SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI KOHA DENGAN GNS3

Tanjaya Jason Winata [1] Richard Souwiko [2] Jason Sutanto [3]

[1) 2) 3)] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara
Jln. Letjen S. Parman No. 1, Jakarta, 11440, Indonesia
Email : [1)]tanjaya.535220041@stu.untar.ac.id, [2)]richard.535220042@stu.untar.ac.id, [3)]jason.535220052@stu.untar.ac.id

ABSTRAK

Penelitian ini bertujuan untuk mensimulasikan sistem terdistribusi Koha pada perpustakaan konvensional dengan menggunakan GNS3. Mengingat sebagian besar perpustakaan saat ini masih mengelola koleksinya secara tradisional, penelitian ini bertujuan untuk mengintegrasikan teknologi dengan sistem perpustakaan konvensional. Melalui simulasi ini, diharapkan dapat mengembangkan solusi terdistribusi yang efisien untuk membantu perpustakaan dalam kegiatan operasional sehari-hari, termasuk katalogisasi, peminjaman, pengembalian, dan pelacakan inventaris. Penelitian ini menggunakan metode deskriptif. Metode ini dipilih untuk memberikan gambaran yang akurat dan terperinci mengenai implementasi Integrated Library System di perpustakaan konvensional. Berdasarkan hasil simulasi, didapatkan bahwa WebClient pada bagian luar, Web Server dan KohaServer pada bagian DMZ dapat berjalan dengan baik. Web Server dan KohaServer untuk klien dapat diakses melalui browser pada WebClient sedangkan KohaServer untuk staff dapat diakses langsung melalui browser pada KohaServer.

Kata Kunci

GNS3, Integrated Library System, Koha, Konvensional

1. Pendahuluan

Saat ini, perkembangan ilmu pengetahuan dan teknologi sudah sangat melekat pada setiap sendi kehidupan masyarakat. Teknologi-teknologi tersebut ditujukan untuk mempermudah kegiatan dan pekerjaan yang kita lakukan. *Integrated Library System* (ILS) merupakan salah satu contoh perkembangan teknologi di bidang pendidikan. *Integrated Library System* "ILS" atau Sistem Perpustakaan Terintegrasi atau disebut juga Sistem Otomasi Perpustakaan merupakan penerapan suatu sistem berupa perangkat lunak yang digunakan pada perpustakaan untuk keperluan pengelolaan, pengadaan, pembuatan katalog, dan layanan distribusi [1].

Penelitian ini bertujuan untuk melakukan simulasi sistem terdistribusi Koha pada perpustakaan konvensional dengan menggunakan GNS3. Mengingat bahwa sebagian besar perpustakaan saat ini masih mengelola koleksi mereka secara tradisional, penelitian ini bertujuan untuk mengintegrasikan teknologi dengan sistem perpustakaan yang konvensional. Melalui simulasi ini, diharapkan dapat dikembangkan solusi terdistribusi yang efisien untuk membantu perpustakaan dalam operasi harian mereka, termasuk katalogisasi, peminjaman, pengembalian, dan pelacakan inventaris. Selain itu, dengan menerapkan teknologi terdistribusi pada perpustakaan konvensional, diharapkan dapat meningkatkan efisiensi dan ketersediaan informasi.

Penelitian ini menggunakan metode deskriptif. Metode ini dipilih untuk memberikan gambaran yang akurat dan rinci tentang implementasi ILS pada perpustakaan konvensional. Penelitian ini diharapkan dapat mendorong penelitian lebih lanjut dan mendorong kemajuan teknologi, terutama di bidang pendidikan.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Jaringan komputer adalah suatu sistem yang menghubungkan beberapa komputer untuk saling bertukar informasi dan sumber daya. Ketika komputer dan perangkat lain saling terhubung, pengguna dapat berkomunikasi dengan lebih mudah [2]. Fungsinya tentu saja untuk memudahkan pekerjaan sehari-hari pengguna.

Keamanan jaringan bertugas melindungi perangkat keras dan perangkat lunak. Sistem ini menargetkan berbagai macam ancaman *cyber* dan mencegah ancaman tersebut memasuki jaringan pengguna. Dengan kata lain, keamanan jaringan adalah seperangkat aturan dan konfigurasi yang dirancang untuk meningkatkan perlindungan jaringan komputer [3].

Beberapa teknologi jaringan yang akan diterapkan dalam simulasi *Integrated Library System* pada website perpustakaan digital meliputi:

1. *Subnetting* adalah Teknik membagi alamat IP jaringan menjadi dua atau lebih jaringan yang lebih kecil dan terpisah [4]. Hal ini dapat membantu meningkatkan efisiensi jaringan dan memudahkan manajemen alamat IP.
2. *Network Address Translation* (NAT) adalah teknologi yang digunakan untuk mengubah alamat IP sumber dan tujuan dalam paket data yang melewati *router* [3]. NAT dapat membantu melindungi jaringan dari serangan dan memungkinkan beberapa perangkat untuk berbagi satu alamat IP publik.
3. *Transport Protocol* adalah protokol yang digunakan untuk mengatur pengiriman data antara perangkat dalam jaringan [5]. *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) adalah dua jenis *Transport Protocol* yang umum digunakan.
4. *Application Services* adalah protokol yang digunakan untuk mengatur komunikasi antara aplikasi yang berjalan pada perangkat dalam jaringan [5]. Beberapa contoh protokol *Application Services* yaitu *Hypertext Transfer Protocol* (HTTP) dan *File Transfer Protocol* (FTP).
5. *Virtual Private Network* (VPN) adalah sistem keamanan yang dirancang untuk melindungi informasi pribadi pengguna saat menjelajahi internet. Cara kerjanya adalah dengan mengenkripsi koneksi dari *endpoint* ke jaringan di internet [3].
6. *Firewall* adalah sistem keamanan yang mencegah jaringan luar dan ancaman memasuki komputer pengguna. Sistem keamanan ini paling banyak ditemukan pada *Personal Computer* (PC) atau laptop [3]. *Firewall* dapat membantu melindungi jaringan dari serangan dan membatasi akses ke sumber daya jaringan yang sensitif.

Dalam simulasi integrated library system pada website perpustakaan digital, teknologi jaringan ini dapat diterapkan untuk meningkatkan efisiensi, keamanan, dan kinerja jaringan.

2.2 Aplikasi Terdistribusi

GNS3, yang merupakan singkatan dari *Graphic Simulator Network*, adalah aplikasi *simulator* jaringan berbasis GUI yang diperkenalkan pada tahun 2008. Aplikasi ini memungkinkan simulasi perangkat asli dengan menggunakan *emulator* dan teknologi virtualisasi. Salah satu teknologi *emulator* yang digunakan adalah dynamips, yang dirancang khusus untuk mensimulasikan *Cisco IOS*. Sebelum adanya GNS3, untuk mensimulasikan *Cisco router*, pengguna perlu menginstal dynamips terlebih dahulu di berbagai sistem operasi seperti Windows, Linux, FreeBSD, atau MAC OS. GNS3 menyederhanakan proses ini dengan menyertakan *dynamips* secara otomatis dengan antarmuka yang ramah pengguna [6].

GNS3 terdiri dari komponen-komponen *emulator* dan teknologi virtualisasi yang memungkinkan pengguna menentukan sendiri perangkat apa yang ingin dijalankan di atas *emulator* tersebut. Meskipun GNS3 menyediakan beberapa perangkat bawaan seperti *virtual switch*, *hub*, dan *cloud*, pengguna harus menyediakan perangkat-perangkat utama seperti *router*, *switch*, *firewall*, dan *server* [6].

Berbagai fitur GNS3 melibatkan penggunaan teknologi seperti:

1. *Dynamips* merupakan sebuah *emulator router Cisco* yang memungkinkan pengguna untuk mensimulasikan perangkat keras dan perangkat lunak *router Cisco*. Sehingga memungkinkan pengguna untuk menjalankan *Operating System* (OS) *Cisco IOS* pada *platform non-Cisco* [7].
2. QEMU *(Quick EMUlator)* adalah sebuah emulator yang digunakan untuk mensimulasikan berbagai perangkat, seperti *server* Linux, PC Windows, dan perangkat jaringan seperti *Cisco ASA* dan *router* Juniper [7].
3. *VMware dan VirtualBox* adalah perangkat lunak virtualisasi yang berguna untuk menjalankan mesin virtual di atas sistem operasi *host*. Mesin virtual ini berfungsi guna menjalankan perangkat lunak jaringan seperti *router* dan *switch* dalam *environment* terisolasi [7].
4. *Docker Container* adalah *platform* perangkat lunak bagi pengguna untuk membuat, menguji, dan menjalankan aplikasi di dalam wadah yang terisolasi. Di dalam GNS3, *Docker Container* dapat digunakan untuk menjalankan perangkat lunak jaringan seperti *switch* dan *router* dalam sebuah *environment* terisolasi [8].
5. IOU (*IOS on Unix*) adalah solusi yang memungkinkan pengguna untuk mensimulasikan perangkat *Cisco IOS* pada sebuah topologi jaringan [7] [8].
6. VPCS (*Virtual PC Simulator*) merupakan salah satu alat yang digunakan untuk mensimulasikan komputer klien yang terhubung ke perangkat jaringan lainnya pada dalam sebuah jaringan [7].
7. *Wireshark* adalah perangkat lunak analisis jaringan yang digunakan untuk jaringan yang dihasilkan oleh perangkat yang disimulasikan dalam topologi GNS3 [7].

Koha ILS (*Integrated Library System*) adalah sistem manajemen perpustakaan berbasis web yang bersifat *open-source* dan dapat digunakan oleh perpustakaan umum, sekolah, dan khusus di seluruh dunia. Koha ILS pertama kali dikembangkan oleh Katipo Communications. Koha dirancang untuk mengotomatisasi berbagai fungsi dalam pengelolaan perpustakaan, mulai dari katalogisasi hingga manajemen peminjaman. Nama "Koha" berasal dari bahasa Māori yang berarti hadiah atau sumbangan [9]. Beberapa fitur Koha ILS meliputi:

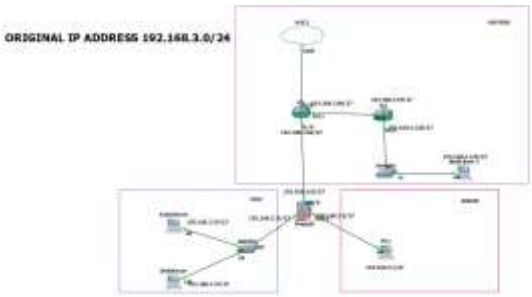
1. Berbasis web: Koha ILS adalah sistem manajemen perpustakaan berbasis web dengan *database* SQL

(MariaDB atau MySQL) dan data katalog disimpan dalam format MARC dan dapat diakses melalui Z39.50 atau SRU [9].
2. Konfigurasi dan adaptabilitas: Antarmuka pengguna Koha ILS sangat dapat dikonfigurasi dan diadaptasi, dan telah diterjemahkan ke banyak bahasa [9].
3. Fitur ILS: Koha ILS memiliki sebagian besar fitur yang diharapkan dalam sistem manajemen perpustakaan, termasuk fasilitas Web 2.0 seperti *tagging*, *feedback*, dan *RSS feed*, fasilitas katalog, pencarian yang dapat disesuaikan, sirkulasi daring, dan pencetakan *barcode* [9].

3. Hasil Percobaan

3.1 Instalasi dan Pengaturan

Layout jaringan yang digunakan kami terdiri atas beberapa komponen berupa *Virtual Machine* (VM), *Cisco firewall*, *router*, dan NAT *router* yang terhubung dengan internet. DNS (*Domain Name System*) 8.8.8.8 dan 8.8.4.4 menjadi pilihan untuk *layout* jaringan penelitian ini. Untuk layout jaringan GNS3 dapat dilihat pada gambar 1.



Gambar 1. *Layout* Jaringan pada GNS3 disertai IP

Berdasarkan *layout* jaringan pada gambar 2, VM yang digunakan sebagai WebServer adalah Ubuntu Server, sedangkan Ubuntu Dekstop dipakai sebagai KohaServer dan Puppy Linux digunakan sebagai WebClient. Untuk IP original yang digunakan adalah 192.168.3.0/24, lalu dibagi dengan metode SLSM (*Static Length Subnet Mask*) sehingga menghasilkan 8 buah *subnet*, dari 8 buah *subnet* tersebut diambil 5 buah *subnet* teratas yang dipakai pada layout jaringan GNS3, yaitu:

1. 192.168.3.0/27
2. 192.168.3.32/27
3. 192.168.3.64/27
4. 192.168.3.96/27
5. 192.168.3.128/27

Berikut ini adalah daftar tabel IP *Address* yang akan digunakan pada *layout* jaringan kami.

Tabel 1 Daftar IP *Address* yang dipakai pada *Router*

Jenis *Device*	*Interface*	IP *Address*
R1	f0/0	DHCP
R1	f0/1	192.168.3.98/27
R1	f1/0	192.168.3.66/27
R2	f0/0	192.168.3.97/27
R2	f1/0	192.168.3.130/27

Tabel 2 Daftar IP *Address* yang dipakai pada *Server* dan *Host*

Jenis *Device*	*Interface*	IP *Address*
WebClient	eth0	192.168.3.129/27
KohaServer	eth0	192.168.3.34/27
WebServer	eth0	192.168.3.33/27
Host	eth0	192.168.3.1/27

Tabel 3 Daftar IP *Address* yang dipakai pada *Firewall Cisco*

Jenis *Device*	*Interface*	IP *Address*
Firewall	gi0/0	192.168.3.65/27
Firewall	gi0/1	192.168.3.35/27
Firewall	gi0/2	192.168.3.2/27

Untuk kepentingan sekuritas, digunakanlah *Cisco firewall* yang terhubung dengan bagian outside, DMZ (Demilitarized Zone), dan *inside*. *Security level* 100 diterapkan pada bagian *inside*, *security level* 50 diterapkan pada bagian DMZ dan *security level* 0 diterapkan pada bagian *inside*. Bagian tersebut diberikan tingkat *security level* yang berbeda-beda supaya tidak ada akses sembarang dari bagian *level* yang lebih rendah ke bagian level yang lebih tinggi. Maka, jika WebClient pada bagian *outside* perlu mengakses ke WebServer dan KohaServer yang terletak pada bagian DMZ, diperlukan sebuah IP perantara yaitu, IP 192.168.3.70/27 untuk WebServer dan IP 192.168.3.68/27 untuk KohaServer. Dengan kata lain tidak ada akses langsung antara bagian outside dengan bagian DMZ.

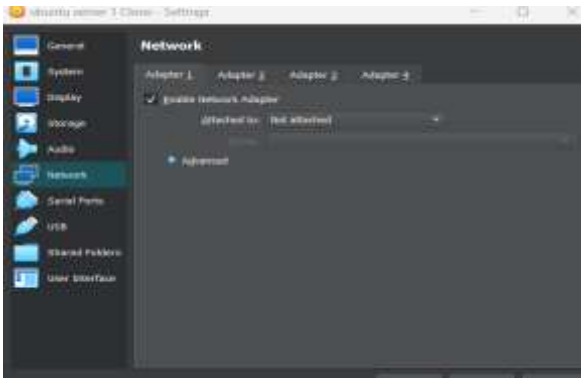
Penggunaan VPN *router to router* juga diterapkan pada *router* R1 dengan *router* R2 pada gambar 2. VPN digunakan pada *layout* tersebut guna untuk mengenkripsi semua aktivitas yang melewati jalur antara *router* R1 dengan *router* R2 atau *subnet* 192.168.3.96/27.

Untuk koneksi internet digunakan NAT *router* (R1) yang terhubung langsung dengan jaringan internet. NAT *router* menyebarkan koneksi internet ke seluruh bagian pada *layout* jaringan dengan

konfigurasi *access list* pada *firewall* dan *static routing* yang tepat.

VM yang perlu diinstalasi berdasarkan *layout* adalah Puppy Linux dan Ubuntu Desktop, sedangkan untuk instalasi Koha dilakukan pada ubuntu desktop. Puppy Linux dipilih sebagai WebClient pada penelitian ini karena ringan dibandingkan yang lainnya. Sedangkan untuk KohaServer, dipilihlah Ubuntu Desktop, karena koha hanya dapat berjalan di Debian atau Ubuntu Desktop. Dibandingkan dengan debian, ubuntu desktop lebih stabil maka dari itu dipilih menjadi KohaServer.

Iso Puppy Linux dan Ubuntu Desktop dapat di *download* melalui *website* resmi masing-masing kedua VM. Untuk Puppy Linux website resminya adalah https://forum.puppylinux.com/puppy-linux-collection, sedangkan *website* resmi dari ubuntu desktop adalah https://ubuntu.com/download/desktop. Untuk versi Puppy Linux yang di *download* adalah 18.04 BionicPup64 dan versi Ubuntu Desktop yang dipakai adalah Ubuntu 22.04.3 LTS (Jammy Jellyfish). Kemudian iso masing-masing diinput pada VM kemudian di *start* dan di instalasi sesuai arahan kedua VM tersebut. Untuk konfigurasi tambahan, buka settings pada Puppy Linux, Ubuntu Desktop dan Ubuntu server lalu ke network. Kemudian ubah konfigurasi *network adapter* 1 menjadi *not attached* seperti gambar 2, sehingga dapat dihubungkan kabel pada *layout* jaringan di GNS3.



Gambar 2. Konfigurasi *Network* VM untuk *Layout* di GNS3

Instalasi Koha dilaksanakan pada Ubuntu Desktop yang sudah diinstalasi pada *layout* tersebut. Instalasinya dapat dilakukan dengan cara seperti pada website resmi koha: https://wiki.koha-community.org/wiki/Koha_on_Debian, kemudian konfigurasi *port* pada koha-site.conf menjadi 8001 untuk *line* 9 dan 8000 untuk *line* 12 seperti gambar 3. *Port* 8001 diperuntukan untuk *staff* sedangkan *port* 8000 diperuntukan bagi *client*.

Gambar 3. Konfigurasi koha-sites.conf

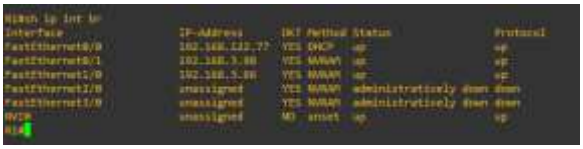
Lanjutkan proses instalasi hingga selesai setelah mengkonfigurasi *port*nya dengan menambahkan *line* "listen 8000 dan listen 8001" pada ports.conf seperti gambar 4.

Gambar 4. Konfigurasi ports.conf

Setup Jaringan yang diperlukan sesuai *layout* jaringan pada gambar 1 adalah:

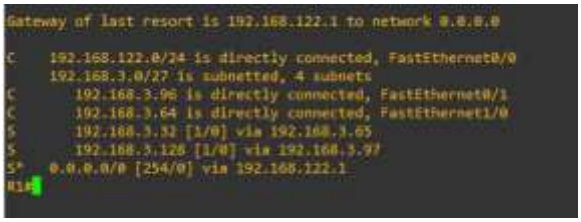
1. *Setup Router* R1

   Untuk *setup router* R1 dapat disesuaikan seperti gambar 5 dengan menambahkan IP pada setiap *interface*, disertai dengan DNS. Lalu menambahkan NAT di *router* R1 serta *Access Control List* (ACL) yang menghubungkan semua bagian pada *layout* jaringan.



Gambar 5. Hasil *Setup* IP *Router* R1

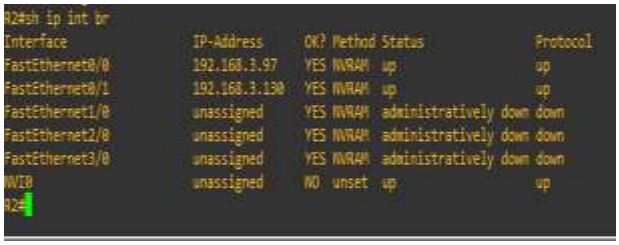
Selanjutnya melakukan *static routing* terhadap *subnet* 192.168.3.32 melalui ip 192.168.3.65 dan *subnet* 192.168.3.128 melalui ip 192.168.3.97, sehingga hasilnya seperti gambar 6.



Gambar 6. Hasil *Setup Static Router* R1

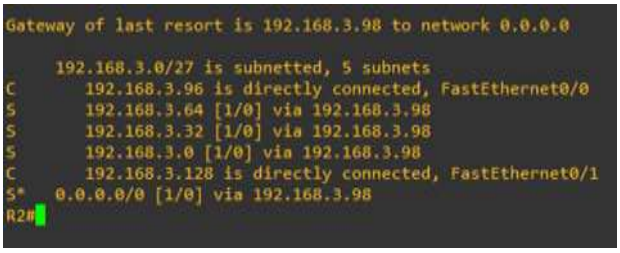
2. *Setup Router* R2

Untuk *setup router* R2, tambahkan IP untuk setiap *interface* yang terhubung, kemudian tambahkan DNS juga.



Gambar 7. Hasil *Setup* IP *Router* R2

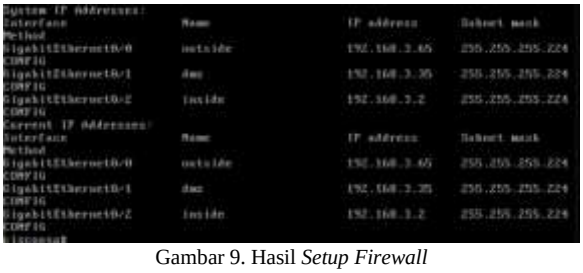
Selanjutnya melakukan *static routing* terhadap *subnet* 192.168.3.64, 192.168.3.32, 192.168.3.0 melalui 192.168.3.98 seperti gambar 8. Menambahkan ip route 0.0.0.0 0.0.0.0 192.168.3.98 supaya *router* R2 mendapatkan koneksi internet.



Gambar 8. Hasil *Setup Static Router* R2

3. *Setup Firewall*

Untuk *Setup Firewall* dapat disesuaikan seperti gambar 9. Menambahkan IP 192.168.3.65 pada *interface* gi0/0 untuk *outside* (nameif outside) dengan *security-level* 0, IP 192.168.3.35 pada *interface* gi0/1 untuk DMZ (nameif dmz) dengan *security-level* 50, IP 192.168.3.2 pada *interface* gi0/2 untuk *inside* (nameif inside) dengan *security-level 100*.

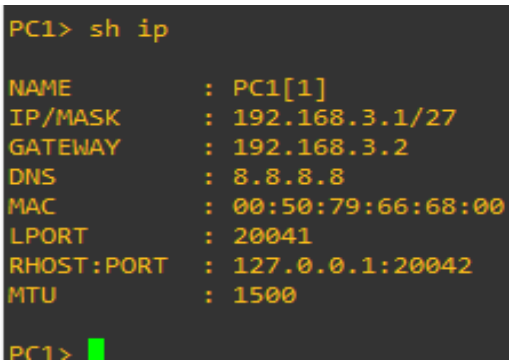


Gambar 9. Hasil *Setup Firewall*

Lalu ditambahkan DNS *lookup* pada *firewall* dan *routing* internet dari *outside* ke ip 192.168.3.66. Dilanjutkan dengan menambahkan NAT dan ACL DMZ to *outside* dengan menggunakan ip perantara 192.168.3.70 untuk WebServer yang berisikan halaman "about us" dan ip perantara 192.168.3.68 untuk KohaServer yang berisikan halaman untuk *client*.

4. *Setup* PC1 (*Host*)

Untuk *setup* pc1 atau host hanya menambahkan ip beserta gateway dan DNS 8.8.8.8, seperti yang ditunjukkan pada gambar 10.



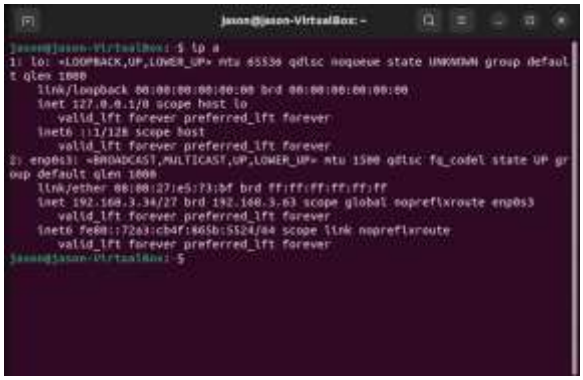
Gambar 10. Hasil *Setup* PC1 (Host)

5. *Setup* KohaServer

Ubah ip *address* dan *gateway* beserta dnsnya pada /etc/netplan/01-network-manager-all.yaml dengan sudo nano di terminal seperti gambar 11.

Gambar 11. *Setup* IP KohaServer

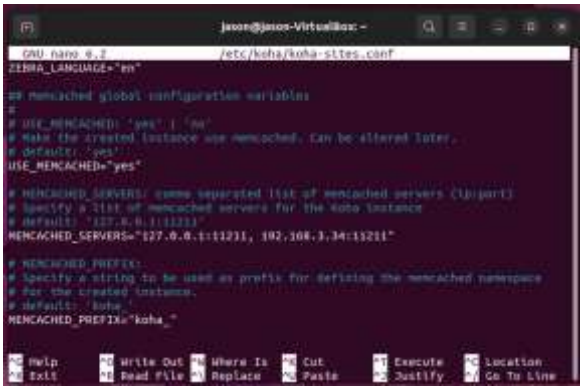
Setelah di konfigurasi maka enp0s3nya sudah berubah menjadi ip 192.168.3.34/27. Untuk memverifikasi dapat dicek dengan menjalankan "ip a", jika tampilannya sama seperti gambar 12 maka konfigurasi sudah berhasil.



Gambar 12. Hasil Konfigurasi KohaServer

Lalu konfigurasi *subdomain* pada /etc/koha/koha-sites.conf dan tambahkan IP yang ingin digunakan. Contohnya pada penelitian ini IP 192.168.3.34

digunakan sebagai *subdomain* dari KohaServer pada *line memcached servers* seperti yang tertera pada gambar 13.

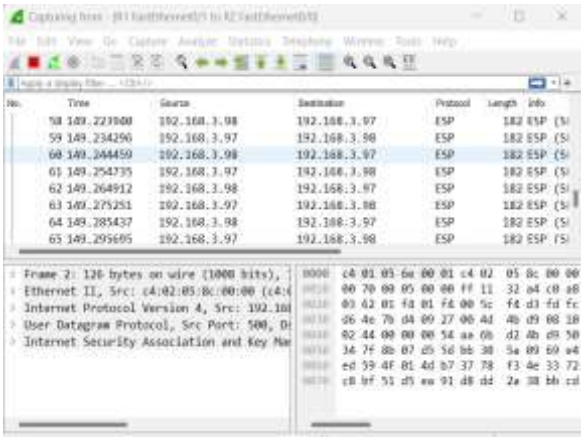


Gambar 13. *Setup* Subdomain KohaServer

6. *Setup* VPN *router* to *router* R1 dengan R2

Untuk *setup* VPN *router* to *router* dilakukan dengan membuat *tunnel* yang menghubungkan kedua *router* yaitu R1 dan R2. Key yang dipakai untuk kedua vpn ini adalah "untar". Hal pertama yang perlu dilakukan pada kedua *router* adalah dengan mengaktifkan dan melakukan konfigurasi ISAKMP dengan key "untar", selanjutnya lakukan IPsec transform set dan konfigurasi ACLnya. IP yang digunakan pada ACL berbeda untuk masing-masing *router*, untuk contoh *router* R1 menghubungkan 192.168.3.64 ke 192.168.3.128. dan sebaliknya untuk *router* R2. Kemudian konfigurasi *crypto map* dan *set peer* beserta menerapkan *crypto map* ke *interface* yang dituju untuk masing-masing *router*.

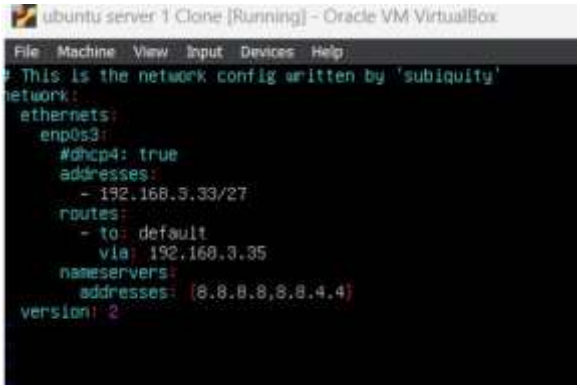
Koneksi VPN dapat dicek dengan melakukan *ping* 192.168.3.130 source 192.168.3.66 pada *router* R2, lalu klik kanan pada kabel *subnet* 192.168.3.96, kemudian *start capture*. Jika sudah terhubung dengan VPN maka pesan atau informasi dari ping tersebut akan di enkripsi dengan protocol *Encapsulating Security Protocol* (ESP) seperti yang ditunjukkan pada gambar 14.



Gambar 14. Hasil *setup* VPN

7. *Setup* WebServer

Edit ip pada WebServer dengan mengetikan sudo vim /etc/netplan/00-installer-config.yaml, lalu masukkan ip dan *set gateway* seperti yang ditampilkan pada gambar 15, beserta dns yang dipakai yaitu 8.8.8.8 dan 8.8.4.4, kemudian cek dengan menjalankan "ip a" untuk memverifikasi ip yang sudah diubah.



Gambar 15. *Setup* IP WebServer

8. *Setup* WebClient

Untuk mengatur ip pada WebClient, buka menu, setup, internet connection wizard, wired or wireless lan, network wizard, select eth0, static ip, lalu isi ipnya sesuai dengan gambar 16.

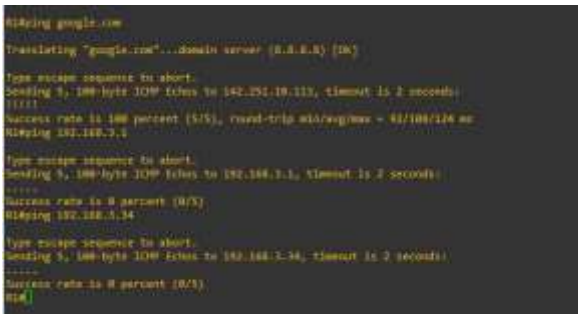
Gambar 16. *Setup* WebClient

3.2 Hasil Simulasi

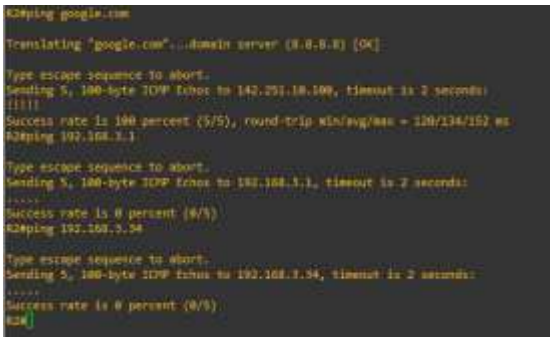
Setelah semua *setup* sudah memenuhi kriteria pada gambar masing-masing. Dapat dilakukan tes *ping* untuk membuktikan *firewall* dan *routing* telah bekerja dengan baik pada *layout* jaringan di GNS3. Tes *ping* akan dilakukan pada *router* R1, *router* R2, PC1 (*host*), WebServer, KohaServer dan WebClient.

Pada *router* R1 dan R2, lakukan *ping* IP terhadap bagian *inside* dan DMZ, serta tes *ping* google.com. Gambar 17 dan 18 membuktikan bahwa koneksi internet dan penerapan *firewall* pada kedua *router*

sudah berhasil. *Router* R1 dan R2 sudah seharusnya tidak bisa melakukan *ping* terhadap ip dengan *security level* yang lebih tinggi.



Gambar 17. Hasil Tes *Ping* pada *Router* R1

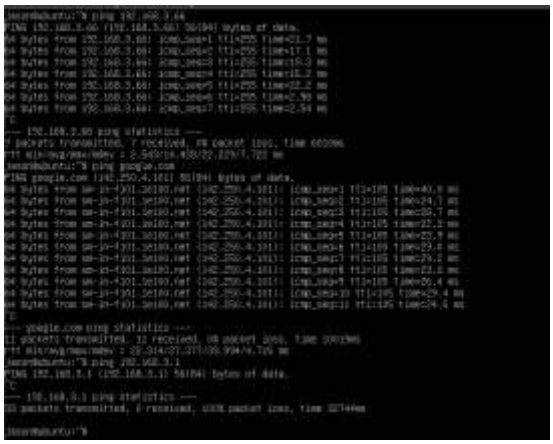


Gambar 18. Hasil Tes *Ping* pada *Router* R2

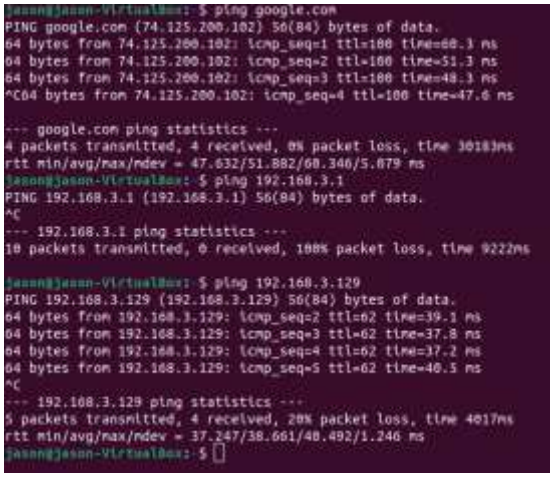
Pada PC1, lakukan *ping* google.com dan ping ke IP pada bagian *outside*. Gambar 19 menunjukkan bahwa PC1 sudah terhubung dengan internet dan dapat melakukan *ping* terhadap IP atau *subnet* dengan *level* yang lebih rendah, karena PC1 termasuk dalam bagian *inside*.

Gambar 19. Hasil Tes *Ping* pada PC1

Lakukan *ping* google.com, IP pada bagian *outside* dan *inside* pada kedua *server*. Gambar 20 dan 21 menunjukkan bahwa kedua *server* sudah terhubung dengan internet dan dapat melakukan *ping* terhadap IP bagian *outside* tetapi tidak bisa *ping* terhadap IP bagian *inside*.



Gambar 20. Hasil Tes *Ping* pada WebServer



Gambar 21. Hasil Tes *Ping* pada KohaServer

Pada WebClient lakukan ping IP pada bagian DMZ dan *inside* pada kedua *server*. Gambar 21 menunjukkan bahwa konfigurasi *firewall* dan internet sudah benar.

Gambar 22. Hasil Tes *Ping* pada WebClient

Tampilan halaman *client*, WebServer dan *staff* dapat dilihat dengan membuka url http://192.168.3.34:8001/ pada *browser* KohaServer dan http://192.168.3.68:8000/ pada *browser* WebClient, sedangkan untuk WebServer dapat dibuka dengan url http://192.168.3.70/ pada *browser* WebClient juga.

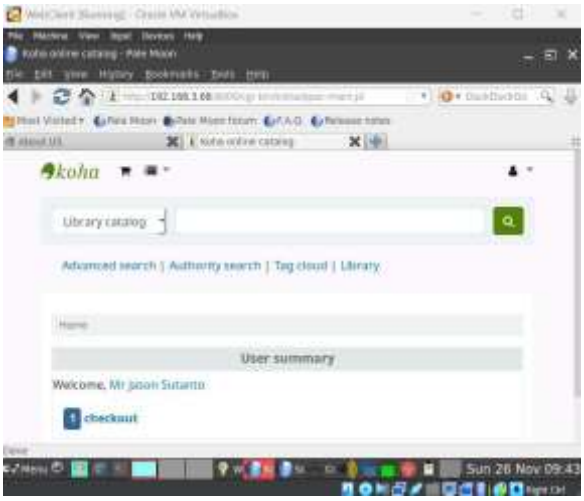
Halaman *login staff* dari KohaServer dapat dilihat pada gambar 23. *Staff* dapat memasukkan *username* dan *password* yang telah di buat pada saat *setup* Koha. *Staff* juga dapat memilih *library* apa yang ingin digunakan.

Gambar 23. Tampilan Halaman *Login Staff* Koha

Setelah *login*, maka akan muncul halaman tampilan utama seperti gambar 24. Pada halaman utama terdapat navbar yang memudahkan *staff* dalam proses administrasi buku maupun para *client*. Lalu juga ada fitur *tools*, *circulation*, *patron*, *koha administration*, *cataloging* dan lain-lain pada bagian tengah halaman.

Gambar 24. Tampilan Utama Halaman *Staff* Koha

Untuk tampilan halaman *login client* dari WebClient sama seperti tampilan halaman *login staff*. Tampilan halaman utama *client* dapat dilihat pada gambar 25.



Gambar 25. Tampilan Utama Halaman *Client* Koha

WebServer pada *layout* jaringan kami berisikan halaman “about us” yang memiliki tampilan simpel. Gambar 26 adalah potongan tampilan dari WebServer kami.

Gambar 26. Tampilan Halaman About Us WebServer

Berdasarkan hasil simulasi *layout* jaringan pada GNS3 dengan Koha, dapat disimpulkan bahwa penggunaan Koha pada jaringan kami memiliki kelebihan dan kekurangan. Kelebihannya diantara lain:

1. Pengelolaan dan akses yang terpusat. Penggunaan Koha memudahkan pengelolaan administrasi perpustakaan konvensional dengan mengintegrasikan layanan perpustakaan ke dalam suatu jaringan dan dapat memberikan akses terpusat ke data dan layanan jaringan
2. *Open Source* dan kemudahan integrasi. Koha yang bersifat *open source* memudahkan pengguna untuk menkonfigurasi sesuai dengan kebutuhan spesifik yang dibutuhkan. Koha juga mudah untuk diintegrasikan dengan sistem manajemen jaringan untuk pemantauan dan manajemen keseluruhan.

Kekurangan dari penggunaan Koha adalah sebagai berikut:

1. Konsumsi sumber daya komputer yang beragam. Penggunaan Koha pada simulasi *layout* jaringan membutuhkan sumber daya yang beragam. Semakin besar ukuran dan kompleksitas yang dikelola, maka semakin besar sumber daya yang dibutuhkan.
2. Kompleksitas konfigurasi. Konfigurasi serta penyesuaian Koha dapat dikatakan sangat kompleks dan rumit. Jadi, butuh pemahaman khusus mengenai perpustakaan dan sistem manajemen di dalamnya.

4. Kesimpulan

Berdasarkan hasil simulasi *layout* jaringan pada GNS3 dengan Koha, dapat ditarik beberapa kesimpulan sebagai berikut ini:

1. Koha dapat diintegrasikan pada jaringan GNS3 dengan mudah dan lancar

2. Simulasi *layout* jaringan pada GNS3 dapat berjalan baik berbagai konfigurasi dan setup yang telah dilakukan.
3. Dua *server* yang digunakan untuk *client* dan *staff* dapat terhubung dengan Koha dengan baik.

Adapun saran yang dapat diberikan untuk penelitian selanjutnya adalah perlunya pemahaman yang lebih matang mengenai infrastruktur jaringan yang akan dibuat terutama pada bagian keamanan pada jaringan itu sendiri seperti enkripsi dan VPN pada *server* yang dipakai. Selain itu penting juga untuk mendalami kemahiran dalam pemeliharaan dan manajemen dengan menggunakan Koha.

REFERENSI

[1] A. Suryadi, "PENGERTIAN OTOMASI PERPUSTAKAAN- TUJUAN, MANFAAT DAN FUNGSI." Diakses: 27 November 2023. [Daring]. Tersedia pada: https://elibrary.bsi.ac.id/readnews/2019/05/17/pengertian-otomasi-perpustakaan-tujuan-manfaat-dan-fungsi.html

[2] Z. Hardiansyah, "Pengertian Jaringan Komputer, Lengkap dengan Jenis dan Perbedaannya." Diakses: 21 November 2023. [Daring]. Tersedia pada: https://tekno.kompas.com/read/2022/05/19/12150067/pengertian-jaringan-komputer-lengkap-dengan-jenis-dan-perbedaannya?page=all

[3] Cloudmatika, "Memahami Apa itu Network Security, Jenis, dan Manfaatnya Bagi Perusahaan." Diakses: 21 November 2023. [Daring]. Tersedia pada: https://cloudmatika.co.id/blog-detail/network-security-adalah

[4] E. M. Ayuningtyas, "Subnetting : Kenali Pengertian, Mekanisme serta Fungsinya." Diakses: 27 November 2023. [Daring]. Tersedia pada: https://it.telkomuniversity.ac.id/subnetting-kenali-pengertian-mekanisme-serta-fungsinya/

[5] B. A. Forouzan, *Data Communication and Networking*, 4th ed. New York, 2013.

[6] P. Agustyaningsih, "Mengenal GNS3 dan Fitur-Fiturnya." Diakses: 27 November 2023. [Daring]. Tersedia pada: https://medium.com/network-evolution/mengenal-gns3-dan-fitur-fiturnya-1170cc9ed514

[7] Fathurhoho, "Panduan Dasar Belajar GNS3: Mengenal GNS3 dan Fitur-Fiturnya." Diakses: 27 November 2023. [Daring]. Tersedia pada: https://ngonfig.net/gns3.html

[8] A. M. Potdar, D. G. Narayan, S. Kengond, dan M. M. Mulla, "Performance Evaluation of Docker Container and Virtual Machine," dalam *Procedia Computer Science*, Elsevier B.V., 2020, hlm. 1419–1428. doi: 10.1016/j.procs.2020.04.152.

[9] V. Bhimrao, "Open Source Software KOHA: An Overview," *International Journal of Library & Information Science*, vol. 2, no. 2, hlm. 11–15, [Daring]. Tersedia pada: http://www.iaeme.com/IJLIS/index.asp11http://www.iaeme.com/IJLIS/issues.asp?JType=IJLIS&VType=9&IType=2JournalImpactFactor