

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong institusi pendidikan tinggi untuk memanfaatkan jaringan internet secara maksimal dalam mendukung proses akademik, administratif, dan komunikasi. Universitas Bina Darma sebagai salah satu perguruan tinggi swasta terkemuka di Palembang telah menyediakan infrastruktur jaringan *internet* yang cukup memadai untuk menunjang kebutuhan tersebut. Sistem *e-learning*, akses jurnal ilmiah, serta aplikasi penunjang perkuliahan lainnya menjadi bagian dari aktivitas harian sivitas akademika.

Namun, meningkatnya jumlah perangkat yang terhubung ke jaringan dan tingginya intensitas akses terhadap situs-situs berbasis SSL (*Secure Socket Layer*) menyebabkan kebutuhan akan *bandwidth* semakin besar. Situs seperti siska.binadarma.ac.id, sisfo.binadarma.ac.id, elearning2.binadarma.ac.id, mbkm.binadarma.ac.id, perpustakaan.binadarma.ac.id, serta platform akademik berbasis HTTPS menjadi kebutuhan utama mahasiswa dan dosen dalam menunjang kegiatan belajar mengajar.

Salah satu pendekatan yang dapat digunakan untuk mengoptimalkan penggunaan *bandwidth* adalah dengan menerapkan teknologi *proxy server caching SSL (Secure Socket Layer)*. *Caching* merupakan metode penyimpanan sementara terhadap konten yang sering diakses, sehingga ketika konten tersebut dibutuhkan kembali, sistem tidak perlu mengunduh ulang dari sumber asal, melainkan dapat menyediakannya langsung dari *cache* lokal

Penelitian ini secara khusus bertujuan untuk menganalisis performa kelima layanan web akademik tersebut sebelum dan sesudah penerapan *caching* SSL (*Secure Socket Layer*) pada *proxy server*. Analisis dilakukan dengan mengukur parameter *response time*, *throughput*, dan penghematan *bandwidth*, sehingga dapat diketahui sejauh mana *caching* SSL (*Secure Socket Layer*) mampu meningkatkan performa layanan



1.2 Rumusan Masalah

Penelitian ini menyoroti kinerja jaringan sebelum dan sesudah dilakukan *caching*, khususnya dalam aspek efisiensi *bandwidth* dan waktu akses terhadap lima layanan web akademik yang sering diakses oleh pengguna Kampus, yaitu *siska.binadarma.ac.id*, *sisfo.binadarma.ac.id*, *elearning2.binadarma.ac.id*, *mbkm.binadarma.ac.id*, dan *perpustakaan.binadarma.ac.id*. Untuk mencapai tujuan tersebut, dilakukan proses pengujian dan perbandingan performa dengan mengukur parameter yang relevan sehingga dapat diketahui sejauh mana peningkatan performa yang dihasilkan dari penerapan sistem *caching* SSL (*Secure Socket Layer*) pada *proxy server*.

1.3 Batasan Masalah

Batasan masalah berikut ditetapkan agar penelitian ini lebih fokus dan tidak menyimpang dari tujuan utamanya:

1. Penelitian dilakukan pada jaringan kampus Universitas Bina Darma di ruangan BR2-203.
2. Aspek keamanan jaringan yang berkaitan dengan privasi pengguna tidak menjadi fokus utama penelitian ini
3. Pengujian hanya dilakukan pada lima layanan web akademik Universitas Bina Darma.
4. Penelitian hanya membahas konfigurasi dan analisis kinerja *caching* SSL dengan *Wireshark*, dan tidak membahas kinerja dalam skala jaringan besar secara real-time dan masif

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis performa lima layanan web akademik Universitas Bina Darma sebelum dan sesudah penerapan caching SSL (*Secure Socket Layer*) pada *proxy server*. Melalui proses konfigurasi dan pengujian pada situs Siska, Sisfo, Elearning2, MBKM, dan Perpustakaan, penelitian ini bertujuan untuk mengukur perubahan waktu respon, kecepatan akses, dan efisiensi penggunaan *bandwidth* setelah penerapan *caching* SSL. Selain itu, penelitian ini juga bertujuan untuk melakukan monitoring dan analisis lalu lintas jaringan menggunakan *Wireshark* guna memperoleh data yang akurat, sehingga dapat memberikan gambaran nyata mengenai efektivitas *caching* SSL (*Secure Socket Layer*) sebagai solusi peningkatan kinerja akses layanan *web* akademik.

1.4.2 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Untuk kampus: Meningkatkan layanan internet untuk mahasiswa, dosen dan karyawan.
2. Bagi Pengguna Jaringan: Memungkinkan akses yang lebih cepat ke situs yang sering digunakan untuk mendukung pekerjaan akademik dan administratif.
3. Bagi Pengelola Jaringan: Memberikan referensi untuk pengelolaan
4. Untuk Peneliti Selanjutnya: Menjadi referensi dan sumber evaluasi dalam mengembangkan penelitian lanjutan tentang caching, proxy server, dan keamanan jaringan.

1.4.3 Penelitian Terdahulu

Sebagai Dasar Refrensi,dalam penelitian yang dilakukan dalam penulis sangat perlu mencamtumkan hasil penelitian terlebih dahulu yang dapat digunakan sebagai salah satu data pendukung untuk penelitian ini:

Table 1.1. Penelitian Terdahulu

Nama Peneliti	Judul penelitian	Hasil Penelitian
(Utomo & Rokhmah, 2022)	<i>Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta</i>	Penerapan SSL pada web server program studi Teknik Informatika UMS berhasil meningkatkan keamanan dengan mencegah serangan sniffing. Sebelum diterapkan SSL, data yang dikirim dapat dengan mudah dimonitor oleh pihak tidak berwenang, namun setelah SSL diterapkan, informasi menjadi terenkripsi dan tidak dapat diakses oleh pengguna yang tidak memiliki otorisasi
(Dharmawanet al., 2022)	<i>Analisis Keamanan Jaringan Universitas Kristen Duta Wacana Dengan Serangan SSL/TLS</i>	Analisis keamanan jaringan menunjukkan bahwa masih terdapat beberapa potensi kerentanan seperti serangan LUCKY13 pada situs web yang diuji. Pembaruan sistem keamanan dan penerapan kebijakan HSTS Preload diperlukan untuk memastikan keamanan komunikasi data melalui protokol SSL/TLS

(Haeruddin & Vincent, 2021)	<i>Analisa dan Perancangan Proxy Server dan Catching SSL menggunakan Squid</i>	Implementasi proxy server caching SSL menggunakan Squid berhasil meningkatkan efisiensi akses internet dengan mengurangi waktu respons hingga rata-rata 56,45%. Penggunaan caching memungkinkan penghematan bandwidth yang signifikan serta mempercepat waktu akses ke situs web yang sering dikunjungi
(Wireshark et al., 2023)	<i>Penggunaan Wireshark Dan Nessus Untuk Analisis SSL/TLS Pada Keamanan Data Penggunaan Website</i>	Hasil pemindaian keamanan menunjukkan bahwa implementasi TLS 1.2 pada web server telah meningkatkan perlindungan data pengguna dengan mengenkripsi pertukaran data menggunakan algoritma hash SHA256. Namun, masih ditemukan tingkat kerentanan menengah yang perlu ditindaklanjuti untuk mengurangi potensi risiko Keamanan