

SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI OPENSTACK DENGAN GNS3

Tigo Ihami Fasyah ¹⁾ Jason Chainara Putra ²⁾ Ruben Tobia Chaiyadi ³⁾

Jafier Andreas ⁴⁾ Timothy Wahyudi Pakpahan ⁵⁾

¹⁾²⁾³⁾⁴⁾⁵⁾ Teknik Informatika, FTI, Universitas Tarumanagara

Jl. Letjen S. Parman No.1, RT.6/RW.16, Tomang, Kec. Grogol petamburan,

Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11440

email : ¹⁾tigo.535220235@stu.untar.ac.id, ²⁾jason.535220045@stu.untar.ac.id, ³⁾ruben.535220051@stu.untar.ac.id, ⁴⁾jafier.535220013@stu.untar.ac.id, ⁵⁾timoty.535220043@stu.untar.ac.id

ABSTRAK

Pergeseran paradigma terhadap kerja jarak jauh telah menekankan kebutuhan akan infrastruktur jaringan yang kuat dan terukur. Penelitian ini menyajikan simulasi jaringan Work From Home (WFH) menggunakan Cloud Infrastructure as a Service (IaaS) yang didukung oleh OpenStack. Simulasi ini berfokus pada evaluasi kinerja, skalabilitas, dan keandalan arsitektur jaringan, dengan mempertimbangkan tantangan yang terkait dengan skenario kerja jarak jauh. OpenStack digunakan untuk menyediakan mesin virtual, jaringan, dan sumber daya penyimpanan, menciptakan lingkungan berbasis cloud untuk simulasi WFH. Hasil penelitian menunjukkan bahwa Client PC di outside zone berhasil mengakses cloud OpenStack melalui dashboard dan Web server (HTTP/HTTPS) dan juga pada Inside PC dapat mengakses semua zona termasuk webserver dan server openstack dengan melakukan ping melalui terminal.

Kata Kunci

Cloud, IaaS, OpenStack, Jaringan, GNS 3

1. Pendahuluan

Peningkatan tren bekerja dari rumah (Work From Home/WFH) dalam dunia kerja modern menunjukkan perlunya infrastruktur jaringan yang handal dan efisien untuk mendukung produktivitas karyawan di berbagai lokasi. Dalam era dimana data menjadi aset krusial dan keamanan informasi adalah kebutuhan utama, menjaga jaringan WFH agar tetap aman dan efisien merupakan tantangan yang semakin mendesak sehingga kita perlu memanfaatkan keunggulan dari *Cloud Computing*.

Cloud Computing merupakan penyediaan sumber daya komputasi seperti server, penyimpanan data, jaringan serta perangkat lunak melalui internet [1]. *Cloud Computing* membuat pemrosesan data menjadi lebih efisien pada beberapa sistem komputasi dan penyimpanan yang aksesnya dilakukan melalui internet [2]. Layanan pada *Cloud Computing* umumnya dibagi menjadi tiga model, yaitu *Infrastructure as a Service*

(IaaS), *Platform as a Service* (PaaS), *Software as a Service* (SaaS). Ketiga layanan tersebut memiliki keunggulan dan kekurangan sesuai kebutuhan perusahaan atau organisasi masing – masing.

Pada simulasi jaringan kali ini digunakan layanan *Cloud Infrastructure as a Service* (IaaS) dalam mendukung Work From Home (WFH) menggunakan OpenStack, dimana disediakan sumber daya dan layanan kepada pengguna yang terdiri dari *network, content delivery, storage, backup dan recovery*, serta *processing*. Dalam IaaS, pengguna tidak diizinkan untuk mengelola infrastruktur *cloud*, mereka hanya diizinkan untuk mengelola sistem operasi dan menggunakan aplikasi [2].

Tujuan dari simulasi ini adalah memberikan wawasan mendalam terkait arsitektur jaringan sistem terdistribusi OpenStack menggunakan GNS3, yang pada akhirnya dapat memberikan kontribusi terhadap pengembangan dan peningkatan kehandalan sistem terdistribusi yang berbasis teknologi OpenStack.u

2. Studi Pustaka

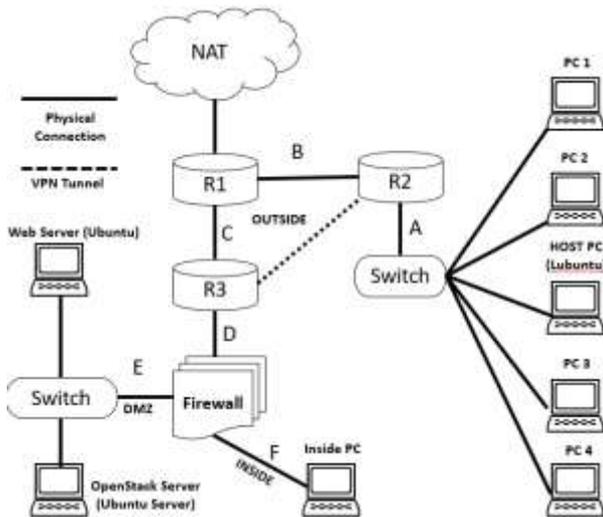
2.1 Jaringan dan keamanan komputer

Pada simulasi jaringan ini digunakan original Network Address yaitu 192.168.2.0/24 kemudian dibagi menjadi 6 Subnet menggunakan *Variable Length Subnet Mask* (VLSM), untuk lebih lengkapnya dapat dilihat pada tabel berikut.

Tabel 1. Tabel informasi subnetting

SubName	Num Host	Range
A	50	192.168.2.1 – ~.62 /26
F	8	192.168.2.65 – ~.78 /28
B	4	192.168.2.81 – ~.86 /29
C	4	192.168.2.89 – ~.94 /29
D	4	192.168.2.97 – ~.102 /29
E	4	192.168.2. 105 – ~.110/29

Setelah dilakukan perhitungan *subnetting* tersebut, langkah selanjutnya adalah membangun rancangan sistem jaringan sesuai dengan jumlah subnet yang telah dibentuk berdasarkan kebutuhan perusahaan atau organisasi. Pada rancangan sistem yang saat ini dibuat dapat dilihat pada Gambar 1 dimana digunakan 3 Router, 2 Switch, NAT, Firewall, 4 WFH PC, 1 Host PC (Lubuntu), 1 Web Server (Ubuntu Server), 1 OpenStack Server (Ubuntu Server), 1 Inside PC (VPCS).



Gambar 1. Topologi desain rancangan sistem

Berdasarkan Gambar 1 dapat diketahui jika router R1 terhubung secara langsung ke NAT dimana NAT berfungsi sebagai akses jaringan internet untuk setiap perangkat yang terhubung, kemudian pada router R2 terhubung langsung ke Switch dimana terdapat PC WFH dan PC Host dengan *virtual machine* Lubuntu.

Selain terhubung ke Switch, router R2 dan R3 juga terhubung ke Firewall melalui *Virtual Private Network* (VPN) *tunnel*. Hal ini memungkinkan komunikasi antara perangkat pada router R2 dan R3 ke dalam server sehingga dapat terhubung ke sumber daya jaringan perusahaan atau organisasi dengan cara yang aman dan terenkripsi.

Firewall merupakan perangkat keamanan jaringan yang memonitor lalu lintas jaringan masuk maupun keluar dan memutuskan atau memblokir lalu lintas tertentu berdasarkan seperangkat aturan keamanan yang ditetapkan [3]. Firewall membagi zona atau segmen jaringan menjadi tiga bagian yang berbeda dalam arsitektur keamanan yaitu Outside (Jaringan eksternal), *Demilitarized Zone* (DMZ) dan Inside (Jaringan internal), masing – masing zona tersebut menggunakan aturan tingkat keamanan sesuai ketentuan perusahaan atau organisasi.

Jenis Firewall yang digunakan pada konfigurasi sistem jaringan di Gambar 1 adalah Cisco Adaptive Security Virtual Appliance (ASAv) 9.8.1, kemudian

digunakan tiga zona atau segmen jaringan sebagai berikut.

1. Outside (Jaringan eksternal)
Merupakan zona jaringan yang mencakup semua perangkat di luar jaringan internal. Hal ini termasuk internet dan WFH PC serta Host PC.
2. Demilitarized Zone (DMZ)
Zona DMZ digunakan untuk menempatkan server dan layanan yang perlu diakses dari jaringan luar, tetapi tidak sepenuhnya dapat diakses oleh jaringan luar. Hal ini mencakup *web server* serta *OpenStack cloud server*.
3. Inside (Jaringan internal)
Zona jaringan yang berisi sumber daya internal perusahaan atau organisasi dan hanya dapat diakses oleh pengguna yang memiliki izin atau otoritas khusus.

2.2 Aplikasi Terdistribusi

Aplikasi terdistribusi adalah program perangkat lunak yang berjalan pada komputer yang berbeda pada suatu jaringan [4], sebuah perusahaan atau organisasi biasanya memiliki aplikasi terdistribusi untuk memproses segala kebutuhan bisnis dan mendukung semua jenis penyimpanan data perusahaan atau organisasi.

Berdasarkan topologi jaringan yang digunakan pada Gambar 1 digunakan dua server dalam zona *Demilitarized Zone* (DMZ) yaitu Ubuntu server 22.04.3 (Jammy Jellyfish) sebagai *web server* dan *OpenStack server* serta Lubuntu 22.04.3 LTS sebagai Host PC. Dengan menggunakan konsep tersebut perusahaan atau organisasi dapat mengoptimalkan kinerja *web server* serta menyediakan infrastruktur *cloud* secara aman dan terkelola didalam zona DMZ, sekaligus menjaga keamanan dan integritas sumber daya internal. Berikut adalah penjelasan lebih lengkap tentang kedua server tersebut.

1. Web server (Ubuntu server 22.04.3)

Dalam aplikasi terdistribusi, *web server* adalah elemen yang memegang peran utama dalam mengelola permintaan HTTP/HTTPS dari klien dan memberikan respons yang sesuai. Dalam konteks arsitektur terdistribusi, konsep ini diperluas melalui pertimbangan terhadap pemisahan tugas dan distribusi beban kerja di antara sejumlah server. Tujuannya adalah untuk meningkatkan efisiensi, daya skala, dan ketersediaan aplikasi.

Web server tidak hanya menjadi elemen vital dalam menyediakan layanan yang handal dan responsif kepada pengguna, tetapi juga memastikan distribusi beban kerja yang seimbang dan efisien. Selain itu, *web server* juga dapat memberikan akses ke layanan

Cloud Computing seperti penyimpanan data, komputasi, dan jaringan. Melalui ubuntu server sebagai basis sistem operasi, *web server* dapat beroperasi di beberapa instance di *cloud*, yang memungkinkan distribusi lalu lintas secara efisien dan memastikan ketersediaan layanan yang tinggi. *Web server* ini dapat diakses oleh pengguna dari berbagai lokasi, fleksibel dan dapat diakses dari mana saja dengan koneksi internet.

2. OpenStack server (Ubuntu server 22.04.3)

OpenStack adalah platform *open source* yang menggunakan sumber daya virtual yang dikumpulkan untuk membangun dan mengelola *private* atau *public cloud*. OpenStack menggunakan *Application programming interfaces (APIs)* untuk mengabstraksi sumber daya virtual seperti Storage, CPU (*Central processing unit*) dan RAM (*Random access memory*) [5]. Dengan menggunakan APIs, pengguna dapat melakukan operasi seperti membuat *virtual machine*, mengatur jaringan, mengelola penyimpanan, dan melakukan tugas-tugas lainnya pada platform OpenStack. Berdasarkan topologi jaringan di Gambar 1. OpenStack Cloud dikelola melalui sebuah *Cloud server* yang menggunakan *virtual machine* Ubuntu 22.04.3.

Tujuan dari penggunaan ubuntu server sebagai sistem operasi utama yaitu karena desain yang ringan dan dapat memberikan efisiensi dalam penggunaan sumber daya, sehingga bermanfaat bagi server – server yang bekerja dalam lingkungan *cloud*. Hal ini cocok untuk lingkungan dimana efisiensi dan kinerja yang baik diperlukan, terutama jika infrastruktur *cloud* tersebut ditujukan untuk lingkungan dengan sumber daya terbatas atau efisiensi energi adalah pertimbangan utama. Dengan menggunakan ubuntu server sebagai basis sistem operasi dan mengintegrasikannya dengan OpenStack, kita dapat membangun dan mengelola infrastruktur *cloud* sesuai dengan kebutuhan sumber daya aplikasi atau ketentuan perusahaan atau organisasi.

3. Hasil Percobaan

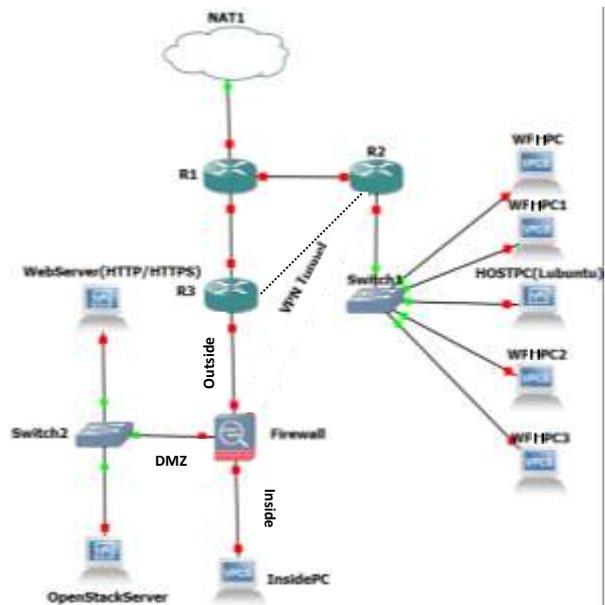
3.1 Instalasi dan Pengaturan

Dalam melakukan instalasi dan pengaturan jaringan hal pertama yang harus dilakukan adalah memiliki atau sudah mendownload software GNS3 dan Oracle VM VirtualBox, melalui GNS3 kita dapat menjalankan topologi kecil yang terdiri dari beberapa perangkat di laptop kita, hingga topologi yang memiliki banyak perangkat yang di-host di beberapa server bahkan pada host di *cloud* [6] dan melalui Virtual Box kita dapat menjalankan *virtual machine* yang dibutuhkan dalam

mendukung pengoperasian GNS3. Selain mendownload software tersebut kita perlu mendownload perangkat perangkat yang akan digunakan sebagai berikut.

1. Router Cisco c3745 124-25d.
2. Cisco Adaptive Security Virtual Appliance (ASAv) Firewall atau Cisco ASAv.
3. GNS3 VM Virtualbox.
4. Ubuntu server 22.04.3 (Jammy Jellyfish).
5. Lubuntu 22.04.3 LTS.

Setelah berhasil melakukan instalasi pada kelima perangkat tersebut dapat dilakukan pengaturan lebih lanjut sehingga dapat digunakan didalam GNS3. Ketika semua perangkat tersebut dapat digunakan di GNS3, maka langkah selanjutnya adalah membangun topologi jaringan seperti pada Gambar 2. berikut.



Gambar 2. Topologi jaringan pada GNS3

Jika topologi jaringan telah dibuat seperti Gambar 2 di GNS3 maka dapat ditentukan IP Address masing – masing interface pada setiap perangkat yang ada seperti Router, Firewall, Web server, OpenStack server, Inside PC, WFH PC dan Host PC. Berikut adalah tabel informasi IP Address.

Tabel 2. Tabel informasi IP Address

Nama Perangkat	IP Address	Interface
WFH PC	192.168.2.2 /26	eth0
WFH PC1	192.168.2.3 /26	eth0
HostPC	192.168.2.4 /26	eth0
WFH PC2	192.168.2.5 /26	eth0
WFH PC3	192.168.2.6 /26	eth0
R1	DHCP	f0/0
R1	192.168.2.81 /29	f1/0
R1	192.168.2.89 /29	f2/0
R2	192.168.2.82 /29	f0/0

R2	192.168.2.1 /29	f1/0
R3	192.168.2.90 /29	f0/0
R3	192.168.2.97 /29	f1/0
Firewall	192.168.2.91 /29	gi0/0
Firewall	192.168.2.105 /29	gi0/1
Firewall	192.168.2.65 /28	gi0/2
Web server	192.168.2.106 /29	eth0
Openstack server	192.168.2.107 /29	eth0
Inside PC	192.168.2.66 /28	eth0

Setelah ditentukan IP Address dari masing masing – masing perangkat maka dilakukan konfigurasi disetiap perangkat sesuai dengan informasi di Tabel 2, berikut adalah langkah – langkah konfigurasi tersebut.

1. Setting router

Lakukan langkah – langkah berikut di setiap router R1, R2 dan R3.

- Setting IP Address dan DNS Server
 - 1) conf t
 - 2) int (interface yang dituju)
 - 3) ip add (IP address / dhcp bagi interface yang terhubung langsung ke NAT) (subnet mask)
 - 4) no shut
 - 5) ulangi dari langkah 1 sampai semua interface terkonfigurasi
 - 6) exit
 - 7) ip route 0.0.0.0 0.0.0.0 (gateway yang menuju ke R1)
 - 8) ip domain-lookup
 - 9) ip name-server 8.8.8.8 8.8.4.4
 - 10)end
- Setting dynamic routing
 - 1) conf t
 - 2) router ospf 1
 - 3) network (network address) (wildcard) area 0
 - 4) end
- Setting NAT di R1
 - 1) conf t
 - 2) int (nama interface router link ke NAT)
 - 3) ip nat outside
 - 4) int (nama interface router tidak link ke NAT)
 - 5) ip nat inside
 - 6) exit
 - 7) access-list 1 permit any
 - 8) ip nat inside source list 1 interface (nama interface router link ke NAT) overload

2. Setting Firewal (Cisco ASA v)

Langkah – langkah untuk mengonfigurasi Firewall sesuai zona dan security-level pengguna.

- Setting IP Address dan zona pada Firewall
 - 1) conf t
 - 2) int (nama interface ke zona masing – masing)
 - 3) ip add (ip address) (subnet mask)
 - 4) nameif (nama zona)

- 5) security-level (security level sesuai zona)
- 6) no shut
- 7) ulangi langkah 1 sampai semua interface terkonfigurasi
- 8) exit
- Setting dynamic routing
 - 1) conf t
 - 2) router ospf 1
 - 3) network (network address) (subnet mask) area 0
 - 4) end
- Setting DNS dan routing ke NAT
 - 1) dns domain-lookup outside
 - 2) dns server-group DefaultDNS
 - 3) name-server 8.8.8.8
 - 4) name-server 8.8.4.4
 - 5) exit
 - 6) route outside 0.0.0.0 0.0.0.0 (gateway yang menuju ke R1)
 - 7) policy-map global_policy
 - 8) class inspection_default
 - 9) inspect icmp
- Setting NAT dan Access List Control (ACL)
 - 1) conf t
 - 2) object network inside-subnet
 - 3) subnet (inside network address) (subnet mask)
 - 4) nat (inside,outside) dynamic interface
 - 5) exit
 - 6) object network dmz-subnet
 - 7) subnet (dmz network address) (subnet mask)
 - 8) nat (dmz,outside) dynamic interface
 - 9) exit

3. Setting VPN tunnel pada R2 dan R3

Langkah – langkah setting VPN dilakukan melalui link berikut, dilakukan konfigurasi di router R2 dan R3 : <https://www.gns3network.com/how-to-configure-ipsec-tunnel-between-cisco-routers/>

4. Setting web dan cloud server (ubuntu server 22.04.3)

Pada *virtual machine* ubuntu server diperlukan setting untuk mengatur IP Address sesuai topologi jaringan yang telah kita buat. Berikut adalah langkah – langkah dalam mengonfigurasi ubuntu server.

- Setting IP Address dan connect ke NAT
 - 1) Login ke ubuntu server
 - 2) Ketik command sudo vim /etc/netplan/00-installer-config.yaml
 - 3) Edit file 00-installer-config.yaml dengan addresses 192.168.2.106/29 dan gateway 192.168.2.105 untuk *web server*, jika dilakukan pada *cloud server* maka IP Address dan Gateway dapat disesuaikan sesuai konfigurasi pada *cloud server*. Berikut adalah

syntax untuk mengonfigurasi jaringan di ubuntu server.

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      #dhcp4: true
      addresses:
        - 192.168.2.106/29
      routes:
        - to: default
          via: 192.168.2.105
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
      version: 2
```

Gambar 3. *Syntax* IP Address ubuntu server

4) `sudo netplan apply`

- Setting apache web server

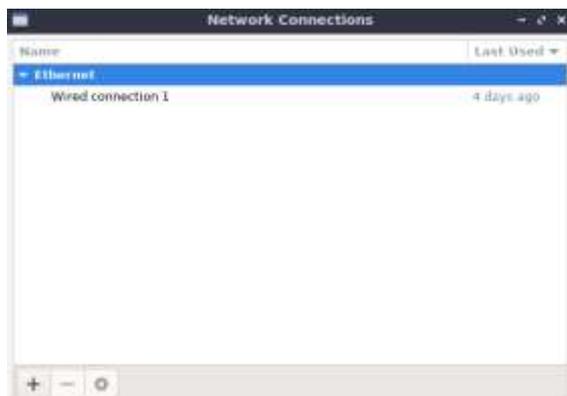
Untuk melakukan setting pada *web server* hingga sampai membuat domain yang kita inginkan dapat dilakukan melalui link tutorial berikut ini : <https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-22-04>.

5. Setting OpenStack (Lubuntu 22.04.3 LTS)

Sebelum melakukan setting pada OpenStack kita harus mengetahui terlebih dahulu spesifikasi minimum untuk menjalankan OpenStack Cloud di *virtual machine*, karena akan dibutuhkan banyak memori, penyimpanan dan CPU yang memadai. Berikut adalah resource yang akan kita alokasikan ke *virtual machine* untuk dapat menjalankan OpenStack Cloud:

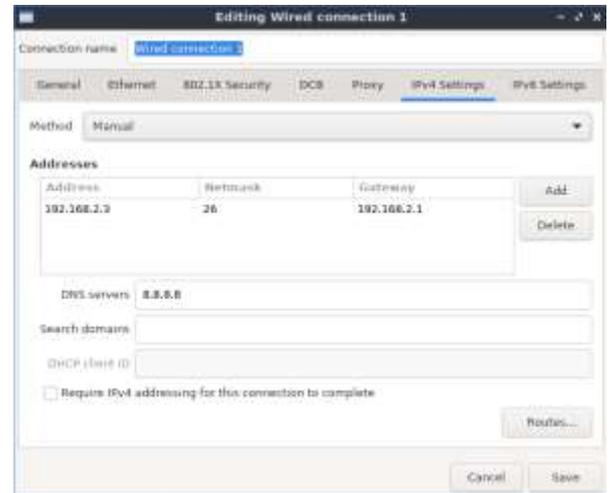
1. 4+ core amd64 CPU
2. 16 GB RAM
3. 100 GB SSD storage

Setelah kita mengalokasikan resource tersebut maka langkah selanjutnya adalah melakukan setting IP Address pada Lubuntu melalui menu search pada bagian bawah kiri kemudian klik preferences dan masuk ke Advanced Network Configuration atau bisa langsung dengan mengetik `network`, jika sudah di klik maka akan muncul seperti berikut.



Gambar 4. Network connections lubuntu

Selanjutnya klik `Wired connection 1 > IPv4 Settings > Method > Manual > Klik Add > Masukkan IP Address, Netmask dan Gateway > Masukkan DNS servers 8.8.8.8 > Save`. Maka Setting IP Address dan DNS telah selesai sehingga Lubuntu dapat connect ke NAT, berikut adalah tampilan konfigurasinya.



Gambar 5. Tampilan IPv4 settings lubuntu

Langkah selanjutnya adalah melakukan instalasi OpenStack Cloud melalui terminal yang ada di *virtual machine* lubuntu, pada halaman selanjutnya disajikan langkah – langkah instalasi OpenStack hingga dapat masuk ke halaman login OpenStack. Untuk konfigurasi pada OpenStack server di bagian DMZ juga memiliki command yang sama seperti konfigurasi melalui lubuntu.

1. Mengunduh snap microstack (versi lightweight dari OpenStack). Command : `sudo snap install microstack --beta`

```
jason@jason-virtualbox:~$ sudo snap install microstack --beta
[sudo] katasandi untuk jason:
microstack (beta) ussuri dari Canonical✓ terpasang
```

Gambar 6. Mengunduh snap microstack

2. Menginisiasi layanan OpenStack. Command : `sudo microstack init --auto --control`

```
jason@jason-virtualbox:~$ sudo microstack init --auto --control
2023-11-24 13:32:53,776 - microstack_init - INFO - Configuring clustering ...
2023-11-24 13:32:54,049 - microstack_init - INFO - Setting up as a control node.
2023-11-24 13:32:57,842 - microstack_init - INFO - Generating TLS Certificate and Key
2023-11-24 13:32:58,986 - microstack_init - INFO - Configuring networking ...
2023-11-24 13:33:07,686 - microstack_init - INFO - Opening horizon dashboard up to *
2023-11-24 13:33:09,019 - microstack_init - INFO - Waiting for RabbitMQ to start ...
Waiting for 192.168.2.122:5672
2023-11-24 13:33:18,712 - microstack_init - INFO - RabbitMQ started!
2023-11-24 13:33:18,712 - microstack_init - INFO - Configuring RabbitMQ ...
2023-11-24 13:33:20,486 - microstack_init - INFO - RabbitMQ Configured!
2023-11-24 13:33:20,518 - microstack_init - INFO - Waiting for MySQL server to start ...
Waiting for 192.168.2.122:3306
```

Gambar 7. Inisialisasi layanan OpenStack

3. Membuat instance, akan keluar IP untuk mengakses dashboard OpenStack. Command : `microstack launch cirros -n test`

```
jason@jason-virtualbox:~$ microstack launch cirros -n test
Creating local "microstack" ssh key at /home/jason/snap/microstack/common/.ssh/id_microstack
Launching server ...
Allocating floating ip ...
Server test launched! (status is BUILD)

Access it with 'ssh -i /home/jason/snap/microstack/common/.ssh/id_microstack cirros@10.20.20.51'
You can also visit the OpenStack dashboard at https://10.20.20.1:443
jason@jason-virtualbox:~$
```

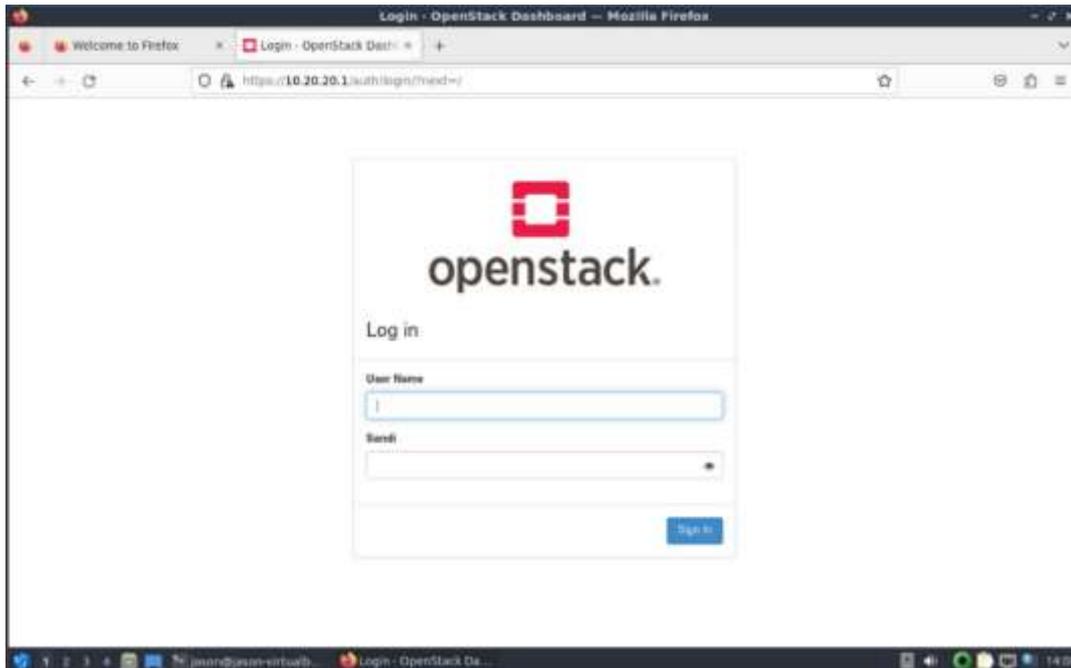
Gambar 8. Menghubungkan ke instance melalui SSH

4. Mendapatkan password yang akan digunakan untuk login di OpenStack. Command : `sudo snap get microstack config.credentials.keystone-password`

```
jason@jason-virtualbox:~$ sudo snap get mi  
e-password  
aSiLCyDxSiUrYcwLQ1k8lKx3wULGy6l3
```

Gambar 9. Password untuk OpenStack

5. Masuk ke browser Lubuntu dan masuk ke alamat <https://10.20.20.1> lalu klik Advanced > Accept the Risk and Continue, kemudian akan diarahkan ke halaman berikut.



Gambar 10. Tampilan login OpenStack

3.2 Hasil Simulasi

Setelah semua konfigurasi telah dilakukan disetiap router beserta Firewall telah terhubung secara dynamic dan juga terhubung ke NAT sehingga dapat mengakses internet serta melakukan ping ke masing – masing router seperti pada gambar berikut.

1. Router R1

```

Gateway of last resort is 192.168.122.1 to network 0.0.0.0

R1#show ip route
C    192.168.122.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
O    192.168.2.96/28 [118/2] via 192.168.2.88, 00:11:22, FastEthernet2/0
C    192.168.2.88/28 is directly connected, FastEthernet2/0
O    192.168.2.88/29 [118/1] via 192.168.2.81, 00:01:38, FastEthernet0/0
O    192.168.2.80/26 [118/2] via 192.168.2.82, 00:11:22, FastEthernet1/0
S*   0.0.0.0/0 [254/0] via 192.168.122.1
R1#ping google.com

Translating "google.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.253.119.138, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/36 ms
R1#
    
```

Gambar 11. IP Route pada R1 dan NAT

2. Router R2

```

Gateway of last resort is 192.168.2.89 to network 0.0.0.0

R2#show ip route
O    192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
O    192.168.2.96/28 [118/1] via 192.168.2.81, 00:01:38, FastEthernet0/0
O    192.168.2.88/29 [118/1] via 192.168.2.81, 00:01:38, FastEthernet0/0
C    192.168.2.80/28 is directly connected, FastEthernet0/0
C    192.168.2.80/26 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 [1/0] via 192.168.2.89
R2#ping google.com

Translating "google.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.253.119.138, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/97/212 ms
R2#
    
```

Gambar 12. IP Route pada R2 dan NAT

3. Router R3

```

Gateway of last resort is 192.168.2.89 to network 0.0.0.0

R3#show ip route
O    192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.2.96/28 is directly connected, FastEthernet1/0
C    192.168.2.88/29 is directly connected, FastEthernet0/0
O    192.168.2.88/29 [118/1] via 192.168.2.81, 00:02:04, FastEthernet0/0
O    192.168.2.80/26 [118/1] via 192.168.2.89, 00:02:04, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.2.89
R3#ping google.com

Translating "google.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.253.119.138, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/98/132 ms
R3#
    
```

Gambar 13. IP Route pada R3 dan NAT

4. Cisco ASA Firewall

```

Gateway of last resort is 192.168.2.97 to network 0.0.0.0

R4#show ip route
S*   0.0.0.0/0 [0/0] via 192.168.2.97, outside
C    192.168.2.64/25 255.255.255.240 is directly connected, inside
C    192.168.2.65/25 255.255.255.255 is directly connected, inside
C    192.168.2.96/25 255.255.255.240 is directly connected, outside
C    192.168.2.98/25 255.255.255.255 is directly connected, outside
C    192.168.2.104/25 255.255.255.240 is directly connected, dmz
C    192.168.2.105/25 255.255.255.255 is directly connected, dmz

R4#show ip nat
R4#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/34/40 ms

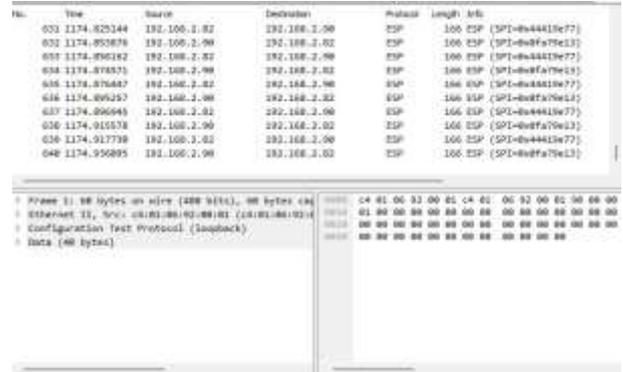
R4#ping google.com

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.253.119.138, timeout is 2 seconds:
Success rate is 60 percent (3/5), round-trip min/avg/max = 110/116/140 ms

R4#
    
```

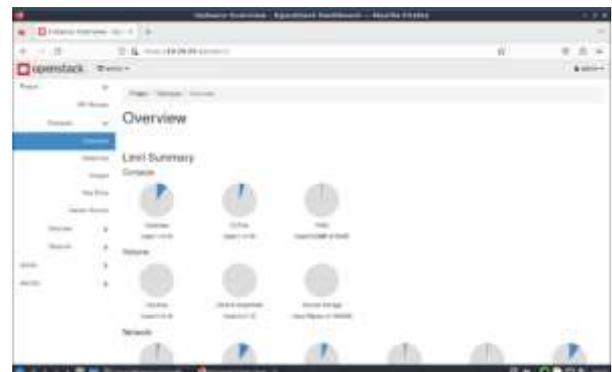
Gambar 14. IP route pada cisco dan NAT

Koneksi antara R2 dan R3 menggunakan protocol ESP (Encapsulating Security Payload) yang berfungsi untuk mengenkripsi data yang dikirim oleh pengguna seperti pada gambar berikut.



Gambar 15. Hasil VPN pada wireshark

Selanjutnya kita dapat masuk ke halaman login OpenStack yaitu dengan cara memasukkan username default dari OpenStack “admin” serta password yang kita masukkan berupa key yang kita peroleh dari Gambar 9. Berikut adalah tampilan halaman ketika berhasil login.



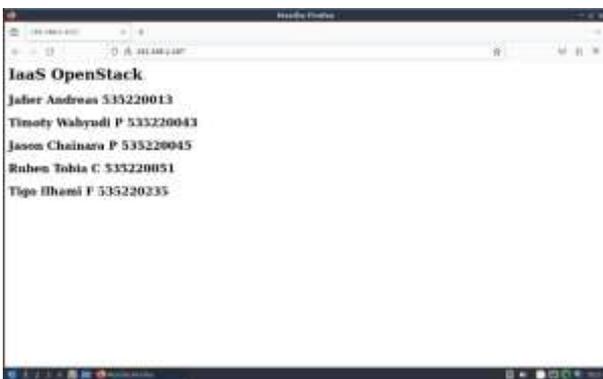
Gambar 16. Tampilan dashboard OpenStack

Kita juga dapat melihat informasi tentang instance cloud yang ada di OpenStack Cloud, sebagai contoh pada Gambar 8 dibuat instance dengan nama test, hasilnya dapat dilihat melalui Gambar 17 instance tersebut ada di bagian pertama dengan beberapa informasi seperti Instance name, Image name, IP Address, Flavor, Key pair, Status, Availability zone, Task, Power state, Age dan Actions.



Gambar 17. Daftar instance cloud

Untuk *web server* dapat diakses menggunakan HTTPS/HTTP melalui web browser dengan cara memasukkan IP Address dari *web server*, untuk lebih lengkapnya dapat dilihat melalui gambar berikut.



Gambar 18. Web server HTTP/HTTPS

4. Kesimpulan

Berdasarkan hasil simulasi jaringan sistem terdistribusi menggunakan OpenStack diperoleh beberapa kesimpulan yaitu:

1. Diperoleh manfaat pada lingkungan jaringan dalam hal efisiensi, keamanan dan fleksibilitas jika menggunakan dua server yang berperan sebagai *web server* serta *cloud server*. Hal ini diperkuat dengan penggunaan VPN dan Firewall.
2. Ubuntu sebagai basis sistem operasi mempunyai kelebihan dalam memberikan efisiensi penggunaan sumber daya, sehingga bermanfaat bagi server – server yang bekerja dalam lingkungan *cloud* serta memiliki desain yang ringan.
3. Dibutuhkan memori, storage dan CPU yang cukup besar untuk menjalankan OpenStack merupakan salah satu kekurangan dari simulasi jaringan sistem terdistribusi ini jika dijalankan melalui software GNS3 di laptop.

Hasil simulasi yang dilakukan secara keseluruhan telah memberikan hasil yang positif akan tetapi hasil ini belum teruji secara nyata karena kondisi simulasi tidak sepenuhnya mencerminkan lingkungan produksi yang kompleks, untuk kedepannya diharapkan kinerja

simulasi ini dapat ditingkatkan dengan menggunakan hardware yang lebih canggih serta peningkatan akurasi keamanan lebih baik lagi agar bisa menjawab segala tantangan keamanan perusahaan atau organisasi.

REFERENSI

- [1] DCloud, "Apa itu Cloud Computing? Pengertian, Jenis Layanan, dan 5 Kelebihan Menggunakannya," PT. Datacomm Diangraha, 15 Agustus 2023. [Online]. Available: <https://dcloud.co.id/blog/apa-itu-cloud-computing.html>. [Accessed 24 November 2023].
- [2] V. C. Q. A. X. X. G. B. S. L. Lewis Golightly, "Adoption of cloud computing as innovation in the organization," *International Journal of Engineering Business Management*, vol. 14, 2022.
- [3] Cisco, "What Is a Firewall?," Cisco Systems, Inc, [Online]. Available: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>. [Accessed 23 November 2023].
- [4] Amazon Web Service, "Apa itu Middleware?," Amazon Web Services, Inc., [Online]. Available: <https://aws.amazon.com/id/what-is/middleware/#:~:text=Aplikasi%20terdistribusi%20adalah%20program%20perangkat,atas%20aplikasi%20frontend%20dan%20backend..> [Accessed 24 November 2023].
- [5] Red Hat, "Understanding OpenStack," Red Hat, Inc., 3 Oktober 2021. [Online]. Available: <https://www.redhat.com/en/topics/openstack>. [Accessed 24 November 2023].
- [6] GNS3, "Getting Started with GNS3," Galaxy Technologies LLC., [Online]. Available: <https://docs.gns3.com/docs/>. [Accessed 24 November 2023].