BAB I

PENDAHULUAN

1.1 Latar Belakang

Dinamika keamanan siber saat ini telah mengalami pergeseran paradigma yang signifikan, di mana pemanfaatan teknologi informasi yang terbuka justru memicu peningkatan risiko kejahatan siber (*cybercrime*) [1]. Ancaman terbesar dalam infrastruktur jaringan modern tidak lagi hanya berasal dari serangan eksternal yang menembus perimeter, melainkan dari pergerakan ancaman di dalam jaringan itu sendiri (*lateral movement*) setelah pertahanan awal ditembus. Literatur menegaskan bahwa mekanisme keamanan konvensional yang hanya mengandalkan perlindungan perimeter sudah tidak memadai; fokus keamanan harus beralih pada upaya memproteksi dan mengontrol lalu lintas (*traffic*) internal secara ketat untuk membatasi ruang gerak serangan [2].

Namun, implementasi keamanan internal pada banyak infrastruktur jaringan masih menghadapi kendala teknis yang mendasar. Mayoritas jaringan masih bergantung pada mekanisme *Standard Access control List* (*Standard* ACL) yang sering dikombinasikan dengan VLAN untuk memisahkan departemen [5]. Meskipun umum digunakan, *Standard* ACL memiliki kelemahan fatal karena hanya mampu memfilter paket berdasarkan alamat IP sumber (*Source IP address*) tanpa melihat protokol atau tujuan spesifik [6]. Akibatnya, mekanisme ini gagal menerapkan prinsip keamanan *Granular*, sehingga jika satu segmen jaringan terinfeksi, ancaman dapat dengan mudah menyebar ke segmen lain tanpa hambatan berarti karena kurangnya filter yang spesifik.

Tuntutan keamanan modern kini mengarah pada penerapan *Zero Trust Architecture* (ZTA) dengan prinsip "*never trust, always verify*" [9]. Implementasi ZTA menuntut penerapan *Micro-segmentation* untuk mengisolasi ancaman [10]. Sayangnya, terdapat kesenjangan penelitian (*research gap*) yang nyata dalam literatur saat ini Sebagian besar penelitian sebelumnya belum melakukan perbandingan efektivitas keamanan antara *Standard* ACL dan *Extended* ACL

dalam konteks *micro-segmentation* berbasis *Zero Trust*. Mayoritas studi hanya membahas ZTA pada tataran konsep teoritis atau menggunakan solusi perangkat lunak canggih yang mahal, tanpa menyentuh aspek implementasi manual pada router standar yang hemat biaya [12].

Oleh karena itu, penelitian ini hadir untuk menjawab urgensi tersebut dengan mengevaluasi efektivitas *Extended* ACL sebagai mekanisme *Policy Enforcement Point* (PEP) dalam arsitektur *Zero Trust*. Penelitian ini bertujuan membuktikan bahwa perangkat router standar mampu mencegah serangan pergerakan lateral secara efektif melalui konfigurasi yang tepat [7].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana perbandingan efektivitas keamanan antara *Standard* ACL dan *Extended* ACL dalam menerapkan prinsip *micro-segmentation* untuk mencegah serangan pergerakan lateral (*lateral movement*) pada jaringan VLAN?
2. Bagaimana efektivitas *Extended* ACL dalam menerapkan kebijakan *default deny* dan *least privilege* sebagai implementasi *Zero Trust Architecture* pada jaringan VLAN?

1.3 Batasan Masalah

Agar penelitian ini lebih terfokus dan terukur, maka pembatasan masalah yang diterapkan adalah sebagai berikut:

1. Penelitian dilakukan dalam bentuk simulasi menggunakan aplikasi Cisco Packet Tracer dan tidak melibatkan pengujian pada perangkat keras jaringan fisik.
2. Jenis *Access control List* yang dianalisis dibatasi pada *Standard* ACL dan *Extended* ACL saja; tipe ACL lain (mis. *dynamic* ACL, *named* ACL) tidak dibahas.

3. Pengujian keamanan difokuskan pada kemampuan ACL dalam mencegah akses tidak sah antar subnet dan kontrol terhadap trafik dasar (mis. ICMP dan HTTP).
4. Skenario pengujian meliputi tiga kondisi: tanpa ACL (*baseline*), dengan *Standard* ACL, dan dengan *Extended* ACL; variasi kombinasi lain atau integrasi dengan solusi keamanan tambahan (mis. *firewall*, IDS/IPS, NGFW) tidak diuji.
5. Konfigurasi ACL yang diterapkan pada simulasi tidak hanya bersifat fungsional, tetapi disusun secara spesifik mengikuti prinsip ZTA, yaitu menerapkan kebijakan *Default Deny* (menolak semua akses secara *default*) dan *Least Privilege* (hanya mengizinkan akses yang mutlak diperlukan) untuk merealisasikan *micro-segmentation*.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menganalisis dan membuktikan perbedaan tingkat keamanan antara *Standard* ACL dan *Extended* ACL dalam membatasi akses ilegal serta efektivitasnya dalam mendukung arsitektur *Zero Trust* pada level segmen jaringan.
2. Mengevaluasi keberhasilan penerapan kebijakan *default deny* dan *least privilege* menggunakan *Extended* ACL dalam membatasi akses antar segmen jaringan.

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis (Kontribusi Akademik)

1. Validasi Empiris Model *Zero Trust* pada Infrastruktur Konvensional Penelitian ini memberikan kontribusi pada literatur keamanan jaringan dengan membuktikan bahwa prinsip arsitektur modern *Zero Trust* (khususnya *micro-segmentation*) tidak selalu memerlukan perangkat keras *Next-Generation Firewall* (NGFW) yang mahal. Hasil penelitian ini

memvalidasi bahwa perangkat router standar dengan fitur *Extended* ACL dapat difungsikan secara efektif sebagai *Policy Enforcement Point* (PEP) sesuai standar NIST SP 800-207.

2. Analisis Efektivitas Kebijakan Keamanan Penelitian ini memberikan kontribusi berupa analisis empiris terhadap efektivitas kebijakan keamanan berbasis Zero Trust pada infrastruktur jaringan konvensional, khususnya dalam membatasi pergerakan lateral dan akses tidak sah antar segmen jaringan.

1.5.2 Manfaat Praktis (Nilai Tambah Implementasi)

1. Solusi *Zero Trust* Hemat Biaya (*Low-Cost Implementation*) Bagi institusi pendidikan (kampus) atau perusahaan menengah-kecil (UMKM) yang memiliki keterbatasan anggaran, penelitian ini menawarkan kerangka kerja (*framework*) keamanan yang efisien. Administrator jaringan dapat mengamankan aset kritis dari serangan pergerakan lateral (*lateral movement*) dengan memaksimalkan utilitas perangkat yang sudah ada (*existing hardware*) tanpa perlu pengadaan lisensi perangkat lunak keamanan tambahan.
2. Panduan Mitigasi Pergerakan Lateral Hasil rancangan ACL dalam penelitian ini memberikan cetak biru (*blueprint*) teknis bagi administrator jaringan untuk menerapkan kebijakan *default-Deny*. Hal ini memberikan nilai tambah berupa peningkatan resiliensi jaringan: jika satu departemen (VLAN) terinfeksi *ransomware* atau malware, konfigurasi ini menjamin ancaman tersebut terisolasi dan tidak menyebar ke server utama atau departemen lain.

1.6 Sistematika Penulisan

BAB I: PENDAHULUAN Berisi latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, serta sistematika penulisan.

BAB II: TINJAUAN PUSTAKA Membahas teori dasar keamanan jaringan, jenis dan konfigurasi ACL (*Standard* dan Extended), prinsip *Zero Trust* Network Access (ZTNA), serta hasil penelitian terdahulu yang relevan.

BAB III: METODOLOGI PENELITIAN Menjelaskan rancangan penelitian, variabel yang diuji, alat dan bahan yang digunakan (Cisco Packet Tracer), topologi jaringan, langkah simulasi, serta metode pengujian efektivitas kebijakan keamanan berbasis Zero Trust.

BAB IV: HASIL DAN PEMBAHASAN Menyajikan hasil simulasi penerapan Standard dan Extended ACL, analisis perbandingan efektivitas keamanan, serta evaluasi keberhasilan penerapan kebijakan default deny dan least privilege dalam mencegah pergerakan lateral antar segmen jaringan.

BAB V: PENUTUP Berisi kesimpulan dari seluruh hasil penelitian serta saran untuk penelitian selanjutnya.