SIMULASI JARINGAN UNTUK SISTEM TERDISTRIBUSI SOHO DENGAN GNS3

Shinzi[1)] Felix Ferdinand[2)] Gabriel Nathanael Irawan[3)]
Jonathan Kennedy[4)] Javier Gustvin[5)]

[1,2,3,4,5)] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara,
Jln. Letjen S. Parman No. 1, Jakarta, 11440, Indonesia
email : [1)]shinzi.535220118@stu.untar.ac.id, [2)]felix.535220161@stu.untar.ac.id,
[3)]gabriel.535220142@stu.untar.ac.id, [4)]jonathan.535220127@stu.untar.ac.id, [5)]javier.535220140@stu.untar.ac.id

ABSTRACT

Penelitian ini membahas mengenai implementasi sistem jaringan terdistribusi dengan layanan cloud, khususnya Software as a Service (SaaS) pada kerangka Small Office Home Office (SOHO) melalui simulasi GNS3. Topologi yang dibangun melibatkan Virtual Machine (VM), router, firewall, dan web server, dengan pembagian area dalam, DMZ, dan luar. Konfigurasi meliputi pengaturan IP, tabel perutean, Network Address Translation (NAT), dan Access Control List (ACL). Desain ini juga melibatkan VPN situs-ke-situs antara router dan Cisco Adaptive Security Appliance (ASAv). Web server diamankan dengan HTTPS, dan juga pengaturan VPN yang melibatkan ISAKMP, IPSec, dan peta kripto. Selain itu, penelitian ini juga mencakup transfer file menggunakan ownCloud, sebuah layanan cloud untuk manajemen file dengan sinkronisasi data antara perangkat yang terhubung.

Hasil penelitian menunjukkan komunikasi yang baik antara klien web dan server dengan tetap menjaga keamanan melalui langkah-langkah yang diterapkan. Penelitian ini memberikan wawasan yang berharga tentang penerapan sistem jaringan terdistribusi, layanan cloud, dan transfer file menggunakan ownCloud dalam desain SOHO, yang berkontribusi dalam pemahaman mengenai teknologi-teknologi tersebut dalam skenario praktis.

Key words

Jaringan, ownCloud, SOHO, GNS3, SaaS

1. Pendahuluan

Pada era digital ini, teknologi informasi mempunyai peran yang sangat penting dalam mendukung operasional suatu bisnis. Perkembangan dalam teknologi jaringan dan layanan cloud telah membawa perubahan yang sangat signifikan dalam memberikan peningkatan dalam aspek efisiensi dan adaptabilitas bisnis [1]. Salah satu kasus contoh penerapan yang sering dilakukan adalah penerapan sistem jaringan terdistribusi pada desain *Small Office Home Office* (SOHO) bagi perusahaan skala kecil dan menengah [2]. Oleh karena itu, dalam usaha untuk melihat lebih dalam mengenai potensi serta cara kerja jaringan terdistribusi dan teknologi cloud, khususnya dalam implementasi *Software as a Service* (SaaS), maka dilakukan simulasi jaringan terdistribusi untuk SOHO dengan layanan cloud, *ownCloud* pada media GNS3.

Desain jaringan simulasi ini terbentuk berdasarkan pemahaman atas kebutuhan infrastruktur teknologi informasi pada desain SOHO. Pembuatan model ini memiliki tujuan dalam memudahkan akses data dari satu perangkat ke perangkat lainnya baik dari bagian internal jaringan, maupun akses dari luar jaringan walaupun memiliki keterbatasan akses. Simulasi jaringan ini diharapkan memberikan kontribusi dalam bentuk pengetahuan dalam penerapan jaringan sistem terdistribusi, beserta dengan layanan cloud pada desain SOHO.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Jaringan komputer merupakan sistem dimana komputer bisa dapat saling berkomunikasi atau berhubungan dengan komputer lain dikarenakan terintegrasi oleh suatu media transmisi [3]. Jaringan komputer memiliki banyak jenis, tetapi pada simulasi ini hanya akan berfokus pada aspek – aspek tertentu berupa Subnetting, NAT, Transport Protocol dengan TCP, Application Service berupa DNS dan HTTPS, VPN, dan Firewall. Melalui penerapan konsep – konsep tersebut, jaringan komputer dirancang dan diatur untuk memberikan keamanan, kinerja optimal dan layanan aplikasi yang sesuai dengan keperluan.

Subnetting merupakan teknik dalam jaringan komputer yang memungkinan pembagian alamat *Internet Protocol* (IP) ke dalam beberapa jaringan yang lebih kecil untuk setiap perangkat [3]. Subnetting pada simulasi ini dilakukan dengan metode *Variable Length Subnet Mask* (VLSM), VLSM digunakan untuk menentukan penggunaan alamat IP yang efisien dengan cara menghitung seberapa banyak kebutuhan pengguna suatu jaringan dan membagi alamat IP sesuai dengan kebutuhan tersebut [4].

Network Address Translation (NAT) memiliki tujuan untuk mengkonservasi alamat IP Publik. Setiap komputer memiliki alamat IP unik, jika semua komputer mempunyai IP Publik masing-masing maka akan menghambat kecepatan internet, sehingga ketika perangkat ingin mengakses internet, maka alamat IP internal akan diterjemahkan oleh NAT menjadi alamat IP publik yang dapat digunakan bersama. NAT dapat berada diantara router ataupun firewall dengan jaringan lokal dan internet [3].

Transport Protokol mengatasi pemeriksaan kesalahan, pengurutan, dan pengendalian aliran [3]. Pada simulasi ini protokol yang diterapkan adalah *Transmission Control Protocol* (TCP), yang dapat mengirim data dari sumber ke tujuan akhir dari *internetwork*, *internetwork* artinya gabungan berbagai jaringan komputer yang saling terhubung menggunakan satu atau lebih perangkat jaringan, dalam hal ini TCP beradaptasi secara cepat terhadap berbagai macam kegagalan yang dapat terjadi pada *internetwork* [3].

Application Layer bertanggung jawab untuk menyediakan layanan jaringan berupa pertukaran informasi antara aplikasi dengan aplikasi lainnya dan memberikan protokol dengan tujuan memberikan interface antara aplikasi saat pertukaran informasi berlangsung [5]. Protokol yang diterapkan pada simulasi ini berupa :

1. DNS singkatan dari “Domain Name System” merupakan cara praktis untuk merujuk pada halaman web dan sumber daya lainnya tanpa harus mengingat alamat IP komputer tempat mereka disimpan. Dengan menggunakan DNS, pengguna dapat dengan mudah mengakses halaman web dan sumber daya lainnya tanpa harus menyimpan alamat IP yang sulit diingat [3].
2. HTTP singkatan dari *“HyperText Transfer Protocol”* merupakan protokol lapisan aplikasi karena berjalan diatas TCP [3]. HTTP menjadi protokol transportasi yang memfasilitasi berbagai proses komunikasi melintasi batas jaringan yang berbeda. HTTP juga biasanya digunakan oleh pemutar media untuk mengambil informasi dari server dan adapun *HyperText Transfer Protocol Secure* (HTTPS) yang memiliki fungsi yang sama seperti HTTP tetapi memiliki keamanan yang lebih baik dikarenakan melakukan enkripsi pada data [3].

VPN (Virtual Private Network) berfungsi untuk membangun sirkuit dan memori virtual dalam bentuk jaringan publik tetapi tetap memiliki fitur jaringan pribadi dan digunakan sebagai terowongan jaringan yang dilalui untuk setiap perangkat yang masuk pada network yang sama [3].

Firewall berperan seperti antivirus yang memeriksa semua paket yang masuk atau keluar, jika paket tidak memenuhi kondisi ingin melalui firewall maka akan ditolak dan jika paket memenuhi kondisi maka akan melewati firewall dengan normal [3].

2.2 Aplikasi Terdistribusi

Aplikasi terdistribusi yang digunakan pada simulasi ini adalah Website HTTPS dan website-based cloud SaaS, ownCloud. Website HTTPS di *hosting* dari Ubuntu Server 22.04.3 (live server) dengan layanan webserver Apache, Website cloud server ownCloud di *hosting* di Ubuntu Server 22.04.3 juga dengan layanan Apache. Website HTTPS berisikan tampilan home dan about us, sedangkan ownCloud digunakan untuk cloud storage lokal.

Gambar 1. Login Page ownCloud

ownCloud merupakan layanan cloud untuk melakukan manajemen file. Layanan yang diberikan ownCloud adalah berupa penyebaran akses dan sinkronisasi data antar perangkat terhubung [6].

3. Hasil Percobaan

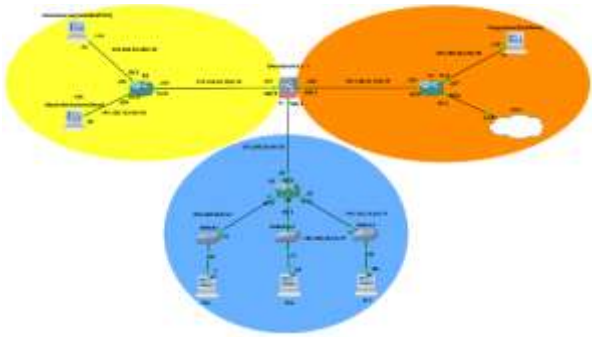
3.1 Instalasi dan Pengaturan

Program yang digunakan pada simulasi ini adalah VirtualBox untuk Virtual Machine (VM), GNS3, GNS3 VM, Ubuntu Server (website HTTPS), Ubuntu Server (website cloud ownCloud), Puppy Linux, *appliance* router Cisco dan *appliance* firewall Cisco ASAv. Pengaturan pada GNS3 seperti, instal GNS3 VM, menambahkan VM ke GNS3, dan memasang ip address pada VPC mengikuti dokumentasi dari GNS3 [7]. Ubuntu Server untuk website HTTPS dan Ubuntu Server untuk website cloud ownCloud akan digunakan sebagai webserver. Aplikasi webserver yang digunakan adalah Apache. Metode subnetting network address yang digunakan adalah *Variable Length Subnet Mask* (VLSM). Network address 192.168.10.0/24 dialokasikan menjadi 9 subnet address.

Gambar 2. Pengaturan preferences di GNS3

Sebelum mendesain topologi jaringan di GNS3, GNS3 VM perlu diinstal pada VirtualBox dan konfigurasi dilakukan di GNS3. Pengaturan GNS3 VM dapat dilakukan di preferences dan pada kategori "GNS3 VM". Setelah penginstalan dan pengaturan GNS3 VM berhasil, VM lainnya diinstal juga di VirtualBox dan GNS3 pada kategori "VirtualBox VMs". Pengaturan network adapter pada semua VM diatur menjadi "not attached". Hal ini bertujuan agar VM dapat disambungkan dengan router atau aplikasi jaringan virtual lainnya dalam GNS3. Aplikasi webserver Apache diinstal pada Ubuntu Server untuk website HTTPS dan Ubuntu Server untuk website cloud ownCloud.

Cloud server ownCloud diinstal pada Ubuntu Server yang digunakan untuk ownCloud. Cara instal ownCloud pada Ubuntu Server mengikuti dokumentasi dari ownCloud [8]. *Appliance* router Cisco dan *appliance* firewall Cisco ASAv masing-masing diinstal pada GNS3 dengan kategori IOS Router dan Qemu VM.



Gambar 3. Topologi Jaringan

Pada gambar 3, area yang berwarna jingga menunjukkan area outside yang dimulai dari interface Gi0/2 pada Cisco ASAv, area berwarna kuning menunjukkan area DMZ, dan area berwarna biru menunjukkan area inside. Dalam pembuatan topologi jaringan ini, terdapat beberapa langkah yang harus diikuti. Tahap pertama adalah mengatur ip address, gateway, dan DNS pada ketiga VPCS sesuai Gambar 3.

Tabel 1. Routing Tabel R2 (Router Area Inside)

Network Address	Gateway	Interface R2
192.168.10.0/27	Connected	f0/0
192.168.10.32/27	Connected	f0/1
192.168.10.64/27	Connected	f1/0
192.168.10.96/30	Connected	f2/0
192.168.10.100/30	192.168.10.97	f2/0
192.168.10.104/30	192.168.10.97	f2/0
192.168.10.108/30	192.168.10.97	f2/0
192.168.10.128/29	192.168.10.97	f2/0
192.168.10.136/30	192.168.10.97	f2/0
0.0.0.0 0.0.0.0	192.168.10.97	f2/0

Tabel 2. Routing Tabel R1 (Router Area DMZ)

Network Address	Gateway	Interface R1
192.168.10.100/30	Connected	f0/0
192.168.10.104/30	Connected	f0/1
192.168.10.108/30	Connected	f1/0
192.168.10.0/27	192.168.10.101	f1/0
192.168.10.32/27	192.168.10.101	f1/0
192.168.10.64/27	192.168.10.101	f1/0
192.168.10.96/30	192.168.10.101	f1/0
192.168.10.128/29	192.168.10.101	f1/0
192.168.10.136/30	192.168.10.101	f1/0
0.0.0.0 0.0.0.0	192.168.10.101	f1/0

Tabel 3. Routing Tabel R3 (Router Area Outside)

Network Address	Gateway	Interface R1
192.168.10.128/29	Connected	f0/0
192.168.10.136/30	Connected	f1/0
DHCP	Connected	f0/1
192.168.10.0/27	192.168.10.130	f0/0
192.168.10.32/27	192.168.10.130	f0/0
192.168.10.64/27	192.168.10.130	f0/0
192.168.10.96/30	192.168.10.130	f0/0
192.168.10.100/30	192.168.10.130	f0/0
192.168.10.104/30	192.168.10.130	f0/0
192.168.10.108/30	192.168.10.130	f0/0

Gambar 4. Access-list (ACL) untuk PAT pada Router 3

Pada tahap selanjutnya perlu mengatur ip address dan DNS pada router 1, router 2, router 3 (DHCP untuk interface f0/1 menuju ke internet), pengaturan default routing ke internet, dan static routing ke semua subnet sesuai dengan tabel 1, tabel 2, dan tabel 3. Untuk router 3, dibuatkan access-list *permit* untuk semua subnet (kecuali subnet DHCP pada router 3). Seperti pada gambar 4, access-list yang dibuat akan digunakan untuk PAT (NAT overload) pada interface f0/1 sebagai NAT outside. NAT inside berada pada interface f0/0 dan f1/0 [9], [10].

Gambar 5. *Object Network* subnet DMZ dan inside pada Cisco ASAv

Langkah berikutnya adalah mengatur ip address pada setiap VM (Ubuntu Server HTTPS, Ubuntu Server ownCloud, dan Puppy Linux). Pengaturan ip address juga dilakukan pada Cisco ASAv dengan interface area outside, DMZ, dan inside. Pengaturan pada Cisco ASAv dilakukan default routing ke internet dan static routing untuk subnet pada setiap area (kecuali subnet DHCP pada

router 3). Selanjutnya adalah membuat *object network* pada subnet DMZ dan inside. *Object network* (ditunjukkan pada gambar 5) yang telah dibuat akan digunakan untuk NAT overload. NAT overload tersebut diatur dari DMZ ke outside dan inside ke outside. Langkah terakhir adalah membuat NAT dan ACL untuk outside agar webclient dapat mengakses website dan ownCloud yang berada di DMZ [11].

Gambar 6. *Object Network* WWW, NAT, dan ACL pada Cisco ASAv

Pembuatan ACL untuk akses outside ke DMZ dilakukan dengan membuat *object network* terlebih dahulu. Ada 4 *object network* yang dibuat, yaitu ip-asal, ip-tujuan, WWW-EXT2, dan WWW-INT2. WWW-EXT2 dan ip-asal adalah ip address dari subnet yang tidak dipakai berada di interface Gi0/2 Cisco ASAv, sedangkan WWW-INT2 adalah ip address dari ownCloud lalu, ip-tujuan adalah ip address dari webserver. Setelah pembuatan *object network* ini, dibuatkan juga NAT dari DMZ ke outside. Pengaturan terakhir dari konfigurasi ini adalah mengatur ACL yang hanya *permit* protokol TCP dengan sumber *any* dan tujuan *object network* ip-tujuan dan WWW-INT2 (sesuai dengan gambar 6). ACL tersebut kemudian diterapkan pada interface Gi0/2 Cisco ASAv dengan *input traffic* [12].

Puppy Linux atau webclient sekarang dapat mengakses webserver dan ownCloud. Namun untuk membuat webserver menjadi HTTPS terdapat langkah tambahan yang harus dilakukan. Tahapan pertama adalah menginstal OpenSSL, lalu membuat key dan sertifikat untuk website digunakan. Setelah itu, terdapat field untuk pengisian data. Langkah berikutnya adalah menduplikasi konfigurasi default SSL, lalu mengganti ServerAdmin, SSLCertificateFile dan SSLCertificateKeyFile sesuai dengan yang sudah dibuat sebelumnya. Tahap terakhir adalah membuka browser dan memasukan alamat ip webserver dengan HTTPS.

Gambar 7. Konfigurasi *Crypto map* router 3

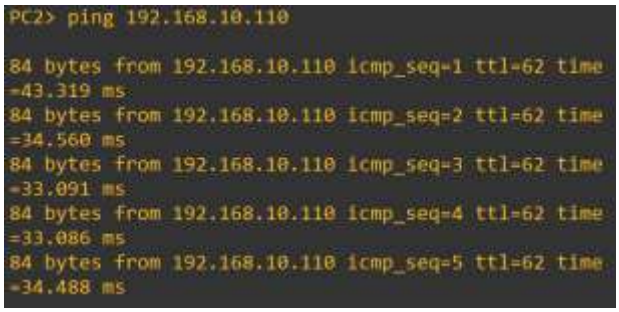
Penambahan *site-to-site* VPN pada topologi jaringan ini dibuat di router 3 dan Cisco ASAv. Pada pengaturan router 3, fase 1 IKEv1 dilakukan untuk menentukan enkripsi, otentikasi, group, *lifetime*, *hash*, dan *pre-shared key*. Pada fase 2 IKEv1 dilakukan pembuatan *transform set*, ACL *extended* untuk permit subnet *local* (subnet pada interface f1/0 router 3) dan subnet *remote* (semua subnet DMZ dan inside). Pengaturan ACL ini bertujuan agar *traffic* subnet *remote* dienkripsi setelah melewati *tunnel* VPN. Selanjutnya, membuat *crypto map* untuk menentukan *peer* (interface Gi0/2 Cisco ASAv), *match address* (ACL *extended*), dan *transform set*. *Crypto map* (sesuai dengan gambar 7) tersebut diterapkan pada interface f0/0 router 3 [13].

Gambar 8. Konfigurasi VPN pada Cisco ASAv

Penambahan *site-to-site* VPN harus dilakukan juga pada Cisco ASAv (*peer* router 3). Pengaturan hampir sama dengan router 3. Cisco ASAv harus membuat *tunnel-group* dengan interface ip router 3 dan memberi tipe *ipsec-l2l*. *tunnel-group* tersebut juga diberikan *pre-shared key* yang sama dengan router 3. ACL yang dibuat pada Cisco ASAv menggunakan *object group*. *Object group* ini terdiri dari *local-network* dan *remote*. Kedua *object group* tersebut berisikan subnet address dari inside, DMZ, dan outside (tidak termasuk subnet DHCP). Subnet *local-network* berasal dari subnet yang ada di DMZ dan inside, sedangkan subnet *remote-network* hanya tersimpan subnet interface f1/0 router 3. *Object group* tersebut kemudian diatur dalam ACL *extended*. Setelah pembuatan ACL selesai, *crypto map* diatur dengan *peer* interface f0/0 router 3, *match address* dengan ACL, dan *transform set*. *Crypto map* (ditunjukkan pada gambar 8) yang sudah selesai dibuat diterapkan di interface outside Cisco ASAv. Karena pada Cisco ASAv diatur dengan NAT overload, maka Cisco ASAv diatur agar *traffic* DMZ dan inside ke outside diberikan pengecualian. Secara *default*, ACL di Cisco ASAv dibebaskan untuk *traffic* VPN. Pengaturan tersebut harus dimatikan agar *traffic* dari outside tidak masuk ke inside [13], [14].

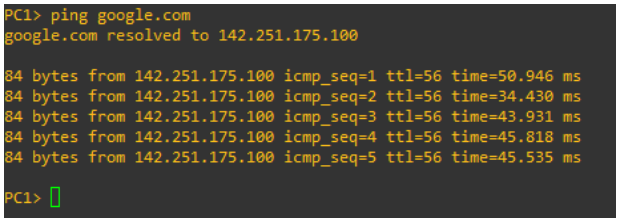
3.2 Hasil Simulasi

Untuk melihat keberhasilan dari topologi, dapat dilakukan percobaan dengan melakukan ping dari satu perangkat ke perangkat lainnya di dalam topologi. Jika ping berhasil atau tidak berhasil dikarenakan firewall, maka topologi dianggap berhasil.



Gambar 9. Percobaan Ping dari PC2 (Inside) ke ownCloud (DMZ)

Gambar 9 menunjukkan bahwa ping dari PC2 (Inside) ke webserver (DMZ) berhasil dikarenakan permintaan dari PC2 dikembalikan oleh webserver. Dalam hal ini PC2 (Inside) memiliki akses untuk membuka webserver.

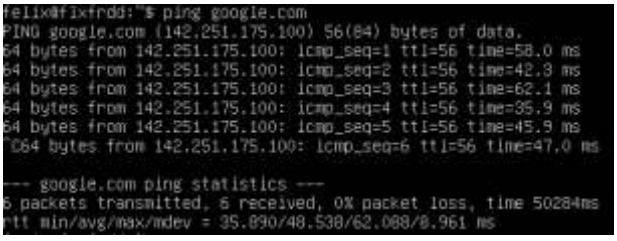


Gambar 10. Percobaan Ping dari PC1 (Inside) ke google.com

Gambar 10 menunjukkan bahwa ping dari PC1 (Inside) menuju google.com berhasil. Hal ini membuktikan bahwa area Inside memiliki akses internet karena DNS.

Gambar 11. Percobaan Ping dari ownCloud (DMZ) ke webClient dengan keadaan firewall dinonaktifkan (Outside)

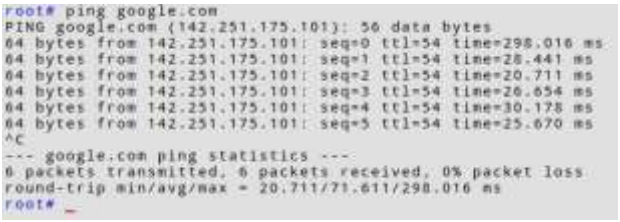
Gambar 11 menunjukkan bahwa ping dari ownCloud (DMZ) ke webclient (Outside) berhasil dikarenakan permintaan dari host dari ownCloud dikembalikan oleh webclient. Hal ini membuktikan bahwa routing dan firewall sudah berhasil.



Gambar 12. Percobaan Ping dari Webserver (DMZ) ke google.com

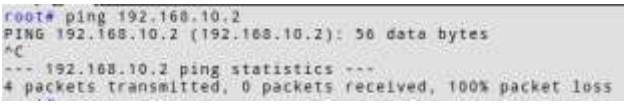
Gambar 12 menunjukkan bahwa ping dari webserver (Inside) menuju google.com berhasil. Hal ini membuktikan bahwa webserver memiliki akses internet.

.



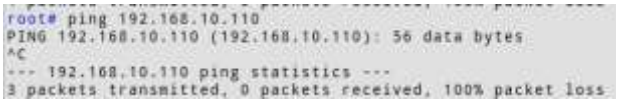
Gambar 13. Percobaan Ping dari Webclient (Outside) ke google.com

Gambar 13 menunjukkan bahwa ping dari webclient (outside) menuju google.com berhasil. Hal ini membuktikan bahwa webclient memiliki akses internet.



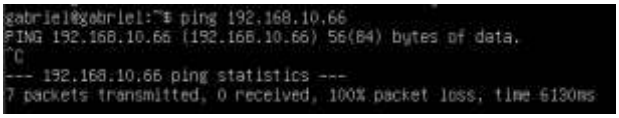
Gambar 14. Percobaan Ping dari Webclient (Outside) ke PC1 (Inside)

Gambar 14 menunjukkan bahwa webclient tidak dapat melakukan Ping ke PC1. Hal ini membuktikan firewall berfungsi (terdapat perbedaan security level pada setiap zona).



Gambar 15. Percobaan Ping dari Webclient (Outside) ke Webserver (DMZ)

Gambar 15 menunjukkan bahwa webclient tidak dapat melakukan Ping ke Webserver. Hal ini membuktikan bahwa firewall sudah berfungsi.

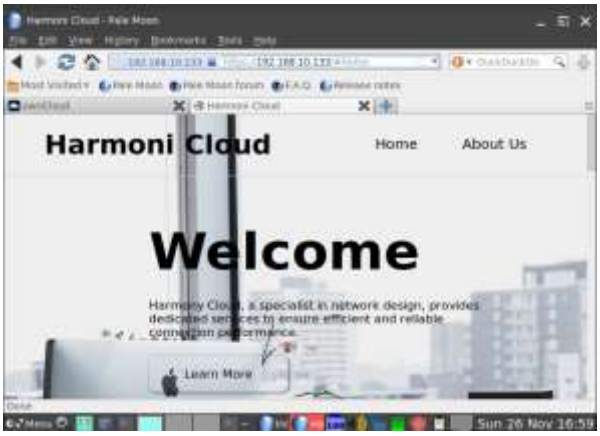


Gambar 16. Percobaan Ping dari Webserver (DMZ) ke PC3 (Inside)

Gambar 16 menunjukkan bahwa webserver tidak dapat melakukan Ping menuju daerah inside yaitu PC3. Hal ini dikarenakan terdapat firewall yang membatasi setiap zona dengan tingkatan security level yang berbeda.

Gambar 17. Percobaan Akses Website ownCloud (DMZ) dari WebClient (Outside)

Percobaan untuk mengakses website ownCloud dapat dilihat pada Gambar 17. Walaupun tidak bisa Ping website owncloud, tetapi dapat mengakses websitenya karena menggunakan ip lain yang tersedia dengan cara mengatur *permit* TCP pada *access-list* di firewall.

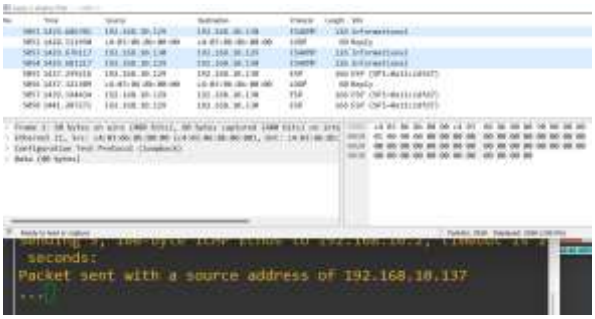


Gambar 18. Akses Webserver (DMZ) dari Webclient (outside)

Seperti website ownCloud, webserver dapat diakses melalui browser pada webclient karena *access-list permit* TCP sudah diatur pada firewall. Namun, webclient tidak dapat ping webserver secara langsung.

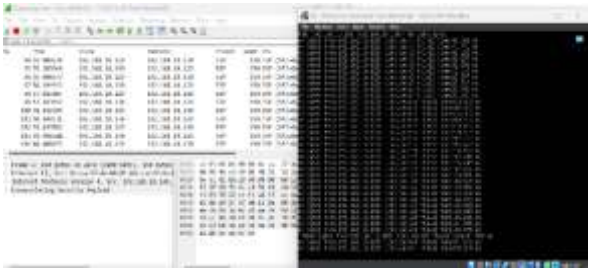
Gambar 19. Akses IP Address Internal Website ownCloud (DMZ) dari Webclient (outside)

Percobaan pada Gambar 19, menunjukkan bahwa webclient di outside dapat mengakses ip internal website ownCloud yang berada di DMZ karena *permit tcp* dari sumber *any* ke webserver dan website ownCloud. Namun, webclient tidak dapat ping secara langsung ke ip internal website ownCloud karena perbedaan security level dan hanya *permit tcp*.



Gambar 20. Cek VPN pada saat Ping dari R3 ke PC1

Ping PC1 dilakukan dengan *source* interface f1/0 router 3 agar ping dimulai dari *local-network* router 3. *Traffic* protokol tersebut sudah menjadi Encapsulating Security Payload (ESP) yang berarti sudah dienkripsi.



Gambar 21. Cek VPN pada saat Ping dari ownCloud ke Webclient

Ping webclient dimulai dari *local-network* ownCloud. Ketika *packet* melewati tunnel diantara Cisco ASAv dan router 3, *packet* akan dienkripsi.

4. Kesimpulan

Simulasi jaringan terdistribusi yang dilakukan untuk Small Office Home Office (SOHO) dengan layanan cloud, yaitu dengan ownCloud, telah meraih kesuksesan dalam menggambarkan integrasi yang efektif antara teknologi jaringan terdistribusi dan layanan cloud. Dengan penerapan konsep-konsep seperti Subnetting, NAT, VPN, dan Firewall, simulasi ini memberikan landasan kokoh bagi efisiensi, keamanan, dan aksesibilitas data dalam konteks SOHO. Salah satu aspek penting yang berhasil diimplementasikan adalah efisiensi penggunaan alamat IP melalui metode Subnetting Variable Length Subnet Mask (VLSM), yang secara signifikan meningkatkan optimalisasi penggunaan alamat IP dalam jaringan.

Keberhasilan dalam menerapkan layanan cloud ownCloud memberikan bukti tentang kemudahan

manajemen file dan fleksibilitas akses data dari berbagai lokasi, mencerminkan relevansi serta kebutuhan akan solusi cloud dalam bisnis skala kecil dan menengah. Pengaturan keamanan jaringan dengan Firewall dan Access Control List (ACL) memberikan perlindungan yang efektif dan mengontrol akses antar zona jaringan. Selain itu, implementasi VPN (Virtual Private Network) berhasil membangun sirkuit virtual, memastikan keamanan komunikasi antar lokasi dengan baik.

Penerapan HTTPS pada webserver dengan sertifikat OpenSSL menunjukkan kesungguhan dalam meningkatkan tingkat keamanan komunikasi, memberikan tambahan lapisan perlindungan terutama ketika berurusan dengan data sensitif. Hasil pengujian yang mencakup berbagai skenario, seperti ping antar perangkat, akses internet, dan koneksi VPN, berhasil membuktikan keberhasilan dan kestabilan implementasi jaringan.

Meskipun berhasil, simulasi ini tetap membuka potensi pengembangan lebih lanjut. Skalabilitas jaringan, peningkatan keamanan dengan tambahan fitur seperti IDS/IPS (Intrusion Detection System/Intrusion Prevention System), pemantauan kinerja jaringan, pengelolaan kapasitas yang lebih proaktif, dan eksplorasi layanan cloud tambahan menjadi potensi pengembangan yang dapat mendukung pertumbuhan dan evolusi bisnis yang berkelanjutan. Keseluruhan, simulasi ini tidak hanya memberikan kontribusi dalam pemahaman teoritis tetapi juga memberikan pengalaman praktis yang berharga dalam penerapan solusi jaringan terdistribusi dan layanan cloud di lingkungan SOHO.

REFERENSI

[1] F. Roshna R, How cloud computing has changed the future of internet technology, 2022.

[2] H. S. Ira Zulfa, "Sistem Jaringan Small Office Home Office (SOHO)", 2023.

[3] N. F. D. J. W. Andrew S. Tanenbaum, Computer Networks, Pearson, 2021.

[4] R. N. D, "IMPLEMENTASI METODE VLSM (VARIABLE LENGTH SUBNET MASK) PADA PEMETAAN IP ADDRESS LAN (LOCAL ARE NETWORK) STIPER SRIWIGAMA PALEMBANG," *Journal of Computer Science and Information Systems,* vol. 2, no. Vol.2 No. 2 (2018): COMPUTATIO : JOURNAL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS, p. 7, 2018.

[5] I. Gunawan, "Analisis Layer Aplikasi (Protokol HTTP) menggunakan Wireshark," *Jurnal Teknik Elektro Smart,* vol. 1, no. Vol 1 No 1 (2021): JES (Jurnal Elektro Smart), p. 3, 2021.

[6] ownCloud, "Why ownCloud," ownCloud, 1 1 2023. [Online]. Available: https://owncloud.com/why-owncloud/. [Diakses 24 November 2023].

[7] ownCloud, “Install ownCloud on Ubuntu 22.04,” [Online]. Available: https://doc.owncloud.com/server/next/admin_manual/installation/quick_guides/ubuntu_22_04.html. [Diakses 12 November 2023].
ownCloud, “Install ownCloud on Ubuntu 22.04,” [Online]. Available: https://doc.owncloud.com/server/next/admin_manual/installation/quick_guides/ubuntu_22_04.html. [Diakses 12 November 2023].

[8] GNS3, “Getting Started with GNS3,” [Online]. Available: https://docs.gns3.com/docs/. [Diakses 12 November 2023].

[9] Cisco, “Configure and Filter IP Access Lists,” 7 Oktober 2022. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html. [Diakses 12 November 2023].

[10] Cisco, “Configure Network Address Translation,” 3 November 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html. [Diakses 12 November 2023].

[11] Cisco, “Configure Network Address Translation and ACLs on an ASA Firewall,” 14 November 2022. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html. [Diakses 12 November 2023].

[12] Cisco, “Configure ASA Access Control List for Various Scenarios,” 18 Oktober 2022. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/217679-asa-access-control-list-configuration-ex.html. [Diakses 12 November 2023].

[13] Cisco, “Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router,” 17 Februari 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios/218432-configure-a-site-to-site-ipsec-ikev1-tun.html. [Diakses 23 November 2023].

[14] E. Jacobsen, "how to restrict traffic thru VPN Site-to-site tunnel," 18 November 2010. [Online]. Available: https://community.cisco.com/t5/vpn/how-to-restrict-traffic-thrue-vpn-site-to-site-tunnel/td-p/1541114. [Diakes 23 November 23].