Model Pengelolaan Akses Web  
dengan *Transparent Web Proxy*  
di Politeknik Negeri Bandung

**Proposal Tugas Akhir**

Proposal ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan Diploma Empat Program Studi Teknik Informatika di  
Jurusan Teknik Komputer dan Informatika

**Oleh:**

**Muhammad Saiful Islam**

**NIM: 141524020**



**Politeknik Negeri Bandung**

**2018**

Model Pengelolaan Akses Web  
dengan *Transparent Web Proxy*  
di Politeknik Negeri Bandung

**Proposal Tugas Akhir**

Oleh:

**Muhammad Saiful Islam**

**NIM: 141524020**

Menyetujui,  
Tim Pembimbing

Bandung, 30 April 2018

|  |  |
| --- | --- |
| Pembimbing I,  Yudi Widhiyasana, S.Si., M.T.  NIP 197407182001121002 | Pembimbing II,  Setiadi Rachmat, B.Eng., M.Eng.  NIP 196904041998031001 |

# ABSTRAK

Penggunaan web sebagai salah satu aplikasi jaringan Internet semakin intens digunakan dalam kehidupan sehari-hari, dan termasuk menjadi alat bantu pembelajaran yang penting di Politeknik Negeri Bandung. Karena penggunaannya yang semakin penting, maka akses web perlu dikelola. PSI sebagai pengelola akses web di Politeknik Negeri Bandung kemudian menggunakan *explicit web proxy* untuk melakukan pengelolaan akses web. Namun, seiring berkembangnya teknologi akses web, terutama protokol HTTPS, penggunaan *explicit web proxy* menghadirkan beberapa masalah, yaitu peningkatan jumlah konfigurasi yang perlu dilakukan pengguna ketika berpindah jaringan (dari luar ke dalam kampus dan sebaliknya) serta beberapa aplikasi yang tidak *proxy-aware* dan tidak dapat digunakan di jaringan Politeknik Negeri Bandung. Tugas akhir ini kemudian akan meneliti model pengelolaan akses web dengan *transparent web proxy*. *Transparent web proxy* ini akan memanfaatkan SNI sebagai media identifikasi protokol HTTPS. Dengan model baru ini, diharapkan kemampuan pengelolaan PSI tidak berkurang, namun dapat menyelesaikan masalah-masalah yang ada.

**Kata Kunci:** HTTP, HTTPS, SNI, *web proxy*, pengelolaan akses web.

# *ABSTRACT*

*World wide web as one of Internet application is being used more intensive. It also played an important role in learning activities in Politeknik Negeri Bandung. High usage of web made its usage important to be managed. Thus, PSI as the administrator of web access in Politeknik Negeri Bandung use explicit web proxy to manage the web access. But as web technologies developed, especially HTTPS, explicit web proxy usage got several problems: increase in amount of configuration that users should do when switching network between campus network and off-campus network, and several non-proxy aware applications that cannot be used in Politeknik Negeri Bandung network. This work will research web access management model using transparent web proxy that will use SNI to identify HTTPS usage. With this new model, existing management capability of PSI should not be decreased, but the stated problems should be solved.*

***Keywords:*** *HTTP, HTTPS, SNI, web proxy, web access management.*

# DAFTAR ISI

[HALAMAN PERSETUJUAN ii](#_Toc512833241)

[ABSTRAK iii](#_Toc512833242)

[*ABSTRACT* iv](#_Toc512833243)

[DAFTAR ISI v](#_Toc512833244)

[DAFTAR GAMBAR vii](#_Toc512833245)

[DAFTAR TABEL vii](#_Toc512833246)

[BAB I PENDAHULUAN 1](#_Toc512833247)

[I.1 Latar Belakang 1](#_Toc512833248)

[I.2 Perumusan Masalah 3](#_Toc512833249)

[I.2.1 *Research Question* 4](#_Toc512833250)

[I.2.2 Hipotesis 4](#_Toc512833251)

[I.3 Tujuan 4](#_Toc512833252)

[I.4 Ruang Lingkup 5](#_Toc512833253)

[BAB II TINJAUAN PUSTAKA 6](#_Toc512833254)

[II.1 Karya Ilmiah Sejenis Sebelumnya 6](#_Toc512833255)

[II.2 Dasar Teori 8](#_Toc512833256)

[II.2.1 HTTP dan HTTPS 8](#_Toc512833257)

[II.2.2 Server Name Indication (SNI) 9](#_Toc512833258)

[II.2.3 *Web Proxy Deployment* 9](#_Toc512833259)

[BAB III METODOLOGI PENELITIAN 11](#_Toc512833260)

[III.1 Pendekatan Penyelesaian Masalah 11](#_Toc512833261)

[III.2 Jenis Penelitian 11](#_Toc512833262)

[III.3 Variabel Penelitian 11](#_Toc512833263)

[III.4 Objek Penelitian 12](#_Toc512833264)

[III.5 Tahapan Penelitian 12](#_Toc512833265)

[III.5.1 Studi Pustaka 12](#_Toc512833266)

[III.5.2 Pengumpulan Data dan Analisis Kondisi *Existing* 12](#_Toc512833267)

[III.5.3 Perancangan Model 13](#_Toc512833268)

[III.5.4 Pengembangan Implementasi Model 15](#_Toc512833269)

[III.5.5 Eksperimen 15](#_Toc512833270)

[III.5.6 Analisis Hasil Eksperimen 18](#_Toc512833271)

[BAB IV JADWAL PENELITIAN DAN RENCANA ANGGARAN BIAYA 19](#_Toc512833272)

[IV.1 Jadwal Penelitian 19](#_Toc512833273)

[IV.2 Rencana Anggaran Biaya 19](#_Toc512833274)

[DAFTAR PUSTAKA 21](#_Toc512833275)

# DAFTAR GAMBAR

[Gambar III.1. Tahapan penelitian 13](#_Toc512833276)

[Gambar IV.1. Jadwal pengerjaan tugas akhir 20](#_Toc512833277)

# DAFTAR TABEL

[Tabel III.1. Subjek studi pustaka 13](#_Toc512833278)

[Tabel III.2. Data yang akan dikumpulkan 14](#_Toc512833279)

[Tabel III.3. Skenario eksperimen identifikasi akses web 16](#_Toc512833280)

[Tabel III.4. Skenario eksperimen autentikasi pengguna jaringan 17](#_Toc512833281)

[Tabel III.5. Skenario eksperimen implementasi model keseluruhan 18](#_Toc512833282)

[Tabel IV.1. Rencana pengeluaran 19](#_Toc512833283)

[Tabel IV.2. Rencana pemasukan 19](#_Toc512833284)

# PENDAHULUAN

## Latar Belakang

Penggunaan web sebagai salah satu aplikasi jaringan Internet semakin intens digunakan dalam kehidupan sehari-hari. Di lingkungan kampus, jaringan Internet juga mulai menjadi alat bantu yang penting, salah satunya dalam kegiatan proses belajar mengajar.

Meningkatnya penggunaan web di seluruh dunia juga menyebabkan protokol HTTPS dibuat. HTTPS adalah protokol yang melakukan enkripsi terhadap protokol HTTP — protokol yang sering digunakan di dunia web — dan diformalkan pada tahun 2000 (The Internet Society, 2000). Enkripsi dilakukan pada pesan HTTP antara klien dengan server, sehingga tidak ada pihak lain di antara kliendan server yang dapat mengetahui isi pesan HTTP.

*Awareness* para penyedia layanan Internet mengenai pentingnya penggunaan HTTPS pun digencarkan. Mulai rilis versi 68 pada bulan Juli 2018, Google Chrome sebagai *web browser* yang banyak dipakai di seluruh dunia akan menampilkan tulisan “*Not secure*” pada *address bar* jika pengguna mengakses *resource* tanpa menggunakan protokol HTTPS (Schechter, 2018). Protokol HTTP terbaru, HTTP/2, bahkan didesain hanya bekerja jika terenkripsi dengan TLS (Chacos, 2013); dengan kata lain, jika dilayani dengan protokol HTTPS.

Peningkatan *awareness* ini kemudian membuahkan hasil. Penggunaan protokol HTTPS meningkat tajam di beberapa tahun terakhir. 67% akses web menggunakan *browser* Firefox di seluruh dunia merupakan koneksi HTTPS (Let’s Encrypt, 2017). Di Jurusan Teknik Komputer dan Informatika dengan porsi penggunaan rata-rata 35% dari pemakaian Politeknik Negeri Bandung, penggunaan HTTPS juga mencapai 60,14%. Sampel tersebut menunjukkan peningkatan tersebut juga terjadi di Politeknik Negeri Bandung.

Perangkat komputasi seperti laptop juga semakin murah dan menawarkan portabilitas yang lebih tinggi daripada komputer *tower*. Aktivitas di suatu organisasi kemudian tak lagi hanya dilakukan dengan komputer yang disediakan oleh pengelola IT, namun juga dilakukan dengan perangkat pribadi. Kondisi ini menjadi sebuah tren yang umum disebut *bring your own device* dan menuntut pengelola IT untuk memberikan kemudahan akses bagi anggota organisasi yang menggunakan perangkat pribadinya (Meru Networks, 2012).

Tren ini juga terjadi di Politeknik Negeri Bandung. Kegiatan pembelajaran tak lagi terbatas dengan penggunaan komputer di laboratorium, namun juga dapat dilakukan dengan laptop pribadi. Dengan demikian, kegiatan pembelajaran secara mandiri bahkan dapat dilakukan di luar jam belajar formal. Akses web ke jaringan Internet juga disediakan melalui jaringan WiFi yang tersebar di lingkungan Politeknik Negeri Bandung.

Akses web di lingkungan Politeknik Negeri Bandung kemudian dikelola oleh Sub Bagian Perencanaan dan Sistem Informasi (PSI) di bawah Pembantu Direktur IV Bidang Perencanaan dan Pengembangan. Untuk mengelola akses web ini, PSI mewajibkan seluruh pengguna untuk menggunakan *explicit web proxy*, yaitu *web proxy* yang perlu diatur secara eksplisit pada aplikasi yang digunakan oleh pengguna (Rabinovich dan Spatscheck, 2001). Dengan *explicit web proxy*, PSI melakukan identifikasi pengguna, manajemen akses berdasarkan kriteria tertentu, dan mencatat akses yang kemudian dianalisis sebagai dasar pengembangan lanjutan. PSI juga menjadikan *explicit web proxy* sebagai satu-satunya rute keluar aplikasi menuju jaringan Internet.

Karena sifatnya yang eksplisit, maka alamat IP dan *port* dari *web proxy* harus diatur di sisi pengguna. Pengaturan ini dapat dilakukan di sistem operasi. Namun, tidak semua aplikasi dapat membaca pengaturan *web proxy* dari sistem operasi (McAfee, 2014). Terdapat aplikasi yang perlu dikonfigurasi secara terpisah dengan cara yang spesifik untuk masing-masing aplikasi. Dengan sifatnya yang eksplisit ini pula, aplikasi akan memiliki cara komunikasi yang berbeda antara ketika melalui *web proxy* dengan ketika tidak melalui *web proxy* (Rabinovich dan Spatscheck, 2001).

Dalam menyikapi perkembangan teknologi, PSI juga menerapkan *transparent web proxy*, yaitu *web proxy* yang diatur secara transparan sehingga tidak perlu pengaturan tambahan di sisi pengguna. Penerapan *transparent web proxy* ini dilakukan pada beberapa jaringan WiFi di lingkungan gedung Direktorat dan gedung H. Namun, *transparent web proxy* yang diimplementasi oleh PSI ini baru mampu mengelola akses web melalui protokol HTTP yang beroperasi di *port* 80. Di luar itu, akses pengguna tidak melalui *web proxy*, melainkan langsung berhadapan ke Internet.

## Perumusan Masalah

Dari latar belakang di atas, muncul beberapa masalah yang dihadapi, yaitu:

* hanya aplikasi yang *proxy-aware* (mendukung penggunaan *explicit web proxy*) saja yang dapat digunakan di mayoritas jaringan Politeknik Negeri Bandung. Terdapat aplikasi yang tidak *proxy-aware* sehingga tidak dapat digunakan di dalam jaringan Politeknik Negeri Bandung namun diperlukan, seperti UniFi Controller, dan digunakan di luar gedung Direktorat dan gedung H yang menerapkan *transparent web proxy*;
* jumlah konfigurasi yang perlu dilakukan oleh pengguna ketika berpindah jaringan bertambah. Hal ini terjadi karena umumnya jaringan di luar Politeknik Negeri Bandung tidak menggunakan *explicit web proxy*, sehingga pengguna perlu mengatur *web proxy* di sistem operasi ketika berpindah jaringan. Jumlah konfigurasi juga dapat bertambah jika pengguna menggunakan aplikasi yang tidak dapat membaca konfigurasi *web proxy* dari sistem operasi. Padahal, di era *bring your own device* seperti sekarang, konfigurasi yang harus dilakukan di setiap perangkat oleh pengguna merupakan tindakan yang meningkatkan kendala pengelolaan jaringan (Meru Networks, 2012); serta
* kemampuan pengelolaan akses web yang dimiliki oleh PSI dengan *transparent web proxy* di jaringan WiFi gedung Direktorat dan gedung H berkurang dibandingkan dengan kemampuan dari *explicit web proxy*. Hal ini karena mayoritas akses web menggunakan HTTPS tidak lagi melalui *web proxy*, melainkan langsung tersambung ke Internet, sehingga PSI tidak memiliki informasi mengenai akses webyang dilakukan oleh pengguna. Akses web menggunakan HTTPS juga perlu diidentifikasi dengan cara khusus, karena sifat protokol HTTPS yang terenkripsi. PSI juga tidak dapat menganalisis penggunaan berdasarkan kelompok pengguna karena fungsi autentikasi pengguna tidak dapat dilakukan secara mandiri oleh *transparent web proxy* (McAfee, 2014).

### *Research Question*

Masalah-masalah tersebut ditambah dengan fakta yang melatarbelakangi kemudian memicu pertanyaan: Bagaimana cara mengelola akses web di Politeknik Negeri Bandung yang memberikan kemudahan kepada pengguna untuk menggunakan aplikasi yang diperlukan, tetapi tetap memberikan kemampuan bagi PSI untuk mengelola akses web sesuai kebutuhan?

### Hipotesis

Ada dua hipotesis dari *research question* tersebut, yaitu:

H0: akses web di Politeknik Negeri Bandung dikelola dengan menerapkan *explicit web proxy* sebagai satu-satunya jalan untuk mengakses web. Pada *web proxy* diterapkan autentikasi dan *logging*, sedangkan pada jaringan diterapkan *null route* ke luar jaringan Politeknik Negeri Bandung; dan

H1: akses web di Politeknik Negeri Bandung dikelola dengan menerapkan *transparent web proxy*. Dengan demikian, *null route* tidak boleh diterapkan di dalam jaringan Politeknik Negeri Bandung. Autentikasi dilakukan di luar *web proxy*, sedangkan *logging* tetap dilakukan di *web proxy*.

## Tujuan

Tujuan dari pekerjaan tugas akhir ini adalah:

1. menghasilkan dan menguji model pengelolaan akses web di Politeknik Negeri Bandung menggunakan *transparent web proxy* dengan Server Name Indication (SNI), sebuah *field* tambahan pada inisiasi koneksi HTTPS sebagai media identifikasi akses web dengan HTTPS, serta autentikasi pengguna yang dilakukan di luar *web proxy*; dan
2. menghasilkan rekomendasi pengelolaan akses web menggunakan model yang dihasilkan untuk digunakan di Politeknik Negeri Bandung.

## Ruang Lingkup

Pekerjaan tugas akhir ini dibatasi sebagai berikut:

* kebutuhan pengelolaan akses web berupa autentikasi pengguna, pengaturan kontrol akses, serta tingkat kedalaman log yang dihasilkan akan di-*capture* dari konfigurasi *web proxy* yang saat ini berjalan;
* *software web proxy* yang akan digunakan adalah Squid, yaitu *software* yang digunakan sebagai *web proxy* di Politeknik Negeri Bandung. *Web proxy* akan berjalan di atas sistem operasi berbasis Linux. Pemilihan ini diambil untuk menjaga agar pengetahuan teknis baru yang diperlukan oleh *stakeholder* lama (dalam hal ini PSI) dalam level minimal;
* autentikasi pengguna yang dilakukan di luar *web proxy* akan diimplementasi menggunakan fasilitas *hotspot* dari Mikrotik RouterOS. Perangkat implementasi yang dipilih ini bukan bagian dari model implementasi yang akan dihasilkan. Aspek detail mengenai autentikasi juga berada di luar lingkup tugas akhir ini;
* model implementasi yang dihasilkan akan dibandingkan dengan kondisi *existing* secara fungsional. Hal-hal lain terkait *metric quality of service* seperti *throughput*, *latency*, dan *jitter* dari topologi yang digunakan, juga performa *web proxy* terkait dengan jumlah *concurrent user* dan *concurrent connection* berada di luar lingkup tugas akhir ini; dan
* aplikasi pengguna yang akan digunakan sebagai bahan uji model secara fungsional diambil dari aplikasi yang digunakan dalam kegiatan pembelajaran di Jurusan Teknik Komputer dan Informatika. Aplikasi digunakan untuk mengukur perbaikan layanan yang dirasakan oleh pengguna, dan tidak mencerminkan kemampuan model, karena tingkat kompatibilitas SNI berada di atas 99% (Nygren, 2017).

# TINJAUAN PUSTAKA

## Karya Ilmiah Sejenis Sebelumnya

Dalam rangka menjawab *research question*, dilakukan studi karya-karya ilmiah sejenis sebelumnya yang membahas mengenai pengelolaan akses web ke jaringan Internet.

Ikechukwu (2017) mengidentifikasi bahwa biaya *bandwidth* merupakan biaya terbesar dari biaya pengadaan layanan jaringan Internet. Dengan demikian, *bandwidth* menjadi salah satu *resource* jaringan yang perlu dikelola. Ikechukwu kemudian melakukan survei mengenai teknik pengelolaan *bandwidth*.

Dalam surveinya, Ikechukwu menemukan bahwa *web proxy* masih (dan relevan) digunakan sebagai salah satu alat untuk melakukan pengelolaan *bandwidth* dengan cara melakukan *caching*, yaitu menyimpan *resource* yang baru-baru ini diakses oleh pengguna. *Caching* berguna jika ada *resource* yang diakses oleh beberapa pengguna dan berukuran cukup besar, sehingga *bandwidth* yang digunakan keluar ke jaringan Internet dapat dihemat.

Di Politeknik Negeri Bandung, *caching* dapat bermanfaat karena terdapat banyak unit komputer (baik yang dikelola oleh institusi maupun perangkat pribadi) yang melakukan akses ke *resource* yang sama dan besar. Salah satu *resource* yang dimaksud adalah *update* sistem operasi.

Selain *caching*, Ikechukwu juga mengungkapkan bahwa penggunaan *web proxy* dapat meningkatkan keamanan, merincikan catatan akses, meningkatkan akuntabilitas, dan meningkatkan performa jaringan.

Yeh (2017) dalam tesisnya meneliti tentang *secure web gateway*. *Secure web gateway* merupakan pengembangan dari *web proxy*. Kelebihan dari *secure web gateway* adalah memberikan fungsi keamanan bagi jaringan, seperti perlindungan dari serangan Cross-Site Scripting. Perusahaan yang membutuhkan sertifikasi tertentu dengan kebutuhan keamanan yang tinggi, misalnya perusahaan yang bergerak di bidang perbankan yang membutuhkan sertifikasi PCI-DSS, membutuhkan fungsi keamanan yang ditawarkan oleh *secure web gateway* dan sulit diperoleh dari sekadar menggunakan *web proxy*. Yeh dalam tesisnya kemudian berargumen bahwa di kemudian hari, *web proxy* akan digantikan dengan *secure web gateway*.

Meski *secure web gateway* dapat menjadi solusi bagi masalah-masalah yang diungkap pada Bab I, penggunaan *secure web gateway* dirasa berlebihan pada konteks pemakaian di Politeknik Negeri Bandung. Hal ini karena:

1. implementasi *secure web gateway* membutuhkan *resource* yang lebih besar daripada mengimplementasi *web proxy*, termasuk:
   1. membutuhkan tingkat keilmuan yang lebih tinggi untuk implementasi, dan
   2. membutuhkan pengubahan infrastruktur yang cukup besar;
2. kebutuhan Politeknik Negeri Bandung saat ini sudah terlayani dengan *web proxy*. Untuk dapat menyelesaikan masalah pada Bab I, ada peluang bahwa model pengelolaan yang saat ini berjalan untuk diperbaiki.

Hal di atas diperkuat dengan pengetahuan bahwa *secure web gateway* Yeh sebenarnya merupakan *superset* penuh dari *web proxy*. Bahkan, Yeh menggunakan Squid sebagai salah satu komponen *secure web gateway*-nya. Squid adalah *software web proxy* yang sama dengan yang digunakan di Politeknik Negeri Bandung. Salah satu hal yang dapat diamati dari *secure web gateway* Yeh adalah penerapan SNI sebagai alat identifikasi akses web menggunakan protokol HTTPS.

Karena itu, meski Yeh sudah membuktikan *secure web gateway­*-nya menyelesaikan masalah yang diungkap pada tesisnya, pada tugas akhir ini implementasi *transparent web proxy* tetap perlu dikaji. Hal ini karena model pengelolaan dengan *transparent web proxy* yang akan diusulkan merupakan *subset* dari *secure web gateway* Yeh. Perlu pembuktian bahwa model yang akan diusulkan ini menyelesaikan masalah yang dialami di Politeknik Negeri Bandung, namun tidak mengurangi kemampuan pengelolaan yang sudah dimiliki sebelumnya.

Pada subbab Dasar Teori, akan dijelaskan bahwa SNI merupakan *extension* dari protokol TLS. Dengan demikian, secara prinsip terbuka kemungkinan bahwa ada klien dan/atau server yang tidak mendukung penggunaan SNI. Kekhawatiran ini kemudian dijawab oleh studi terbaru Akamai (2017) yang menyatakan bahwa tingkat penggunaan SNI pada akses web menggunakan protokol HTTPS telah mencapai 99,4% pada bulan Maret 2017. Peningkatan protokol HTTPS juga didorong oleh *requirement* protokol HTTP/2 yang mensyaratkan klien yang akan menggunakan protokol tersebut harus menggunakan SNI ketika menginisiasi koneksi dengan server (Nygren, 2017).

## Dasar Teori

### HTTP dan HTTPS

HTTP (Hypertext Transfer Protocol) adalah protokol *application layer* untuk sistem informasi yang terdistribusi dan kolaboratif (The Internet Society, 1999). HTTP adalah protokol yang menjadi fondasi web di jaringan Internet.

Protokol HTTP berbasis *request-response*. Klien mengirim *request* ke server berupa *request method*, URI (*uniform resource identifier*), dan versi protokol yang digunakan (hingga kini protokol HTTP sudah berkembang hingga versi HTTP/2), diikuti *header-header* HTTP, dan dilanjutkan dengan *body request* jika ada. Server kemudian akan merespons dengan *status code*, diikuti *header-header* HTTP, dan dilanjutkan dengan *body response* (jika ada).

Protokol ini bersifat *plaintext*. Dengan sifat *plaintext*-nya ini, pihak-pihak di antara klien dan server dapat membaca pertukaran pesan yang terjadi, dan dapat melakukan modifikasi. Hal ini berbahaya jika pesan yang dipertukarkan merupakan pesan sensitif, misalnya *request-response* untuk layanan perbankan.

Namun, penggunaan protokol ini untuk aplikasi yang sensitif meningkat. Untuk menyikapi hal tersebut, Netscape Communications mulai mengembangkan protokol HTTPS pada tahun 1994 (Walls, 2006). Protokol HTTPS digunakan untuk mentransmisikan pesan HTTP yang dienkripsi dengan Transport Layer Security (TLS) dan diformalkan pada tahun 2000 (The Internet Society, 2000).

Dengan HTTPS, transmisi dienkripsi sejak meninggalkan klien hingga tiba di server, kemudian dilakukan dekripsi. Pesan yang dipertukarkan tak lagi bersifat *plaintext*. Dengan demikian, jalur yang dilalui di antara klien dan server tidak dapat melihat isi transmisi dan memodifikasinya, termasuk *header* dan *payload* HTTP yang terkandung di dalamnya.

Dengan protokol HTTPS, ada tambahan *handshake* yang perlu dikerjakan oleh kliendengan server, yakni proses permintaan sertifikat server dari klien, untuk kemudian digunakan sebagai media autentikasi transmisi. Transmisi dari server kemudian hanya dapat divalidasi dengan sertifikat tersebut, sehingga klien dapat menolak transmisi jika diketahui terjadi perubahan data di tengah jalan yang mengakibatkan sertifikat server tidak dapat melakukan validasi. Hal inilah yang menyebabkan *resource* yang diakses menggunakan protokol HTTPS tidak dapat di-*cache* oleh *web proxy*.

### Server Name Indication (SNI)

SNI merupakan *field* yang dikirimkan oleh klien ke server untuk mengindikasikan *hostname* apa yang ingin diakses oleh klien. SNI memungkinkan sebuah server dengan satu alamat IP dan *port* yang sama untuk melayani lebih dari satu situs yang dienkripsi dengan HTTPS tanpa mengharuskan semua situs menggunakan sertifikat yang sama (The Internet Society, 2011). SNI merupakan *extension* terhadap protokol TLS, sehingga penerapannya sangat bergantung pada klien dan server yang berinteraksi.

### *Web Proxy Deployment*

Rabinovich dan Spatscheck (2001) mengungkapkan dua cara *deployment* *web proxy* dalam suatu jaringan, yaitu secara *nontransparent* dan secara *transparent*. *Web proxy* yang di-*deploy* secara *non-transparent* umum disebut sebagai *explicit web proxy*.

Pada *nontransparent web proxy deployment*, klien sadar bahwa ada *web proxy* yang perlu dituju agar dapat melakukan akses web ke jaringan Internet. Dengan demikian, klien akan mengirim semua *request*-nya ke *web proxy*, tanpa memandang bahwa *request* tersebut seharusnya dikirim ke server yang diindikasikan pada URL (Uniform Resource Locator).

Pada kondisi di mana klien tidak sadar ada *web proxy* yang perlu dituju, klien akan langsung melakukan *lookup* terhadap *hostname* server yang dituju ke suatu server DNS. Server DNS akan mengembalikan alamat IP yang kemudian akan dihubungi langsung oleh klien.

Dengan keberadaan *explicit web proxy*, klien akan langsung membuat koneksi ke *web proxy*, kemudian mengirimkan seluruh URL dari *resource* yang ingin diakses (termasuk *hostname* dari server yang dituju). *Lookup* terhadap *hostname* kemudian akan dilakukan oleh *web proxy*.

Di Politeknik Negeri Bandung, pada jaringan yang membutuhkan *explicit web proxy*, klien dikonfigurasi secara langsung berupa alamat IP dan *port* dari *web proxy* serta *credentials* yang diperlukan untuk autentikasi.

Cara lainnya untuk melakukan *deployment web proxy* adalah dengan melakukannya secara *transparent*. Pada cara ini, klien tidak mengetahui bahwa ada *web proxy* yang akan dituju. Dengan demikian, cara klien mengakses *resource* tidak ada bedanya dengan ketika tidak ada *web proxy* sama sekali.

*Web proxy* dapat digunakan sebagai media autentikasi dengan membalas *request* dari klien dengan *status code* HTTP 407 (Proxy Authentication Required).

Dengan cara ini, jika dikonfigurasi secara *explicit*, *web proxy* dapat melakukan *response* untuk protokol apapun (baik HTTP, maupun non-HTTP seperti HTTPS yang membutuhkan pembuatan *tunnel*). Berbeda jika dikonfigurasi secara *transparent*, *web proxy* belum tentu dapat melakukan *response* untuk protokol non-HTTP seperti HTTPS, karena tidak ada *request* pembuatan *tunnel* dari klien ke *web proxy*.

# METODOLOGI PENELITIAN

## Pendekatan Penyelesaian Masalah

Masalah yang diungkap pada Bab I akan diselesaikan dengan membuat model pengelolaan akses web di Politeknik Negeri Bandung menggunakan *transparent web proxy* dengan tiga hal utama, yaitu:

* akses web dengan protokol HTTP dilewatkan secara *transparent* sesuai dengan kondisi *existing* yang ada di Politeknik Negeri Bandung pada implementasi di gedung Direktorat dan gedung H (sehingga berada di luar topik kajian);
* akses webdengan protokol HTTPS dilewatkan secara *transparent* menggunakan SNI sebagai media identifikasi server tujuan; serta
* autentikasi pengguna dilakukan di luar *web proxy*, dan *web proxy* harus memiliki kemampuan untuk melakukan *mapping* antara alamat IP klien dengan identitas autentikasinya.

## Jenis Penelitian

Penelitian ini dilakukan dengan pendekatan kuantitatif dengan teknik penelitian eksperimental, sebab dalam penelitian ini fokus pada elemen yang spesifik, yaitu fungsionalitas aplikasi pengguna serta kedalaman log yang dihasilkan bagi pengelola. Eksperimen dilakukan dengan membandingkan elemen tersebut pada kondisi *existing* dengan model implementasi yang akan dihasilkan.

## Variabel Penelitian

Variabel-variabel yang terlibat dalam penelitian ini adalah:

1. variabel bebas (*independent variables*):
   1. *deployment* dari *web proxy* (apakah *explicit* atau *transparent*),
   2. aplikasi yang digunakan dalam kegiatan pembelajaran beserta protokol yang digunakan aplikasi tersebut (HTTP atau HTTPS),
   3. pengautentikasi pengguna agar mendapat akses web (*explicit web proxy* atau di luar *web proxy* pada jenis *deployment* *transparent web proxy*);
2. variabel terikat (*dependent variables*):
   1. tingkat perincian log yang dihasilkan (untuk protokol HTTP: mampu mencatat URL secara lengkap; untuk protokol HTTPS: mampu mencatat *hostname* yang dituju),
   2. kemampuan aplikasi terkait *proxy* (apakah *proxy-aware* atau tidak, serta kemampuannya mendapatkan akses web dalam jaringan),
   3. kemampuan *web proxy* untuk mencatat pengguna jaringan,
   4. tingkat kemudahan pengguna melakukan konfigurasi aplikasi agar mendapat akses web dari jaringan, dan
   5. tingkat kemampuan pengelola jaringan untuk melakukan manajemen akses web.

## Objek Penelitian

Objek yang digunakan dalam penelitian ini adalah jaringan komputer dengan sebuah *web proxy* untuk mengelola akses web dari dalam jaringan komputer. Terdapat dua model yang akan diamati, yaitu model pada H0 (menggunakan *explicit web proxy* dengan autentikasi yang dilakukan oleh *web proxy*) dengan model yang diusulkan pada H1 (menggunakan *transparent web proxy* dengan autentikasi yang dilakukan di luar *web proxy*).

## Tahapan Penelitian

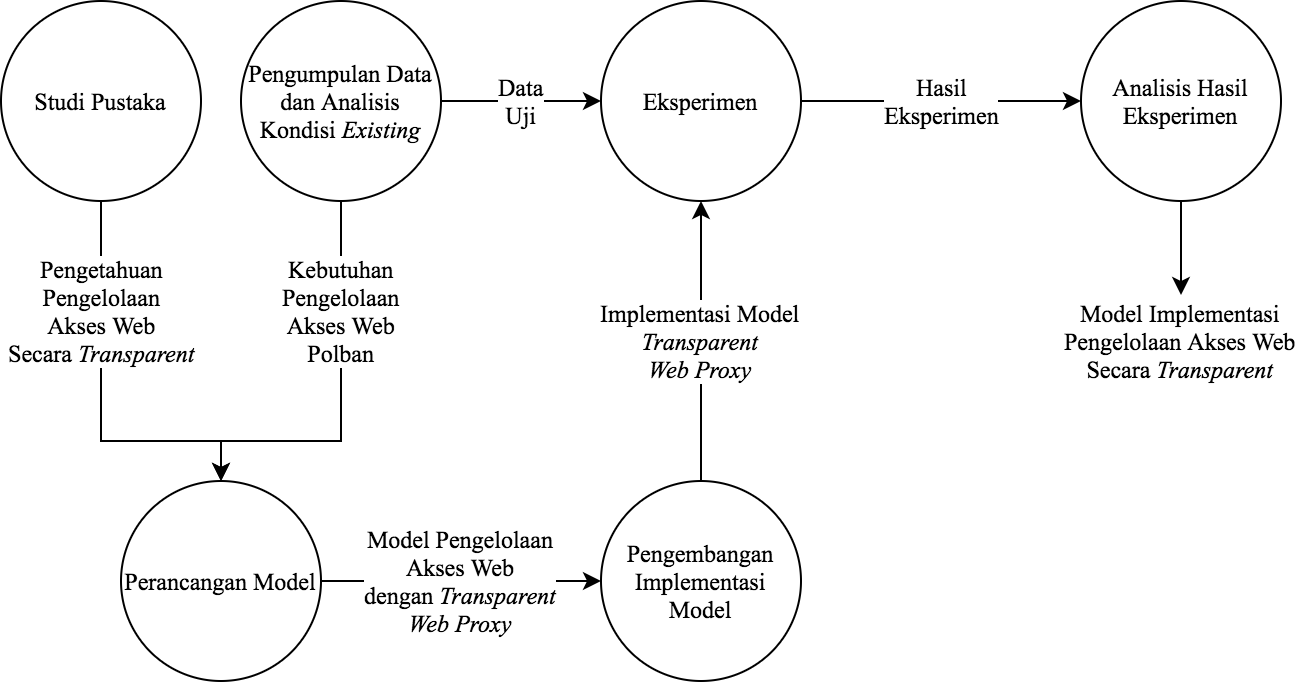
Tahapan penelitian ini secara umum digambarkan pada Gambar III.1.

### Studi Pustaka

Studi pustaka bertujuan mencari dan mempelajari sumber-sumber yang relevan dan terpercaya dengan permasalahan yang dihadapi sebagai landasan teori dan bahan kajian dari penelitian ini. Hal-hal yang akan distudi diuraikan pada Tabel III.1.

### Pengumpulan Data dan Analisis Kondisi *Existing*

Pada tahap ini, akan dilakukan pengumpulan data-data pada Tabel III.2. Data yang sudah dikumpulkan kemudian akan dianalisis. Analisis terhadap data tersebut akan menghasilkan uraian kebutuhan pengelolaan akses web di Politeknik Negeri Bandung. Selain itu, pengumpulan data juga dilakukan sebagai data uji yang akan digunakan pada tahap eksperimen.



Gambar III.1. Tahapan penelitian

Tabel III.1. Subjek studi pustaka

|  |  |
| --- | --- |
| Subjek Studi | Hasil Studi |
| Metode penerapan *transparent web proxy* dalam jaringan komputer | Metode penerapan *transparent web proxy* yang akan digunakan dalam model alternatif (H1) |
| Penerapan SNI untuk identifikasi akses web dengan protokol HTTPS | Hal-hal yang perlu diperhatikan dalam menggunakan SNI sebagai alat identifikasi akses web dengan protokol HTTPS |
| Metode autentikasi pengguna untuk akses web | Metode autentikasi pengguna yang akan digunakan dalam model alternatif (H1) |
| Rekomendasi arsitektur jaringan Politeknik Negeri Bandung | Arsitektur jaringan yang menjadi asumsi untuk membangun model *transparent web proxy* |
| Rekomendasi desain arsitektur jaringan dari *vendor-vendor* jaringan | Pertimbangan dalam merancang model *transparent web proxy* |

### Perancangan Model

Dari hasil studi pustaka dan analisis kondisi *existing*, akan dirancang sebuah model pengelolaan akses web menggunakan *transparent web proxy* dengan autentikasi pengguna yang dilakukan di luar *web proxy*. Identifikasi akses web dengan protokol HTTPS akan dilakukan dengan SNI, sedangkan autentikasi akan dilakukan di luar *web proxy*.

Tabel III.2. Data yang akan dikumpulkan

|  |  |
| --- | --- |
| Data | Sumber Data dan Cara Perolehan |
| Topologi *existing* jaringan Politeknik Negeri Bandung yang berkaitan dengan akses web ke jaringan Internet | PSI, dengan melakukan *tracing* terhadap konfigurasi perangkat jaringan terkait (utamanya *router* terluar dan *firewall* pada *gateway* internal) |
| Konfigurasi *web proxy* (baik *explicit* maupun *transparent*) *existing* di Politeknik Negeri Bandung | PSI, dengan mengambil konfigurasi dari *web proxy* yang sedang berjalan |
| Kebutuhan log yang dihasilkan dari *web proxy* sebagai bahan analisis PSI | PSI, dengan mengambil arsip log dari *web proxy* yang sedang berjalan, serta wawancara dengan staf PSI |
| *Software* yang digunakan sebagai alat pembelajaran di Jurusan Teknik Komputer dan Informatika beserta kemampuan *proxy-aware* dan tidaknya (serta apakah konfigurasi *proxy* dapat mengambil dari konfigurasi sistem operasi, jika *proxy-aware*) | Survei ke semua ketua kelas untuk mengumpulkan daftar *software*, kemudian survei ke mahasiswa di kelas masing-masing mengenai kemampuan aplikasi terkait *proxy* |

Hal-hal yang akan dibuat modelnya adalah:

* alur autentikasi pengguna sejak perangkat bergabung di jaringan hingga dapat mengakses web;
* topologi dari pengguna, *web proxy*, dan server autentikasi serta hubungannya ke jaringan Internet; serta
* konfigurasi dari *web proxy*, server autentikasi, dan perangkat jaringan yang menghubungkan keduanya dengan pengguna.

Model akan diuji sesudah dibuat. Pengujian model dilakukan berdasarkan teori-teori yang sudah diperoleh pada studi pustaka serta kebutuhan yang diperoleh dari hasil analisis kondisi *existing*. Pengujian dilakukan dengan menguji apakah kebutuhan yang ada dapat dipenuhi oleh model, serta apakah model sudah cukup komprehensif sehingga dapat melingkupi batasan masalah yang disampaikan pada Bab I.

### Pengembangan Implementasi Model

Model yang sudah dihasilkan di tahap sebelumnya kemudian akan diimplementasi untuk keperluan eksperimen. Implementasi akan dilakukan menggunakan perangkat-perangkat berikut:

* Squid 3.5 sebagai *web proxy* yang berjalan di atas sistem operasi ber-*kernel* Linux;
* Mikrotik RouterOS sebagai sistem operasi yang melakukan *routing* dan autentikasi pengguna;
* GNS3 sebagai *software* simulator topologi jaringan untuk melakukan pengujian implementasi sebelum dieksperimenkan; dan
* Go sebagai bahasa pemrograman untuk membuat implementasi penghubung antara *web proxy* dengan server autentikasi.

### Eksperimen

Untuk menguji hipotesis yang dibangun, eksperimen perlu dilakukan. Eksperimen akan dilakukan dengan menjalankan implementasi model yang sudah dibuat.

Ada tiga eksperimen yang akan dilakukan, meliputi eksperimen terhadap unsur-unsur model (identifikasi akses web dengan protokol HTTPS serta autentikasi pengguna) secara terpisah, diikuti eksperimen terhadap implementasi model secara keseluruhan.

Seluruh eksperimen membutuhkan perlengkapan *hardware* berupa Raspberry Pi 3 akan digunakan sebagai *web proxy*, dan Mikrotik RB750 sebagai *router*. Kedua *hardware* ini digunakan karena relatif tidak membutuhkan biaya yang terlalu besar dan cocok untuk lingkungan yang kecil.

Eksperimen akan dilakukan di ruangan e-Library Jurusan Teknik Komputer dan Informatika agar perubahan terhadap infrastruktur jaringan dapat dilokalisasi. Komputer yang ada di ruangan tersebut akan diinstalasi aplikasi-aplikasi yang diperoleh pada tahap pengumpulan data.

#### Eksperimen Identifikasi Akses Web

Eksperimen dilakukan untuk menguji:

* apakah benar penerapan SNI pada *transparent web proxy* dapat menghasilkan log yang sama jelasnya dengan penerapan *explicit web proxy* untuk mengidentifikasi akses web dengan protokol HTTPS; serta
* apakah benar semua aplikasi dapat berjalan baik pada penerapan *transparent web proxy*.

Eksperimen ini akan dilakukan dengan skenario yang diuraikan pada Tabel III.3.

Eksperimen dilakukan dengan menjalankan setiap skenario tersebut di atas pada jaringan tertutup (ruang e-Library) dengan satu unit komputer. Perpindahan dari skenario 1 ke skenario 2 dilakukan dengan mengubah konfigurasi pada komputer, *router*, dan *web proxy*. Dari eksperimen tersebut dapat diketahui tingkat keberhasilan masing-masing skenario dalam mengidentifikasi akses web yang dilakukan, baik menggunakan protokol HTTP maupun protokol HTTPS.

Tabel III.3. Skenario eksperimen identifikasi akses web

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Skenario 1-A | Skenario 1-B | Skenario 2-A | Skenario 2-B |
| *Web Proxy Deployment* | *Explicit* dengan *null route* | *Explicit* dengan *null route* | *Transparent* | *Transparent* |
| Protokol Akses Web | HTTP | HTTPS | HTTP | HTTPS |
| Metode Identifikasi | Melalui *header* HTTP | Melalui *header* permintaan *tunneling* | Melalui *header* HTTP | Dengan SNI |
| Aplikasi yang Diuji | A1, A2, A3, ... | A1, A2, A3, ... | A1, A2, A3, ... | A1, A2, A3, ... |
| Hipotesis Hasil Eksperimen | URL tercatat lengkap jika aplikasi *proxy-aware*; aplikasi tidak dapat bekerja jika tidak *proxy-aware* | *Hostname* dan *port* tercatat jika aplikasi *proxy-aware*; aplikasi tidak dapat bekerja jika tidak *proxy-aware* | URL tercatat lengkap pada penggunaan semua aplikasi; semua aplikasi dapat digunakan | *Hostname* dan *port* tercatat pada penggunaan semua aplikasi; semua aplikasi dapat digunakan |
| Tingkat Keberhasilan | ...% | ...% | ...% | ...% |

#### Eksperimen Autentikasi Pengguna Jaringan

Eksperimen dilakukan untuk menguji apakah benar *transparent web proxy* bersama server autentikasi dapat melakukan autentikasi pengguna atas penggunaan semua aplikasi yang dibutuhkan dalam kegiatan pembelajaran.

Eksperimen ini akan dilakukan dengan skenario yang diuraikan pada Tabel III.4.

Tabel III.4. Skenario eksperimen autentikasi pengguna jaringan

|  |  |  |
| --- | --- | --- |
|  | Skenario 1 | Skenario 2 |
| *Web Proxy Deployment* | *Explicit* tanpa *null route* | *Transparent*, tanpa identifikasi akses web dengan SNI |
| Pengautentikasi | *Web proxy* (Squid 3.5) | Mikrotik RouterOS |
| Hipotesis Hasil Eksperimen | Hanya aplikasi yang *proxy-aware* yang dapat dicatat bersama identitas penggunanya | Semua penggunaan aplikasi dapat dicatat bersama identitas penggunanya |
| Tingkat Keberhasilan | ...% | ...% |

Eksperimen ini dilakukan dengan menjalankan setiap skenario tersebut di atas pada jaringan tertutup (ruang e-Library) dengan tiga unit komputer. Tiga unit komputer digunakan untuk memastikan hasil eksperimen berlaku umum untuk masing-masing skenario. Perpindahan dari skenario 1 ke skenario 2 dilakukan dengan mengubah konfigurasi pada *router* dan *web proxy*. Dari eksperimen tersebut dapat diketahui tingkat keberhasilan masing-masing skenario dalam mengidentifikasi akses web yang dilakukan oleh pengguna. Persentase dihitung berdasarkan jumlah aplikasi yang dapat diasosiasikan dengan pengguna.

Eksperimen ini tidak memperhatikan tingkat kedalaman log yang dihasilkan, sehingga tidak masalah apabila pada skenario 2, akses web dengan protokol HTTPS hanya dapat mencatat alamat IP server tujuan klien.

#### Eksperimen Implementasi Model Keseluruhan

Eksperimen dilakukan untuk menguji:

* apakah benar model yang dihasilkan pada tugas akhir ini dapat memberikan kemudahan kepada pengguna daripada kondisi *existing* saat ini; serta
* apakah benar model yang dihasilkan dapat memberikan kemampuan yang sama bagi pengelola jaringan untuk mengelola akses web ke Internet seperti halnya pada kondisi *existing* saat ini.

Eksperimen ini akan dilakukan dengan skenario yang diuraikan pada Tabel III.5. Skenario 1 menggambarkan kondisi *existing* saat ini, sementara skenario 2 menggambarkan model yang dihasilkan dari tugas akhir ini.

### Analisis Hasil Eksperimen

Pada tahap ini akan dilakukan pengkajian dan analisis berdasarkan hasil eksperimen yang dilakukan pada tahap selanjutnya. Analisis ini akan menghasilkan kesimpulan berupa model implementasi pengelolaan akses web yang baik untuk Politeknik Negeri Bandung. Analisis ini juga akan menguji hipotesis sehingga dapat dibuktikan apakah H1 diterima atau ditolak.

Tabel III.5. Skenario eksperimen implementasi model keseluruhan

|  |  |  |
| --- | --- | --- |
|  | Skenario 1 | Skenario 2 |
| *Web Proxy Deployment* | *Explicit* dengan *null route* | *Transparent* |
| Identifikasi Akses HTTP | Melalui *header* HTTP | Melalui *header* HTTP |
| Identifikasi Akses HTTPS | Melalui *header* permintaan *tunneling* | Dengan SNI |
| Pengautentikasi | *Web proxy* (Squid 3.5) | Mikrotik RouterOS |
| Aplikasi yang Diuji | A1, A2, A3, ... | A1, A2, A3, ... |
| Tingkat Kemudahan Konfigurasi Pengguna | ... dari skala 5; 1 – sulit, 5 – mudah, untuk masing-masing aplikasi | ... dari skala 5; 1 – sulit, 5 – mudah, untuk masing-masing aplikasi |
| Tingkat Kemampuan Pengelolaan Akses Web | ... dari skala 5: 1 – sulit, 5 – mudah | ... dari skala 5: 1 – sulit, 5 – mudah |

# JADWAL PENELITIAN DAN RENCANA ANGGARAN BIAYA

## Jadwal Penelitian

Pekerjaan tugas akhir dengan metodologi yang sudah diuraikan di Bab III akan dikerjakan dengan penjadwalan yang ditunjukkan pada Gambar IV.1.

## Rencana Anggaran Biaya

Untuk menunjang pekerjaan tugas akhir ini dibutuhkan anggaran biaya sebesar Rp2.135.000,00 dengan perincian yang dituliskan pada Tabel IV.1.

Tabel IV.1. Rencana pengeluaran

|  |  |  |  |
| --- | --- | --- | --- |
| Pengeluaran | Volume | Harga Satuan (Rp) | Sub Total (Rp) |
| Raspberry Pi 3 Model B (*full set*) | 1 set | 925.000 | 925.000 |
| Kabel Ethernet (*full set*) | 2 set | 75.000 | 150.000 |
| Kertas A4, 80 gsm | 3 rim | 40.000 | 120.000 |
| Tinta Epson T664 hitam | 3 botol | 90.000 | 270.000 |
| Tinta Epson T664 warna | 3 botol | 90.000 | 270.000 |
| Alat tulis kantor, penjilidan, dan penggandaan | 1 set | 400.000 | 400.000 |
| Total (Rp) |  |  | 2.135.000 |

Kebutuhan anggaran biaya tersebut direncanakan ditutupi dengan pemasukan yang dituliskan pada Tabel IV.2.

Tabel IV.2. Rencana pemasukan

|  |  |
| --- | --- |
| Pemasukan | Sub Total (Rp) |
| Politeknik Negeri Bandung | 1.400.000 |
| Swadaya | 735.000 |
| Total (Rp) | 2.135.000 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Februari** | | | **Maret** | | | | **April** | | | | | **Mei** | | | | **Juni** |
| **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **1** |
| 1 | Studi pustaka |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Pengumpulan data dan analisis kondisi *existing* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Target Seminar 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Perancangan model |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Target Seminar 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Pengembangan implementasi model |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Eksperimen |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Target Seminar 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Analisis hasil eksperimen |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Target Sidang Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Gambar IV.1. Jadwal pengerjaan tugas akhir

# DAFTAR PUSTAKA

Campos, J. (2015) *Citrix NetScaler: How to Apply Multiple Certificates to One Virtual Server*. Tersedia pada: http://bit.ly/2IlQyl4 (Diakses: 1 Maret 2018).

Chacos, B. (2013) *Next-gen HTTP 2.0 protocol will require HTTPS encryption (most of the time)*, *PCWorld*. Tersedia pada: http://bit.ly/2q09T3R (Diakses: 5 Maret 2018).

Ikechukwu, U. I. (2017) “A Survey on Bandwidth Management Techniques Via the OSI Model Network and Application Layers,” *Global Journal of Computer Science and Technology*.

Let’s Encrypt (2017) *Percentage of Web Pages Loaded by Firefox Using HTTPS*. Tersedia pada: https://letsencrypt.org/stats/ (Diakses: 21 Desember 2017).

Li, Q. dan Clark, G. (2015) *Security Intelligence: A Practitioner’s Guide to Solving Enterprise Security Challenges*. Indianapolis: John Wiley & Sons, Inc.

McAfee (2014) “Direct or Transparent Proxy?” Tersedia pada: http://bit.ly/2JegIr5.

Meru Networks (2012) *BYOD Best Practices: Requirements and Challenges*.

Nygren, E. (2017) *Reaching toward universal TLS SNI*, *The Akamai Blog*. Tersedia pada: http://bit.ly/2Gsk8Jk (Diakses: 20 Maret 2018).

Rabinovich, M. dan Spatscheck, O. (2001) *Web Caching and Replication*. Addison-Wesley Professional.

Schechter, E. (2018) *A secure web is here to stay*, *Chromium Blog*. Tersedia pada: http://bit.ly/2H53AnQ (Diakses: 5 Maret 2018).

The Internet Society (1999) *RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1*.

The Internet Society (2000) *RFC 2818 - HTTP Over TLS*. Tersedia pada: https://tools.ietf.org/html/rfc2818 (Diakses: 5 Maret 2018).

The Internet Society (2011) *RFC 6066 - Transport Layer Security (TLS) Extensions: Extension Definitions*. Tersedia pada: https://tools.ietf.org/html/rfc6066 (Diakses: 5 Maret 2018).

Walls, C. (2006) *Embedded Software: The Works*. Elsevier.

Yeh, J. (2017) *Key factors in building a Secure Web Gateway*. The University of Waikato.