SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI LMS MOODLE DENGAN GNS3

Vie Huang [1] Hezekiah Ivandi[2] Darren Natanael S[3] Dave Keane Wijaya[4] Kane Pradipa Komala[5]

[1] [2] [3] [4] [5]Teknik Informatika Universitas Tarumanagara
Jl. Letjen S. Parman No. 1, Jakarta Barat 11440
email : [1] vie.535220016@stu.untar.ac.id, [2] hezekiah.535220021@stu.untar.ac.id, [3] darren.535220046@stu.untar.ac.id, [4] dave.535220022@stu.untar.ac.id, [5] kane.535220007@stu.untar.ac.id

ABSTRACT

Dalam lanskap teknologi pendidikan yang berubah dengan cepat, integrasi langkah-langkah keamanan seperti Virtual Private Networks (VPN) dan Firewall ke dalam Leaning Management Systems (LMS) menjadi keharusan. Penelitian ini bertujuan untuk menyelidiki dan mengimplementasikan LMS yang mencakup fungsi VPN dan Firewall, dengan fokus pada peningkatan keamanan data, kontrol akses, dan integritas sistem secara keseluruhan. Metodologi penelitian memerlukan pemeriksaan menyeluruh terhadap arsitektur LMS, teknologi VPN, dan solusi Firewall yang ada. Mengambil wawasan dari literatur, prototipe LMS akan dikembangkan, menggabungkan fitur VPN dan Firewall. Efektivitas langkah-langkah keamanan terintegrasi ini akan dinilai melalui pengujian kinerja, umpan balik pengguna, dan evaluasi keamanan. Dalam penelitian ini digunakan perangkat lunak bernama GNS3 (Graphical Network Simulator 3) untuk simulasi tata letak jaringan, Cisco ASAv untuk Firewall, Moodle sebagai LMS dan Virtualbox untuk membuat mesin virtual yang dapat digunakan untuk Web Server. dan Klien Web. Jadi seperti yang ditunjukkan dalam penelitian ini, Web Client berhasil mengakses Web Server dengan aman menggunakan VPN dan Firewall untuk membuka Website LMS Moodle.

Kata kunci

LMS, VPN, Firewall, Keamanan

1. Pendahuluan

Organisasi modern berhadapan dengan tantangan besar dalam upaya membangun serta mengelola sistem jaringan yang memadai, yang tidak hanya dapat mendukung operasi kerja sehari-hari tetapi juga menjaga keamanan informasi. Di era dinamika dunia kerja saat ini, di mana mobilitas dan fleksibilitas menjadi kunci, kebutuhan akan solusi jaringan yang mendukung kerja dari rumah (*Work From Home*) dengan tingkat keamanan yang optimal semakin berkembang [1].

Pentingnya keamanan informasi dan konektivitas membuat perlunya ada usaha untuk merancang dan mensimulasikan sistem jaringan yang memenuhi persyaratan ini. Dalam konteks ini, proyek dan simulasi sistem jaringan ini dilakukan untuk memberikan solusi yang efektif .

Maksud dan tujuan dari penelitian ini adalah untuk merancang serta mensimulasikan sistem jaringan yang dapat mendukung kerja yang fleksibel, terutama dalam konteks bekerja dari rumah (*Work From Home*).

Simulasi rangkaian pada penelitian ini menggunakan aplikasi GNS3 (*Graphical Network Simulator* 3). GNS3 dapat menggunakan berbagai software seperti Vmware Workstation, Hyper-V dan Virtualbox untuk menjalankan virtualisasi sebuah sistem komputer [2]. Pada penelitian ini, *software* yang digunakan untuk virtualisasi adalah *Virtualbox*. Selain itu, perangkat-perangkat jaringan seperti router dan firewall juga bisa dijalankan melalui sebuah *GNS3 VM*.

Rangkaian yang disimulasi merupakan sebuah rangkaian jaringan untuk hosting website LMS Moodle pada *web server* dan diakses dari sebuah *web client* melalui firewall serta menggunakan VPN. *Web server* yang digunakan merupakan Ubuntu Server dan web client yang digunakan adalah Lubuntu. *Web server* dan web client tersebut dijalankan *dengan* dengan Virtualbox. Kemudian untuk firewall yang digunakan yaitu Cisco ASAv 9.8.1 yang dijalankan pada GNS3 VM.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Firewall adalah teknologi yang sangat berguna dan penting untuk melindungi jaringan, firewall adalah model atau sistem mekanisme yang diterapkan pada perangkat keras, perangkat lunak, atau sistem itu sendiri untuk memberikan perlindungan melalui keamanan apa pun. Firewall juga dapat memfilter, membatasi, dan menolak satu atau semua koneksi.

Untuk aktivitas segmen pada jaringan pribadi dan jaringan eksternal di luar cakupannya, segmen dapat

Berupa workstation, server, router, jaringan LAN, dan sebagainya.Untuk terhubung ke Internet (jaringan lain), diharuskan login (jarak jauh atau langsung) ke server firewall. Server firewall adalah sistem perangkat lunak yang memungkinkan lalu lintas jaringan yang tergolong aman untuk melewatinya dan memblokir lalu lintas jaringan yang tergolong tidak aman. [3]

Subnetting adalah pembagian sekelompok alamat IP menjadi beberapa jaringan ID tambahan dengan anggota jaringan lebih sedikit, yang disebut *subnet (subnetwork).* [4]

NAT (*Network Address Translation*) merupakan proses pemetaan alamat IP dimana perangkat jaringan komputer memberikan alamat IP publik ke perangkat jaringan lokal sehingga banyak IP privat yang dapat mengakses IP publik. Dengan kata lain *NAT* menerjemahkan alamat IP sehingga alamat IP di jaringan lokal dapat mengakses IP publik di jaringan *WAN*. [5]

Virtual Private Network (VPN) merupakan adalah metode membuat jaringan pribadi melalui jaringan publik atau Internet untuk akses jarak jauh yang aman. [6]

Transmission Control Protocol (TCP) adalah jenis protokol yang memungkinkan kelompok komputer untuk berkomunikasi dan bertukar data dalam jaringan .[7]

UDP adalah singkatan dari *User Datagram Protocol*, sebuah protokol lapisan transport TCP/IP yang mendukung komunikasi yang tidak dapat diandalkan dan tanpa koneksi antar host di jaringan menggunakan TCP/IP.[7]

2.2 Aplikasi Terdistribusi

Pengertian Moodle : Lingkungan pembelajaran yang dinamis dan modular berorientasi objek, atau yang dikenal dengan singkatan Moodle, adalah sebuah platform yang mendukung sistem manajemen pembelajaran online dan komputasi. Oleh karena itu, jika berencana untuk mengembangkan aplikasi pembelajaran seperti *e-learning*, Moodle dapat dianggap sebagai opsi yang optimal. Moodle juga merupakan aplikasi berbasis web. Aktivitas pembelajaran, termasuk akses materi, diskusi, tanya jawab, dan evaluasi, dapat dilakukan melalui antarmuka situs web menggunakan peramban (browser).

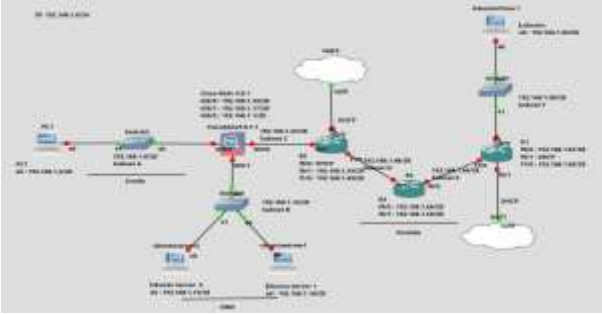
Fungsi Moodle : Fungsi utama dan tujuan pengembangan Moodle bertujuan untuk mempermudah antarmuka sistem aplikasi manajemen pembelajaran berbasis web. Platform ini juga sesuai untuk model pembelajaran jarak jauh dan online yang dapat diakses oleh guru, siswa, dan semua pihak yang terlibat dalam proses pendidikan., Fitur Moodle ada 6 yaitu :

1. *Personalized DashBoard* : Fitur utama dan tujuan dalam pengembangan Moodle adalah menyederhanakan antarmuka sistem aplikasi manajemen pembelajaran online berbasis web. Platform ini juga cocok untuk model pembelajaran jarak jauh dan *online* yang dapat diakses oleh guru, siswa, dan semua pihak yang terlibat dalam proses pendidikan.
2. *Progress Tracking* : fitur kedua ini untuk mengawasi dan menyajikan hasil evaluasi dari setiap kegiatan pembelajaran yang dilaksanakan. Dengan demikian, dapat memberikan penilaian atau hasil asesmen yang baik berdasarkan data yang *valid* dan berkualitas. Terkait fitur *Tracking* digunakan ada 5 yaitu *Course Completion, Grades, Badges, Activity Completion, Competencies.*
3. *File management* : Fitur yang ketiga ini berguna untuk menambahkan file baru yang diberi nama sesuai subjek masing-masing pengguna.Cukup tambahkan file secara otomatis menggunakan *drag* and *drop*. Cara lainnya adalah dengan menambahkan sumber daya (file, folder, link URL, dll) dari materi kursus lainnya.
4. *Peer assessment* : fitur keempat ini memiliki keunikan dimana guru dapat meminta peserta untuk membagikan ulasannya kepada teman dan peserta lainnya. Guru memiliki kendali penuh atas fitur-fitur ini dan berkomitmen untuk membantu siswa mencapai hasil yang memuaskan.
5. *Inline Feedback* : Dengan Moodle, guru tidak perlu khawatir mengenai koreksi atau umpan balik terhadap keberhasilan pembelajaran peserta. Karena Moodle memungkinkan Pengguna untuk melihat semua hasil evaluasi langsung di browser. Moodle dapat memberikan catatan tambahan (*highlight*) langsung pada file dokumen yang diunggah oleh pengguna.
6. *Multimedia Integration* : Fitur terakhir yang ditawarkan Moodle adalah integrasi dengan berbagai jenis media yang mendukung format berbeda. Hal ini menjamin pengalaman belajar yang menyenangkan dan tidak monoton. Memasukkan file multimedia seperti audio, video, dan gambar dapat dilakukan secara manual atau dengan cara embedding. Pengguna juga dapat mengunggah video langsung dari platform seperti YouTube. Untuk mengaktifkan format media lain, konfigurasi pengaturan administrator sudah cukup.

3. Hasil Percobaan

3.1 Instalasi dan Pengaturan

Rangkaian jaringan pada penelitian ini terdapat sebuah *virtual machine Lubuntu* sebagai *web client* dan dua buah *virtual machine* Ubuntu Server sebagai *web server* dan database *server*. *Web client* tersebut akan dihubungkan ke *web server* melalui berbagai router dan melewati sebuah *firewall*, selain itu untuk menjamin keamanan koneksi dari *web client* ke *web server* akan digunakan juga *VPN*. Untuk *layout* rangkaian jaringan tersebut bisa dilihat pada Gambar 1.



Gambar 1 Layout dan IP Rangkaian Jaringan

Dapat dilihat dari Gambar 1, rangkaian ini dapat dibagi menjadi 3 bagian berdasarkan level keamanannya yaitu, *inside*, *dmz* dan *outside*.

Bagian *inside* disimulasikan sebagai tempat sistem admin mengkonfigurasi rangkaian jaringannya, pada bagian ini diberikan *security* level 100 sehingga bagian lain yang security levelnya lebih rendah seperti dmz dan *outside* tidak bisa mengaksesnya.

Kemudian untuk bagian dmz, bagian ini disimulasikan sebagai tempat *hosting web server* dan *database server*. *Security level* pada bagian ini adalah 50, berarti bagian *inside* dapat mengakses bagian ini namun bagian *outside* tidak dapat mengaksesnya. Maka, agar *web client* yang terdapat di *outside* dapat mengakses *web server*, digunakan sebuah ip pada *outside* untuk sebagai ip dummy *web servernya*.

Terakhir, untuk bagian outside disimulasikan sebagai tempat dimana *user* mengakses *web servernya*. Pada bagian ini juga terdapat dua *NAT* yang berfungsi untuk memberikan akses internet. *NAT* pertama berfungsi untuk memberikan akses internet kepada *web client* dan *NAT* yang kedua untuk memberikan akses internet untuk bagian inside dan dmz melalui *firewall*. Bagian ini memiliki *security level* yang paling rendah yaitu 0 sehingga bagian-bagian lain dapat mengakses bagian ini, namun untuk bagian *outside* dapat mengakses ke bagian lain diperlukan konfigurasi access list pada *firewall.*

Instalasi yang dilakukan pada simulasi rangkaian ini yaitu instalasi Lubuntu, Ubuntu Server, Cisco ASAv 9.8.1 sebagai *firewall* dan instalasi Moodle dan PostgreSQL pada ubuntu server sebagai *Website* LMS yang digunakan.

Instalasi Lubuntu hanya mengikuti saja langkah-langkah yang tertera pada *installer* Lubuntu kemudian *reboot* pada sudah selesai instalasi. Instalasi Ubuntu *server* juga demikian dengan langkah tambahan untuk mencentang opsi instalasi *Openssh Server* pada saat instalasi.

Instalasi Cisco ASAv 9.8.1 dilakukan dengan tahap-tahap sebagai berikut :

1. Tekan menu *file* pada *GNS3* kemudian tekan menu *import appliance.*
2. Akan muncul *pop up* untuk *browse* dimana letak *appliance* Cisco ASAv yang ingin di *import* dan pilih sesuai dengan tempat *download appliance* Cisco ASAv tersebut.
3. Setelah itu terdapat beberapa opsi yang dapat dipilih. Pilih install the appliance on *GNS3 VM*. Kemudian tekan tombol *next*.
4. Pada pilihan *Qemu binary* pilihlah *qemu-system-x86_64*. Kemudian tekan tombol *next*.
5. Pilihlah versi Cisco ASAv yang ingin di *install.* Untuk penelitian ini, versi yang di install adalah ASA versi 9.8.1 Apabila belum ada yang bisa diinstall perlu di import terlebih dahulu. Setelah pilih *versinya* tekan tombol *next.*
6. Tekan tombol *finish* dan Cisco ASAv telah ter install.

Instalasi Moodle dilakukan pada Ubuntu Server. Sebelum Moodle dapat diinstall butuh beberapa hal yang perlu di install terlebih dahulu yaitu Apache2, PHP dan sebuah *database server*. Pada penelitian ini, *database server* yang digunakan adalah PostgreSQL. Berikut adalah langkah-langkah menginstalasi Moodle.

1. Apache2, PHP dan PostgreSQL bisa diinstall pada Ubuntu server menggunakan package manager apt. Cara menginstallnya yaitu dengan menjalankan *command "apt install apache2* php postgresql" sebagai *root*.
2. Kemudian dapat download file-file yang diperlukan untuk instalasi Moodle dari website http://moodle.org/downloads atau bisa juga *clone* dari *repository git* moodle dengan "*git clone -b MOODLE_{{Version3}}_STABLE* git://git.moodle.org/moodle.git".
3. Setelah di didownload agar file-file pada folder moodle tidak dapat di *write* oleh *user* web perlu dijalankan *command* "*chown -R root /path/to/moodle" dan "chmod -R 0755 /path/to/moodle"*
4. Setelah itu perlu dibuat sebuah *database* kosong yang digunakan untuk Moodle. Pembuatan database tersebut dapat dilakukan dengan "psql -U postgres" sebagai *user postgres*. Kemudian membuat *user* dengan nama moodle *user* dengan "*postgres=# CREATE USER moodleuser WITH PASSWORD 'yourpassword';"*. Kemudian dapat dibuat juga database bernama moodle dengan *"postgres=# CREATE DATABASE moodle WITH OWNER moodleuser;".*
5. Sebelum melakukan instalasi, perlu dibuat sebuah *directory* untuk menyimpan data yang digunakan moodle. *Directory* tersebut dapat dibuat dengan *command "mkdir /path/to/moodledata"* dan kemudian jalankan *"chmod 0777 /path/to/moodledata"* untuk *installer* moodle dapat mengakses *directory* tersebut. Setelah instalasi moodle selesai disarankan untuk merubah akses dari *directory* moodledata agar tidak mudah diubah oleh pihak lain.
6. Setelah itu selesai, jalankan *installer* Moodle dengan command berikut:

1. *cd /path/to/moodle/admin/cli*
2. *sudo -u www-data /usr/bin/php install.php*
3. *chown -R root /path/to/moodle*

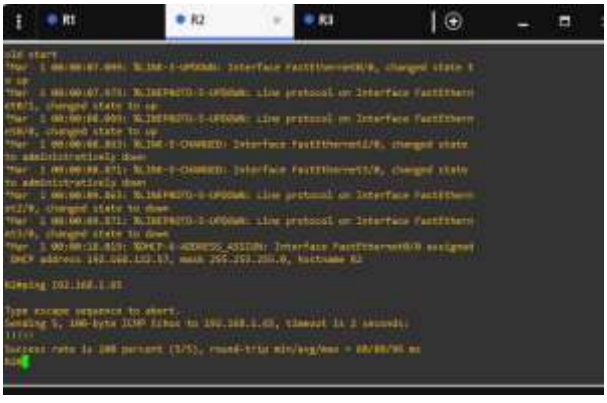
7. Jalankanlah *installer* Moodle sesuai dengan petunjuk pada *installer*. Kemudian untuk membuka *website* Moodle dapat dibuka pada *web browser* pada *web address* yang dimasukan pada saat instalasi.

3.2 Hasil Simulasi

1. Tahap Pengujian:
   1. Uji Keterhubungan: Verifikasi keterhubungan antara *web client*, *firewall*, dan *web server*. Pastikan setiap *node* dapat saling ping dan terhubung.
   2. Uji *VPN*: Konfigurasikan *VPN* antara *web client* dan *web server*. Pastikan koneksi *VPN* dapat dibuat dan data dapat dikirim secara aman.
   3. Uji *Firewall*: Konfigurasikan *firewall* untuk memblokir akses yang tidak sah. Coba akses *web server* dari *web client* tanpa *VPN* untuk memastikan *firewall* berfungsi.
   4. Uji Akses *Website*: Mencoba mengakses *website* pada *Web Server* dengan menggunakan *VPN* dan *web browser* pada *Web Client.*

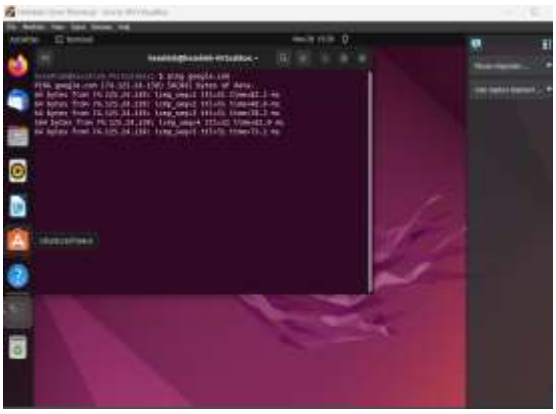
2 . Hasil Pengujian dan bukti (*screenshot*):

Uji Keterhubungan: pada tahap ini akan dilakukan pengujian setiap perangkat yang terdapat di dalam rangkaian. Tujuan dari dilakukan pengujian tahap ini yaitu untuk memastikan bahwa semua perangkat saling terhubung dengan baik. Pertama dilakukan pengujian ping antara sesama router. Pada pengujian ini akan dilakukan ping dari Router 2 ke Router 1 yang melewati Router 3. Maka dengan pengujian ini dapat membuktikan bahwa semua router dapat terhubung antara yang satu dan yang lain. Berikut adalah gambar bukti aksi ping tersebut.



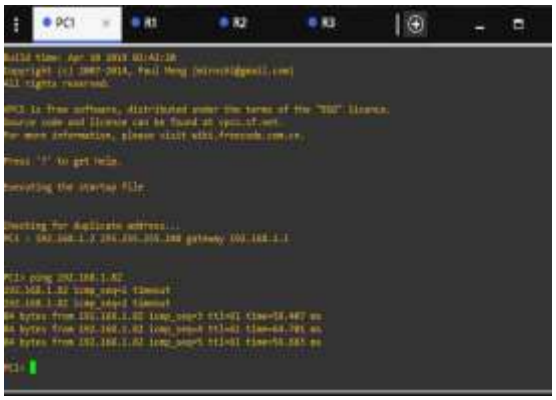
Gambar 2 Ping antara *router* 2 ke *router* 1

Kedua dilakukan pengujian ping dari Web Client ke internet. Pada pengujian ini akan dilakukan ping ke internet yang diwakili dengan ping ke google.com. Maka dengan pengujian ini dapat membuktikan bahwa koneksi NAT pada Web Client sudah terkonfigurasi dengan benar. Berikut adalah gamabr bukti aksi ping tersebut.



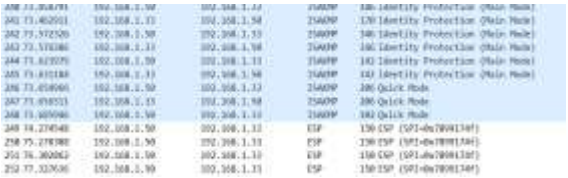
Gambar 3 Ping antara *Client* ke *internet*

Terakhir dilakukan peungujian ping dari bagian Inside ke Web Client. Pada pengujian ini akan dilakukan ping ke Web Client dari Inside dengan melewati Firewall Cisco ASAv, Router 2, Router 3, dan pada akhirnya melewari Router 1 untuk dapat terhubung ke Web Client. Maka dengan pengujian ini dapat membuktikan bahwa Firewall telah terkonfigurasi dengan baik dan dapat terhubung dengan semua ruter. Berikut adalah gambar bukti aksi ping tersebut.



Gambar 4 Ping antara *inside* ke *web client*

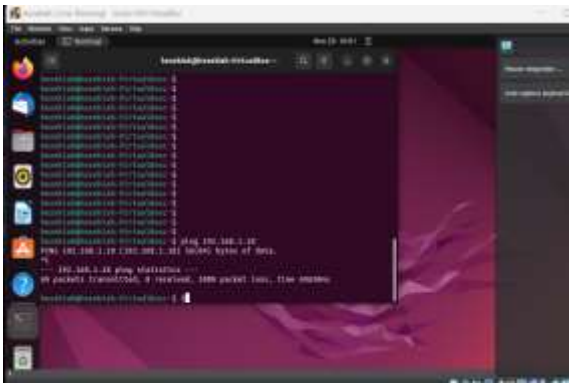
Uji VPN: pada tahap ini akan dilakukan pengujian koneksi VPN untuk mengakses Web Server dari Web Client. VPN pada rangkaian ini dikonfigurasi antara Firewall Cisco ASAv dan Router 3. Berikut adalah bukti berfungsinya koneksi VPN dengan melihat detail koneksi tersebut melalui aplikasi Wireshark.



Gambar 5 Status koneksi *VPN* di *wireshark.*

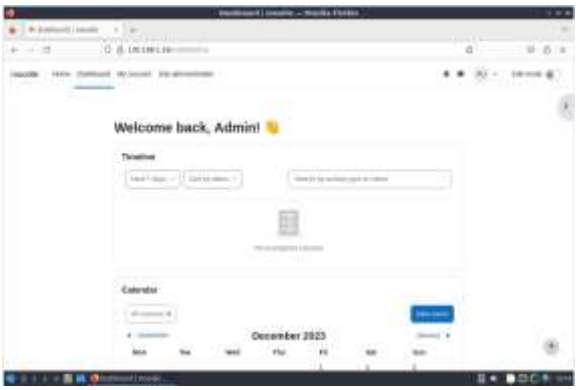
Berdasarkan gambar di atas dapat dilihat bahwa koneksi VPN telah terkonfigurasi dengan baik. Hal tersebut dapat dilihat dari IP address source dan destinationnya. IP address asli Web Client adalah 192.168.1.82 dan IP asli Web Server adalah 192.168.1.18, namun pada Wireshark dapat dilihat bahwa IP address sourcenya adalah 192.168.1.50 (IP address interface fa0/1 Router 3) dan IP address destinationnya adalah 192.168.1.33 (IP address interface Gi0/0 pada Firewall Cisco ASAv). Selain itu, protocol koneksinya juga merupakan ISAKMP dibandingkan protocol ICMP yang biasanya digunakan apabila tanpa VPN.

Uji Firewall: pada tahap ini akan dilakukan pengujian mengenai fungsionalitas Firewall tanpa VPN. Pengujian yang dilakukan yaitu ping dari Web Client ke Web Server tanpa VPN, karena Web Server berada pada bagian dmz dan Web Client berada pada bagian outside, maka tanpa penggunaan VPN Web Client tidak dapat mengakses Web Server secara langsung karena terblokir oleh Firewall. Berikut adalah bukti gambar Firewall memblokir akses Web Server dari Web Client.



Gambar 6 Ping gagal diblokir oleh *firewall.*

Uji Akses Website: pada tahap ini akan dilakukan pengujian untuk membuka website LMS Moodle yang sudah terkonfigurasi pada Web Server. Pengaksesan tersebut dilakukan pada Web Client dengan koneksi VPN, tanpa penggunaan VPN maka website tidak dapat diakses dari Web Client. Hal tersebut dikarenakan Web Client terdapat pada bagian outside yang memiliki tingkat keamanan yang lebih rendah dibandingkan bagiian dmz dimana Web Server berada. Berikut adalah bukti gambar bahwa website LMS Moodle telah diakses dengan berhasil pada Web Client.



Gambar 7 Akses *website* LMS Moodle dari *web Client.*

4. Kesimpulan

Dalam penelitian ini, keterhubungan antara *web client, firewall,* dan *web server* berhasil terhubung dengan baik. Selain itu, dengan diterapkannya *VPN*, koneksi antara *web client* dan *web server* menjadi lebih aman. Namun, tantangan atau kelemahan dalam penelitian ini terletak pada kompleksitas konfigurasi *VPN* dan *Firewall* yang membutuhkan pemahaman teknis. Selain itu, *firewall* yang terlalu ketat dapat menyulitkan akses yang seharusnya diizinkan.
Kemungkinan Pengembangan Selanjutnya yaitu:

a. Implementasi *Multi-Factor Authentication (MFA):* Menerapkan *MFA* dapat memberikan keamanan tambahan dengan memerlukan verifikasi lebih untuk mengakses sistem.
b. Peningkatan automasi pada konfigurasi *VPN* dan *Firewall* untuk memudahkan penggunaan oleh pihak non-teknis.

Secara keseluruhan, implementasi *VPN* dan *Firewall* pada simulasi sistem jaringan pada *LMS Moodle* memberikan keamanan yang penting.

REFERENSI

[1] K. Subandi and V. I. Sugara, “Analisis Serangan Vulnerabilities Terhadap Server Selama Work from Home saat Pandemi Covid-19 sebagai Prosedur Mitigasi”, *ASIIMETRIK*, vol. 4, no. 1, pp. 125-132, Jul. 2022.
[2] B. Korniyenko, L. Galata, and L. Ladieva, “Research of Information Protection System of Corporate Network Based on GNS3,” IEEE Xplore, Dec. 01, 2019. https://ieeexplore.ieee.org/abstract/document/9030472 (accessed May 09, 2022).
[3] Sugiyono, "SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE," Jurnal CKI On SPOT, p. 5, 2016.
[4] S. Thomas Susel, "Subnetting Local Area Network," p. 18, 2011.
[5] A. N. Hidasaputra, "MENGENAL KONSEP GATEWAY DAN NAT," p. 1, 2010.

[6] F. L. Rosmana, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN)," Jurnal Techno Nusa Mandiri, 2015.
[7] N. Humairah, "Penjelasan tentang Layanan pada Protokol TCP dan UDP".