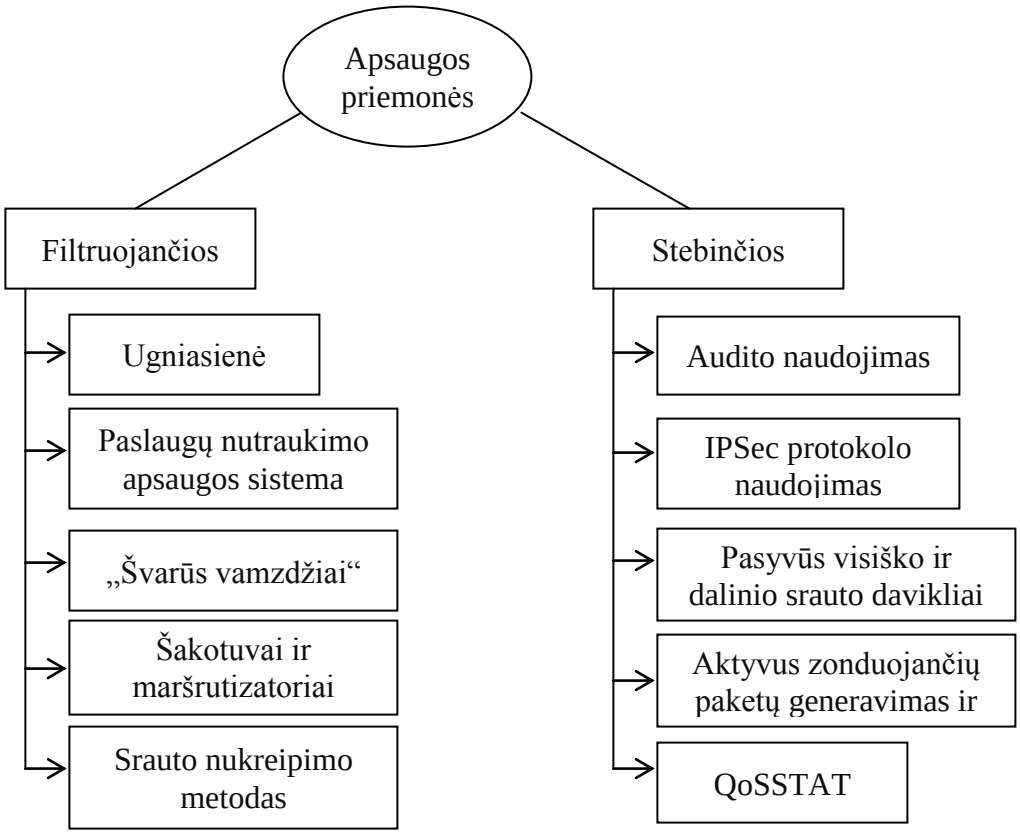
2.4 Skyriaus išvados

DDoS atakų tipų yra įvairių, vienos atakos naudojamos tinklo pralaidumui išnaudoti, kitos resursų išnaudojimui. Taip pat šios atakos naudoja skirtingus protokolus, todėl sukurti apsaugos priemonę, kuri galėtų tiksliai identifikuoti ir blokuoti vykstančią ataką yra sunku. Tačiau galima sukurti apsaugos priemonę, kuri galėtų atlikti paketų filtravimą pagal tam tikrus požymius. Tokiu atveju bent dalis atakos sugeneruotų paketų būtų blokuojami.

3 SAUGOS PRIEMONĖS NUO DDOS ATAKŲ

Norint apsisaugoti nuo paslaugų nutraukimo atakų, reikia užtikrinti tam tikrą saugumo lygį, pvz.: paketų filtravimą tinklo įrenginiuose, kad atakuotojai turėtų kuo mažiau galimybių paveikti atakuojamos sistemos darbą. Saugumą galimą užtikrinti naudojant šias priemones:

- Ugniasienės, kurios filtruoja IP paketus
- Paslaugų nutraukimo apsaugos sistema (DDS) [15]
- „Švarūs vamzdžiai“ principas [16]
- Apsaugos nustatymai šakotuvuose ir maršruto parinktuvuose
- Srauto nukreipimo metodas [17]
- Audito naudojimas [18]
- IPSec protokolo naudojimas [18]
- Pasyvūs visiško ir dalinio srauto davikliai [19]
- Aktyvus zonduojančių paketų generavimas ir stebėjimas [19]
- QoSSTAT – nustatytų parametrų neatitinkančių anomalijų tyrimas [19]



14 pav. Bendra saugos priemonių nuo DDoS atakų schema

Pagal veikimo pobūdį, šias priemones galima suklasifikuoti į dvi grupes (žr. 14 pav.):

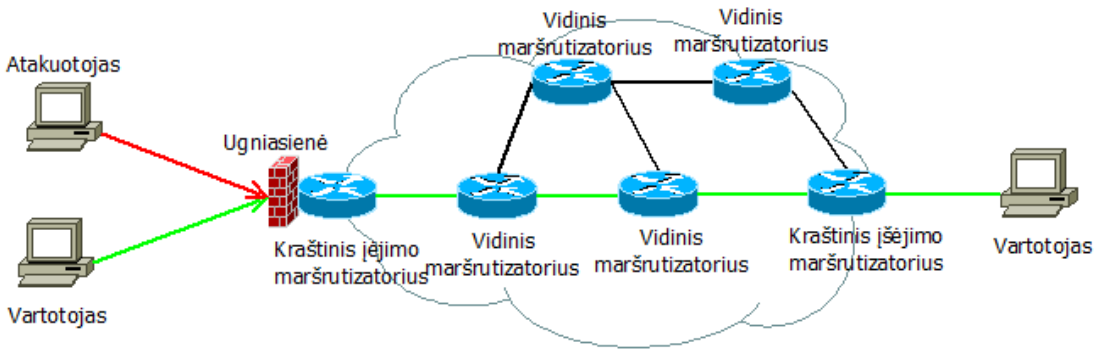
1) priemonės, kurios filtruoja arba blokuoja įtartiną srautą;
2) priemonės, kurios stebi tam tikrus požymius ir informuoja apie pastebėtus pakitimus atitinkamus reikalingus objektus.

Sekančiuose skyriuose aptarsime šias priemones detaliau.

3.1 Priemonės filtruojančios arba blokuojančios duomenų srautus

3.1.1 Ugniasienės, filtruojančios IP paketus

Ugniasienės veikimas pagrįstas srauto filtravimu. Jose nustatytos tam tikros taisyklės, pagal kurias ateinantis arba išeinantis srautas yra analizuojamas, pvz.: praleisti arba uždrausti tam tikrą srautą, kuriuose nurodyti tam tikri prievadai, IP adresai ar protokolai. Tačiau ugniasienės ne visada gali nustatyti ar ateinantis duomenų srautas yra paslaugų nutraukimo ataka, pvz.: jeigu ataka vykdoma per/panaudojant 80 prievadą, ugniasienė negali užkirsti atakos, kadangi nesugeba atskirti teisėto srauto nuo paslaugos nutraukimo atakos srauto. Tačiau ugniasienės pagalba galima uždrausti paprastiems vartotojams paleisti paprastas duomenų srauto siuntimo atakas.



15 pav. Ugniasienės panaudojimas maršrutizatoriuje

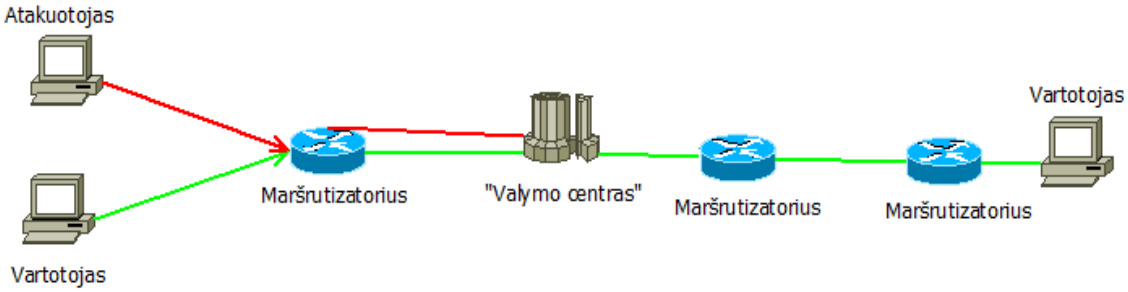
15 pav. parodyta ugniasienės vieta diferencijuotų paslaugų domeno atveju. Žalia linija rodo vartotojo siunčiamą srautą. Raudona linija rodo atakuotojo siunčiamą srautą.

3.1.2 Paslaugų nutraukimo apsaugos sistema (DDS)

Paslaugų nutraukimo apsaugos sistema gali blokuoti susijungimą jei naudojamas įprastas srautas, tačiau juo siekiama atlikti ataką. Ši sistema taip pat gali aptikti tiek protokolų atakas („Teardrop“ arba „Ping of death“) tiek paketų dydžiu paremtas atakas (ICMP ar SYN srauto atakas). Šią sistemą sudaro įrenginys su įdiegta operacine sistema. Taip pat naudojama ReputationWatch paslauga iš kurios gaunama naujausia informacija apie kenkėjiškus IP adresus ir šiame įrenginyje automatiškai atnaujinama informacija apie pasikeitimus.

3.1.3 „Švarūs vamzdžiai“ principas.

Visas srautas per tarpinį serverį perduodamas „valymo centrui“, kuris atskiria blogą srautą (paskirstytas paslaugų nutraukimo ir kitas atakas) ir perduoda tik gerą srautą kitiems tinklo įrenginiams. Tiekėjams reikalingas prisijungimas prie interneto norint valdyti šią paslaugą.



16 pav. „Švarūs vamzdžiai“ veikimo principas

Žalia linija rodo vartotojo siunčiamą srautą. Raudona linija rodo atakuotojo siunčiamą srautą.

Srauto „valymas“ atliekamas šiais 3 veiksmais:

- Aptikimas – svarbiausias dalykas siekiant aptikti atakas yra srauto anomalijų aptikimas lyginant su įprastu srautu
- Kenkėjiško srauto mažinimas– tai procesas, kuriame srautas yra valomas t.y. tikrinama ar nėra suklastotas, ieškoma anomalijų, tikrinami paketai ir šalinamas blogas srautas, leidžiant teisėtui srautui būti perduotam toliau
- Srauto nukreipimas ir įterpimas – srauto nukreipimas yra mechanizmas, kuris nurodo maršrutizatoriui aptiktą įtartiną srautą nukreipti „valymo“ įrenginiui.

3.1.4 Apsaugos nustatymai šakotuvuose ir maršruto parinktuvuose

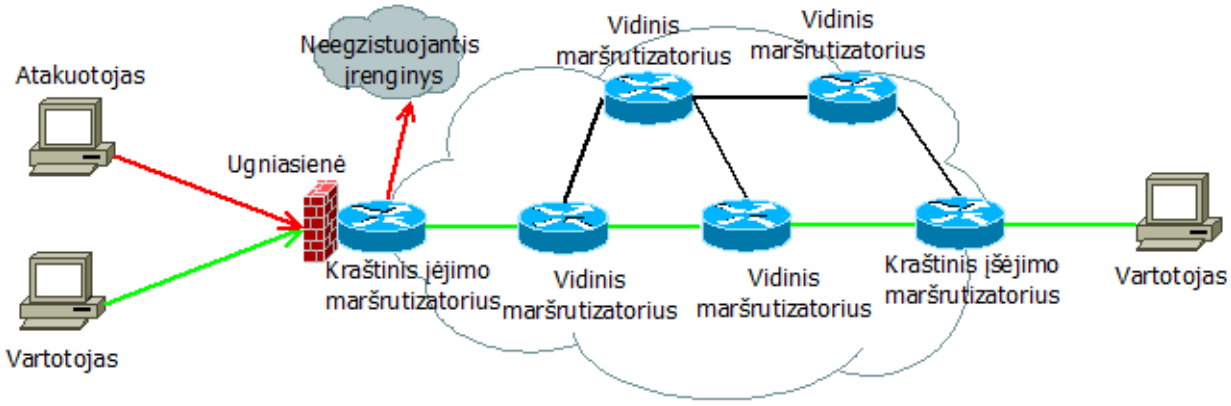
Dauguma šakotuvų ir maršrutų parinktuvų turi greičio apribojimo nustatymo galimybes. Šie įrenginiai gali užtikrinti automatinį srauto perdavimo apribojimą ar paketų atidėjimą, nuodugnias paketų patikrinimo galimybes, (pvz.: SYN srauto ataka gali būti sustabdyta atlikus paketų siuntimo atidėjimą). 17 pav. pateikta Cisco IoS įrenginiuose naudojama konfigūracija [20] skirta apsisaugojimui nuo užtvindymo atakų.

```
ip inspect max-incomplete high seconds
ip inspect one-minute high seconds
ip inspect udp idle-time seconds
ip inspect dns-timeout seconds
ip inspect tcp idle-time seconds
ip inspect tcp finwait-time seconds
ip inspect tcp synwait-time seconds
```

17 pav. Cisco IOS konfigūracija

3.1.5 Srauto nukreipimo metodas

Naudojant srauto nukreipimo metodą visas srautas skirtas atakai yra nukreipiamas į „juodąją skylę“ t.y. neegzistuojantį serverį ar virtualią tinklo sąsają. Norint išvengti įtakos tinklo apkrovai, srauto nukreipimas gali būti valdomas interneto paslaugų tiekėjų.



18 pav. Srauto nukreipimo metodas

Žalia linija rodo vartotojo siunčiamą srautą.

Raudona linija rodo atakuotojo siunčiamą srautą.

3.2 Priemonių filtruojančių arba blokuojančių duomenų srautus palyginimas

2 lentelėje pateiktas priemonių, filtruojančių arba blokuojančių duomenų srautus palyginimas. Lyginant priemones buvo analizuojama:

- kam priemonė skirta,
- kaip ji veikia,
- kokius analizuoja parametrus nelegalaus srauto aptikimui,
- ar priemonė pritaikyta veikti lokaliai, ar ji paskirstyta.
- Kaip srauto analizė apkrauna tinklo mazgą
- Sąlygos prie kurių geriausiai priemonė veikia
- Kur kaupiami ir kaip saugojami užfiksuoti neatitikimai
- Ar sudaromos taisyklės srauto analizei?
- Kitos savybės

2 lentelė. Priemonių filtruojančių arba blokuojančių duomenų srautus palyginimas.

Pavadinimas	Paskirtis	Veikimo principas	Analizuojami (stebimi) parametrai	Metodo veikimas (lokaliai/centralizuotai)	Ar sudaromi srauto analizavimo taisyklės	Reikšmių koregavimas pagal sąlygas	Atakos, kurias priemonė gali aptikti	Trūkumai
Ugniasienės, filtruojančios IP paketus	Filtruoti paketus, siekiant atskirti suklastotus paketus nuo teisėtų paketų	Sukuriamos taisyklės ugniasienėje, kurioje filtruojami paketai. Taisyklių neatitinkantys paketai yra nepersiunčiami toliau į domeno vidų	IP adresai, protokolai, prievadai	Lokaliai	Taip	-	UDP, TCP SYN, ICMP echo request užtvindymas, IP klastojimas	Sunku aptikti ataką, kai ji atliekama iš vidinio tinklo.
Paslaugų nutraukimo apsaugos sistema (DDS)	Blokuoti susijungimą/ paketų perdavimą	-	IP adresai, atakų tipai	Centralizuotai	-	Taip, realiu laiku	UDP, TCP SYN, ICMP echo request užtvindymas, atkartojimo atakos.	-
„Švarūs vamzdžiai“ principas	Atskirti teisėtą srautą nuo kenkėjiško	Naudojamas tarpinis serveris, kuris veikia kaip „valymo centras“, kuris atskiria blogą srautą nuo gero.	Ieškoma tinklo anomalijų	Centralizuotai	Taip	-	Teardrop	-
Apsaugos nustatymai šakotuvuose ir maršruto parinktuvuose	Riboti perduodamus paketus	Apribojamas paketų perdavimo greitis, atliekamas nuodugnus paketų tikrinimas.	-	Lokaliai	Taip	Taip	UDP, TCP SYN, ICMP echo request užtvindymas	-
Srauto nukreipimo metodas	Nukreipti kenkėjišką srautą į neegzistuojantį įrenginį	Aptikus kenkėjiška srautą, jis yra nukreipiamas į neegzistuojančią tinklo sąsają ar tinklo įrenginį	IP adresai, protokolai, prievadai	Lokaliai	Taip	-	UDP, TCP SYN, ICMP echo request užtvindymas	Atakos sukeltas srautas kartu su legaliu srautu yra nukreipiami į neegzistuojantį įrenginį.

3.3 Priemonės, stebinčios tam tikrus duomenų srautų požymius

3.3.1 Audito naudojimas

Auditavimas naudojamas stebėti įtartinus veiksmus diferencijuotų paslaugų architektūros ir kituose tinkluose. Jis nėra būtinas diferencijuotų paslaugų domeno dalis, tačiau patartina naudoti kai sistemos palaiko duomenų tikrinimo galimybes. Tikrinamas įvykis domeno vidiniuose maršrutizatoriuose gali būti keliaujantys paketai, kuriuose įrašyta žymė nėra naudojama. Auditavimas gali padidinti tinklo saugumą. Tačiau, siekiant išvengti galimos paslaugų nutraukimo atakos nereikalaujama, kad maršrutizatorius aptikęs įtartinus veiksmus praneštų siuntėjui.

3.3.2 IPSec protokolo naudojimas

IPSec protokolas yra IP protokolo plėtinys, kuris leidžia saugiai perduoti duomenis. IPSec protokolas esant įprastam rėžimui neužtikrina kriptografinio „DS“ lauko apskaičiavimo ir nesuteikia didelio saugumo lygio diferencijuotų paslaugų domeno tinkluose.

Tačiau IPSec tuneliavimo rėžimas užtikrina apsaugą, kuri tiesiogiai susijusi su šiuo domenu. Tuneliavimo rėžimas apima du IP antraštės atvejus: vidinę užšifruotą antraštę ir išorinę, skirtą perdavimui. Tačiau galima „atakuotojas viduryje“ ataka, kadangi išorinė IP antraštė nėra užšifruota.

Norint tinkamai naudoti IPSec tuneliavimo rėžimą reikia aptarti keletą punktų. Pirmiausia vidiniai maršrutizatoriai gali patikrinti tik išorinę IP antraštę, o kraštiniai maršrutizatoriai gali patikrinti vidinę IP antraštę. Kraštinis maršrutizatorius gali naudoti IPSec protokolą norint teisingai identifikuoti šaltinį su jam aprašytais SLA, o kraštinis išėjimo maršrutizatorius gali patikrinti paketo vientisumą.

Kraštiniame diferencijuotų paslaugų domeno išėjimo maršrutizatoriuje uždrausta modifikuoti „DS“ lauką, kad būtų tenkinamos srauto perdavimo sąlygos. Tačiau, jei modifikacija yra galima, tai padidintų tinklo saugumą.

3.3.3 Pasyvūs visiško ir dalinio srauto davikliai

Šiame metode naudojami du davikliai – DSMon ir TrafMon. DSMon daviklis periodiškai išsaugo perduodamų paketų skaičių ir perdavimo spartą. Šio daviklio pagalba galima nustatyti bendrą diferencijuotų paslaugų domeno būklę.

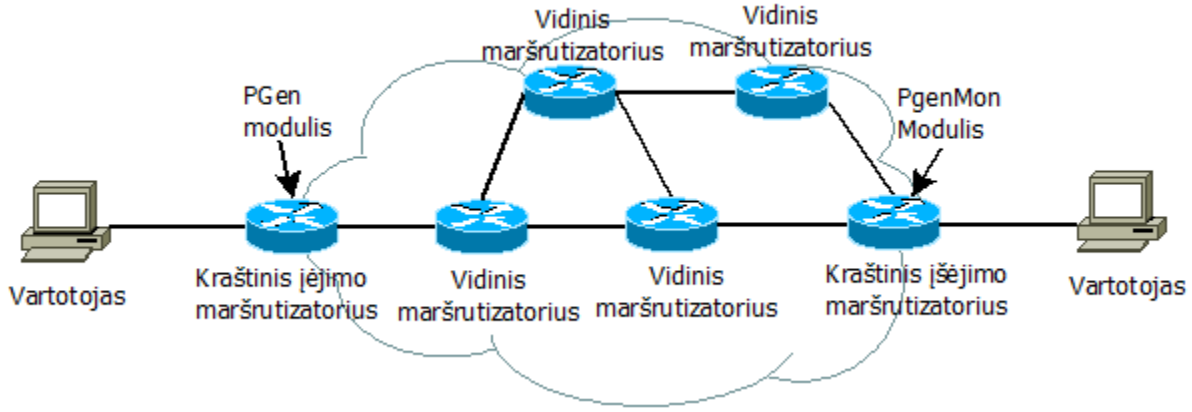
TrafMon daviklis saugo tuos pačius parametrus kaip ir DSMon daviklis, tačiau šis daviklis saugo virtualių linijų srautus vidiniuose ar kraštiniuose maršrutizatoriuose.

3.3.4 Aktyvus zonduojančių paketų generavimas ir stebėjimas

Šiame modelyje naudojamas PGen – slaptas paketų generavimo modulis. Šis modulis naudojamas įėjimo maršrutizatoriuje, kuriame stebimos virtualios linijos. PGen periodiškai atlieka virtualių linijų paketų kopijas ir pažymi šias kopijas maišos funkcijomis.

Stebėjimo modulis PgenMon yra išėjimo maršrutizatoriuje. Jis naikina Pgen modulio sukurtus paketus. Tokiu būdu apskaičiuojami vėlinimo skirtumai ir perdavimo sparta, o šie apskaičiuoti parametrai perduodami į analizavimo įrenginį.

Generuoti paketus reikia mažais kiekiais, kad neperkrauti domeno, bet generavimas turi būti pakankamai dažnas, kad aptikti atsiradusias anomalijas.



19 pav. Aktyvus zonduojančių paketų generavimo ir stebėjimo modulių išsidėstymas

3.3.5 QoSSTAT – nustatytų parametrų neatitinkančių anomalijų tyrimas

QoSSTAT priima visas ataskaitas gautas iš daviklių esančių vietiniame ar nutolusiame tinkle. QoSSTAT gali būti naudojamas viename iš kraštinių maršrutizatorių.

Naudojant QoSSTAT stebimi šie parametrai: perduotų duomenų kiekio skaičiavimas, kuris yra perduotas per tam tikrą laiką. Paketų skaičiavimas – perduodų paketų skaičius per tam tikrą laiką. Vėlinimo svyravimai – apibūdinami kaip skirtumai tarp dviejų ir daugiau išmatuotų vėlinimų. QoSSTAT algoritmas apibūdina kintamąjį „S“ skirtą nustatyti esamos sistemos būsenos lygį. Naudojami trys lygiai: raudonas, geltonas ir žalias.

Raudonas lygis reiškia, kad kintamasis „S“ yra intervale, kuris priklauso tikimybei $\alpha \leq 0.001$. Geltonas lygis reiškia, kad kintamasis „S“ yra intervale $0.001 < \alpha \leq 0.01$. Žalias lygis reiškia, kad kad kintamasis „S“ yra intervale $\alpha > 0.01$.

3.4 Priemonių stebinčių tam tikrus duomenų srautų požymius palyginimas

3 lentelėje pateiktas priemonių, stebinčių tam tikrus duomenų srautų požymius, palyginimas. Lyginant priemones buvo analizuojama paskirtis, veikimo principas ir naudojami analizavimo moduliai. Atlikus palyginimą, galima pastebėti, kad priemonės atlieka skirtingus veiksmus: vienos stebi ar paketuose esanti informacija yra teisinga, kitos stebėti duomenų srautų būklę įvertinant perdavimo spartą ir vėlinimus.

3 lentelė. Stebinčių priemonių palyginimas

Pavadinimas	Paskirtis	Veikimo principas	Naudojami generavimo/ analizavimo moduliai
Audito naudojimas	Stebėti įtartinus veiksmus susijusius su domene esančiu srautu	Stebėti nustatytus įvykius domeno vidiniuose maršrutizatoriuose, pvz.: keliaujantys paketai, kuriuose įrašyta žymė nėra naudojama	-
IPSec protokolo naudojimas	Užtikrinti didesni tiklo saugumą	Saugiai perduoti paketus, užšifruojant IP paketo antraštes.	-
Pasyvūs visiško ir dalinio srauto davikliai	Nustatyti paslaugų kokybę stebint bendrą domeno būklę	Naudojami du davikliai: DSMon ir TrafMon, kurie periodiškai išsaugo perduodamų paketų skaičių ir perdavimo spartą.	+
Aktyvus zonduojančių paketų generavimas ir stebėjimas	Aptikti prasidedančias atakas	Naudojami du moduliai: PGen ir PgenMon. PGen modulis periodiškai atlieka paketų kopijas ir jas atitinkamai pažymi. PgenMon modulis atlieka šių paketų naikinimą bei apskaičiuoja perdavimo spartą ir vėlinimo skirtumus. Gautus duomenis siunčia analizavimo įrenginiui.	+
QoSSTAT	Aptikti nustatytų parametrų neatitinkančias anomalijas	Stebimi šie parametrai: perduotų duomenų kiekis, perduotų paketų kiekis ir vėlinimo svyravimai. Taip pat naudojamas kintamasis „S“ skirtas nustatyti sistemos būseną.	-

3.5 Priemonių, galinčių užtikrinti diferencijuotų paslaugų domeno saugą, analizė

Atsižvelgiant į tai, kad siekiama apsaugoti diferencijuotų paslaugų domeno kraštinį įėjimo maršrutizatorių, dalis nagrinėtų apsaugos priemonių mažiau tinkamos panaudojimui. Šiuo atveju labiau tinka tos apsaugos priemonės, kurios atlieka paketų filtravimą/blokavimą. Tokiu atveju būtų galima panaudoti ugniasienę, srauto nukreipimo metodą/principą. Kitos priemonės netinka dėl didelių investicinių išlaidų, gali pareikalauti daug laiko jų konfigūracijai. Taip pat nėra apsaugos priemonės, kuri apsaugotų nuo visų atakų tipų, todėl atsižvelgiant į atakų tipus (pvz., TCP SYN, UDP ar ICMP užtvindymo atakas), kurie gali būti panaudoti prieš diferencijuotų paslaugų architektūros tinklus, galima naudoti/sukurti paprastesnes apsaugos priemones, pavyzdžiui tokias kaip ugniasienę.

Taip pat būtų galima panaudoti ir stebėjimo principu veikiančias apsaugos priemones tuo atveju, jei apsaugos mechanizmas kraštiniame įėjimo maršrutizatoriuje veiktų nekorektiškai, t.y. praleistų didelius atakų srautus į domeno vidų.

Kadangi interneto paslaugų tiekėjai žino savo vartotojų IP adresus, žino kokios paslaugos teikiamos tam tikrais prievadais, vienas iš pagrindinių dalykų siekiant apsisaugoti nuo DDoS atakų, yra taisyklių įdėjimas į ugniasienę, blokuojant visus gaunamus duomenų srautus ne iš savo tinklo adresų erdvės. Tokių atveju apsisaugoma nuo IP klastojimo (spoofing) atakos. Tačiau jei ataka atliekama iš vidinio tinklo, kuriam priklauso teisėti vartotojai, ją sunkiau aptikti, nes atrodys, kad teisėtas vartotojas siunčia didelius duomenų srautus, pvz, naudojasi FTP paslauga. Todėl reikia labai tiksliai aprašyti ugniasienės taisykles įtraukiant į jas šiuos pagrindinius parametrus: IP adresas, paketų dydis, naudojamos vėliavėlės. Tokiu atveju, būtų atliekamas griežtesnis paketų filtravimas.

Taip pat vienas iš sprendimo būdų būtų dinamiškai dėti taisykles į ugniasienę. Tokiu atveju aptikus ataką pagal tam tikrus požymius, būtų blokuojami gaunami duomenų srautai iš atakų sukėlėjų. Kadangi atakos sukelėjas gali būti ir teisėtas vartotojas, tai dinamiškai sukurtos taisyklės turėtų būti pašalinamos po tam tikro laiko.?

Papildomai galima naudoti ir srauto nukreipimo būdą. Šiuo atveju kenkėjiškas srautas būtų persiunčiamas į neegzistuojantį įrenginį. Įvertinant, kad šis metodas neatskiria teisėto srauto nuo kenkėjiško, jį reikėtų taikyti kraštutiniu atveju, kai ugniasienė nebesugeba sustabdyti kenkėjiško srauto.

Reiktų atkreipti dėmesį į tai, kad kraštiniame domeno įėjimo maršrutizatoriuje atliekamas paketų žymėjimas į tam tikras klases. Todėl reikia užtikrinti apsaugą šiuo aspektu. Pavyzdžiui, jei į kraštinį įėjimo maršrutizatorių patenka paketai jau su jose įrašyta DSCP reikšme, šiuos paketus reiktų taip pat atmesti arba peržymėti į geriausių pastangų (BE) klasę.

Jei domeno vidiniai maršrutizatoriai nebespėja apdoroti gaunamų paketų tam tikrose klasėse, tai juos būtų galima perkelti į žemesnę klasę. Tokiu atveju gauti paketai nebus prarandami, bet perduodami su mažesniais kokybės reikalavimas.

Taip pat būtų galima apriboti priimamų paketų skaičių per laiko vienetą kraštiniame įėjimo maršrutizatoriuje. Taip užtikrinama, kad nebus išnaudojami visi maršrutizatoriaus resursai paketų apdorojimui

3.6 Skyriaus išvados

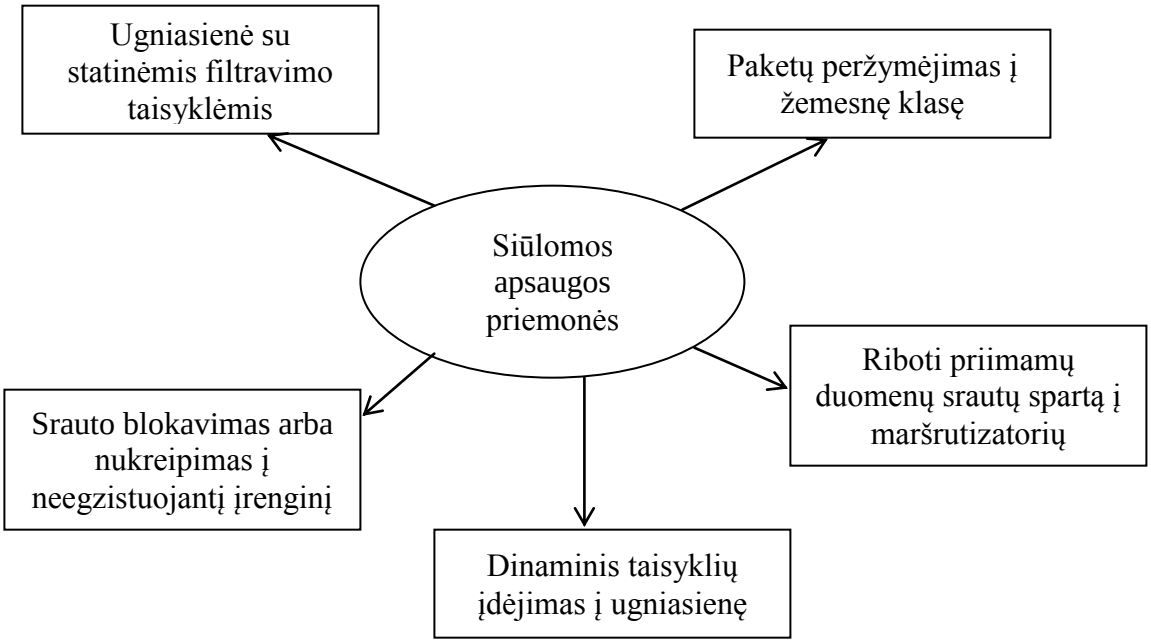
Šiais technologijų laikais, kai daugėja kompiuterių vartotojų ir kuriamos įvairios sistemos, taip pat padaugėja ir atakuotojų, kurie bando pakenkti šioms sistemoms. Vienas iš populiaresnių kenkimo būdų - paslaugų nutraukimo arba paskirstytos paslaugų nutraukimo atakos. Atlikus diferencijuotų

paslaugų architektūros tinklų analizę paaiškėjo, kad šie tinklai taip pat turi pažeidžiamumų. Užtvindžius diferencijuotų paslaugų domeną daugybe paketų, šis nustoja tinkamai veikti, apkraunami maršrutizatoriai, kuriuose atliekami paketų apdorojimo procesai ir tinklas nebegali teikti kokybiškų paslaugų. Analizės metu nustatyta, kad diferencijuotų paslaugų domeno kritine pažeidžiama vieta pirmiausia tampa kraštinis įėjimo maršrutizatorius, tačiau pažeidžiami gali būti ir vidiniai maršrutizatoriai.

Norint apsaugoti diferencijuotų paslaugų architektūros tinklus nuo DDoS atakų siūlomi įvairūs sprendimo būdai, tačiau jie negali visiškai užtikrinti, kad visos DDoS atakos bus aptiktos ir sustabdytos. Pagal veikimo pobūdį, šias priemones galima suklasifikuoti į priemones, filtruojančias arba blokuojančias įtartiną srautą bei priemones, stebinčias tam tikrus požymius ir informuojančias apie pastebėtus pakitimus atitinkamus reikalingus objektus. Atlikus abiejų tipų priemonių analizę nuspręsta projektuojant diferencijuotų paslaugų architektūros tinklų apsaugos nuo DDoS atakų sistemą naudoti dalį pirmosios grupės priemonių (ugniasienė, srauto nukreipimo metodas/principas) lygiagrečiai jas papildant naujais apsaugos elementais, leidžiančiais užtikrinti didesnį diferencijuoto paslaugų domeno apsaugojimo nuo DDoS atakų lygį.

4 DDOS ATAKŲ APTIKIMO MODELIS DIFERENCIJUOTŲ PASLAUGŲ ARCHITEKTŪROS TINKLUOSE

Remiantis atlikta analize diferencijuotų paslaugų domeno tinklo apsaugai nuo DDoS atakų siūloma naudoti tam tikras apsaugos priemones (žr. 20 pav).



20 pav. Siūlomos apsaugos priemonės

Šios priemonės turi užtikrinti:

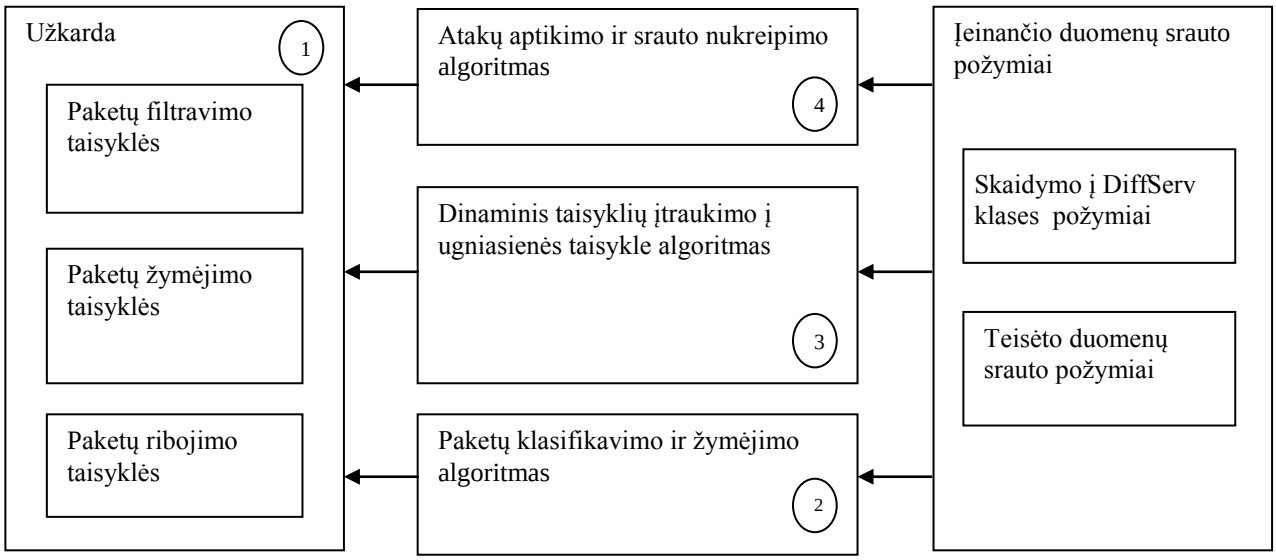
- paketus filtravimą ir žymėjimą pagal tam tikras aprašytas taisykles domeno įėjimo maršrutizatoriuje,
- priimamų paketų spartos į kraštinį įėjimo maršrutizatorių ribojimą,
- dinaminį naujų taisyklių į ugniasienės taisyklių sąrašą įtraukimą,
- informacijos apie atakas fiksavimą į įvykių žurnalus

Kuriant apsaugos modulį atakų aptikimui ir sustabdymui reikia atsižvelgti į tai, kokios komponentės ir procesai veiks nuolatos, o kurie pagal būtinybę veiks papildomai. Įprastai maršrutizatoriuje nuolatos veiks ugniasienė, kuri atitinkamai sukonfigūruota srauto priėmimui. Kadangi marštur izatorius veikia Linux pagrindu, todėl ugniasienė kuriama naudojant „iptables“ taisykles. Taip pat ugniasienėje yra apribotas priimamų paketų kiekis per laiko vienetą. Tokiu atveju išvengiama visų maršrutizatoriaus resursų išnaudojimo.

Papildomai yra panaudotas dinaminis taisyklių įdėjimas į ugniasienę su srauto blokavimu ar nukreipimu. Šis procesas vykdomas tada, kai aptinkamas didelis duomenų siuntimas per laiko vienetą

(pvz., 10000 paketų/sekundę) ir automatiškai įdedama taisyklė į ugniasienę, kuri blokuos siuntėjo IP adresą.

Siūlomas DDoS atakų aptikimo mechanizmas pavaizduotas 21 paveiksliuke.



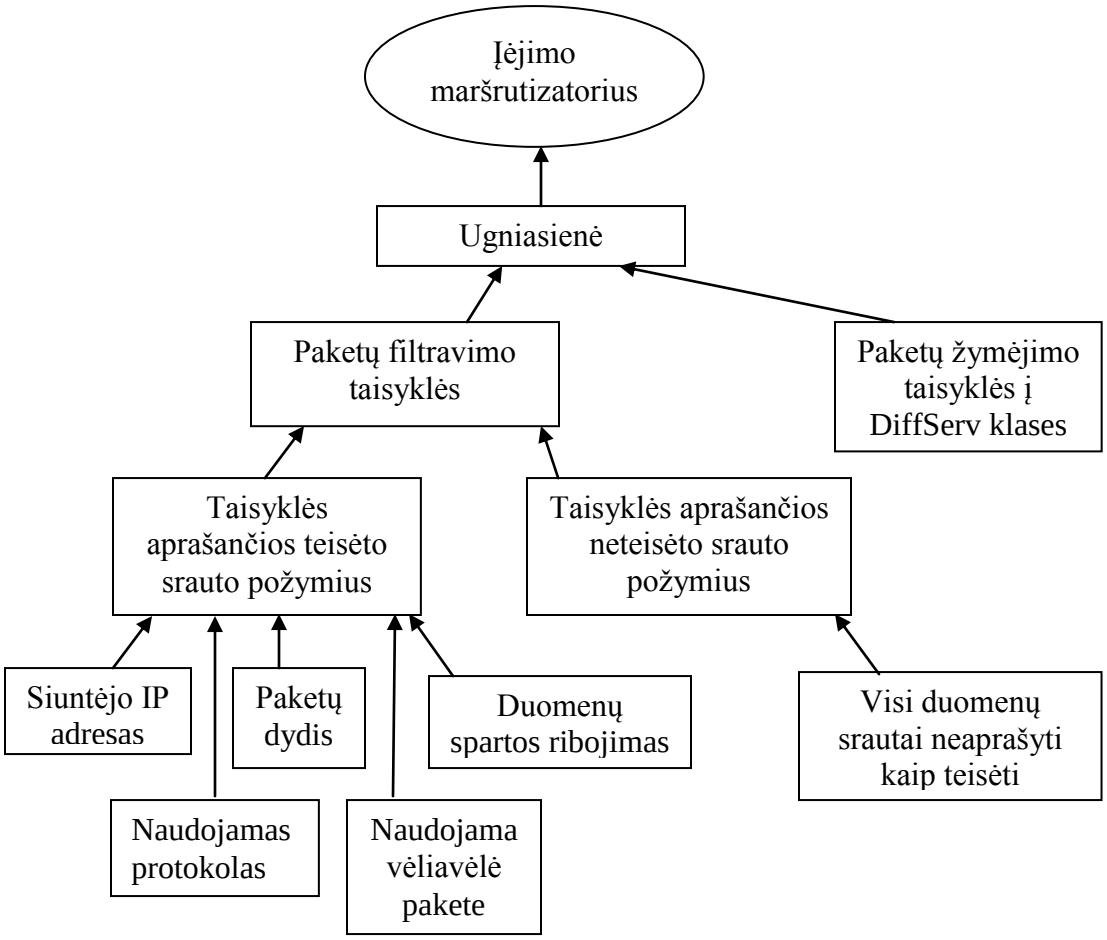
21 pav. DDoS atakų aptikimo mechanizmo schema

Toliau kiekvieną iš schemoje pateiktų komponentų aptarsime detaliau.

4.1 DDoS atakų aptikimo mechanizmas ir jo komponentės

DDoS atakų aptikimo mechanizmas sudarytas iš keletos būtinų komponenčių nusakančių informaciją apie gautą paketą. Iš jų galima įvertinti ar atliekama ataka prieš diferencijuotų paslaugų domeną ar ne.

4.1.1 Apsaugos komponentės išoriniam įėjimo maršrutizatoriui



22 pav. Realizuojamas modelis ir jį sudarančios komponentės

Įėjimo maršrutizatoriuje įdiegta ugniasienė, kurią susidarosmulkesnės atskiros komponentės.: paketų filtravimo taisyk lės ir paketų žymėjimo taisyklės. Paketų filtravimo taisyklės sudarytos dar iš dviejų papildomų komponenčių: taisyklių rinkinio, kuris aprašo kokie srautai gali būti perduodami toliau, ir taisyklių rinkinio, kuris nusako, kokie srautai turi būti neperduodami.

4.1.2 Požymių panaudojimas apsaugos modulyje

Paketų filtravimas apsaugos modulyje atliekamas pagal žemiau išvardintus požymius:

- Siuntėjo IP adresas.

  Naudojama nurodyti iš kokių IP adresų galima priimti duomenų srautus. Siekiant apsisaugoti nuo IP klastojimo atakų ar duomenų priėmimo iš kitų adresų, nurodoma, kad duomenų srautai gali būti priimami tik iš tų vartotojų, kurie yra domeno adresų erdvėje.

- Paketų dydis.

Šis požymis naudojamas nustatyti, kokie paketų dydžiai gali būti priimami. Šiuo atveju galima apsisaugoti nuo suklastotų paketų apdorojimo. Taip pat šis dydis nusakys, kokie paketų dydžiai kartu su naudojamu protokolu turi būti pažymėti atitinkamai paslaugų kokybės klasei.

- Naudojamas protokolas

  Nusakoma, kokio protokolo srautus apdoroti. Dažniausiai duomenims perduoti naujami TCP ir UDP protokolai.

- Naudojama vėliavėlė pakete

  Šis požymis naudojamas nustatyti ar paketai siučiami su teisinga vėliavėle pakete. Pavyzdžiui, naujam susijungimui sudaryti naudojama tik SYN vėliavėlė. Jei naudojama kitokia vėliavėlė, šie paketai atmetami. Taip pat apsisaugoma nuo prievadų skanavimo atakų.

4.2 DDoS atakų aptikimo mechanizmo procesai

Žemiau išvardinti procesai, kurie atliks tam tikrus veiksmus apsaugos modulyje.

- Priimamų duomenų spartos apribojimas

  Naudojama nustatyti priimamų duomenų kiekį per laiko vienetą. Jei paketai siunčiami žymiai greičiau nei nusakytą taisyklėse, šie paketai yra blokuojami. Todėl priimami tik tie duomenų srautai, kurie neviršyja nurodyto limito.

- Dinaminis taisyklių įdėjimas į ugniasienę

  Naudojama blokuoti tuos vartotojus, kurie dažnai/pastoviai siunčia didelius duomenų srautus mažais laiko intervalais (pvz. 10000 paketų/sekundę). Tokiu atveju galima įtarti, kad siekiama išeikvoti tinklo pralaidumą suklastotais duomenų srautais. Vartotojo blokavimas turi būti laikinas, pvz 10 min. Poto turi būti atblokuojamas, jei iš jo negaunami dideli duomenų srautai.

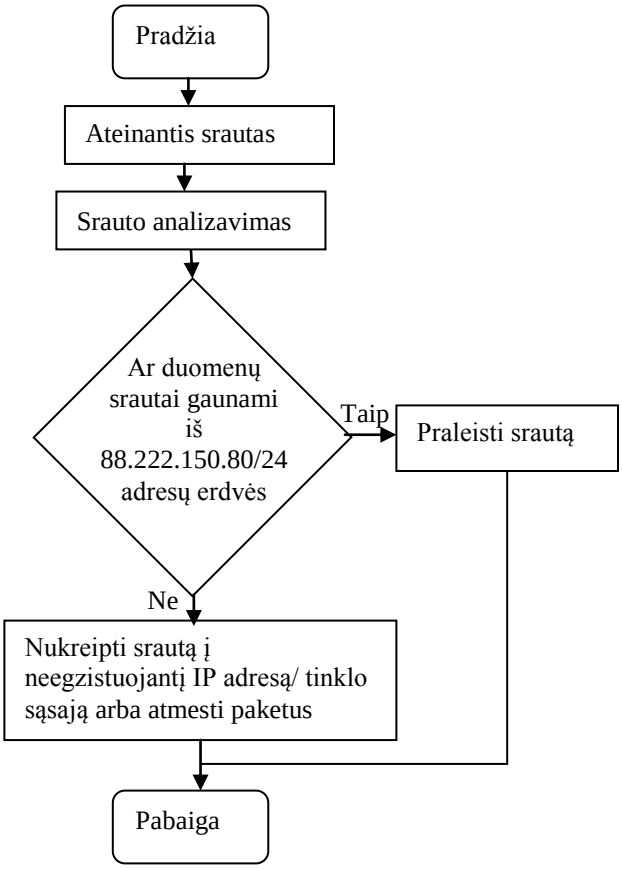
- Srauto nukreipimas

  Naudojamas tuo atveju, jei nebespėjama blokuoti kenkėjiškų duomenų srautų. Tokiu atveju kenkėjiškas srautas nukreipiamas į neegzistuojantį tinklo įrenginį ar IP adresą.

4.3 DDoS atakų aptikimo mechanizme naudojami algoritmai

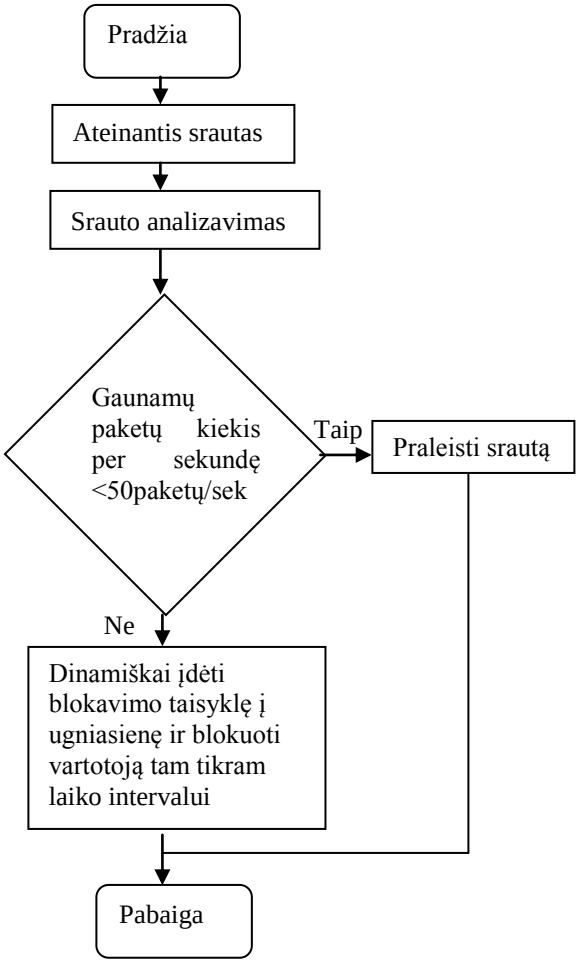
Atakų aptikimo ir srauto nukreipimo algoritmas

Siekiant išvengti nereikalingo atakos sugeneruotų paketų klasifikavimo ir žymėjimo, naudojamas atakų aptikimo ir sustabdymo algoritmas. Algoritmo pavyzdys pateiktas 23 paveikslėlyje.



23 pav. Atakų aptikimo ir srauto nukreipimo algoritmas

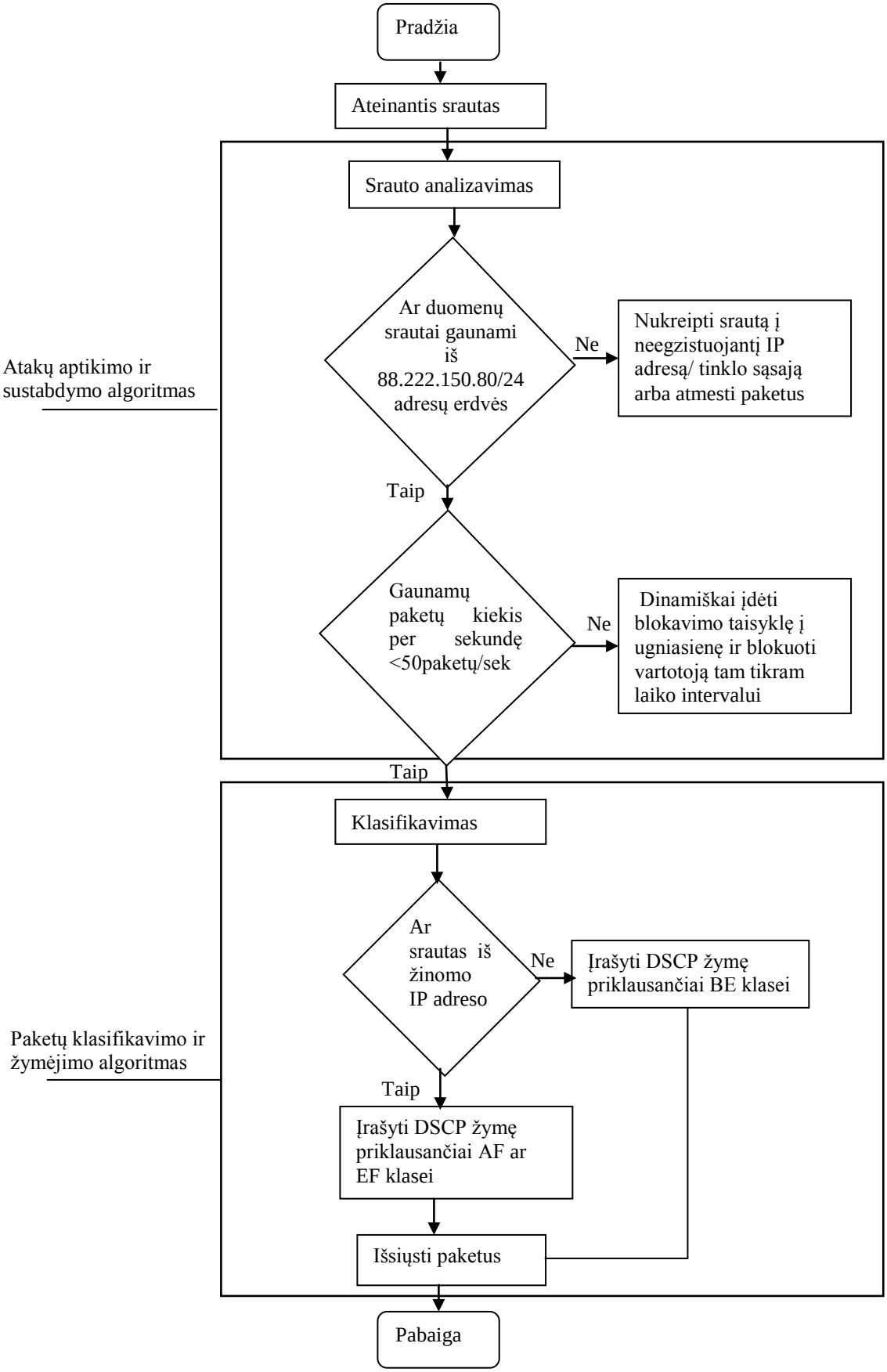
Dinaminis taisyklių įdėjimas į ugniasienę/ vartotojo laikino blokavimo algoritmas



24 pav. Dinaminis taisyklių įdėjimas į ugniasienę ir blokavimas

24 paveiksliuke esantis algoritmas vaizduoja vartotojo blokavimą tam tikram laikotarpiui. Iš pradžių ateinantis duomenų srautas yra analizuojamas ir jei nustatoma, kad iš legalaus vartotojo ateina dideli duomenų srautai per labai trumpą laiko tarpą, dinamiškai įdedama taisyklė į ugniasienę, kad blokuoti šį vartotoją.

25 paveiksliuke pavaizduotas bendras algoritmas, kuris realizuotas kraštiniame maršrutizatoriuje.

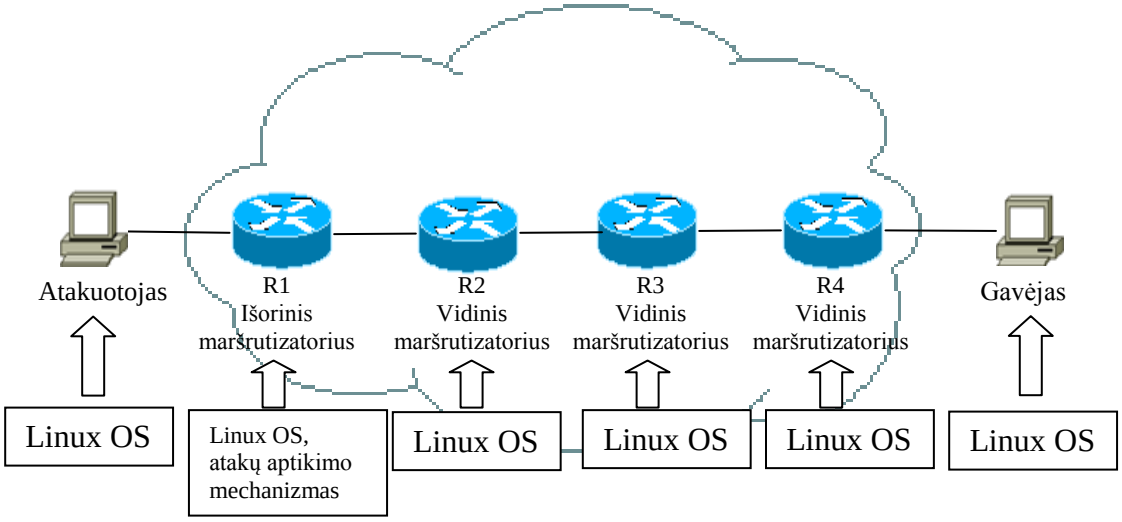


25 pav. Atakų aptikimo ir sustabdymo algoritmas bei paketų klasifikavimo ir žymėjimo algoritmas

Šis algoritmas padalintas į dvi dalis ir pažymėta, kuri dalis priklauso atitinkamam algoritmui. Pavaizduotame algoritme matyti, kad pirmiausia ateinantis srautas apdorojamas maršrutizatoriuje įdiegto atakų aptikimo mechanizmo. Jame atliekamas srauto analizavimas siekiant aptikti atakas. Nustačius, kad paketai neatitinka nusakytas teisėto srauto taisykles, jie iškarto yra nukreipiami į neegzistuojantį IP adresą ar tinklo sąsają, arba visiškai atmetami išvengiant maršrutizatoriaus darbo sutrikdymo. Ne atakos srautas perduodamas paketų klasifikavimo ir žymėjimo algoritmui, kurio metu paketai suklasifikuojami ir pažymimi bei perduodami į vidinius diferencijuotų paslaugų domeno maršrutizatorius.

Šio algoritmo specifiniai duomenys ir pavyzdžiai pateikti "**Atakų aptikimo ir sustabdymo mechanizmo konfigūracija**" skyrelyje.

4.4 DDoS atakų aptikimo mechanizmo išdėstymas techninėje įrangoje



26 pav. Techninėje įrangoje panaudota programinė įranga

Pirmas apsaugos taškas yra išorinis maršrutizatorius, kuriame atliekamas paketų žymėjimas į klases. Papildomai jame sukonfigūruota ugniasienė, kuri pirmiausia atliks paketų filtravimą pagal tam tikrus požymius, tokius kaip IP adresas, protokolas, paketo dydis ir pan. Tokių atveju nufiltravus atakos sugeneruotus paketus, į domeno vidų nepateks arba dalinai pateks kenkėjiško srauto. Priklausomai nuo pirmame apsaugos taške užtikrinamo apsaugos lygio, gali tekti papildomai įdiegti apsaugos priemonę ir vidiniame maršrutizatoriuje.

4.5 Skyriaus išvados

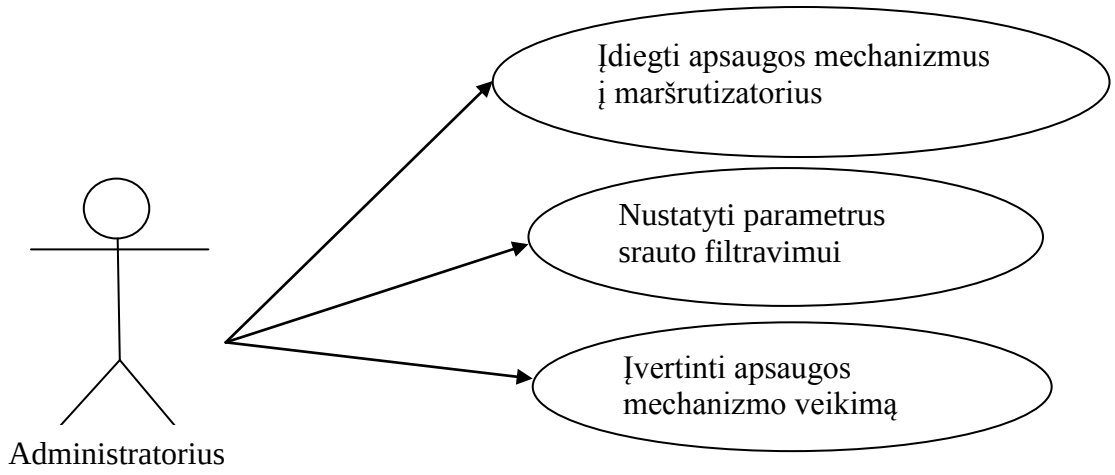
Šiame skyriuje aptartas ir pasiūlytas apsaugos modelis pritaikytas diferencijuotų paslaugų domeno tinklams. Projektuojamame apsaugos modelyje apibrėžti kokie naudojami procesai ir kokie požymiai naudojami paketų filtravime. Taip pat pavaizduota iš kokių požymių sudaromos teisėto srauto filtravimo taisyklės. Algoritmų paveiksliukuose pavaizduota kaip veiks naudojami procesai.

Šiuo apsaugos modeliu siekiama filtruoti ateinančius duomenų srautus į kraštinį maršrutizatorių ir pagal tam tikrus požymius atskirti teisėtą srautą nuo neteisėto. Remiantis šiuo pasiūlytu apsaugos modeliu realizuojama DDoS atakų aptikimo sistema, kuri veiks kraštiniame įėjimo maršrutizatoriuje.

5 DIFERENCIJUOTŲ PASLAUGŲ DOMENO APSAUGOS NUO DDOS ATAKŲ SISTEMOS PROJEKTINIAI IR REALIZACINIAI ASPEKTAI

5.1 Vartotojų poreikių specifikacija

Kuriama apsaugos sistema turi ne tik korektiškai veikti, bet ir būti lengvai įdiegiama bei turėti galimybę pagal poreikį pakeisti jos konfigūraciją. Žemiau esančiame paveiksliuke pavaizduoti poreikiai kuriamam produktui.

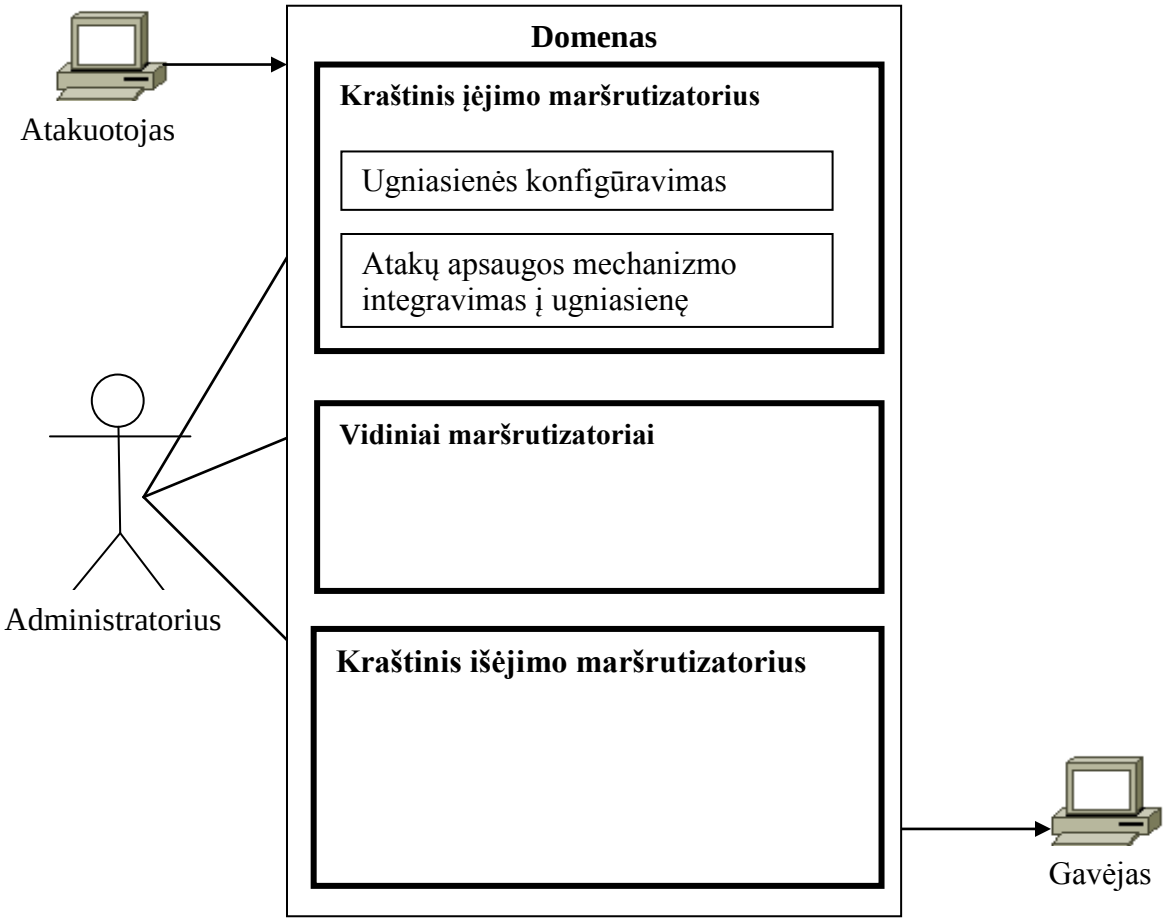


27 pav. Vartotojų poreikiai kuriamam produktui

Administratorius privalo turėti galimybę sukonfigūruoti maršrutizatorius paketų perdavimui bei įdiegti apsaugos mechanizmą nuo atakų, t.y. parašyti scenarijus (skriptus) skirtus apsaugai bei nustatyti parametrus pagal kuriuos analizuojamas srautas (naudojamas protokolas, vėliavėlė, perduotų paketų skaičius). Taip pat įvertinti apsaugos mechanizmo veikimą atsižvelgiant kiek ir kokių atakų aptikta bei sustabdyta.

5.2 Apibendrintas sukurto produkto modelis

Diferencijuotų paslaugų domenas sudarytas iš kraštinių įėjimo ir išėjimo maršrutizatorių bei vidinių maršrutizatorių (žr. 28 Pav.). Įėjimo maršrutizatoriuje realizuojami tam tikri komponentai, kurie yra atitinkamai sukonfigūruojami.

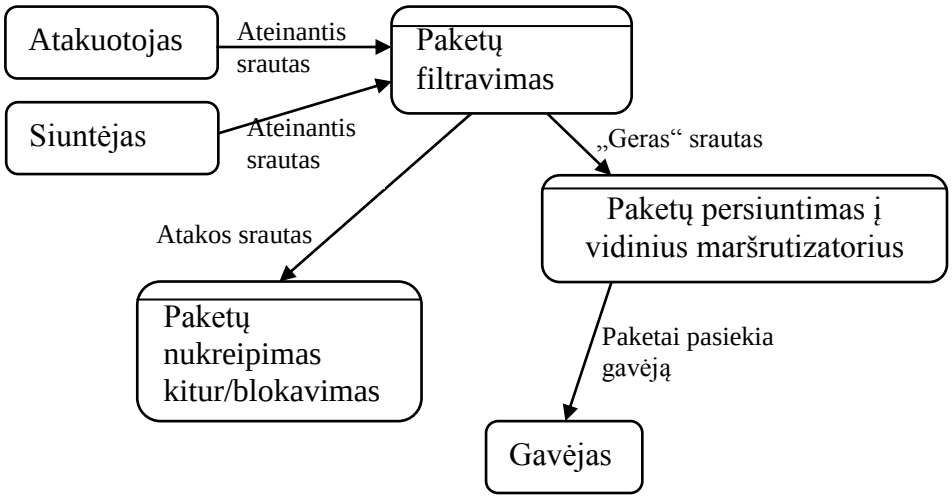


28 pav. Apibendrintas sukurtos sistemos modelis, nurodant svarbiausias sudėtines jos dalis

Įėjimo maršrutizatoriuje realizuota ugniasienė į kurią papildomai integruotas apsaugos mechanizmas nuo atakų. Jame nustatytos tam tikros taisyklės, pagal kurias srautas yra praleidžiamas toliau į vidinius maršrutizatorius, arba blokuojamas ir nukreipiamas kitur, nes traktuojamas kaip atakos srautas.

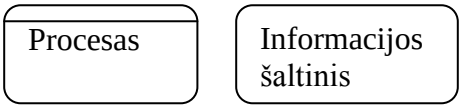
Siekiant išvengti atakos metu sugeneruotų ir pasiųstų paketų į kraštinį įėjimo maršrutizatorių, atakų aptikimo mechanizmas realizuojamas prieš atliekant paketų žymėjimą į juos įrašant tam tikrą DSCP [21] reikšmę.

5.3 Duomenų srautų diagrama



29 pav. Duomenų srautų diagrama

Žymėjimas:



Pagal 29 paveiksliuke pavaizduotą duomenų srautų diagramą, yra generuojamas ir siunčiamas duomenų srautas į kraštinį įėjimo maršrutizatorių. Jame atliekamas srauto filtravimas pagal tam tikrus kriterijus. Srautas atitinkantis tam tikrus reikalavimus siunčiamas toliau į vidinius domeno maršrutizatorius, o iš jų perduodamas gavėjui. Reikalavimų neatitinkantis srautas, traktuojamas kaip atakos srautas, nukreipiamas kitur arba blokuojamas.

5.4 Ugniasienės konfigūracija

Siekiant užtikrinti maršrutizatoriaus gynybinę liniją ugniasienė sukonfigūruota kaip pirminė apsaugą. Joje nustatyti šie parametrai:

- Kokie leidžiami protokolai
- Naudojamos tinklo sąsajos duomenų perdavimui
- Leistini paketų dydžiai

Pavyzdinis ugniasienės taisyklių sudarymas:

```
iptables -A INPUT –i eth0 -p tcp -s 192.168.0.2 -j ACCEPT
```

Ši taisyklė reiškia, kad priimti TCP protokolo srautą per tinklo sąsają eth0 iš siuntėjo, kurio IP adresas yra 192.168.0.2

```
iptables -A INPUT -i eth0 -s 192.168.0.10 -m length --length 20 -j DROP
```

Aukščiau parašytoje taisyklėje nurodoma, kad paketai, kurių dydis yra 20 baitų ir atėję iš siuntėjo, kurio IP adresas yra 192.168.0.10 atmetami.

5.5 Atakų aptikimo ir sustabdymo mechanizmo konfigūracija

Atakų aptikimo ir sustabdymo mechanizmas panaudotas kaip papildoma apsauga. Jis sudarytas iš specifinių taisyklių, kurias panaudojus galima aptikti kenkėjišką srautą ir jį nukreipti kitur. Šios taisyklės yra integruotos į pirminę maršrutizatoriaus apsaugą – ugniasienę. Norint apsisaugoti nuo TCP SYN srauto, UDP srauto ir ICMP srauto atakų, kiekvienu atveju reikia užsibrėžti tam tikrus parametrus, tokius kaip perduodamų paketų skaičius per sekundę, nurodyti naudojamus protokolus (TCP, UDP ir pan) bei kitus parametrus, pagal kuriuos yra filtruojamas srautas. Pavyzdžiui, žinant, kad TCP SYN srauto ataka remiasi mažu paketo dydžiu, jame esančia SYN vėliavėle ir siunčiama dideliais kiekiais, šios atakos aptikimui sukurta taisyklė, kurioje nurodyta kiek galima perduoti paketų per sekundę (pvz., 5 paketai per sekundę) ir tikrins ar pakete yra SYN vėliavėlė. Nustačius, kad paketai su SYN veliavėle siunčiami dažniau nei nurodyta taisyklėje, šis paketų srautas yra nukreipiamas kitur arba visai užblokuojamas.

Žemiau pavaizduota, kaip atrodo pavyzdinis atakų aptikimo ir sustabdymo mechanizmo taisyklių rinkinys.

Syn srauto atakos apsauga:

```
iptables -A INPUT -p tcp –syn -m limit --limit 5/s –s 192.168.0.5 -j ACCEPT
```

Ši taisyklė reiškia, kad jei siunčiami TCP protokolo paketai su SYN vėliavėle iš IP adreso 192.168.0.5 ne daugiau nei 5 paketai per sekundę, jie priimami.

UDP srauto atakos apsauga:

```
iptables -A INPUT -p udp -m limit --limit 5/s –d 192.168.0.5 -j ACCEPT
```

Ši taisyklė reiškia, kad jei siunčiami UDP protokolo paketai ne daugiau nei 5 paketai per sekundę iš IP adreso 192.168.0.5, jie priimami

Apsauga nuo “ping” atakos srauto:

```
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 3/s -j
ACCEPT
```

Ši taisyklė naudojama norint apsisaugoti nuo “ping” paketų srauto atakos. Paketai yra priimami, jei ICMP protokolo paketai gaunami ne dažniau nei 3 paketai per sekundę.

Visose taisyklėse naudojamas parametras `-m limit --limit paketai/sek`. Tai reiškia, kad yra priimamas tam tikras kiekis paketų per sekundę. Viršijus šį limitą, paketai yra numetami/neapdorojami.

5.6 Skyriaus išvados

Sukurta DDoS atakų aptikimo diferencijuotų paslaugų architektūros tinkluose sistema, padės aptikti atakas nukreiptas į diferencijuotų paslaugų domeną. Tam tikslui sukurta ir sukonfigūruota ugniasienė kaip pirminė apsauga. Taip pat sukurtos ir pavaizduotos taisyklės skirtos atakų aptikimui ir sustabdymui. Jos integruotos į ugniasienę kaip papildoma apsauga. Panaudoti algoritmai, kurie atliks srauto filtravimą siekiant atskirti teisėtą srautą nuo atakos srauto. Atakos srautas nukreipiamas į neegzistuojantį IP adresą ar tinklo sąsają, o teisėtas srautas perduodamas toliau. Taip pat nusakyti vartotojo poreikiai šiai atakų aptikimo sistemai, pavaizduotas algoritmo veikimo principas bei duomenų srautų diagrama, kurioje atvaizduota kaip keliauja srautas.

6 Eksperimentiniai tyrimai

6.1 Įrenginių sukūrimas

Darbo realizacija atliekama virtualiai, t.y. pasinaudojant „VMware“ programinę įrangą [22]. Jos pagrindu įdiegtos keturios virtualios mašinos su Linux operacine sistema, kurios sukonfigūruotos taip, kad galėtų priimti ir persiųsti paketus bei tarpusavyje bendrauti pasinaudojant TCP/IP [23] protokolu ir veiks kaip maršrutizatoriai. Šie maršrutizatoriai sudarys diferencijuotų paslaugų domeną.

Maršrutizatorių konfigūracija pateikta 4 ir 5 lentelėse. Taip pat maršrutizatoriui yra skirtas tam tikras kiekis resursų (atminties, kietojo disko talpos, procesoriaus).

4 lentelė. Maršrutizatorių IP adresai

Maršrutzatorius	**Tinklo sąsaja**	**IP adresas**
R1	eth0	192.168.2.254
R1	eth1	192.168.3.128
R1	eth2	192.168.1.254
R2	eth0	192.168.3.254
R2	eth1	192.168.4.128
R3	eth0	192.168.4.254
R3	eth1	192.168.5.128
R4	eth0	192.168.5.254
R4	eth1	192.168.6.128

5 lentelė. Maršrutizatorių konfigūracija srauto perdavimui

Maršrutzatorius	**Intefeisų konfigūracija „/etc/network/interfaces“ faile**	**Maršrutų nustatymas „/etc/rc.local“ faile**
R1	auto eth0 iface eth0 inet static address 192.168.2.254 netmask 255.255.255.0 auto eth1 iface eth1 inet static address 192.168.3.128 netmask 255.255.255.0 auto eth2 iface eth2 inet static address 192.168.1.254 netmask 255.255.255.0	route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.3.254 route add -net 192.168.5.0 netmask 255.255.255.0 gw 192.168. 3.254 route add -net 192.168.6.0 netmask 255.255.255.0 gw 192.168. 3.254
R2	auto eth0 iface eth0 inet static address 192.168.3.254 netmask 255.255.255.0 auto eth1 iface eth1 inet static address 192.168.4.128	route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.3.128 route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.3.128 route add -net 192.168.5.0 netmask 255.255.255.0 gw 192.168.4.254 route add -net 192.168.6.0 netmask 255.255.255.0 gw 192.168.4.254

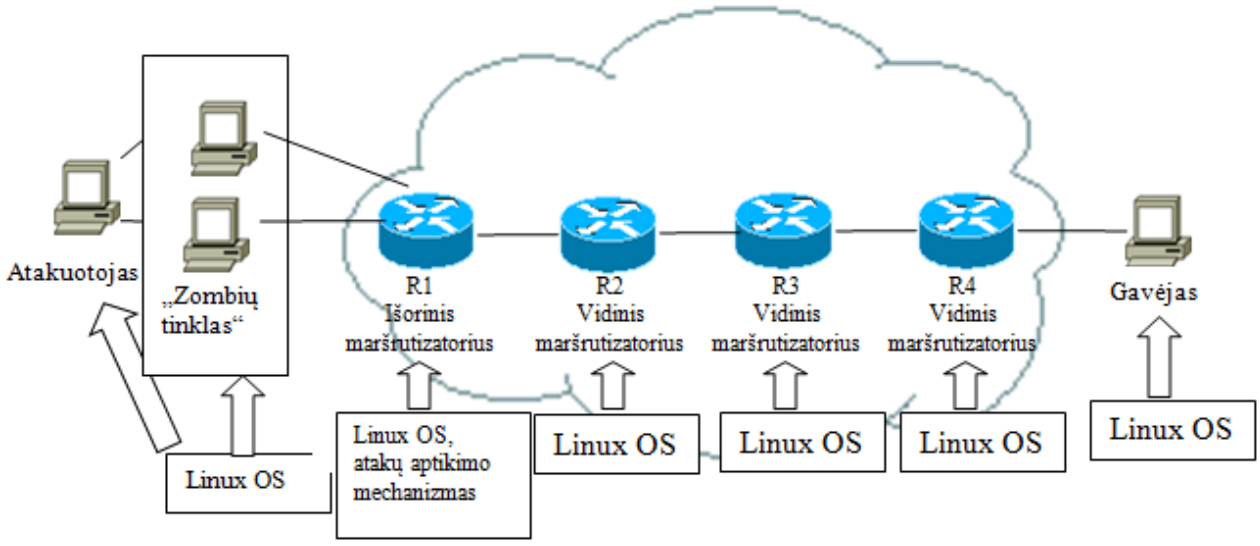
	netmask 255.255.255.0	
R3	auto eth0 iface eth0 inet static address 192.168.4.254 netmask 255.255.255.0 auto eth1 iface eth1 inet static address 192.168.5.128 netmask 255.255.255.0	route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.4.128 route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.4.128 route add -net 192.168.6.0 netmask 255.255.255.0 gw 192.168.5.254
R4	auto eth0 iface eth0 inet static address 192.168.5.254 netmask 255.255.255.0 auto eth1 iface eth1 inet static address 192.168.6.128 netmask 255.255.255.0	route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.5.128 route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.5.128 route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.5.128

Taip pat realizuotas atakuotojų tinklas sudarytas iš kelių virtualių kompiuterių, kurie generuos duomenų srautus ir siųs į maršrutizatorius bei vienas kompiuteris veiks kaip paslaugų gavėjas, kuris prijungtas prie domeno. Kompiuterių konfigūracija pateikta žemiau esančioje lentelėje. Kompiuteriai realizuoti Linux pagrindu.

6 lentelė. Kompiuterių konfigūracija

Atakuotojų tinklas	**Sąsajos konfigūracija „/etc/network/interfaces“ faile**	**Paslaugų gavėjas**	**Sąsajos konfigūracija „/etc/network/interfaces“ faile**
Pc1	auto eth0 iface eth0 inet static address 192.168.2.130 netmask 255.255.255.0 gateway 192.168.2.254	Pc4	auto eth0 iface eth0 inet static address 192.168.6.254 netmask 255.255.255.0 gateway 192.168.6.128
Pc2	auto eth0 iface eth0 inet static address 192.168.2.252 netmask 255.255.255.0 gateway 192.168.2.254		
Pc3	auto eth0 iface eth0 inet static address 192.168.1.130 netmask 255.255.255.0 gateway 192.168.1.254		

Realizavus prieš tai minėtus įrenginius gauname tokią topologiją:



30 pav. Įrenginių topologija

6.2 Maršrutizatoriaus apsaugos mechanizmų sukūrimas

Linux operacinėje sistemoje srauto filtravimas atliekamas naudojant “iptables” [24] paketą. Iptables galima traktuoti kaip ugniasienę. Dauguma sistemų, kurios veikia Linux pagrindu turi būti sukonfigūruota ugniasienė siekiant apsisaugoti nuo neteisėto srauto patekimo į sistemos vidų. Vienas iš būdų tai atlikti – pasinaudoti “iptables” galimybėmis.

Iptables konfigūracijoje naudojamos šios pagrindinės grandys:

- INPUT – skirta sudaryti taisykles, kurios naudojamos ateinančiam srautui iš įšorės analizuoti.
- OUTPUT – skirta sudaryti taisykles, kurios analizuos srautą išeinantį į išorę.
- FORWARD – skirta sudaryti taisykles, kurios analizuos srautą kurį reikia persiųsti į kitą įrenginį.

Įprastai Linux operacinėje sistemoje šios trys grandys yra sukurtos ir nustatyta, kad visi paketai būtų priimami, t.y. nustatyta “ACCEPT” elgsena. Tokiu atveju esama sistema yra pažeidžiama, nes gali priimti visus duomenų srautus neatskiriant ar tai teisėtas srautas ar sugeneruotas srautas skirtas sistemos sutridymui. Todėl pirmiausia reikia šioms trims grandims nustatyti, kad visi duomenų srautai būtų atmetami, t.y. nustatyti “DROP” elgseną. Tokiu atveju joks duomenų srautas nebus perduodamas į sistemą, iš jos išsiunčiamas ar persiunčiamas kitur.

Siekiant, kad sistema galėtų priimti tik tam tikrus duomenų srautus, reikia sukurti specifines taisykles tam tikroje grandyje bei nurodyti “ACCEPT” požymį. Tokiu atveju, tik su taisykles atitinkančiu duomenų srautu atliekami tam tikri veiksmai, o duomenų srautas neatitinkantis aprašytų taisyklių - atmetamas.

Norint apsisaugoti nuo paslaugų nutraukimo atakų ar paskirstytų paslaugų nutraukimo atakų, reikia analizuoti duomenų srautą įvertinant šiuos požymius: naudojamą protokolą (TCP, UDP, ICMP), perduodamų paketų skaičių per laiko vienetą, paketuose naudojamas vėliavėles, paketo dydį. Pagal šiuos požymius galima sukurti atitinkamas taisykles, pagal kurias analizuojamas srautas.

6.2.1 Maršrutizatorių sisteminių parametrų konfigūravimas

Darbo metu maršrutizatoriai sukonfigūruoti taip, kad praleistų tą duomenų srautą, kuris atitinka nustatytas taisykles. Taisyklių neatitinkantis duomenų srautas yra atmetamas. Papildomai be taisyklių sudarymo yra sukonfigūruojamas Linux branduolys:

Įjungiama IP klastojimo apsauga

```
for i in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 1 > $i; done
```

Įjungiama apsauga nuo SYN srauto

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Ignoruojame ICMP echo request užklausų transliavimą

```
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

Nepriimame ar nepersiunčiame ICMP nukreipimus

```
for i in /proc/sys/net/ipv4/conf/*/accept_redirects; do echo 0 > $i;
done
for i in /proc/sys/net/ipv4/conf/*/send_redirects; do echo 0 > $i;
done
```

Nepriimame siuntėjo mašrutizuojamų paketų

```
for i in /proc/sys/net/ipv4/conf/*/accept_source_route; do echo 0 >
$i; done
```

Išjungiame “multicast” maršrutizavimą

```
for i in /proc/sys/net/ipv4/conf/*/mc_forwarding; do echo 0 > $i; done
```

Atlikus šią konfigūraciją, sukuriame taisykles, kurios naudojamos siunčiamų duomenų analizei.

Ištriname visas taisykles

```
iptables –F
```

Nustatome INPUT, OUTPUT ir FORWARD grandims DROP elgseną.

```
iptables –P INPUT DROP
iptables –P OUTPUT DROP
iptables –P FORWARD DROP
```

Sukuriam taisykles nuo „Ping of death“ atakos

```
iptables -A INPUT -p ICMP --icmp-type echo-request -m length --length 60:800 -m
limit --limit 10/s --limit-burst 10 -j ACCEPT
iptables -A INPUT -p icmp -m limit --limit 10/s --limit-burst 10 -j LOG --log-prefix
"PING-DROP: "
iptables -A INPUT -p ICMP --icmp-type echo-request -m length ! --length 60:800 -j
LOG --log-prefix "per didelis ping paketas "
iptables -A INPUT -p ICMP --icmp-type echo-request -j DROP
iptables -A OUTPUT -p icmp -j ACCEPT
```

Sukuriam taisykles, kurios registruos ir blokuos visus ICMP paketus atėjusius ne iš vidinio tinklo

```
iptables -A INPUT  ! --source 192.168.2.0/24 -p icmp -j LOG --log-prefix "icmp
paketai is isores "
iptables -A INPUT -p icmp -j DROP
```

Sukuriam taisykles, kurios registruos ir blokuos visus TCP SYN paketus atėjusius ne iš vidinio tinklo

```
iptables -A INPUT  ! --source 192.168.2.0/24 -p tcp --syn -j LOG --log-prefix "SYN
paketai is isores "
iptables -A INPUT  ! --source 192.168.2.0/24 -j DROP
```

Apribojam TCP SYN paketų priėmimą iki tam tikro limito, o viršijus limitą – registruojam ir atmetam juos

```
iptables -A INPUT -p tcp --syn -m limit --limit 10/s --limit-burst 10 -j ACCEPT
iptables -A INPUT -p tcp --syn -m limit --limit 10/s --limit-burst 10 -j LOG --log-
prefix "SYN-DROP: "
iptables -A INPUT -p tcp -j DROP
iptables -A OUTPUT -p tcp -j ACCEPT
```

Sukuriam taisykles, kurios blokuos prievadų skanavimą

```
iptables -A INPUT  -p tcp --tcp-flags ACK,FIN FIN -j LOG --log-prefix "FIN ataka: "
iptables -A INPUT  -p tcp --tcp-flags ACK,FIN FIN -j DROP
iptables -A INPUT  -p tcp --tcp-flags ACK ACK -j LOG --log-prefix "ACK ataka: "
iptables -A INPUT  -p tcp --tcp-flags ACK ACK -j DROP
iptables -A INPUT  -p tcp --tcp-flags RST RST -j LOG --log-prefix "RST ataka: "
iptables -A INPUT  -p tcp --tcp-flags RST RST -j DROP
iptables -A INPUT  -p tcp --tcp-flags ACK,PSH PSH -j LOG --log-prefix "PSH ataka: "
iptables -A INPUT  -p tcp --tcp-flags ACK,PSH PSH -j DROP
iptables -A INPUT  -p tcp --tcp-flags ACK,URG URG -j LOG --log-prefix "URG ataka: "
iptables -A INPUT  -p tcp --tcp-flags ACK,URG URG -j DROP
```

```
iptables -A INPUT  -p tcp --tcp-flags ALL ALL -j LOG --log-prefix "XMAS scan ataka:
"
iptables -A INPUT  -p tcp --tcp-flags ALL ALL -j DROP
iptables -A INPUT  -p tcp --tcp-flags ALL NONE -j LOG --log-prefix "NULL scan ataka:
"
iptables -A INPUT  -p tcp --tcp-flags ALL NONE -j DROP
iptables -A INPUT  -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j LOG --log-prefix
"prievadu skanavimas: "
iptables -A INPUT  -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
iptables -A INPUT  -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG --log-prefix "SYN-FIN
ataka: "
iptables -A INPUT  -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
iptables -A INPUT  -p tcp --tcp-flags FIN,RST FIN,RST -j LOG --log-prefix "FIN-RST
ataka: "
iptables -A INPUT  -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -A INPUT  -p tcp --tcp-flags ALL URG,PSH,FIN -j LOG --log-prefix "XMAS-SCAN
ataka: "
iptables -A INPUT  -p tcp --tcp-flags ALL URG,PSH,FIN -j DROP
iptables -A INPUT  -p tcp --tcp-flags ALL FIN -j LOG --log-prefix "FIN-SCAN ataka: "
iptables -A INPUT  -p tcp --tcp-flags ALL FIN -j DROP
iptables -A INPUT  -p tcp --tcp-flags SYN,RST SYN,RST -j LOG --log-prefix "SYN-RST
ataka: "
iptables -A INPUT  -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
```

Uždraudžiam UDP paketų priėmimą iš išorės tinklų

```
iptables -A INPUT -p udp ! --source 192.168.2.0/24 -j LOG --log-prefix "UDP paketai
is isores"
iptables -A INPUT -p udp ! --source 192.168.2.0/24 -j DROP
```

Apribojam UDP paketų priėmimą iki tam tikros ribos. Viršijus ribą – paketai registruojami ir atmetami.

```
iptables -A INPUT -p udp -m limit --limit 10/s --limit-burst 10 -j ACCEPT
iptables -A INPUT -p udp -m limit --limit 10/s --limit-burst 10 -j LOG --log-prefix
"UDP-DROP: "
iptables -A INPUT -p udp -j DROP
iptables -A OUTPUT -p udp -j ACCEPT
```

6.3 Duomenų srauto analizavimas

Siekiant įvertinti kaip tiksliai veikia sukurtas apsaugos modulis reikia nustatyti kokį duomenų srautą praleido, o kokį atpažino kaip kenkėjišką. Šiam tikslui pasiekti naudojamas „Tcpdump“ [25]

paketas, kuris gali rinkti informaciją apie duomenų srautus. Šis paketas veikia iš komandinės eilutės ir geba surinkti įvairią informaciją, pvz.: IP adresus, naudojamus paketus ir vėliavėles, paketo dydžius ir pan.

Šis paketas įdiegtas maršrutizatoriuje, kuriame yra įdiegtas ir apsaugos modulis. Tokiu atveju galima stebėti kokius duomenų srautus apsaugos modulis praleidžia, o kokius nepraleidžia.

Norint naudotis „Tcpdump“ paketu, pirmiausia jį reikia įsidiegti. Atlikus šį žingsnį galime stebėti informaciją apie duomenų srautus komandiniame lange arba visą informaciją įrašyti į failą.

Tcpdump paketo iškvietimas pradedamas nuo „tcpdump“ žodžio suvedimo į komandinę eilutę. Toliau pateikiami pavyzdžiai kaip naudoti šį paketą.

```
tcpdump –i eth0 port 80 –w paketai.log (1)
tcpdump –i eth0 udp –w paketai.log     (2)
```

Pirma eilutė nurodo, kad įrašinėtų duomenų srautą į failą „paketai.log“, kuriame duomenys siunčiami tcp protokolu į 80 prievadą per eth0 tinklo sąsają.

Antra eilutė nurodo, kad įrašinėtų duomenų srautą į failą „paketai.log“, kuriame duomenys siunčiami udp protokolu per eth0 tinklo sąsają.

Norint išsifiltruoti TCP protokolo paketus su SYN vėliavėle siųstus į 80 prievadą suvedame šią komandą:

```
tcpdump tcp and port 80 and 'tcp[tcpflags] & tcp-syn == tcp-syn'
```

6.4 Duomenų srauto generavimas

Generuoti duomenų srautui naudojamas „Hping3“ [26] paketas. Pagrindinės jo savybės:

- veikia iš komandinės eilutės
- galima generuoti įvairių protokolų paketus
- galima nurodyti į koki prievadą siųsti paketus
- galima nurodyti kokias naudoti vėliavėles
- galima nurodyti kiek siųsti paketų
- galima nurodyti kaip greitai siųsti paketus.

Duomenims generuoti ir testuoti sukurtą apsaugos modulį naudosime šias komandas.

```
1. hping3 –i u1000 –c 20 –S 192.168.2.254
2. hping3 --icmp --icmptype 8 192.168. 192.168.2.254
3. hping3 --udp  -i u1000 192.168.2.254
```

1 eilutės komanda naudojama TCP srauto su SYN vėliavėle generavimui.

2 eilutė naudojama ICMP protokolo „ping request“ užklausai generuoti.

3 eilutė naudojama UDP srauto generavimui.

Komandinės eilutės paaiškinimas:

`hping3` – iškviečiamas pats įrankis

`-i u1000` – nurodoma, kad siunčiama 100 paketų per sekundę

`-c 20` – nurodoma, kad siunčiama 20 paketų

`-S` – nurodoma, kad naudojama SYN vėliavėlė

`192.168.11.134` – nurodomas įrenginio IP adresas

`--icmp --icmptype 8` – nurodoma, kad generuojamas icmp protokolo paketai su „ping request“ uzklausa

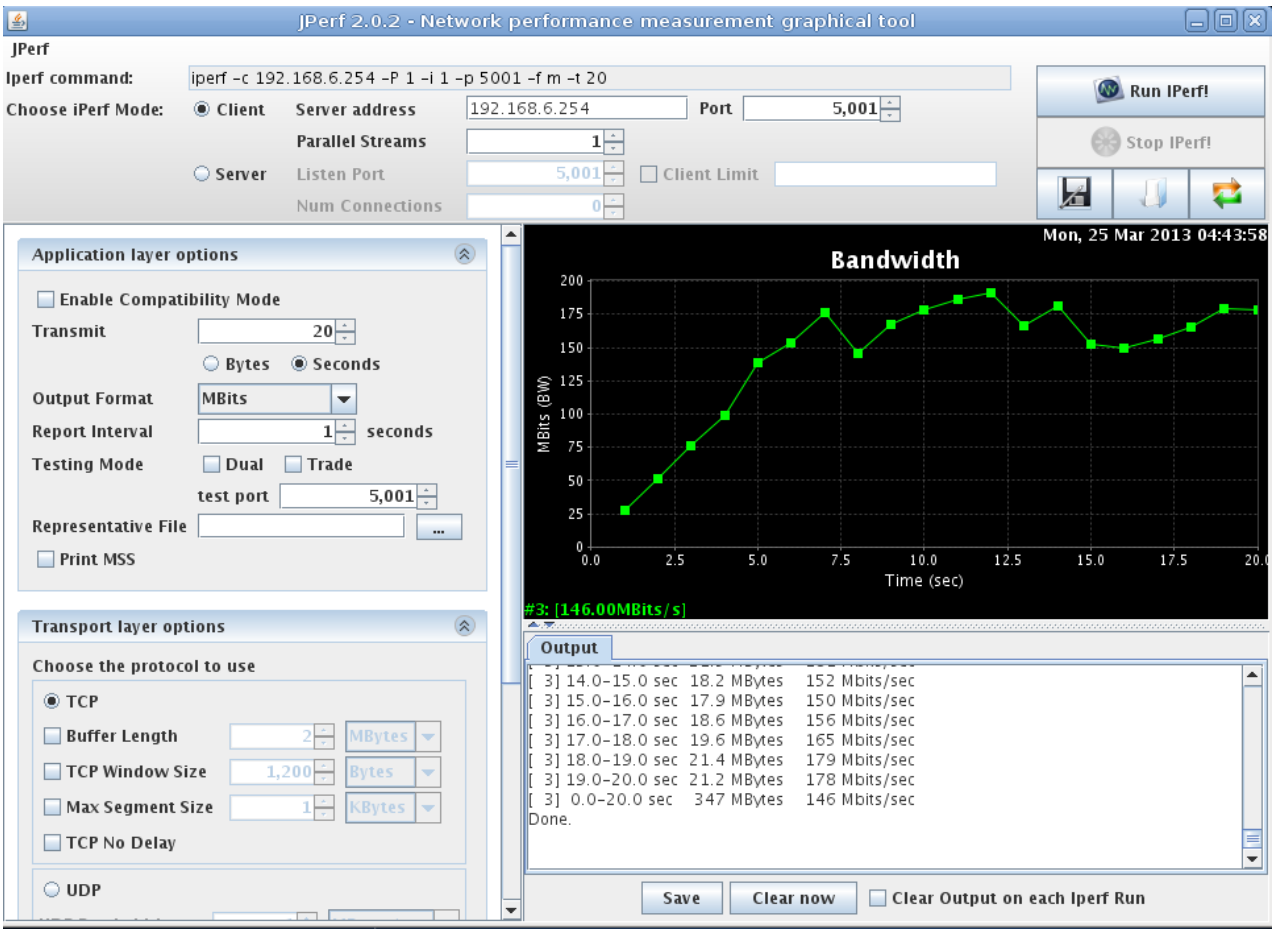
`--udp` – nurodoma, kad generuojamas „UDP“ protokolo srautas.

6.5 Eksperimento eigos aprašymas

Eksperimentas atliktas dviem etapais:

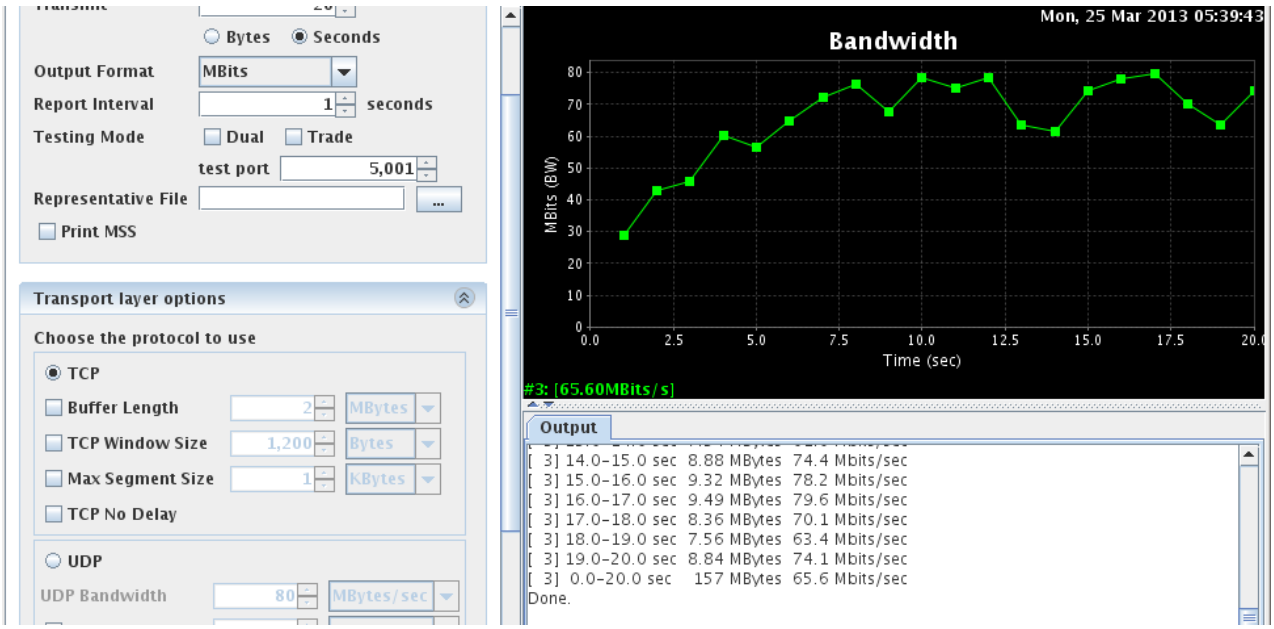
1. Srauto matavimas su realizuota paspartinto perdavimo klase domene.
   - Atliekant srauto matavimą naudojant Jperf įrankį
   - Atliekant srauto matavimą naudojant Jperf įrankį ir Hping3 įrankį sukelti DDoS ataką
   - Atliekant srauto matavimą naudojant ir nenaudojant apsaugos modelį.
   - Atliekant srauto matavimą naudojant Jperf ir Hping3 įrankius bei panaudojant apsaugos modelį.
2. Įvertinant kokias atakas apsaugos modelis aptinka ir sustabo.
   - Atliekant srauto generavimą naudojant Hping3 įrankį sukelti DDoS ataką ir panaudojus apsaugos modelį.

Pirmo eksperimento etapo metu buvo naudojami du kompiuteriai – gavėjas ir siuntėjas, bei diferencijuotų paslaugų domenas. Abejuose kompiuteriuose įdiegta Linux operacinė sistema ir Jperf įrankis. Šiuo įrankiu buvo generuojamas TCP protokolo srautas iš siuntėjo kompiuterio, kuris keliavio per visą domeną iki gavėjo. Domene nebuvo nustatyti jokie srauto apribojimo ir filtravimo taisyklės. Gavėjo kompiuteryje buvo rodomi rezultatai apie perduotą duomenų kiekį ir spartą. Rezultate galėjome pamatyti tinklo pralaidumą (žr 31 pav.), jis buvo apie 150 Mbytes/s.



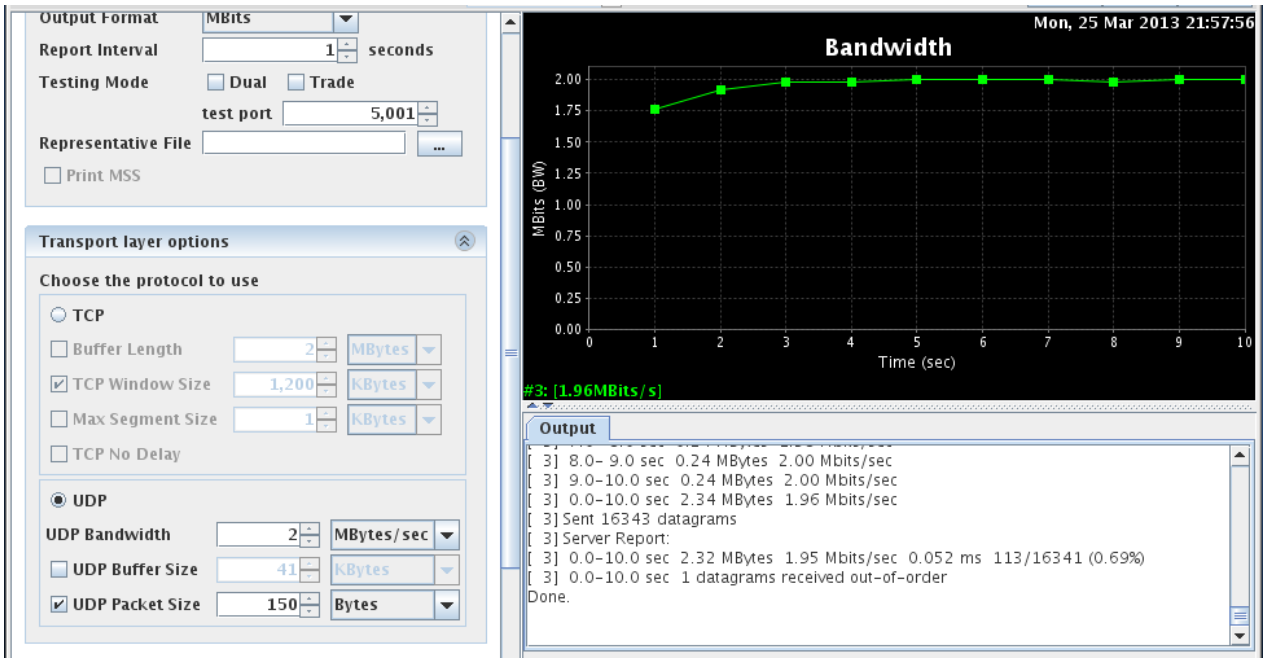
31 pav. TCP srauto pralaidumas

Papildomai buvo prie domeno prijungti du kompiuteriai, kurie veikia kaip atakuotojai. Šiose kompiuteriuose taip pat įdiegta Linux operacinė sistema ir Hping3 įrankis, skirtas generuoti kenkėjiškam srautui. Šis srautas buvo siunčiamas į gavėjo kompiuterį. Tuo pat metu buvo generuojamas srautas Jperf įrankiu iš siuntėjo į gavėjo kompiuterį. Šiuo etapu tinklo srauto pralaidumas (žr. 32 pav.) buvo apie 66 Mbytes/s. Priklausomai nuo generuojamų kenkėjiškų paketų (siuntimo greitis, paketų dydis, paketų defragmentacijos) galima sumažinti perduodamų srautų spartą tinkluose arba visiškai užkirsti kelią teisėto srauto gavimui. Tai įrodo, kad diferencijuotų paslaugų domeno tinklai yra pažeidžiami DDoS atakų.

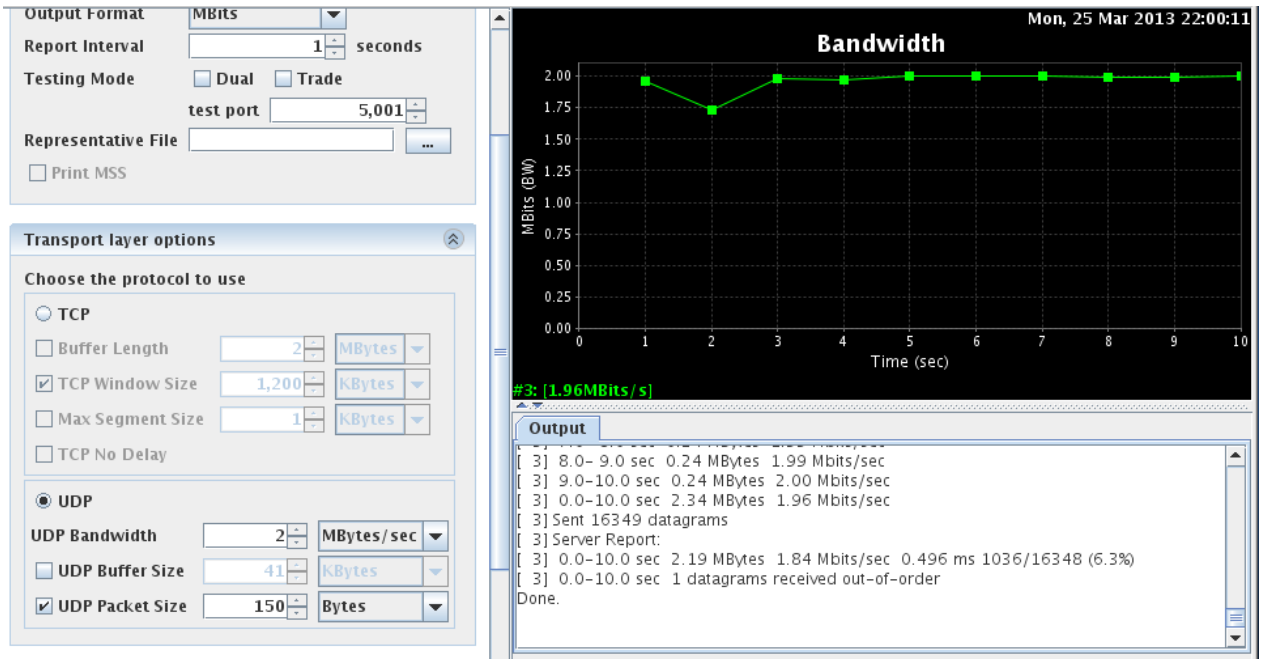


32 pav. TCP srauto pralaidumas įvykdžius ataką

Žemiau esančiame paveiksliuke (žr. 33 pav.) pavaizduotas UDP srauto pralaidumas kai realizuota paspartinto perdavimo klasė domene. Iš paveikslio matyti, kad generuojamas 2 Mbytes/s srautas su 150 baitų paketais. Po grafiku pateiktoje rezultatų lange matome, kad paketų praradimas yra apie 0,7 procento.

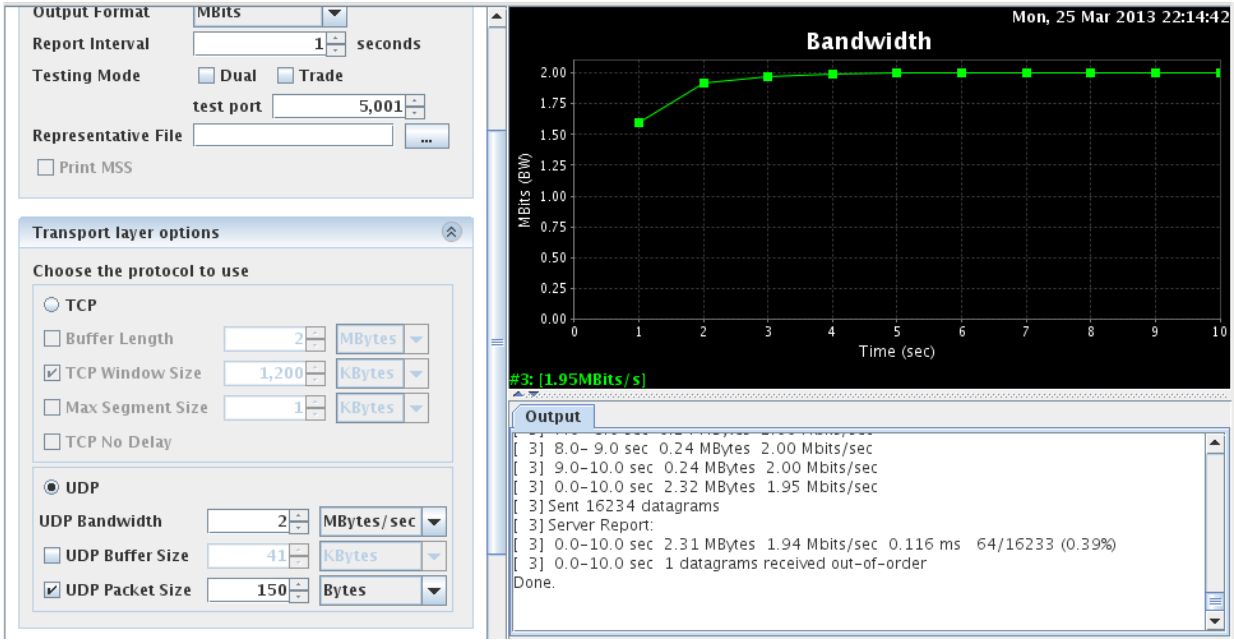


33 pav. UDP srauto pralaidumas su paspartinto perdavimo klase



34 pav. UDP srauto pralaidumas įvykdžius ataką

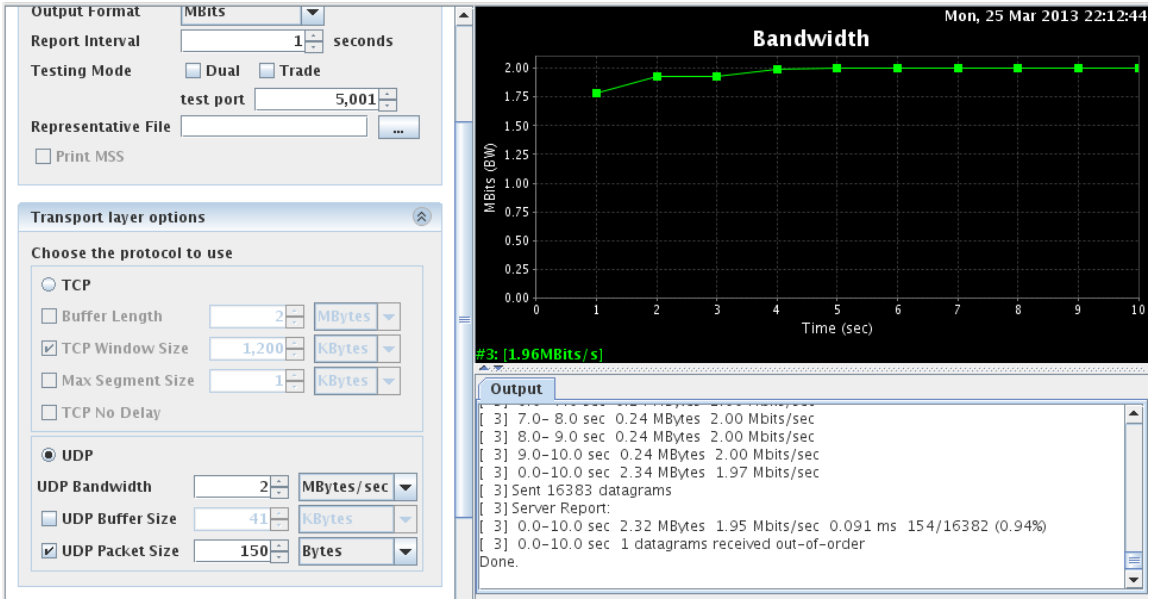
34 pav. pateiktas grafikas, kuris parodo kaip keičiasi UDP srauto pralaidumas, kai atliekama ataka. Rezultatų lange galima pamatyti, kad šiuo atveju prarasta 1036 paketai iš 16348 paketų, o vėlinimų svyravimai yra apie puse sekundės.



35 pav. Srauto generavimas be srauto apribojimo ugniasienėje

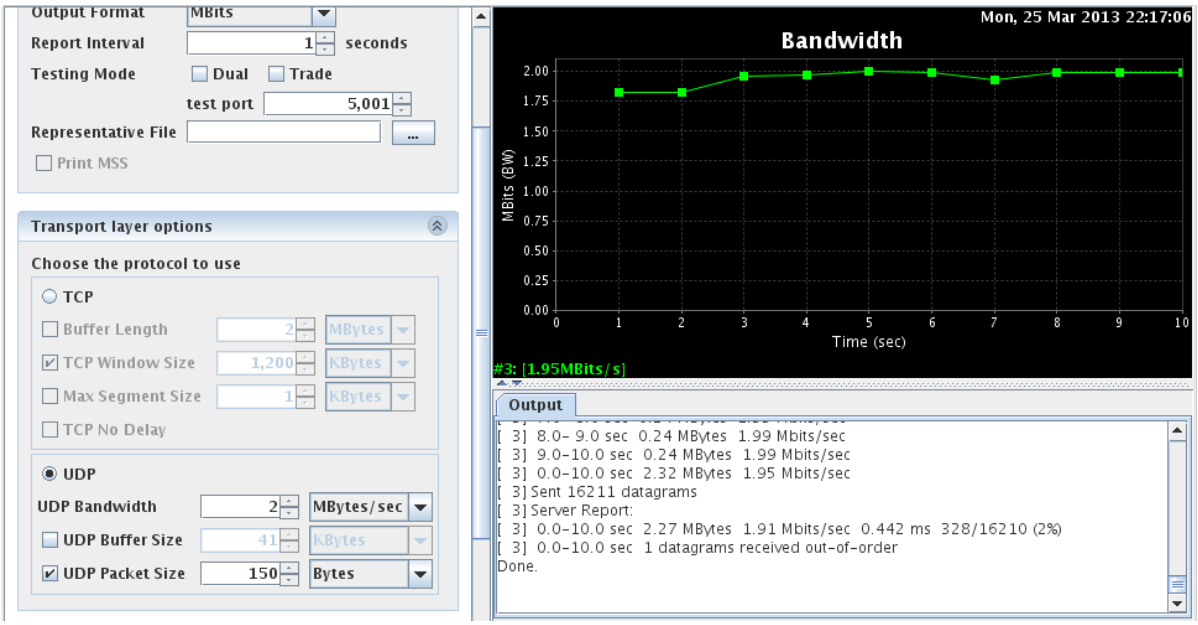
Aukščiau pavaizduotame paveiksliuke (žr. 35 pav.) atliktas srauto generavimas, kai nerealizuota ugniasienė su priimamų paketų per laiko vienetą limitą. Rezultatų lange matyti, kad paketų praradimas yra mažas.

Žemiau esančiame paveiksliuke (žr. 36 pav.) pavaizduotas srauto generavimas, kai ugniasienėje nustatytas priimamų paketų skaičius per laiko vienetą limitas. Šiuo atveju, prarastų paketų skaičius padidėjo lyginant su atveju, kai ugniasienėje nebuvo realizuotas priimamų duomenų limitas.



36 pav. Srauto generavimas su srauto apribojimo ugniasienėje.

Paskutiniu atveju generuojamas srautas (žr. 37 pav.) kai vykdoma ataka ir ungiasienėje nustačius filtravimo taisykles su priimamų paketų kiekiu per laiko vienetą limitą. Rezultatų lange esanti informacija parodo, kad prarastų paketų skaičius yra mažesnis nei atakos atveju be sukonfigūruotos ugniasienės.



37 pav. Srauto generavimas vykdant ataką ir sukonfigūravus ugniasienę

Antro etapo metu panaudojus Hping3 įrankį buvo generuojamos DDoS atakos ir siunčiamos į kraštinį maršrutizatorių. Šiame maršrutizatoriuje realizuota apsaugos sistema, kuri analizuoja ir blokuoja arba praleidžia duomenų srautus. Informacija apie sukeltas atakas ir jų aptikimą pateikta 8 lentelėje.

Vienas iš atakų generavimo pavyzdžių pateikta 38 pav., kuriame pavaizduota kaip atliekama TCP SYN ataka panaudojus Hping3 įrankį:

```
hping3 -S -i u10000 192.168.2.254
```

hping3 – nurodo, kad iškviečiam hping3 įrankį.

-S – nurodo, kad naudosim SYN vėliavėlę siunčiamuose paketuose

-i u10000 – nurodo, kad siunčiama 100 paketų per sekundę

192.168.2.254 – nurodomas atakuojamas kompiteris

38 pav. TCP SYN atakos pavyzdys panaudojus Hping3 įrankį

Atakų lentelėje pavaizduota kiek kartų ir kokios atakos buvo įvykdytos.

7 lentelė. Atakų įvykdymo Hping3 įrankio komandos

	Siuntimo intensyvumas paketai/s	Atakos įvykdymo komanda	Paketo dydis, baitais
TCP SYN ataka	10000	hping3 –S –i u1000 –d 5000 192.168.2.254	5000
Ping of death ataka	10000	hping3 –1 –i u1000 –d 200 192.168.2.254	200
Prievadų skanavimas siunčiant ACK paketus	100	hping3 –A –i u10000 192.168.2.254	100
Prievadų skanavimas siunčiant RST paketus	100	hping3 –R –i u1000 192.168.2.254	100
ICMP srauto siuntimas iš išorės suklastojus siuntėjo IP adresą	100	hping3 –1 –a 192.168.2.222 –i u1000 –d 200 192.168.2.254	100
TCP SYN srauto siuntimas iš išorės suklastojus siuntėjo IP adresą	100	hping3 –S –a 192.168.2.222 –i u1000 –d 200 192.168.2.254	100
UDP srauto siuntimas iš išorės suklastojus siuntėjo IP adresą	100	hping3 --udp –a 192.168.2.222 –i u1000 –d 200 192.168.2.254	100

6.6 Eksperimentiniai rezultatai

8-9 lentelėse pateikti eksperimento metu gauti rezultatai. 8 lentelėje pateikti filtravimo taisyklių rezultatai, 9 lentelėje pateikti duomenys rodantys koks yra DDoS atakų aptikimo efektyvumas panaudojus įdiegtą apsaugos modulį kraštiniame maršrutizatoriuje.

8 lentelė. Filtavimo taisyklių rezultatai

	Siųsta paketų	Gauta paketų	Prarasta, %	Atakų pranešimai
TCP SYN paketai iš vidinio tinklo	309	44	86	Apr 29 03:57:45 R1 kernel: [27635.312995] **SYN-DROP**: IN=eth0 OUT= SRC=**192.168.2.252** DST=**192.168.2.254** LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=64945 PROTO=TCP SPT=2056 DPT=0 WINDOW=512 RES=0x00 **SYN** URGP=0
Ping of death ataka	326	45	87	Apr 29 04:01:18 R1 kernel: [27848.239412] **PING-DROP**: IN=eth0 OUT= SRC=**192.168.2.252** DST=**192.168.2.254** LEN=28 TOS=0x00 PREC=0x00 TTL=64 ID=9653 PROTO=**ICMP TYPE=8** CODE=0 ID=20745 SEQ=3584
Prievadų skanavimas	100	10	90	Apr 29 06:38:06 R1 kernel: [37242.402415] ACK: IN=eth0 OUT= SRC=**192.168.2.252** DST=**192.168.2.254** LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=26051 PROTO=TCP SPT=1205 DPT=0 WINDOW=512 RES=0x00 **ACK** URGP=0
ICMP paketai iš išorės	845	0	100	Apr 29 04:08:45 R1 kernel: [28295.189070] **icmp paketai is isores** IN=eth2 SRC=192.168.1.130 DST=192.168.2.254 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=876 PROTO=**ICMP TYPE=8** CODE=0 ID=54793 SEQ=512
TCP SYN paketai iš išorės	584	0	100	Apr 29 04:28:31 R1 kernel: [29479.163016] **SYN paketai is isores** IN=eth2 OUT= SRC=**192.168.1.130** DST=**192.168.2.254** LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=55417 PROTO=TCP SPT=2964 DPT=0 WINDOW=512 RES=0x00 **SYN** URGP=0
UDP srauto blokavimas nuo išorės	100	0	100	Apr 29 04:28:31 R1 kernel: [29479.163016] **UDP paketai is isores** IN=eth2 OUT=

				SRC=**192.168.1.130** DST=**192.168.2.254** LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=55417 PROTO=UDP SPT=2964 DPT=0 WINDOW=512 RES=0x00 URGP=0

9 lentelė. Įvykdytos atakos ir jų aptikimas

	Generuotas atakų skaičius	Aptiktų atakų skaičius	Aptikimo efektyvumas, %
TCP SYN ataka	15	12	80
Prievadų skanavimo ataka	15	15	100
Ping of death ataka	14	12	87,5
TCP srauto blokavimas nuo nenustatytų IP adresų	14	11	78,5
ICMP srauto blokavimas nuo nenustatytų IP adresų	14	13	93
UDP srauto blokavimas nuo nenustatytų IP adresų	14	12	87,5

Iš lentelės matyti, kad įvykdytų atakų ir aptiktų atakų skaičius yra panašus, tai reiškia, kad kiek kartų įvykdyta ataka beveik tiek pat kartų ji yra ir aptikta/sustabdyta. Dalis atakų galėjo praeiti pro apsaugos modelį, nes galbūt atakuotojas nurodė labai specifinius parametrus, todėl apsaugos modelis galėjo neaptikti atakos. Kita priežastis kodėl ataka galėjo būti neaptikta yra neteisingas filtravimo taisyklių nustatymas.

8 lentelėje pateikta informacija parodo kaip veikia filtravimo taisyklės. Pavyzdžiui „Ping of Death“ atakos metu, atakuotojo kompiuteryje buvo generuojamas ICMP protokolo srautas ir siunčiamas į kraštinį maršrutizatorių. Iš lentelės matyti, kad buvo generuojami 326 paketai, tačiau į šią užklausą buvo atsakyti tik 45 paketai. Visi kiti paketai buvo atmesti, o tai sudarė 86% visų gautų paketų. Taip pat nustatytų filtravimo taisyklių neatitinkantys srautai buvo registruojami įvykių žurnale. Įvykių žurnale pateikiama pakankamai išsami informacija apie gautus paketus (siuntėjo ir gavėvo IP, protokolas, vėliavėlė, dydis ir pan).

6.7 Skyriaus išvados

Šio darbo dalyje aptarti darbo realizacijos principai. Visa sistemos realizacija atlikta virtualiai pasinaudojant VMware programine įranga. Iš viso sukurtos 8 virtualios mašinos, 4 iš jų naudojamos kaip maršrutizatoriai, o likusios naudojamos sudaryti atakuotojų tinklui bei gavėjui. Virtualių mašinų operacinė sistema – Linux ir jos tarpusavyje bendraus TCP/IP protokolo pagrindu.

Paketų analizei naudojamas „TCPdump“ įrankis. Šiuo įrankiu galima rinkti įvairią informaciją apie duomenų srautus, pvz.: protokolus, paketų dydžius, siuntėjo ir gavėjo IP adresus ir kitokią informaciją.

Atakoms generuoti pasitelktas „Hping3“ įrankis. Šis įrankis gali generuoti įvairių protokolų paketus su įvairiais parametrais, pvz.: nurodyti prievadus, paketų dydžius, vėliavėles, siuntimo greitį, kiek paketų siųsti ir pan.

Apsaugos modulis diegiamas pirmame maršrutizatoriuje. Šį apsaugos modulį sudaro Linux branduolio konfigūracija ir specifinės taisyklės skirtos srauto analizavimui. Jei ateinantis duomenų srautas tenkins nustatytas taisykles, jis perduodamas toliau, kitu atvejų – atmetamas.

Srauto analizavimo taisyklių kūrimo metu labai svarbu tiksliai jas įvertinti ir nustatyti pagal tam tikrus parametrus, nes blogai jas sukūrus, pvz, nustačius labai grieztus parametrus galima susidurti su teisėto srauto priėmimo problemomis. Kitu atveju, nustačius abstrakčias taisykles, galimas kenkėjiško srauto priėmimas ir apdorojimas kaip ir teisėto srauto atveju.

Šio eksperimento metu stebimi šie parametrai: perduodamų paketų skaičius per laiko vienetą, naudojamas vėliavėles, paketo dydžius ir protokolus. Ištirus šiuos parametrus galima įvertinti kaip tiksliai dirba sistema siekiant apsisaugoti nuo atakų.

Eksperimentas atliktas dviem etapais: pirmu etapu buvo realizuota paspartinto perdavimo klasė domene. Taip pat atliktas srauto generavimas įvairiom sąlygom. Pirmiausia buvo generuojamas srautas įvertinant kaip veikia realizuota klasė. Poto buvo generuojamas srautas ir stebimi paketų praradimai kai tuo pačiu metu generuojamas atakos srautas. Paskutinis bandymas buvo atliktas generuojant teisėtą srautą ir atakos srautą vienu metu su realizuotu apsaugos modeliu. Iš rezultatų matyti, kad apsaugos modelis apsaugo nuo atakų, nes prarasta mažiau paketų, nei be apsaugos modelio.

Antru etapu buvo generuojamos įvairios atakos ir stebima kiek ir kokių atakų apsaugos modelis sugeba aptikti. 8 lentelėje pavaizduota kiek kievienos atakos paketų siuntė atakuotojas, kiek paketų buvo apdorota ir kiek buvo nufiltruota. 9 lentelėje pateikti rezultatai parodo, kad apsaugos modelio efektyvumas yra apie 80-90%.

IŠVADOS

1. Diferencijuotų paslaugų architektūros tinklai naudojami duomenų srautų, o tuo pačiu ir paslaugų, kokybės užtikrinimui. Tokio tipo tinklo savybių analizė parodė, kad diferencijuotų paslaugų domeno kritine pažeidžiama vieta pirmiausia tampa kraštinis įėjimo į domeną maršrutizatorius, tačiau pažeidžiami gali būti ir vidiniai maršrutizatoriai.

2. DDoS atakos gali būti įvairios, todėl identifikuoti jas pagal vieną parametrą neefektyvu. Parenkant apsaugos nuo DDoS atakų priemones, atakų aptikimui ir duomenų paketų filtravimui tikslinga naudoti keletą duomenų srauto požymių analizuojančius įrankius arba juos apjungti.

3. Norint apsaugoti diferencijuotų paslaugų architektūros tinklus nuo DDoS atakų siūlomi įvairūs sprendimo būdai, tačiau jie negali visiškai užtikrinti, kad visos DDoS atakos bus aptiktos ir sustabdytos. Atlikus šių priemonių analizę nuspręsta projektuoti diferencijuotų paslaugų architektūros tinklų apsaugos nuo DDoS atakų sistemą panaudojant duomenų srauto filtravimo ir blokavimo priemones (ugniasienė, srauto nukreipimo metodas/principas) lygiagrečiai jas papildant naujais apsaugos elementais, leidžiančiais užtikrinti didesnį diferencijuoto paslaugų domeno apsaugojimo nuo DDoS atakų lygį.

4. Darbe pasiūlytas apsaugos nuo DDoS atakų modelis pritaikytas diferencijuotų paslaugų architektūros tinklams – šioje architektūroje apibrėžtas standartinis klasifikavimo procesas papildytas duomenų srauto analize pagal papildomus, DDoS atakoms būdingus požymius. Taip pat standartinis duomenų srauto priskyrimo tam tikrai srauto klasei (su atitinkama duomenų srauto apdorojimo elgsena) procesas papildytas taisyklėmis, leidžiančiomis įtartiną srautą priskirti žemiausią aptarnavimo prioritetą turinčiai srauto klasei, taip išvengiant nepageidaujamo poveikio aukštesnį prioritetą turintiems srautams.

5. Pasiūlyto modelio pagrindu suprojektuotas ir realizuotas DDoS atakų aptikimo sistemos prototipas – į ugniasienę integruotos taisyklės skirtos DDoS atakų aptikimui ir sustabdymui, dinaminis jų įtraukimas ir išmetimas į/iš taisyklių sąrašo, realizuoti duomenų srauto filtravimo ir duomenų paketų peržymėjimo algoritmai.

6. Realizuota sistema įvertinta eksperimentiniu būdu. Nustatyta, kad sukurta sistema aptinka 80-90 % visų generuotų DDoS atakų.

LITERATŪRA

[1] Diferencijuotų paslaugų architektūra [žiūrėta 2012-01-23] Internetinė prieiga http://www.ietf.org/rfc/rfc2475.txt

[2] Paspartinto perdavimo klasė [žiūrėta 2012-01-23] Internetinė prieiga http://www.faqs.org/rfcs/rfc2598.html

[3] Garantuoto perdavimo klasė [žiūrėta 2012-01-23] Internetinė prieiga http://www.faqs.org/rfcs/rfc2597.html

[4] Geriausių pastangų klasė [žiūrėta 2012-01-23] Internetinė prieiga http://www.faqs.org/rfcs/rfc5290.html

[5] WRR eilių aptarnavimo disciplinos algoritmas [žiūrėta 2012-02-23] Internetinė prieiga http://www.cse.iitb.ac.in/~varsha/allpapers/packet-scheduling/wfqJuniper.pdf

[6] A.Striegel. „Security Issues in a Differentiated Services Internet“. University of Notre Dame, USA, 2002. P. 3

[7] Khaled M. Elleithy et. al., Denial of Service Attack Techniques: Analysis, Implementation and Comparison [žiūrėta 2012-02-23] Internetinė prieiga http://www.iiisci.org/Journal/CV$/sci/pdfs/P129065.pdf

[8] Lau, F.; Rubin, S.H.; Smith, M.H.; Trajkovic, L. „Distributed denial of service attacks“ IEEE International conference. USA. 2000. P. 2275-2277

[9] Stephen M. Specht; Ruby B. Lee. “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures“. Princeton, NJ, 2004. P.1-2

[10] Sanjeev Kumar. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. Texas, USA. 2007 July. P. 2-3

[11] Lasse Huovinen, Jani Hursti, Denial of Service Attacks: Teardrop and Land [žiūrėta 2012-10-23] Internetinė prieiga http://users.tkk.fi/lhuovine/study/hacker98/dos.html

[12] Naoum Naoumov, Keith Ross. Exploiting P2P Systems for DDoS Attacks. Brooklyn, New York. 2006. P. 1-5

[13] Subramani rao Sridhar rao, Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis [žiūrėta 2012-10-23] Internetinė prieiga http://www.sans.org/reading_room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi_33764

[14] Paskirstyta apspindėta paslaugų nutraukimo ataka (DRDoS) [žiūrėta 2012-10-23] Internetinė prieiga http://palpapers.plynt.com/issues/2006Apr/ddos-reflection/

[15] Paslaugų nutraukimo apsaugos sistema [žiūrėta 2013-01-23] http://www.vigilsoftware.com/index.php/corero-dds

[16] Ciso DDoS Protection Solution —Delivering “CLEAN PIPES” Capabilities for Service providers

and Their Customers [žiūrėta 2013-02-10] Internetinė prieiga http://www.cisco.com/cdc_content_elements/networking_solutions/service_provider/ddos_protection_sol/ddos_protection_sol_wp_0603.pdf, P.4

[17] Victor Oppleman, Network Defense Applications using IP Sinkholes [žiūrėta 2013-03-15] Internetinė prieiga vostrom.com/get/netdef_en.pdf

[18] A. Striegel Security Issues in a Differentiated Services Internet, University of Notre Dame, USA, 2002. P.4

[19] Xiaoyong Wu Vinay A. Mahadik, Douglas S. Reeves. A summary of Detection of Denial-of-QoS Attacks on DiffServ Networks. 2003. P.1-2

[20] Cisco IoS konfigūracija [žiūrėta 2013-03-15] Internetinė prieiga http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i2.html

[21] DSCP žymė. [žiūrėta 2011-03-15] Internetinė prieiga http://tools.ietf.org/html/rfc5865

[22] VMware programinė įranga [žiūrėta 2012-12-10] Internetinė prieiga http://www.vmware.com/

[23] TCP/IP protokolas [žiūrėta 2012-12-10] Internetinė prieiga http://lt.wikipedia.org/wiki/TCP/IP

[24] Iptables administravimo įrankis [žiūrėta 2013-01-15] Internetinė prieiga http://ipset.netfilter.org/iptables.man.html

[25] TCPdump paketų analizavimo įrankis [žiūrėta 2013-02-17] Internetinė prieiga http://www.tcpdump.org/

[26] Hping3 paketų generavimo įrankis [žiūrėta 2013-02-18] Internetinė prieiga http://www.hping.org/hping3.html

Priedai

1 Priedas. Prisijungimo duomenys prie įrenginių

10 lentelė. Prisijungimo duomenys prie maršrutizatorių ir kompiuterių:

Maršrutzatorius	**Prisijungimo vardas**	**Slaptažodis**	**Administratoriaus slaptažodis**
R1	router1	router1	l1nuxr00t
R2	router1	router1	l1nuxr00t
R3	router1	router1	l1nuxr00t
R4	router1	router1	l1nuxr00t
Kompiuteris	**Prisijungimo vardas**	**Slaptažodis**	**Administratoriaus slaptažodis**
Pc1	pc1	pc1	l1nuxr00t
Pc2	pc1	pc1	l1nuxr00t
Pc3	pc1	pc1	l1nuxr00t
Pc4	pc1	pc1	l1nuxr00t