

IMPLEMENTASI MONITORING JARINGAN VPN PADA WEB DAN MAIL SERVER

Regian Andi N¹, Rinaldy Fadillah S², Mohamad Dawud P³, Roni Kriswanto⁴, Edi Pratama P⁵

¹6302100116, ²6302100181, ³6302090124, ⁴6302090100, ⁵6302090093

¹regianandi8@gmail.com, ²aldiefadillah@gmail.com, ³mohamad.dawud@gmail.com,
⁴roni.kriswanto@gmail.com, ⁵tama.191090@gmail.com

Abstrak

Permasalahan jaringan yang umum terjadi adalah menyediakan jalur yang tingkat ketersediaan tinggi. Hal ini tidak bisa dilakukan tanpa arsitektur jalur data. Load balancing merupakan salah satu metode untuk meningkatkan ketersediaan.

Virtual Private Network (VPN) merupakan sebuah teknologi yang memungkinkan adanya koneksi jaringan data *private* pada jaringan publik untuk menghubungkan antara *client* dan *server*. *VPN server* dibuat dengan menggunakan *router virtual* yang disebut *Pfsense*. *Pfsense* adalah sistem operasi *open source FreeBSD* yang dirancang sebagai *firewall* dan *router*. Tampilan yang sederhana dengan *web GUI administrator* memudahkan untuk menjaga sistem.

Kata Kunci : *Router, Pfsense dan Virtual Privat Network*

Abstract

A common problem in the network was providing a high level of availability. This can not be accomplished without modifying data bus architecture. Load balancing is one of many methods to increase the availability.

Virtual Private Network (VPN) is a technology which allows for a private data network connections on the public network to connect between client to server. *VPN server* are created using a virtual router called *Pfsense*. *Pfsense* is a *FreeBSD open source operating system* that is designed as a *firewall and router*. Simple display with *web GUI* makes it easy for administrator maintain the system.

Keywords: *Router, Pfsense dan Virtual Private Network.*

1. Pendahuluan

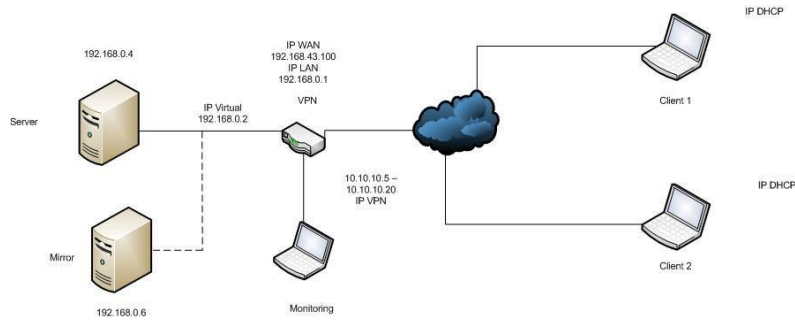
Masalah keamanan kemudahan dan kecepatan *transfer* (pertukaran data) adalah satu aspek yang penting dari suatu jaringan komunikasi terutama untuk perusahaan-perusahaan skala menengah keatas dan universitas teknologi internet dahulu digunakan oleh perusahaan-perusahaan dan universitas sebagai sebuah jaringan komunikasi yang terbuka yang dapat mengakses, berbagai dan menambah informasi semudah mungkin sehingga jatuhnya informasi yang bersifat rahasia dari satu perusahaan dan universitas kemungkinan besar bisa terjadi yang dapat menyebabkan kerugian bagi perusahaan dan universitas tersebut. Selain itu *transfer* (pertukaran data) yang awalnya melalui *hardcopy* berupa tulisan tangan, dokumen, laporan bulanan, melalui media *flaskdisk*, dan sebagainya, telah berkembang menjadi komunikasi menggunakan jaringan internet karena tuntutan waktu dan efisiensi.

Komunikasi data pada internet masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data) hal ini yang harus diperhatikan pemilik dan *administratorsystem* informasi suatu perusahaan dalam melakukan kegiatan di dunia internet, sehingga kerahasiaan informasi suatu perusahaan dan universitas bisa terjaga dengan baik dan kemudahan dan kecepatan (pertukaran data) bisa diimplementasikan menjadi nilai lebih yang bisa berpengaruh pada *cost* perusahaan dan universitas.

Secara umum VPN adalah suatu proses di mana jaringan umum (*public network* atau internet) diamankan untuk memfungsikan sebagai jaringan *private (private network)* sebuah VPN tidak didefinisikan sebagai rangkaian khusus atau rute, tetapi didefinisikan oleh mekanisme keamanan dan prosedur prosedur yang hanya mengizinkan pengguna yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya.

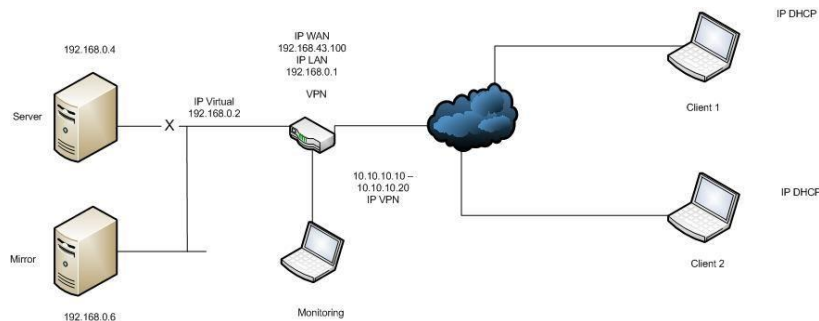
2. Simulasi Sistem

Untuk gambar simulasi dibawah ini menjelaskan tentang sistem kerja jaringan vpn yang dimana terdapat 1 server dan 1 mirror yang digunakan saat kondisi normal. Saat kondisi normal user yang telah terkoneksi dengan vpn akan mendapatkan hak akses untuk mengakses *Web* dan *Mail Server* yang telah disediakan dan mirror akan tidak akan dapat diakses.



Gambar3 1 Tampilan skenario kondisi normal

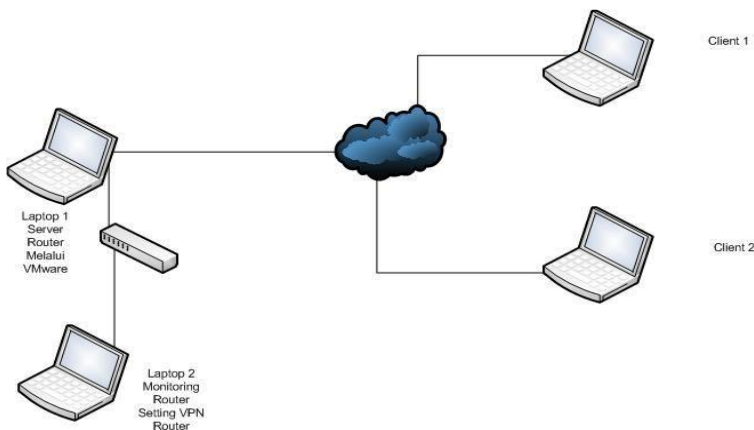
Untuk gambar simulasi dibawah, server akan dibuat down. Dan secara otomatis *user* yang mengakses server utama akan dialihkan ke server *mirror* yang telah ada.



Gambar3 2 Skenario Saat Server 1 Mati

1.1 Persiapan Perangkat

Simulasi yang dilakukan seperti gambar 3.3 Skenario yang berjalan. Dalam simulasi menggunakan 4 buah laptop yang mempunyai tugas berbeda. Laptop 1 berguna sebagai *router* sekaligus *server* yang berjalan di VMware. Laptop 2 berguna sebagai monitoring jaringan yang telah terhubung dengan laptop 1 menggunakan kabel UTP. Laptop 3 dan 4 terhubung dengan laptop 1 menggunakan jaringan internet yang tersedia. Untuk dapat mengakses server Laptop 1 dan 2 akan mendapatkan *user* dan *password* yang akan diberikan oleh Openvpn.



Gambar3 3 Skenario yang berjalan

Perangkat keras yang digunakan

1. 4 Buah Notebook
2. 1 Buah kabel Ethernet straight
3. Tablet Advan T1j sebagai tethering hotspot

Tabel 3 1 Spesifikasi Perangkat Keras

	Laptop 1		Laptop 2	Laptop 3	Laptop 4	Tablet
Device	Server (Virtual)	Router (Virtual)	Aspire 4750z	Ienovo S 206	Aspire One D270	Advan T1j
Processor	Shared Virtual	Shared Virtual	Intel Core	Dual Core 1.2 Ghz	Intel Atom 1.6 Ghz	ARM Cortex A7 DualCore – 1.3Ghz
Memory	1 Gb	256 Gb	2 Gb DDR 3	2 Gb	2 Gb DDR 3	512 Mb
Disk	20 Gb	20 Gb	500 Gb	320 Gb	320 Gb	2 Gb
Network 1	192.168.0.6	192.168.0.0	192.168.0.3	DHCP (Wireless)	DHCP (Wireless)	192.168.43.0
Network 2	192.168.0.4	192.168.43.0				

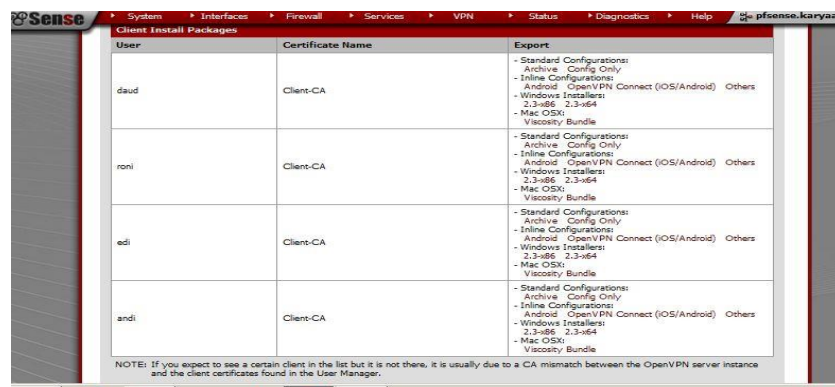
Perangkat Lunak Yang Digunakan

Tabel 3 2 Perangkat Lunak

No	Perangkat Lunak	Kegunaan
1	VM Ware 9.0	Virtual Machine
2	Ubuntu Server 12.04	OS Untuk Server
3	Linux Mint	OS Untuk Client 1
4	Windows 7 Ultimate	OS Untuk Client 2
5	Pfsense	Virtual Router
6	Apache	Web Server
7	Joomla	Web Server
8	Bind9	Mail Server
9	Squirrel Mail	Mail Server
10	Post Fix	Mail Server
11	Mozilla Firefox	Browser
12	Google Chrome	Browser

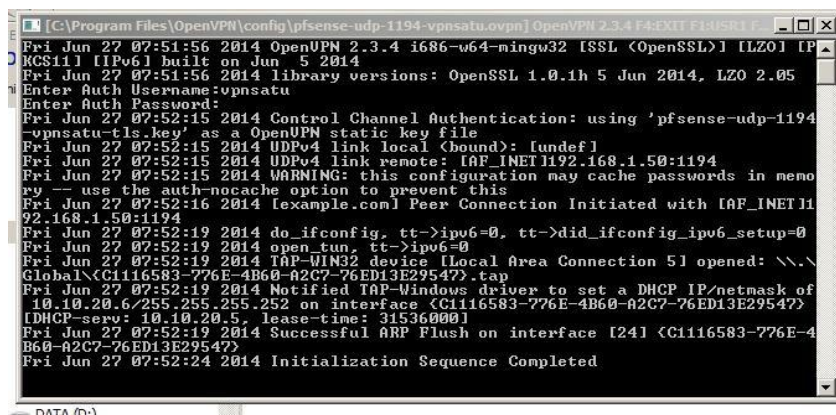
3.3 Simulasi Sistem

Sebelum *Client* dapat terhubung dengan server, *client* terlebih dahulu akan mendapat hak akses yang akan diberikan oleh Pfsense. Hak akses ini digunakan agar *client* dapat mengakses *web server* dan *mail server*. Apabila *client* tidak mendapat hak akses maka *client* tidak dapat mengakses *server* yang telah disediakan. Untuk mendapatkannya *admin* membuka VPN-Openvpn-client install packages, kemudian export nama client yang sudah dibuat.



Gambar3 4 Tampilan packages router

Dalam melakukan simulasi client menggunakan browser Mozilla firefox dan Google Chrome. Untuk pertama kali *Client* terkoneksi terlebih dahulu ke jaringan VPN. Untuk dapat mengakses jaringan VPN *Client* terlebih dahulu menginstall Openvpn untuk windows. Hasil dari membuka Openvpn akan terlihat seperti gambar



Gambar3 5 Client Terkoneksi dengan VPN untuk Windows

Untuk *Client 2* untuk terhubung langsung ke dalam VPN *Client* tidak perlu menginstall Openvpn terlebih. *Client* bisa membuka langsung lewat dari terminal

```

Terminal
urang@neva ~-/Documents/pfsense-udp-1194-daud $ sudo openvpn pfsense-udp-1194-daud.ovpn
Wed Jul 2 13:59:34 2014 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11]
[eurephia] [MH] [IPv6] built on Feb  4 2014
Enter Auth Username:daud
Enter Auth Password:
Wed Jul 2 13:59:38 2014 WARNING: file 'pfsense-udp-1194-daud.p12' is group or others accessible
Wed Jul 2 13:59:38 2014 WARNING: file 'pfsense-udp-1194-daud-tls.key' is group or others accessible
Wed Jul 2 13:59:38 2014 Control Channel Authentication: using 'pfsense-udp-1194-daud-tls.key'
as a OpenVPN static key file
Wed Jul 2 13:59:38 2014 UDPv4 link local (bound): [undef]
Wed Jul 2 13:59:38 2014 UDPv4 link remote: [AF_INET]192.168.43.100:1194
Wed Jul 2 13:59:38 2014 WARNING: this configuration may cache passwords in memory -- use the
auth-nocache option to prevent this
Wed Jul 2 14:00:01 2014 [www.tass.com] Peer Connection Initiated with [AF_INET]192.168.43.100:1194
Wed Jul 2 14:00:03 2014 TUN/TAP device tun0 opened
Wed Jul 2 14:00:03 2014 do ifconfig, tt->ipv6=0, tt->did ifconfig ipv6_setup=0
Wed Jul 2 14:00:03 2014 /sbin/ip link set dev tun0 up mtu 1500
Wed Jul 2 14:00:03 2014 /sbin/ip addr add dev tun0 local 10.10.10.6 peer 10.10.10.5
RTNETLINK answers: File exists
Wed Jul 2 14:00:04 2014 ERROR: Linux route add command failed: external program exited with error
status: 2
Wed Jul 2 14:00:04 2014 Initialization Sequence Completed

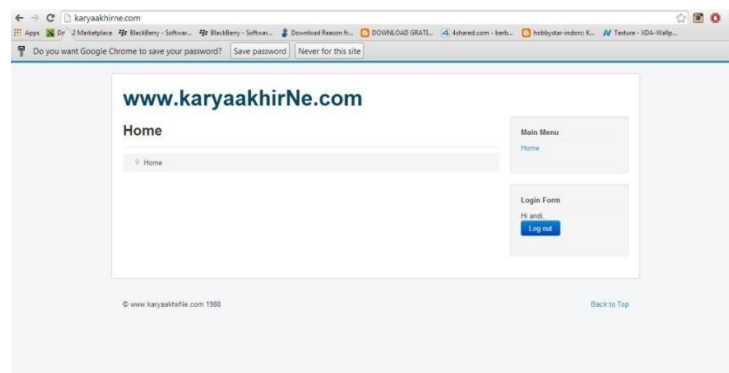
```

Gambar3 6 Client terkoneksi dengan VPN lewat Linux Mint

Dalam melakukan simulasi *client* yang telah terhubung *client* bisa menjadi *administrator* untuk *web server* dan *mail server*. Selain dari hal tersebut *client* bisa melakukan monitoring jaringan melalui pfsense. Seperti gambar 3.5 *client* yang telah mendapat hak akses dapat menggunakan membuka *web server joomla* dan sisi *client*. *Joomla* digunakan dikarenakan karena konfigurasi yang lebih mudah dan telah berbasis *web*. Di sisi *joomla client* bisa mendaftar menjadi user seperti gambar 3.6



Gambar3 7 Tampilan Joomla Administrator

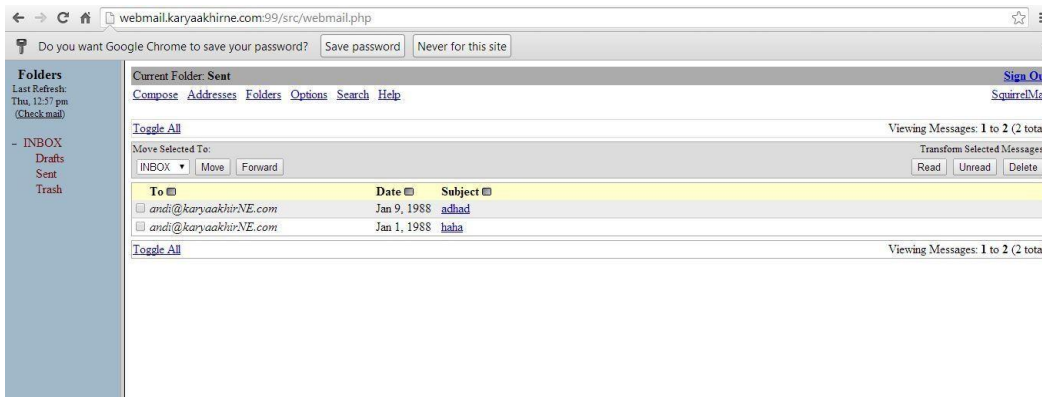


Gambar3 8 Tampilan Joomla User

Selain menggunakan *web server* ada juga *mail server* yang bisa diakses oleh *client*. Untuk *mail server* yang digunakan adalah *squirrelmail* seperti gambar 3.7. *Squirrelmail* digunakan dikarenakan telah berbasis web dan tidak membutuhkan *syntax* yang panjang. Seperti halnya pada *joomla*, pertama-tama *client* harus membuat username terlebih dahulu untuk dapat mengakses *squirrelmail*. Dalam gambar 3.8 *usernama* telah dibuat dan dapat membuka

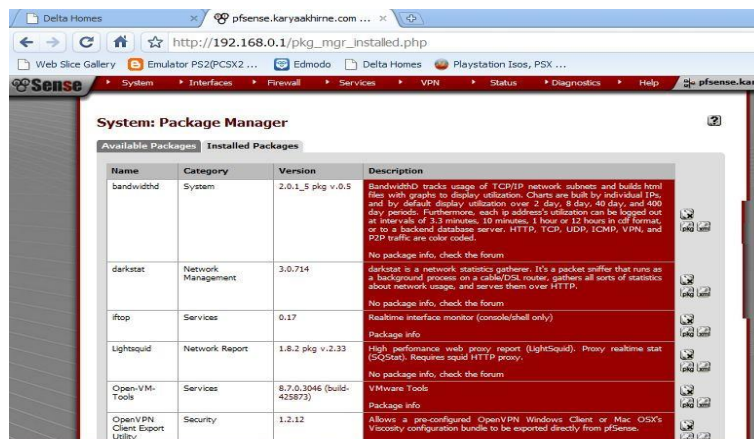


Gambar3 9 Tampilan SquirrelMail



Gambar3 10 Tampilan User SquirrelMail

Penggunaan *virtual router* mempunyai peran yang sangat penting dalam membangun sebuah jaringan, dalam hal ini penggunaan pfsense sebagai *virtual router* mempunyai banyak kegunaan pfsense mempunyai banyak *source* yang bisa dapat digunakan. Mulai dari konfigurasi VPN, *routing table*, dan monitoring dapat dilakukan dalam pfsense. Akan tetapi untuk dapat menggunakan *source* yang ada di pfsense pertama-tama *admin* harus menambah packet yang akan digunakan seperti *openvpn*, *darkstat*, dan *vnstat*. Masing-masing *packet* mempunyai kegunaan masing-masing. *Openvpn* berguna dalam melakukan *instalasi* VPN. *Darkstat* dan *vnstat* berguna dalam melakukan monitoring jaringan. Seperti tampak pada gambar 3.9 beberapa paketyang telah terinstall.



Gambar3 11 Tampil paket yang telah terinstall di pfsense

Ucapan Terima Kasih

Assalamu'alaikum Warahmatullahi Wabarakaatuh

Puji dan Syukur kami panjatkan ke Hadirat Tuhan Yang Maha Esa, karena berkat limpahan Rahmat dan Karunia-nya sehingga kami dapat menyusun Karya Akhir ini dengan baik dan tepat pada waktunya. Dalam Karya Akhir ini yang berjudul "**Implementasi Monitoring Jaringan VPN Pada Web dan Mail Server**" dengan segala kelebihan maupun kekurangannya. Tidak lupa shalawat dan salam selalu kita limpahkan pada junjungan Baginda Rasulullah Muhammad SAW beserta keluarga, para sahabat.

Karya Akhir ini dibuat dalam rangka memenuhi salah satu syarat untuk menyelesaikan Program Diploma-3 Program Studi Teknik Komputer Telkom Aplied and Science School.

Penyusunan Karya Akhir ini tidak terlepas dari dukungan, doa, dan bantuan banyak pihak, baik moril maupun materil. Maka pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Seluruh keluarga tercinta, atas segala doanya, dukungan moril, memberikan kasih sayang dan materil.
2. Untuk Teman ku, Amri yang telah memberikan dukungan dan pelatihan akhirnya bisa terselesaikan Karya Akhir ini.
3. Kepada Bapak Periyadi, ST, selaku pembimbing atas segala bimbingan dan motivasi yang selalu diberikan sehingga penulis dapat menyelesaikan Karya Akhir ini.

Penulis Menyadari Bahwa dalam Pengerjaan Karya Akhir ini masih banyak kekurangannya, oleh karena itu penulis mengharapkan kritik dan saran dari para pembaca agar dapat dijadikan sebagai perbaikan dan penyempurnaan Karya Akhir ini.

Akhir kata penulis mengucapkan terima kasih.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh

Daftar Pustaka

- 1) Chris Buechler and Scott Ullrich,(2004), *Pfsense. Electric Sheep Fencing, LLC*
- 2) Alfaqih, Muhammad iiq (2010). *Implementasi Load Balancing dan Manajemen Bandwidth Dengan Menggunakan Satu Mesin Vyatta Router OS*. Bandung. Karya Akhir
- 3) Sucipto, (2013). *From Membuat-virtual-host-di-apache2-dengan-port-berbeda*, 2 Juli 2014
- 4) Al-Atsary, Riz. *From : www.slideshare.net/ziRRiz/Tutorial-mudah-membuat-server-email-postfix-dovecot-squirrelmailubuntu-server-1204*, 2 Juli 2014
- 5) Ubuntu Server Guide, 2014. <http://ubuntuserverguide.com/2012/10/how-to-installing-cms-joomla-3-0-on-ubuntu-server-12-04.html>, 8 Juli 2014
- 6) Rizal, 2013. <http://rizalubuntu.blogspot.com/2013/08/clustering-failover-untuk-web-server.html>, 8 Juli 2014
- 7) Cemun, 2012. <http://cemun.wordpress.com/2012/05/28/membuat-replicationmirroring-websserver-secara-otomatis-di-ubuntu/>. 8 Juli 2014