KAJIAN IP VIRTUAL *(VIRTUAL SERVER)* TERHADAP KEAMANAN JARINGAN

Felix Wuryo Handono
Program Studi Manajemen Informatika
AMIK BSI Jakarta
Jl. Kramat Raya No.18 Jakarta Pusat, Indonesia
felix@bsi.ac.id

ABSTRACT

The large number of Internet users has made the business people expand their business network with a wide variety of products or packages offered to the users of Internet services. Including, network security systems and infrastructure, hire a data center with costs less Infrastructure financing, easier management of servers in the cloud, DRC (Disaster Recovery Center), ease of backup server in the event of a crash or constraints, and much more. The rapid growth of the internet industry in addition to increasing competition among businesses has also become the target of the search for security holes such data retrieval, data of customers or transactions, vandalism system to network flooding. Good anticipation needed to handle various security problems mentioned above. Utilization of the network infrastructure configuration using virtual IP can be used to reduce one of securities gap.

Keyword: Internet users, infrastructure, security, virtual IP

I. PENDAHULUAN

Berdasarkan data yang diperoleh dari kemenkominfo melalui situs antara.com bahwa jumlah pengguna internet di Indonesia pada survey tahun 2013 sebesar 71,19 juta jiwa yang naik sekitar 13 persen dibanding jumlah pengguna pada tahun 2012 sebanyak 63 juta. Menunjukan bahwa di Indonesia sendiri perkembangan penggunaan internet terus mengalami kenaikan, dan akan terus bertambah jika didukung terus oleh partisipasi pemerintah dalam membangun infrastruktur jaringan di Indonesia.

Perkembangan internet tidak hanya dipergunakan untuk semata-mata mendapatkan akses informasi, pertukaran data, transaksi dan bisnis menjadikan internet sebagai media yang paling mudah dan cepat yang dapat digunakan manfaatnya. Tidak lagi harus dilakukan secara konvensional dan melakukan perjalanan namun semua kemudahan akses tersebut dapat dilakukan cukup hanya mengkoneksikan perangkat komputer dan kemudian akan terhubung dengan jaringan diseluruh dunia.

Pemanfaatan akses penggunaan internet dapat dilakukan melalui media yang universal, mulai dari telepon genggam, tablet, laptop hingga perangkat standard PC. Kemudahan akses dari beragam perangkat mobile pun membuat pengguna dapat kapan saja melakukan akses dan terhubung ke internet.

Dengan beberapa kemudahan yang ingin diperoleh dan didapat, tentunya sebagai penggiat internet yang mengerti manfaatnya, akan meng-ekspansi segala bentuk kegiatan bisnis dan data kedalamnya.

Dibutuhkan pembangunan aplikasi, web dan infrastruktur jaringan maupun server untuk meletakan penghubung antara pengguna/pengakses dengan pemberi layanan. Dengan kemampuan masyarakat saat ini, para pembuat program, designer, network dan system engineer dapat dicari dan diberdayakan.

Setelah semuanya terhubung, yang tidak kalah pentingnya adalah keamanan data dari si pengakses maupun data pemilik. Data transaksi pembelian, dana nasabah atau pelanggan, kartu kredit, asuransi, dan lain sebagainya yang harus dijaga kerahasiannya. Data tersebut merupakan data penting yang tidak sembarang orang boleh meng-aksesnya. Namun siapa yang tahu bahwa dari sekian banyak orang yang mengakses ada kemungkinan banyak yang akan mencoba untuk membajak atau mendapatkan data-data tersebut, merubah atau menghilangkannya.

Bagi seorang yang mengerti akan permasalahan tersebut, tentu mereka akan melakukan pengamanan seperti backup data, pemasangan *firewall* dan lainnya. Salah satu cara untuk memberikan pengamanan data

adalah dengan melakukan virtualisasi ip dari ip-ip perangkat server maupun jaringan agar perangkat tersebut tidak mengalami serangan langsung dari luar atau *hacker*.

II. TINJAUAN PUSTAKA

A. Internet (interconnection-networking)

Adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global *Transmission Control Protocol/Internet Protocol Suite (TCP/IP)* sebagai protokol pertukaran paket *(packet switching communication protocol)* untuk melayani miliaran pengguna di seluruh dunia. Internet merupakan sekumpulan jaringan yang terhubung satu dengan lainnya, dimana jaringan menyediakan sambungan menuju global informasi. Sutedjo et al. (2013:117).

IP address merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tanda titik pada setiap 8bitnya. Berikut contoh alamat ip dengan pengalamatan 32 bitnya. Sopandi (2008:63).
IP 192.168.0.1
Bit
11000000.10100000.00000000.00000001

Jaringan komputer adalah sekumpulan komputer individu yang dihubungkan satu dengan lainnya menggunakan protokol *transmission control protocol* atau internet protocol (TCP/IP). Sutedjo et al. (2008:115)

B. Keamanan Jaringan

Adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer (jaringankomputer.org/keamanan-jaringan-komputer/, 24 November 2015).
Garfinkel (2011): bahwa keamanan komputer melingkupi empat aspek, yaitu:

1. *Privacy*
   Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
2. *Integrity*
   Informasi tidak boleh diubah tanpa seijin pemilik informasi
3. *Authentication*
   Metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.
4. *Avaibility*
   Ketersediaan hubungan dengan ketersediaan informasi ketika dibutuhkan.

C. Server

Adalah sebuah system komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan system operasi khusus yang disebut sebagai system operasi jaringan atau network operating system. Server juga menjalankan perangkat lunak *administrative* yang mengontrol akses terhadap jaringan dari sumber daya yang terdapat didalamnya, seperti halnya berkas atau alat pencetak, dan memberikan akses kepada *workstation* anggota jaringan. (technopark.surakarta.go.id, 2015)
Jadi secara umum, server dengan system operasi jaringan, menjalankan aplikasi yang memiliki arsitektur *client-server*.

Ada beberapa macam aplikasi server, diantaranya: http, ftp, dhcp, database, mail, proxy dan masih banyak lagi. Penggunaan aplikasi server disesuaikan dengan kebutuhan penggunaannya.

D. IP Virtual

Sebuah IP *Virtual* (IPV) memetakan satu alamat IP eksternal dan satu port eksternal menjadi sejumlah beberapa alamat IP dan port. IPV juga dapat menerjemahkan port eksternal ke port internal yang berbeda. IPV memberikan peta lalu lintas yang diterima di salah satu alamat IP ke alamat lain berdasarkan nomor port tujuan dalam header segmen TCP atau UDP. (kb.juniper.net, 2015)

III. METODE PENELITIAN

Penelitian menggunakan pendekatan kualitatif dengan analisis deskriptif, yaitu mencatat dan menggambarkan secara teliti fenomena yang ditemukan di lapangan, dalam hal ini teknologi *Virtual Server* itu sendiri yang dibangun menggunakan mesin virtual. Peneliti mengamati objek penelitian secara langsung untuk melakukan interpretasi data, sekaligus memilih alat penguji sebagai sumber data dan melakukan penilaian kualitas data, menafsirkan serta membuat kesimpulan atas temuan pengujian. Penguji menggunakan metode ini berdasar perkembangan teknologi informasi khusunya infrastruktur jaringan komputer yang menjadi pondasi dasar berjalannya

system pada teknologi jaringan. Analisa dilakukan dengan membandingkan hasil temuan yang diperoleh penguji dengan beberapa aspek pada artikel atau jurnal yang mendeskripsikan tentang keamanan jaringan komputer.

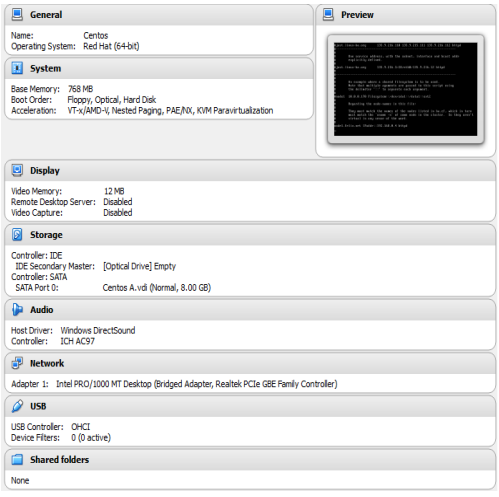
IV. PEMBAHASAN

A. Analisis Permasalahan dan Kebutuhan

Ketika membuka sebuah portal untuk dapat diakses memiliki resiko bahwa portal tersebut hingga data yang terdapat didalamnya dapat saja diretas, dirubah ataupun dihapus. Menjadi kekhawatiran tersendiri apabila hal tersebut terjadi dan bukannya tidak mungkin karena hak akses yang kita berikan dapat diakses oleh banyak sekali pengguna internet yang kita sendiri tidak mengetahui *track-record* pengguna tersebut. Untuk itu dibutuhkan pendukung untuk memberikan keamanan dan kenyamanan terhadap pengguna internet agar data yang terdapat didalamnya adalah data yang benar.

Penelitian menggunakan 2 perangkat virtual mewakili 2 perangkat server standard yang digunakan menggunakan system operasi linux (centos).
Berikut spesifikasi perangkat yang digunakan untuk pengujian:

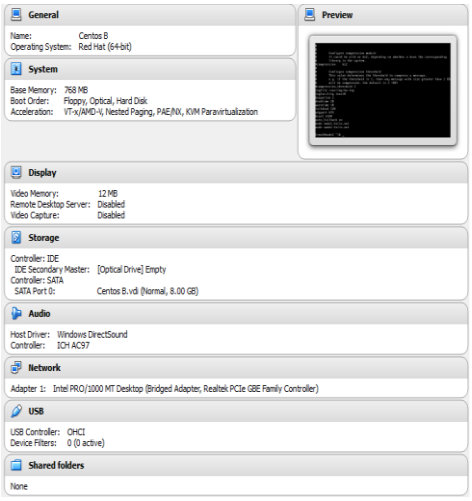
1. Server1 (node1)



Sumber: Hasil Penelitian (2015)

Gambar 1. Spesifikasi server1 (node1)

2. Server2 (node2)

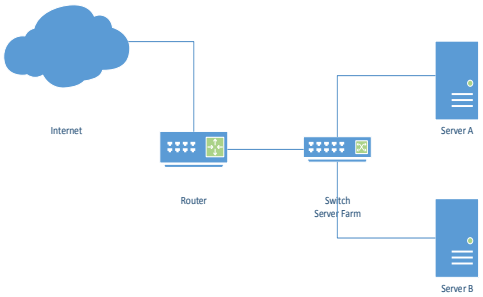


Sumber: Hasil Penelitian (2015)

Gambar 2. Spesifikasi server2 (node2)

B. Desain Topologi

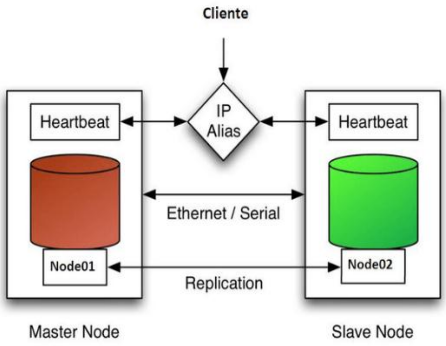
Berikut desain topologi standard yang umum digunakan untuk infrastruktur server.



Sumber: Hasil Penelitian (2015)

Gambar 3. Desain Topologi Jaringan Server

Pengguna internet dapat mengakses internet melalui media apapun kemudian mengakses server yang terdapat didalam sebuah jaringan. Jaringan terdiri dari sebuah perangkat *Router*, *Switch* dan Server yang hendak dituju.
Untuk instalasi virtual server, peneliti menggunakan acuan seperti dibawah ini:



Sumber: http://www.karloscetina.com, 2015

Gambar 4. Topologi IP Virtual atau Virtual Server

Diatas adalah desain service yang akan ditempatkan/dikonfigur pada server dengan menerapkan IP *Virtual* sehingga perangkat server tidak langsung berhubungan dengan end user.

Berikut table IP yang digunakan untuk implementasi *Virtual Server*

Tabel I. Tabel IP Address

NO	Perangkat	IP	OS	Service
1	Server A	172.16.0.2/24	Centos	Httpd, heartbeat
2	Server B	172.16.0.3/24	Centos	Httpd, heartbeat
3	Virtual Server	172.16.0.4/24	-	-

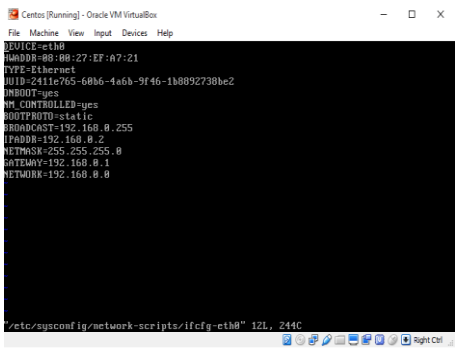
Sumber: Hasil Penelitian (2015)

C. Implementasi IP Virtual/Virtual Server

Web Server A

Beberapa konfigurasi yang dilakukan diantaranya:

1. *Network*



Sumber: Hasil Penelitian (2015)

Gambar 5. Konfigurasi server1 (node1)

2. Httpd.conf (/etc/httpd/conf/httpd.conf)
   Berikut beberapa hal yang dirubah:
   ServerAdmin root@192.168.0.2
   ServerName 192.168.0.2:80
   DirectoryIndex index.html index.htm
3. Index.html (/var/www/html/index.html)
   Membuat isi halaman web
   isi dengan
   <html><head>
   <title>Web Server A</title>
   <body><h1>Hai, anda mengakses web server A</h1></body>
   </head></html>

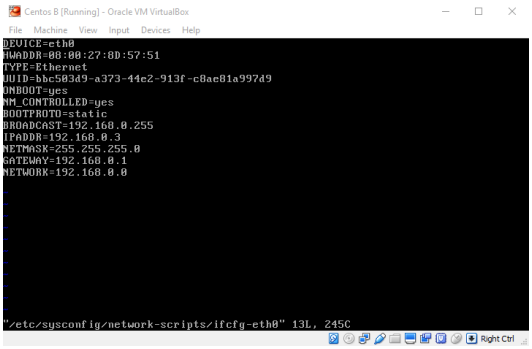
Sumber: Hasil Penelitian (2015)

Gambar 6. Tampilan browser yang mengakses server1 (node1)

Web Server B

Beberapa konfigurasi yang dilakukan diantaranya:

1. *Network*



Sumber: Hasil Penelitian (2015)

Gambar 7. Konfigurasi server2 (node2)

2. Httpd.conf (/etc/httpd/conf/httpd.conf)
   Berikut beberapa hal yang dirubah:
   ServerAdmin root@192.168.0.3
   ServerName 192.168.0.3:80
   DirectoryIndex index.html index.htm
3. Index.html (/var/www/html/index.html)
   Membuat isi halaman web
   isi dengan
   <html><head>
   <title>Web Server B</title>
   <body><h1>Hai, anda mengakses web server B</h1></body>
   </head></html>

Sumber: Olahan Penelitian

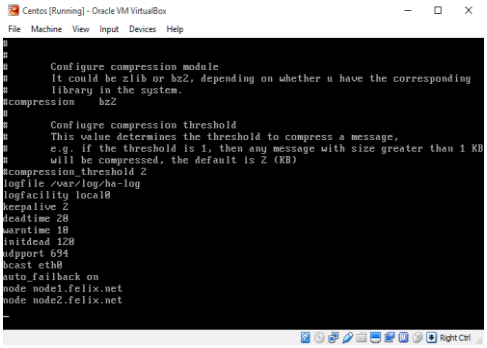
Gambar 8. Tampilan browser yang meng-akses server2 (node2)

Virtual Server

Beberapa konfigurasi yang dilakukan diantaranya:

1. Install heartbeat
   Heartbeat adalah *daemon* yang menyediakan infrastruktur cluster (komunikasi dan keanggotaan) layanan kepada klien. Hal ini memungkinkan klien untuk mengetahui tentang keberadaan (atau hilangnya!) dari proses peer pada mesin lain dan dengan mudah bertukar pesan dengan mereka. (linux-ha.org)
2. Konfigurasi tiga file yang terdiri dari ha.cf, authkeys, dan haresources

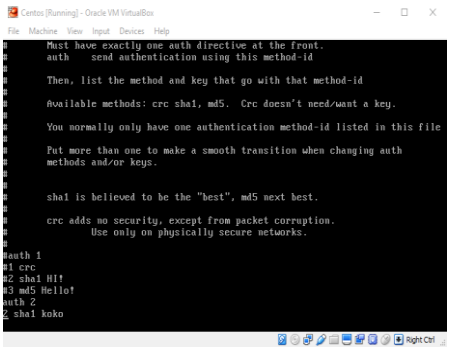
a. Ha.cf
   File ha.cf adalah salah satu file yang penting ketika melakukan konfigurasi Heartbeat. Didalamnya terdapat daftar node cluster, topologi komunikasi, dan fitur yang diaktifkan. (linux-ha.org)



Sumber: Hasil Penelitian (2015)

Gambar 9. Konfigurasi file ha.cf pada server1 (node1)

b. Authkeys
   file ini berisi kunci untuk otentikasi node bersama.

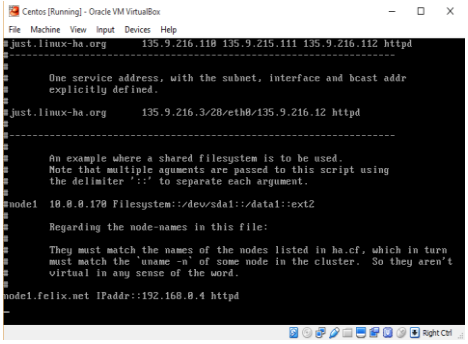


Sumber: Olahan Penelitian

Gambar 10. Konfigurasi file authkeys pada server1 (node1)

"koko" adalah kunci atau password yang digunakan untuk autentikasi.

c. Haresources
   Haresources digunakan untuk menentukan node server yang aktif, sementara lainnya adalah pasif.

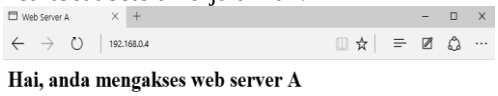


Sumber: Hasil Penelitian (2015)

Gambar 11. Konfigurasi file haresources pada server1 (node1)

Berdasarkan konfigurasi diatas, maka node yang aktif adalah node1.
Lakukan peng-kopian ketiga file tersebut diatas ke node1.

Dan berikut adalah hasil konfigurasi heartbeat setelah dijalankan.



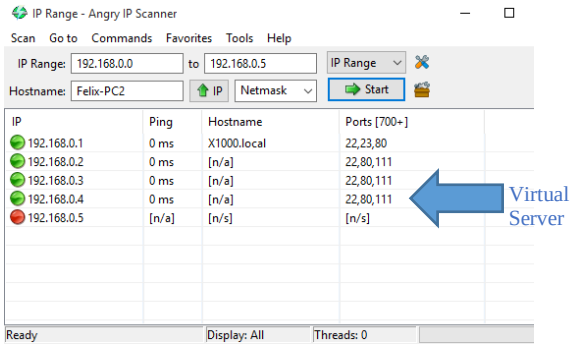
Sumber: Olahan Penelitian

Gambar 12. Tampilan pada browser yang meng-akses virtual server

Hasil pada gambar menunjukkan bahwa *virtual server* mengarah kepada node1, hal ini terkait pada konfigurasi pada file haresources. Virtual server akan mengarah

ke node2 jika pada file tersebut, node aktif yang dimasukkan dalam konfigurasi adalah node2.

D. Pengujian IP dan Port



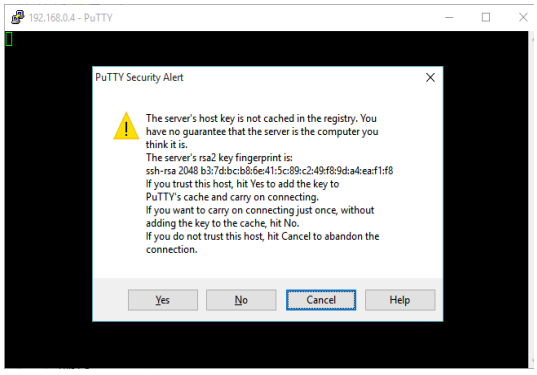
Sumber: Olahan Penelitian

Gambar 13. Hasil pengetesan port-IP pada jaringan

Berdasar hasil pengetesan terhadap ip dan *port* pada jaringan, didapat bahwa virtual server dapat dideteksi dan memiliki konfigurasi port yang sama dengan port server asli pada node1 dan node2.

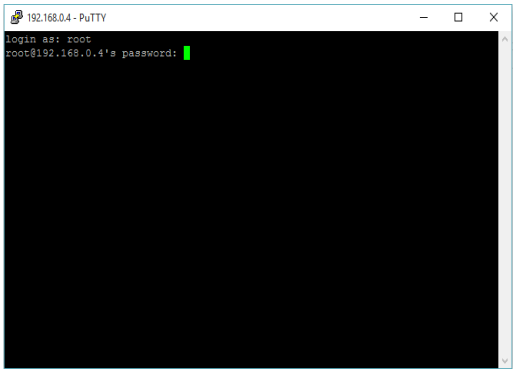
E. Pengujian Akses Server

Pengujian menggunakan aplikasi PuTTy dengan meng-akses server *virtual* menggunakan *SSH (Secure Shell) port* 22.



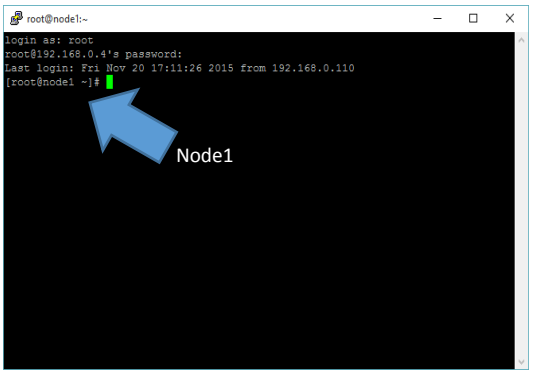
Sumber: Hasil Penelitian (2015)

Gambar 14. Akses Sistem Operasi Jaringan Virtual Server dengan PutTTy



Sumber: Hasil Penelitian (2015)

Gambar 15. Akses Root Sistem Operasi Jaringan Virtual Server



Sumber: Hasil Penelitian (2015)

Gambar 16. Login Virtual Server berhasil me-remote root server node1

Hasil uji akses *SSH* menunjukkan bahwa system operasi yang diakses mengarah kepada sistem operasi jaringan pada node1, ini menunjukkan bahwa *virtual* server aktif merujuk pada node1 sesuai konfigurasi pada file haresources

Berdasar hasil beberapa pengujian diatas, didapat:

1. *Virtual* Server menampilkan data yang sama yang dimiliki oleh server aktif, ditampilkan pada browser sesuai hasil *running test* pada *service heartbeat.*
2. Untuk dapat mengakses *Virtual* Server, diperlukan hak akses yang sama terhadap hak akses baik pada node1 maupun node2. Virtual Server tidak dapat diakses jika tidak memiliki hak akses pada node aktif.
3. *Virtual* Server menggunakan autentifikasi terhadap masing-masing node, sehingga hanya node-node yang memiliki kode autentifikasi yang sama

sajalah yang dapat berkomunikasi dan dijalankan.

4. Karena Virtual Server menjalankan node aktif, maka isi data maupun informasi yang ditampilkan pada Virtual Server adalah sama dengan isi data maupun informasi pada node aktif, sehingga ketersediaan data dan informasi pada Virtual Server tetap terjaga.

IV. PENUTUP

A. Kesimpulan

Dari hasil penerapan virtual server diatas, didapat kesimpulan bahwa *Virtual Server* memenuhi empat aspek keamanan jaringan yakni:

1. *Privacy*
   Virtual server tetap menjaga informasi yang dimiliki server asli, sesuai karena memiliki pengaturan hak akses yang sama dengan server asli.
2. *Integrity*
   Untuk merubah system, virtual server hanya dapat diakses oleh si pemilik system karena memiliki system keamanan yang sama seperti server asli yang dikonfigurasi.
3. *Authentication*
   Virtual server menggunakan authentication key untuk menghubungkan dua server yang dimaksud atau dituju. Sehingga hanya server yang benar dan dibutuhkan saja yang dihubungkan.
4. *Avaibility*
   Virtual server tetap memberikan ketersediaan informasi dari server asli saat dibutuhkan.

B. Saran

Berdasarkan hasil penelitian dan kesimpulan diatas, beberapa hal dapat kami sarankan ialah:

1. Lakukan replikasi server terhadap data atau informasi sehingga baik data pada node1 maupun node2 sama.
2. Selain penggunaan port dan user akses, penggunaan iptables pada server dapat dimanfaatkan untuk pembatasan akses user maupun administrator baik dari jaringan luar maupun dalam.
3. Penggunaan ip virtual dengan heartbeat memiliki keterbatasan penggunaan resource server, sebaiknya kedepan penggunaan server dapat dibagi kesemua server sehingga dapat membagi jumlah concurrent user yang masuk.
4. Penulisan jurnal ini kedepan dapat digunakan sebagai acuan penulisan tentang penggunaan server secara bersamaan.

DAFTAR PUSTAKA

Garfinkel, Simson, Gene Spafford, Alan Schwartz. 2011. *Practical UNIX and Internet Security, 3rd Edition. Safari Books Online*: O'reilly Media

http://www.antaranews.com/berita/414167/apjii-penguna-internet-di-indonesia-terus-meningkat, 27 November 2015

http://www.karloscetina.com/, 27 November 2015

jaringankomputer.org/keamanan-jaringan-komputer/, 24 November 2015

kb.juniper.net/InfoCenter/Index?page=content&id=KB4751&actp=search, 25 November 2015

Sopandi, Dede. 2008. Instalasi dan konfigurasi jaringan computer, dede sopandi. Bandung: Informatika

Sutedjo, Budi SD, Dharmo Oetomo, Wibowo Esther, Eddy Hartono, Samuel Prakoso. 2013 Tahun. Pengantar Teknologi Informasi Internet, Konsep dan Aplikasi. Jogjakarta: Andi.

technopark.surakarta.go.id/id/media-ublik/computer-teknologi-informasi/188-definisi-client-server, 25 November 2015