BAB I

PENDAHULUAN

1.1 Latar Belakang

Digitalisasi dalam dunia pendidikan tidak sekadar mengubah medium belajar dari kertas ke layar, tetapi juga merombak total tata kelola administrasi dan interaksi di sekolah [1]. Institusi pendidikan kini dituntut untuk menjadikan internet sebagai infrastruktur utama guna membuka akses informasi yang inklusif sekaligus menciptakan ruang kelas yang interaktif. Namun, ketergantungan pada koneksi global ini membawa paradoks; di satu sisi internet memperluas cakrawala akademis, di sisi lain ia menyediakan distraksi tanpa batas yang sulit dikendalikan [2].

Tantangan paling nyata yang muncul di ruang kelas saat ini adalah fenomena *cyberslacking*—sebuah perilaku di mana siswa memanfaatkan fasilitas internet sekolah untuk kepentingan non-akademik di tengah jam Pelajaran [3]. Di lingkungan sekolah yang memiliki laboratorium komputer atau akses Wi-Fi terbuka, gejala ini makin mengkhawatirkan. Alih-alih fokus pada materi, siswa sering kali hanyut dalam media sosial, *streaming* video, hingga gim daring. Dampaknya tidak hanya berhenti pada merosotnya konsentrasi dan efisiensi belajar mandiri, melainkan juga memicu degradasi performa jaringan lokal akibat lonjakan lalu lintas data (*traffic*) yang dihabiskan untuk aktivitas non-produktif [4].

Kondisi ini tercermin jelas di Kabupaten Gorontalo, di mana pemerintah dan pihak sekolah telah berupaya memenuhi kebutuhan digital dengan menyediakan fasilitas internet. Di SMP Negeri 1 Tibawa, misalnya, akses internet sudah tersedia di area krusial seperti laboratorium komputer demi menyokong kegiatan belajar-mengajar. Sayangnya, ketersediaan fasilitas ini belum diimbangi dengan sistem pengawasan dan pembatasan yang ketat. Berdasarkan observasi awal di sekolah tersebut, tidak adanya proteksi atau filter membuat siswa bebas berselancar ke situs-situs hiburan saat guru sedang mengajar. Jika dibiarkan, habitasi *cyberslacking* ini akan terus mengikis produktivitas belajar siswa dan menciptakan iklim kelas yang tidak

kondusif. Oleh sebab itu, urgensi penerapan sistem kendali akses yang taktis menjadi hal yang mendesak.

Beberapa pendekatan teknis sebenarnya telah jamak diuji untuk meredam isu ini. Filter berbasis Layer 7 (*Application Layer*) mampu mengenali aplikasi secara spesifik, namun kompensasinya adalah beban komputasi perangkat yang melonjak drastis, terutama pada jaringan padat pengguna [5]. Metode *Deep Packet Inspection* (DPI) menawarkan analisis paket data yang lebih mendalam, tetapi kerap kali lumpuh saat berhadapan dengan enkripsi HTTPS, belum lagi adanya resistensi terkait isu privasi pengguna [6]. Sementara itu, benteng konvensional seperti *proxy server* dan *firewall* juga memiliki celah; siswa yang memiliki literasi digital lebih tinggi dengan mudah mengelabuinya lewat pemakaian VPN atau manipulasi DNS terenkripsi seperti *DNS over HTTPS* (DoH) [7].

Ketika metode-metode yang kompleks tersebut membentur dinding keterbatasan sumber daya perangkat, *DNS Filtering* hadir sebagai alternatif yang jauh lebih ringkas namun tetap bertenaga. Dengan memotong jalur resolusi domain ke alamat IP, situs-situs non-produktif dapat langsung diblokir di hulu sebelum sempat dimuat. Karena tidak memerlukan inspeksi isi paket data secara mendalam, beban komputasi metode ini sangat rendah sehingga ideal untuk diimplementasikan pada infrastruktur sekolah yang rata-rata memiliki spesifikasi perangkat terbatas [8].

Efektivitas *DNS Filtering* dalam menekan akses konten negatif juga telah divalidasi oleh berbagai praktik di lapangan. Sebagai contoh, integrasi *DNS Filtering* dengan sistem *firewall* berbasis Pi-hole di IDN Boarding School terbukti mampu menyaring lebih dari 95% situs pornografi tanpa mengorbankan akses siswa terhadap referensi ilmiah yang valid [9]. Fleksibilitas konfigurasi dan efisiensi sumber daya inilah yang menempatkan *DNS Filtering* sebagai opsi paling rasional untuk mengendalikan aktivitas siber di ekosistem pendidikan saat ini [10].

Pada ekosistem perangkat MikroTik, taktik ini dapat dieksekusi secara instan memanfaatkan fitur *Static DNS*. Administrator jaringan cukup memetakan domain target ke IP fiktif atau mengarahkannya ke halaman peringatan (*landing page*) lokal. Selain murah dan minim konfigurasi, sistem kendali terpusat ini bekerja mandiri tanpa perlu menyentuh atau menginstal

aplikasi apa pun di perangkat milik siswa. Berangkat dari potensi tersebut, penelitian ini dilakukan dengan judul **"Analisis Efektivitas DNS Filtering terhadap Pengendalian Cyberslacking"** untuk menguji dan mengukur sejauh mana metode ini mampu menekan aktivitas non-produktif di jaringan sekolah melalui pendekatan eksperimen berbasis simulasi.

1.2 Identifikasi Masalah

1. Penggunaan internet yang tidak terkendali di laboratorium komputer memungkinkan siswa mengakses situs non-produktif seperti media sosial, streaming, dan game online saat belajar.
2. Praktik cyberslacking dapat mengganggu pembelajaran, menurunkan konsentrasi, dan mengurangi efektivitas jaringan. Oleh karena itu, dibutuhkan metode pengendalian akses yang efektif, salah satunya DNS Filtering.

1.3 Rumusan Masalah

1. Bagaimana mengetahui efektivitas penerapan DNS Filtering menggunakan perangkat MikroTik dalam membatasi akses ke situs non-produktif pada jaringan pendidikan?
2. Bagaimana mengukur keberhasilan pemblokiran situs non-produktif oleh DNS Filtering sebelum dan sesudah penerapan konfigurasi?

1.4 Batasan Masalah

1. Penelitian ini hanya fokus pada penerapan DNS Filtering untuk memblokir situs non-produktif pada jaringan lokal sekolah.
2. Penelitian ini tidak membahas dan menambahkan metode pemblokiran lain selain DNS Filtering.
3. Pengujian efektivitas sistem difokuskan pada kondisi normal sebagai indikator keberhasilan utama, sedangkan pengujian dengan VPN dan Secure DNS dilakukan untuk menilai batas sistem terhadap upaya bypass

dan digunakan sebagai informasi pendukung serta pelengkap analisis dalam mengidentifikasi kelemahan dan keterbatasan pada kondisi nyata, tanpa menjadi tolok ukur utama efektivitas sistem.

1.5 Tujuan Penelitian

1. Untuk mengetahui efektivitas penerapan DNS Filtering menggunakan perangkat MikroTik dalam membatasi akses ke situs non-produktif pada jaringan pendidikan.
2. Untuk mengukur keberhasilan pemblokiran situs non-produktif oleh DNS Filtering sebelum dan sesudah penerapan konfigurasi.

1.6 Manfaat Penelitian

1. **Bagi Peneliti**

   Mengasah kemampuan teknis dalam penerapan DNS Filtering secara sistematis penelitian ini memungkinkan peneliti untuk menguji secara langsung konfigurasi MikroTik dalam menangani cyberslacking, serta mempelajari metrik efektivitas seperti tingkat pemblokiran dan frekuensi akses, yang akan memperdalam pemahaman dan keahlian tentang keamanan jaringan dan kontrol akses internet.
2. **Bagi Pembaca**

   Menyediakan referensi praktis mengenai efektivitas DNS Filtering dalam pengendalian akses internet – sehingga pembaca yang mengelola jaringan pendidikan bisa memahami mekanisme, keuntungan, dan batasan dari pendekatan ini untuk diterapkan di jaringan mereka.
3. **Bagi Institusi**

   Memberikan dasar kebijakan berbasis bukti untuk mengatur penggunaan internet di lingkungan pendidikan – temuan mengenai efektivitas DNS Filtering membantu institusi merancang regulasi dan pengaturan teknis yang mendukung fokus belajar dan keamanan jaringan, sekaligus menekan potensi cyberslacking peserta didik.