

VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Kursinis darbas

VPN tuneliavimo protokolai

Atliko: 3 kurso, 9 grupės studentas

Džiugas Baltrūnas (parašas)

Darbo vadovas:

A. Maisiejus (parašas)

Vilnius

2004

Turinys

1. VPN tuneliavimas	4
1.1. Enkapsuliacija	4
1.2. Tunelio komponentai	4
1.3. Tuneliavimo (pernešimo) protokolų sąrašas	4
1.4. Tunelių tipai	5
1.4.1. Laisvieji tuneliai	5
1.4.2. Priverstiniai tuneliai	5
2. Tuneliavimo protokolai	6
2.1. Antrojo sluoksnio tuneliavimo protokolai	6
2.1.1. PPTP	6
2.1.2. L2TP	8
2.2. Trečiojo sluoksnio protokolai	9
2.2.1. IPSec	9
3. VPN protokolų našumo tyrimas.....	12
3.1. PPTP našumas	13
3.2. L2TP tyrimas.....	14
3.3. IPSec tyrimas	16
3.3.1. Tunelio režimas	16
3.3.2. Transporto režimas	18
Literatūros sąrašas.....	21
Priedas Nr. 1.....	22

Įvadas

VPN (angl. k. Virtual Private Network) – virtualus privatus tinklas. Tai tokia privačių tinklų realizavimo technologija, kurioje duomenų perdavimui iš vieno privataus tinklo į kitą yra naudojamas viešasis tinklas – Internetas. Tinklas čia virtualus todėl, kad fizinio susijungimo pagrindu yra formuojamas loginis ryšys – sukuriamas „tunelis“ tarp susijungiančių taškų.

Šiandien vis daugiau įmonių, turinčių savo padalinių skirtinguose geografiniuose regionuose, atsisako įprastinių nutolusių kompiuterinių tinklų sujungimo technologijų, tokių kaip skirtinės ar dedikuotos linijos ir renkasi virtualaus privataus tinklo technologijas. Galima išskirti dvi pagrindines tokio pasirinkimo priežastis. Pirmoji - sutaupomos lėšos palyginti brangiai tinklų sujungimo aparatūrai bei mokesčiams telekomunikacijų operatoriams, kadangi tinklų sujungimui pasinaudojama jau egzistuojančia Interneto infrastruktūra. Antroji - užtikrinama įmonės duomenų apsauga, kadangi VPN technologijos leidžia lanksčiai panaudoti įvairius saugumo mechanizmus.

Pagrindiniai VPN technologijos trūkumai yra palyginti sunkus įdiegimo procesas, kurio priežastys yra gilių žinių apie Interneto technologijas būtinybė, skirtingų programinės ar kompiuterinės įrangos gamintojų produktų nesuderinamumas, bei darbo našumo tinkle sumažėjimas. Todėl šio darbo tikslas yra iširti kelėtos pagrindinių VPN protokolų savybės bei jų panaudojimo galimybes ir palyginti protokolus pagal nustatytus našumo kriterijus.

1. VPN tuneliavimas

1.1. Enkapsuliacija

Tuneliavimas – tai procesas, kuomet vieno kompiuterinio tinklo protokolo paketo informacija yra „pernešama“ kitame pakete. Šis procesas dažnai yra vadinamas enkapsuliacija. Paketų seka tarp dviejų galinių tinklo taškų vadinama tuneliu todėl, kad po to, kai enkapsuliuota informacija yra pašalinama, nutolę taškai tarsi tiesiogiai, be „tarpininkų“ keičiasi informacija vienas su kitu. Tuneliavimo pagalba vienu protokolu galima „pernešti“ kito protokolo paketus, tačiau enkapsuliuoti paketai nebūtinai yra užkoduoti. Enkapsuliacija taip pat prideda maršrutizavimo protokolo informaciją šalia kito tipo informacijos. Tai yra svarbu todėl, kad IP paketas, keliaudamas per eilę Interneto maršrutizatorių, visada turi turėti gavėjo adresą, pagal kuri maršrutizatorius nusprendžia, kaip paketas turi keliauti toliau. VPN atveju, gavėjo adresas paprastai būna iš privačių adresų erdvės, todėl jei pakete nebūtų papildomos maršrutizavimo informacijos, išsiųstas paketas paprasčiausiai nepasiektų gavėjo.

1.2. Tunelio komponentai

Tuneliui sukurti reikalingi trijų tipų protokolai: transporto, pernešimo ir vidinis. Transporto protokolas yra atsakingas už paketo persiuntimą tarp dviejų galinių taškų. Būtent šio protokolo paketai yra matomi abiems komunikuojančioms šalims. Dažniausiai transporto protokolu yra pasirenkamas IP. Pernešimo, arba enkapsuliacijos, protokolas enkapsuliuoja vidinį protokolą ir juo siunčiamą informaciją. Pernešimo protokolas taip pat yra atsakingas už tunelio sukūrimą ir sunaikinimą. Vidinis protokolas yra tas protokolas, kuriuo iš tiesų bendrauja galiniai taškai arba jų aptarnaujami potinkliai. Tai gali būti tiek IP protokolas, tiek bet koks kitas, pavyzdžiui AppleTalk, NetBIOS, IPX/SPX ir pan. Svarbu paminėti, kad kiekviename VPN pakete yra pernešama visų trijų protokolų informacija. Tai yra būtina sąlyga tunelio egzistavimui.

1.3. Tuneliavimo (pernešimo) protokolų sąrašas

Trumpinys	Angliškas pavadinimas	RFC standartas
GRE	Generic Routing Encapsulation	1701/2
PPTP	Point-to-point Tunneling Protocol	2637
L2F	Layer 2 Forwarding	2341
ATMP	Ascend Tunnel Management Protocol	2107
DLSW	Data Link SWitching	1795, 2166
IPSec	Internet Protocol Security	2401, 2402, 2406
Mobile IP tunnel	-	2002

Lentelėje yra pateikti pagrindiniai VPN tuneliavimo protokolai, tačiau šiame darbe daugiau detaliau apžvelgsime ir panagrinėsime tik tris labiausiai paplitusius tuneliavimo protokolus – PPTP, L2TP ir IPSec.

1.4. Tunelių tipai

1.4.1. Laisvieji tuneliai

Laisvieji (angl. voluntary) tuneliai – tai tokie tuneliai, kai už tunelio sukūrimą ir gyvavimą yra visiškai atsakinga tunelį inicijuojanti šalis, paprastai vartotojo kompiuteris. Laisvasis tunelis yra įprastas būdas įmonės darbuotojui iš vieno biuro pasiekti kitą VPN pagalbą. Kaip tik šis tuneliavimo būdas yra akcentuojamas šiame darbe.

1.4.2. Priverstiniai tuneliai

Priverstinis (angl. compulsory) tunelis, priešingai nei laisvasis, nėra sukuriamas vartotojo kompiuterio. Už jo sukūrimą ir gyvavimą yra atsakingas tinklo prieigos serveris NAS (angl. Network Access server), kurį prižiūri vartotojo IPT (Interneto Paslaugų Tiekėjas). Šis tunelio tipas yra patogus tuomet, jei prie įmonės VPN tinklo yra jungiamasi per vieną ir tą patį IPT, kadangi tunelis yra sukuriamas tarp vartotojo IPT ir įmonės biuro, o vartotojas IPT dažniausiai pasiekia modemo ar kitu prieigos būdu.

2. Tuneliavimo protokolai

Šiame skyriuje aptarsime VPN tuneliavimo protokolus, kurie dirba antrajame ir trečiajame OSI modelio sluoksniuose. OSI (angl. Open System Interconnection) modelis – tai daugiasluoksnė struktūra, kuri atspindi tinklo programinės ir techninės įrangos sąveiką darbo seanso metu. OSI modelyje tinklo funkcijos paskirstytos į septynis sluoksnius. Kiekvienam sluoksniui priskirtos tam tikros tinklinės operacijos, įranga ir protokolai.

2.1. Antrojo sluoksnio tuneliavimo protokolai

Antrasis OSI modelio sluoksnis kartais dar vadinamas kanaliniu sluoksniu (angl. Data Link layer). Šiame sluoksnyje suformuojami duomenų kadrai, arba freimai – logiškai organizuota struktūra, kurioje talpinami duomenys ir perduodami iš trečiojo (tinklo) sluoksnio į pirmąjį (fizinį). Būtent freimas yra šio tinklo lygio duomenų apsikeitimo vienetas. Po to, kai šiame lygyje yra sukuriamas VPN tunelis, vartotojui turi būti išskiriamas IP adresas.

2.1.1. PPTP

PPTP (angl. Point-to-Point Tunneling Protocol) – kanalinio lygio protokolas, kaip vienas VPN sprendimų sukurtas PPTP forumo, kurį sudaro kompanijos Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics ir U.S. Robotics. PPTP protokolas dirba panaudodamas kitą plačiai paplitusį protokolą – PPP (angl. Point-to-Point Protocol).

Tradicinė PPTP architektūra yra skirstoma į tris dalis:

- PPP ryšio užmezgimas ir palaikymas
- PPTP kontrolinis susijungimas
- PPTP duomenų tuneliavimas

PPP ryšio užmezgimas ir palaikymas

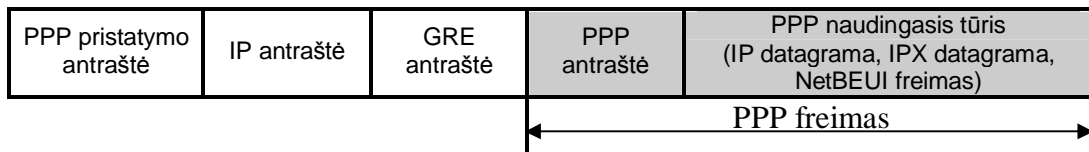
PPTP klientas užmezga ryšį su vartotojo tinklo prieigos serveriu, paprastai naudojantis standartine telefono linija arba ISDN. Šiam susijungimui yra naudojamas PPP protokolas. Šiuo protokolu taip pat yra koduojami duomenys.

PPTP kontrolinis susijungimas

Šiame žingsnyje PPTP uždavinys yra sukurti kontrolinį susijungimą tarp inicijuojančios „namų“ ir nutolusios stoties, dar vadinamos PPTP serveriu. Šis susijungimas atliekamas TCP protokolu, pasinaudojant praeitame žingsnyje sukurtu ryšio kanalu. Šis kontrolinis susijungimas dar vadinamas PPTP tuneliu.

PPTP duomenų tuneliavimas

Po to, kai sukuriamas PPTP tunelis, PPTP protokolas rūpinasi duomenų persiuntimu tarp PPTP kliento ir serverio. Duomenys yra siunčiami IP paketais, taip pat pernešančiais PPP freimais. Pastarieji freimai dažniausiai vadinami kaip enkapsuliuoti PPP paketai. Tuo tarpu PPP paketuose yra pernešami, arba enkapsuliuojami, įvairių protokolų, dažniausiai TCP/IP, IPX ar NetBEUI paketai. PPTP serverio uždavinys yra „išpakuoti“ IP paketą į PPP, atkoduoti pakete pernešamą informaciją ir dekoduoti paketą nukreipti gavėjui. Žemiau yra pateikiama paketo struktūra:



■ - gali būti koduojama

Šis architektūros modelis paprastai taikomas tais atvejais, kai vartotojas prieš sukuriant tunelį, neturi interneto ryšio. Priešingu atveju PPTP tunelio sukūrimui yra nereikalingas tinklo prieigos serveris, todėl architektūra susiaurėja iki dviejų žingsnių. Taip pat PPTP pakete nebelieka PPP pristatymo antraštės (angl. PPP delivery header), kadangi PPTP klientas ir serveris bendrauja TCP/IP protokolu, todėl šiuo atveju PPTP bendrauja trečiojo sluoksnio protokolais. PPTP serveris naudoja 1723 portą, o klientui tunelio sukūrimo metu operacinė sistema išskiria atsitiktinį (paprastai iš intervalo 1024-65535) portą.

Gana menkai dokumentuotas ir architektūroje neatsispindi privačių adresų maršrutizavimo informacijos pernešimas per išorinius adresus. PPTP atveju tam yra naudojamas GRE protokolas, į kurio antraštę (angl. header) yra įrašoma maršrutizavimo informacija, kuri naudojama viso tuneliavimo proceso metu. GRE antraštė taip pat yra naudojama PPP paketo enkapsuliacijai į IP paketą.

PPTP palaiko standartinius saugumo mechanizmus, bet daugiausia yra pasinaudojama esamomis PPP galimybėmis. Vartotojo autorizacijai, paprastai vartotojo vardui ir slaptažodžiui užkoduoti, naudojami EAP (ang. Extensible Authentication Protocol), PAP (Password Authentication Protocol), MSCHAP (Microsoft Challenge Handshake Authentication Protocol) ir keletas kitų protokolų. Persiunčiami duomenys PPTP protokole standartiškai nėra koduojami, tačiau, paprastai klientinėje dalyje naudojant Windows operacinę sistemą, yra galimybė informaciją koduoti MPPE (angl. Microsoft Point to Point Encryption) protokolu.

PPTP protokolas yra populiariausias tarp įmonių, naudojančių Microsoft programinę įrangą, kadangi prie operacinės sistemos yra nemokamai pridodamas PPTP įrankių paketas, leidžiantis palyginti nesudėtingai sukurti VPN.

Pagrindinis PPTP trūkumas – palyginti silpni saugumo mechanizmai. Prieš keletę metų internete buvo pateikta detali analizė apie PPTP autorizacijai naudojamo MSCHAP (pirmoji ir antroji versijos) protokolo spragas – galimybę atkoduoti vartotojo slaptažodį. Pats PPP protokolas, kurį PPTP naudoja duomenų pernešimui, yra optimizuotas griežtam duomenių apsikeitimui tarp dviejų galinių taškų (arba kompiuterių) ir todėl neturi daugumos kitų tinklo protokolų charakteristikų, pavyzdžiui, paketų adresacijos galimybės ir MAC mechanizmo. Kitas šio protokolo trūkumas – PPTP tunelio sukūrimui yra reikalinga, kad tiek klientinė, tiek serverinė dalis palaikytų IP protokolą (kai kurie kiti tuneliavimo protokolai tokio reikalavimo neturi). Taip pat svarbu paminėti, kad šis protokolas vis dar nėra oficialus standartas. Jis dažnai vadinamas „industriniu standartu“, padiktuotu Microsoft kompanijos.

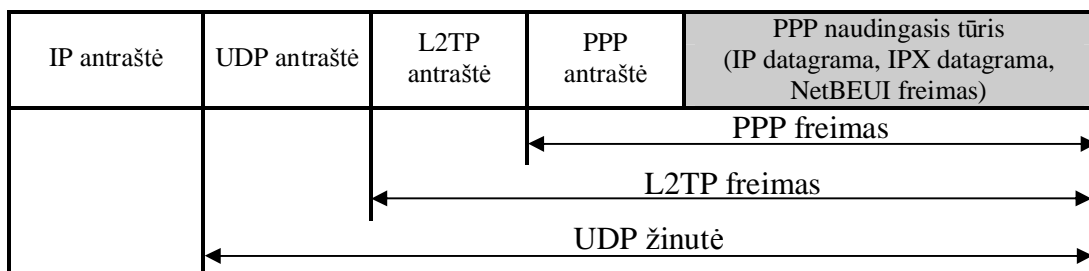
PPTP protokolo dokumentaciją galima rasti RFC 2637.

2.1.2. L2TP

L2TP (angl. Layer 2 Tunneling Protocol) – tai dar vienas antrojo sluoksnio tuneliavimo protokolas, kuris jungia geriausias kitų dviejų tuneliavimo protokolų – tai aukščiau aprašyto PPTP bei L2F savybes.

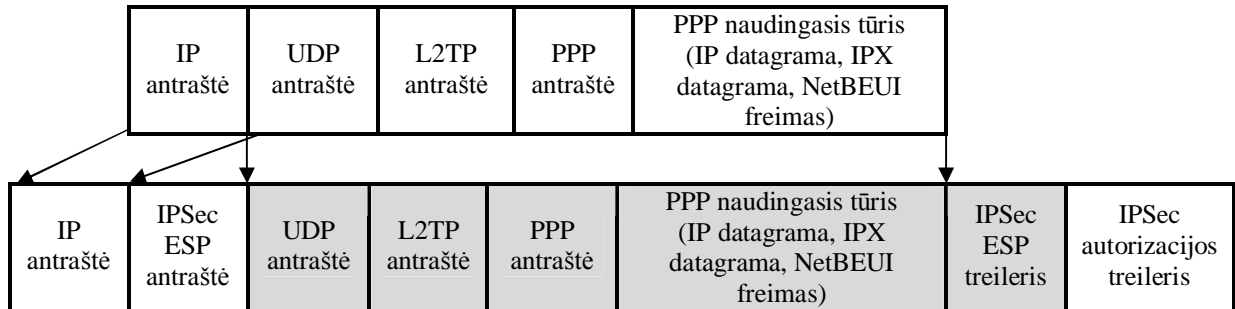
L2TP protokolas, panašiai kaip ir PPTP, enkapsuliuoja PPP freimus į vieną iš šių protokolų: IP, X.25, Frame Relay ar ATM (angl. Asynchronous Transfer Mode). Būtent tuo atveju, jeigu transportavimo protokolu pasirenkamas IP, L2TP veikia kaip tuneliavimo protokolas.

Pastaruoju atveju L2TP naudoja UDP protokolą bei specialią L2TP pranešimų rinkinį tunelio palaikymui. L2TP taip pat naudoja UDP protokolą enkapsuliuotų PPP freimų, kuriais pernešama informacija, išsiuntimui. Naudingasis enkapsuliuotų PPP freimų tūris (angl. payload) gali būti suspaudžiama bei, esant poreikiui, koduojamas. PPTP protokolo paketo struktūra atrodo štai taip:



L2TP, taip pat kaip ir PPTP, palaiko tuos pačius autorizacijos protokolus, o duomenys

standartiškai nėra koduojami, tačiau L2TP protokole yra numatyta galimybė ne tik duomenis (naudingąjį tūrį), bet ir paketų antraštės koduoti IPsec standartu, kuris yra aptartas šiame darbe. Užkoduojama yra visa UDP žinutė. Tokia L2TP paketo struktūra, užkodauta vienu iš dviejų IPsec protokolų ESP atrodo taip:



■ - koduojama IPsec standartu

L2TP protokolo paketų kodavimas IPsec standartu įgalina autorizuoti vartotoją ne tik pagal pateikiamą vartotoją vardą ir slaptažodžį, tačiau ir kompiuteriniu lygmeniu, naudojant IP adresų kontrolę. Pats bendravimas tarp L2TP kliento ir serverio vyksta tik koduotais duomenimis, kadangi prieš užmezgant tunelį yra sukuriamos IPsec apsaugos sąsajos SA (angl. Security Associations). Tam vartotojas taip pat turi pateikti autorizacijos sertifikatą arba dalinį raktą (angl. pre-shared key).

L2TP protokolo dokumentaciją galima rasti RFC 2661.

2.2. Trečiojo sluoksnio protokolai

Trečiasis OSI modelio sluoksnis tikrina adresavimą ir loginius adresus verčia fizinius. Čia nustatomas maršrutas nuo kompiuterio siuntėjo iki kompiuterio gavėjo, sprendžiamos tinklo greitaveikos problemos bei paketų komutavimas. Kompiuteriniuose tinkluose, kurie palaiko IP protokolą, šis sluoksnis dar vadinamas IP sluoksniu. Šiame darbe aptarsime pagrindinį IP sluoksnyje dirbantį tuneliavimo protokolą – IPsec.

2.2.1. IPsec

IPsec (angl. Internet Protocol Security) – tai protokolų rinkinys ir kartu standartas, sukurtas IETF (angl. Internet Engineering Task Force) grupės. Jis yra paremtas galingomis šiuolaikinėmis duomenų kodavimo technologijomis ir suteikia saugumo mechanizmus jau IP lygyje. Tai yra didelis privalumas tinklo vartotojui, kuriam nereikia rūpintis tunelio sukūrimu ar valdymu. IPsec yra visiškai suderinamas su šiuo metu naudojama ketvirtąją IP protokolo versija (IPv4) bei naujosios kartos – šeštąja (IPv6). IPsec pagalba galima kurti saugius VPN tinklus, pasinaudojant esama tinklo infrastruktūra. IPsec pagrindinių protokolų, aptartų šiame darbe, rinkinį sudaro šie protokolai:

- AH

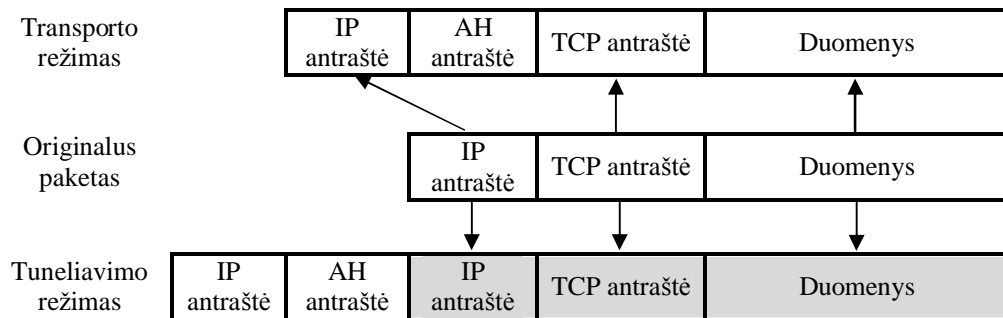
- ESP
- IKE

2.2.1.1. IPSec režimai

IPSec gali dirbti dviem režimais:

- Transporto. Šiame režime yra skaičiuojama paketo kontrolinė suma (AH) arba koduojamas (ESP) tik IP paketo naudingasis tūris į paketą įterpian AH ar ESP antraštę tarp IP ir aukštesniojo lygio protokolo, pavyzdžiui, TCP, antraščių.
- Tunelio. Dirbant šiuo režimu, IP paketas yra pilnai enkapsuliuojamas į naują IP paketą.

AH atveju, kai aukštesniojo lygio protokolas yra TCP, šių režimų paketų struktūra atrodytų taip:



2.2.1.2. Autentiškumo antraštė

AH (angl. Authentication Header) protokolas užtikrina paketų autentiškumą, kadangi prie kiekvieno paketo yra prisegama užkoduota paketo kontrolinė suma (angl. checksum). Jeigu gaunamas AH paketas ir kontrolinės sumos apskaičiavimo operacija buvo sėkminga, tuomet galima tvirtinti, jog abi bendraujančios šalys naudoja slaptą raktą ir tas raktas žinomoms tik toms dviem bendraujančioms šalims. Tai užtikrina, jog paketas buvo išsiųstas būtent iš to siuntėjo, iš kurio turėjo būti atsiųstas bei kad paketas nebuvo kaip nors pakeistas siuntimo metu. AH kontrolinė suma apima ne kurią nors paketo dalį (atskirą protokolą), o visą IP paketą nuo jo antraštės iki pabaigos.

2.2.1.3. Enkapsuliuota saugioji apkrova (ESP)

ESP (angl. Encapsulating Security Payload) suteikia paketams konfidencialumo garantiją, juos užkoduojant pasirinktais kodavimo algoritmais. Jeigu gaunamas ESP paketas ir jį pavyko sėkmingai atkoduoti, tuomet galima tvirtinti, jog paketo jokia trečioji šalis siuntimo metu negalėjo atkoduoti su sąlyga, jog abi bendraujančios šalys dalinasi slaptuoju seanso raktu ir tik jos žino tą raktą.

2.2.1.4. Interneto raktų apsisikeitimas (IKE)

Kaip jau minėta, tiek AH, tiek ESP protokolams reikalingas saugus seanso raktas, kurį žino tik dvi bendraujančios šalys. Butent IKE (angl. Internet Key Exchange) rūpinasi šių raktų generavimo ir saugaus apsisikeitimo mechanizmais. Šis protokolas nėra gyvybiškai svarbus IPsec funkcionavimui, kadangi įmanoma naudoti iš anksto apibrėžtą vieną ir tą patį raktą, tačiau paprastai raktų apsisikeitimu IKE protokolu rūpinasi tam skirti programų rinkiniai, kurie procesą pilnai automatizuoja.

2.2.1.5. Apsaugos sąsajos (SA)

Dviems bendraujančioms šalims norint enkapsuliuoti ir dekapsuliuoti IPsec paketus yra būtina žinoti slaptuosius seanso raktus, kodavimo algoritmus bei IP adresus, kurie dalyvauja bendravime. Visi šie parametrai, reikalingi IP paketų apsaugai, yra saugomi apsaugos sąsajoje SA (angl. Security Association), o pačios apsaugos sąsajos saugomos apsaugos sąsajų duomenų bazėje SAD (angl. Security Association Database). Bet kuri apsaugos sąsaja apibrėžia tokius parametrus:

- Išėities (angl. source) ir įėities (angl. destination) bendraujančių šalių IP adresus ir, jei reikia, jų šablonus (angl. netmask).
- IPsec protokolą (AH arba ESP)
- Kodavimo algoritmą ir saugųjį raktą
- Apsaugos parametrų indeksą SPI (angl. Security Parameter Index). Tai 32 bitų skaičius, kuris identifikuoja konkrečią apsaugos sąsają.
- IPsec režimą (tunelio arba transporto)
- Slankiojančio lango dydį paketų pakartojimo atakoms išvengti
- Apsaugos sąsajos gyvavimo laiką

Kadangi viena apsaugos sąsaja apibrėžia tik viena įėities ir išėities IP adresų ir jų šablonų rinkinių porą, viena taisykle koduojami bus tik išsiunčiami arba gaunami paketai. Todėl norint koduoti tiek išsiunčiamus, tiek gaunamus paketus tarp dviejų bendraujančių šalių, reikalingos mažiausiai dvi apsaugos sąsajos.

Apsaugos sąsaja tik nurodo, kaip IPsec apsaugos duomenų srautą, tačiau reikalinga papildoma informacija, kuri apibrėžtu, kada ir kokį srautą reikia apsaugoti. Ši informacija yra saugoma apsaugos taisyklių rinkinyje SP (angl. Security Policy), kuris kartu su SA saugomas apsaugos sąsajų duomenų bazėje.

3. VPN protokolų našumo tyrimas

Tyrimo buvo nuspręsta patyrinėti šiame darbe jau aptartus VPN tuneliavimo protokolus. Tradicinis VPN tuneliavimo modelis yra štai toks:



Tokiame modelyje tyrimui būtų reikalingi mažiausiai keturi kompiuteriai, tačiau tuomet tyrimo metu būtų neišvengta priklausomybės nuo išorinių renginių – maršrutizatorių ar interneto ryšio spartos. Tam, kad pastarieji veiksniai neturėtų įtakos, tyrimo metu buvo pasinaudota tik dviem kompiuteriais, kurių kiekviename buvo nustatyta po du IP adresus, iš kurių pirmasis atitinka privataus tinklo adresų erdvės adresą, o antrasis – maršrutizatoriaus, arba išorinių adresų erdvės. Taigi, tyrimo metu standartinis VPN modelis buvo supaprastintas, iš jo eliminavus maršrutizatorius bei tarpinę grandį – Internetą.

Tyrimo buvo naudojami du kompiuteriai su tokia konfigūracija:

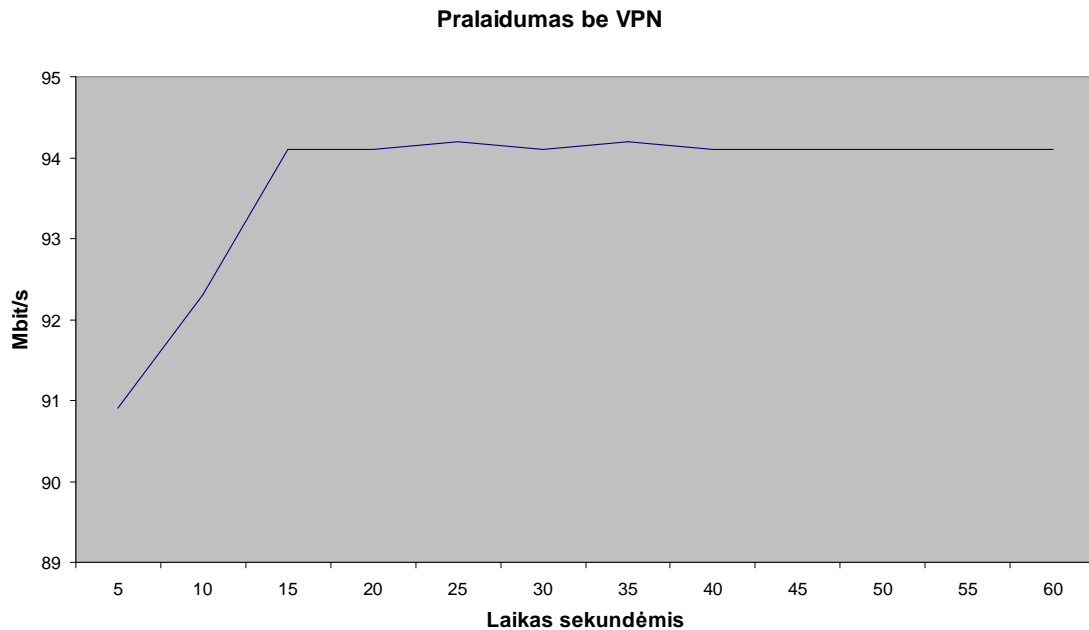
	Pirmasis kompiuteris	Antrasis kompiuteris
Pavadinimas	Test1	Test2
Operacinė sistema	Windows XP Professional	FreeBSD 5.2.1-RELEASE
Privačių adresų erdvė	10.0.1.1/24	10.0.0.1/24
Išorinių adresų erdvė	192.168.0.2/24	192.168.0.1/24
Procesorius	AMD Athlon, 1000 MHz	Intel Centrino, 1400 Mhz
Operatyvioji atmintis	256 MB	256 MB
Ethernet tinkle adapteris	Realtek RTL8139, 100Mbps	RealTek 8139C+, 100Mbps

Interneto ryšio spartai išmatuoti buvo pasirinktas atvirojo kodo paketas Iperf. Jį galima parsisiųsti adresu <http://dast.nlanr.net/Projects/Iperf/>. Iperf – tai įrankis, kurio pagalba galima išmatuoti maksimalų pralaidumą, TCP (arba UDP) protokolu simuliuojant informacijos paketus. Iperf veikia klientas-serveris architektūros principu, t.y. Iperf serveris yra paleidžiamas ant kurio nors vieno iš testuojamų kompiuterių, o Iperf klientas jungiasi į tą serverį ir pasirinktais laiko intervalais pateikia statistinę informaciją, kiek ir kokia sparta per tą intervalą buvo prasiųsta duomenų.

Iperf galima užduoti nemažai parametrų, nuo kurių priklauso testavimo pobūdis. Tyrimo metu buvo pasirinkta matuoti ryšį TCP protokolu – tai yra standartinis protokolas, su kuriuo dirba Iperf. Taip pat buvo užduotas TCP lango dydis (angl. TCP Window size), lygus 64 kilobaitams. Tai buvo padaryta **-w** parametro pagalba. Matavimo trukmė visuose testuose – 60 sekundžių (**-t 60**), o intervalas ataskaitoms – 5 sekundės (**-i 5**).

Visų tyrinėtų protokolų rezultatų lentelę galima rasti pirmajame šio darbo priede.

Visų pirma išmatavome ryšio pralaidumą tarp Test1 ir Test2 nenaudodami jokio VPN protokolo.



Kaip matyti iš grafiko, vidutinis pralaidumas yra 93,7 Mbit/s. Tai beveik atitinka maksimalų pralaidumą, kurį leidžia kompiuterių tinklo adapteriai (100 Mbit/s).

3.1. PPTP našumas

Kadangi PPTP protokolas veikia klientas – serveris ryšio principu, kompiuteris Test1 buvo pasirinktas kaip PPTP klientas, o Test2 – PPTP serveris. Kartu su Windows XP Professional operacine sistema yra pateikiamas patogus PPTP klientas, todėl tyrimo metu jis ir buvo naudojamas. PPTP serveriui buvo pasirinktas atvirojo kodo PPTP serveris Poptop. Ji galima atsisiųsti adresu <http://www.poptop.org>. Poptop serveris yra pilnai suderinamas su Windows šeimos PPTP klientais.

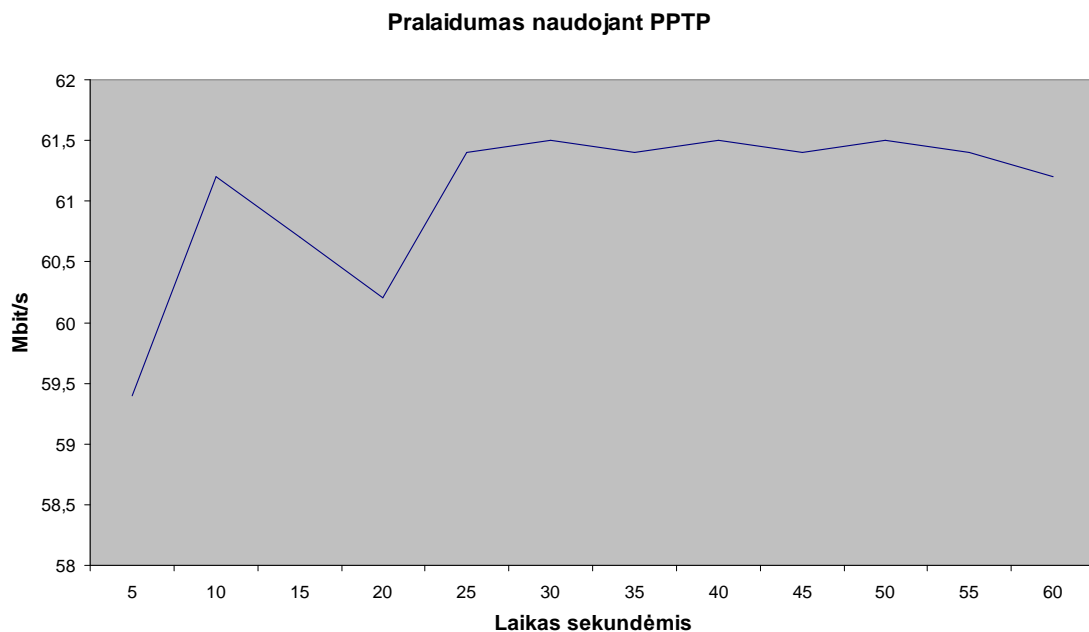
Svarbu paminėti, kad Poptop turi būti sukompiliuotas su vartotojišku PPP (angl. user-ppp) programų rinkiniu, nes sisteminis (pppd) MPPE kodavimo nepalaiko. Taip taip pat buvo reikalinga perkompiliuoti Test2 operacinės sistemos branduolį su papildoma direktyva „device tun“, leidžiančia kurti virtualius tinklo interfeisus.

Pagal nutylėjamą Windows PPTP kliente yra parenkama „Security options: typical“ bei „Require data encryption (disconnect if none)“. Žinoma, direktyvas galima pakeisti, tačiau šiame darbe buvo siekta iširti tuneliavimo protokolus su jų standartiniais nustatymais klientinės dalies atžvilgiu. „Require data encryption“ Windows PPTP kliente reiškia, jog bus naudojamas MPPE kodavimo protokolas, skirtas PPP diagramoms koduoti. Tam tikslui Test2 kompiuterio /etc/ppp/ppp.conf faile prie **pptp** sekcijos teko įrašyti direktyvas **set mppe 128 ***

ir **enable mppe**. Šioje sekcijoje taip pat reikėjo įrašyti direktyvą **set ifaddr 10.0.0.1 10.0.1.1 255.255.255.0**, kuri nurodo, kad prisijungusiam PPTP klientui (Test1) išskirsime 10.0.1.1 IP adresą, kuris pagal pasirinktą modelį ir priklausytų Test1 privačių adresų erdvei.

Tam, kad kompiuteris Test2 iš adreso 10.0.0.1, priklausančio jo privačių adresų erdvei, galētu pasiekti PPTP klientą su adresu 10.0.1.1, operacinei sistemai buvo būtina nurodyti, kad branduolio direktyva **net.inet.ip.forwarding** būtų įjungta. Tai buvo atlikta įvykdant komandą **sysctl -w net.inet.ip.forwarding=1**.

Po sėkmingo PPTP susijungimo, atlikus Ipef testus gauti tokie rezultatai:



Iš grafiko matyti, kad vidutinis pralaidumas yra 61 Mbit/s. Tai reiškia, kad naudodami šį tuneliavimo protokolą, patyrėme maždaug 32 Mbit/s nuostolio, t.y. jie buvo išnaudoti tunelio reikmėms (paketų enkapsuliacijai ir pan.).

3.2. L2TP tyrimas

Šio protokolo klientas taip pat yra platinamas kartu su Windows XP operacine sistema, o serverinei daliai buvo pasirinktas taip pat atvirojo kodo paketas L2TPD (angl. Layer 2 Tunneling Protocol Daemon). Jį galima parsisiųsti adresu <http://www.l2ptd.org/>. IPSec raktų pasikeitimui IKE protokolu naudojome organizacijos KAME, stipriai prisidedančios prie IPSec vystymo ir palaikymo UNIX operacinėse sistemose, programų paketą Racoon, kurį galima atsisiųsti iš <http://www.kame.net/racoon/>.

Windows XP L2TP kliente, kaip ir PPTP atveju, „Security“ sekcijoje standartiškai yra įjungta direktyva „Require data encryption (disconnect if none)“. Tai reiškia, jog persiunčiama informacija bus koduojama IPSec ESP protokolu, tačiau jei L2PT serveris

reikalauja ir AH protokolo, jis taip pat bus naudojamas. L2TP atveju, turi būti naudojamas IPSec transport režimas. Informacijai IPSec protokolais koduoti Windows XP operacinė sistema gali naudoti DES arba 3DES šifravimo algoritmą, o paketo vientisumui užtikrinti – SHA1 arba MD5. Kurie konkrečiai algoritmai bus naudojami, apsprendžia L2TP serveris. IPSec nustatymuose pažymėjome, kad autentiškumui užtikrinti naudosime dalinį raktą (angl. pre-shared key), kadangi standartiškai Windows XP siūlo naudoti apsikeitimą sertifikatais, kuriuos reikėtų susigeneruoti. Kadangi darbo tikslas yra patyrinėti pačius tuneliavimo protokolus, o ne jų saugumo mechanizmus, pasirinkome paprastesnį, dalinių raktų variantą.

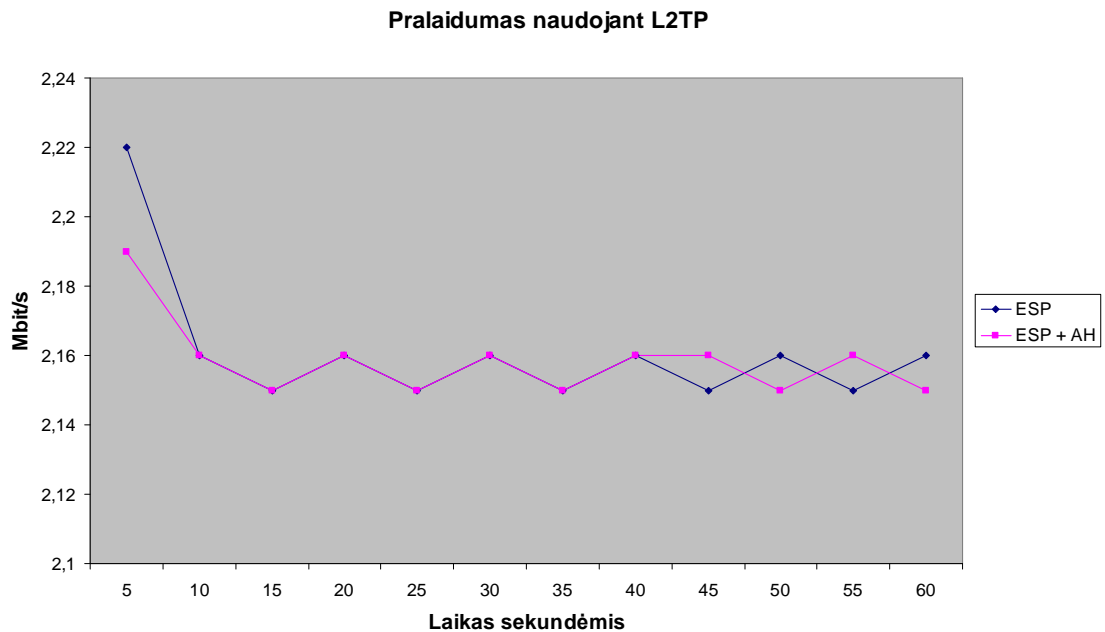
Serverinėje dalyje, panašiai kaip ir L2TP atveju, operacinės sistemos branduolį buvo reikalinga perkompiliuoti su „device ppp“ direktyva, kadangi L2TPD naudoja sisteminį PPP paketą. IPSec kodavimui į /etc/ipsec.conf buvo reikalinga įrašyti tokias apsaugos sąsajas:

```
spdadd 0.0.0.0/0 192.168.0.1/32[1701] any -P in ipsec
        esp/transport/192.168.0.2-192.168.0.1/require
        ah/transport/192.168.0.2 192.168.0.1/require;
spdadd 192.168.0.1/32[1701] 0.0.0.0/0 any -P out ipsec
        esp/transport/192.168.0.1-192.168.0.2/require
        eh/transport/192.168.0.1-192.168.0.2/require;
```

Šios taisyklės reiškia, kad IP paketai, kurių siuntėjas yra bet koks IP adresas, o gavėjas - 192.168.0.1 su 1701 portu, turi būti užkoduojami pirma ESP, o po to AH protokolu, o IPSec režimas yra transporto. Taisyklės užkraunamos komanda **setkey -f /etc/ipsec.conf**. Informacijos kodavimui buvo pasirinktas 3DES, o vientisumui – SHA1 algoritmas. Tam tikslui Racoon programos konfigūraciniame faile /usr/local/etc/racoon/racoon.conf **remote** sekcijoje direktyvai **encryption_algorithm** priskyrėme reikšmę reikšmę **3des**, o **authentication_algorithm** - **hmac_sha1**.

Windows XP L2TP klientas taip pat reikalauja, kad būtų naudojama vartotojo autorizacija vienu iš autorizacijos protokolų, todėl šiam tikslui mes pasirinkome CHAP protokolą ir į /etc/ppp/options failą įrašėme direktyvą **require-chap**, o /etc/ppp/chap-secrets faile nurodėme vartotojo vardą ir slaptažodį, kuriuo jungsis L2TP klientas.

Tirdami L2TP našumą, atlikome du testus – naudojant tik ESP protokolą ir naudojant ESP kartu su AH. Pirmuoju atveju iš apsaugos sąsajų taisyklių reikėjo tiesiog išmesti AH protokolo reikalavimą. Gauti tokie rezultatai:



Iš grafiko matyti, kad naudojant tik ESP ir ESP kartu su AH, pralaidumas yra panašus – vidutiniškai apie 2.15 Mbit/s. Kaip rodo tyrimo rezultatai, L2TP, duomenis koduojant IPSec protokolais, naudojimas duomenų pralaidumą sumažino daugiau nei 40 kartų.

3.3. IPSec tyrimas

Atlikti IPSec našumo tyrimą buvo viena iš sudėtingiausių darbo dalių, visų pirma dėl to, kad Windows XP operacinėje sistemoje nėra patogaus kliento interfeiso, leidžiančio atlikti IPSec susijungimą turbūt dėl tos priežasties, kad darbe jau tyrinėtą L2TP protokolą yra siuloma naudoti tik kartu su IPSec. Kita vertus, IPSec susijungimo negalima priskirti klientas – serveris architektūrai, nes abi susijungime dalyvaujančios šalys yra „lygiavertės“.

Tam, kad sukurti IPSec tunelį, buvo reikalinga tiek Test1, tiek Test2 kompiuteriuose sukurti atitinkamas IPSec apsaugos sąsajų taisykles. Test2 kompiuteryje tai buvo atlikta tokiu pačiu principu, kaip ir L2TP atveju, o Test1 kompiuteryje teko pasinaudoti valdymo konsole (MMC – angl. Microsoft Management Console), kuri iškviečiama komanda **mmc.exe**. Konsolėje yra reikalinga pridėti IPSec taisyklių valdymo komponentą (angl. snap-in) ir jame sukurti naują IPSec apsaugos taisyklę. Serverinėje dalyje raktų apsikeitimui, kaip ir L2TP atveju, buvo naudojamas Racoon programų paketas.

3.3.1. Tunelio režimas

Kadangi darbe tyrinėjame VPN tuneliavimo protokolus, šis IPSec režimas mums yra svarbiausias būtent dėl tos priežasties, kad naudojant šį režimą galima pernešti privačios erdvės adresus per išorinius, kadangi naudojant tiek ESP, tiek AH protokolus tunelio režime kiekvienam paketui yra sukuriama nauja IP antraštė.

Naudojant IPSec tunelius, priešingai nei PPTP ar L2TP, dinamiškai IP adresai išskiriami nėra. Tai sąlygoja pati IPSec architektūra, kuri, naudojant tuneliavimo režimą, yra skirta dviem privatiems tinklams sujungti paketus pernešant per tarp išorinių (maršrutizatorių) adresų susikurtą tunelį. Būtent dėl šios priežasties, tiek Test1, tiek Test2 kompiuteriai buvo sukonfigūruoti su IP adresais iš privačios IP adresų erdvės. Kadangi kiekvienas iš kompiuterių dabar turi po du IP adresus kiekvienam tinklo adapteriui, buvo reikalinga sukurti maršrutizavimo taisykles, kurios leistų IP adresui iš privačios erdvės pasiekti kitą privačią adresų erdvę. Paprastai tuo pasirūpina maršrutizatorius, tačiau mūsų atveju Test1 kompiuteryje įvykdėme komandą **route add 10.0.0.0 mask 255.255.255.0 10.0.1.1**, o Test2 – **route add 10.0.1.1 netmask 255.255.255.0 10.0.0.1**. Šios maršrutizavimo taisyklės iš principo nėra visiškai taisyklingos, kadangi jose nurodoma, kad tam tikra adresų erdvė bus pasiekama per vieną iš tinklo adapterio adresų. Tačiau šių taisyklių pakanka, kad potinkliai **10.0.1.1/24** ir **10.0.0.1/24** galėtų bendrauti.

Atskirai buvo testuojami IPSec ESP, AH protokolai bei jų kombinacija, tačiau kaip tik su pastaruoju variantu iškilo keblumų. Jei IPSec tunelio režime ESP yra naudojamas kartu su AH, tuomet visų pirma ESP protokolas turėtų užkoduoti visą IP paketą bei sukurti naująją IP antraštę, o AH – suskaičiuoti jau pakete esančio ESP protokolo kontrolinę sumą ir įterpti savo antraštę tarp išorinės IP ir ESP antraščių. Tyrimo metu paaiškėjo, kad Windows XP ir FreeBSD šiuo atveju elgiasi visiškai skirtingai. Windows XP operacinė sistema siųsdavo tokios struktūros paketą:

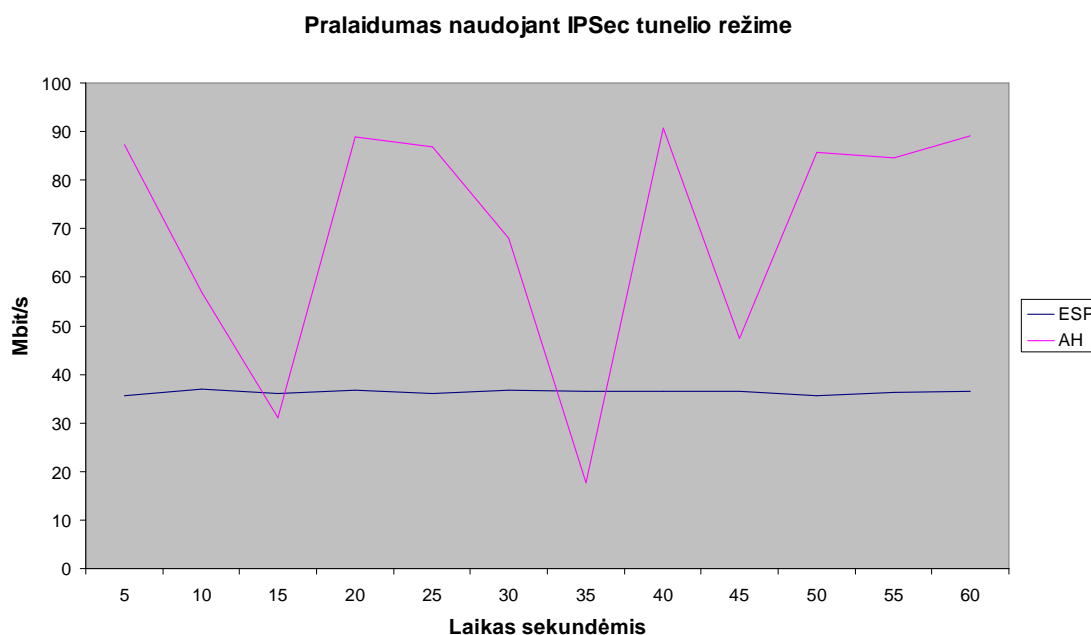
IP antraštė	AH antraštė	ESP antraštė ir duomenys
-------------	-------------	--------------------------

O FreeBSD atveju paketas atrodė štai taip:

IP antraštė	AH antraštė	IP antraštė	ESP antraštė ir duomenys
-------------	-------------	-------------	--------------------------

Pabandžius išsiaiškinti tokio skirtumo priežastį paaiškėjo, kad problema yra dabartinėje FreeBSD operacinės sistemos IPSec realizacijoje. Jei AH yra naudojamas tunelio režime, tai yra tikrinamas paketo autentiškumas imant išorinę IP antraštę, bet ne jau su ESP enkapsuliuotą vidinę. Problema turėtų būti išspręsta tuomet, kai IPSec realizacija leis sekti visą paketo dekapuliacijos seką.

Dėl pastarosios priežasties testai buvo atlikti naudojant ESP ir AH protokolus tik atskirai, bet ne abu kartu. Gauti tokie rezultatai:



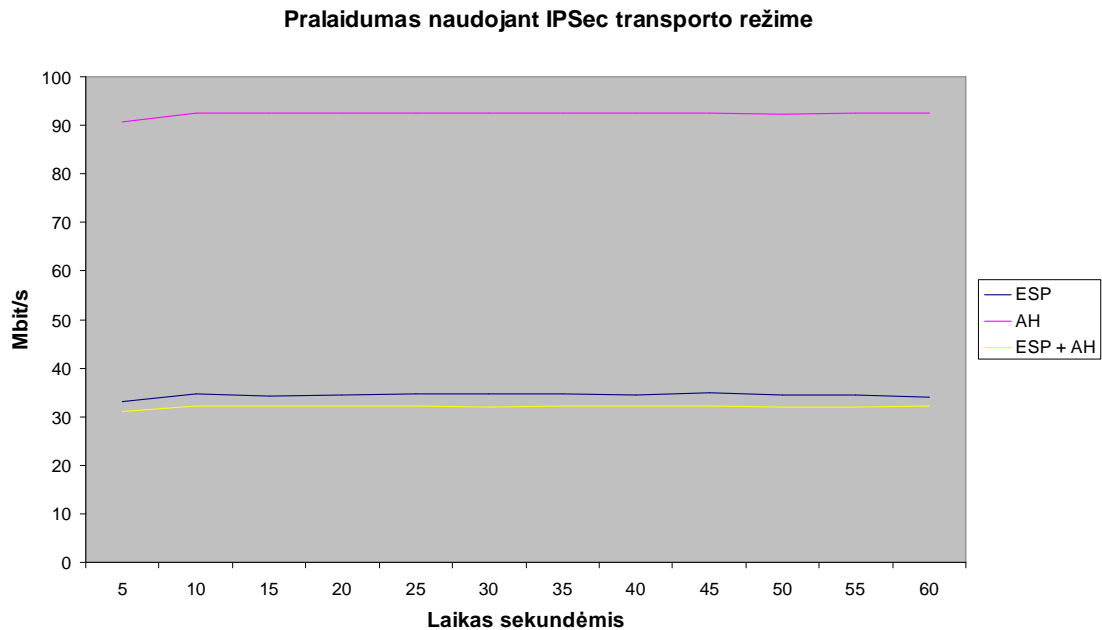
Iš grafiko matyti, kad yra nemaži svyravimai naudojant AH protokolą. To priežastis taip pat galėtų būti IPSec realizacijos FreeBSD operacinėje sistemoje problemos. Tačiau naudojant ESP, vidutinis pralaidumas yra 36,35 Mbit/s, t.y. našumas sumažėja maždaug 61%, lyginant su pradiniu (be VPN). Kita vertus, naudojant IPSec tunelio režimą, kaip ir L2TP atveju, galime virtualiai sujungti du privačius tinklus. Tačiau, kaip rodo tyrimo rezultatai, lyginat L2TP su IPSec ir šį tuneliavimo variantą (imant tik ESP protokolo naudojimą), pastarasis yra net 16 kartų spartesnis.

3.3.2. Transporto režimas

Kaip jau minėta, transporto režimas yra skirtas tik ryšiui tarp dviejų taškų apsaugoti, kadangi naudojant tiek ESP, tiek AH ar abu kartu, originali IP paketo antraštė išlieka nepakitusi. Išmatuoti šio režimo našumą buvo įdomu todėl, kad šiame darbe jau aptartas L2TP protokolas irgi naudoja IPSec transporto režimą duomenims apsaugoti. Taigi, ištyrę sužinosime, kiek našumo yra prarandama grynai L2TP tuneliavimo reikmėms, atmetant IPSec kodavimo kaštus.

Tyrimo metu abiejuose kompiuteriuose buvo naudojami tik išorinės erdvės adresai, kadangi kaip jau minėta, transporto režimas yra skirtas ryšiui tarp dviejų taškų, paprastai su išoriniais IP adresais, apsaugoti. Abiejų kompiuterių IPSec saugumo sąsajų taisyklės buvo pakoreguotos taip, kad IPSec būtų naudojamas tik tuo atveju, jei gavėjas yra 192.168.0.1 ar Test1 kompiuteryje ir 192.168.0.2 Test2 kompiuteryje. Algoritmai informacijai užkoduoti ir jos vientisumui užtikrinti buvo pasirinkti tokie patys, kaip ir kituose tyrimuose – 3DES ir

SHA1. Atlikus Iperf testus visais trim galimais atvejais (ESP, AH, ESP ir AH kartu), gauti tokie rezultatai:



Kaip matyti iš grafiko, šiame režime naudojant tik AH protokolą, našumas sumažėja labai nežymiai. Taip yra todėl, kad AH protokolas yra skirtas tik duomenų autentiškumui užtikrinti. Tuo tarpu tinklo našumas naudojant tik ESP protokolą yra labai panašus, kaip ir tunelio režimo atveju. Dabar jau galime patvirtinti, kad L2TP protokolas tinklo našumą sumažina net 32 Mbit/s, kadangi, kaip rodo tyrimas, IPSec transporto režime su ESP gavome 34,38 Mbit/s tinklo našumą.

Išvados

Šiame darbe aptarėme pagrindinius VPN tuneliavimo protokolus, bei ištyrėme, kiek daug vieno ar kito protokolo naudojimas įtakoja duomenų pralaidumą. Iš gautų tyrimo rezultatų negalima spėti apie bendrą vieno ar kito tuneliavimo protokolo našumą, tačiau kadangi tyrimo metu visais atvejais buvo naudojama ta pati kompiuterinė ir tinklo įranga, galėjome palyginti, kaip skiriasi duomenų transportavimo kaštai naudojant skirtingus tuneliavimo protokolus.

Tyrimo metu buvo susidurta su tam tikrais sunkumais siekiant sukurti VPN tunelius skirtingose operacinėse sistemose – Windows XP Professional ir FreeBSD, todėl svarbiausi konfiguracioniai aspektai šiame darbe taip pat yra paminėti.

Pirmiesiems dviems nagrinėtiems tuneliams – PPTP ir L2TP serverinėje dalyje buvo naudojami tam skirti programų paketai, o IPSec atveju beveik viskuo pasirūpino pati operacinė sistema. Tik raktų apsikeitimui IKE protokolu serverinėje dalyje buvo panaudota specialus programų paketas, nors tam tikrais atvejais jo galima atsisakyti. IPSec standartas šiuo metu yra palaikomas ne tik populiariose operacinėse sistemose, bet ir daugelyje aparatūrinių maršrutizavimo įrenginių, gaminamų tokių stambių kompanijų, kaip Cisco, Zyxel, D-Link ir pan. Tai, jog IPSec palaiko vis daugiau operacinių sistemų ir aparatūrinių įrenginių, rodo šio standarto efektyvų panaudojimą tiek duomenų apsaugai, tiek VPN tuneliavimui. PPTP protokolas, galima sakyti, yra nebevystomas, kadangi kaip jau minėta darbe, visos jo geriausios savybės yra naudojamos L2TP protokole. Deja, abiejų pastarųjų protokolų vystymuisi daugiausia įtakos turi kompanija Microsoft, todėl šių protokolų palaikymas kitose operacinėse sistemose ar aparatūriniuose maršrutizatoriuose tampa labiau komplikotas.

Privalu pastebėti, kad tiek naudojant kitokią nei tyrime kompiuterinę ar tinklo įranga, tiek kitas operacines sistemas, tyrimo rezultatai greičiausia būtų buvę skirtingi. Vienintelis universalus būdas VPN protokolų našumui padidinti galėtų būti aparatūrinių šifravimo įrenginių naudojimas. Tokie įrenginiai dažnai naudojami aparatūriniuose maršrutizatoriuose, tačiau gali būti naudojami ir personaliniuose kompiuteriuose kaip atskiras įrenginys. Vienintelis reikalavimas, kad tokį įrenginį palaikytų operacinė sistema.

Literatūros saraksts

- [Mic99] Microsoft Corporation. Virtual Private Networking in Windows 2000: An Overview. URL:
<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp>, 192 KB, 2001 09 04
- [Alc01] Alcatel. Understanding the IPSec Protocol Suite.
URL: http://vpn.shmoo.com/vpn/ipsec_nn.pdf. 697 KB, 2001, 54 pages.
- [Lav02] Dru Lavigne. VPNs and IPSec Demystified.
URL: http://www.onlamp.com/pub/a/bsd/2002/12/12/FreeBSD_Basics.html. 2002 12 12.
- [Cla02] Nik Clayton. VPN over Ipsec.
URL: http://www.freebsd.org/doc/en_US.ISO88591/books/handbook/ipsec.html.
- [Mas02] Andrew Mason. IPSec Overview Part One: General IPSec Standards
URL: <http://www.ciscopress.com/articles/printerfriendly.asp?p=25470>. 11 KB, 2002 02 22.
- [Vpn04] VPN Consortium. VPN technologies: Definitions and Requirements.
URL: <http://www.vpnc.org/vpn-technologies.html>, 13,7 KB, 2004 01.

Priedas Nr. 1.

VPN protokolų tyrimo rezultatų lentelė

Laikas (sekundėmis)	Be VPN	PPTP	L2TP, ESP	L2TP, ESP+AH	IPSec, tunnel, ESP	IPSec, tunnel, AH	IPSec, transport, ESP	IPSec, transport, AH	IPSec, transport, ESP+AH
5	90,9	59,4	2,22	2,19	35,7	87,2	33,1	90,6	31
10	92,3	61,2	2,16	2,16	36,9	56,9	34,6	92,6	32,1
15	94,1	60,7	2,15	2,15	36,1	31	34,3	92,5	32,2
20	94,1	60,2	2,16	2,16	36,7	88,9	34,4	92,6	32,2
25	94,2	61,4	2,15	2,15	36,1	86,9	34,6	92,6	32,1
30	94,1	61,5	2,16	2,16	36,8	68,1	34,7	92,6	32
35	94,2	61,4	2,15	2,15	36,4	17,6	34,6	92,5	32,2
40	94,1	61,5	2,16	2,16	36,6	90,8	34,4	92,5	32,2
45	94,1	61,4	2,15	2,16	36,6	47,5	34,9	92,5	32,2
50	94,1	61,5	2,16	2,15	35,6	85,8	34,5	92,4	32
55	94,1	61,4	2,15	2,16	36,3	84,5	34,4	92,5	32
60	94,1	61,2	2,16	2,15	36,4	89,2	34,1	92,6	32,2
Vidurkis, Mbit/s	93,7	61,0666667	2,160833333	2,158333333	36,35	69,53333333	34,38333333	92,375	32,03333333