CLOUD
Jurnal Networking System and Security System
E-ISSN 3090-6601

Implementasi Keamanan Anti Ddos Menggunkan Router Mikrotik Pada Layanan Cloud Storage Basis Local Di Sekolah Menengah Kejuruan

M.Ihsan Siregar[1], Imran Lubis[2], Risko Liza[3*]

[1,2,3] Universitas Harapan, Medan, Indonesia
[1*]mihsansrg@gmail.com, [2]imran.loebis.medan@gmail.com, [3]risko.liza@gmail.com
[*)] mihsansrg@gmail.com

Abstrak−Penelitian ini mengembangkan sistem Cloud Storage berbasis lokal di Sekolah Menengah Kejuruan dengan menggunakan OwnCloud sebagai platform penyimpanan, Linux Ubuntu 20.04 LTS sebagai sistem operasi, dan Router Mikrotik sebagai perlindungan terhadap serangan DDoS. Pengujian dilakukan dalam dua skenario, di mana tanpa perlindungan, serangan DDoS menyebabkan server tidak dapat diakses, sedangkan dengan perlindungan Router Mikrotik, server tetap stabil. Hasil penelitian menunjukkan bahwa penggunaan Filter Rules pada Router Mikrotik efektif dalam menangkal serangan Syn Flood, sehingga Cloud Storage lokal dapat meningkatkan keamanan data serta mempermudah akses dan berbagi dokumen di lingkungan sekolah.

Kata Kunci : *Komputasi Awan, Mikrotik, Owncloud, DDOS, Ubuntu,*

Abstract−This research develops a local-based Cloud Storage system at Vocational High Schools using OwnCloud as a storage platform, Linux Ubuntu 20.04 LTS as an operating system, and Mikrotik Router as protection against DDoS attacks. Tests were carried out in two scenarios, where without protection, DDoS attacks caused the server to be inaccessible, while with Mikrotik Router protection, the server remained stable. The results show that the use of Filter Rules on the Mikrotik Router is effective in warding off Syn Flood attacks, so that local Cloud Storage can increase data security and facilitate access and sharing of documents in the school environment.

Keyword : *Cloud Computing, Mikrotik, Owncloud, DDOS, Ubuntu*

1. PENDAHULUAN

Perkembangan teknologi informasi dapat meningkatkan kinerja dan memungkinkan berbagai kegiatan dapat dilaksanakan dengan cepat, tepat dan akurat, sehingga akhirnya akan meningkatkan produktivitas.[1] Perkembangan ini membawa berbagai dampak dalam kehidupan bermasayarakat, berbangsa dan bernegara, setiap individu tertarik untuk mengunakan dan memanfaatkan setiap perkembangan ini.[2]

Data merupakan informasi penting dan berharga dalam suatu lembaga atau instansi, baik itu yang bergerak di bidang pendidikan, kebudayaan, politik, ekonomi dan sebagainya. Oleh karena itu data sangat penting untuk dijaga atau dimanajemen dengan baik oleh instansi yang bersangkutan.[3]

Namun, penyimpanan data di media internal yang bergantung pada sistem lokal memiliki beberapa kelemahan, terutama dalam hal keamanan dan kemudahan penggunaan. Keamanan penting karena media penyimpanan internal bisa terhapus atau rusak karena virus atau hal lainnya. Selain itu, media penyimpanan internal tidak selalu praktis karena harus dibawa ke mana-mana. Keterbatasan dalam penyimpanan data sering dijumpai ketika kita akan menyimpan file-file yang akan dipindahkan ke database internet seperti yang biasa dilakukan saat ini dengan melakukan penyimpanan data pada email, google drive, ataupun dropbox.[4]

Menurut National Institute of Standard and Technology (NIST)[5], terdapat lima karakteristik yang membedakan cloud computing dari layanan teknologi lainnya, yaitu layanan on-demand self-Service, akses jaringan yang luas, sumber daya pooling, elastisitas yang cepat, dan terukur layanan. Manfaat dari teknologi cloud adalah kemampuan mengakses data dari mana saja dan kapan saja, serta menyinkronkan data tersebut ke smartphone dan gadget lainnya. Penggunaan teknologi cloud di instansi pendidikan sangat penting karena manfaatnya. Namun, implementasi cloud tidak mudah dan membutuhkan teknik serta pemahaman yang baik.[6]

Masalah ini terjadi di Sekolah Menengah Kejuruan Citra Harapan, di mana banyak guru dan pegawai mengeluhkan kurangnya media penyimpanan dan kesulitan menyimpan dokumen sekolah karena jumlah dokumen yang terlalu banyak dan tidak rapi. Kehilangan data penting tentu sangat merepotkan, sehingga diperlukan media penyimpanan tambahan untuk mengatasi masalah ini. Solusi yang tepat untuk menjawab permasalahan tersebut diatas adalah dengan penerapan teknologi cloud storage menggunakan teknologi virtualisasi. Implementasi teknologi cloud storage yang akan digunakan adalah aplikasi owncloud.[7]

Pada penelitian ini terdapat penelitian terkait yaitu “Perancangan Cloud Storage Menggunakan Owncloud pada Fakultas Teknik Universitas Andi Djemma” membahas penerapan Owncloud sebagai solusi manajemen file

di Universitas Andi Djemma, menggantikan sistem file sharing konvensional yang rentan terhadap kerusakan data. Cloud storage tersebut diakses melalui jaringan lokal dan internet dengan IP Public dari IndiHome.[8]

Penelitian saya berfokus pada aspek keamanan, khususnya perlindungan terhadap serangan DDoS dengan Router Mikrotik. Pengujian menunjukkan bahwa tanpa perlindungan, server rentan terhadap serangan, sedangkan dengan Filter Rules pada Router Mikrotik, jaringan tetap stabil dan aman. Kontribusi penelitian ini adalah menghadirkan solusi cloud storage berbasis lokal yang lebih aman bagi institusi pendidikan, memastikan akses data tetap stabil dan terlindungi.

Teknologi Owncloud berbasis client Server dapat menjadi solusi yang tepat, dengan menambahkan sistem keamanan yang disediakan oleh Router Mikrotik yang dapat mencegah serangan Distributed Denial of Service (DDoS) bertujuan untuk melemahkan target sehingga target yang diserang menjadi down ataupun hang.[9] Menurut[10]. Serangan Denial-of-Service adalah serangan yang dilakukan oleh hacker untuk melumpuhkan suatu sistem jaringan web dengan membanjiri server dengan jumlah lalu lintas data yang tinggi, atau melakukan request data ke sebuah server sehingga server tidak lagi dapat memberikan layanan dan menjadi crash.

Penelitian ini bertujuan untuk merancang sistem keamanan anti-DDoS menggunakan Router Mikrotik pada layanan Cloud Storage berbasis lokal di SMK, sehingga layanan tersebut dapat terlindungi dari serangan DDoS yang berpotensi mengganggu akses dan kinerja sistem. Selain itu, penelitian ini juga mengevaluasi pengaruh implementasi sistem keamanan tersebut terhadap kinerja layanan Cloud Storage, dengan membandingkan kondisi sebelum dan sesudah penerapan keamanan. Hasil penelitian menunjukkan bahwa tanpa perlindungan, serangan DDoS dapat menyebabkan server tidak dapat diakses dan mengalami downtime. Namun, setelah menerapkan Filter Rules pada Router Mikrotik, jaringan tetap stabil, lalu lintas data terjaga, dan server tidak terpengaruh secara signifikan oleh serangan. Dengan demikian, penerapan sistem keamanan ini terbukti efektif dalam meningkatkan ketahanan Cloud Storage berbasis lokal di SMK, memastikan akses yang aman dan andal bagi pengguna.

2. METODE PENELITIAN

Berikut metode penelitian yang digunakan dalam penelitian:

Gambar 1. Metodologi Penelitian

2.1 Studi Literatur

Mengkaji konsep serangan DDoS dan metode mitigasinya. Menganalisis fitur keamanan MikroTik yang dapat digunakan untuk mitigasi serangan DDoS. Meneliti praktik terbaik dalam pengamanan layanan cloud storage lokal

2.2 Perancangan Sistem

Menentukan parameter keamanan yang akan diterapkan pada router MikroTik. Mendesain skenario pengujian dengan berbagai jenis serangan DDoS.

2.3 Implementasi Dan Konfigurasi

Mengonfigurasi firewall dan fitur keamanan lainnya di MikroTik. Menerapkan metode filtering dan rate-limiting untuk mitigasi DDoS. Mengintegrasikan sistem monitoring lalu lintas jaringan.

2.4 Pengujian dan Analisis

Melakukan simulasi serangan DDoS terhadap cloud storage lokal. Mengukur efektivitas mitigasi berdasarkan parameter seperti packet drop rate, bandwidth usage, dan response time. Membandingkan kondisi jaringan sebelum dan sesudah implementasi keamanan.

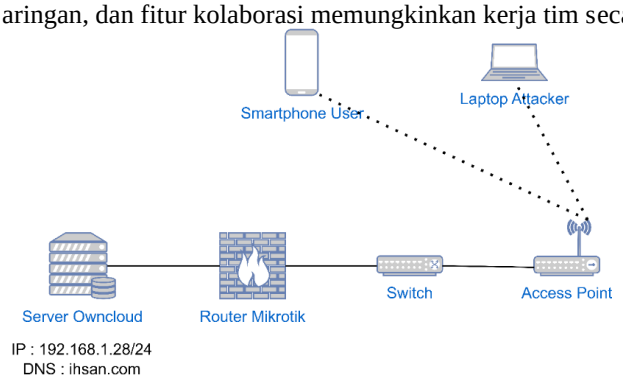
2.5 Evaluasi dan Kesimpulan

Mengevaluasi efektivitas konfigurasi yang telah diterapkan. Menarik kesimpulan dan memberikan rekomendasi untuk optimalisasi keamanan cloud storage lokal di SMK.

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Skema Topologi

Penggambaran skema topologi yang akan diimplementasikan pada penelitian ini menggunakan bantuan aplikasi berbasis Web Draw.io. Draw.io sebagai aplikasi web, memberikan kemudahan aksesibilitas tanpa perlu instalasi, memungkinkan pengguna merancang topologi jaringan dari berbagai perangkat. Antarmuka intuitif dan alat gambar yang lengkap mempermudah pengguna membuat Diagram jaringan dengan cepat. Visualisasi yang jelas membantu memahami struktur jaringan, dan fitur kolaborasi memungkinkan kerja tim secara real-time.



Gambar 2. Skema Topologi Jaringan Menggunakan Draw.io

3.1.1 Instalasi *Owncloud* pada *Ubuntu* 20.04 LTS

Ada beberapa *Software* pendukung yang harus terpasang pada komputer untuk membangun *Owncloud* system seperti PHP 7.1, Web *Server* Apache2, *DNS Server* Bind9, Database *Server* MariaDB, dan aplikasi *Owncloud*, Berikut beberapa syntak yang digunakan untuk rancangan pembuatan *Owncloud* pada sistem operasi *Ubuntu*, yaitu:

1. Interfaces Konfigurasi IP Address

   "root@ihsan:apt-get install net-tools" "root@ihsan:/home/ihsan# nano /etc/netplan/00-installer-config.yaml"

   Keterangan : Merupakan perintah untuk melihat dan mengedit konfigurasi jaringan yang terkait dengan sistem operasi *Ubuntu* 20.04 LTS "root@ihsan:*Service* netplan apply"

2. Pengalamatan IP Address

network: ethernets: enp0s3: addresses: [192.168.1.28/24] gateway4: 192.168.1.1 name*Server*s: search: [ihsan.com] addresses: [192.168.1.28,8.8.8.8] enp0s8: *DHCP*4: true version: 2

Keterangan :

a. *Network* = merupakan bagian awal dari konfigurasi yang menandakan bahwa ini adalah konfigurasi jaringan.

b. Ethernets = adalah bagian di mana Anda dapat mengonfigurasi antarmuka Ethernet.

c. enp0s3 = adalah nama antarmuka Ethernet yang dikonfigurasi dalam contoh ini.

d. Addresses = menentukan alamat IP yang diberikan pada antarmuka Ethernet tersebut. Dalam contoh ini, alamat IP yang diberikan adalah 192.168.1.28 dengan subnet mask /24.

e. Gateway4 = menentukan gateway default yang digunakan untuk mengirimkan lalu lintas keluar dari jaringan. Dalam contoh ini, gateway default adalah 192.168.1.1.

f. Name*Server*s = menentukan *Server DNS* yang akan digunakan. Dalam contoh ini, domain pencarian adalah "ihsan.com" dan ada dua alamat *DNS* yang digunakan, yaitu 192.168.1.28 dan 8.8.8.8.

g. enp0s8 = adalah antarmuka Ethernet kedua yang dikonfigurasi dalam contoh ini.

h. *DHCP*4: true = menandakan bahwa antarmuka tersebut akan menggunakan konfigurasi *DHCP* untuk mendapatkan alamat IP secara otomatis.

i. version: 2 = menunjukkan versi konfigurasi jaringan yang digunakan.

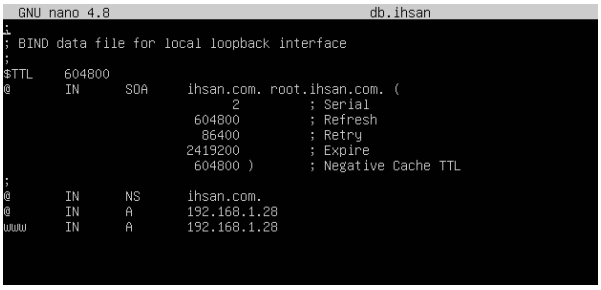
j. Versi 2 adalah format konfigurasi yang umum digunakan pada sistem operasi *Linux* untuk mengkonfigurasi jaringan.

Dengan konfigurasi ini, antarmuka "enp0s3" akan memiliki alamat IP statis (192.168.1.28/24) dengan gateway default 192.168.1.1 dan menggunakan *Server DNS* 192.168.1.28 dan 8.8.8.8. Sementara itu, antarmuka "enp0s8" akan menggunakan konfigurasi *DHCP* untuk mendapatkan alamat IP secara otomatis.

3. Instalasi Bind9 dan Konfigurasi Bind9

“root@ihsan:/home/ihsan# apt-get install bind9 lynx apache2”“root@ihsan:#sudo sed -i "s/Options Indexes FollowSymLinks/Options FollowSymLinks/" /etc/apache2/apache2.conf”

Keterangan : Perintah untuk menginstal paket *DNS Server* yaitu bind9 “root@ihsan:nano /etc/resolv.conf” “name*Server* 127.0.0.53 options e*DNS*0 trust-ad search ihsan.com” “root@ihsan:nano /etc/hosts” “127.0.0.1 localhost 127.0.1.1 ihsan” root@ihsan:cd /etc/bind/ root@ihsan:/etc/bind# cp db.local db.ihsan root@ihsan:/etc/bind# cp db.127 db.192 root@ihsan:/etc/bind#nano db.ihsan

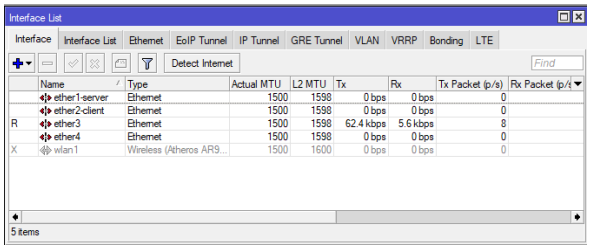


Gambar 3. Konfigurasi Pada db.ihsan

3.2 Implementasi Firewall Filter Rules Pada Router Mikrotik

Sebelum mengkonfigurasi aturan-aturan yang akan dIPakai sebagai Rule untuk mencegah serangan *DDoS*, Ada beberapa Konfigurasi yang harus disetting terlebih dahulu pada *Router Mikrotik* untuk membangun system Keamanan Anti *DDoS* seperti Interfaces List, Konfigurasi IP Address pada port yang dIPakai, konfigurasi *NAT*, dan konfigurasi Rule IP *Filter*ing RAW. Berikut beberapa konfigurasi yang digunakan, yaitu :

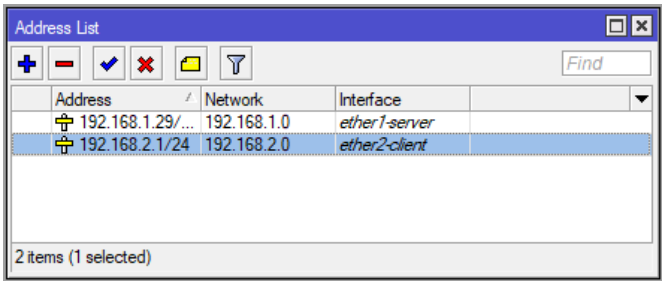
1. Konfigurasi Interfaces



Gambar 4. Konfigurasi Interfaces List

Dengan memberi nama yang deskriptif pada setiap interface, administrator dapat dengan mudah mengidentifikasi dan membedakan fungsi dari masing-masing port, seperti untuk koneksi *Server* atau client. Hal ini mempermudah pemantauan dan pemecahan masalah jaringan, karena dapat dengan cepat mengetahui peran masing-masing interface.

2. Konfigurasi IP Address

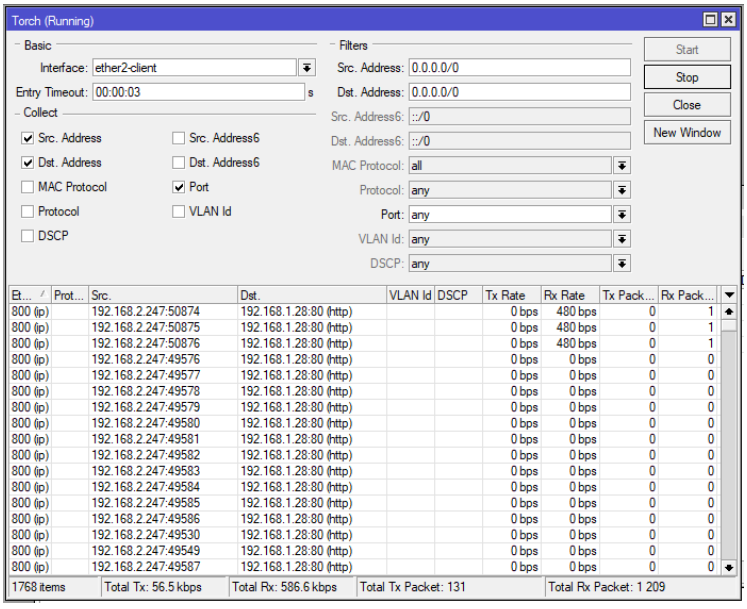


Gambar 5. Konfigurasi IP Address Pada port *Server* dan Client

Gambar diatas menampilkan konfigurasi IP Address pada 2 port. Pada port 1 bernama *Server* yang memiliki IP Address 192.168.1.29/24 yang mengarah langsung ke Laptop *Server*. Sementara pada Port 2 bernama Client memiliki IP Address 192.168.2.1/24 yang terhubung langsung pada Switch dan Access Point yg terhubung ke Client.

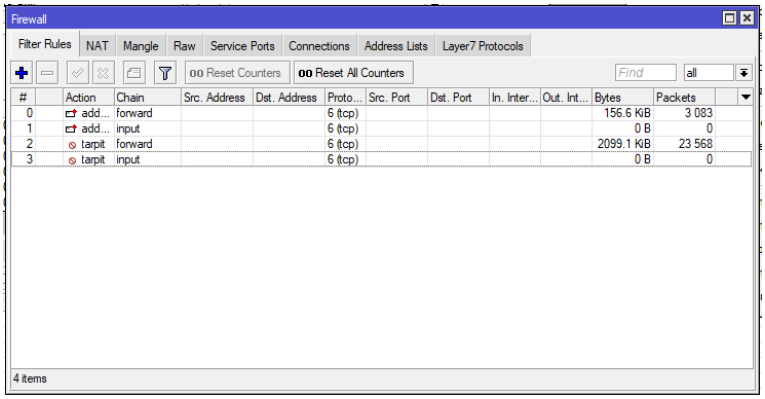
3.3 Hasil Pengujian Serangan *DDoS Server Owncloud* Dengan Tambahan Keamanan

Dalam sub bab ini akan membahas hasil dari serangan *DDoS* setelah menerapkan langkah-langkah keamanan tambahan melalui *Router Mikrotik*. Akan menampilkan hasil sejauh mana efektivitas perlindungan yang telah diimplementasikan dalam menjaga ketersediaan layanan dan respons dari *Server Owncloud*.



Gambar 6. Tampilan Trafik Jaringan Pada Saat Penyerangan

Pada gambar diatas, terlihat kondisi trafik yang tetap stabil saat dilakukan serangan *DDoS*. Meskipun terjadi upaya serangan, terlihat bahwa tidak ada peningkatan yang signifikan dalam tingkat transmisi (TX) dan penerimaan (RX) atau jumlah paket yang melebihi ambang normal. Hal ini menunjukkan keberhasilan sistem dalam menangani serangan *DDoS* tanpa terpengaruh secara signifikan pada kinerja atau ketersediaan layanan.



Gambar 7. Tampilan Firewall *Filter Rules*

3.4 Hasil Analisis *QOS (Quality Of Service)* dari Pengujian Serangan

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. Salah satu parameter untuk menilai QoS (Quality of Service) dari sebuah jaringan adalah delay. Delay atau waktu paket di dalam system adalah waktu sejak paket tiba ke dalam system sampai paket selesai ditransmisikan. Salah satu jenis delay adalah delay transmisi, yaitu waktu yang dibutuhkan untuk sebuah pengirim mengirimkan sebuah paket. Delay dapat dipengaruhi oleh kongesti, media fisik, jarak atau juga waktu proses yang lama. Untuk pengukuran parameter QoS, penulis menggunakan aplikasi Wireshark. Wireshark adalah packet analyzer gratis dan open Source. Tools ini seringkali digunakan untuk menemukan masalah pada jaringan, pengembangan perangkat lunak dan protokol komunikasi, dan pendidikan. Wireshark dapat berjalan pada hampir semua system operasi yang tersedia.

Tabel 1 Rekapitulasi Parameter *QOS*

No	Pengukuran	*Parameter QOS*			
		Packet Loss	***Delay (ms)***	***Jitter (ms)***	***Throughtput (bps)***
1	Pengujian Serangan DDoS Server Owncloud Tanpa Keamanan	0%	0,528	0,529	2.679
2	Pengujian Serangan DDoS Server Owncloud Dengan Tambahan Keamanan Router Mikrotik	0%	7,5	7,6	328,8

Hasil pengukuran QoS pada Pengujian Serangan DDoS Server Owncloud Tanpa Keamanan : Packet Loss yaitu 0% dengan kategori “Sangat Bagus”, Delay yaitu 0,528 dengan kategori “Sangat Bagus”, Jitter yaitu 0,529 dengan kategori “Sangat Bagus”, dan Throughtput yaitu 2.679 dengan kategori “Sangat Bagus“ Hasil pengukuran QoS pada Pengujian Serangan DDoS Server Owncloud Dengan Tambahan Keamanan Router Mikrotik : Packet Loss yaitu 0% dengan kategori “Sangat Bagus”, Delay yaitu 7,5 dengan kategori “Sangat Bagus”, Jitter yaitu 7,6 dengan kategori “Bagus”, dan Throughtput yaitu 328,8 dengan kategori “Sangat Bagus Dari hasil pengujian diatas, dapat disimpulkan bahwa penerapan keamanan anti DDoS menggunakan router mikrotik fektif dalam mencegah kehilangan paket data meskipun mengorbankan beberapa aspek kualitas layanan lainnya seperti delay, jitter, dan throughtput.

4. KESIMPULAN

Berdasarkan pembahasan diatas, berikut adalah beberapa kesimpulan yang dapat diambil :

1. Keamanan anti-DDoS dirancang dengan mengimplementasikan Filter firewall pada Router Mikrotik, yang memblokir paket data berlebih dan mencurigakan, serta menambahkan Filter Rules untuk mengidentifikasi dan memblokir IP Address penyerang. Langkah ini terbukti efektif dalam melindungi sistem jaringan dari serangan DDoS.
2. Implementasi keamanan anti-DDoS membuat sistem jaringan tetap stabil dan tidak terganggu oleh serangan. Penggunaan CPU dan memori tetap stabil, dan Owncloud dapat beroperasi normal. Keamanan jaringan yang ditingkatkan juga mengurangi risiko gangguan dan memastikan layanan Cloud Storage di SMK efisien dan aman.

3. Owncloud sebagai layanan penyimpanan cloud memudahkan akses dan berbagi dokumen di Sekolah Menengah Kejuruan, serta memfasilitasi kerja tim dan kolaborasi. Pengguna dapat mengelola dokumen secara terpusat melalui jaringan lokal dan web browser dengan menggunakan Owncloud.
4. Serangan Denial of Service (DOS) dapat merusak target dan meningkatkan konsumsi sumber daya seperti CPU, sehingga diperlukan tindakan pencegahan yang efektif. Implementasi Filter firewall pada Router Mikrotik terbukti efektif dalam mengurangi jumlah paket data yang dikirimkan oleh attacker, memungkinkan router beroperasi normal tanpa gangguan signifikan. Filter Rules pada Router Mikrotik efektif dalam mengamankan sistem jaringan dari serangan Syn Flood dengan memblokir IP Address yang mencurigakan.
5. Owncloud hanya dapat diakses melalui jaringan lokal Sekolah (intranet), menunjukkan langkah-langkah pengamanan yang diterapkan untuk membatasi akses dari luar dan mengurangi penggunaan paket data berbayar serta gangguan jaringan.

REFERENCES

[1] S. U. Lathifah, "Perkembangan Teknologi Informasi di Indonesia | kumparan.com," *Kompasiana.com*, pp. 1–7, 2022.

[2] M. Danuri, "Development and transformation of digital technology," *Infokam*, vol. XV, no. II, pp. 116–123, 2019.

[3] Muhammad Ibrahim, "Analisis Dan Implementasi Owncloud sebagai media penyimpanan pada Yayasan Salman Al-Farisi Yogyakarta Pendahuluan Landasan Teori Pembahasan," *Anal. Sist. Penyimpanan Data Menggunakan Sist. Cloud Comput. Stud. Kasus SMK N 2 Karanganyar*, vol. 14, no. 04, p. 32, 2013.

[4] E. Rakhmat, S. Dwiyatno, S. Sulistiyon, A. Irawan, and F. Setiawan, "Pemanfaatan Aplikasi Owncloud Pada Sistem Keamanan Cloud Computing," *J. Sist. Inf. dan Inform.*, vol. 4, no. 2, pp. 146–155, 2021, doi: 10.47080/simika.v4i2.1454.

[5] G. A. Osorio, C. S. Del Real, C. A. F. Valdez, M. C. Miranda, and A. H. Garay, "Effect of inclusion of cactus pear cladodes in diets for growing-finishing lambs in central Mexico," *Acta Hortic.*, vol. 728, pp. 269–274, 2006.

[6] A. Widarma, H. F. Siregar, and I. R. Sitorus, "Implementasi Cloud Computing Menggunakan Nextcloud Berbasis Infrastructure as a Service (IaaS) Implementation," *J. Comput. Eng. Syst. Sci.*, vol. 9, no. 1, pp. 336–346, 2024.

[7] A. Manalu and S. Sitanggang, "Perancangan Dan Implementasi Private Cloud Storage Dengan Owncloud Pada Jaringan Lokal Menggunakan Virtualbox.," *J. Comput. Networks*, vol. 1, no. 2, pp. 60–71, 2019.

[8] D. Dasril and A. Laswi, "Perancangan Cloud Storage Menggunakan Owncloud pada Fakultas Teknik Universitas Andi Djemma," *Semantik*, pp. 150–155, 2019.

[9] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes.," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 6, no. 1, pp. 172–180, 2022.

[10] Q. Gu and P. Liu, "Denial of Service Attacks," *Handb. Comput. Networks*, vol. 3, no. 9, pp. 454–468, 2012, doi: 10.1002/9781118256107.ch29.