Simulasi Jaringan untuk Sistem Terdistribusi E-Commerce Joomla dengan GNS3

Kevin Jonathan JM [1] Marchella Angelina [2] Arya Wira Kristanto [3]
Nicholas Martin [4] Jason Permana [5]
[1) 2) 3) 4) 5)]Teknik Informatika, FTI, Universitas Tarumanagara
Jl. Letjen S Parman no 1, Jakarta 11440 Indonesia
email : [1)] kevin.5352200038@stu.untar.ac.id, [2)] marchella.535220001@stu.untar.ac.id,
[3)] arya.535220004@stu.untar.ac.id, [4)] nicholas.5352200027@stu.untar.ac.id, [5)] jason.535220002@stu.untar.ac.id

ABSTRAK

Di era ini, E-Commerce bukanlah hal yang asing lagi karena hadir dalam berbagai bentuk, seperti website, dan untuk mengakomodasi layanan tersebut, dibutuhkan server database dan server web untuk menjaga semua data yang diperlukan. Ketika berbicara tentang E-Commerce, hosting server mungkin akan dilakukan oleh pihak lain, karena koneksi internet dibutuhkan antara klien E-Commerce (klien web) dan server hosting.

Melalui penggunaan GNS3, dimungkinkan untuk mensimulasikan koneksi-koneksi yang disebutkan di atas secara virtual. Dalam artikel jurnal ini, koneksi antara web client sebagai outside zone, web server, Joomla server, dan client server sebagai demilitarized zone (DMZ), dan host client sebagai inside zone akan dibangun melalui Cisco ASA untuk mensimulasikan akses yang aman ke website yang dihosting oleh web server dan Joomla server melalui web client.

Hasil simulasi menunjukkan keberhasilan untuk mengakses Web Server dan Joomla Server menggunakan web browser melalui client pada outside zone sementara client pada inside zone berhasil mengakses Web Server dan Joomla Server baik melalui web browser maupun ping di terminal.

Kata Kunci

E-Commerce, Joomla, GNS3, Firewall, NAT, VPN, VLSM

1. Pendahuluan

Dewasa ini, *E-Commerce* atau perdagangan elektronik telah menjadi salah satu aspek fundamental yang berhasil menunjang perekonomian digital dunia, mengungguli pertumbuhan ekonomi dari bisnis konvensional. Tak dapat dipungkiri, tak sedikit bisnis konvensional yang kini beralih untuk mengadopsi model bisnis berbasis internet atau *E-Commerce* [1]. Pasalnya, penyebaran *E-Commerce* dewasa ini belum sepenuhnya optimal dan menyimpan segudang aspek yang masih perlu ditingkatkan.

Dalam perancangan *E-Commerce* berbasis *website*, berbagai macam *tools* menjadi kunci untuk memastikan pengembangan dan pengujian berjalan secara efisien. Tahapan perancangan ini melibatkan GNS3 sebagai simulator jaringan yang memfasilitasi pembuatan infrastruktur jaringan untuk mendukung dan menguji operasional situs *E-Commerce*, VirtualBox VM untuk membuat mesin virtual dan menciptakan lingkungan pengembangan yang terisolasi, memungkinkan pengujian tanpa risiko pada sistem operasi *host*, Joomla sebagai *Content Management System* (CMS) yang memberikan kemampuan untuk membuat dan mengelola konten situs *E-Commerce*, termasuk halaman produk dan katalog, MySQL sebagai *Relational Database Management System* (RDBMS) yang digunakan untuk menyimpan dan mengelola data transaksi, produk, dan pelanggan, XAMPP sebagai *web server localhost*, dan WinSCP sebagai aplikasi untuk transfer *file* yang dapat memudahkan pengembang dalam mentransfer *file* situs *E-Commerce* dari lingkungan pengembangan lokal ke *server*.

2. Studi Pustaka

2.1 Rancangan Topologi Jaringan

Pada perancangan ini, topologi jaringan yang penulis sediakan mengusung arsitektur DMZ yang berfokus pada 3 zona yang umum digunakan dalam *enterprise networks*. Topologi ini terdiri dari 3 zona berbeda dengan masing-masing zona memiliki tujuan spesifik dalam melindungi data dan sumber daya jaringan untuk memastikan penggunaan protokol komunikasi yang aman.

2.1.1 *Firewall*

Firewall adalah perangkat jaringan yang dapat melindungi keamanan jaringan komputer dengan menyaring masuk dan keluarnya data di jaringan. Lalu lintas jaringan yang tidak diinginkan akan diblokir untuk melindungi dari berbagai serangan merugikan, seperti halnya *Denial-of-Service* (DoS) atau *malware*. *Firewall* menggunakan *Access Control List* (ACL) untuk mengatur izin akses ke internet. ACL akan memeriksa setiap jaringan yang masuk untuk menyaring jaringan yang tidak memiliki izin agar tidak dapat mengakses internet. Pada topologi ini, ACL memberikan semua *subnet* akses ke internet.

Firewall bekerja dengan membagi jaringan menjadi 3 zona berbeda. Pembagian zona ini didasarkan pada tingkat kepercayaan lalu lintas yang berasal dari zona

yang bersangkutan. Berikut adalah penjelasan dari masing-masing zona:

2.1.1.1 *Inside Zone*

Inside Zone adalah zona paling aman (*trusted zone)* yang digunakan sebagai jaringan internal *enterprise* dan umumnya menampung *database* yang berisi data dan sumber daya sensitif yang tidak dapat diakses oleh karyawan biasa [2]. Dikatakan paling aman karena *firewall* pada zona ini dikonfigurasi dengan *security level* 100 yang artinya *firewall* memblokir seluruh lalu lintas jaringan yang tidak dikenal, tidak sah, atau dianggap berbahaya untuk lolos ke zona ini. Zona ini berisi perangkat-perangkat yang digunakan oleh *client work from office*.

2.1.1.2 *Demilitarized Zone* (DMZ)

DMZ adalah zona perantara (*buffer*) di antara *inside zone* dan *outside* yang dirancang untuk meningkatkan keamanan jaringan dengan mengisolasi dan melindungi data dan sumber daya sensitif *inside zone* dari kemungkinan berbagai serangan merugikan yang terjadi dari luar (internet). *Enterprise* atau organisasi yang menggunakan metode DMZ dapat memastikan bahwa *web server* dan *database* mereka tidak secara langsung terhubung dengan internet, sehingga efektif dalam meminimalisir risiko serangan. Zona ini harus dilindungi dari akses publik yang tidak sah, tetapi juga harus dapat diakses oleh siapapun memiliki izin, seperti karyawan, pelanggan, atau mitra bisnis [3].

Zona ini digunakan untuk menampung *web server* dan *database* yang berisi data dan sumber daya kurang sensitif yang dapat diakses oleh karyawan, pelanggan, atau siapapun yang memiliki izin. Karena lalu lintas jaringan pada zona ini mengalir keluar dari jaringan internal ke jaringan eksternal (*outgoing*), maka dapat dikatakan bahwa zona ini kurang aman (*less secure*). Tidak seperti *inside zone*, *firewall* pada zona ini dikonfigurasi dengan *security level* 50 yang artinya *firewall* akan memblokir sebagian besar lalu lintas jaringan yang tidak dikenal atau dianggap berbahaya untuk lolos ke zona ini.

2.1.1.3 *Outside Zone*

Outside Zone adalah zona yang terbuka ke internet. Zona ini berisi perangkat-perangkat yang digunakan oleh *client work from branch office* atau *work from home*. *Firewall* pada zona ini dikonfigurasi dengan *security level* 0 yang artinya tidak ada aturan *firewall* sama sekali atau *firewall* tidak memblokir lalu lintas jaringan yang tidak dikenal, tidak sah, atau dianggap berbahaya untuk lolos ke zona ini.

2.1.2 *Network Address Translation* (NAT)

Dalam topologi rancangan penulis, terdapat 2 jaringan: privat dan publik. Jaringan privat adalah jaringan yang digunakan oleh perangkat-perangkat internal, seperti PC dan *server*. Sedangkan, jaringan publik adalah jaringan yang digunakan untuk berkomunikasi dengan perangkat di luar jaringan publik, seperti internet.

Network Address Translation (NAT) adalah perangkat yang mengubah alamat IP dari perangkat di jaringan privat menjadi alamat IP publik yang digunakan di internet. Penulis melakukan konfigurasi NAT pada *router* (R1) yang memiliki 2 antarmuka: satu untuk jaringan privat dan satu untuk publik (internet). Ketika perangkat di jaringan privat mengirimkan paket data ke jaringan publik, *router* akan mengubah alamat IP dari paket data tersebut menjadi alamat IP publik. Untuk memperoleh IP publik, penulis menggunakan *website* https://WhatsMyIP.com yang diakses dari dalam *inside zone*. IP publik pada topologi rancangan penulis adalah 182.3.51.47.

2.1.3 *Variable Length Subnet Mask* (VLSM)

Variable Length Subnet Mask (VLSM) adalah teknik *subnetting* yang penulis implementasikan untuk memungkinkan administrator jaringan membagi ruang alamat IP ke dalam *subnet* dengan ukuran yang berbeda-beda berdasarkan jumlah *host*. Teknik ini dilakukan untuk meningkatkan keamanan dan efisiensi penggunaan alamat IP dengan mengalokasikan alamat secara efisien sesuai dengan kebutuhan masing-masing *subnet*. Penulis memilih menggunakan teknik VLSM, karena *Static Length Subnet Mask* (SLSM) hanya dapat menggunakan *subnet mask* dengan panjang yang sama untuk setiap *subnet*. Hal ini tentu menyebabkan pengalokasian alamat IP yang tidak efisien. Sebaliknya, VLSM dapat menggunakan *subnet mask* dengan panjang yang berbeda-beda untuk setiap *subnet*. Oleh karena ini, VLMS adalah pilihan yang tepat untuk mengakomodasi kebutuhan 5 *subnet* penulis.

2.2 Joomla

Joomla adalah *open-source Content Management System* (CMS) yang digunakan untuk mempublikasikan konten *web* dan ditulis menggunakan bahasa pemrograman PHP dan MySQL. Penulis menggunakan Joomla 5.0.0 Stable yang telah diunduh dari halaman https://downloads.joomla.org/ untuk membangun *website e-commerce* karena sifatnya yang fleksibel dan dapat dengan mudah disesuaikan dengan kebutuhan *enterprise*. Joomla menyediakan beraneka ragam modul dan ekstensi yang dapat digunakan untuk menambah fungsionalitas baru ke *website* penulis. Pasalnya, Joomla juga telah dilengkapi dengan fitur keamanan yang ketat untuk meminimalisir risiko serangan dengan menyediakan pembaruan keamanan secara berkala. Joomla juga mengimplementasikan teknik *caching* untuk memberikan kinerja yang lebih optimal. Terlepas dari itu, Joomla juga menyediakan komunitas dan sumber daya yang besar untuk membantu penulis menggunakan Joomla.

Penulis melakukan proses instalasi Joomla secara manual, yang melibatkan serangkaian langkah-langkah berikut:

1. *Database* MySQL dibuat menggunakan XAMPP melalui phpMyAdmin,
2. Berkas direktori Joomla diunduh, diunggah, dan di ekstrak ke dalam direktori *root* pada *website* penulis, direktori ini bernama "htdocs",
3. Pengaturan *website* Joomla dijalankan melalui http://localhost/(nama-ecommerce),
4. Pengaturan di konfigurasi dan instalasi Joomla dikonfirmasi.

3. Hasil Percobaan

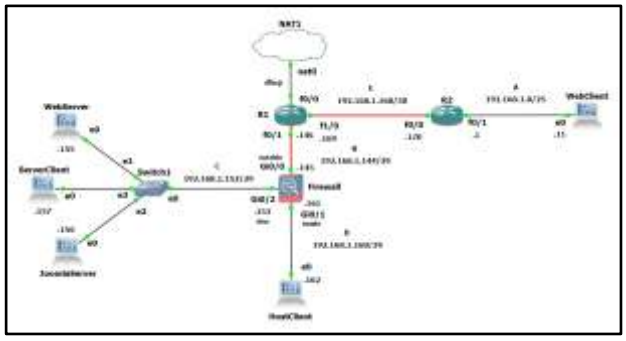
3.1 Instalasi dan Pengaturan

Alamat IP asli adalah 192.168.1.0/24 yang dapat menampung hingga 256 - 2 = 254 *hosts*. Namun, penulis perlu membaginya menjadi 5 s*ubnet* dengan jumlah *host* 100, 4, 4, 4, dan 2. Tabel 1 menunjukkan hasil *subnetting* menggunakan metode *Variable Length Subnet Mask* (VLSM) untuk alamat IP asli 192.168.1.0/24, S adalah nama *subnet*, N (*needed*) adalah jumlah *host* yang diperlukan, A (*allocated*) adalah jumlah *host* yang dialokasikan, dan R (*range*) adalah rentang alamat IP yang dapat digunakan.

Tabel 1 Hasil *Subnetting* untuk alamat IP asli 192.168.1.0/24

S	**N**	**A**	**Network**	**Broadcast**
A	100	126	192.168.1.0	192.168.1.127
			R: 192.168.1.1-192.168.1.126 Mask: /25	
B	4	6	192.168.1.144	192.168.1.151
			R: 192.168.1.145-192.168.1.150 Mask: /29	
C	4	6	192.168.1.152	192.168.1.159
			R: 192.168.1.153-192.168.1.158 Mask: /29	
D	4	6	192.168.1.160	192.168.1.167
			R: 192.168.1.161-192.168.1.166 Mask: /29	
E	2	2	192.168.1.168	192.168.1.171
			R: 192.168.1.169-192.168.1.170 Mask: /30	

Gambar 1 menunjukkan *layout* rancangan topologi *e-commerce* Joomla dengan GNS3 yang terdiri dari 3 buah PC, 2 buah *server*, 1 buah *switch*, 1 buah *firewall*, 2 buah *router*, dan 1 buah NAT.



Gambar 1. *Layout* Rancangan Topologi *E-Commerce* Joomla dengan GNS3

Topologi penulis terdiri dari 3 zona digunakan untuk meningkatkan keamanan jaringan dengan cara memisahkan perangkat-perangkat dengan tingkat keamanan yang berbeda-beda.

Inside zone terdiri dari 1 buah PC sebagai HostClient yang telah diinstalasi dengan sistem operasi Lubuntu 22.04 LTS dan memiliki akses penuh terhadap jaringan untuk menguji konektivitas dengan *server*. *Client* pada zona ini dapat mengakses *server* baik melalui *web browser* atau ping di *terminal* / *command prompt*.

DMZ terdiri dari 2 buah *server*: 1 untuk WebServer yang menampung halaman HTML berisi *platform showroom* mobil Porsche bernama "Ngemudi" dan 1 untuk JoomlaServer yang menampung integrasi Joomla beserta *built-in* MySQL *database*, zona ini juga terdiri dari 1 buah PC yang telah diinstalasi dengan sistem operasi Tiny10 sebagai ServerClient yang berfungsi untuk mentransfer *file* ke kedua *server*: WebServer dan JoomlaServer dengan menggunakan bantuan *third-party app* WinSCP. Adapun protokol yang digunakan adalah *Secure File Transfer Protocol* (SFTP). Pada zona ini juga terdapat 1 buah *switch* yang menghubungkan WebServer, JoomlaServer, dan ServerClient ke *router*.

O*utside zone* terdiri dari 1 buah PC sebagai WebClient yang telah diinstalasi dengan sistem operasi Lubuntu 22.04 LTS (*Clone*) dan tidak memiliki akses penuh ke *server*. *Client* pada zona ini hanya dapat mengakses *server* melalui *web browser*, tepatnya melalui 2 *port*: *port* 80 untuk http dan *port* 443 untuk https menggunakan *assigned* IP. Pada zona ini juga terdapat 2 buah *router* yang digunakan untuk menghubungkan internet ke *firewall* dan *client* ke internet melalui VPN, dan 1 buah NAT.

Tabel 2 menunjukkan rincian alamat IP untuk *layout* rancangan topologi *e-commerce* Joomla dengan GNS3.

Tabel 2 Rincian IP untuk *Layout* Rancangan Topologi pada Gambar 1

Device	**IP Asal**	**Tujuan Interface**	**IP Koneksi**
Cisco Asa	192.168.1.161	Lubuntu #Gi0/1	192.168.1.162
Cisco Asa	192.168.1.153	Web Server Joomla Server Server Client #Gi0/2	192.168.1.155 192.168.1.156 192.168.1.157
Cisco Asa	192.168.1.145	R1 #Gi0/0	192.168.1.146
Inside Zone			
Lubuntu	192.168.1.162	Cisco Asa #Eth0	192.168.1.161
DMZ			
Web Server	192.168.1.155	Cisco Asa#Eth0	192.168.1.153
Joomla Server	192.168.1.156	Cisco Asa#Eth0	192.168.1.153
Server Client	192.168.1.157	Cisco Asa#Eth0	192.168.1.153
Outside Zone			
Web Client	192.168.1.11	R2 #Eth0	192.168.1.1
R2	192.168.1.1	Web Client #f0/1	192.168.1.11
R2	192.168.1.170	R1 #f0/0	192.168.1.169
R1	192.168.1.146	Cisco Asa #f0/1	192.168.1.145
R1	192.168.1.169	R2 #f1/0	192.168.1.170
R1	192.168.122.217 (DHCP)	NAT #f0/0	182.3.51.47 (IP Publik)

3.1.1 *Setup* Jaringan

Beberapa hal yang perlu diperhatikan untuk *setup* jaringan adalah sebagai berikut:

1. PC, *server*, *switch*, *firewall*, *router*, dan NAT disusun seperti *layout* rancangan topologi Gambar 1 di GNS3.
2. Semua perangkat dihubungkan dan dinyalakan.
3. Alamat IP ditambahkan untuk R1, R2, WebClient, ServerClient, HostClient, WebServer, dan JoomlaServer.

Adapun langkah-langkah yang perlu dilakukan untuk *setup* jaringan adalah sebagai berikut:

1. Lakukan *setup* pada *router* R1 dengan membuka *console*. Masuk ke mode konfigurasi dan mengatur IP DHCP pada *interface* f0/0. Kemudian, tetapkan alamat IP untuk *interface* f0/1 dan f1/0 sesuai pada Gambar 1. Terakhir, lakukan *routing* terhadap masing-masing *interface* dengan *gateway* yang berbeda.
2. Untuk *setup* pada *router* R2, buka *console* PuTTY. Selanjutnya, masuk ke mode konfigurasi dan tetapkan alamat IP pada *interface* f0/1 dan f0/0 sesuai pada Gambar 1. Lakukan pengaturan *routing* terhadap masing-masing *interface* dengan *gateway* yang berbeda.
3. Lakukan *setup* untuk alamat IP, *netmask*, dan *gateway* pada HostClient, WebClient, dan ServerClient sesuai dengan Gambar 1.
4. Terakhir, *setup* alamat IP pada WebServer dan JoomlaServer menggunakan Ubuntu Server.

3.1.2 *Setup Firewall*

Untuk melakukan *setup* pada *firewall*, penulis perlu masuk ke dalam mode konfigurasi. Kemudian, tetapkan alamat IP dan tingkat keamanan pada *interface* Gi0/1 yang merupakan *inside zone*. Lakukan hal yang sama untuk *interface* Gi0/2 sebagai DMZ, dan *interface* Gi0/0 sebagai *outside zone*.

3.1.3 *Setup* NAT

Pertama, lakukan *setup* NAT untuk *inside zone* di Cisco ASA. Dalam mode konfigurasi, buat *network object* untuk *subnet inside*. Lakukan penyetelan NAT dinamis antara *inside zone* dan *outside zone* menggunakan *interface*.

Berikutnya, untuk *setup* pada DMZ di Cisco ASA, masuk ke mode konfigurasi dan buat *network object* untuk *subnet* DMZ. Lakukan penyetelan NAT dinamis antara DMZ dan *outside zone* menggunakan *interface*.

Terakhir, untuk *setup* pada *outside zone* di Cisco ASA, masuk ke mode konfigurasi dan tetapkan server DNS. Kemudian, tetapkan rute default dan lakukan inspeksi ICMP dalam *policy-map global*.

Kemudian, lakukan *setup* pada *router* R1. Dalam mode konfigurasi, tetapkan *interface* f0/0 sebagai *outside* untuk NAT dan *interface* f0/1 serta f1/0 sebagai *inside*.

Selanjutnya, lakukan *setup Access Control List* (ACL) untuk memberikan izin terhadap beberapa *subnet* untuk mengakses NAT. Tetapkan sumber NAT dari *access-list* 1 dan *overload interface* f0/0. *Overload* memungkinkan banyak alamat IP internal untuk dikonversi ke satu alamat IP eksternal pada *interface* f0/0.

Pada tahap akhir, lakukan *setup* ACL pada *firewall*. Dalam mode konfigurasi, buat *network object* untuk alamat IP eksternal WebServer dan JoomlaServer dengan host yang telah ditentukan. Kemudian, buat *network object* untuk alamat IP internal WebServer dan lakukan penyetelan NAT statis antara DMZ dan *outside* ke alamat IP eksternal WebServer. Selanjutnya, buat *network object* untuk alamat IP internal JoomlaServer dan lakukan penyetelan NAT statis antara DMZ dan *outside* ke alamat IP eksternal JoomlaServer. Terakhir, lakukan pengaturan ACL pada interface *outside* untuk mengizinkan *outside zone* mengakses WebServer dan JoomlaServer melalui *port* 80 untuk http dan *port* 443 untuk https.

3.1.4 *Setup Web Servers*

Untuk melakukan *setup* pada WebServer dan JoomlaServer, penulis menggunakan *third-party apps* WinSCP yang sudah terinstall pada ServerClient untuk memindahkan data terkait *web* "Ngemudi" ke WebServer dan Joomla ke JoomlaServer.

Gambar 2. *Setup* WebServer pada ServerClient

Gambar 3. *Setup* JoomlaServer pada ServerClient

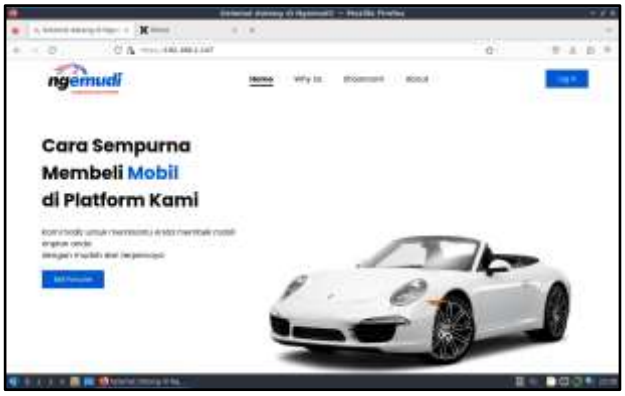
3.2 Hasil Simulasi

Dalam perancangan topologi *e-commerce* Joomla dan WebServer dengan GNS3, penulis menggunakan laptop dengan spesifikasi sebagai berikut:

Tabel 3 Spesifikasi laptop penulis

CPU	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz
GPU	NVIDIA GeForce RTX 3050 Laptop GPU GA107
RAM	16GB SODIMM DDR4-3200MHz Micron Technology 349323C9
Storage	512GB SSD NVMe PCIe 3.0 x4 SAMSUNG MZVLQ512HBLU-00B00
OS	Windows 11 Home Single Language 22H2 22621.2715

Setelah melakukan perancangan topologi pada *e-commerce*, penulis mendapatkan hasil sebagai berikut:

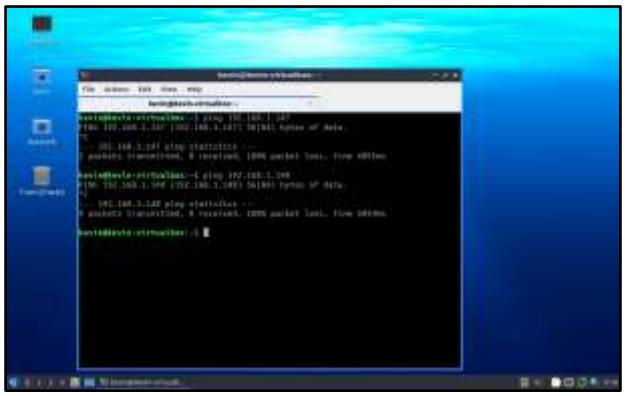


Gambar 4. Tampilan *website* Ngemudi melalui WebClient

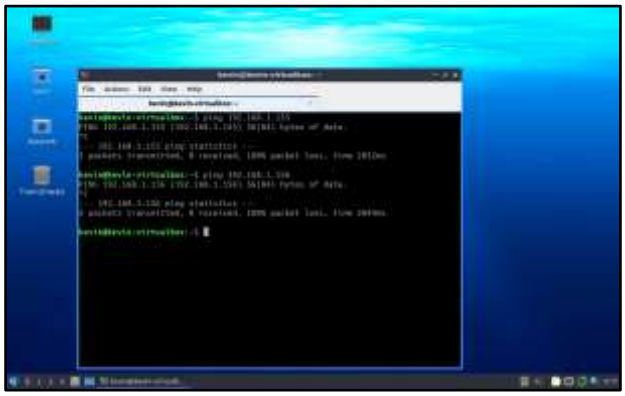
Gambar 5. Tampilan *website* Joomla melalui WebClient

Gambar 4 dan Gambar 5 menunjukkan WebClient pada *outside zone* telah berhasil mengakses *website* "Ngemudi" pada WebServer dan *E-Commerce* Joomla

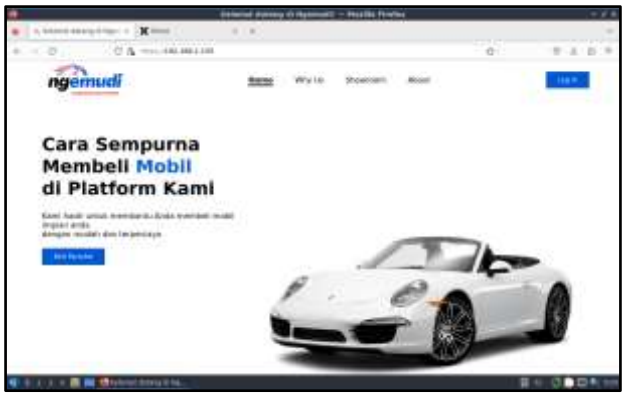
pada JoomlaServer melalui *assigned* IP 192.168.1.147 untuk WebServer dan 192.168.1.148 untuk JoomlaServer di *web browser*. Namun, WebClient hanya dapat mengakses melalui port www (port 80) dan port https (port 443), dan tidak dapat mengakses kedua *server* melalui terminal, baik menggunakan *assigned* IP ataupun menggunakan IP *server* seperti pada Gambar 6 dan Gambar 7.



Gambar 6. WebClient tidak dapat *ping* WebServer dan JoomlaServer menggunakan *assigned* IP



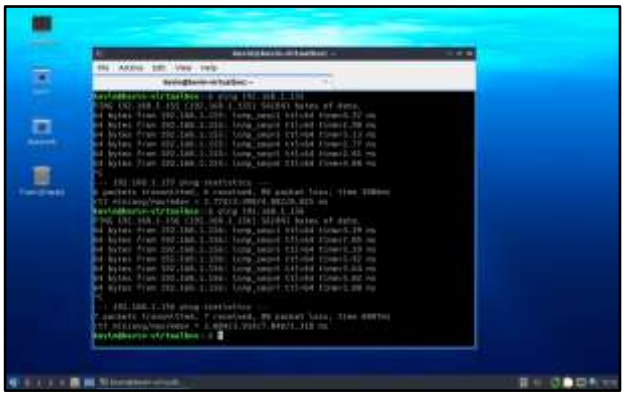
Gambar 7. WebClient tidak dapat *ping* WebServer dan JoomlaServer menggunakan IP *server*



Gambar 8. Tampilan *website* "Ngemudi melalui HostClient

Sedangkan, HostClient pada *inside zone* dapat mengakses *website* Ngemudi pada WebServer menggunakan IP *server* 192.168.1.155 dan website E-Commerce Joomla pada JoomlaServer menggunakan IP *server* 192.168.1.156 baik akses melalui *web browser* seperti pada Gambar 8 dan Gambar 9 atau melalui *ping* di *terminal/command prompt* seperti pada Gambar 10.

Gambar 9. Tampilan *website* Joomla melalui HostClient



Gambar 10. Ping WebServer dan JoomlaServer melalui *terminal* pada HostClient

4. Kesimpulan

Dalam perancangan dan simulasi jaringan untuk sistem terdistribusi *e-commerce* Joomla dan WebServer, *client* pada *outside zone* berhasil berhasil mengakses WebServer dan JoomlaServer melalui *web browser*. Sedangkan, *client* pada *inside zone* berhasil mengakses WebServer dan JoomlaServer baik melalui *web browser* atau ping di *terminal*. Keberhasilan ini mencerminkan efektivitas konfigurasi keamanan yang diterapkan dalam topologi DMZ, memberikan isolasi yang baik antara zona-zona.

Terlepas dari diperolehnya hasil yang positif, penulis belum menerapkan teknologi VPN untuk memungkinkan *client work from branch office* atau *work from home* untuk masuk ke jaringan internal enterprise dari jarak jauh. Oleh karena itu, dalam pengembangan selanjutnya, penulis menyarankan untuk mengevaluasi dan menerapkan teknologi VPN guna memperluas akses ke jaringan internal, menjaga keamanan dengan menggunakan teknologi enkripsi, hingga mendukung fleksibilitas kerja.

REFERENSI

[1] S. E. Ullah, T. Alauddin and H. U. Zaman, "Developing an E-commerce website," 2016 International Conference on

Microelectronics, Computing and Communications (MicroCom), Durgapur, India, 2016, pp. 1-4, doi: 10.1109/MicroCom.2016.7522526.

[2] C. Judd, "Network Security Zones," 9 October 2018. [Online]. Available: https://www.kwtrain.com/blog/network-security-zones.

[3] Fortinet, “DMZ Networks,” Fortinet, Inc., [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-dmz. [Accessed 25 November 2023].

[4] C. Scott, P. Wolfe and M. Erwin, Virtual Private Networks 2nd Edition, Sevastopol: O’Reilly & Associates, Inc., 1999.