Simulasi Jaringan untuk LMS Moodle dengan GNS3

Hanson Nicholas[1)] Aldo Hartanto[2)] Stefanus Anthony[3)] Benaya Juanda[4)]

[1) 2) 3) 4)]Teknik Informatika Universitas Tarumanagara,
Jl. Letjen S. Parman No. 1, Jakarta 11440 Indonesia
email : [1)] hanson.535220121@stu.untar.ac.id, [2)] aldo.535220135@stu.untar.ac.id,
[3)]stefanus.535220146@stu.untar.ac.id,[4)] benaya.535220266@stu.untar.ac.id

ABSTRAK

Pada jurnal ini dijelaskan tentang simulasi Jaringan Sekolah yang dirancang dengan website sekolah dan fitur Moodle LMS. Simulasi ini memungkinkan pekerja yang terdaftar di database untuk mengakses materi dan memanfaatkan fasilitas Moodle yang ada. Selain itu, akses diberikan kepada pegawai/staf sekolah untuk memperoleh informasi dan data dari database. Karyawan juga dapat mengakses situs web sekolah, yang didasarkan pada HTTPS, sehingga menjamin keamanannya. Website sekolah berisi konten seperti informasi tentang sekolah, program studi, kontak, dan nama anggota tim proyek. Sistem ini memberikan manfaat yang signifikan bagi pekerja sekolah seperti guru dan staf administrasi. Mereka dapat mengakses database untuk mengumpulkan informasi penting seperti tugas siswa, jadwal kelas, dan materi pembelajaran. Selanjutnya, mereka dapat mengelola data siswa, mengirimkan pengumuman ke seluruh komunitas sekolah, dan memantau kemajuan akademik siswa melalui LMS. Desain integrasi Jaringan menggunakan GNS3 untuk menciptakan struktur Jaringan yang aman dan terkendali. Semua perangkat di Jaringan memiliki konektivitas yang baik, sedangkan perangkat di DMZ memiliki akses terbatas yang hanya terbatas pada koneksi keluar. Hasilnya, keamanan Jaringan dapat dijaga secara efektif, dan perangkat di luar Jaringan tidak memiliki akses ke perangkat di dalamnya. Secara keseluruhan, simulasi ini menghasilkan DMZ dapat mengakses NAT/Internet, dan zona luar mampu mengakses aplikasi Moodle yang didistribusikan dan website sekolah berbasis HTTPS.

Keywords : *LMS, Jaringan, GNS3, Moodle, HTTPS*

1. Pendahuluan

Sistem jaringan yang efisien dan handal merupakan salah satu aspek penting dalam pengembangan dan pengujian aplikasi web. Dalam konteks ini, penggunaan GNS3 (*Graphical Network Simulator*) dapat mempermudah simulasi dan pengujian sistem jaringan yang melibatkan berbagai komponen, termasuk web server dan web client.

Proyek ini akan fokus pada pengujian akses dari web client ke dua web server yang berbeda, yaitu website sekolah dengan protokol HTTPS (*Hypertext Transfer Protocol Secure*) dan aplikasi terdistribusi Moodle dengan protokol HTTP (*Hypertext Transfer – Transfer Protoco*l). Pendekatan ini memungkinkan kita untuk menguji koneksi terhadap dua jenis server yang umum digunakan dalam lingkungan web saat ini. Moodle merupakan LMS (*Learning Management System*) yang menyediakan fasilitas yang biasa digunakan dalam pembelajaran sekolah seperti mengunggah materi, tugas, maupun ujian.

GNS3 adalah alat simulasi jaringan yang kuat yang memungkinkan untuk membuat topologi jaringan virtual dengan menggunakan berbagai perangkat jaringan seperti router, switch, dan firewall. Dalam skenario ini [1], *GNS3* akan digunakan untuk membuat jaringan virtual yang terdiri dari web client, web server berbasis HTTP, aplikasi terdistribusi Moodle, router ,switch, dan firewall Cisco ASA. Web client akan berfungsi sebagai pengguna yang mencoba mengakses kedua web server. Web sekolah akan memberikan akses ke website dengan protokol keamanan HTTPS, sedangkan web server Moodle akan memberikan akses ke platform pembelajaran Moodle. Dengan menggunakan GNS3, maka dapat mengatur konfigurasi jaringan virtual yang mencerminkan infrastruktur yang sebenarnya. Infrastruktur yang dimaksud dimana konfigurasi pada router, NAT, firewall Cisco ASA, web client, dan web server.

Pada akhirnya, tujuan dari proyek ini adalah untuk memastikan bahwa web client dapat mengakses kedua web server dengan sukses. Dalam proses pengujian ini, juga diperiksa ketersediaan jaringan, keandalan koneksi, serta keamanan akses menuju web server. Pada langkah selanjutnya, akan dijelaskan tata cara perancangan jaringan untuk mencapai tujuan yang ingin dicapai. Kemudian, konfigurasi jaringan, pengaturan server, serta pengujian koneksi dari web client juga tercangkup dalam langkah-langkah yang akan dijelaskan secara rinci.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Jaringan komputer dan keamanan komputer memiliki hubungan erat satu sama lain. Jaringan komputer merupakan koneksi antara dua atau lebih komputer yang digunakan untuk berkomunikasi antar

perangkat serta pertukaran data [2]. Di sisi lain, keamanan komputer merupakan upaya untuk melindungi sistem dari serangan atau ancaman yang dapat membahayakan. Agar jaringan komputer dapat berjalan lancar dan terlindungi dari ancaman luar, semua aspek di dalamnya harus terintegrasi dengan baik. Simulasi ini akan difokuskan pada aspek-aspek dalam jaringan seperti Subnetting, NAT, Protokol Transport dengan TCP, Layanan Aplikasi berupa DNS dan HTTPS, dan Firewall. Integrasi jaringan merupakan proses mengkoordinasikan berbagai komponen dan elemen agar jaringan dapat beroperasi secara lancar dan efisien [3]. Semua perangkat simulasi jaringan diintegrasikan agar dapat bekerja sesuai dengan kegunaannya masing-masing. Pada simulasi jaringan ini dibutuhkan IP publik untuk mengakses internet. NAT (*Network Address* Translator) berfungsi untuk mengubah alamat IP lokal ke alamat IP publik sebelum mengirimkan sebuah informasi. Ketika jaringan lokal mengirim permintaan untuk mengakses alamat publik, NAT mengubah alamat IP dari paket data yang masuk atau keluar dari jaringan, sehingga alamat IP pribadi jaringan lokal tidak terlihat oleh jaringan publik, dan kerahasiaan dari alamat IP pribadi dapat terjaga [4].

Perangkat lain yang digunakan adalah cisco ASAv yang digunakan sebagai firewall. Firewall adalah sistem keamanan yang berfungsi untuk melindungi jaringan komputer dari ancaman yang datang dari internet. Firewall berperan sebagai tembok pembatas antara jaringan lokal dan jaringan luar, sehingga meminimalisir kemungkinan pencurian data.) [5]. Router dan Switch memiliki fungsi yang hampir sama. Kedua perangkat ini memiliki fungsi untuk menghubungkan perangkat dan memproses lalu lintas data. Router berfungsi untuk menghubungkan perangkat yang berada di jaringan lokal (*Local Area Network*/LAN) dengan jaringan luar seperti internet, sedangkan Switch menghubungkan perangkat dalam satu lingkup jaringan lokal seperti laptop, printer dan lain sebagainya [6].

GNS3 merupakan aplikasi simulasi jaringan yang memungkinkan pengguna untuk membangun, merancang dan menguji jaringan di lingkungan virtual. GNS3 dapat mensimulasikan berbagai perangkat yang dibutuhkan dalam pengerjaan simulasi ini seperti router, switch, firewall dan masih banyak lagi [7]. Terdapat beberapa fasilitas dan kelebihan dari GNS3 seperti:

1. Memungkinkan membuat peta jaringan yang dinamis dan pengujian fitur-fitur tertentu seperti uji kinerja jaringan, keamanan jaringan, skalabilitas dan lain sebagainya.
2. Memiliki beban aplikasi yang ringan dengan persyaratan minimum, seperti 4 GB RAM memory, penyimpanan sebesar 1 GB, dan sistem operasi minimum untuk Windows adalah Windows 7.
3. Menjalankan dan menguji perangkat keras dari beberapa vendor [7].

Subnetting adalah sebuah proses untuk membagi sebuah IP jaringan yang besar menjadi beberapa subnet yang lebih kecil. Tujuan dari subnetting adalah untuk meningkatkan efisiensi penggunaan alamat IP, sehingga *Network* yang dibuat dapat memiliki batasan host yang sesuai dengan kebutuhan [8]. Teknik subnetting yang digunakan adalah VLSM (*Variable Length Subnet Masking*) yaitu merupakan pembagian IP berdasarkan jumlah host yang dibutuhkan setiap subnet, dengan ini penggunaan alamat ip dapat lebih optimal dan menghindari pemborosan ip [9].

Transport Protocol adalah sebuah aturan atau standar yang mengatur atau memungkinkan terjadinya koneksi, perpindahan informasi, dan transfer data antara dua atau lebih titik komputer [10]. Terdapat dua transport protocol yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP adalah protokol berbasis koneksi yang digunakan oleh sesama komputer untuk mentransfer data di dalam jaringan internet. TCP merupakan protokol yang sering digunakan pada saat ini dikarenakan kemudahan akses nya yang tersedia di banyak sistem operasi dan kelebihannya dalam mengintegrasikan banyak sekali *Network* mulai dari ethernet dial up, token ring dan lain sebagainya [11], sedangkan untuk UDP merupakan merupakan protokol yang bersifat tanpa koneksi. Cara kerja UDP yaitu membuat koneksi secara formal sebelum data ditransfer. Hal ini menyebabkan UDP memiliki respon yang cepat dan cocok digunakan untuk transmisi yang sensitif terhadap waktu, seperti pemutaran video atau pencarian DNS [12]. Dikarenakan simulasi ini membutuhkan koneksi yang stabil dan terjamin dalam pengiriman data maka digunakanlah Transmission Control Protocol untuk simulasi ini.

Application Layer merupakan layer teratas pada *Open Systems Interconnection* (OSI) yang bertujuan untuk mengatur pertukaran data yang didapat dari transmisi melalui jaringan dan menampilkannya kepada user dalam bentuk aplikasi [13]. Pada simulasi jaringan ini, layer akan bekerja dengan bantuan beberapa protokol, yaitu:

1. DNS (*Domain Name System*) bertujuan untuk mengubah URL website ke dalam bentuk IP *Address*. Dengan DNS ketika pengguna ingin mengunjungi sebuah website maka tidak perlu lagi untuk mengetikkan IP *Address* [14].

2. HTTP (*HyperText Transfer Protoco*l) merupakan protokol yang mengatur perizinan akses untuk pertukaran data antara web client dengan web server [15]. Kelemahan dari HTTP adalah keamanan yang tidak terjamin. Pada setiap informasi yang dikirim ke luar server, ada kemungkinan bahwa informasi tersebut mengalami kebocoran dan keamanan informasi menjadi tidak terjamin. HTTPS

memiliki fungsi yang sama dengan HTTP, hanya saja HTTPS menggunakan metode enkripsi pada saat mengirimkan informasi[15]. Hal ini membuat penerima menjadi satu-satunya orang yang dapat mengakses informasi tersebut, sehingga integritas informasi dapat terjaga[15].

2.2 Aplikasi terdistribusi

Simulasi ini menggunakan dua aplikasi terdistribusi yaitu website berbasis HTTPS (Website SDN 01 Anak bangsa) dan *Learning Management System* (LMS) yaitu Moodle. User dapat mengakses kedua Aplikasi terdistribusi ini dengan cara mengakses web client yang telah dihubungkan melalui router ke webserver. Moodle dirancang bagi pendidik atau administrator sebagai platform pembelajaran dengan sistem yang aman dan terintegrasi [16]. User dapat dengan mudah mengakses Moodle baik dari rumah maupun sekolah. Moodle dipilih dalam pengerjaan simulasi jaringan ini karena beberapa alasan seperti :

1. Fleksibilitas : dikarenakan Moodle menyediakan beragam alat dan fitur pembelajaran, seperti forum diskusi, pengunggahan tugas, ujian, dan lain - lain.
2. *Easy to track* : Moodle sangat mudah untuk dipantau / dilacak.
3. Teruji : Moodle merupakan LMS yang teruji dikarenakan Pengembangan yang terus berkelanjutan, dan memiliki keamanan dan privasi yang terjamin.

Website HTTPS merupakan website resmi SDN 01 Anak Bangsa yang mengandung beberapa informasi seperti program studi, kontak, anggota tim dan lain sebagainya.

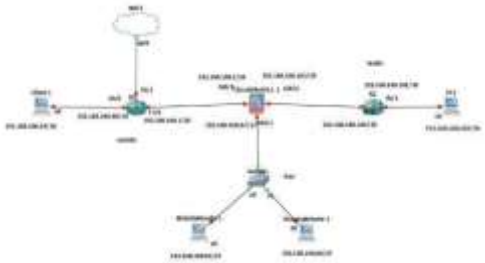
3. Hasil Percobaan

Hasil percobaan bertujuan untuk memastikan bahwa simulasi jaringan yang sudah dibuat sudah sesuai dengan rancangan dan menguji apakah pengujian akses dari web client ke dua web server yang berbeda, yaitu website sekolah dengan protokol HTTPS (*Hypertext Transfer Protocol Secure*) dan aplikasi terdistribusi Moodle dengan protokol HTTP (*Hypertext Transfer – Transfer Protoco*l) berjalan dengan baik.

3.1 Instalasi dan Pengaturan

Pada simulasi ini digunakan beberapa program seperti VirtualBox, GNS3(Graphical Network Simulator-3), dan dua Ubuntu Server yaitu website HTTPS (Website SDN 01 Anak Bangsa) dan aplikasi terdistribusi Moodle. Langkah pertama dalam pengerjaan simulasi ini adalah menentukan topologi dari simulasi jaringan. Perangkat virtual yang dibutuhkan meliputi 2 buah router, 1 VPCS (*Virtual PC Simulator)*, 1 web client berbasis Ubuntu Desktop, 1 firewall dengan menggunakan Cisco *Adaptive Security Virtual Appliance* (ASAv), 1 switch, dua buah web server berbasis ubuntu server dan komponen terakhir adalah NAT. Dalam topologi jaringan ini terdapat 3 daerah yaitu outside, dmz dan inside.

Pada daerah "outside," terdapat Router 1 yang berfungsi sebagai *Gateway* untuk web client, yang berfungsi sebagai simulasi pengguna yang ingin mengakses Moodle maupun website sekolah. Selain itu, terdapat *Network Address* Translation (NAT) yang memungkinkan akses internet bagi pengguna melalui Router 1. Di dalam zona demilitarized zone (DMZ), firewall berperan sebagai lapisan pertahanan untuk melindungi web server dari ancaman yang mungkin datang dari luar. Switch yang terhubung ke firewall di zona DMZ memiliki peran dalam mengelola koneksi antara Moodle dan website sekolah. Sementara itu, pada bagian "inside", Router 2 bertindak sebagai *Gateway* untuk PC1, memberikan akses ke jaringan internal dari luar zona DMZ.



Gambar 1. Layout Jaringan Sekolah

Setelah menentukan layout jaringan, tahap berikutnya yaitu menentukkan ip address dengan cara subnetting. Metode subnetting yang digunakan adalah *Variable Length Subnet Mask* (VLSM) dengan *Original Network* yaitu 192.168.100.0/24 dan 5 subnet dengan max hostpada tabel 1. Perhitungan VLSM didasarkan pada dokumen ngonfig.net pada bagian *references* [10].

Tabel 1. Maxhost

Subnet	Max Host
I	2
II	2
III	30
IV	2
V	60

Setelah semua subnet berhasil dibagi maka didapatkan tabel dengan *Network Address*, Gateaway dan *Interface* dari masing-masing router. Tabel ini yang akan digunakan untuk langkah selanjutnya, yaitu memberikan ip address untuk setiap perangkat seperti VPCS, web client, web server, firewall, dan router.

Tabel 2 Routing Tabel R2 (Router Area Outside)

Network	Gateaway	Interface R1

Address		
192.168.100.96/30	Connected	eth 0
192.168.100.0/26	Connected	eth 2
192.168.100.64/27	192.168.100.2	eth 2
192.168.100.104/30	192.168.100.2	eth 2
192.168.100.0/26	192.168.100.2	eth 2

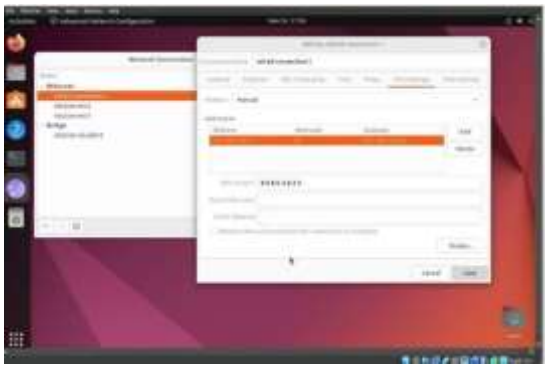
Tabel 3. Routing Tabel R2 (Router Area Inside)

Network Address	Gateway	Interface R2
192.168.100.0/30	Connected	eth 1
192.168.100.104/30	Connected	eth 0
192.168.100.64/30	192.168.100.105	eth 0
192.168.100.0/26	192.168.100.105	eth 0
192.168.100.64/27	192.168.100.105	eth 0

Langkah berikutnya adalah melakukan static routing pada router. Hal ini bertujuan untuk menentukan jalur terbaik untuk mengirimkan data pada jaringan. Gambar 2 dibawah merupakan contoh proses routing yang berhasil dimana akan muncul huruf "S" yang mengindikasikan jenis routing yang digunakan yaitu static routing dan huruf "C" yang menunjukkan rute-rute yang telah terhubung.

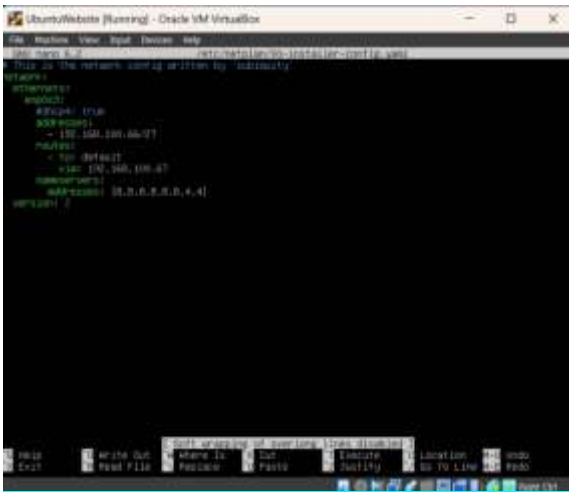
Gambar 2. Routing

Setelah melakukan konfigurasi ip *Address* pada setiap router, langkah selanjutnya yaitu melakukan konfigurasi terhadap NAT dengan cara menambahkan DHCP dan set DNS server. Selanjutnya dilakukan konfigurasi webclient (Ubuntu Desktop) yang dimulai dengan membuka Ubuntu Desktop lalu menuju menu utilities. Pada menu utilities terdapat bagian *Advanced Network Configuration* setelah itu menuju bagian wired connect untuk set *Address* dan *Gateway* (menuju kolom IPv4) seperti yang terlihat pada gambar 2.



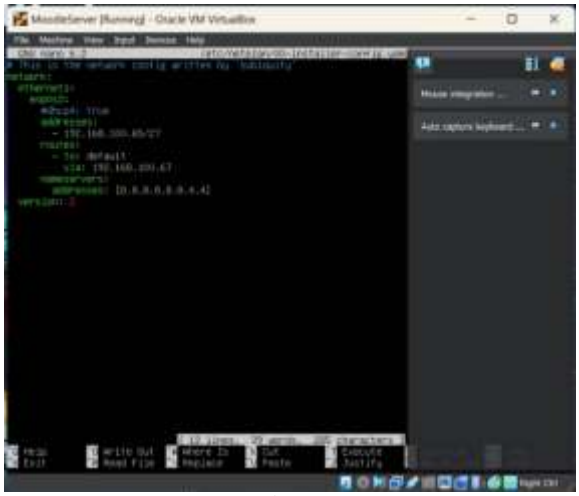
Gambar 3. Konfigurasi Web Client

Setelah proses konfigurasi webclient, dapat dilakukan proses selanjutnya yaitu konfigurasi firewall pada GNS3 dengan menggunakan perangkat Cisco-ASAv. Pada layout jaringan yang telah ada kita dapat melakukan setup Cisco ASAv dengan mendefinisikan security level dari setiap daerah. Pada daerah inside diberikan 100 security level. Hal dilakukan karena daerah inside menyimpan data internal sekolah yang penting sehingga perlu diberikan keamanan yang ekstra. DMZ diberi 50 security level dikarenakan tersimpan data-data dari web server yaitu website sekolah dan Moodle yang bersifat terbuka untuk publik, sehingga tidak memerlukan pengamanan yang terlalu ketat. Daerah outside merupakan daerah yang rentan terhadap serangan dikarenakan memiliki 0 security level.



Gambar 4. Konfigurasi Ip Web Server HTTPS

Langkah selanjutnya adalah mengkonfigurasi kedua web server. Pertama download ubuntu server lalu tambahkan dalam virtual machine, kemudian setting ip untuk web server pertama melalui terminal dengan mengetik "sudo nano /etc/netplan/00-installer-config.yaml". Lalu setting ip sesuai dengan layout jaringan yaitu 192.168.100.65/27.

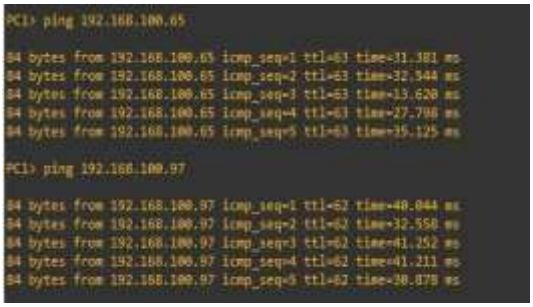


Gambar 5. Konfigurasi Ip Moodle Server

Pada Moodle Server dilakukan hal yang sama dengan konfigurasi ip yang berbeda. Pada web server yang pertama, file html bisa diedit dengan mengetikan "sudo nano /var/www/html/index.html" yang dimana disini tempat untuk mengedit segala teks maupun komponen yang ada. Untuk Moodle Server langkah pertama adalah dengan mengunggah Moodle terlebih dahulu dengan cara "wget link_moodle". Kemudian lakukan pengekstrakan Moodle kedalam file html. setelah itu buka pada web client dan akses menggunakan ip sisa atau ip eksternal. ip sisa atau eksternal disini adalah 192.168.100.15/moodle. Selanjutnya lakukan penginstalan Moodle dengan mengikuti perintah bawaan dari Moodle itu sendiri.

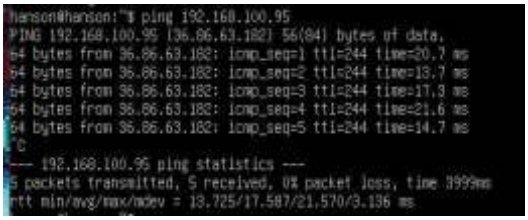
3.2 Hasil Simulasi

Setelah melakukan instalasi dan pengaturan yang tepat, hasil yang berhasil dicapai adalah sebagai berikut. Pertama, di dalam jaringan, semua perangkat yang berada di zona dalam (inside) dapat saling melakukan ping, baik ke perangkat yang berada di luar (outside) maupun ke perangkat yang berada di zona demiliterisasi (DMZ). Hal ini menunjukkan adanya konektivitas yang baik antara perangkat-perangkat di dalam jaringan, dan hasil ping dapat dilihat pada gambar 3.



Gambar 6. Hasil ping inside menuju DMZ dan outside

Kedua, pada zona demiliterisasi (DMZ), perangkat-perangkat yang berada di sana hanya dapat melakukan ping ke perangkat di luar jaringan (outside), tetapi tidak dapat melakukan ping ke perangkat yang berada di dalam (inside), seperti yang terdapat pada gambar 4.



Gambar 7. Hasil ping DMZ menuju Outside

Ketiga, di luar jaringan (outside), perangkat-perangkat yang berada di sana tidak dapat melakukan ping ke perangkat yang berada di dalam (inside). Namun, mereka masih dapat melakukan ping ke perangkat yang berada di DMZ. Hal ini mengisolasi akses dari luar ke zona dalam jaringan.

Gambar 8. Hasil Akses Website HTTPS dari Web Client

Keempat, keberhasilan dalam mengakses kedua web server akan diuji. Pertama, web pertama yang berisikan HTTPS berhasil diakses jika dari web client di ketik ip eksternalnya yaitu 192.168.100.11. Website akan muncul yang bertuliskan SDN 01 Anak Bangsa dan sudah tercangkup HTTPS.

Gambar 9. Hasil Akses Moodle dari Web Client

Terakhir, keberhasilan akses Moodle server. cara mengakses kurang lebih sama dengan cara mengakses website HTTPS yaitu dengan menggunakan ip sisa atau eksternal yang sudah dikonfigurasi. Di sini, ip sisa yang digunakan adalah 192.168.100.15/moodle. Jika di ketik, maka Moodle berhasil di akses dari web client melalui sistem jaringan yang sudah dirancang.

Secara keseluruhan, hasil instalasi dan pengaturan ini menciptakan struktur jaringan yang aman dan terkendali. Perangkat-perangkat di dalam jaringan memiliki konektivitas yang baik, sementara perangkat di DMZ memiliki akses terbatas hanya keluar jaringan. Di sisi lain, perangkat-perangkat di luar jaringan tidak dapat mengakses perangkat-perangkat di dalam.

4. Kesimpulan

Dalam artikel ini, fungsionalitas Moodle LMS digunakan untuk merancang simulasi jaringan sekolah. Ini memungkinkan siswa di database untuk mengakses materi dan memanfaatkan fungsionalitas LMS yang sudah ada. Akses juga diberikan kepada pejabat/pegawai sekolah untuk mengambil informasi dan data dari database. Staf sekolah seperti guru dan administrator juga mendapatkan manfaat dari skema ini. Database dapat diakses untuk mengumpulkan informasi penting seperti tugas siswa, jadwal kelas, dan materi siswa. Selain itu, melalui LMS, Anda dapat mengelola data siswa, mengirimkan pemberitahuan ke seluruh komunitas sekolah, dan memantau kemajuan akademik siswa. Perancangan integrasi jaringan ini menggunakan

Untuk Kesempatan yang akan datang LMS Moodle yang telah dirancang mungkin dapat diperkembangkan lagi dengan menambahkan fitur-fitur unik lainnya ataupun juga menggunakan data yang lebih lengkap agar mendapatkan hasil yang lebih detail dan efektif dalam pemakaian.

Referensi

[1] Wikipedia Contributors, “Graphical Network Simulator-3,” *Wikipedia*, Oct. 28, 2019. https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3

[2] A. A. Winarsih, "Jaringan Komputer, Pengertian, Jenis, Transmisi, dan Topologi," Media Indonesia, 18 1 2023. [Online]. Available: *HTTP*s://mediaindonesia.com/teknologi/433330/jaringan-komputerpengertian-jenis-transmisi-dan-topologi. [Accessed 1 12 2023].

[3] Binus University , "Binus University Online Learning," Binus University, 24 10 2021. [Online]. Available: *HTTP*s://onlinelearning.binus.ac.id/computer-science/post/protocol-jaringan. [Accessed 1 12 2023].

[4] Telkom University, "Apakah Yang Dimaksud Dengan NAT (*Network Address* Translator)," Telkom University, 9 7 2020. [Online]. Available: *HTTP*s://it.telkomuniversity.ac.id/apakah-yang-dimaksud-dengan-nat-*Network-Address*-translator/. [Accessed 1 12 2023].

[5] Ariffud Muhammad, "Firewall: Pengertian, Fungsi, Manfaat, Jenis, Cara Kerjanya!," Niaga Hoster, 2 10 2022. [Online]. Available: *HTTP*s://www.niagahoster.co.id/blog/firewall-adalah/. [Accessed 1 12 2023].

[6] Lintasarta Cloudeka, "Agar Tidak Keliru, Kenali 8 Perbedaan Router dan Switch Ini!," Lintasarta Cloudeka, 23 Juni 2023. [Online]. Available: *HTTP*s://www.cloudeka.id/id/berita/teknologi/perbedaan-router-dan-switch/#:~:text=Router%20bekerja%20di%20lapisan%20jaringan,menerima%20data%20di%20jaringan%20lokal. [Accessed 01 12 2023].

[7] GNS3, "Getting Started with GNS3," GNS3, 2 April 2020. [Online]. Available: *HTTP*s://docs.gns3.com/docs/. [Accessed 2 Desember 2023].

[8] fathurhoho, "VLSM atau Variable Length Subnet Mask," config.net, 19 Juli 2020. [Online]. Available: *HTTP*s://ngonfig.net/vlsm.html. [Accessed 2 Desember 2023].

[9] Binus University, "TCP/IP (Transmission Control Protocol/Internet Protocol)," Binus University, 24 September 2021. [Online]. Available: *HTTP*s://onlinelearning.binus.ac.id/computer-science/post/tcp-ip-transmission-control-protocol-internet-protocol. [Accessed 02 Desember 2023].

[10] "What is UDP?," Cloudflare, 12 Mei 2020. [Online]. Available: *HTTP*s://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/. [Accessed 2 Desember 2023].

[11] "Apa Itu Application Layer ? Apa Saja Fungsinya ?," Web Developer Indonesia, 13

Oktober 2021. [Online]. Available: *HTTP*s://webdev-id.com/berita/application-layer/. [Accessed 3 Desember 2023].

[12] Biznetgio, "Ketahui Perbedaan *HTTP* dan *HTTP*S," Biznet, 21 Maret 2021. [Online]. Available: *HTTP*s://www.biznetgio.com/news/perbedaan-*HTTP*-dan-*HTTP*s. [Accessed 3 Desember 2023].

[13] Imas Indra, "Apa Itu DNS? Pengertian, Fungsi, Cara Kerja, dan Cara Settingnya," Niagahoster, 5 September 2022. [Online]. Available: *HTTP*s://www.niagahoster.co.id/blog/apa-itu-dns/. [Accessed 4 Desember 2023].

[14] LABORATORIUM KOMPUTER FAKULTAS TEKNIK UNIVERSITAS PANCASILA, "Pengantar Subnetting," *Modul Jaringan*, vol. 15, no. Memahami Konsep Dasar Subnetting, pp. 3-5, 2019.

[15] "What Is Computing-*Network* Integration?," Huawei, 29 April 2020. [Online]. Available: *HTTP*s://info.support.huawei.com/info-finder/encyclopedia/en/Computing-*Network*+integration.html. [Accessed 3 Desember 2023].

[16] Moodle, "Moodle Documentation," Moodle, 14 September 2023. [Online]. Available: *HTTP*s://docs.moodle.org/403/en/Main_page. [Accessed 4 Desember 2023].