SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI OWNCLOUD DENGAN GNS3

[1] Sheila Tania [2] Olivia Clarabella Khotiera [3] Ferdinand [4] Paulina Agusia [5] Jonathan Setiawan
[1] [2] [3] [4] [5]Teknik Informatika Universitas Tarumanagara
Jl. Letjen S. Parman No. 1, Jakarta 11440 Indonesia
email : [1] sheila.535220028@stu.untar.ac.id, [2] olivia.535220050@stu.untar.ac.id, [3] ferdinand.535220031@stu.untar.ac.id , [4] paulina.535220048@stu.untar.ac.id, [5] jonathan.535220234@stu.untar.ac.id

ABSTRACT

Belajar dari pengalaman sebelumnya selama pandemi COVID-19, banyak perusahaan menghadapi tantangan dalam operasional mereka. Banyak karyawan yang dirumahkan, dan tenaga kerja yang tersisa beralih ke pekerjaan jarak jauh. Namun, kendala yang cukup besar muncul karena tidak semua karyawan memiliki komputer pribadi atau laptop di rumah. Menanggapi hal ini, perusahaan memberikan solusi dengan menawarkan setiap karyawan sebuah laptop yang dikeluarkan oleh perusahaan. Laptop ini dikonfigurasikan untuk hanya mengakses server yang dibuat oleh perusahaan, memastikan akses yang aman dan terkendali. Selain itu, menyadari kebutuhan akan penyimpanan data yang efisien, perusahaan menerapkan sistem cloud sendiri. Sistem cloud ini berfungsi sebagai solusi penyimpanan terpusat yang dapat diakses oleh perusahaan dan karyawannya. Jadi, kami menggunakan GNS3 untuk membuat server dan dengan menggunakan VPN untuk karyawan yang bekerja dari rumah.

Dalam hal ini, OwnCloud berhasil diakses dari dalam dan luar. Di mana PC1 dan Ubuntu Desktop dapat mengakses OwnCloud dengan menggunakan IP server yang sudah diatur.

Key words
GNS3, OwnCloud, Server, Subnetting, VPN

1. Pendahuluan

Melihat dari adanya pandemi *COVID-19* yang lalu, timbul banyak kendala, diantaranya adalah para karyawan yang pada mulanya dapat bekerja di kantor, kini tidak dapat melaksanakan pekerjaan di kantor lagi, dikarenakan dampak dari pandemi *COVID-19* yang mengharuskan mereka untuk bekerja dari rumah [1]. Untuk menjalankan tugas harian, diperlukan penggunaan komputer atau laptop. Namun, permasalahan muncul karena tidak semua karyawan pada sebuah perusahaan memiliki perangkat untuk melakukan pekerjaan mereka. Situasi ini menjadi inspirasi dalam pembuatan penelitian ini agar para karyawan dapat menjalankan tugas mereka dari rumah. Oleh karena itu dengan adanya penelitian ini kami ingin agar perusahaan memberikan fasilitas berupa satu laptop kepada setiap karyawan. Dengan adanya fasilitas laptop ini membuat sebuah pertimbangan agar karyawan tidak menyalahgunakan perangkat yang telah difasilitasi oleh perusahaan, perusahaan dapat menciptakan sebuah server yang hanya dapat diakses oleh perusahaan dan perangkat yang diberikan kepada karyawan。

Selain itu, untuk mempertimbangkan penyimpanan data dengan jumlah yang lumayan besar, pihak Perusahaan juga ingin menggunakan sebuah perangkat lunak yang bisa menyimpan data tersebut. Oleh karena itu, penelitian ini memilih untuk menggunakan OwnCloud sebagai perangkat lunak yang dapat mempermudah pihak Perusahaan untuk melakukan akses dan menyimpan data pada OwnCloud.

Dengan menggunakan OwnCloud ini hanya bisa diakses oleh orang yang telah terdaftar di dalam server. OwnCloud ini sangat efisien dalam penggunaannya, ketika memiliki banyak pekerjaan, para pengguna tidak perlu lagi mengandalkan flashdisk [2]. Cukup dengan adanya penggunaan OwnCloud, pengguna dapat menyimpan dan membagikan data di mana saja dan kapan saja.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Jaringan komputer merupakan infrastruktur yang memfasilitasi pertukaran data antar perangkat melalui konektivitas, sementara keamanan jaringan menjadi salah satu aspek krusial dalam menjaga integritas dan kerahasiaan informasi [3].

Pada penelitian simulasi jaringan menggunakan *OwnCloud* ini dibutuhkannya subnetting pada lapisan jaringan yang memungkinkan pengelompokan *alamat Internet Protocol (IP)* untuk efisiensi dan keamanan yang lebih baik [4]. *Network Address Translation (NAT)* berfungsi sebagai perantara antara jaringan internet internal dan external, meningkatkan keamanan dengan menyamarkan alamat *IP internal* [5]. *Virtual Private Network (VPN)* memastikan amannya komunikasi melalui jaringan publik, menyematkan lapisan keamanan tambahan [6]. *Firewall*, yang dapat berupa perangkat keras atau perangkat lunak, mengatur lalu lintas jaringan dengan menerapkan aturan keamanan, menjadi sebuah benteng pertahanan terdepan dalam melindungi jaringan dari serangan dan ancaman yang mungkin muncul.

Pada penelitian ini pembuatan server jaringannya berisikan bagian outside yang berada pada bagian luar *Cisco ASAv*, pada bagian outside ini berfungsi untuk

digunakan oleh para karyawan yang melakukan *Work From Home (WFH)* dikarenakan secara *security level* yang digunakan hanya 0. Sehingga untuk melakukan akses ke dalam bagian inside diperlukannya *VPN*. *VPN* ini berfungsi sebagai cara yang aman untuk mengakses *local area network* pada jangkauan tertentu karena karyawan yang *WFH* berada di luar akses kantor. Kemudian ada juga bagian *inside* yang berada didalam jalur *Cisco ASAv*, bagian *inside* ini merupakan kebalikkan dari bagian *outside* di mana bagian *outside* ini diibaratkan sebagai para karyawan yang melakukan pekerjaan di kantor sehingga pada *security level* yang digunakan lebih besar di mana hal ini berfungsi untuk menjaga keamanan integritas dokumen – dokumen yang penting.

Cisco Asav memiliki fungsi sebagai melindungi jaringan agar hanya dapat diakses oleh pemilik perangkat dari perusahaan serta orang yang diberikan akses mengaksesnya supaya tidak terjadinya ancaman dan serangan yang berpotensi untuk merusak data serta sumber data yang ada didalamnya [7]. Oleh karena itu, posisi *Cisco Asav* ini terletak pada bagian tengah jalur *inside* dengan jalur *outside*.

Kemudian pada bagian bawah pada layout jaringan terdapat bagian yang disebut sebagai *Demilitarized Zone (DMZ)*, di mana pada *DMZ* ini digunakan sebagai perantara antara internet internal dan eksternal sehingga pihak perusahaan tidak perlu takut akan serangan dari luar dikarenakan pada bagian internet tidak langsung terhubung secara langsung [8]. Pada penelitian ini digunakan *Ubuntu Desktop* sebagai *browser* untuk mengakses *OwnCloud* nya di karena *OwnCloud* ini diunduh di dalam *Ubuntu Desktop* itu sendiri. *OwnCloud* ini memiliki kesamaan dengan *GoogleDrive*, di mana kedua layanan ini berfungsi sebagai tempat untuk menyimpan data serta mengaksesnya.

Dengan *OwnCloud* ini, karyawan dari perusahaan dapat melakukan unggah dokumen dan pihak perusahaan juga dapat mengakses layanan tersebut.

2.2 Aplikasi Terdistribusi

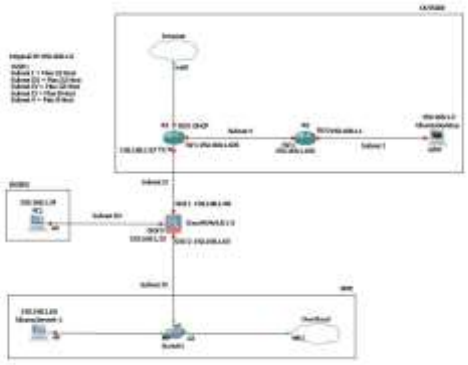
OwnCloud merupakan salah satu perangkat *client-server* yang berfungsi untuk mengunggah dan mengakses dokumen didalamnya dengan menggunakan *server* yang telah dibuat [9].

OwnCloud merupakan salah satu *software open source* yang bersifat terbuka karena secara penginstalan dan pengoperasiannya dilakuakan secara gratis dan dapat digunakan dengan *server* tertentu. Tujuan digunakan OwnCloud pada penelitian ini untuk mempermudah karyawan serta pihak perusahaan mengakses dan mengupload dokumen [10].

3. Hasil Percobaan

3.1 Instalasi dan Pengaturan

Pada penelitian ini menggunakan aplikasi *GNS3*, *GNS3* ini berfungsi sebagai tempat untuk melakukan simulasi jaringan yang telah dibuat.



Gambar 1. Layout Pada GNS3

Langkah-langkah melakukan *setting* :

1. Membuat *layout* jaringan.
   Pada tahap ini merupakan tahap yang akan menentukan bagaimana nantinya *system* jaringannya akan bekerja. Pada *layout* jaringan yang tertera pada gambar 1. terdapat 1 *Ubuntu Desktop* sebagai perangkat diluar kantor, 1 buah *Cisco ASAv* yang berfungsi sebagai *Firewall*, 2 *router* dan 1 *switch* yang berfungsi sebagai penghubung antar jaringan, serta *NAT* yang berfungsi sebagai sarana internet.
2. Melakukan *Subnetting*
   Pada tahap s*ubnetting* dilakukan penggunaan metode *VLSM* di mana pada metode ini menetapkan berapa jumlah maksimal *host* yang akan dipakai oleh masing-masing *subnet*. untuk melakukan *subnetting, IP original* yang digunakan adalah 192.168.1.0/24. Pada penelitian ini membutuhkan 5 *subnet*. Pada *subnet* I,III,IV dengan maksimal 32 *host*, sedangkan *subnet* II, dan V dengan maksimal 8 *host*.

Berikut adalah hasil dari masing - masing subnet yang telah dilakukan alokasi *IP Address* :

Tabel 1. Alokasi IP Pada R1

Interface	IP Address	Subnet Mask
F0/0	DHCP	-
F0/1	192.168.1.105	(29) 255.255.255.248
F1/0	192.168.1.97	(29) 255.255.255.248

Tabel 2. Alokasi *IP Address* Pada R2

Interface	IP Address	Subnet Mask
F0/0	192.168.1.1	(27) 255.255.255.224
F0/1	192.168.1.106	(29) 255.255.255.248

Tabel 3. Alokasi *IP Address* Pada *CiscoASAv*

Interface	IP Address	Subnet Mask	Security Level
Gi0/0	192.168.1.33	(27) 255.255.255.224	Inside 100
Gi0/1	192.168.1.98	(29) 255.255.255.248	Outside 0
Gi0/2	192.168.1.65	(27) 255.255.255.224	DMZ 50

Tabel 4. Alokasi *IP Address* Pada PC1

Interface	IP Address	Subnet Mask	Default Gateway
ETH0	192.168.1.34	(27) 255.255.255.224	192.168. 1.33

Tabel 5. Alokasi *IP Address* Pada *Ubuntu Server*

Interface	IP Address	Subnet Mask	Default Gateway
ETH0	192.168.1.66	(27) 255.255.255.224	192.168. 1.65

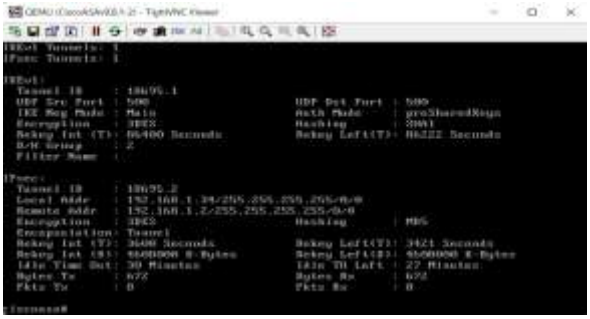
Tabel 6. Alokasi *IP Address* Pada *Ubuntu Dekstop*

Interface	IP Address	Subnet Mask	Default Gateway
ETH0	192.168.1.2	(27) 255.255.255.224	192.168. 1.1

3.2 Hasil Simulasi

Pada penelitian ini dilangsungkannya uji test *Pack Internet or Inter-Network Grapher (PING)* di mana *PING* ini merupakan perangkat lunak administrasi jaringan komputer yang digunakan untuk menguji keterjangkauan suatu *host* pada jaringan *IP* dan untuk mengukur pengaruh waktu sebagai parameter dari kualiatas pelayanan [5]. Uji *PING* ini dilakukan dalam pengujian ini untuk melihat apakah pada bagian *outside* (*Ubuntu Desktop*) tersambung dengan jalur *inside* (*PC1*). Untuk itu, berikut adalah beberapa gambar yang menunjukkan uji *PING* antara *outside* ke *inside*, *inside* ke *outside*, tampilan akses masuk kedalam *OwnCloud*, *inside* ke *OwnCloud*, tampilan awal pada *OwnCloud* serta penggunaan *VPN* yang telah disetting pada *R2* dan *Cisco ASAv* :

Pada tahap pertama, berisikan hasil dari *setting VPN* pada *Cisco Asav* yang dapat dilihat pada Gambar 2. Untuk melihat apakah *VPN* nya sudah berjalan dapat dilakukan pengecekkan dengan melakukan *command show-vpn sessiondb detail l2l filter ip address 192.168.1.106*. Jika dilihat pada *layout* jaringan pada penelitian ini, *IP* 192.168.1.106 berada pada R2 yang berarti terdapat *VPN* yang di *setting* juga pada jalur R2.

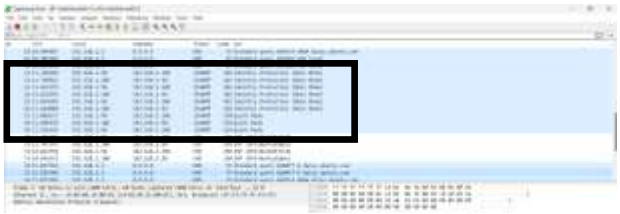


Gambar 2. *VPN* Pada *Cisco Asav*

Pada tahap selanjutnya, pada penelitian ini dilakukannya pengecekkan *VPN* pada R2 untuk memastikan apakan *VPN* nya sudah terpasang dengan baik. Terlihat pada Gambar 3 di mana *VPN* yang berada di R2 sudah di *setting*.

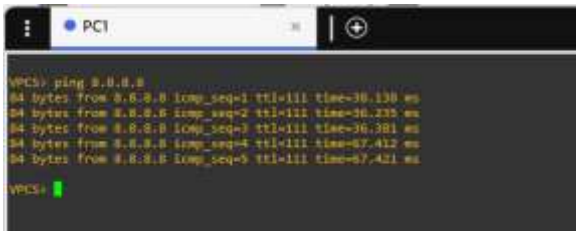
Gambar 3. *VPN* Pada R2

Seperti yang ditunjukkan pada Gamabr 4, pada tahap ini berisikan hasil dari *WireShark*. Pengecekkan ini dilakukan dengan melakukan *PING* dari *PC1* ke *IP* 192.168.1.106 untuk melihat apakah sudah terdapat *VPN* yang menyala.



Gambar 4. Hasil *WireShark* Pada Pengecekan *VPN*

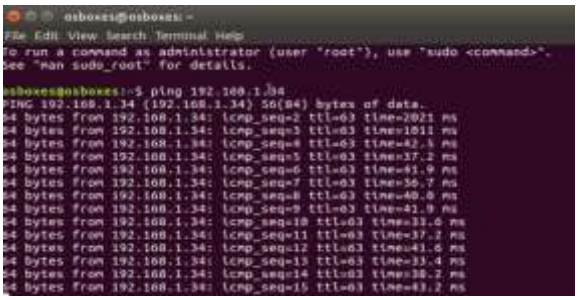
Pada tahap ini dilakukannya uji test *PING* dari *PC1* ke *google domain*. Di mana pada Gambar 5 terlihat bahwa *PC1* berhasil melakukan *PING* ke dalam *Google Domain*. Hal ini menyatakan bahwa dapat melakukan akses kedalam *OwnCloud*.



Gambar 5. Hasil *PING* PC1 ke 8.8.8.8

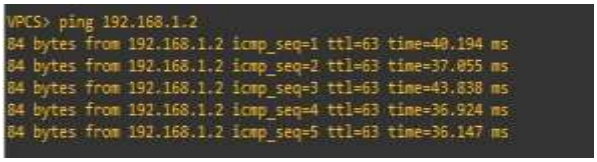
Pada tahap selanjutnya, dapat dilihat pada Gambar 6 di mana *Ubuntu Desktop* yang berada dibagian *outside layout* jaringan dapat mengakses ke bagian *inside* pada

layout jaringan. Hal ini memungkinkan bahwa perangkat yang berada di bagian *outside* sudah bisa melakukan akses ke dalam *OwnCloud*.



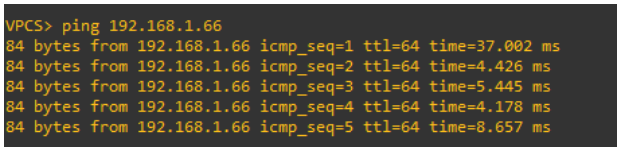
Gambar 6. Hasil Ping Dari Outside to Inside.

Pada tahap selanjutnya, dapat dilihat pada Gambar 7 di mana dilakukan simulasi *PING* dari *PC1* ke *Ubuntu Desktop*. Hal ini memperjelas bahwa bagian *inside* dengan *outside* sudah terhubung dengan baik.



Gambar 7. Hasil Ping Dari Inside to Outside

Seperti yang ditunjukkan pada Gambar 8, pada tahap ini dilakukannya juga uji coba *PING* dari perangkat *PC1* ke dalam *OwnCloud*. Pada *PC1* dapat melakukan akses ke dalam *OwnCloud* pada 192.168.1.66



Gambar 8. Hasil Ping PC1 ke OwnCloud

Pada tahap selanjutnya, dilakukan uji akses dari bagian *outside* jaringan menuju *server OwnCloud*. Pada Gambar 9 dapat terlihat bahwa *Ubuntu Desktop* yang berada pada bagian *outside* sudah dapat melakukan akses ke dalam *OwnCloud* dengan 192.168.1.99.

Gambar 9. Bagian Outside melakukan Akses ke OwnCloud

Setelah berhasil melakukan akses kedalam *OwnCloud*, pengguna juga dapat *login* kedalam *OwnCloud* dan sudah dapat melakukan pemasukkan dokumen dan menyimpan dokumen pada *OwnCloud*.

Gambar 10. Akses kedalam OwnCloud

4. Kesimpulan

Berdasarkan hasil simulasi yang telah dilakukan, implementasi jaringan simulasi untuk sistem terdistribusi *OwnCloud* menggunakan aplikasi *GNS3* telah berhasil dengan baik. Integrasi antara bagian *inside* dan *outside* terhubung dengan lancar, terbukti melalui uji coba *PING* dan akses ke berbagai alamat *IP* yang berhasil tanpa kendala. Keamanan jaringan juga terbukti efektif melalui uji coba *VPN* yang menunjukkan hasil positif. Untuk pengembangan lebih lanjut, fokus pada optimalisasi kinerja jaringan dan perluasan fungsionalitas sangat dianjurkan. Evaluasi performa jaringan, termasuk penyesuaian *bandwidth* dan konfigurasi perangkat, serta penambahan fitur keamanan seperti *firewall* atau *IDS*, dapat meningkatkan efisiensi dan keamanan sistem. Selain itu, penerapan mekanisme pemulihan data yang efektif juga perlu diperhatikan untuk memastikan keberlanjutan operasional dalam situasi darurat.

REFERENSI

[1] A. V. B. G. Mery Sulianty H. Sitanggang, "Pengaruh Pandemi Covid-19 Terhadap Kinerja Karyawan Pada PT Superintending Company Of Indonesia (Persero) Medan," *Jurnal Ekonomi Bisnis dan Teknologi*, no. 2, p. 28, 2022.

[2] S. D. S. A. I. F. S. Edy Rakhmat, "PEMANFAATAN APLIKASI OWNCLOUD PADA SISTEM KEAMANA CLOUD COMPUTING," *Jurnal Sistem Informasi dan Informatika (SIMIKA)*, no. 4, p. 149, 2021.

[3] kominfo, "Keamanan Jaringan Internet dan Firewall," *Keamanan Jaringan Internet dan Firewall*, p. 1, 29 Juni 2017.

[4] A. K. Wardana, "Simulasi Subnetting IPv4 dengan Packet Tracer," *SEMINAR NASIONAL Dinamika Informatika*, p. 55, 2020.

[5] E. S. d. G. K. Ilmalik Muhammad Alviendra, "Pengembangan danPenerapan Sistem Virtual

Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi," *Pengembangan danPenerapan Sistem Virtual Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi*, vol. II, no. Institut Teknologi Sepuluh Nopember (ITS), pp. A15-A19, 2022.

[6] R. Subekti, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI SECURITY SELAMA WORK FROM HOME," *JURNAL NASIONAL INFORMATIKA*, no. 1, p. 57, 2020.

[7] D. Ananta Kwarta Durianto, "Konfigurasi Cicso ASA Firewall," *Konfigurasi Cicso ASA Firewall*, vol. I, no. Universitas Negeri Semarang, p. 298, 2021.

[8] Rizki Tujuhbelas Kelola, "MENGENAL DMZ (DEMILITARISASI ZONE): FUNGSI DAN MANFAATNYA DALAM KEAMANAN JARINGAN," *MENGENAL DMZ (DEMILITARISASI ZONE): FUNGSI DAN MANFAATNYA DALAM KEAMANAN JARINGAN*, p. 1, Kamis Juni 2023.

[9] D. I. R. W. S. M. Ainun Isnainudin, "Implementasi Cloud Computing Menggunakan OwnCloud Dengan Memanfaatkan Redundant Array of Independent Disk 1 Sebagai Media Penyimpanan," *Implementasi Cloud Computing Menggunakan OwnCloud Dengan Memanfaatkan Redundant Array of Independent Disk 1 Sebagai Media Penyimpanan*, vol. II, no. Universitas Kristen Satya Wacana, p. 1, 2019.

[10] H. N. P. A. H. Michael Adi, "Aplikasi Private Cloud Storage untuk Menyimpan Data Operasional Program Studi Teknik Informatika dan Sistem Informasi Bisnis Menggunakan Open Source," *Aplikasi Private Cloud Storage untuk Menyimpan Data Operasional Program Studi Teknik Informatika dan Sistem Informasi Bisnis Menggunakan Open Source*, vol. II, no. Universitas Kristen Petra Surabaya, p. 2, 2017.