BAB III
ANALISIS DAN PERANCANGAN

3.1 Analisis

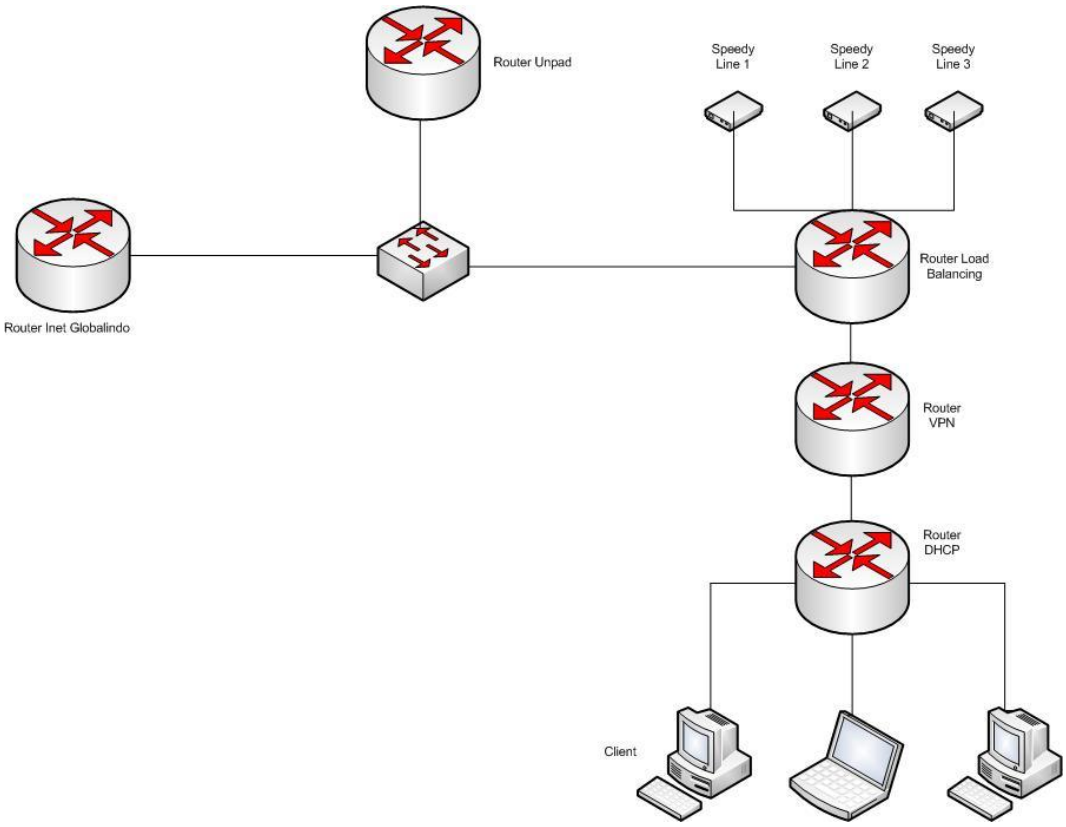
Analisis adalah pembagian suatu masalah menjadi komponen – komponen yang lebih kecil untuk mengidentifikasi dan mengevaluasi masalah dan hambatan yang ditemui, dan kebutuhan yang diharapkan sehingga nantinya dapat diusulkan perbaikan-perbaikannya. Bab ini menguraikan proses analisis pengujian terhadap *VPN* yang berjalan di PT.Padjadjaran Mitra, serta melakukan perancangan dan implementasi metode yang digunakan dalam meningkatkan keamanan dalam *VPN* sistem. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan–kebutuhan pokok sitem *VPN* yang akan dibangun.

3.1.1 Analisis Sistem Yang Telah Berjalan

PT.Padjadjaran Mitra menerapkan *VPN server* untuk mengelola bisnis penjualan koneksi internet dengan dengan menggunakan *protokol PPTP*.Dan pada penerapan *VPN* tersebut penulis mencoba menganalisa penerapan keamanan terhadap penerapan *VPN* server tersebut.

3.1.1.1 Analisis Jaringan Internet

PT.Padjadjaran Mitra mempunya sumber *bandwidth* dengan menggunakan 3 line speedy yang di*load balancingkan* dengan masing-masing *line bandwith* 3Mbps, bandwith tambahan dari UNPAD sebesar 10 Mbps dan tambaha dari ISP Inet Globalindo sebesar 2 Mbps *dedicated*, sehingga total bandwith yang dikelola PT,Padjadjaran Mitra sebesar 21 Mbps.

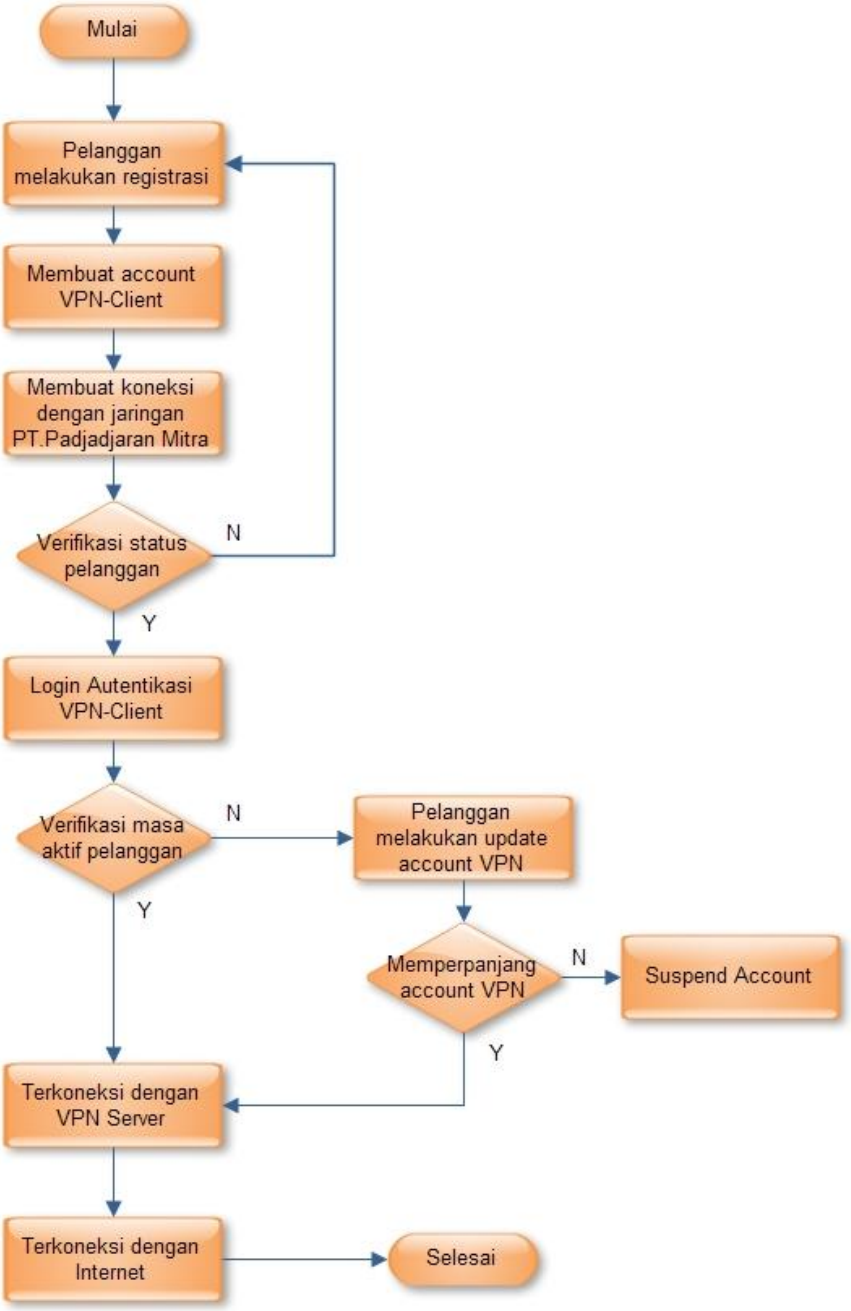


Gambar 3. 1 Topologi Jaringan Internet

Pada gambar 3. 1 , yang berperan penting dalam pengaturan dan pengalokasian gateway untuk mencapai *internet* yaitu *Router Load balancing*.Karena *Router load balancing* berfungsi untuk membagi atau mendistribusikan jalur internet yang diakses oleh client dengan mengatur jalur-jalur mana saja yang kosong untuk dilalui menuju internet.

3.1.1.2 Analisis Jaringan VPN

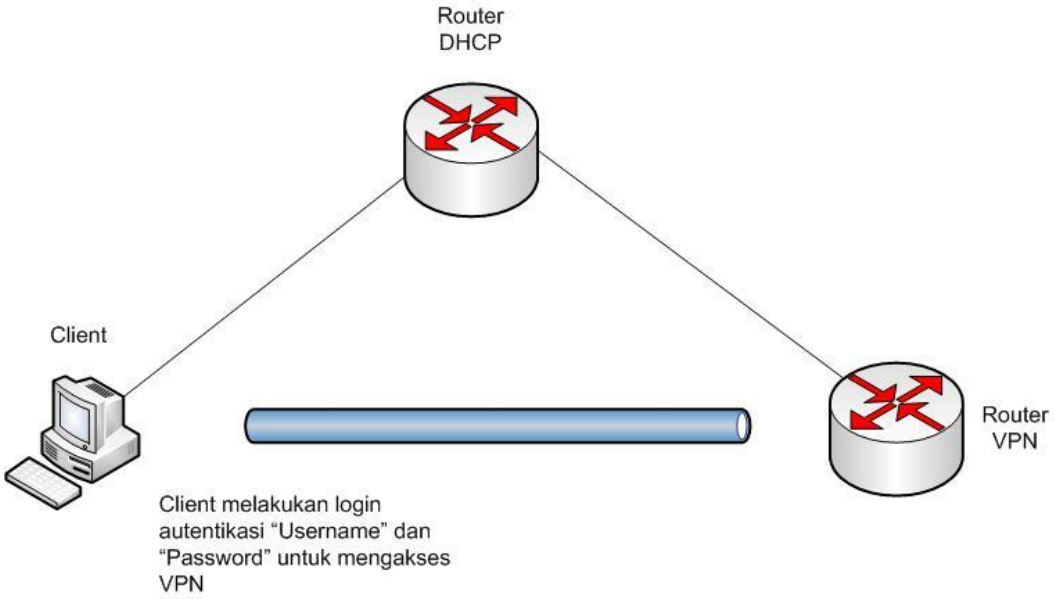
Dalam penjualan koneksi internet, PT.Padjadjaran Mitra menggunakan VPN server dengan protokol yang dipakai yaitu protokol PPTP. Dalam hal ini pelanggan yang terhubung ke jaringan PT.Padjadjaran Mitra harus melakukan *login* sebagai *autentikasi* yang dilakukan untuk mengakses internet.



Gambar 3. 2 Flow chart Pelanggan VPN

Pada gambar 3.2, diperlihatkan flow chart dari pelanggan VPN. Proses dimulai dengan melakukan registrasi baru terlebih dahulu, setelah ter registrasi pelanggan akan mendapakat *username* dan *password* yang digunakan untuk *autentikasi* login ke VPN server. Pada saat melakukan login, pelanggan akan di

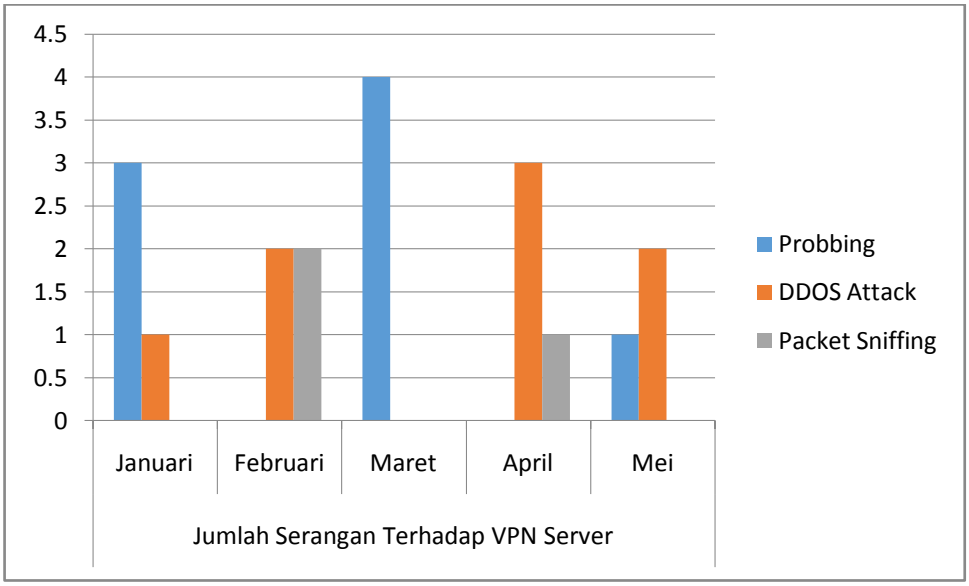
verifikasi terlebih dahulu apakah *username* yang digunakan masih valid atausudah suspend. Apabila *username* tersebut suspend, maka pelanggan diharuskan melakukan pembayaran atau registrasi ulang bulanan untuk me-*Renew* username tersebut agar bisa terkoneksi dengan VPN Server.



Gambar 3. 3 Topologi VPN

3.1.2 Analisis Masalah

Setelah melakukan penganalisisan terlebih dahulu terhadap sistem yang berjalan di PT.Padjadjaran Mitra, VPN memiliki beberapa kelemahan. Ada beberapa serangan terhadap VPN server yang dilakukan pihak yang tidak ber tanggung jawab agar dapat melakukan koneksi secara ilegal maupun merusak sistem yang berjalan.



Gambar 3. 4 Grafik Jumlah serangan terhadap VPN Server

Pada gambar 3.4 dijelaskan grafik jumlah serangan terhadap *VPN Server* yang dilakukan pihak-pihak yang tidak bertanggung jawab. Dan dijelaskan pula dengan tabel 3.1 .

Tabel 3. 1 Jumlah Serangan VPN

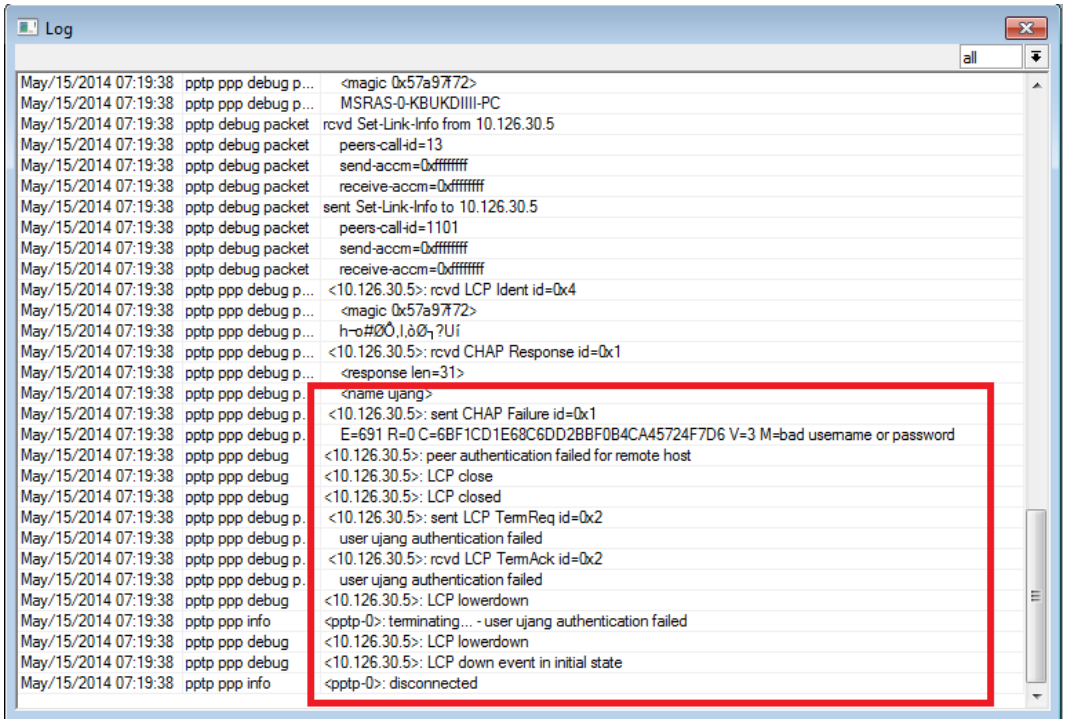
Bentuk Serangan	Jumlah Serangan Terhadap VPN Server				
	Januari	Februari	Maret	April	Mei
Probbing	3	0	4	0	1
DDOS Attack	1	2	0	3	2
Packet Sniffing	0	2	0	1	0

3.1.2.1 Analisis Metode Serangan

Kegiatan dan hal-hal yang membahayakan keamanan jaringan*VPN-Server* antara lain adalah hal-hal sebagai berikut:

1. Probe

Ditemukan serangan dengan bentuk *probe* atau yang biasa disebut *probing* terhadap *VPNServer* PT.Padjadjaran Mitra dengan melakukan percobaan log in suatu account VPN client secara berulang-ulang dengan tujuan terkoneksi dengan VPN Server .



Gambar 3. 5 Tindakan Probing

2. Scan

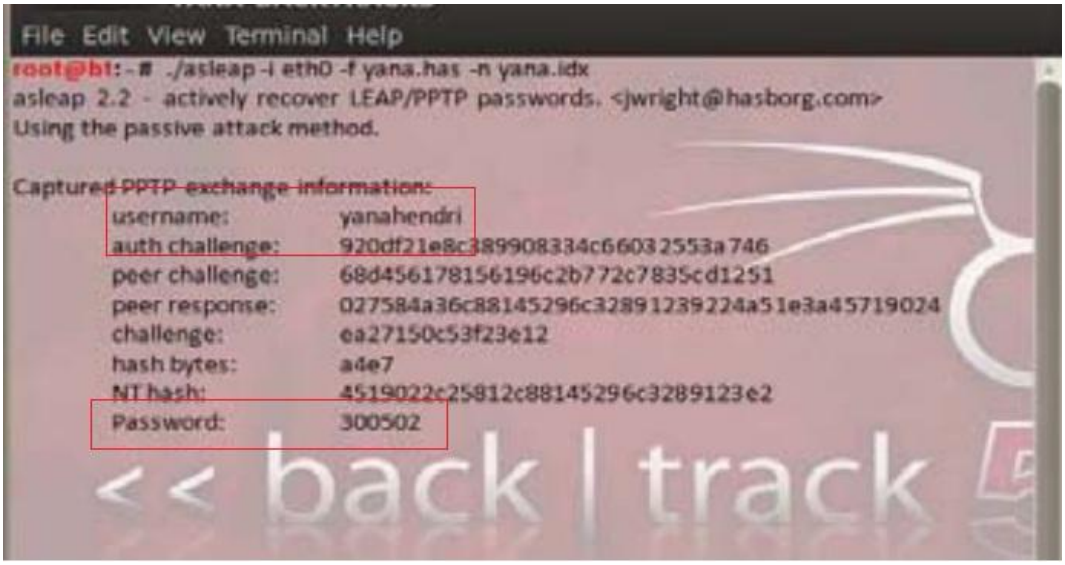
Pada sistem yang berjalan saat ini, ketika dilakukan scanning port terhadap *VPN Server* PT.Padjadjaran mitra yang ditemukan beberapa port yang terbuka. Port-port yang terbuka tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab unutk melakukan penetrasi atau serangan-serangan dengan tujuan mendapatkan informasi atau melakukan pengerusakan terhadap sistem. Port yang terbuka pada VPN Server PT.Padjadjaran Mitra dapat dilihat pada gambar 3.6



Gambar 3. 6 Scanning port

3. Packet Sniffer

Selain itu kelemahan-kelamahan pada VPN Server PT.Padjadjaran Mitra , *Packet sniffer* yang dapat mengcapture paket-paket yang menuju VPN Server tersebut dengan dilakukan *arp poisoning* terhadap target sehingga target diharuskan melewati komputer penyerang terlebih dahulu sebelum mengakses VPN Server yang dituju dan meng *captureusername* dan *password* adalah target tersebut. Yang mengakibatkan pihak yang melakukan *packet sniffer* ini dapat melakukan koneksi terhadap *VPN Server* PT.Padjadjaran Mitra.

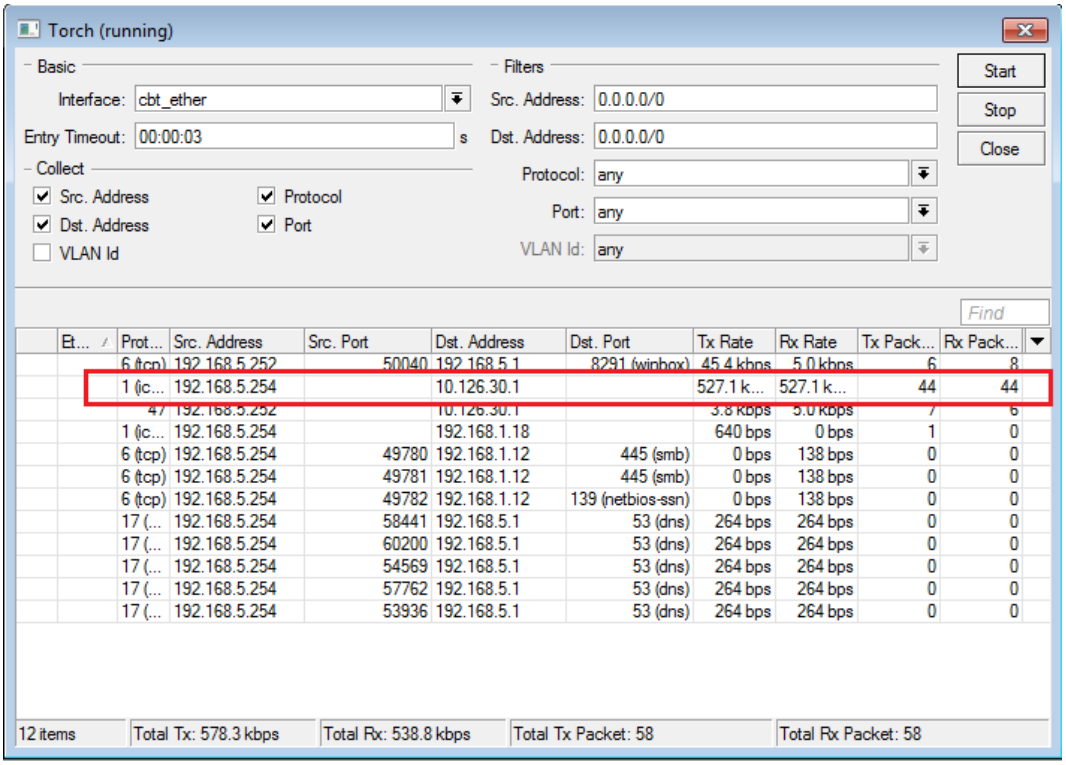


Gambar 3. 7 paket snifer user dan password

Penyerang yang berada satu lingkungan jaringan dengan korban akan melakukan arp poisoning terlebih dahulu, agar list arp yang dikenali pada netwok tersebut merubah mac address pc penyerang menjadi mac address gateway. Sehingga menyebabkan paket-paket yang semula hendak dikirim langsung melewati router gateway, paket tersebut dibelokan terlebih dahulu ke pc penyerang yang dengan kondisi ini paket tersebut bisa disadap oleh penyerang tersebut.

4. Denial of Service (DoS)

Selain itu, bentuk serangan-serangan terhadap *VPN Server* PT.Padjadjaran Mitra yaitu dengan serangan DoS, salah penyerang melakukan kiriman paket dalam jumlah besar terhadap VPN Server, sehingga menyebabkan load CPU meningkat dan *traffic* pun menjadi padat.



Gambar 3. 8 ping flood

Ditemukan ip 192.168.5.254 dengan protokol 1 (icmp) sedang melakukan ping, dengan jumlah paket yang besar yang mencapai 527 kbps.

Efek dari attack dengan pingflood ini berpengaruh pada koneksi antara client vpn dengan server vpn, karena dengan serangan terus menerus dan dalam jumlah yang banyak menyebabkan jalur atau *traffic*menjadi padat dan membuat koneksinya mengalami down dengan adanya tampilan Request time out.

Denial of Service (DoS) Attack dengan menggunakan pingflood ternyata memiliki efek yang lebih parah daripada perintah ping biasa, sehingga dapat disimpulkanbahwa eksperimen Denial of Service (DoS) attack khususnya pingflood ternyata berhasil menyerang dan mengganggu aktivitas jaringan di server vpn, hal ini merupakan salah satu kelemahan jaringan pada VPN server tersebut. Solusi untuk mengatasi permasalahan kelemahan vpn tersebut dengan meningkatkan pengamanan di level server dan gateway/router-nya.

3.1.3 Analisis Metode Pengamanan VPN

Pada sistem pengamanan VPN , dilakukan penambahan metode keamanan :

1. Filter port pada VPN Server, memfilter port-port yang terbuka pada VPN Server. Memfilter port yang terbuka tersebut bertujuan untuk mengefektifkan penggunaan port komunikasi sesuai dengan kebutuhan dan pengguna yang berhak mengakses port tersebut.
2. TLS(Transpor Layer Security) mengimplementasikan metode port knocking pada server VPN mikrotik tersebut.

Pada penelitian ini , pemilihan terhadap *port knocking* sebagai upaya peningkatan keamanan pada VPN Padjadjaran Mitra berdasarkan atas kemampuan nya untuk membuat keamanan berlapis.

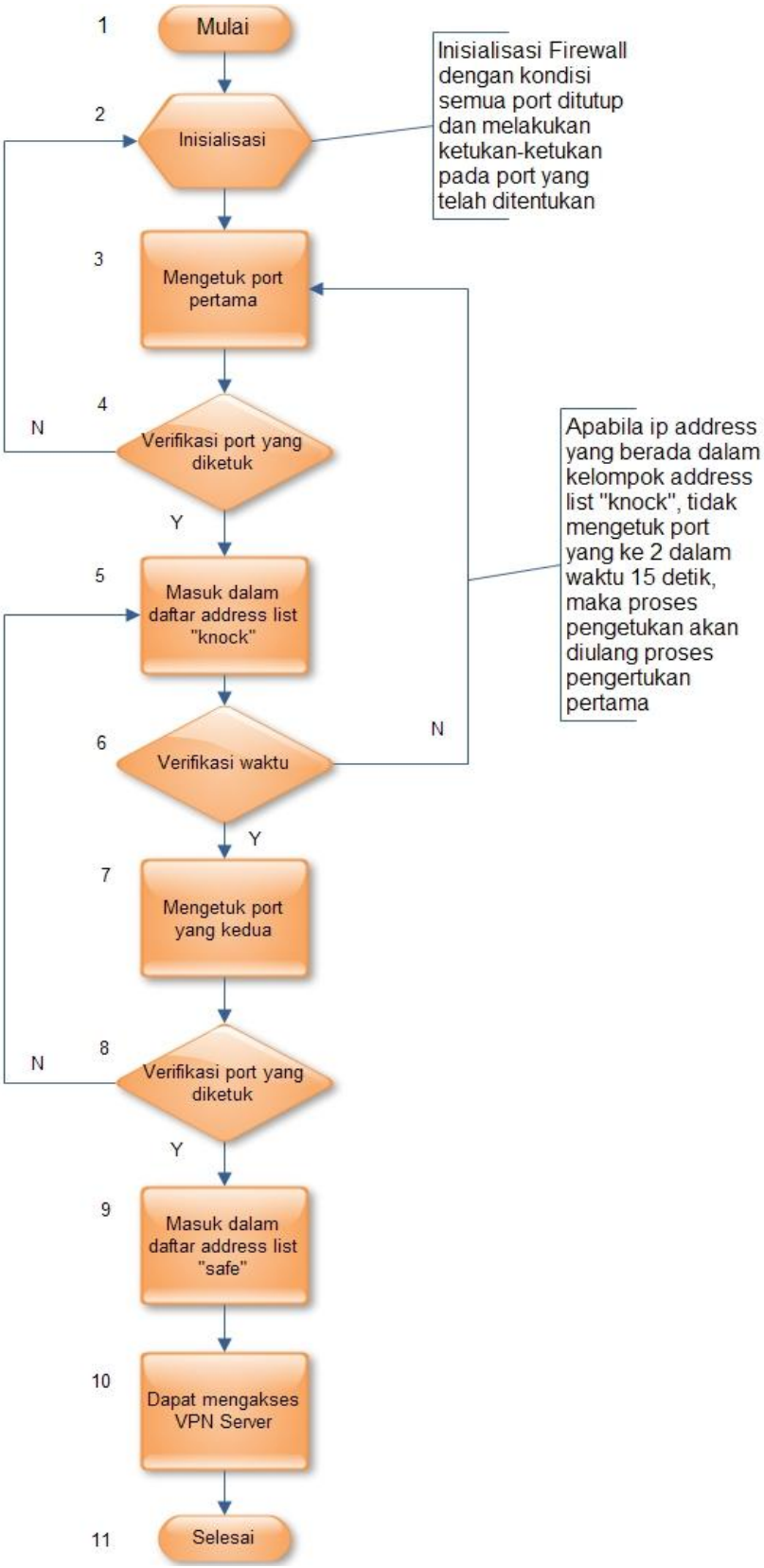
3.1.4 Analisis Port Knocking

Untuk mendapatkan keamanan yang diperlukan dan kemampuan untuk mengizinkan user yang berhak untuk mengakses VPN server maka diperlukan suatu metode yang memenuhi kedua kriteria tersebut. Salah satu metoda baru yang memiliki kemampuan untuk memenuhi kedua kriteria tersebut adalah port knocking.

Berdasarkan analisis masalah yang didapat, beberapa serangan terhadap VPN server berdasarkan atas penyalah gunaan port-port komunikasi yang terbuka pada server sehingga pengimplementasian port knocking bertujuan untuk memberikan keamanan berlapis pada VPN Server PT.Padjadjaran Mitra dan memfilter ip address mana saja yang diperkenankan terkoneki terhadap server.

Selain itu kelebihan port knocking pada pengimplementasian VPN Server diantaranya:

1. Dimana komputer remote berkomunikasi dengan sebuah server melalui port yang tertutup.
2. Meskipun port ditutup, layanan yang disediakan tetap berjalan.



Gambar 3. 9 Flow chart Port Knocking

Pada gambar 3.9 digambarkan alur pengimplentasian port knocking pada VPN router OS tersebut.Pada gambar 3.9 terdapat gambar 1-11 yang menunjukan tiap proses nya.

1. Nomer 1 proses memulai akan melakukan knocking port.
2. Nomor 2 menunjukan inisialisasi port berapa saja yang akan diketuk agar koneksi atau port yang dikehendaki dapat terbuka.
3. Nomor 3 menunjukan proses mengetuk port tahap pertama,
4. Nomor 4 validasi port yang diketuk , apabila port yang diketuk sudah benar maka ip addressnya akan dikelompokan pada address list *"knock"*, apabila salah akan diulang ke proses Nomor 2.
5. Nomor 5 menunjukan ip address yang mengetuk sesuai dengan port yang telah diatur akan dikelompokan dalam address list *"knock"*.
6. Nomor 6 validasi waktu, apabila ip address yang berada dalam kelompok address list "knock" dalam waktu <=15 detik tidak melakukan ketukan port selanjutnya, maka akan proses akan diulang dari Nomor 3.
7. Nomor 7 menunjukan proses mengetuk port tahap ke dua dalam waktu < 15 detik.
8. Nomor 8 verifikasi port yang di ketuk, apabila port yang diketuk sesuai dengan port yang telah ditentukan, maka ip addressnya akan dikelompokan pada address list *"safe"*, apabila salah akan diulang ke proses Nomor 5.
9. Nomor 9 ip address yang mengetuk port sesuai dengan port yang telah ditentukan, maka ip addressnya akan dikelompokan pada address list *"safe"*.
10. Nomor 10 ip address yang telah berada dalam kelompok address list *"safe"* akan diperkenan kan untuk mengakses VPN Server.
11. Nomor 11 selesai.

3.1.5 Analisis Kebutuhan Infrastruktur

Kebutuhan perangkat keras untuk server VPNdan lain nya dibutuhkan perangakat keras sebagai berikut :

Tabel 3. 2 Perangkat keras pc

	Pengakses	*Penyerang*
Processor	Dualcore 2.4 Ghz	Intel core i3
Memory	1024 MB	2GB
Harddisk	40 GB	20 GB
Sistem Operasi	Windows 7	Backtrack 5



Gambar 3. 10 Mikrotik RB 750 G

Tabel 3. 3 Spesifikasi Mikrotik rb750 G

SpesifikasiProduk

CPU	AR7161 680/800MHz CPU
Memory	32MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Five 10/100/1000 gigabit ethernet ports (with switch chip)
miniPCI	None
Extras	Reset switch, Beeper
Serial port	no serial port
LEDs	Power, NAND activity, 5 Ethernet LEDs
Power options	Power over Ethernet: 9-28V DC (except power over datalines). Power jack: 9.28V DC
Dimensions	113x89x28mm. Weight without packaging and cables: 130g
Power consumption	Up to 3W
Operating System	MikroTikRouterOS v3, Level4 license

3.1.5 Analisis Perangkat Lunak

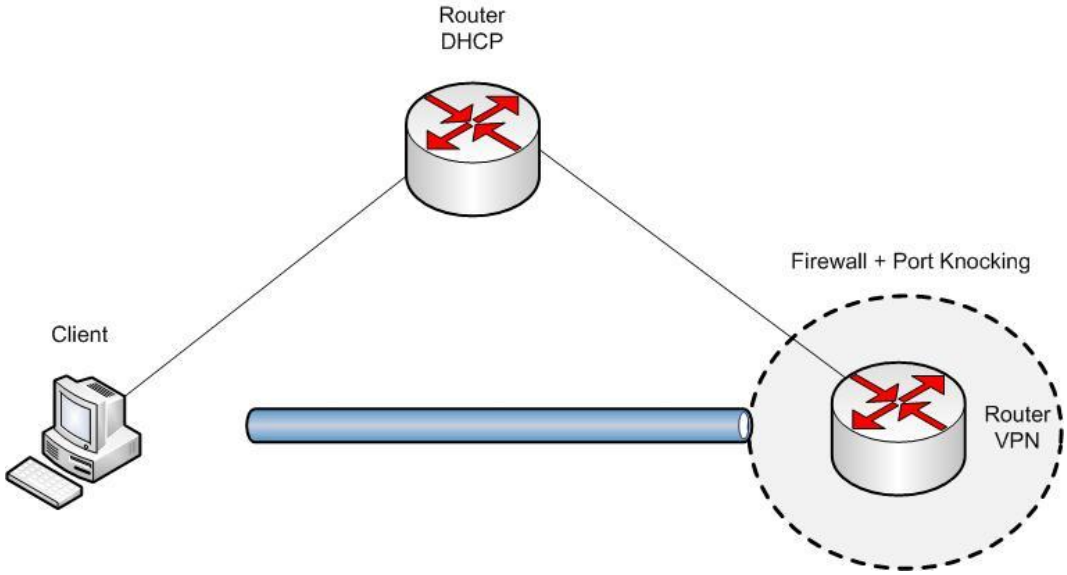
Kebutuhan perangkat lunak untuk server VPN,

Tabel 3. 4 Kebutuhan perangkat lunak

Nama Perangkat	Perangkat Lunak	Keterangan
Router OS	v.5.4	Router os versi 5.4
Client	VPN client windows	Digunakan untuk vpn client
Penguji	Arpspoof	*Arpspoof* digunakan untuk penyerangan terhadap ARP
	Wireshark	Wireshark digunakan sebgai packet *sniffer, username dan password*

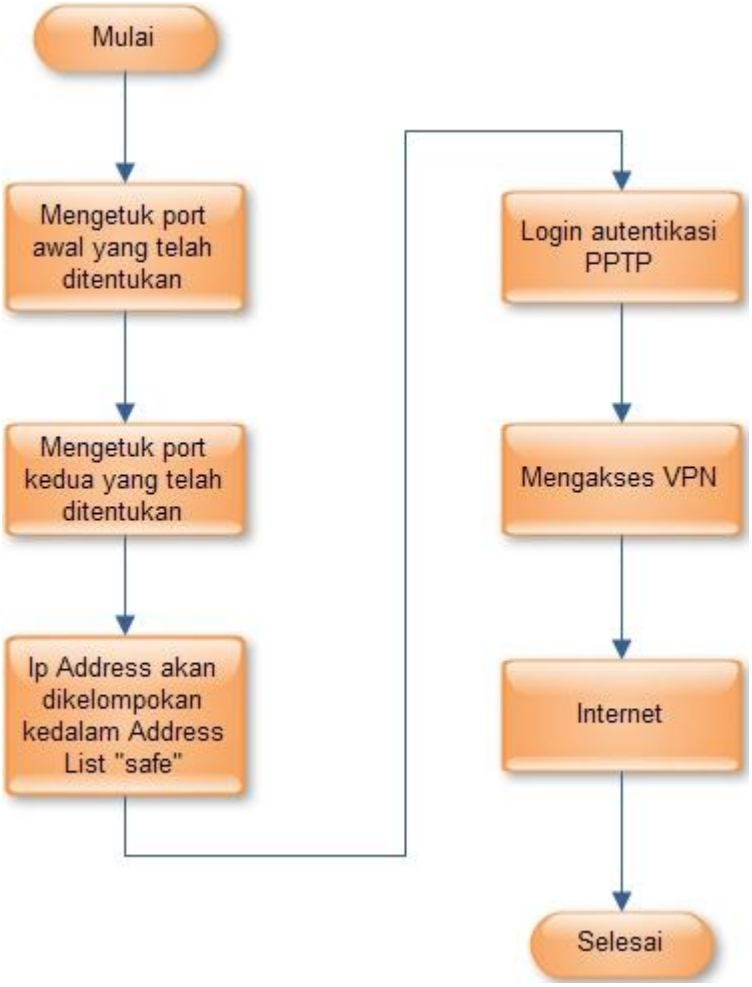
3.2 Perancangan Sistem

Pada peracangan sistem akan dijelaskan mengenai, perancangan simulasi, perancangan arsitektur pengujian dan beberapa percangangan lainya.



Gambar 3. 11 Infrastruktur VPN + port knocking

Perancangan dilakukan dengan menambahkan pengamanan VPN server tersebut dengan penutupan semua port yang terbuka dengan penambahan metode port *knocking* untuk mengakses VPN server tersebut.



Gambar 3. 12 Alur port knocking dan PPTP

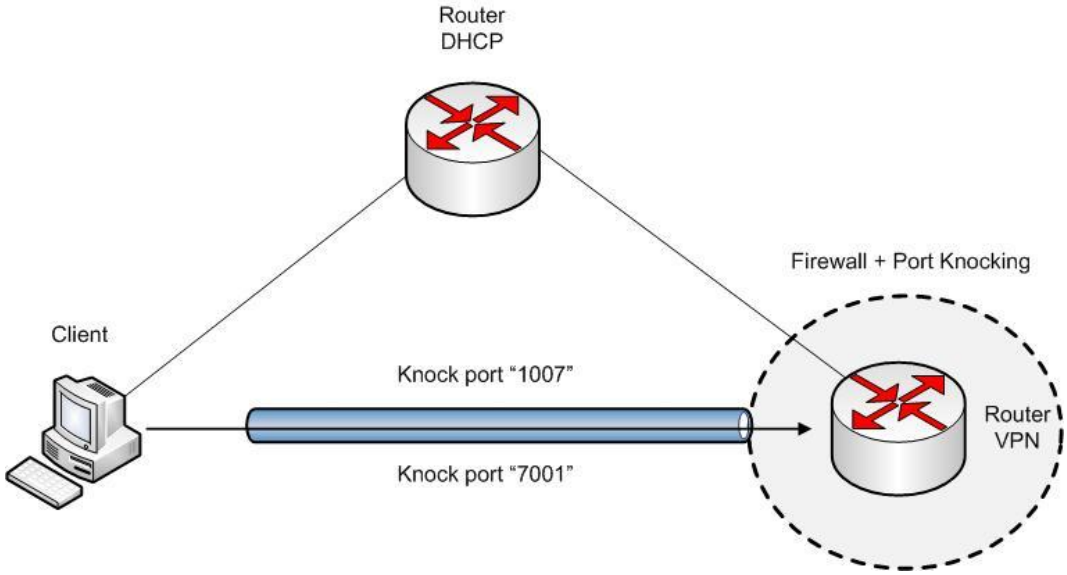
Pada gambar 3.12 telah digambarkan alur penggunaan metode port knocking yang dilanjutkan dengan pengaksesan VPN Server

3.2.1 Tujuan Perancangan Sistem

Perancangan sistem merupakan suatu proses tindak lanjut dari tahap analisis. Setelah mendapat gambaran umum mengenai sistem pada tahap analisis lalu penelitin melanjutkan dengan perancangan sistem yang bertujuan untuk memberikan gambaran sistem yang akan dibuat.

3.2.2 Perancangan Arsitektur

Perancangan arsitektur simulasi pada gambar dibuat untuk memberikan gambaran arsitektur infrastruktur yang digunakanuntuk membangun server VPN port knocking.

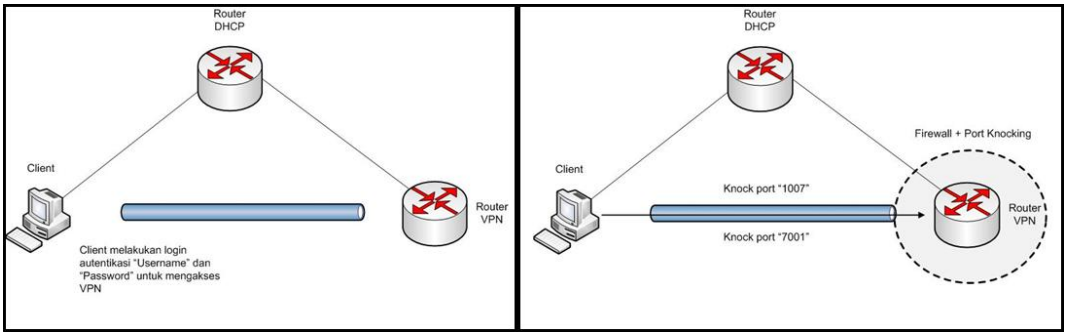


Gambar 3. 13 Arsitektur *VPN port knocking*

Client melakukan knocking atau mengetuk *port-port* yang ditentukan, misal port 1007 dan 7001 agar dapat mengakses *VPN server* tersebut.

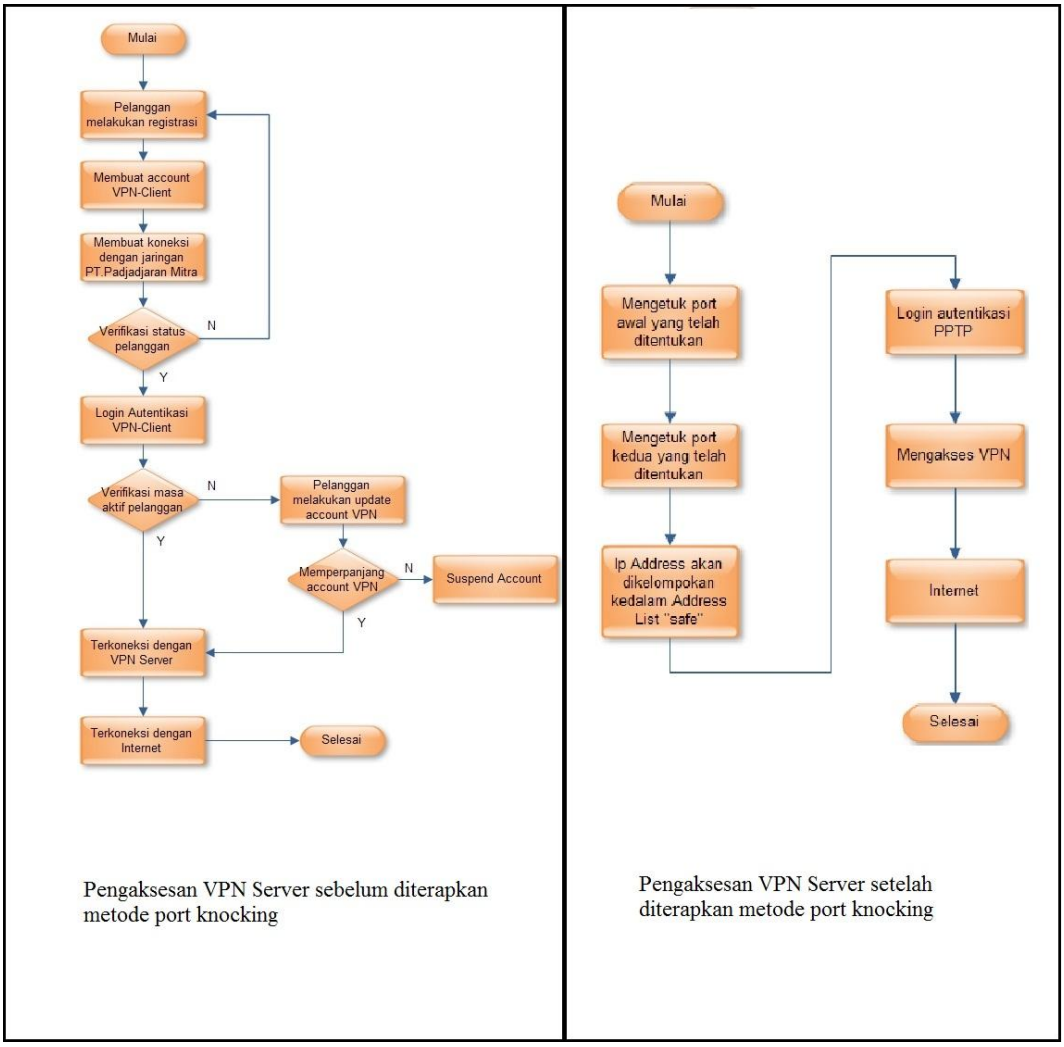
Tabel 3. 5 Keterangan port

Port	Keterangan
1007	Mengelompokan ip ke kelompok "knock"
7001	Mengelompokan ip ke kelompok "safe" dan dapat melakukan koneksi ke VPN server



Gambar 3. 14 Perbandingan Infrastruktur

Pada gambar 3.14 digambarkan mengenai perbandingan infrastruktur sebelum dan sesudah penerapan metode *port knocking* pada PT.Padjadjaran Mitra.



Gambar 3. 15 Perbedaan alur pengaksesan VPN Server

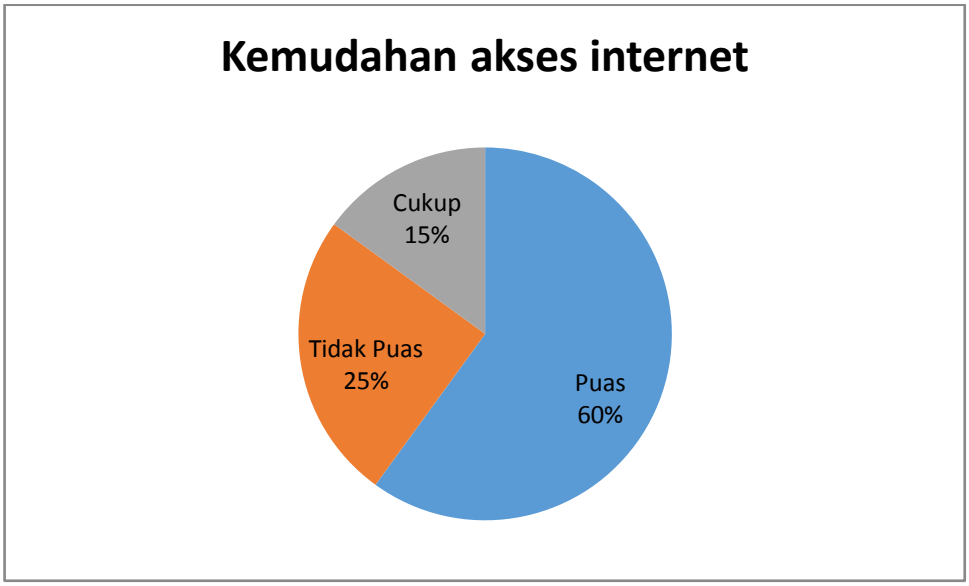
Pada gambar 3. 15 pun dijelaskan mengenai perbedaan alur pengaksesan VPN server sebelum penerapan *port knocking* dan sesudah penerapan *port knocking*.

Setelah diterapkannya metode port knocking pada sistem keamanan *VPN Server*, diberikan beberapan kuisioner terhadap pelanggan terkait dengan penerapan metode baru port knocking pada VPN Server.

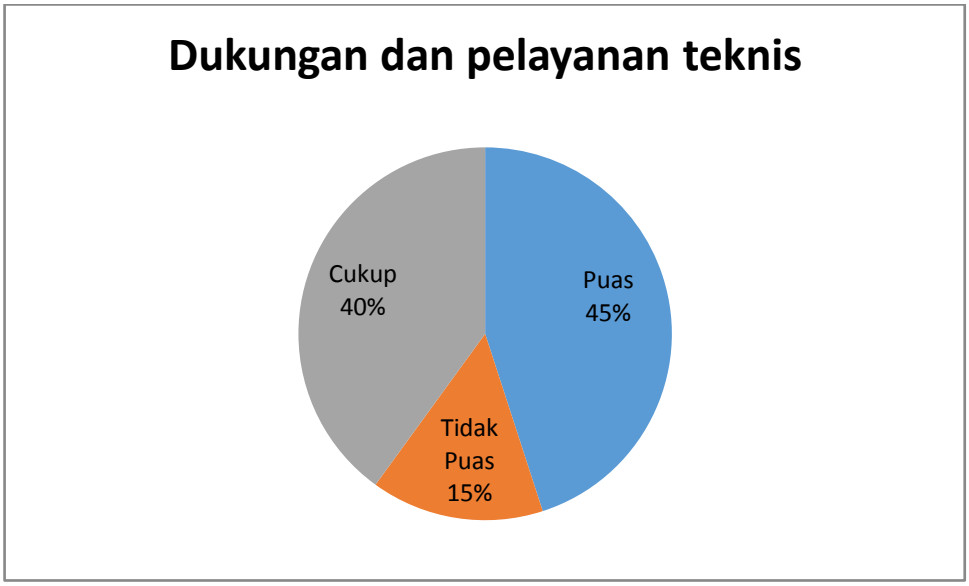
Hasil yang didapat dari kuisioner pelanggan diantaranya:

Tabel 3. 6 Hasil Kuisioner

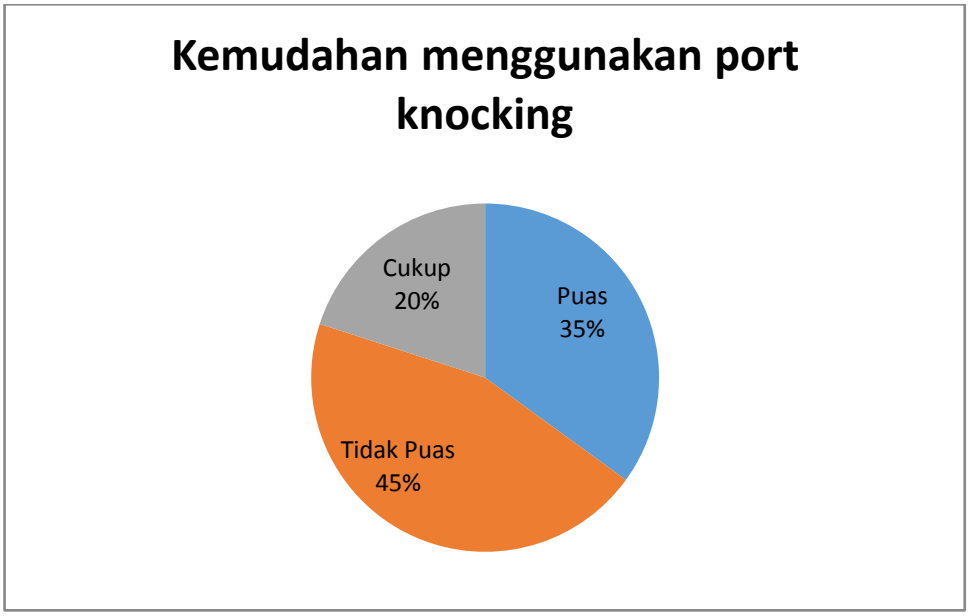
	Menjawab		
	Puas	Tidak Puas	Cukup
Kemudahan akses internet	12	5	3
Dukungan dan pelayanan teknis terhadap user pengguna jaringan internet	9	3	8
Kemudahan akses menggunakan port knocking	7	9	4
Keamanan saat interaksi internet setalah menggunakan port knocking	8	6	6



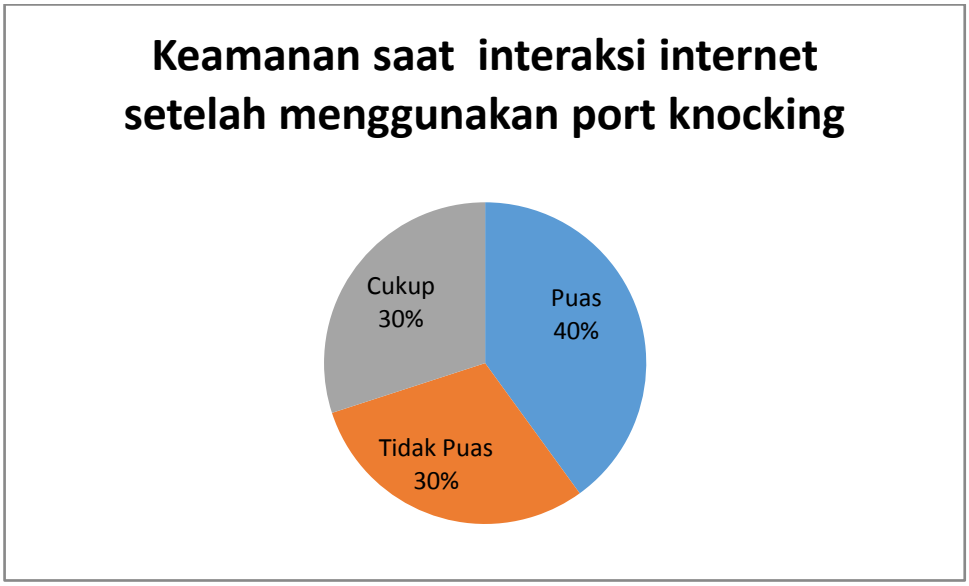
Gambar 3. 16 Hasil kuisioner kemudahan akses internet



Gambar 3. 17 Hasil kuisioner dukungan pelayanan teknis



Gambar 3. 18 Hasil kuisioner kemudahan menggunakan port knocking



Gambar 3. 19 Hasil kuisioner keamanan setelah menggunakan port knocking

Setelah diperloeh data dari hasil kuisioner terhadap pelanggan, sebanyak 45 % menyatakan kurang puas mengenai kemudahan menggunakan port knocking akan tetapi dilihat dari hasi kuisioner keamanan saat ber interaksi setelah menggunakan port kncokinghampi 40 % menyatakan puas dan 30% menyatakan cukup puas. Oleh karena kesimpulan dari hasil kuisioner ini didapat penilaian keamanan pelanggan terhadap penerapan port knocking sudah cukup baik, hanya saja perlu ditingkatkan pengenalan atau tata cara penggunakan port knocking yang dipermudah penggunaannya.

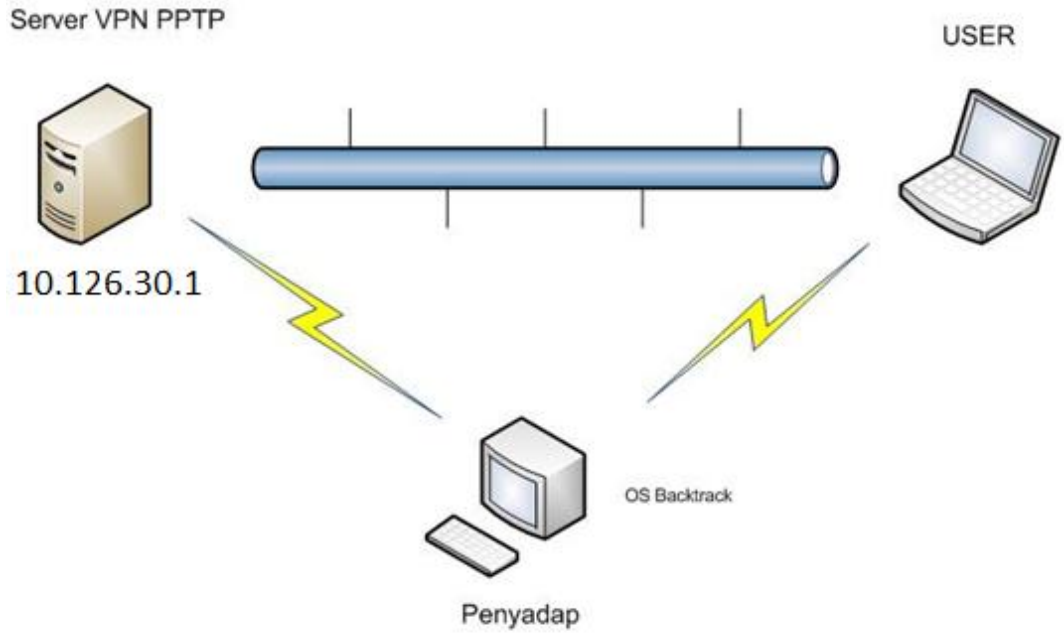
3.2.3 Perancangan Arsitektur Pengujian

Perancangan arsitektur pengujian akan dilakukan untuk menguji keamanan *VPN* terhadap serangan – serangan yang datang terhadap *VPN server* tersebut.

3.2.3.1 Perancangan Pengujian Penyadapan

Perancangan arsitektur pengujian dilakukan untuk menguji penyadapan autentikasi User dan password yang digunakan untuk mengakses VPN dengan metode penyerangan menggunakan *Packet Sniffing*. Pengujian dilakukan pada

pengaksesan *VPN* tanpa menggunakan metode port knocking dan pengaksesan menggunakan metode port knocking.



Gambar 3. 20 Simulasi penyadapan

Pada gambar 3.16 menunjukan ilustrasi dari penyerangan. Penyerang melakukan spoofing terhadap user yang hendak melakukan koneksi *vpn*.

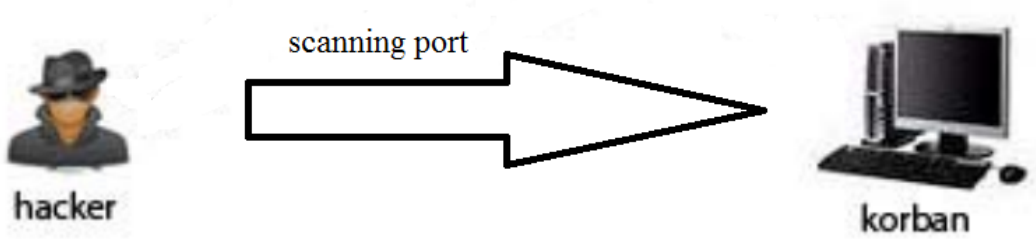
Pengujian dilakukan menggunakan tiga skenario. Skenario tersebut dibuat dengan tujuan untuk membuktikan keamanan *VPN* pada sistem dan cara penyerangan yang berbeda yang ditampilkan pada Tabel 3.6

Tabel 3. 7 Skenario Pengujian

No	Server VPN	Waktu Penyerangan
1	Tidak menggunakan port knocking	Sebelum mengakses VPN
2	Menggunakan port knocking	Saat hendak mengakses VPN
3	Menggunakan port knocking	Ketika sudah terhubung VPN

3.2.3.2 Perancangan Pengujian Port Scanning

Perancangan arsitektur pengujian port scanning dilakukan untuk menguji terhadap seseorang yang melakukan port-port scanner sebelum melakukan penyerangan terhadap target yang dituju.



Gambar 3. 21 scanning port

Pada gambar 3.17 menunjuka ilustrasi yang dilakukan oleh port scanner. Penyerang melakukan scanning port-port yang terbuka untuk melakukan penetrasi terhadap port-port tersebut.

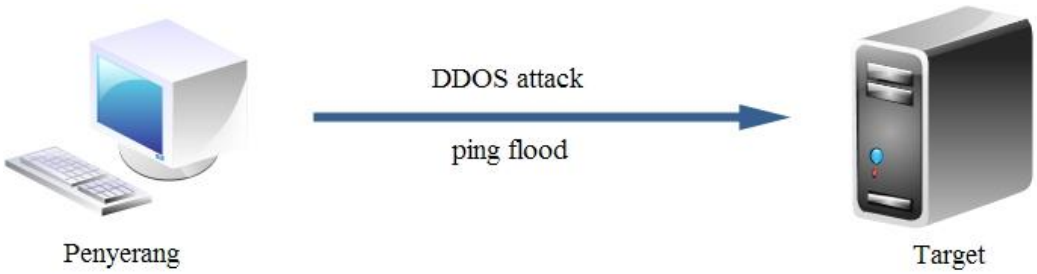
Pengujian dilakukan menggunakan skenario. Skenario tersebut dibuat dengan tujuan untuk membuktikan keamanan *VPN* dari port scanner.

Tabel 3. 8 Skenario pengujian ke 2

No	Server VPN	Waktu Penyerangan
1	Tidak menggunakan port knocking	Sebelum mengakses VPN
2	Menggunakan port knocking	Saat hendak mengakses VPN
3	Menggunakan port knocking	Ketika sudah terhubung VPN

3.2.3.3 Perancangan Pengujian DDOS Attack

Perancangan pengujian *DDOS Attack* dilakukan untuk menguji kemanan *VPN server* dari serangan pingflood.Pengujian dilakukan pada saat sebelum penerapan port knocking dan sesudah penerapan port knocking.



Gambar 3. 22 DDOS attack

Pada gambar 3.18 menunjukan ilustrasi yang dilakukan oleh penyerang yang melakukan serangan *DDOS pingflood*terhadap target yang dituju.

Pengujian dilakukan menggunakan skenario.Skenario tersebut dibuat dengan tujuan untuk membuktikan keamanan *VPN* dari port scanner.

Tabel 3. 9 Skenario pengujian ke 3

No	Server VPN	Waktu Penyerangan
1	Tidak menggunakan port knocking	Sebelum mengakses VPN
2	Menggunakan port knocking	Ketika sudah terhubung VPN