EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

MUHAMMAD MUJAHIDDIN RAIS

22.83.0809

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

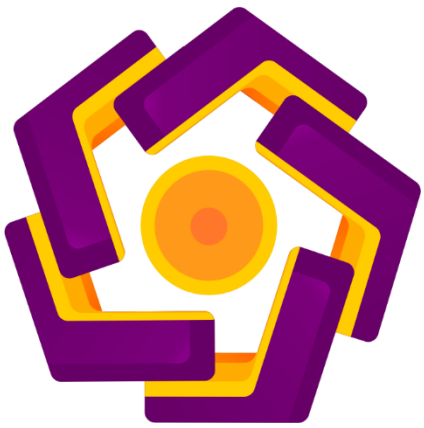
2026

EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

MUHAMMAD MUJAHIDDIN RAIS

22.83.0809

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER

yang disusun dan diajukan oleh

Muhammad Mujahiddin Rais

22.83.0809

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 9 Januari 2026

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER

yang disusun dan diajukan oleh

Muhammad Mujahiddin Rais

22.83.0809

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Januari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Lukman, S.Kom., M.Kom **NIK. 190302151**	
Eko Pramono, S.Si, M.T **NIK. 190302580**	
Melwin Syafrizal, S.Kom., M.Eng., Ph.D **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Januari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Mujahiddin Rais
NIM : 22.83.0809

Menyatakan bahwa Skripsi dengan judul berikut:

EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER

Dosen Pembimbing : Melwin Syafrizal, S.Kom., M.Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 26 Januari 2026

Yang Menyatakan,

Muhammad Mujahiddin Rais

HALAMAN PERSEMBAHAN

Dengan rasa syukur ke hadirat Allah SWT, skripsi ini saya persembahkan kepada:

1. Bapak Hendro Gunawan dan Ibu Sutami, yang selalu menjadi sumber doa, semangat, dan kekuatan dalam setiap langkah hidup saya.
2. Keluarga besar yang senantiasa memberikan dukungan, kasih sayang, dan motivasi yang tiada henti.
3. Dosen pembimbing bapak Melwin Syafrizal, S.Kom., M.Eng., Ph.D. atas ilmu dan bimbingan selama masa studi.
4. Rekan-rekan seperjuangan, khususnya anak KATSU FC dan Novus Mundus, atas kebersamaan, semangat, dan dukungan selama proses penyusunan skripsi ini.
5. Seseorang yang penulis sayangi (23.82.1750), yang telah memberikan dukungan, motivasi, serta semangat selama proses penyusunan skripsi ini.

Semoga karya ini menjadi bentuk dedikasi dan wujud terima kasih saya kepada semua pihak yang telah mendukung

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT karena atas limpahan rahmat, karunia, dan hidayah-Nya, penulis dapat menyelesaikan skripsi yang berjudul "EVALUASI PENERAPAN STANDART & EXTENDED ACCESS CONTROL LIST (ACL) SEBAGAI LAPISAN KEAMANAN JARINGAN MENGGUNAKAN CISCO PACKET TRACER" dengan baik dan lancar.

Penyusunan skripsi ini tidak lepas dari dukungan, bimbingan, dan bantuan dari berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak **Prof. Dr. M. Suyanto, M.M.,** selaku Rektor Universitas AMIKOM Yogyakarta yang telah memberikan fasilitas dan suasana akademik yang kondusif.
2. Ibu **Prof. Dr. Kusrini, M.Kom**. selaku Dekan Fakultas Ilmu Komputer yang telah memberikan dukungan penuh dalam proses penyelesaian skripsi ini.
3. Bapak **Dony Arius, S.T., M.Eng**., selaku Ketua Program Studi Teknik Komputer Universitas AMIKOM Yogyakarta yang telah memberikan arah dan motivasi selama studi.
4. Bapak **Melwin Syafrizal, S.Kom., M.Eng., Ph.D.** selaku Dosen Pembimbing yang telah memberikan bimbingan, arahan, dan motivasi dengan sabar serta penuh perhatian selama proses penyusunan skripsi ini.
5. Tim Dosen Penguji yang telah memberikan kritik dan saran membangun untuk kesempurnaan karya tulis ini.
6. Seluruh dosen dan staf pengajar Program Studi Teknik Komputer yang telah memberikan ilmu dan pengalaman selama masa studi.
7. Bapak Hendro Gunawan dan Ibu Sutami yang selalu menjadi sumber kekuatan, inspirasi, dan doa yang tak terhingga.

8. Rekan-rekan seperjuangan, khususnya teman-teman anak Kobas, atas semangat, dukungan, dan kebersamaan yang berarti sepanjang proses penyusunan tugas akhir ini.
9. Seseorang yang penulis sayangi (23.82.1750), yang telah memberikan dukungan, motivasi, serta semangat selama proses penyusunan skripsi ini.
10. Semua pihak yang tidak dapat disebutkan satu per satu, namun telah memberikan dukungan dalam bentuk apa pun.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, saya mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang.

Yogyakarta, 28 Januari 2026
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Keamanan jaringan tradisional yang mengandalkan perlindungan perimeter cenderung menerapkan kepercayaan implisit (*implicit trust*) terhadap lalu lintas internal, sehingga rentan terhadap serangan yang berhasil menembus pertahanan awal dan bergerak secara lateral di dalam jaringan. Penelitian ini bertujuan untuk menganalisis penerapan arsitektur keamanan *Zero Trust Architecture* (ZTA) menggunakan *Extended Access Control List* (ACL) sebagai mekanisme *Policy Enforcement Point* (PEP) pada simulator Cisco Packet Tracer. Prinsip *Zero Trust* yang diterapkan meliputi *micro-segmentation*, *verify explicitly*, dan *least privilege* untuk membatasi akses antar zona jaringan, yaitu Marketing, Finance, dan Server.

Metode penelitian dilakukan melalui simulasi dan pengujian tiga skenario jaringan, yaitu jaringan tanpa ACL (*baseline*), jaringan dengan *Standard* ACL, dan jaringan dengan *Extended* ACL. Evaluasi difokuskan pada efektivitas mekanisme kontrol akses dalam membatasi akses tidak sah dan mencegah pergerakan lateral antar VLAN. Hasil pengujian menunjukkan bahwa *Extended* ACL mampu menerapkan kontrol akses secara granular dengan memblokir 100% akses ilegal berbasis protokol ICMP (Ping) serta hanya mengizinkan layanan HTTP sesuai kebijakan yang ditetapkan.

Selain peningkatan keamanan, penerapan *Extended* ACL juga memberikan dampak terhadap kinerja jaringan berupa peningkatan latensi pemrosesan dan penurunan kapasitas lalu lintas data. Meskipun terjadi penurunan performa akibat proses inspeksi paket, nilai keterlambatan yang dihasilkan masih berada dalam batas toleransi jaringan lokal. Dengan demikian, penelitian ini menyimpulkan bahwa *Extended* ACL efektif digunakan untuk merealisasikan prinsip *Zero Trust Architecture* dan meningkatkan keamanan internal jaringan tanpa mengorbankan ketersediaan layanan secara signifikan.

Kata kunci: *Zero Trust Architecture*, *Access control List* (ACL), Keamanan Jaringan, *Micro-segmentation*, Cisco Packet Tracer.

ABSTRACT

Traditional network security that relies on perimeter-based protection often applies implicit trust to internal traffic, making it vulnerable to attacks that successfully bypass initial defenses and move laterally within the network. This study aims to analyze the implementation of Zero Trust Architecture (ZTA) using Extended Access Control List (ACL) as a Policy Enforcement Point (PEP) in a Cisco Packet Tracer simulation environment. The applied Zero Trust principles include micro-segmentation, verify explicitly, and least privilege to restrict access between network zones, namely Marketing, Finance, and Server.

The research method is conducted through simulation and testing of three network scenarios: a network without ACL (baseline), a network using Standard ACL, and a network using Extended ACL. The evaluation focuses on the effectiveness of access control mechanisms in preventing unauthorized access and lateral movement across VLANs. The results indicate that Extended ACL successfully enforces granular access control by blocking 100% of unauthorized ICMP (Ping) traffic while explicitly allowing HTTP services according to predefined policies.

In addition to improving network security, the implementation of Extended ACL introduces additional processing overhead that affects network performance. However, the resulting latency remains within acceptable limits for local area networks. Therefore, this study concludes that Extended ACL is an effective mechanism for implementing Zero Trust Architecture and enhancing internal network security without significantly degrading service availability.

Keyword: *Zero Trust Architecture, Access control List (*ACL*), Network Security, Micro-segmentation, Cisco Packet Tracer.*