

**ANALISA PERBANDINGAN KINERJA VPN PPTP, PROXY, DAN SSH
TUNNEL MENGGUNAKAN VIRTUAL PRIVATE SERVER
(Studi kasus : ISP Cobralink Minomartani)**

SKRIPSI



disusun oleh

Ery Rizal Hidayat

12.11.6151

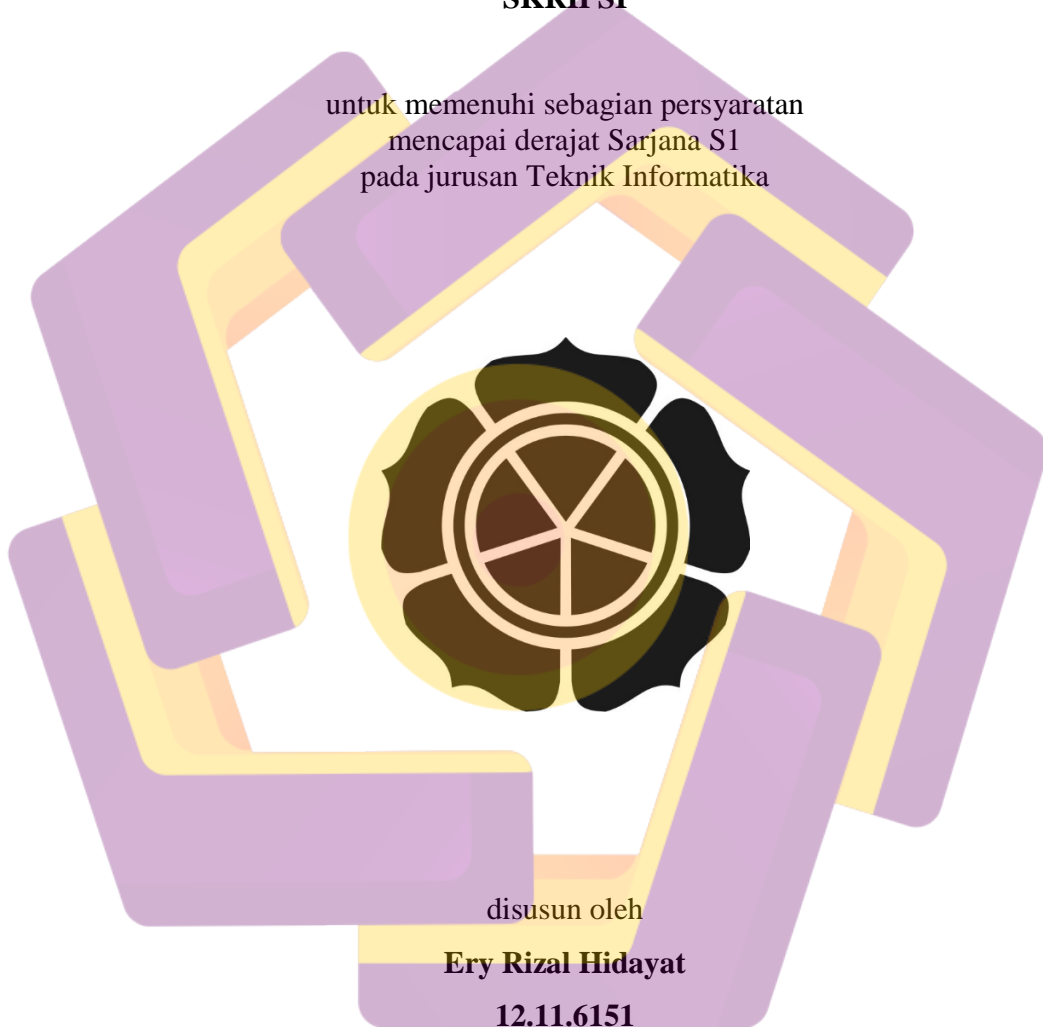
**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**ANALISA PERBANDINGAN KINERJA VPN PPTP, PROXY, DAN SSH
TUNNEL MENGGUNAKAN VIRTUAL PRIVATE SERVER**

(Studi kasus : ISP Cobralink Minomartani)

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Ery Rizal Hidayat

12.11.6151

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

**ANALISA PERBANDINGAN KINERJA VPN PPTP, PROXY, DAN SSH
TUNNEL MENGGUNAKAN VIRTUAL PRIVATE SERVER**

(Studi kasus :ISP Cobralink Minomartani)

Yang dipersiapkan dan disusun oleh

Ery Rizal Hidayat

12.11.6151

Telah disetujui oleh Dosen Pembimbing skripsi

Pada tanggal 22 April 2015

Dosen Pembimbing,

Emha Taufiq Luthfi, S.T.,M.Kom.

NIK. 190302125

PENGESAHAN

SKRIPSI

**ANALISA PERBANDINGAN KINERJA VPN PPTP, PROXY, DAN SSH
TUNNEL MENGGUNAKAN VIRTUAL PRIVATE SERVER**

Studi Kasus : ISP Cobralink Minomartani

yang disusun oleh
Ery Rizal Hidayat

12.11.6151

telah dipertahankan di depan Dewan Penguji
Pada tanggal 22 Februari 2016

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105



Hartatik, ST, M.Cs
NIK. 190302232



Emha Taufiq Luthfi, ST, M.Kom
NIK. 190302125



Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 08 Maret 2016



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 8 Maret 2016

Ery Rizal Hidayat
12.11.6151

MOTTO

"Be who you are dont compare your self to others"

(Onizuka GTO)

"Humans cannot gain anything without presenting something of equal value"

(Alphose Elric, FMA)

"If i don't have to do it, i won't. If i Have to do it, i wll make it quick"

(OrekiHotarou, Hyoka)



PERSEMBAHAN

Puji syukur kehadiran Allah SWT, karena berkat rahmat dan ridho-Nya penulis dapat menyelesaikan Skripsi ini

Skripsi ini saya persembahkan untuk:

Ayah Marsum raharjo dan Ibu Sri Murni

Terimakasih atas dukungan, motivasi, kerja keras, kasih sayang, kepercayaan, dan do'a yang sudah diberikan. Saya merasa sangat bersyukur sudah memiliki Orang tua seperti kalian. Adik dan saudara yang telah membantu mendo'akan saya.

Emha Taufiq Luthfi

Terimakasih banyak atas arahan, bimbingan, saran dan waktu yang sudah diberikan sehingga saya dapat menyelesaikan Skripsi saya dengan maksimal.

Teman - teman

Terimakasih untuk teman – teman 12-SITI-06 dan para sahabat yang tidak bisa saya sebutkan namanya satu persatu, terimakasih telah memberikan dukungan sampai selesainya Skripsi ini.

STMIK AMIKOM Yogyakarta

Terimakasih untuk semua ilmu pengetahuan yang sudah diberikan selama masa kuliah, semoga lebih bermanfaat, dan Amikom menjadi lebih baik serta sukses.

KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan nikmat iman, islam dan kesehatan sehingga penulis dapat menyelesaikan skripsi ini tanpa kendala apapun. Tidak lupa sholawat serta salam penulis haturkan pada junjungan umat yaitu Nabi Muhammad SAW, yang telah membawa umatnya dari jaman kegelapan kepada jaman yang terang yaitu jalan yang di ridhai oleh Allah SWT.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. Selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Emha Taufiq Luthfi, ST, M.Kom selaku dosen pembimbing.
3. Ayahhanda Marsum Raharjo & Ibunda Sri Murni serta kaka dan adik saya Mbak Eka & Esi yang selalu memberikan do'a dan dukungan kepada saya.
4. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama perkuliahan.
5. Dan juga tidak lupa teman-teman seperjuangan dan para sahabat yang membantu kelancaran penulisan laporan skripsi

Yogyakarta, 8 Maret 2016

Penulis

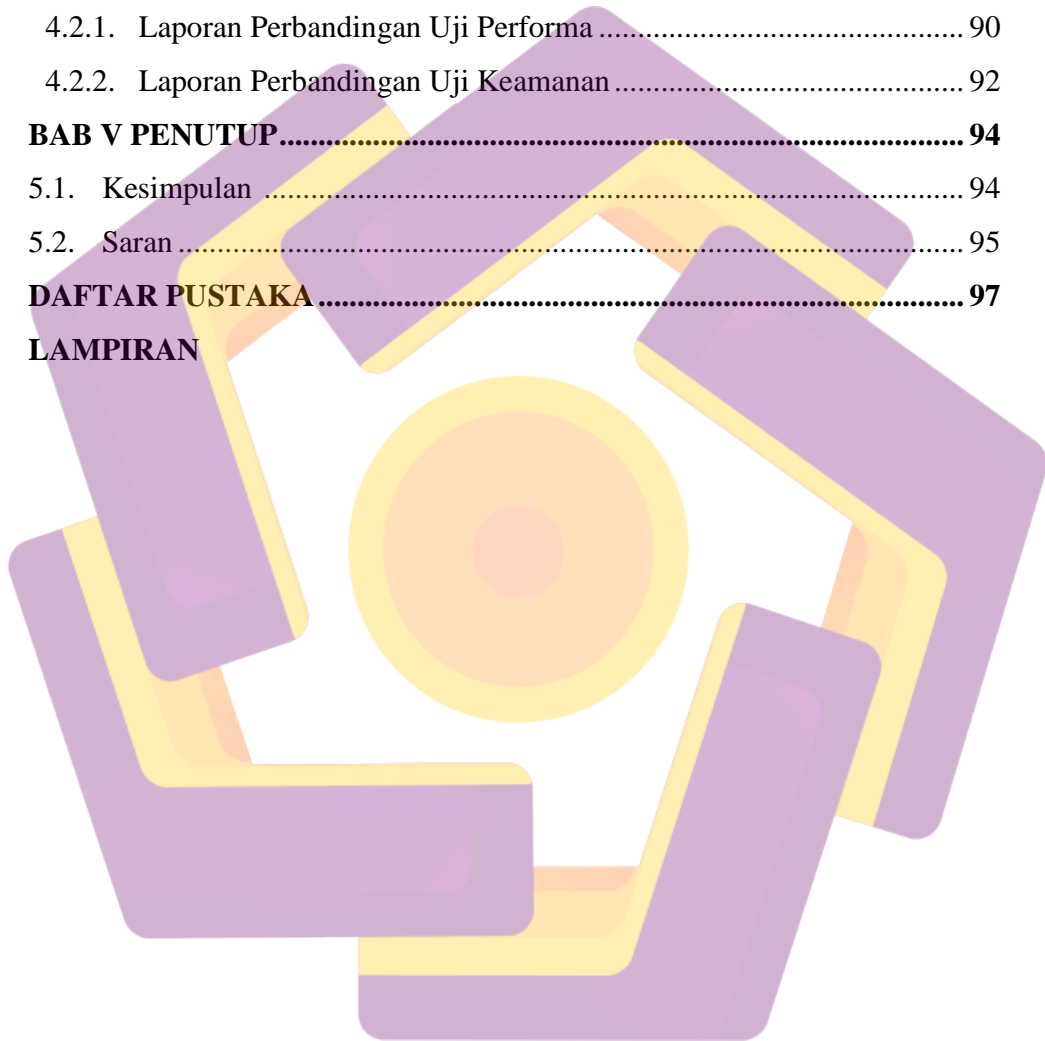
DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN.....	ih
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Masalah	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah	2
1.4. Tujuan Penelitian	3
1.5. Manfaat penelitian	4
1.6. Metode Penelitian	4
1.7. Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1. Tinjauan Pustaka.....	7
2.2. Virtual Private Network.....	8
2.2.1 Jenis – jenis VPN	8
2.2.1.1 <i>Remote Acces</i> VPN.....	9
2.2.1.2 <i>Site do Site</i> VPN	10

2.2.2 Fungsi Utama VPN.....	11
2.2.2.1 <i>Confidentiality</i>	11
2.2.2.2 <i>Data Integrity</i>	11
2.2.2.3 <i>Origin Authentication</i>	12
2.2.3 Teknologi VPN.....	12
2.2.3.1 Teknologi Tunneling.....	12
2.2.3.2 Teknologi Enkripsi.....	13
2.3 <i>Point to Point Tunneling Protocol</i>	14
2.3.1 Arsitektur PPTP.....	15
2.3.2 Cara kerja Protokol PPTP.....	16
2.4 Proxy.....	21
2.4.1 Cara kerja Proxy.....	22
2.4.1.1 Firewall.....	22
2.4.1.2 Pendekatan Layer OSI.....	23
2.4.1.3 <i>Chaching</i>	25
2.4.2 Jenis –jenis Proxy.....	26
2.4.2.1 <i>Transparant proxy</i>	26
2.4.2.2 <i>Anonymous proxy</i>	27
2.5 SSH Tunnel.....	29
2.5.1 <i>Port forwarding</i>	30
2.5.2 Konsep SSH Tunneling.....	30
2.6 Aplikasi yang digunakan.....	34
2.6.1 Bitwise SSH Client.....	34
2.6.2 Wireshark.....	34
2.6.3 Ettercap.....	36
2.6.4 CURL.....	36
BAB III PERANCANGAN SISTEM	37
3.1. Gambaran Umum.....	37
3.2. Metode Penelitian.....	37

3.3. Objek Penelitian.....	38
3.4. Analisis Sistem	39
3.4.1. Analisis Kondisi Lingkungan.....	39
3.4.1.1 Analisis Kondisi Lingkungan Fisik	39
3.4.1.2 Analisis Kondisi Lingkungan nun Fisik	40
3.4.2. Analisis keamanan WAN yang Digunakan	40
3.4.3. Analisis Kelemahan Sistem	41
3.4.4 Solusi Terhadap Masalah.....	41
3.5. Analisis Topologi Jaringan	41
3.6. Analisis Kebutuhan.....	42
3.6.1. Analisis Kebutuhan Perangkat Keras	42
3.6.2. Analisis Kebutuhan Sumber Daya Manusia.....	46
3.7. Analisis kelayakan	46
3.7.1 Kelayakan Hukum.....	46
3.7.2 Kelayakan teknologi.....	46
3.8 Simulasi Pengujian.....	47
3.8.1 Simulasi Uji Performa.....	47
3.8.2 Simulasi Uji Keamanan.....	48
BAB IV IMPLEMENTASI DAN PEMBAHASAN	50
4.1. Proses Pengujian Performa dan Keamanan	50
4.1.1. Instalasi Dan Konfigurasi Server	50
4.1.1.1. Instalasi Dan Konfigurasi VPN PPTPD.....	50
4.1.1.2. Instalasi Dan Konfigurasi Squid Proxy Server	52
4.1.1.3. Instalasi Dan Konfigurasi OpenSSH.....	58
4.1.2. Pengujian Performa.....	59
4.1.2.1. Analisa Pengukuran dengan data berupa Gambar.....	60
4.1.2.2. Analisa Pengukuran dengan data berupa Suara	63
4.1.3. Pengujian keamanan	66
4.1.3.1.Pengujian Keamanan Pada ISP Cobralink	67

4.1.3.2.Pengujian Keamanan Pada VPN PPTP	76
4.1.3.3.Pengujian Keamanan Pada Proxy <i>Anonymous</i>	82
4.1.3.4.Pengujian Keamanan Pada SSH Tunnel	85
4.2. Laporan Perbandingan	90
4.2.1. Laporan Perbandingan Uji Performa	90
4.2.2. Laporan Perbandingan Uji Keamanan	92
BAB V PENUTUP	94
5.1. Kesimpulan	94
5.2. Saran	95
DAFTAR PUSTAKA	97
LAMPIRAN	



DAFTAR TABEL

Tabel 3.1. Jaringan WAN pada ISP Cobralink Minomartani	40
Tabel 3.2. Spesifikasi Antena Grid TJD-2400	42
Tabel 3.3. Spesifikasi UBIQUITI Bullet2 Outdoor Wireless	42
Tabel 3.4. Spesifikasi Swith / HUB	43
Tabel 3.5. Spesifikasi Virtual Private Server (VPS)	43
Tabel 3.6. Spesifikasi Personal Computer (PC) / Notebook 1	44
Tabel 3.7. Spesifikasi Personal Computer (PC) / Notebook 2	42
Tabel 4.1. Data Throughput File Gambar	60
Tabel 4.2. Waktu Transfer File Suara	62
Tabel 4.3. Data Throughput File Suara	63
Tabel 4.4. Waktu Transfer File Suara	65
Tabel 4.5. IP dan MAC Target	70
Tabel 4.6. IP dan MAC Target	76
Tabel 4.7. Tabel Perbandingan Rata-rata Throughput	90
Tabel 4.8. Tabel Perbandingan Rata-rata Transfer Time	90
Tabel 4.7. Laporan Hasil Pengujian Penyerangan	92

DAFTAR GAMBAR

Gambar 2.1	<i>Virtual Private Network</i>	8
Gambar 2.2	<i>Remote Access VPN</i>	9
Gambar 2.3	<i>Site to site VPN</i>	10
Gambar 2.4	Arsitektur PPTP	16
Gambar 2.5	Proses PPTP	17
Gambar 2.6	Pengirim paket PPTP	18
Gambar 2.7	Penerima paket PPTP	20
Gambar 2.8	Proxy Server	21
Gambar 2.9	Proses Chaching Proxy	26
Gambar 2.10	Proses Transparat proxy	27
Gambar 2.11	Konsep SSH Tunneling	31
Gambar 2.12	<i>Local forwarding</i> dan <i>remote forwarding</i> SSH	32
Gambar 2.13	<i>Local port forwarding</i> SSH tunnel	33
Gambar 2.14	<i>Remote port forwarding</i> SSH tunnel	33
Gambar 2.15	Tampilan Awal Wireshark	36
Gambar 3.1	Denah Lokasi BTS Cobralink dan Pengujian	39
Gambar 3.2	Jaringan WAN yang digunakan penguji	40
Gambar 3.3	Topologi Jaringan	41
Gambar 4.1	Konfigurasi Port OpenSSH	58
Gambar 4.2	Pengambilan Nilai <i>throughput</i>	59
Gambar 4.3	Pengambilan Nilai <i>Transfer time</i>	59
Gambar 4.4	Diagram Data Throughput File Gambar	61
Gambar 4.5	Diagram Perbandingan <i>Transfer Time</i> File Gambar	63
Gambar 4.6	Diagram data throughput file Suara	65
Gambar 4.7	Diagram Perbandingan <i>Transfer Time</i> File Suara	66
Gambar 4.8	List paket IP target yang ditangkap pada ISP Cobralink	68

Gambar 4.9 Paket filter http pada ISP Cobralink.....	69
Gambar 4.10 Pilih interface ettercap.....	71
Gambar 4.11 Ettercap Host list ISP Cobralink	72
Gambar 4.12 Pemilihan Target ARP <i>Spoofing</i>	73
Gambar 4.13 Kotak dialog Sniff ARP poisoning.....	73
Gambar 4.14 Gagal login ISP cobralink	74
Gambar 4.15 Hasil ARP <i>Spoofing</i> ISP Cobralink	75
Gambar 4.16 List paket http saat menggunakan MITM	75
Gambar 4.17 Hasil ARP <i>Spoofing</i> ISP Cobralink	75
Gambar 4.18 list Paket pada IP target menggunakan VPN PPTP	77
Gambar 4.19 Analisa Paket PPP gagal	78
Gambar 4.20 Pilih interface ettercap.....	79
Gambar 4.21 Ettercap Host list pada Router.....	80
Gambar 4.22 Kotak dialog Sniff ARP poisoning.....	81
Gambar 4.23 Hasil MITM pada VPN PPTP.....	81
Gambar 4.24 List Paket pada http target menggunakan Proxy anonymous	83
Gambar 4.25 List Paket pada imap target menggunakan Proxy anonymous.....	83
Gambar 4.26 Hasil Analisa Paket Imap pada Proxy Anonymous	84
Gambar 4.27 Hasil MITM pada penggunaan Proxy anonymous.....	85
Gambar 4.28 list Paket pada http target menggunakan SSH Tunnel	86
Gambar 4.29 list Paket pada IP target menggunakan SSH Tunnel.....	87
Gambar 4.30 Analisa Paket SSH gagal.....	88
Gambar 4.31 Hasil MITM pada penggunaan SSH tunnel	89
Gambar 4.32 Diagram Perbandingan Rata-rata <i>Throughput</i>	85
Gambar 4.34 Diagram Perbandingan Rata-rata <i>Transfer Time</i>	85

INTISARI

Dalam era globalisasi saat ini, kemudahan akses terhadap informasi merupakan salah satu kunci untuk dapat bersaing dan memenangkan kompetisi, karena dengan adanya informasi yang cepat dan akurat dapat meningkatkan kinerja suatu organisasi.

Menggunakan Internet sebagai sarana untuk mendapatkan jaringan publik atau mengirim informasi Menjadi resiko tersendiri karena internet terbuka untuk umum, maka masalah kerahasiaan dan otentikasi dari informasi yang diterima dan dikirim juga terbuka. Beberapa cara untuk mengatasi masalah di atas termasuk menggunakan PPTP VPN, proxy, dan SSH Tunnel yang menggunakan *server* luar negeri, yang terbebas batasan.

Peneliti melakukan pengujian simulasi dengan menguji kinerja dan keamanan, untuk melakukan pengujian tersebut diharapkan untuk mendapatkan informasi yang diinginkan tentang apa yang terbaik dalam *membypass* akses terbatas ke semua situs.

Kata Kunci : Linux, VPN (Virtual Private Network), Proxy Anonymouse, SSH Tunnel, VPS (Virtual Private Server).

ABSTRACT

In the current era of globalization, access to information is one of the keys to be able to compete and win the competition, because with a fast and accurate information that can improve the performance of an organization. Although Internet access is now easy to get around the world, but there are some sites that are limited to certain countries.

Using Internet as a means to get the public network or sending an information have its own risks because the Internet is open to the public, then the issue of confidentiality and authentication of the information received and sent were also open. Some ways to overcome the above problems include using PPTP VPN, proxy, and SSH Tunnel that use servers outside the country, which is free limits.

Researchers do simulation testing is done by testing the performance and security, to do such testing is expected to get the desired information about what is best to bypass the limited acces to all site

Keywords - Linux, VPN (Virtual Private Network), Proxy Annymous, SSH Tunnel, VPS (Virtual Private Server).