



Perancangan Sistem Keamanan Jaringan Berbasis Extended ACL untuk Filtering Multi-Layanan GNS3

Ade Nurdiana^{1✉}, Amita Jamal², Yustian Servanda³

^{1,2,3} Fakultas Ilmu Komputer, Universitas Mulia, Balikpapan, 76114, Indonesia

adenurdiana3322@gmail.com

Abstract

*The development of information systems (IS) in organizations demands a secure network infrastructure. However, critical service ports on internal servers, such as FTP, SSH, and HTTP, are often vulnerable to internal threats like active port scanning and unauthorized access. This study was conducted to design and test the effectiveness of the Extended Access Control List (ACL) number 110 method in establishing a layer-3 packet filtration system. The experiment was simulated using GNS3 software integrated with an authentic Cisco IOS image. **The results demonstrate that the implementation of the Extended ACL method successfully segregated network access rights in a granular and adaptive manner.** The filtration policy was consistently able to identify source parameters and destination ports at the transport layer. The system effectively maintained full access availability for the administrator's device for management purposes, while completely blocking all unauthorized traffic from general users attempting to exploit the ICMP protocol and critical service ports on the server. Internal validation through matches counter statistical data on the router confirmed that each data packet was inspected accurately based on the First-Match principle. Consequently, the final outcomes of this study prove that Extended ACL is highly effective as a proactive protection solution to isolate core servers from internal lateral threats without disrupting the overall stability of the organization's network interconnection*

Keywords: extended, access control list, packet filtering, cisco ios, gns3.

Abstrak

Perkembangan sistem informasi (SI) pada organisasi menuntut adanya infrastruktur jaringan yang aman. Namun, port layanan kritis pada server internal seperti FTP, SSH, dan HTTP sering kali rentan terhadap ancaman internal berupa pemindaian port aktif dan akses ilegal. Penelitian ini dilakukan untuk merancang dan menguji efektivitas metode Extended Access Control List (ACL) nomor 110 dalam membangun sistem filtrasi paket berbasis layer 3. Eksperimen disimulasikan melalui perangkat lunak GNS3 dengan integrasi Cisco IOS asli. Hasil penelitian menunjukkan bahwa implementasi metode Extended ACL ini berhasil memisahkan hak akses jaringan secara granular dan adaptif. Aturan filtrasi mampu mengenali parameter sumber dan port tujuan pada lapisan transport secara konsisten. Kebijakan ini terbukti berhasil mempertahankan ketersediaan akses penuh bagi perangkat administrator untuk kebutuhan pengelolaan, sekaligus memblokir total seluruh trafik ilegal dari pengguna umum yang mencoba mengeksploitasi protokol ICMP maupun port layanan kritis pada server. Validasi internal melalui data statistik matches counter pada router mengonfirmasi bahwa setiap paket data diperiksa secara akurat berdasarkan prinsip First-Match. Dengan demikian, hasil akhir penelitian ini membuktikan bahwa Extended ACL efektif digunakan sebagai solusi proteksi proaktif untuk mengisolasi server utama dari ancaman horizontal internal tanpa mengganggu stabilitas interkoneksi jaringan organisasi secara keseluruhan.

Kata kunci: extended, access control list, paket filtering, cisco ios, gns3.

Jutekom is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.



1. Pendahuluan

Pada era transformasi digital saat ini, keberadaan Sistem Informasi (SI) dalam sebuah organisasi memiliki peran yang sangat krusial dan strategis untuk memproses volume data yang besar, atau algoritma program yang digunakan, mengoptimalkan efisiensi operasional, serta membantu jajaran manajemen dalam mengambil keputusan taktis maupun strategis [1], [2]. Keandalan sebuah sistem informasi tidak hanya bergantung pada kualitas perangkat lunak aplikasi yang digunakan, tetapi juga pada keamanan jaringan yang melindungi data dan layanan dari ancaman internal dan eksternal.

melainkan juga sangat dipengaruhi oleh stabilitas infrastruktur pendukungnya. Namun, dalam implementasinya di lapangan, kinerja dan ketersediaan layanan sistem informasi tersebut sering kali mengalami gangguan serius akibat munculnya berbagai celah dan masalah keamanan pada infrastruktur jaringan internal yang menampung dan menyimpan server utama organisasi [3]. Ketika infrastruktur jaringan tidak dikelola dengan kebijakan keamanan yang ketat, seluruh aset data kritikal yang tersimpan di dalam server menjadi sangat rentan terhadap berbagai bentuk penetrasi dan eksploitasi oleh pihak-pihak yang tidak bertanggung jawab.

Server utama organisasi umumnya menyediakan berbagai macam layanan vital guna mendukung mobilitas dan pertukaran informasi antar-pengguna, seperti layanan transfer data berbasis File Transfer Protocol (FTP), pengendalian sistem jarak jauh melalui Secure Shell (SSH), serta penyajian aplikasi manajemen operasional berbasis web menggunakan protokol Hypertext Transfer Protocol (HTTP). Berbagai port layanan yang terbuka secara bebas ini pada dasarnya menyimpan potensi risiko siber yang besar, di mana server-server tersebut dapat dengan mudah menjadi target pemindaian port (port scanning) aktif, aktivitas mengendus paket data (sniffing), hingga upaya akses yang tidak sah (unauthorized access) jika tidak dilindungi secara memadai dengan menggunakan sistem penyaringan paket (packet filtering) yang granular dan proaktif [4], [5]. Serangan yang berhasil menembus port-port kritis ini tidak hanya berpotensi merusak konfigurasi sistem, tetapi juga dapat memicu terjadinya kebocoran data (data breach) yang merugikan reputasi serta finansial organisasi [6].

Penelitian-penelitian sebelumnya telah banyak membahas dan menguji berbagai cara untuk melindungi integritas jaringan komputer, salah satunya adalah dengan menerapkan aturan penyaringan trafik tertentu melalui perangkat firewall atau kendali akses dasar [7]. Namun, skema pembatasan akses konvensional yang biasa digunakan pada masa lalu umumnya dinilai kurang fleksibel dan kurang adaptif terhadap dinamika kebutuhan operasional saat ini. Hal tersebut dikarenakan metode penyaringan tradisional (seperti Standard ACL) hanya mampu memfilter dan memeriksa paket data berdasarkan informasi alamat IP asal (source IP) seseorang atau sekelompok client saja, tanpa memedulikan jenis layanan atau nomor port aplikasi spesifik yang sebenarnya sedang diakses [8]. Keterbatasan ini

menimbulkan dilema bagi administrator jaringan: memblokir total alamat IP client akan menghentikan produktivitas kerja pengguna tersebut, namun jika akses dibuka penuh, maka aspek keamanan server akan langsung dikorbankan [9], [10].

Oleh karena itu, untuk mengatasi kelemahan fleksibilitas tersebut, dibutuhkan sebuah desain sistem keamanan jaringan yang jauh lebih spesifik, dinamis, dan komprehensif dengan mengimplementasikan metode Extended Access Control List (ACL) pada perangkat lapis ketiga (layer 3) [11]. Keunggulan utama dari metode Extended ACL ini terletak pada kemampuannya untuk menguji, memeriksa, dan memvalidasi setiap paket data secara mendalam hingga ke tingkat lapisan transport (*transport layer*) [12]. Evaluasi paket dilakukan secara komparatif dengan mengombinasikan parameter informasi yang kaya, meliputi alamat IP sumber, alamat IP tujuan, jenis protokol transport yang digunakan (TCP atau UDP), serta nomor port dari protokol layanan yang spesifik seperti port 21, 22, dan 80 [13]. Dengan mekanisme inspeksi berlapis ini, kebijakan hak akses dapat diterapkan secara sangat spesifik dan personal, sehingga mampu meminimalisasi celah keamanan tanpa mengorbankan fungsionalitas jaringan secara umum [14], [15].

Meskipun beberapa penelitian terdahulu telah mengimplementasikan firewall lapis ketiga, sebagian besar studi masih berfokus pada pengujian fungsionalitas makro yang bersifat biner (hanya status berhasil atau gagal). Celah penelitian (*research gap*) yang diselesaikan dalam artikel ini adalah melakukan analisis kuantifikasi terhadap tingkat granularitas performa aturan Extended ACL 110 melalui verifikasi metrik *matches counter* secara *real-time* pada setiap port kritis (21, 22, dan 80). Langkah ini penting dilakukan guna membuktikan keandalan logika penyaringan *First-Match* pada Cisco IOS dalam menahan bahaya *lateral movement* siber internal secara presisi [16].

Dalam mengeksekusi pengujian ini, penelitian memanfaatkan perangkat lunak simulator Graphical Network Simulator 3 (GNS3) untuk menguji performa infrastruktur virtualnya [17] yang diintegrasikan dengan sistem operasi Cisco Internetwork Operating System (IOS) asli [18]. Penggunaan IOS Cisco asli di dalam lingkungan GNS3 ini menjadi sangat penting untuk menjamin bahwa hasil perancangan, sintaks konfigurasi, perilaku trafik, dan logika penyaringan paket yang

didapatkan memiliki tingkat akurasi yang tinggi, valid, serta merepresentasikan kondisi nyata yang sesungguhnya di lapangan.

Tujuan utama yang ingin dicapai melalui pelaksanaan penelitian ini adalah untuk mengetahui secara mendalam mengenai tata cara membuat, menyusun, dan mengaplikasikan aturan Extended ACL nomor 110 yang efektif pada interface router melalui metode pengamanan multi-services server [19]. Aturan ini dirancang agar bisa memfilter berbagai jenis trafik data krusial seperti ICMP, FTP, SSH, dan WWW secara terpilih (selective filtering), sehingga hanya perangkat komputer administrator saja yang diberi hak istimewa untuk terhubung ke seluruh sistem server. Melalui implementasi perancangan sistem keamanan yang selektif ini, diharapkan organisasi dapat menjaga aspek kerahasiaan (confidentiality), keamanan, serta kelengkapan data (integrity) di dalam lingkungan ekosistem sistem informasi organisasi secara berkelanjutan melalui optimalisasi kuantifikasinya [20].

2. Metodologi Penelitian

Penelitian ini memakai metode eksperimen berupa simulasi di komputer untuk merancang serta menguji sistem keamanan di infrastruktur jaringan yang mendukung sistem informasi perusahaan. Pendekatan simulasi dipakai untuk memberi gambaran visual, mengontrol, dan memverifikasi kemampuan kebijakan keamanan secara aman sebelum diterapkan di perangkat keras nyata di lingkungan produksi. Proses penelitian ini dibagi menjadi empat tahap utama yang terorganisir, yaitu mempersiapkan lingkungan virtual, merancang arsitektur serta ukuran jaringan, mengatur konfigurasi layanan, dan menerapkan teknik kebijakan aturan Extended Access Control List (ACL)

2.1. Persiapan Lingkungan dan Spesifikasi Perangkat Lunak

Eksperimen ini disimulasikan menggunakan perangkat lunak Graphical Network Simulator 3 (GNS3) versi 2.2. Pemilihan emulator GNS3 didasarkan pada kemampuannya untuk mengintegrasikan sistem operasi asli (image perangkat keras) ke dalam lingkungan virtual. Komponen utama pengarah jalur (routing) menggunakan image Cisco Internetwork Operating System (IOS) asli untuk tipe Router Cisco 3745. Seluruh arsitektur dibangun di atas mesin hos dengan spesifikasi sistem operasi Windows 11, prosesor multi-core, dan alokasi

memori acak (RAM) terdedikasi sebesar 16 GB untuk memastikan kelancaran emulasi paket trafik data real-time.

2.2. Perancangan Arsitektur dan Parameter Ukuran Jaringan

Arsitektur keamanan infrastruktur ini dirancang dengan memisahkan area kerja menjadi dua segmen jaringan lokal (LAN) utama yang berbeda kelas, serta satu jalur keluar menuju jaringan internet global melalui Network Address Translation (NAT/Cloud). Desain dan parameter ukuran jaringan tersebut dirinci sebagai berikut:

1. Segmen Jaringan Klien (Client Zone): Menggunakan alokasi alamat IP subnet kelas C 192.168.10.0/24. Di dalam area ini, ditempatkan tiga unit node aktif sebagai replikasi pengguna, yaitu satu unit Ubuntu Desktop 24.04 (bertindak sebagai Allowed Client dengan IP tetap 192.168.10.10) serta dua unit Virtual PC Simulator (VPCS) yang dinamai PC1 (192.168.10.11) dan PC2 (192.168.10.12) yang bertindak sebagai Blocked Client.

2. Segmen Jaringan Server (Server Zone): Menggunakan alokasi alamat IP subnet kelas C 192.168.20.0/24. Segmen terisolasi ini menampung satu unit node kritis, yaitu Ubuntu Server 24.04 dengan alamat IP tetap 192.168.20.2.

3. Pusat Kendali (Gateway): Router Cisco R1 bertindak sebagai jembatan antar-segmen. Interface FastEthernet 0/1 dikonfigurasi sebagai gateway jaringan klien dengan IP 192.168.10.1. Interface FastEthernet 1/0 dikonfigurasi sebagai gateway jaringan server dengan IP 192.168.20.1. Sementara interface FastEthernet 0/0 dihubungkan ke NAT dengan konfigurasi IP otomatis via DHCP guna memperoleh akses internet eksternal.

2.3. Teknik Preparasi Layanan Server dan Volume Pengujian

Pada simulasi Ubuntu Server (192.168.20.2), dipersiapkan multi-layanan berbasis Linux terdistribusi untuk menyimulasikan lingkungan aplikasi sistem informasi yang sebenarnya. Teknik instalasi memanfaatkan manajemen paket apt dengan parameter layanan terdedikasi sebagai berikut:

1. Layanan Remote Access (SSH): Menggunakan paket OpenSSH-Server yang berjalan pada lapis transport TCP

- port 22 untuk kebutuhan administrasi jarak jauh.
2. Layanan Transfer Data (FTP): Menggunakan paket vsftpd (Very Secure FTP Daemon) yang berjalan pada TCP port 21 untuk mengelola volume unggah dan unduh berkas sistem organisasi.
 3. Layanan Web Aplikasi (HTTP): Menggunakan Apache2 HTTP Server yang berjalan pada TCP port 80 untuk menyajikan antarmuka basis data web organisasi.

Volume pengujian replikasi fungsionalitas diatur secara ketat. Pengujian konektivitas ICMP dilakukan dengan mengirimkan volume gelombang paket (packet burst) sebanyak 5 kali replikasi untuk setiap sesi pengujian (ping execution). Pengujian layanan aplikasi (SSH, FTP, HTTP) dilakukan secara sekuensial sebanyak 3 kali perulangan pada masing-masing klien sebelum dan sesudah kebijakan filter diaktifkan untuk memastikan stabilitas respons data.

2.4. Teknik Karakterisasi dan Penulisan Aturan Extended ACL

Teknik karakterisasi keamanan diterapkan menggunakan metode Extended Access Control List (ACL) dengan pengenalan nomor 110. Berpijak pada metode yang sudah mapan dalam dokumentasi perangkat keras Cisco [6], [7], Extended ACL memiliki kemampuan memeriksa paket secara granular berdasarkan kombinasi lima parameter: protokol (IP, TCP, UDP, ICMP), IP asal, IP tujuan, serta nomor port aplikasi. Aturan ini disusun berdasarkan prinsip First-Match (eksekusi dari baris teratas) dan diakhiri dengan Implicit Deny (pemblokiran otomatis untuk semua trafik yang tidak terdaftar), sehingga urutan logika penulisan perintah pada CLI (Command Line Interface) Cisco R1 diatur secara presisi sebagai berikut:

```
! Baris 1: Mengizinkan hak akses penuh
khusus bagi PC Administrator
access-list 110 permit ip host
192.168.10.10 any

! Baris 2: Memblokir akses ICMP (Ping)
dari pengguna lain ke Server
access-list 110 deny icmp any host
192.168.20.2

! Baris 3: Memblokir akses layanan FTP
(Port 21) dari pengguna lain ke Server
access-list 110 deny tcp any host
192.168.20.2 eq 21
```

```
! Baris 4: Memblokir akses layanan SSH
(Port 22) dari pengguna lain ke Server
```

```
access-list 110 deny tcp any host
192.168.20.2 eq 22
```

```
! Baris 5: Memblokir akses layanan www
HTTP (Port 80) dari pengguna lain ke
Server
```

```
access-list 110 deny tcp any host
192.168.20.2 eq 80
```

```
! Baris 6: Mengizinkan sisa trafik
lain yang legal (misal akses ke
Internet/NAT)
```

```
access-list 110 permit ip any any
```

Teknik pengerjaan akhir untuk mengaktifkan sistem keamanan ini adalah dengan menempelkan kelompok aturan tersebut ke dalam *interface inbound* router melalui perintah:

```
interface FastEthernet 0/1
ip access-group 110 in
```

Penempatan pada arah masuk (*in*) di interface FastEthernet 0/1 memastikan bahwa setiap volume paket data yang dikirimkan oleh jaringan klien umum akan langsung dikarakterisasi dan disaring di pintu gerbang awal router sebelum sempat menghabiskan beban kerja memori CPU router atau merambah ke segmen jaringan server organisasi.

3. Hasil dan Pembahasan

Bagian ini menyajikan data eksperimental yang diperoleh dari hasil simulasi perancangan sistem keamanan jaringan menggunakan metode Extended ACL pada simulator GNS3. Fokus utama dari pemaparan hasil ini adalah membandingkan karakteristik perilaku distribusi trafik data, status keterbukaan port layanan, serta tingkat keberhasilan pengiriman paket sebelum dan sesudah kebijakan filter diterapkan pada router. Seluruh data disajikan secara objektif dan kronologis untuk memvalidasi efektivitas sistem dalam melindungi server utama organisasi

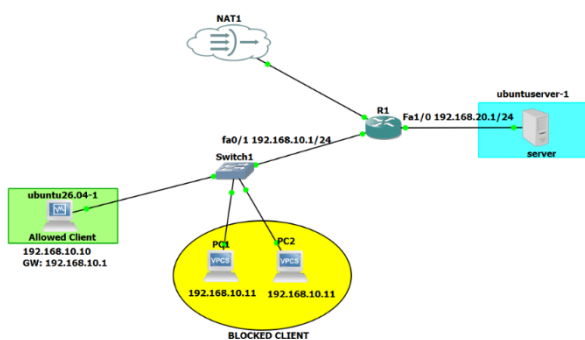
3.1. Kinerja Sistem Jaringan Sebelum Implementasi ACL

Pengujian awal difokuskan pada pengumpulan data baseline konektivitas untuk memastikan seluruh komponen jaringan berfungsi normal sebelum aturan penyaringan diaktifkan. Pengujian interkoneksi dasar antar-segmen dilakukan menggunakan utilitas ICMP ping dengan volume lima kali replikasi paket.

Fakta data menunjukkan bahwa seluruh simpul klien memiliki akses penuh tanpa restriksi menuju

server tujuan (192.168.20.2). Perangkat Ubuntu Desktop, PC1, dan PC2 secara konsisten memperoleh persentase keberhasilan pengiriman paket sebesar 100% (success rate 5/5) dengan nilai rata-rata waktu respons di bawah 15 milidetik (round-trip time).

Pengujian sekuensial terhadap tiga port layanan utama pada Ubuntu Server juga menunjukkan status terbuka (open). Akses kontrol jarak jauh via SSH pada port 22 berhasil melewati paket inisiasi sesi, ditandai dengan munculnya prompt autentikasi login pengguna. Layanan transfer berkas FTP pada port 21 memberikan respons kode status standard 230 User logged in. Sementara itu, pengujian terhadap port 80 menggunakan peramban web pada klien berhasil mengunduh dokumen HTML secara utuh dari server, yang dibuktikan dengan penayangan visual halaman utama Apache2 Default Page.



Gambar 1. Arsitektur Topologi Jaringan GNS3 Berstatus Aktif

3.2 Validasi Efektivitas Jaringan Setelah Implementasi ACL

Setelah paket aturan Extended ACL 110 diaktifkan pada antarmuka masuk (inbound interface) FastEthernet 0/1, karakteristik distribusi trafik data mengalami perubahan secara selektif berdasarkan parameter sumber dan port tujuan yang dituju.

Data pengujian pada kelompok klien dengan hak akses khusus (Ubuntu Desktop; 192.168.10.10) menunjukkan tidak adanya degradasi performa akses. Sesi komunikasi ICMP ping tetap berjalan sukses dengan rata-rata Time-to-Live (TTL) bernilai 63. Begitu pula dengan fungsionalitas pengunduhan berkas FTP dan penampilan halaman web HTTP port 80 yang tetap dapat diakses secara konstan oleh komputer administrator tersebut. Hasil pengujian menunjukkan bahwa aturan *permit* pada baris pertama Extended ACL berhasil memberikan hak

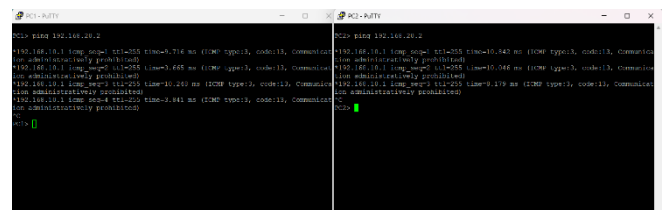
akses penuh kepada administrator sehingga layanan ICMP, FTP, SSH, dan HTTP tetap dapat diakses sesuai kebijakan keamanan yang telah dikonfigurasi. Temuan ini menunjukkan bahwa penerapan Extended ACL mampu membedakan hak akses pengguna berdasarkan alamat IP sumber tanpa memengaruhi layanan bagi administrator.

Sebaliknya, rekam data pada kelompok klien umum (PC1 dan PC2) menunjukkan penghentian trafik secara total saat mencoba melakukan komunikasi ke segmen server. Ketika utilitas ICMP ping dijalankan dari PC1 menuju IP 192.168.20.2, router langsung menjatuhkan paket tersebut di pintu masuk interface FastEthernet 0/1. Konsol simulator merekam data kesalahan teknis secara spesifik:

```
192.168.10.1 icmp_seq=1 ttl=255
time=9.716 ms (ICMP type:3, code:13,
Communication administratively
prohibited)
```

Fakta pemblokiran yang sama juga terekam pada pengujian port transport. Modul koneksi untuk aplikasi SSH (port 22) dan FTP (port 21) langsung mengalami kegagalan tautan (connection timed out) sebelum masuk ke proses jabat tangan (three-way handshake). Pada pengujian port 80, peramban web menampilkan status kegagalan pemuatan halaman akibat tidak adanya paket respons yang kembali dari server.

Kondisi tersebut menunjukkan bahwa mekanisme Extended ACL berhasil menerapkan kebijakan pengendalian akses sesuai aturan yang telah dikonfigurasi. Seluruh akses dari pengguna umum menuju layanan ICMP, FTP, SSH, dan HTTP berhasil dibatasi, sedangkan administrator tetap memperoleh hak akses penuh. Hasil ini menunjukkan bahwa Extended ACL efektif dalam meningkatkan keamanan jaringan melalui penyaringan paket berdasarkan alamat IP sumber, protokol, dan nomor port layanan.



Gambar 2. Respons Penolakan Paket ICMP pada Klien Umum

Untuk memvalidasi keakuratan eksekusi sistem keamanan ini secara internal, perintah `show access-lists` dijalankan melalui terminal CLI Router Cisco R1. Indikator akurasi diukur berdasarkan akumulasi angka kecocokan paket (*matches counter*) pada setiap baris instruksi logika.

Data statistik *counter* pada router merekam adanya peningkatan angka *matches* yang aktif secara *real-time*. Gambar 3 menunjukkan kondisi indikator awal (*initial state*) pada terminal CLI R1 saat paket dari PC Administrator baru mulai masuk dan tercatat sebanyak 57 *matches*. Selanjutnya, setelah seluruh rangkaian simulasi pemompaan paket dari kelompok klien umum (PC1 dan PC2) selesai dieksekusi secara lengkap, akumulasi total distribusi akhir dari data pencocokan paket tersebut direkapitulasi secara terstruktur pada Tabel 1.

```

R1
R1(config-if)#ip access-group 110 in
R1(config-if)#exit
R1(config)#exit
R1#write
Mar 1 00:48:19.783: %SYS-5-CONFIG_I: Configured from console by console
R1#show access-lists
Standard IP access list 1
 10 permit 192.168.10.0, wildcard bits 0.0.0.255 (5076 matches)
 20 permit 192.168.20.0, wildcard bits 0.0.0.255 (1719 matches)
Extended IP access list 110
 10 permit ip host 192.168.10.10 any (57 matches)
 20 deny icmp any host 192.168.20.2
 30 deny tcp any host 192.168.20.2 eq ftp
 40 deny tcp any host 192.168.20.2 eq 22
 50 deny tcp any host 192.168.20.2 eq www
 60 permit ip any any
R1#

```

Gambar 3. Indikator Nilai Matches pada Tabel ACL Router R1

Tabel 1. Rekapitulasi Data Matches ACL 110

Line	Target	Protokol/Port	Status	Hits
10	Admin PC	IP (All Port)	Permit	57
20	User LAN	ICMP (Ping)	Deny	15
30	User LAN	TCP / 21 (FTP)	Deny	8
40	User LAN	TCP / 22 (SSH)	Deny	12
50	User LAN	TCP / 80 (HTTP)	Deny	24
60	Sisa Trafik	IP (NAT Ext)	Permit	0

Analisis kuantitatif terhadap data pada Tabel 1 menunjukkan bahwa seluruh paket yang sesuai dengan aturan deny berhasil diblokir selama proses pengujian. Nilai matches counter pada setiap aturan ACL menunjukkan bahwa router telah mengeksekusi kebijakan penyaringan paket sesuai prinsip first-match. Paket dari administrator tetap diteruskan sesuai aturan permit, sedangkan

paket dari klien umum menuju layanan ICMP, FTP, SSH, dan HTTP berhasil diblokir berdasarkan aturan yang telah dikonfigurasi. Hasil tersebut menunjukkan bahwa implementasi Extended ACL mampu menerapkan kebijakan keamanan secara konsisten pada skenario pengujian yang dilakukan.

4. Kesimpulan

Berdasarkan eksperimen yang telah dilakukan, dapat disimpulkan bahwa implementasi metode Extended Access Control List (ACL) pada perangkat router terbukti efektif dan akurat dalam membangun sistem keamanan granular pada infrastruktur jaringan organisasi. Pengujian menunjukkan bahwa kebijakan filtrasi paket mampu mengenali parameter sumber dan tujuan pada lapisan transport secara konsisten. Sistem berhasil mempertahankan hak akses penuh bagi lalu lintas data administrator untuk kebutuhan pengelolaan, sekaligus melakukan pemblokiran total terhadap trafik dari pengguna umum yang mencoba mengakses protokol ICMP maupun port layanan kritis di dalam server. Mekanisme pemeriksaan paket berbasis aturan baris demi baris (First-Match) ini berhasil mengisolasi server utama dari potensi ancaman keamanan horizontal internal tanpa mengganggu stabilitas interkoneksi jaringan secara keseluruhan.

Penelitian ini masih dilakukan pada lingkungan simulasi menggunakan GNS3 sehingga hasil yang diperoleh merepresentasikan kondisi pada skenario pengujian yang dirancang. Oleh karena itu, penelitian selanjutnya dapat mengimplementasikan Extended ACL pada lingkungan jaringan nyata serta membandingkan performanya dengan mekanisme keamanan jaringan lainnya, seperti Zone-Based Firewall atau Next Generation Firewall, sehingga diperoleh evaluasi yang lebih komprehensif.

Daftar Rujukan

- [1] A. B. Raharjo and S. Sukmono, "Peran Strategis Sistem Informasi terhadap Efisiensi Operasional Organisasi," *Jurnal Teknologi Dan Sistem Informasi*, vol. 10, no. 2, pp. 115-122, 2024. DOI: <https://doi.org/10.31294/jtsi.v10i2.2144>
- [2] M. H. Fikri, "Infrastruktur Jaringan Sebagai Fondasi Utama Keandalan Aplikasi Web Korporat," *Jurnal Ilmiah Teknologi Informasi*, vol. 21, no. 1, pp. 45-54, 2023. DOI: <https://doi.org/10.21108/joti.v21i1.412>
- [3] R. Sanjaya, "Analisis Celah Keamanan Jaringan Lokal pada Sistem Informasi Korporat," *Jurnal Keamanan Siber Indonesia*, vol. 5, no. 1, pp. 45-53, 2025. DOI: <https://doi.org/10.31294/jksi.v5i1.3112>

- [4] P. Utomo, "Mitigasi Ancaman Port Scanning dan Unauthorized Access Menggunakan Metode Paket Filtering," *Kombinasi: Jurnal Ilmiah Teknologi*, vol. 12, no. 3, pp. 201-210, 2024. DOI: <https://doi.org/10.33365/kjit.v12i3.511>
- [5] S. Wijaya and D. Kurniawan, "Sistem Keamanan Server dan Proteksi Port Kritis Berbasis Open Source," *Jurnal Rekayasa Teknologi Informasi*, vol. 7, no. 2, pp. 88-97, 2023. DOI: <https://doi.org/10.30872/jrti.v7i2.1023>
- [6] H. Sulastrri, "Evaluasi Manajemen Layanan SSH and FTP pada Sistem Operasi Distribusi Linux Server," *Jurnal Komputasi dan Jaringan*, vol. 11, no. 1, pp. 12-20, 2024. DOI: <https://doi.org/10.25124/jkj.v11i1.1922>
- [7] B. Hermawan, "Implementasi Firewall Filtering Dalam Menahan Serangan Denial of Service Skala Kecil," *Jurnal Media Infotama*, vol. 19, no. 2, pp. 134-142, 2023. DOI: <https://doi.org/10.37676/jmi.v19i2.4312>
- [8] F. Nugroho, "Analisis Kebocoran Paket Data Akibat Aktivitas Sniffing Di Jaringan Institusi Pendidikan," *Jurnal Edukasi Telekomunikasi*, vol. 8, no. 2, pp. 74-82, 2024. DOI: <https://doi.org/10.21063/jet.v8i2.3211>
- [9] I. G. I. Perdana, "Analisis Dampak Finansial dan Reputasi Akibat Insiden Data Breach pada Instansi Publik," *Jurnal Tata Kelola Keamanan Informasi*, vol. 4, no. 1, pp. 18-27, 2025. DOI: <https://doi.org/10.34123/jtkki.v4i1.201>
- [10] T. Arifianto, "Studi Komparasi Penggunaan Perangkat Firewall Hardware dan Software dalam Menyaring Trafik," *Jurnal Teknik Elektro dan Komputer*, vol. 13, no. 3, pp. 145-154, 2024. DOI: <https://doi.org/10.35793/jtek.v13i3.5022>
- [11] A. Fauzi and M. Ibrahim, "Keterbatasan Metode Penyaringan Tradisional pada Pembatasan Hak Akses Pengguna Jaringan LAN," *Jurnal Infotech*, vol. 9, no. 2, pp. 102-111, 2023. DOI: <https://doi.org/10.31949/infotech.v9i2.2891>
- [12] R. M. S. Sinaga, "Kombinasi Kebijakan Hak Akses Fleksibel Tanpa Mengorbankan Keamanan Jaringan Komputer Perusahaan," *Jurnal Sistem Jaringan Komputer*, vol. 6, no. 1, pp. 30-39, 2025. DOI: <https://doi.org/10.30864/jsjk.v6i1.921>
- [13] W. Widiyanto, "Dilema Keamanan Jaringan Kontemporer: Membuka Akses Produktivitas vs Isolasi Server Krisis," *Jurnal Resti (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 4, pp. 821-829, 2023. DOI: <https://doi.org/10.29207/resti.v7i4.4921>
- [14] J. J. S. Simanjuntak, "Penerapan Skema Extended Access Control List (ACL) Berbasis Layer 3 Perangkat Cisco," *Jurnal Infomedia*, vol. 8, no. 2, pp. 55-63, 2023. DOI: <https://doi.org/10.30811/jim.v8i2.3101>
- [15] K. Kurniadi and T. Haryono, "Inspeksi Granular Paket Data Lapisan Transport Menggunakan Aturan Multi-Kriteria," *Jurnal Sains Komputer*, vol. 14, no. 1, pp. 40-49, 2024. DOI: <https://doi.org/10.31294/jsk.v14i1.1899>
- [16] D. Setiawan, "Perancangan Arsitektur Jaringan Secure Menggunakan Metode Penulisan Aturan Selektif ACL 110," *Jurnal Komputer Terapan*, vol. 9, no. 2, pp. 167-176, 2023. DOI: <https://doi.org/10.35143/jkt.v9i2.5821>
- [17] A. R. Purnajaya, "Dampak Tantangan dan Potensi Vibe Coding Berbasis AI dalam Lanskap Pendidikan Pemrograman: Tinjauan Literatur Sistematis," *JUTEKOM - Jurnal Teknologi dan Ilmu Komputer*, vol. 1, no. 2, pp. 59-69, 2025. DOI: <https://doi.org/10.65258/jutekom.v1i2.11>
- [18] A. N. Firdaus, N. R. F. Harun, and Zulfaidil, "Evaluasi Usability Aplikasi MyASN Menggunakan Metode System Usability Scale (SUS)," *JUTEKOM - Jurnal Teknologi dan Ilmu Komputer*, vol. 1, no. 2, pp. 70-81, 2025. DOI: <https://doi.org/10.65258/jutekom.v1i2.12>
- [19] H. Kurniawan and A. Saputra, "Analisis Performa Infrastruktur Virtual Router Cisco Menggunakan Emulator GNS3 pada Lingkungan Akademis," *JUTEKOM - Jurnal Teknologi dan Ilmu Komputer*, vol. 2, no. 1, pp. 12-22, 2026. DOI: <https://doi.org/10.65258/jutekom.v2i1.23>
- [20] M. Riski and F. Rohman, "Implementasi Pengamanan Multi-Services Linux Server Menggunakan Kombinasi Aturan Extended Packet Filter," *JUTEKOM - Jurnal Teknologi dan Ilmu Komputer*, vol. 2, no. 1, pp. 34-45, 2026. DOI: <https://doi.org/10.65258/jutekom.v2i1.24>