

**ANALISA DAN PERANCANGAN KEAMANAN OTENTIKASI VPN
SERVER MENGGUNAKAN METODE PORT KNOCKING
PADA UPT LABORATORIUM UNIVERSITAS
AMIKOM YOGYAKARTA**

SKRIPSI



disusun oleh

Muh. Syamil Alansyar

13.11.7239

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

**ANALISA DAN PERANCANGAN KEAMANAN OTENTIKASI VPN
SERVER MENGGUNAKAN METODE PORT KNOCKING
PADA UPT LABORATORIUM UNIVERSITAS
AMIKOM YOGYAKARTA**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muh. Syamil Alansyar

13.11.7239

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

PERSETUJUAN

SKRIPSI

**ANALISA DAN PERANCANGAN KEAMANAN OTENTIKASI VPN
SERVER MENGGUNAKAN METODE PORT KNOCKING
PADA UPT LABORATORIUM UNIVERSITAS
AMIKOM YOGYAKARTA**

yang dipersiapkan dan disusun oleh

Muh. Syamil Alansyar

13.11.7239

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 November 2016

Dosen Pembimbing,



Nila Feby Puspitasari, S.Kom, M.Cs
NIK. 190302161

PENGESAHAN

SKRIPSI

ANALISA DAN PERANCANGAN KEAMANAN OTENTIKASI VPN
SERVER MENGGUNAKAN METODE PORT KNOCKING
PADA UPT LABORATORIUM UNIVERSITAS
AMIKOM YOGYAKARTA

yang dipersiapkan dan disusun oleh

Muh. Syamil Alansyar

13.11.7239

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Mei 2017

Susunan Dewan Penguji

Nama Penguji

Yuli Astuti, M.Kom
NIK. 190302146

Andi Sunyoto, M.Kom
NIK. 190302052

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 3 Juni 2017

DEKAN FAKULTAS ILMU KOMPUTER

Khrisnawati, S.Si, M.T.
NIK. 190302038

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 tinggi manapun, 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, 5 Juni 2017

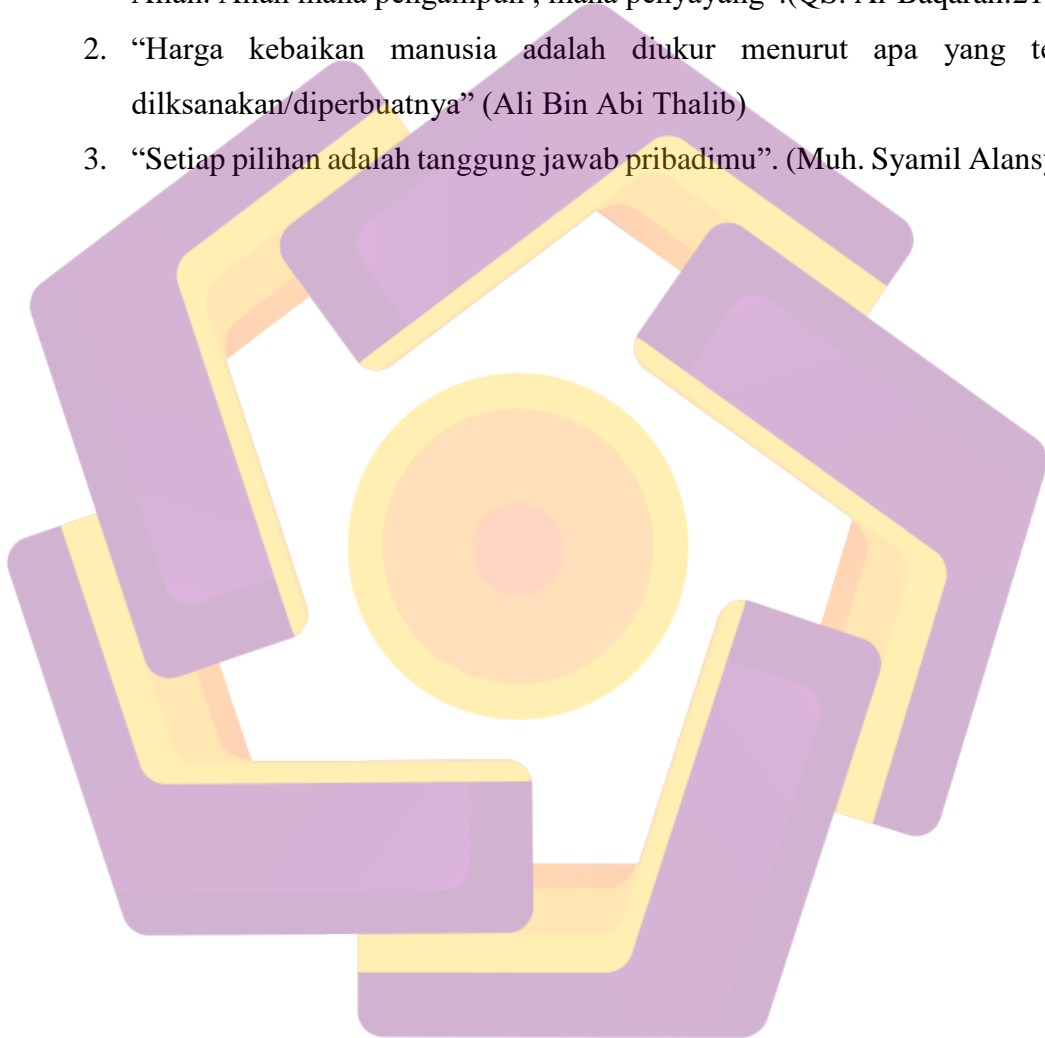


Muh. Syamil Alansyar

NIM. 13.11.7239

MOTTO

1. “Sesungguhnya orang-orang yang beriman, dan orang-orang yang berhijrah dan berjihad di jalan Allah, mereka itulah yang mengharapkan rahmat Allah. Allah maha pengampun , maha penyayang”.(QS. Al-Baqarah:218)
2. “Harga kebaikan manusia adalah diukur menurut apa yang telah dilaksanakan/diperbuatnya” (Ali Bin Abi Thalib)
3. “Setiap pilihan adalah tanggung jawab pribadimu”. (Muh. Syamil Alansyar)



PERSEMBAHAN

Pujisyukur kepada Tuhan yang maha kuasa, yang telah melimpahkan rahmat serta karunia Nya sehingga tugas akhir ini dapat terselesaikan dengan baik dan lancar.

Dengan segenap hati dan jiwa tugas akhir ini saya persembahkan kepada :

- Kedua orang tua dan adik - adiku yang amat sangat dicintai, Bapak Marwan (Uma) dan Ibu tercinta Sri Muharammah , yang telah memberikan segalanya, yang tak henti – hentinya memberikan doa dan dukungan serta semangat untuk saya. Kedua adikku Muhammda Teguh Pengabdian dan Rian Imamul Akram yang telah memberikan doa dan dukungan.
- Kerabat-kerabat penulis yang selalu ada dalam keadaan apapun, terima kasih Bagas yang bersedia meminjamkan alat Router Mikrotik nya. Angga dan Sovi yang selalu bareng kalau mau bimbingan. Said, Amirulah, Bayu, dan lainnya yang tidak bias saua sebutkan satu persatu terima kasih atas dukungan dan doa nya. Ucapan terima kasih juga pada teman-teman student staff UPT Amikom dan Keluarga Kos “BUDE”, semoga sukses dan sehat selalu.
- Bu Nila, selaku pembimbing, terima kasih telah memberikan bimbingan tugas akhir mulai dari awal pengerjaan hingga selesai serta Bu Hartatik dan Pak Rudy selaku penguji tugas akhir, terima kasih banyak dan sukses selalu.
- Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmu selama penulis kuliah.

- Teman-teman S1-TI-07, terimakasih atas 3,5 tahun yang menyenangkan ini, semoga sukses semua meraih apa yang dicitatakan.
- Kepala UPT AMIKOM Yogyakarta Pak Aji dan Seluruh karyawan, terimakasih sudah memberikan izin untuk melakukan penelitian dan membimbing sehingga dapat terlaksana dengan baik, semoga sukses selalu.
- The Big Family HMIF AMIKOM Yogyakarta sebuah ikatan dalam Himpunan yang sangat menyenangkan dan membuat cerita indah dalam kepanitiaan. Terimakasih atas ilmu, doa dan dukungannya, semoga tetap menjadi Himpunan rasa keluarga, Salam Himpunan #almamaterhitam.
- Keluarga Besar PERMATA AMIKOM Yogyakarta.
- Semua pihak yang telah membantu dalam penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Alhamdulillah, penulis ucapkan sebagai ungkapan syukur yang mendalam kepada Allah SWT atas limpahan nikmat dan hidayah yang diberikan sehingga penulis dapat menyelesaikan karya tulis ini. Shalawat dan salam senantiasa kita haturkan kepada Nabi dan suri tauladan kita, Rasulullah Muhammad SAW yang telah mengajarkan ilmu-ilmu Islam sehingga dapat menjadi bekal bagi kehidupan sekarang dan akhirat kelak.

Adapun skripsi ini dibuat untuk memenuhi syarat guna memperoleh gelar kesarjanaan Strata Satu (S1) Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Bagi penulis, proses penyusunan laporan skripsi ini tidak mudah. Banyak kekurangan dan hambatan yang penulis alami dikarenakan keterbatasan kemampuan penulis sendiri. Penulis sadari ada banyak pihak yang ikut membantu dan memberi dukungan kepada penulis sehingga tugas akhir yang ini dapat terselesaikan. Oleh karena itu, penulis ucapkan banyak terima kasih kepada semua pihak yang terlibat, terutama kepada:

1. Allah SWT atas limpahan rahmat, hidayah dan nikmat kehidupan.
2. Nabi Muhammad SAW sebagai Nabi dan suri tauladan bagi umat-Nya.
3. Bapak, Ibu dan seluruh keluarga tercinta atas segala dukungan, nasihat dan motivasi dalam menyelesaikan tugas akhri sebagai syarat mencapai gelar pendidikan sarjana ini.
4. Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas AMIKOM Yogyakarta.

5. Sudarmawan, S.T., M.T. selaku Ketua Program Studi S1 Informatika Universitas AMIKOM Yogyakarta.
6. Nila Feby Puspitasari S.Kom, M.Cs sebagai Dosen Pembimbing yang telah memberikan arahan dan bimbingan selama proses pengerjaan tugas akhir.
7. Yuli Astuti, M.Kom, sebagai dosen penguji 1. Andi Sunyoto, M.Kom, sebagai penguji 2 dan Ferry Wahyu Wibowo, S.Si, M.Cs, yang telah bersedia menjadi dosen pengganti pembimbing dalam sidang pendadaran tugas akhir ini, terima kasih banyak dan sukses selalu.
8. UPT Universitas AMIKOM Yogyakarta, terima kasih telah memberikan izin dan kesempatan untuk melakukan penelitian.
9. Seluruh dosen, staff pengajar dan karyawan Universitas AMIKOM Yogyakarta.
10. Sahabat-sahabat yang selalu mendukung penulis dalam kondisi apapun.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari kata sempurna karena keterbatasan dan minimnya pengalaman penulis. Penulis mengharap kritik dan saran yang membangun dari para pembaca agar untuk kedepannya penulis dapat berkarya dengan lebih baik lagi. Akhir kata, penulis berharap susunan tugas akhir ini dapat memberi manfaat bagi para pembaca.

Yogyakarta, 5 Juni 2017

Penulis

DAFTAR ISI

SAMPUL DEPAN	ii
JUDUL	ii
PERSETUJUAN	ii
PENGESAHAN	iiiv
PERNYATAAN	Error! Bookmark not defined.
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	ix
DAFTAR ISI	xi
DAFTAR TABEL	xv
DAFTAR GAMBAR	xvi
INTISARI	xix
ABSTARCT	xx
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4

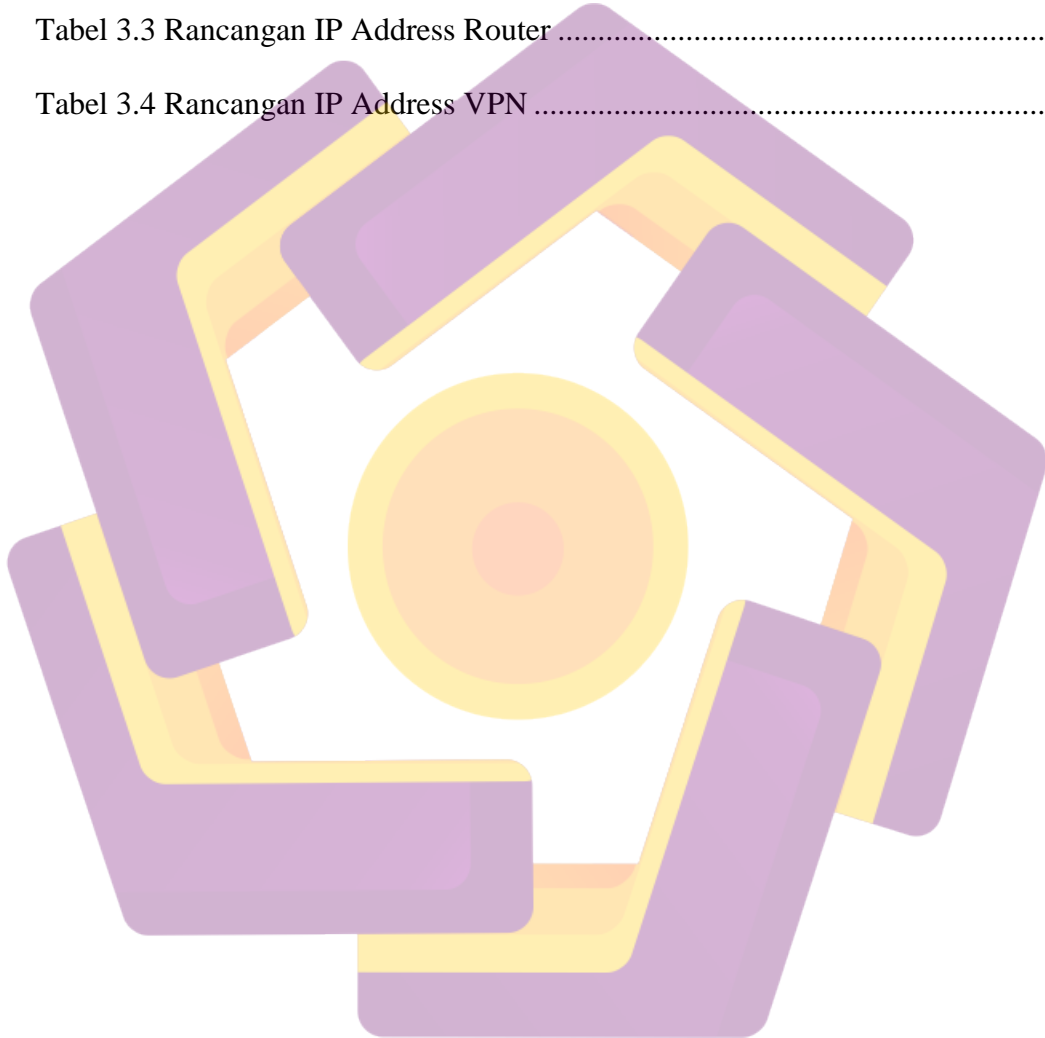
1.5	Manfaat Penelitian.....	5
1.6	Metode Penelitian.....	6
1.6.1	Metode Pengumpulan Data	6
1.6.2	Metode Pengembangan	7
1.7	Sistematika Penulisan.....	8
BAB II LANDASAN TEORI.....		10
2.1	Tinjauan Pustaka	10
2.2	Dasar Teori.....	11
2.2.1	Jaringan Komputer	11
2.2.2	Topologi Jaringan.....	14
2.2.3	Virtual Privat Network (VPN).....	17
2.2.4	OSI Layer	19
2.2.5	Port Komputer	20
2.2.6	Port Knocking.....	20
2.2.7	Perangkat Lunak yang Digunakan	22
2.2.8	Metode Penyerangan	24
2.2.9	Metode Pengembangan	25
BAB III METODE PENELITIAN.....		28
3.1	Lokasi Penelitian	28
3.1.1	Deskripsi Singkat UPT Laboratorium	28

3.1.2	Struktur Organisasi UPT	29
3.2	Tahapan Persiapan (Preapare)	30
3.2.1	Rancangan Topologi Awal	30
3.2.2	Pengumpulan Data	30
3.2.3	Identifikasi Masalah	31
3.2.4	Analisis Kelemahan Sistem	31
3.2.5	Analisis Kerugian yang Timbul Akibat Penyerangan	32
3.2.6	Analisis Pengujian Peforma Jaringan	33
3.2.7	Solusi Terhadap Masalah	37
3.3	Tahapan Perencanaan (Plan)	38
3.3.1	Analisis Kebutuhan Fungsional	38
3.3.2	Analisis Kebutuhan Non-Fungsional	38
3.3.3	Analisis Kebutuhan Sumber Daya Manusia (SDM)	41
3.4	Tahapan Perancangan (Design)	41
3.4.1	Rancangan Topoologi VPN	43
3.4.2	Konfigurasi Sistem	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN		49
4.1	Tahap Implementasi (Implement)	49
4.1.1	Konfigurasi IP Address Pada Routerboard	49
4.1.2	Konfigurasi IP Pool Untuk User VPN	50

4.1.3	Perubahan Port Default Otentikasi Router	50
4.1.4	Penerapan VPN Server	51
4.1.5	Penerapan Metode Port knocking pada VPN Server.....	56
4.1.6	Penerapan Perlindungan Port Otentikasi	59
4.1.7	Penerapan Alarm Deteksi Penyerangan VPN	60
4.1.8	Konfigurasi Email	62
4.2	Tahapan Pengoperasian (Operate).....	63
4.2.1	Pengujian Port Scanning	64
4.2.2	Pengujian Akses Otentikasi Router Tanpa VPN	65
4.2.3	Pengujian Port Knocking Remote Akses VPN	71
4.2.4	Pengujian Akses Otentikasi Router Dengan VPN.....	74
4.2.5	Pengujian Akses Server Lokal dari Publik.....	76
4.2.6	Pengujian Sniffing Traffic	77
4.3	Tahap Optimalisasi (Optimize)	78
BAB V	PENUTUP.....	79
5.1	Kesimpulan.....	79
5.2	Saran	80
DAFTAR PUSTAKA	81

DAFTAR TABEL

Tabel 3.1 Rancangan Pemindahan Port	45
Tabel 3.2 Rancangan Port Knocking VPN	46
Tabel 3.3 Rancangan IP Address Router	47
Tabel 3.4 Rancangan IP Address VPN	47



DAFTAR GAMBAR

Gambar 2.1 Tampilan Jaringan WAN	12
Gambar 2.2 Tampilan Jaringan MAN.....	13
Gambar 2.3 Tampilan Jaringan MAN.....	14
Gambar 2.4 Topologi Bus	14
Gambar 2.5 Topologi Star.....	15
Gambar 2.6 Topologi Ring	15
Gambar 2.7 Topologi Mesh	16
Gambar 2.8 Topologi Tree.....	16
Gambar 2.9 Topologi Hybrid	17
Gambar 2.10 Remote Akses VPN.....	18
Gambar 2.11 Komunikasi Osi Layer	20
Gambar 2.12 User tidak melalui port knocking	21
Gambar 2.13 User melakukan Port Knocking	21
Gambar 2.14 Mikrotik Router OS.....	22
Gambar 2.15 Login Winbox	23
Gambar 2.16 List Paket Aplikasi Mikrotik.....	24
Gambar 2.17 Proses medote PPDIOO Network lifecycle	26
Gambar 3.18 Struktur Organisasi UPT Laboratorium	29
Gambar 3.19 Topologi Awal.....	30
Gambar 3.20 Skenario Pengujian.....	34
Gambar 3.21 Port Scanning	35

Gambar 3.22 Percobaan Brute Force SSH.....	36
Gambar 3.23 Sniffing Traffic.....	37
Gambar 3.24 RB941-2nD-TC.....	39
Gambar 3.25 Alur Penelitian.....	42
Gambar 3.26 Rancangan Topologi VPN.....	43
Gambar 3.27 Enkapsulasi L2TP/IPSec.....	44
Gambar 3.28 Konfigurasi IP Address.....	49
Gambar 4.29 Konfigurasi IP Pool.....	50
Gambar 4.30 Pemindahan Port.....	51
Gambar 4.31 Pembuatan Proffile VPN.....	52
Gambar 4.32 Pembuatan User VPN.....	53
Gambar 4.33 Mengaktifkan Protokol L2TP/IPsec.....	53
Gambar 4.34 Monitoring User Aktif.....	54
Gambar 4.35 Konfigurasi Peers.....	55
Gambar 4.36 Konfigurasi Prposal.....	56
Gambar 4.37 Script Konfigurasi Port Knocking.....	57
Gambar 4.38 Hasil Script Port Knocking VPN.....	57
Gambar 4.39 Konfigurasi Filter Otentikasi.....	58
Gambar 4.40 Nat Masquerade.....	58
Gambar 4.41 Akses Sever Lokal.....	59
Gambar 4.42 Konfigurasi Perlindungan Port.....	59
Gambar 4.43 Pengaturan Alarm Deteksi Penyerangan.....	60
Gambar 4.44 Script Alarm VPN.....	61

Gambar 4.45 Hasil Baris Perintah Script Alarm.....	62
Gambar 4.46 Konfigurasi Tools Email.....	62
Gambar 4.47 Pengaturan Imap Pada Gmail.....	63
Gambar 4.48 Sebelum di Lindungi.....	64
Gambar 4.49 Hasil Setelah di Lindungi.....	65
Gambar 4.50 Percobaan Otentikasi Webfig Tidak Berhasil.....	66
Gambar 4.51 Percobaan Otentikasi SSH Tidak Berhasil.....	67
Gambar 4.52 Percobaan Otentikasi FTP Tidak Berhasil.....	68
Gambar 4.53 Percobaan Otentikasi Winbox Tidak Berhasil.....	69
Gambar 4.54 Otentikasi VPN tanpa Port Knocking.....	70
Gambar 4.55 Log Mencatat Kode Telah Terjadi Penyerangan.....	70
Gambar 4.56 Pesan yang di Terima dari Sistem.....	71
Gambar 4.57 Pengujian Port Knocking VPN.....	71
Gambar 4.58 Log Mencatat Proses Terjadinya Koneksi User VPN.....	72
Gambar 4.59 Otentikasi Berhasil.....	72
Gambar 4.60 Status User Aktif VPN.....	73
Gambar 4.61 Pengujian Koneksi Otentikasi Webfig Berhasil.....	74
Gambar 4.62 Pengujian Koneksi Otentikasi SSH Berhasil.....	75
Gambar 4.63 Pengujian Koneksi Otentikasi FTP Berhasil.....	75
Gambar 4.64 Pengujian Koneksi Otentikasi Winbox Berhasil.....	76
Gambar 4.65 Akses Server dari Publik.....	76
Gambar 4.66 Traffic yang telah di Enkapsulasi.....	77

INTISARI

Perkembangan akan kebutuhan pengolahan data dan informasi saat ini semakin meningkat, dan dibutuhkan lebih dari satu komputer yang digunakan. Komputer dan komunikasi data dapat dilakukan apabila komputer-komputer yang akan digunakan dihubungkan satu dengan yang lain dengan menggunakan router.

Perancangan dan implementasi Virtual Private Petwork (VPN) membantu menghubungkan dua jaringan berbeda dalam satu jaringan private yang aman, dimana VPN server adalah pusat penanganan semua registrasi dari *client* sehingga kedua jaringan tetap terhubung melalui tunnel VPN. Implementasi VPN akan memaksimalkan komunikasi antar jaringan yang berlangsung selama 24 jam.

Penulis lebih berkonsentrasi terhadap segi keamanan jaringan serta perangkat-perangkat yang bakal terhubung dengan tunnel VPN, seperti router tempat implementasi yang nantinya bakal menjadi sentral utama untuk pengamanan otentikasi VPN Server. Untuk mengatasi kekhawatiran tersebut dibutuhkan suatu kemandu yang dapat menjaga otentikasi yang aman, memiliki langkah-langkah masuk serta dapat memproteksi. Oleh karena itu, penulis mencoba merancang sistem kerja Port Knocking dengan Firewall terhadap otentikasi VPN Server pada Mikrotik, sehingga dapat memperkuat serta memproteksi user atau *client* yang tidak memiliki akses masuk pada VPN Server.

Kata Kunci : VPN, Mikrotik, Firewall, Port Knocking

ABSTARCT

The development of data processing needs and current information, and it takes more than one computer is used. Computer and data communication can be done when the computers will be used to be connected with one another by using the router.

Design and implementation of Virtual Private (VPN) Petwork help connect two different networks in a secure, private network where VPN server is handling all the registration centers from the client so that the two networks remain connected through the VPN tunnel. Implementation of VPN will maximize the communication between a network that lasted for 24 hours.

The authors concentrate more towards network security as well as in terms of the devices which are connected by a tunnel to the VPN router, such as the place of implementation that later would be central to the VPN Server authentication security. To address these concerns needed a safety who can maintain a secure authentication, have the entrance steps and can therefore protect the author tried to design a working system of Port Knocking Firewall with VPN Server authentication against at Arabian Ranches, so that it can strengthen and protect the user or client who does not have access to the VPN Server.

Keyword : VPN, Mikrotik, Firewall, Port Knocking