Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 4, **Number** 1, Maret 2024
https://doi.org/10.47709/digitech.v4i1.4261

Peningkatan Keamanan Jaringan LAN dan WLAN Melalui Standard Acces Control List

Muhlis Tahir [1*], Hariyanto[2], M. Imam Firdausi[3], Saim[4], Nuriyah[5] , Maimunah[6]
[1,2,3,4,5,6]Universitas Trunojoyo Madura
[1]muhlistahir@trunojoyo.ac.id [2]riyanwin16@gmail.com [3]mimamfirdausii@gmail.com [4]ardukduko@gmail.com
[5]Nuriyariya097@gmail.com [6]ainasyafania5@gmail.com

Histori Artikel:
Diajukan: 10 Juli 2024
Disetujui: 8 Agustus 2024
Dipublikasi: 9 Agustus 2024

Kata Kunci:
LAN, WLAN, Jaringan Komputer, Standard Acces Control Lists, Router

Abstrak
Penelitian ini bertujuan untuk meningkatkan keamanan jaringan komputer SMK Negeri 1 Blega dengan menerapkan access control list (ACL). Menambah kompleksitas Keamanan dunia maya memerlukan perlindungan jaringan komputer yang kuat. ACL adalah mekanisme keamanan yang memungkinkan Anda mengatur dan membatasi lalu lintas yang masuk dan keluar dari jaringan Anda. Penelitian ini dilakukan dalam tahap percobaan yang meliputi pengujian keamanan jaringan awal, implementasi langkah-langkah keamanan yang diusulkan, dan pengujian jaringan internal router. Pengujian telah memungkinkan kami untuk menutup celah keamanan dan membatasi akses tidak sah ke server dari PC klien Lab Komputer. Akses perangkat Wi-Fi ke server juga berhasil dibatasi kecuali PC Admin Lab Komputer, yang diizinkan mengakses server. Penerapan ACL kini dapat secara efektif meningkatkan keamanan jaringan. Ini juga menyediakan pemantauan rutin dan evaluasi harian terhadap aturan ACL dan rekomendasi untuk mengintegrasikan fitur keamanan tambahan untuk terus menjaga keamanan jaringan Anda. Hasil penelitian ini akan memberikan kontribusi positif dalam mengatasi tantangan keamanan di era digital yang semakin kompleks.

PENDAHULUAN

Dalam era Digital yang semakin berkembang ini, jaringan komputer sangat penting bagi banyak perusahaan dan lembaga, termasuk lembaga pendidikan seperti SMKN 1 Blega, untuk menjalankan tugas sehari-hari mereka. Namun, ancaman keamanan cyber yang semakin kompleks membutuhkan perlindungan yang kuat terhadap jaringan komputer. Penerbitan Daftar Kontrol A kses Standar (ACL) adalah salah satu cara untuk meningkatkan keamanan jaringan komputer (Krianto Sulaiman & Saripurna, 2021)

Dalam penerapan e-learning, tenaga pendidik dan peserta didik memiliki perannya masing-masing. Tenaga pendidik (guru/dosen/instruktur ataupun widyaiswara memiliki peran sebagai fasilitator dan pembimbing dalam kegiatan pembelajaran, sedangkan peserta didik (siswSa dan mahasiswa) memiliki peran sebagai konstruktor pengetahuan, pebelajar mandiri (independent learners), dan pemecah masalah (problem solvers).

Salah satu masalah yang muncul di intranet SMKN 1 Blega adalah peningkatan konektivitas dan penggunaan teknologi, yang pada gilirannya memungkinkan serangan cyber. Ancaman ini dapat merusak dan mencuri informasi pribadi, mengganggu integritas jaringan, dan memberikan akses yang tidak sah.Untuk mengatasi masalah ini, daftar kontrol akses standar (ACL) harus diterapkan untuk meningkatkan keamanan jaringan komputer di SMKN 1 Blega.

Tujuan dari Standard Access Control List (ACL) adalah untuk mengatur dan mengontrol akses ke jaringan komputer. ACL adalah mekanisme keamanan yang memungkinkan administrator jaringan untuk mengatur dan membatasi lalu lintas data yang masuk dan keluar dari jaringan jaringan (Laksono & Nasution, 2020) Dengan menggunakan ACL, administrator jaringan dapat mengontrol dan membatasi hak akses pengguna, perangkat, atau bahkan aplikasi tertentu ke jaringan, sehingga memungkinkan keamanan jaringan (Chaidir & Wirawan, 2018).

Sebagai langkah untuk meningkatkan keamanan jaringan, studi sebelumnya telah menunjukkan bahwa penerapan Daftar Pengendalian Masuk Standar (ACL) di berbagai jaringan telah berhasil. Studi menunjukkan bahwa penerapan ACL pada jaringan perusahaan dapat secara signifikan mengurangi insiden keamanan. Penelitian juga melihat seberapa baik ACL menghadapi serangan DDoS (Chandra, 2022). Dalam referensi ini, Kurnia dan Mandasari memberikan 40 perspektif tentang berbagai pilihan penerapan ACL yang dapat digunakan untuk memecahkan masalah keamanan di SMKN 1 Blega.

Saat ini, kebutuhan akan keamanan jaringan komputer akan meningkat. Banyak lembaga, termasuk perusahaan, sekolah, dan pemerintah, menyadari betapa pentingnya melindungi data sensitif, menjaga integritas jaringan, dan mencegah akses yang tidak sah. Oleh karena itu, penerapan Standard Access Control List (ACL) untuk melindungi jaringan komputer menjadi sangat penting dan krusial.

Seperti yang ditunjukkan oleh penelitian ini, penggunaan List Control Access Standard (ACL) telah ditunjukkan sebagai strategi yang efektif untuk melindungi jaringan dari serangan yang tidak diinginkan (Kamarudin & Gazali, 2021). Tujuan dari penelitian ini adalah untuk mempelajari bagaimana ACL digunakan dalam konteks keamanan jaringan komputer (Christanto et al., 2018). Metode yang disarankan mencakup pemeriksaan menyeluruh terhadap aturan ACL yang sesuai, penerapan kebijakan akses yang ketat, serta pengawasan dan penegakan rutin. Penelitian baru - baru ini berfokus pada pembuatan solusi keamanan jaringan komputer lengkap yang menggunakan ACL . Dengan menggunakan metode ini, penelitian ini menawarkan keunggulan dan inovasi dalam bentuk perlindungan yang lebih baik terhadap ancaman internal dan eksternal serta manajemen akses yang lebih efektif dan efisien.

Implementasi keamanan jaringan komputer menggunakan Standard Access Control List (ACL) bertujuan untuk mengatur dan mengontrol akses ke jaringan tersebut (Kurniati & Dasmen, 2019).

Beberapa penelitian sebelumnya telah berhasil mengimplementasikan Standard Access Control List (ACL) dalam berbagai jaringan sebagai langkah untuk meningkatkan keamanan. Sebagai contoh, penelitian (Herdiana et al., 2021) menunjukkan bahwa penerapan ACL pada jaringan perusahaan dapat mengurangi insiden keamanan secara signifikan

Fokus penelitian ini adalah bagaimana menerapkan keamanan jaringan komputer di SMKN 1 Blega dengan menggunakan Daftar Pengendalian Akses Standar (ACL) untuk melindungi data siswa, menjaga keamanan jaringan, dan mencegah akses yang tidak sah. Dalam situasi seperti ini, penerapan ACL akan memberikan perlindungan yang kuat dan dapat diandalkan.

STUDI LITERATUR

Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan komputer saling berinteraksi dan bertukar informasi. Terdapat dua peran dalam jaringan komputer, yaitu client (penerima/meminta layanan) dan server (penyedia/pengirim layanan). Jaringan komputer membutuhkan kartu jaringan dan perangkat lunak sistem operasi jaringan (Azmi et al., 2022).

1. LAN (Local Area Network): Jaringan lokal dengan jarak pendek, seperti di rumah, sekolah, atau kantor. Menggunakan konektivitas Ethernet atau WLAN (Wireless Local Area Network).
2. MAN (Metropolitan Area Network): Jaringan kota ke kota yang lebih luas daripada LAN. Memerlukan perangkat khusus dan operator telekomunikasi.
3. WAN (Wide Area Network): Jaringan dengan jangkauan yang sangat luas, mencakup benua. Digunakan untuk koneksi antar negara dengan menggunakan teknologi canggih seperti serat optik.
4.

Setiap jaringan komputer memiliki topologi, yaitu tata letak perangkat yang terhubung. Beberapa jenis topologi meliputi:

1. Bus: Menggunakan satu kabel sebagai media transmisi, semua perangkat terhubung pada kabel utama.
2. Ring: Jaringan membentuk cincin, setiap komputer terhubung satu sama lain.
3. Star: Terdapat satu pusat penghubung (HUB atau Switch) yang menghubungkan semua komputer.
4. Mesh: Komputer terhubung secara langsung satu sama lain, memberikan akses pengiriman data yang cepat.
5. Tree: Topologi bertingkat dan hierarkis dengan menggunakan HUB atau Switch sebagai penghubung dengan file server.

Kabel Jaringan

Kabel jaringan digunakan sebagai media untuk penyaluran data antar komputer. Beberapa jenis kabel jaringan yang umum digunakan meliputi (Dasmen & Rasmila, 2019):

1. . Coaxial: Kabel yang digunakan sebagai penghantar sinyal listrik untuk mentransmisikan data. Biasanya digunakan dalam perpindahan arus.
2. Unshielded Twisted Pair (UTP): Kabel yang terbuat dari bahan penghantar tembaga, dengan isolasi plastik dan lapisan pelindung yang melindungi dari kebakaran dan kerusakan fisik. Kabel UTP terdiri dari empat pasang inti kabel yang dijalin bersama dengan kode warna yang berbeda.
3. Fiber Optic: Kabel yang terbuat dari serat kaca dengan kecepatan transfer data lebih cepat daripada kabel biasa. Biasanya digunakan dalam jaringan backbone karena membutuhkan kecepatan yang tinggi.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan dalam jaringan komputer (Heryanto & Azizah, 2019). TCP/IP memiliki kelas-kelas IP Address (alamat IP) yang terdiri dari kelas A, B, C, D, dan E. Setiap kelas memiliki ukuran dan jumlah yang berbeda.

- Keamanan Jaringan

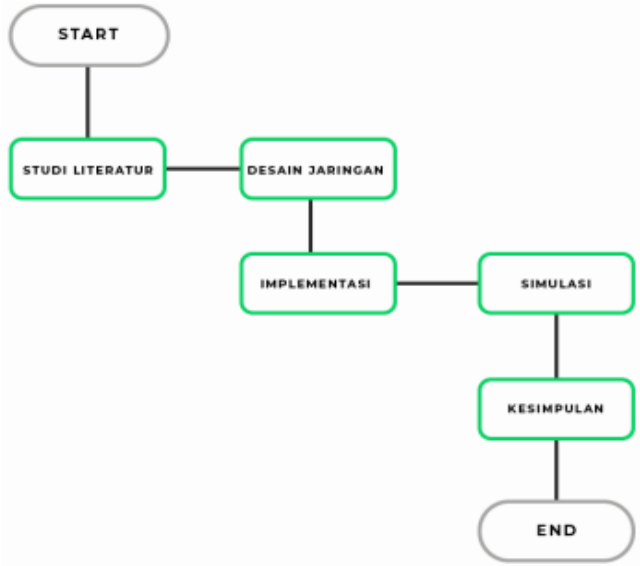
Keamanan jaringan komputer melibatkan empat aspek utama dalam menggambarkan bentuk ancaman keamanan jaringan. Keempat aspek tersebut adalah penyalahgunaan informasi Internet of Things (IoT) (Ramadhani et al., 2018), serangan penolakan layanan (ardiyansyah, M, 2023), kerusakan integritas lingkungan jaringan komputer (Putra et al., 2021), dan kebocoran informasi komputer.

Access Control List merupakan salah satu teknologi pengawasan paket yang umum digunakan dalam jaringan komputer (Chaidir & Wirawan, 2018). ACL digunakan untuk meninjau isi paket dan menerapkan aturan untuk menentukan apakah paket tersebut diizinkan atau ditolak. ACL umumnya berfokus pada penyaringan berdasarkan alamat IP sumber dan tujuan dalam header paket TCP/IP (Heryanto & Azizah, 2019).

METODE

1. Tahap Penelitian

Untuk mencapai tujuan pengembangan keamanan jaringan komputer, penelitian ini melibatkan beberapa tahapan yang terstruktur dan sistematis. Berikut adalah flowchart tahap penelitian:



Gambar 1 Tahap Penelitian

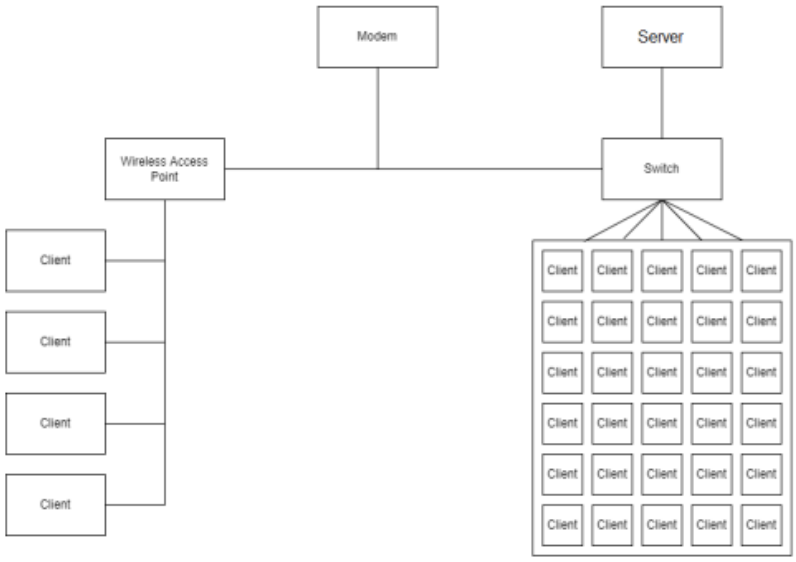
Penelitian ini menggunakan metode eksperimental. Metode eksperimental dalam konteks jaringan adalah pendekatan ilmiah yang digunakan untuk menguji hipotesis atau teori tertentu mengenai perilaku jaringan. Dengan melakukan eksperimen, kita dapat mengamati secara langsung bagaimana perubahan pada suatu variabel dalam jaringan mempengaruhi variabel lainnya. Untuk memulai formulasi hipotesis tentukan pertanyaan penelitian yang ingin dijawab. Buat hipotesis yang jelas dan spesifik tentang hubungan antara variabel-variabel yang akan diuji. seseorang harus membaca literatur untuk mempelajari ide-ide tentang ACL dan keamanan jaringan komputer. Setelah itu, desain eksperimen variabel bebas faktor yang sengaja diubah oleh peneliti untuk mengamati pengaruhnya. Contoh: bandwidth, protokol routing, jumlah perangkat. variabel terikat faktor yang diukur untuk melihat pengaruh perubahan variabel bebas. Contoh: latency, throughput, jitter. Grup Kontrol: Jaringan dalam kondisi normal yang digunakan sebagai pembanding. Grup Eksperimen: Jaringan dengan perubahan pada variabel bebas. desain jaringan yang melibatkan penerapan ACL sesuai dengan persyaratan keamanan dilakukan. Terakhir Pengumpulan Data: Alat Pengukuran: Gunakan alat seperti Wireshark, iperf, ping, dan SNMP untuk mengumpulkan data kinerja jaringan. Metrik Kinerja: Ukur metrik seperti latency, throughput, jitter, packet loss, dan CPU utilization. Simulasi: Jika eksperimen pada jaringan nyata tidak memungkinkan, gunakan simulator jaringan seperti NS-3 atau Mininet. implementasi ACL dilakukan dengan mengonfigurasi perangkat jaringan. Selanjutnya, simulasi dilakukan untuk menguji kemampuan ACL untuk mengontrol akses dan melindungi jaringan dari ancaman keamanan. Data dari simulasi dikumpulkan dan dianalisis untuk analisis kinerja ACL Statistik: Gunakan analisis statistik untuk menguji signifikansi perbedaan antara kelompok kontrol dan eksperimen. Visualisasi: Gunakan grafik dan diagram untuk menyajikan data secara visual dan memudahkan interpretasi.. Pada akhirnya, hasil penelitian digunakan untuk membuat saran tentang bagaimana ACL dapat digunakan dengan lebih baik jika diperlukan. Metode penelitian eksperimental ini memungkinkan untuk secara langsung mengidentifikasi tingkat keberhasilan ACL dalam meningkatkan keamanan jaringan komputer. penarikan kesimpulan: verifikasi hipotesis: terima atau tolak hipotesis berdasarkan hasil analisis data. interpretasi hasil: jelaskan implikasi dari hasil eksperimen terhadap kinerja jaringan.

2. Blog Diagram

Di dalam sistem jaringan komputer di SMKN 1 Blega, secara umum menggunakan jaringan client ke modem menggunakan koneksi kabel. Terdapat 1 unit modem yang berfungsi meneruskan jaringan ke internet.

Tabel 1 Perangkat Jaringan

No	Nama Perangkat	Jumlah	Fungsi
1	ISP (Internet Service Provider)	1	Sebagai pemberi layanan akses internet provider Skynet dengan kecepatan 10Mbps
2	Modem ADSL (Asychronus Digital Subscriber Line)	1	Sebagai penghubung ISP (Internet Service Provider) dengan perangkat Switch dan Access Point. Modem ADSL yang digunakan adalah jenis D-Link DSL-2640B yang memiliki 4 port ethernet
3	Switch	1	Sebagai penghubung antara modem ADSL dengan PC (Personal Computer) Admin dan Client yang terdapat di ruang lab komputer. Switch yang digunakan adalah TP-Link TLSG1024D yang memiliki 24 port ethernet
4	Server	1	Berfungsi sebagai database.
5	PC (Personal Computer) Admin	1	Berfungsi mengatur dan mengkonfigurasi lalu lintas jaringan di SMKN 1 Blega
6	Client Lab Komputer	29	Sebagai fasilitas perangkat pembelajaran siswa terhubung menggunakan transmisi kabel LAN.
7	Client Laptop Kepala sekolah, staf TU, staf administrasi, staf bendahara	4	Sebagai fasilitas perangkat komputer karyawan transmisi WLAN
8	Client Laptop Guru	Tidak tetap	Sebagai fasilitas perangkat komputer karyawan transmisi WLAN.
9	Kabel	Tidak tetap	Menggunakan jenis twisted pair yaitu UTP Cat 5e dan menggunakan RJ45 sebagai konektornya sedangkan kabel modem ADSL ke ISP adalah kabel telepon.



Gambar 2 Blok Diagram Jaringan SMKN 1 Blega

Sesuai Gambar 2 jaringan di SMKN 1 Blega yang digunakan dari Server-Switch, Modem-Switch, Switch-Client, Wireless Access Point-Client yang mengasumsikan bahwa topologi berpusat pada modem dan switch. Analisa topologi yang digunakan di SMKN 1 Blega adalah topologi star.

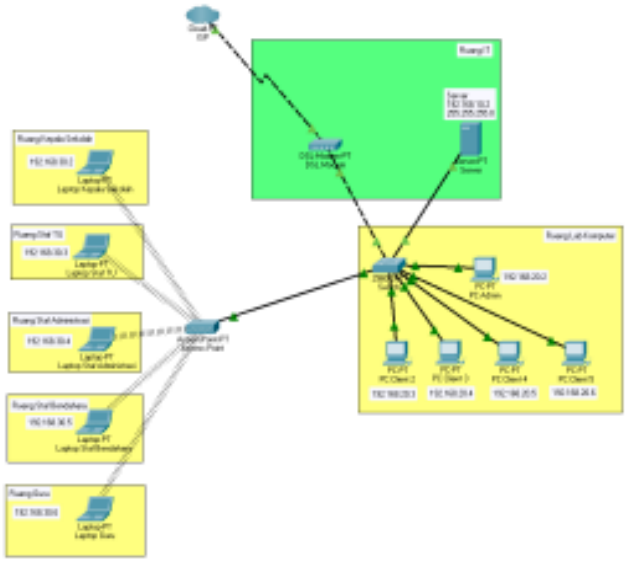
3. Rancangan Pengujian

Pengujian terdiri dari empat tahap: pengujian keamanan jaringan awal, pengujian implementasi keamanan langkah-langkah standar, pengujian keamanan jaringan WLAN, dan pengujian keamanan router internal. Tujuan dari pengujian keamanan jaringan awal adalah untuk menemukan celah keamanan pada jaringan dan menentukan perangkat mana yang dapat mengakses server dengan melakukan pengujian PING dari PC klien Lab Komputer ke server (192.168.10.2) dan mengantongi sertifikat.

Selanjutnya, pada pengujian implementasi langkah-langkah keamanan usulan, tujuannya adalah untuk memverifikasi keberhasilan implementasi langkah-langkah keamanan yang telah diusulkan untuk mengatasi celah keamanan yang ada. Pengujian ini melibatkan pengujian PING dari PC client Lab Komputer ke server setelah implementasi keamanan, pengujian PING dari PC Admin Lab Komputer ke server, dan pengujian PING dari PC client Lab Komputer ke router (192.168.20.1). Hasil yang diharapkan adalah akses dari PC client Lab Komputer ke server akan ditutup, sementara akses dari PC Admin Lab Komputer ke server dan akses internet dari PC client Lab Komputer tetap berfungsi setelah implementasi keamanan.

Pengujian keamanan jaringan WLAN juga bertujuan untuk menguji keamanan jaringan WLAN pada perangkat yang terhubung. Semua laptop (Kepala Sekolah, Staf TU, Bendahara, Staf Administrasi, dan Guru) diuji PING ke server 192.168.10.2. Hasil yang diharapkan adalah bahwa semua laptop, kecuali PC Admin Lab dan PC Client Lab, tidak dapat mengirimkan paket PING ke server. Ini menunjukkan bahwa akses ke laptop-laptop telah diblokir. koneksi ke server telah diblokir.

Terakhir, pengujian jaringan internal router dilakukan untuk memverifikasi koneksi antara perangkat pada masing-masing antarmuka router. Pengujian PING dilakukan ke router 192.168.20.1 di PC Admin Lab Komputer dan ke router 192.168.20.1 di PC client Lab Komputer. Hasilnya diharapkan menunjukkan koneksi antarmuka yang baik .



Gambar 3 Skema Jaringan

Di SMKN 1 Blega, jaringan bertopologi bintang terdiri dari jaringan Local Area Network (LAN) dan Wireless Local Area Network (WLAN). Pada jaringan LAN, ISP menyediakan akses internet melalui modem ADSL ke switch, yang kemudian melalui switch yang berbeda terhubung ke server dan PC Admin. Di Laboratorium Komputer, sakelar tambahan terhubung ke klien.

Jaringan nirkabel dan jaringan kabel berbeda dengan ID jaringan karena menggunakan kelas IP yang sama. Jaringan SMKN 1 Blega menggunakan alamat IP ini untuk memberikan pengalamatan unik kepada setiap klien yang terhubung.

4. Rencana Pengujian Sistem

Pengujian terdiri dari empat tahap: pengujian keamanan jaringan awal, pengujian implementasi keamanan langkah-langkah standar, pengujian keamanan jaringan WLAN, dan pengujian keamanan router internal. Tujuan

dari pengujian keamanan jaringan awal adalah untuk menemukan celah keamanan pada jaringan dan menentukan perangkat mana yang dapat mengakses server dengan melakukan pengujian PING dari PC klien Lab Komputer ke server (192.168.10.2) dan mengantongi sertifikat.

Selanjutnya, pada pengujian implementasi langkah-langkah keamanan usulan, tujuannya adalah untuk memverifikasi keberhasilan implementasi langkah-langkah keamanan yang telah diusulkan untuk mengatasi celah keamanan yang ada. Pengujian ini melibatkan pengujian PING dari PC client Lab Komputer ke server setelah implementasi keamanan, pengujian PING dari PC Admin Lab Komputer ke server, dan pengujian PING dari PC client Lab Komputer ke router (192.168.20.1). Hasil yang diharapkan adalah akses dari PC client Lab Komputer ke server akan ditutup, sementara akses dari PC Admin Lab Komputer ke server dan akses internet dari PC client Lab Komputer tetap berfungsi setelah implementasi keamanan.

Pengujian keamanan jaringan WLAN juga bertujuan untuk menguji keamanan jaringan WLAN pada perangkat yang terhubung. Semua laptop (Kepala Sekolah, Staf TU, Bendahara, Staf Administrasi, dan Guru) diuji PING ke server 192.168.10.2. Hasil yang diharapkan adalah bahwa semua laptop, kecuali PC Admin Lab dan PC Client Lab, tidak dapat mengirimkan paket PING ke server. Ini menunjukkan bahwa akses ke laptop-laptop telah diblokir. koneksi ke server telah diblokir.

Terakhir, pengujian jaringan internal router dilakukan untuk memverifikasi koneksi antara perangkat pada masing-masing antarmuka router. Pengujian PING dilakukan ke router 192.168.20.1 di PC Admin Lab Komputer dan ke router 192.168.20.1 di PC client Lab Komputer. Hasilnya diharapkan menunjukkan koneksi antarmuka yang baik

Pengujian terdiri dari empat tahap: pengujian keamanan jaringan awal, pengujian implementasi keamanan langkah-langkah standar, pengujian keamanan jaringan WLAN, dan pengujian keamanan router internal. Tujuan dari pengujian keamanan jaringan awal adalah untuk menemukan celah keamanan pada jaringan dan menentukan perangkat mana yang dapat mengakses server dengan melakukan pengujian PING dari PC klien Lab Komputer ke server (192.168.10.2) dan mengantongi sertifikat.

Selanjutnya, pada pengujian implementasi langkah-langkah keamanan usulan, tujuannya adalah untuk memverifikasi keberhasilan implementasi langkah-langkah keamanan yang telah diusulkan untuk mengatasi celah keamanan yang ada. Pengujian ini melibatkan pengujian PING dari PC client Lab Komputer ke server setelah implementasi keamanan, pengujian PING dari PC Admin Lab Komputer ke server, dan pengujian PING dari PC client Lab Komputer ke router (192.168.20.1). Hasil yang diharapkan adalah akses dari PC client Lab Komputer ke server akan ditutup, sementara akses dari PC Admin Lab Komputer ke server dan akses internet dari PC client Lab Komputer tetap berfungsi setelah implementasi keamanan.

Pengujian keamanan jaringan WLAN juga bertujuan untuk menguji keamanan jaringan WLAN pada perangkat yang terhubung. Semua laptop (Kepala Sekolah, Staf TU, Bendahara, Staf Administrasi, dan Guru) diuji PING ke server 192.168.10.2. Hasil yang diharapkan adalah bahwa semua laptop, kecuali PC Admin Lab dan PC Client Lab, tidak dapat mengirimkan paket PING ke server. Ini menunjukkan bahwa akses ke laptop-laptop telah diblokir. koneksi ke server telah diblokir.

Terakhir, pengujian jaringan internal router dilakukan untuk memverifikasi koneksi antara perangkat pada masing-masing antarmuka router. Pengujian PING dilakukan ke router 192.168.20.1 di PC Admin Lab Komputer dan ke router 192.168.20.1 di PC client Lab Komputer. Hasilnya diharapkan menunjukkan koneksi antarmuka yang baik .

HASIL

Konfigurasi jaringan pada Tabel 2 menunjukkan bahwa router memiliki empat antarmuka yang terhubung ke jaringan yang berbeda dengan alamat IP dan subnet mask yang sesuai. Server berada di jaringan 192.168.10.0/24 dengan alamat IP 192.168.10.2 dan gateway 192.168.10.1. PC Admin Lab Komputer berada di jaringan 192.168.20.0/24 dengan alamat IP 192.168.20.2 dan gateway 192.168.20.1. Sementara itu, PC Client Lab Komputer memiliki 29 antarmuka (Fa0/4 hingga Fa0/32) dengan alamat IP dari 192.168.20.3 hingga 192.168.20.32 dan gateway 192.168.20.1. Sedangkan Laptop Kepala Sekolah, Laptop Staf TU, Laptop Staf Bendahara, Laptop Staf Administrasi, dan Laptop Guru terhubung ke jaringan WLAN dengan subnet mask 255.255.255.0 dan gateway 192.168.30.1.

Tabel 2 Hasil Pengujian

No	Perangkat	Interface	IP Addres	Gateway	Hasil Pengujian	Keterangan
1	Router	Fa0/0	192.168.1.1	-	-	-
2		Fa1/0	192.168.10.1	-	-	-
3		Fa2/0	192.168.20.1	-	-	-
4		Fa3/0	192.168.30.1	-	-	-
5	Server	Fa0	192.168.10.2	192.168.10.1	PC Admin Lab	

					Komputer dapat mengirim paket PING ke Server	AdminServer (berhasil)
6	PC Admin Lab Komputer	Fa0/3 1	192.168.20.2	192.168.20.1	PC Admin Lab Komputer dapat mengirim paket PING ke Server	AdminServer (berhasil)
7	PC Client Lab Komputer	Fa0/4-32	192.168.20.3-32	192.168.20.1	PC client Lab Komputer tidak bisa mengirim paket PING ke Server	ClientServer (berhasil)
8	Laptop Kepala Sekolah	WLAN	192.168.30.2	192.168.30.1	PC client Lab Komputer tidak bisa mengirim paket PING ke Server	ClientServer (berhasil)
9	Laptop Staf TU	WLAN	192.168.30.3	192.168.30.1	PC client Lab Komputer tidak bisa mengirim paket PING ke Server	ClientServer (berhasil)

PEMBAHASAN

Hasil pengujian keamanan jaringan komputer di SMKN 1 Blega yang melibatkan penerapan Access Control List (ACL) telah menunjukkan hasil yang positif. Pengujian ini berfokus pada seberapa efektif langkah-langkah keamanan yang telah diambil, termasuk penerapan ACL, untuk meningkatkan keamanan sistem secara keseluruhan. Untuk mengidentifikasi perubahan keamanan setelah penerapan tindakan keamanan, pengujian melibatkan skenario akses LAN dan WLAN.

Hasil pengujian menunjukkan bahwa prosedur keamanan telah mencapai tujuannya. Sebelum penerapan ACL, PC klien Lab Komputer memiliki kemampuan untuk mengirim paket PING ke server, menunjukkan celah keamanan yang dapat membahayakan keamanan jaringan. Namun, setelah penerapan prosedur keamanan, akses PC klien Lab Komputer ke server berhasil dibatasi dengan sukses. Hasil ini menunjukkan bahwa ACL dapat mengontrol dan membatasi akses klien ke server dari LAN dan WLAN dengan baik , mengurangi kemungkinan akses yang tidak sah.

Selain itu, pengujian memastikan bahwa setelah penerapan prosedur keamanan, akses ke perangkat WLAN, termasuk laptop Kepala Sekolah, Staf TU, Bendahara, Staf Administrasi, dan Guru, telah berhasil dibatasi. Hanya komputer PC Admin Lab yang diizinkan untuk mengirim paket PING ke server.

Hasil dan analisis pengujian ini menunjukkan bahwa jaringan komputer di SMKN 1 Blega telah aman karena penerapan langkah-langkah keamanan seperti pengaturan ACL. Dengan sukses, celah keamanan yang sebelumnya memungkinkan akses ke server dari PC klien Lab Komputer dan perangkat WLAN telah ditutup. Hal ini menunjukkan bahwa strategi keamanan yang disarankan dapat menangani masalah keamanan di era digital yang semakin kompleks.

Disarankan untuk melakukan evaluasi rutin terhadap aturan ACL yang telah diterapkan dan pemantauan berkala terhadap keamanan jaringan untuk perbaikan tambahan. Untuk meningkatkan lapisan keamanan secara menyeluruh, Anda juga dapat mempertimbangkan untuk memasukkan fitur keamanan tambahan, seperti firewall dan IDS/IPS. Dengan menerapkan prosedur keamanan yang tepat dan melakukan perbaikan yang berkelanjutan, jaringan komputer di SMKN 1 Blega diharapkan dapat terlindungi dengan baik dari ancaman keamanan yang mungkin muncul di masa mendatang. Ini akan menjaga integritas dan kerahasiaan data.

.KESIMPULAN

SMKN 1 Blega memiliki jaringan yang lebih aman berkat penggunaan List Control Access (ACL). Pengujian menunjukkan bahwa ACL berhasil mengatasi celah keamanan dan membatasi akses tidak sah dari PC klien Lab ke server. ACL juga berhasil mencegah akses tidak sah dari perangkat WLAN ke server. Sistem ini melindungi jaringan lebih baik dari serangan cyber. Rekomendasi berfokus pada penerapan fitur keamanan tambahan serta pemantauan dan evaluasi aturan ACL rutin . Hasilnya sesuai dengan penelitian serupa dan memberikan bantuan positif untuk mengatasi tantangan keamanan di era teknologi yang kompleks.

REFERENSI

Ardiyansyah, M, A. M. (2023). Analisis struktur kovarians indikator terkait kesehatan pada lansia yang tinggal di rumah dengan fokus pada rasa kesehatan subjektif. Judul 8, 1–14.

Azmi, F., Kalsum, T. U., & Alamsyah, H. (2022). Analysis and Application of Access Control List (ACL) Methods on Computer Networks Analisa dan Penerapan Metode Access Control List (ACL) pada Jaringan Komputer. *Jurnal Komputer, Informasi Dan Teknologi*, *2*(1), 81–88.

Chaidir, I., & Wirawan, R. R. (2018). Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List. *Jurnal Teknik Komputer AMIK BSI (JTK)*, *4*(1), 212–216.

Chandra, J. C. (2022). Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur. *Jurnal TICOM: Technology of Information and Communication*, *10*(3), 2022.

Christanto, F. W., Nugroho, A., & Adhiwibowo, W. (2018). *Garuda799966*. *07*(September), 121–129.

Dasmen, R. N., & Rasmila. (2019). Rancang Bangun Vlan Pada Jaringan Komputer Rri Palembang Dengan Simulasi Cisco Packet Tracer. *Jurnal Teknologi*, *Vol. 11 No*(1), 47–56.

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology*, *20*(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Heryanto, D., & Azizah, S. (2019). *Application of Access Control List for*. 71–76.

Kamarudin, K., & Gazali, M. (2021). Sistem Keamanan Berlapis Menggunakan Metode Access Control List Dan Enkripsi Source Code Pada Web Login. *Jurnal Teknologi Informasi (JUTECH)*, *2*(2), 48–60. https://doi.org/10.32546/jutech.v2i2.1657

Krianto Sulaiman, O., & Saripurna, D. (2021). Network Security System Analysis Using Access Control List (ACL). *International Journal of Information System & Technology Akreditasi*, *5*(2), 192–197.

Kurniati, K., & Dasmen, R. N. (2019). The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *10*(1), 49. https://doi.org/10.24843/lkjiti.2019.v10.i01.p06

Agung A, Nur W, Rahmi N.S (2021). Analisis Efektifitas Open Shortest Path First (OSPF) Dengan dan Tanpa Menggunakan Acces Control List (ACL) (1), 83-88.

Laksono, A. T., & Nasution, M. A. H. (2020). Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 83. https://doi.org/10.30865/json.v1i2.1920

Putra, N. A., Riyanto, V., Wijaya, G., & Herlinawati, N. (2021). Firewall Design Using Access Control List Method As Data Filtering. *Jurnal Mantik*, *5*(3), 1684–1693.

Ramadhani, A. R., Bhawiyuga, A., & Siregar, R. A. (2018). *Implementasi Access Control List Berbasis Protokol MQTT pada Perangkat NodeMCU*. *2*(8), 2824–2831.