# BAB II
# TINJAUAN PUSTAKA

## 2.1 Penelitian Terdahulu

Pada tinjauan pustaka ini terdapat beberapa hasil yang dapat di jadikan referensi laporan agar dapat memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Berikut merupakan penelitian terdahulu berupa beberapa jurnal yang terkait dengan judul laporan akhir penulis.

Penelitian yang dilakukan oleh Batara Sakti , Abdul Aziz, dan Afrizal Doewes (2013) tentang "Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing ". Menghasilkan mengukur tingkat keamanan SSH dalam mengamankan transmisi FTP. Penelitian dilakukan dengan menerapkan penetration testing pada sistem yang menggunakan *service SSH* dan FTP. Penetration testing adalah teknik pengujian untuk mencari kelemahan dan kekurangan suatu sistem dengan menghindari atau menerobos mekanisme keamanan yang ada untuk mensimulasikan teknik penyerangan yang mungkin untuk dilakukan. Tingkat keamanan SSH akan diukur dari ketahanannya dalam menghadapi setiap proses serangan yang disimulasikan dalam penetration testing.

Penelitian yang dilakukan oleh Dasri dan Andryanto A(2018) tentang "Perancangan FTP Server dengan keamanan SSL pada kampus amik ibnu khaldun palopo ". Menghasilkan Data dalam bentuk digital merupakan salah satu bentuk utama penyimpanan data. Dengan sendirinya, pertukaran data dalam bentuk digital merupakan satu hal yang penting dalam pertukaran data tersebut. File adalah salah satu bentuk data digital yang bentuknya dapat dilihat dan dipindahka.

Penelitian yang dilakukan oleh Sahari (2016) tentang "Implementasi sistem keamanan web server berbasis distro linux debian pada cv.karya baru perabot ".Menghasilkan Sistem keamanan web server menggunakan linux debian dan mikrotik ini dapat mempermudah dalam pemahaman konsep karena adanya media nyata berupa cara melakukan keamanan server dengan linux debian dan mikrotik. Dengan menggunakan linux debian dan mikrotik dapat meningkatkan

sistem keamanan komputer server dari gangguan pihak luar dengan memanfaatkan penyetingan firewall pada debian dan mikrotik.

Penelitian yang dilakukan oleh Ahmad Fali Oklillas dan Budi Irawan (2014) tentang “Implementasi FTP Server dengan Metode Transfer Layer Security untuk Keamanan Transfer Data Menggunakan CentOS 5.8 “ .Menghasilkan FTP server tidak menggunakan secure socket layer dan secure shell dapat terbaca oleh tool wireshark nama user, password, maupun file yang di-unggah atau diunduh oleh user FTP. Sebaliknya, user FTP tidak dapat terbaca oleh tool wireshark. FTP server yang telah diterapkan disk quota berfungsi sebagai pembatasan penggunaan kapasitas hard disk untuk mencegah penuhnya hard disk pada server .

Penelitian yang dilakukan oleh Devi Ruwaida, Dian Kurnia(2018) tentang “Rancang bangun file transfer protocol (FTP) dengan pengamanan open ssl pada jaringan VPN  Mikrotik di smk dwidarma “.Menghasilkan perbandingan antara Ftp server yang menggunakan seritifikat ssl sebagai pengaman lebih aman dari pada Ftp server yang tidak memasang sertifikat sll . Dengan menggunakan VPN pada mikrotik dalam melakukan remote dan mengirim data lebih aman sebab berbasis Tcp/Ip

Penelitian yang dilakukan oleh  Feby Ardiant, Eliza tentang “Penggunaan Mikrotik Router sebagai jaringan Server “. Menghasilkan Konfigurasi IP Adreess Server: 192.168.8.1 , Subnet mask : 255.255.255.0 Class C/24, sedangkan untuk client menggunakan IP address antara 192.168.8.2 – 192.168.8.254 dengan subnet mask255.255.255.0 . Menggunakan topologi star dikaranakan jika terjadi gangguan pada salah client tidak menggunnguclient yang lain.

## 2.2 Pengertian FTP Server

FTP Server adalah server yang memberi layanan untuk saling berbagi file antarkomputer yang terhubung dalam satu jaringan. FTP Server dapat diakses melalui dua aplikasi,yaitu melalui Browser dan juga FileZilla. Jika menggunakan browser, kita hanya bisa mengunduhfile. Namun bila menggunakan FileZilla, kita dapat mengunduh dan mengrim file ke Server

FTP adalah sebuah protokol internet yang berfungsi untuk mengirim atau menerima file dalam suatu jaringan (network) yang dilakukan oleh FTP server dan FTP client. Layanan FTP bisa diakses oleh semua orang dengan mengatur menjadi FTP public atau diatur menjadi FTP privat dimana hanya pengguna yang terdaftar saja yang dapat mengaksesnya.

File Transfer Protocol (FTP) adalah protokol jaringan standar yang digunakan untuk mentransfer file komputer dari satu host ke host lain melalui jaringan berbasis TCP, seperti Internet. FTP dibangun di atas arsitektur server klien dan menggunakan kontrol terpisah dan koneksi data antara klien dan server. Pengguna APP dapat mengotentikasi dirinya dengan menggunakan protokol masuk yang jelas, biasanya dalam bentuk nama pengguna dan kata sandi, namun dapat terhubung secara anonim jika server dikonfigurasi untuk mengizinkannya Untuk transmisi aman yang melindungi username dan password, dan mengenkripsi isinya, FTP sering diamankan dengan SSL / TLS (FTPS) (Ranie, Leena, Preeti Narula dan Neeti Panchal, 2014).

FTP (File Tranfer Protocol) umumnya berfungsi sebagai media tukar menukar file atau data dalam suatu network yang menggunakan TCP koneksi. FTP yang digunakan menggunakan berbasis Open Source guna menunjang tingkat stabilitas tinggi dan tidak mudah terinfeksi virus dan malware. FTP merupakan metode protokol pilihan yang paling tepat dalam penyimpanan file/data secara cepat dalam proses upload dan download dari komputer server ke klien tanpa menggunakan flashdisk untuk mengambil data dari komputer server (Arman, Molavi, 2017).

SSL (Secure Socket Layer) diperlukan untuk menjaga proses autentikasi dan proses transfer data yang terlebih dahulu dienkripsi. SSL memiliki beberapa versi dan yang terbaru adalah SSLv3 namun pengembangan dari SSLv3 dinamakan TLS (Transfer Layer Security). TLS yang merupakan pengembangan SSL tidak luput juga dari serangan pihak ketiga, serangan tersebut dinamakan Padding Oracle On Downgraded Legacy Encryption (POODLE) yang memanfaatkan layanan yang dimiliki TLS yaitu Downgrade dance yang artinya ada penurunan tingkat keamanan dalam hal ini TLS ke protocol yang lebih

rendah. Saat ini solusi untuk terhindar dari serangan POODLE adalah dengan menonaktifkan SSL dan hanya menggunakan TLS sebagai pengamanannya. Namun dengan menonaktifkan SSL pasti memiliki dampak tersendiri ketika client yang terhubung hanya mendukung SSL ( Tehupeiory, Nardi, dan Dian W Chandra, 2016).

Dalam Implementasinya VPN (Virtual Privet network) dibagi menjadi dua jenis yaitu remote access dan site-to-site VPN, VPN Remote access merupakan suatu cara meremote server atau host privet melalui jaringan public dengan aman. Sedangkan VPN siteto-site digunakan untuk menghubungkan dua tempat yang berjauhan, misal antara sekolah satu dengan sekolah lainnya (Fatoni, dan Dedi Irawan, 2015).

Dalam penelitian ini juga didasari oleh pengembang yang sudah melakukan penelitian dalam membangun FTP dengan SSL yang di lakukan oleh Molavi Arman berjudul Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer, dengan adanya penelitian tersebut, peneliti akan menyederhanakan dan penambahan sedikit pengembangan yang sebelumnya menggunakan Ftp server dengan konfigurasi ssl, apache, php dan maria db, , apache atau mariadb. Dimana dalam pengembangan ini menggunakansistem mekanisme yang diberikan SSL langsung ke dalam pengamanan koneksi antara FTP Client dan FTP Server. Yang semula ProFTPD berjalan pada protocol yang tidak terlindungi di dalam port 21, kemudian dengan OpenSSL ini di amankan agar data dapat sampai ke tujuan secara aman dan pemanfaatan Point-to-Point Tunneling Protocol (PPTP) suatu protokol jaringan yang bisa memungkinkan client dalam pengiriman data secara aman melalui remote client kepada server sekolah dibangunnya suatu virtual private network (VPN)

### 2.2.1 Keamanan FTP

FTP sebenarnya cara yang tidak aman dalam mentransfer suatu file karena file dikirimkan tanpa di-enkripsi terlebih dahulu tetapi melalui clear text. Mode text yang dipakai untuk transfer data adalah format ASCII atau format binary. Secara default, FTP menggunakan mode ASCII dalamtransfer data.

Karenapengirimannya tanpa enkripsi, username, password, data yang di transfer, maupun perintah yang dikirim dapat di sniffing oleh orang dengan menggunakan protocol analyzer (sniffer). Solusi yang digunakan adalah dengan menggunakan SFTP (SSH FTP) yaitu FTP yang berbasis pada SSH atau menggunakan FTPS (FTP over SSL) sehingga data yang dikirim terlebih dahulu di enkripsi.

## 2.3. FTPS (FTP Secure)

Karena transfer data pada layanan FTP tidak memiliki enkripsi dan sangat beresiko, maka dibuat FTPS sebagai solusi masalah tersebut. Dalam FTPS, server perlu memiliki sertifikat sertifikat keamanan dan software tambahan, yaitu SSL untuk mengamankan layanan FTP. FTPS atau biasa disebut FTP Secure adalah bentuk keamanan dari FTP, dimana akan menggunakan bantuan enkripsi SSL untuk melakukan transfer data. Karena sudah banyaknya tools yang beredar di internet untuk memonitoring kegiatan transfer data dengan FTP, maka disarankan melakukan pengamanan server ftp kita salah satunya menggunakan FTPS ini

Dikarenakan security pada FTP sangat beresiko karena tidak di encrypt maka diusulkanlah dalam RFC 2228 untuk melindungi data FTP saat dikirimkan melalui jaringan menggunakan enkripsi SSL.

Security

1. FTPS implicit SSL
2. FTPS Explicit SSL

*FTPS Implicit SSL*

1. Implicit SSL membutuhkan SSL session untuk menghubungkan antara client dan server sebelum terjadi pertukaran data.
2. Setiap koneksi yang dibuat oleh client tanpa SSL akan di tolak oleh server.
3. SSL implicit berjalan diatas port 990.

*FTPS Explicit SSL*

1. Di dalam *Explicit SSL mode*, client dan server bernegosiasi tentang level proteksi yang digunakan.
2. Server akan menawarkan *unencrypted FTP* atau *encrypted FTPS*

*session* dalam sebuah port.

3. Session yang dibentuk ketika client melakukan koneksi pertama adalah *unencrypted.*
4. Sebelum mengirimkan *user credentials,* client akan meminta kepada Server untuk menukar command channel ke SSL encrypted channel dengan mengirimkan perintah*AUTH TLS* atau *AUTH SSLcommand.*
5. Setelah berhasil melakukan konfigurasi SSL channel maka client akan mengirimkan user credentials ke FTP server.

Firewall

- Server mengijinkan koneksi masuk pada port 21 atau 990

dan PASSIVE on-demand port antara 2000-2500 .

- Client mengijinkan koneksi keluar pada port 21 dan passive sama seperti server.

## 2.4 Pengertian Secure Socket Layer(SSL)

SSL (Secure Socket Layer) adalah cara untuk sebuah website untuk membangun koneksi yang aman (terenkripsi) antara webserver (website) dengan client (Browser) atau antara mail server dengan mail client. Sehingga koneksi antara *client* dan *server* dapat berjalan secara aman dari pihak lain yang tidak berkepentingan.Setiap kali seorang pengunjung web mengunjungi situs yang menggunakan teknologi SSL, *website* akan menciptakan sebuah link yang terenkripsi antara sesi browser mereka dan web server. SSL adalah standar industry/protokol untuk komunikasi web yang aman dan digunakan untuk melindungi jutaan transaksi online setiap hari. SSL memungkinkan informasi sensitif seperti data kartu kredit,username,password dan informasi penting ditransmisikan cari server ke client atau sebaliknya dengan aman karena data yang dikirim akan diaca (dienkripsi). Web server harus memiliki sertifikat SSL sebelum dapat membuat koneksi SSL. Ketika seseorang mengaktifkan protokol SSL di server web mereka, mereka diminta untuk menjawab pertanyaan yang akan membangun identitas mereka. Pertanyaan meminta informasi tentang kedua situs

dan perusahaan. Setelah sertifikat SSL yang diminta, server web menciptakan dua kunci kriptografi, yaitu *Public Key* dan *Private Key.*

- ***Public key*** akan diberikan ke browser bersama dengan certificate ketika koneksi terenkripsi (secure connection)antara browser dan server terbentuk ,Publilc key ini akan digunakan oleh browser untuk mengenkripsi data yang yang akan dikirim ke server.
- ***Private Key*** akan digunakan oleh server untuk mendecrypt informasi terenkripsi dari browser, Private key ini sifatnya sangat rahasia dan tidak ada yang boleh tau (bocor) karena kunci ini yang digunakan untuk membongkar enkripsi data dari dan ke server.

### 2.4.1 Proses enkripsi menggunakan SSL

1. Client /Browser meminta koneksi SSL (SSL Hello)
2. Server membalas permintaan dengan mengirimkan SSL Certificate yang berisi Public key
3. Client menerima dan memfalidasi keabsahan certificate tersebut (ngecek pihak CA yang menandatangi,masa berlaku,owner dll)
4. Client membuat Symmetric Encryption key (sering disebut session key) dan meng enkripsi session key dengan public key yang ada di dalam certificate lalu mengirimkan nya ke server.
5. Server medekripsi dengan private key data dari client yang berisi symmetric session key, dan menggukanan key tersebut untuk mengirim data dari server ke client . koneksi SSL pun terbentuk

## 2.5 Definisi SSL Certificate

SSL pada SSL Certificate merupakan singkatan dari “Secure Socket Layer”. SSL ini merupakan teknologi yang menyediakan link session yang aman antara pengunjung atau web visitor dari browser dan website Anda. Pengaruhnya, semua komunikasi yang terjadi dapat ditransmisi lewat enkripsi sehingga komunikasi aman dari pihak ketiga. SSL juga digunakan untuk melakukan transmisi bagi secure email, secure files, dan berbagai bentuk informasi lainnya yang perlu diamankan.

Sebuah SSL Certificate adalah digital computer file berupa potongan kode yang pada dasarnya memiliki dua fungsi spesifik berikut:

1. Authentication and Verification

   SSL Certification mengandung informasi tentang keaslian dari detail-detail yang ada pada identitas seseorang, sebuah bisnis, maupun sebuah website. Jika aman, akan ditampilkan pada web visitor Anda lewat padlock symbol (gambar gembok) atau trust mark pada browser (Salah satu contohnya adalah Dewaweb yang menggunakan Norton Symantec, terdapat Norton Secured Seal). Kriteria yang digunakan oleh Certificate Authorities adalah apakah SSL Certification sudah termasuk Extended Validation (EV), SSL Certification paling terpercaya.

2. Data Encryption

   SSL Certificate juga dapat melakukan encyptrion di mana informasi-informasi yang tergolong data sensitif yang dipertukarkan lewat website yang ada tidak dapat diintervensi atau dibaca oleh pihak ketiga (pihak yang tak seharusnya memantau pertukaran pesan atau info yang ada, selain penerima yang diharapkan pengirim).

Bila Anda kesulitan memahaminya, kami akan memberi analogi sederhana seperti pada kehidupan sehari-hari di mana paspor atau dokumen yang berisi identitas kita. Data-datanya pasti hanya dapat dikeluarkan secara resmi oleh para pejabat atau instansi pemerintahan yang berwenang. Selain sumber itu, bisa jadi keasliannya diragukan (otentik atau tindakanya). SSL Certificate ini paling dapat diandalkan kredibilitasnya bila dikeluarkan oleh Certificate Authority (CA) yang terpercaya. Saat ini terdapat 3 CA besar yang telah mengeluarkan 3/4 sertifikat SSL yang ada di seluruh dunia, yakni: Comodo, Symantec, dan GoDaddy. CA ini perlu mengikuti aturan dan kebijakan ketat yang sudah terstandar soal siapa atau website mana yang layak atau tak layak mendapat SSL Certificate ini.

### 2.5.1 Manfaat SSL Certificate

Setelah Anda mengetahui definisi dan sedikit sejarah dari SSL, Anda mungkin ingin tahu lebih lagi soal kegunaan SSL Certificate. Berikut adalah manfaat-manfaatnya:

- Encrypted Communication dan Data

  Apakah web visitor atau customer Anda harus login dengan alamat email dan memasukkan beberapa informasi atau data sensitif seperti identitas atau nomor kartu kredit pada website Anda? Jika jawabannya ya, maka Anda perlu SSL Certification. Karena tanpa SSL, para peretas akan sangat mudah mengintervensi jalur komunikasi yang ada antara klien dengan server. Anda pasti tidak mau itu terjadi pada para pengguna website Anda.

- Performance dan HTTP/2

  Sekarang ini, para pengguna internet mulai beralih ke versi baru dari HTTP, yaitu HTTP/2. Hal ini disebabkan oleh keunggulannya yaitu setelah melalui beberapa perbaikan menjadi lebih bagus kinerjanya dibanding HTTP sebelumnya. Peningkatan yang dihasilkan sekitar 50-70% lebih baik dibanding situs yang melalui HTTP/1.1. Lalu apa hubungannya dengan SSL? Jika Anda hendak memanfaatkan HTTP/2 untuk meningkatkan performa website Anda seperti yang telah kami sebutkan tadi, Anda perlu SSL Certificate. Seluruh server Dewaweb saat ini sudah support HTTP/2 sehingga setiap website yang menggunakan sertifikat SSL bahkan SSL gratis sekalipun akan merasakan performa maksimal pada websitenya.

- SEO dan Ranking di Google

  Pada tahun 2014 lalu, Google sempat mengumumkan bahwa HTTPS menjadi salah satu faktor ranking di mesin penelusurnya. Karena hal itu, banyak pengelola website yang mengalihkan websitenya dari HTTP menjadi HTTPS. Mereka tentu tidak ingin mendapatkan penalti dari Google. Penalti ini dapat menurunkan peringkat website mereka di SERP atau halaman hasil pencarian Google, yang juga dapat berdampak pada kecilnya kemungkinan website mereka mendapat visitor dari browser yang

dipakai banyak orang itu. Brian Dean, seorang ahli di bidang SEO, sempat melakukan penelitian terhadap 1 juta hasil pencarian dan menemukan fakta bahwa korelasi HTTPS dengan Google Rank itu benar. Tetapi jangan khawatir, terkait itu juga, sebelumnya kami telah membuat panduan lebih lengkap agar Anda dapat membuat konten yang berperingkat tinggi dan terhindar dari penalti Google .

- Membangun Kepercayaan Klien

  Berhubungan dengan manfaat-manfaat yang telah kami infokan sebelumnya di atas, SSL Certificate dapat menolong bisnis Anda bertumbuh dengan lebih baik. Bagaimana caranya? SSL Certificate ini membangun kepercayaan di antara para pengguna atau klien Anda.

### 2.5.2 Jenis-Jenis SSL Certificate

Ada sejumlah SSL Certificate yang berbeda yang ada di pasaran saat ini. Jenis pertama SSL Certificate adalah sertifikat yang ditandatangani sendiri. Sesuai namanya, ini adalah sertifikat yang dihasilkan untuk keperluan internal dan tidak dikeluarkan oleh CA. Karena pemilik situs membuat sertifikat mereka sendiri, maka pemilik situs tersebut tidak memiliki sertifikat sendiri yang sama kualitasnya seperti SSL Certificate yang terotentikasi dan terverifikasi yang dikeluarkan oleh CA.

- Domain Validated Certificate dianggap sebagai SSL Certificate tingkat pemula dan bisa dikeluarkan dengan cepat atau mudah. Satu-satunya cara pemeriksaan verifikasi yang dilakukan adalah dengan memastikan bahwa si pemohon memiliki domain (alamat website) di mana mereka berencana untuk menerapkan SSL Certificate. Tidak ada pemeriksaan tambahan yang dilakukan untuk memastikan apakah si pemilik domain memiliki bisnis yang valid atau sesuai standar.
- Fully Authenticated SSL Certificate adalah langkah pertama untuk mendapatkan keamanan online yang maksimal demi membangun kepercayaan klien Anda. Walaupun waktu yang dibutuhkan sedikit lebih

lama untuk mengeluarkan sertifikat ini, sertifikat ini bisa saja diberikan begitu perusahaan Anda melewati sejumlah prosedur validasi dan pemeriksaan untuk mengkonfirmasi keberadaan bisnis Anda, kepemilikan domain, dan wewenang pengguna untuk mengajukan sertifikat.

### 2.5.3 Cara Kerja SSL Certificate

Dengan cara yang sama seperti Anda mengunci dan membuka gembok di pagar rumah Anda dengan menggunakan kunci, encryption ini digunakan sebagai kunci untuk mengunci dan membuka kunci informasi Anda. Jika Anda tidak memiliki kunci yang benar, maka Anda tidak bisa membuka informasinya.

Setiap sesi SSL terdiri dari dua kunci:

- Kunci publik, yang digunakan untuk mengenkripsi (mengacak) informasinya.
- Kunci privat, yang digunakan untuk mendekripsi (un-scramble) informasi dan mengembalikannya ke format aslinya lagi sehingga bisa dibaca.

  Proses: Setiap SSL Certificate yang dikeluarkan untuk jadi entitas yang diverifikasi CA saat dikeluarkan bagi domain server dan website tertentu.

  Bila seseorang menggunakan browser mereka untuk menavigasi ke alamat sebuah website dengan SSL Certificate, SSL Handshake (selayaknya jabat tangan ketika pertemuan pertama Anda terjadi di dunia nyata) terjadi antara browser dan server Anda. Informasi diminta dari server – yang kemudian dibuat terlihat oleh orang yang berada di dalam jalurnya. Lalu, jendela browser Anda akan meninjau sebuah perubahan untuk mengetahui bahwa sesi yang aman sudah mulai dilakukan (pada proses ini, trusted mark akan muncul). Jika Anda mengklik trusted mark-nya, Anda akan melihat informasi tambahan seperti masa berlakunya SSL Certificate domain tersebut, jenis SSL Certificate, dan siapa yang mengeluarkan CA. Semua ini berarti bahwa tautan aman ketika sesi itu

sedang berjalan, dengan session key yang unik (berbeda-beda tiap sesi), maka komunikasi yang aman bisa dimulai.

### 2.5.4 Cara Mengetahui Sebuah Website Sudah SSL Certified

Ada beberapa cara untuk mengetahui apakah sebuah website telah SSL Certified yaitu :

- Situs web standar tanpa keamanan SSL menampilkan “http: //” sebelum situs web alamat di bilah alamat browser Moniker ini singkatan dari “Hypertext Transfer Protocol “. Ini merupakan cara konvensional untuk mengirimkan informasi Internet. Namun, sebuah situs web yang diamankan dengan SSL Certificate kini akan menampilkan “https: //” sebelum alamatnya. HTTPS ini seperti yang telah disebutkan sebelumnya, adalah singkatan dari “Secure HTTP.”
- Anda juga akan melihat simbol gembok di bagian atas atau bawah browser Internet (hal ini tergantung pada browser yang Anda gunakan).
- Seringkali, Anda juga akan melihat trusted mark yang ditampilkan pada situs Anda sendiri. Contohnya, pada pelanggan Symantec yang menggunakan tanda kepercayaan Norton Secured Seal di situs web mereka. Saat Anda klik Norton Secured Seal atau simbol gembok di halamannya, ia akan menampilkan detail sertifikat dengan semua informasi perusahaan yang telah diverifikasi dan diautentikasi oleh CA.
- Dengan mengklik gembok tertutup di jendela browser, atau tanda kepercayaan SSL tertentu, pengunjung situs dapat melihat nama organisasi yang sudah diautentikasi. Di browser dengan keamanan tinggi, nama organisasi yang diautentikasi ditampilkan dengan jelas dan bilah alamatnya menjadi hijau saat SSL Certificate Extended Validation (EV) terdeteksi. Jika informasinya tidak cocok, atau sertifikatnya sudah kedaluwarsa, browser akan menampilkan pesan bahwa terjadi kesalahan atau peringatan.

### 2.5.5 Instalasi SSL Certificate

Karena panduan ini tidak dimaksudkan untuk menunjukkan bagaimana menerapkan SSL Certificate secara teknis (yang bisa menjadi topik untuk keseluruhan posting yang baru di blog kami), kami akan menjelaskan langkah-langkah dan tindakan secara garis besar yang harus Anda lakukan tanpa membahas hal-hal teknisnya.

Inilah yang harus Anda perhatikan saat melakukan instalasi SSL Certificate:

- Anda perlu memahami jenis SSL Certificate mana yang sesuai untuk website Anda baru kemudian membelinya.
- Anda perlu memasang SSL Certificate yang sudah Anda beli pada situs Anda
- Anda perlu menyiapkan 301 Redirects dari HTTP ke HTTPS, sesuai standar kini
- Anda harus benar-benar menguji situs web Anda apakah ada tautan rusak dan mungkin juga ada masalah mixed content
- Anda dapat menemukan SSL Certificate dari vendor SSL Certificate yang ada di pasaran, atau seringnya orang-orang langsung saja meminta penyedia hosting mereka untuk melakukan instalasi pada website mereka. Ada ratusan website tempat di mana Anda bisa membeli sertifikat Anda sendiri tetapi cobalah menggunakan jasa yang telah terpercaya.

Berikut adalah informasi tambahan yang kami berikan terkait instalasi SSL Certificate:

1. Anda bisa meminta penyedia hosting Anda. Kalau penyedia hosting Anda menyediakan layanan seperti ini dan penyedia hosting Anda dapat melakukannya buat Anda, Anda sangat beruntung! Catatan: tidak semua penyedia layanan hosting menawarkan layanan seperti itu, apalagi penyedia hosting yang belum disertifikasi. Jadi jangan marah apabila hosting Anda tidak memberikannya kepada Anda. Mungkin saja mereka mulai memikirkan untuk mengubah layanan penyedia hosting mereka

menjadi lebih profesional. Dewaweb sendiri telah menjadi layanan hosting bersertifikat yang cepat dan aman sekaligus menyediakan bantuan untuk instalasi SSL Certificate ini. Anda dapat membaca sampai akhir artikel, untuk langsung ke halaman produk SSL Certificate dari kami.

2. Anda bisa belajar dan melakukannya sendiri tetapi cobalah untuk berhati-hati. Hal ini karena Anda bisa "merusak situs Anda" dengan sangat buruk jika hal-hal atau langkah instalasi tidak dilakukan dengan benar.

Terakhir, ini adalah info tambahan yang harus anda pikirkan (dan tidak boleh lupa) saat pindah ke HTTPS. Berikut adalah daftar hal-hal yang bisa saja terjadi ketika Anda mengubah website Anda dari HTTP ke HTTPS:

- Lalu lintas turun untuk sementara, bahkan secara signifikan, tapi cobalah untuk tenang. Hal ini hanya sementara.
- Jangan lupakan CDN Anda. jika Anda menggunakan CDN, Anda perlu memastikan bahwa CDN Anda mendukung HTTPS yang ada.
- Anda akan mengalami beberapa link yang rusak: semakin banyak feature link di website atau eCommerce Anda, semakin tinggi pula kemungkinan beberapa dari mereka mungkin rusak setelah beralih ke HTTPS. Perbaiki itu dengan memanfaatkan 301 Redirect. Hal yang sama bisa terjadi pada link ke gambar Anda, jadi antisipasi apabila hal itu terjadi, coba untuk bersiap-siap terlebih dahulu.
- Jangan lupa untuk men-tweak Google Analytics demi mengumpulkan data dengan benar di situs Anda kembali (beralih ke HTTPS sebagai domain default).
- Tambahkan situs web HTTPS Anda ke Google Console lagi dan kirimkan ulang sitemap Anda yang baru.
-

## 2.6 Pengertian Linux Debian

Linux Debian adalah sistem operasi komputer yang tersusun dari paket-paket perangkat lunak yang dirilis sebagai perangkat lunak bebas dan terbuka dengan lisensi mayoritas *GNU General Public License* dan lisensi perangkat

lunak bebas lainnya. Debian GNU/Linux memuat perkakas sistem operasi GNU dan kernel Linux merupakan distribusi Linux yang populer dan berpengaruh. Debian didistribusikan dengan akses ke repositori dengan ribuan paket perangkat lunak yang siap untuk instalasi dan digunakan.

Debian terkenal dengan sikap tegas pada filosofi dari Unix dan perangkat lunak bebas. Debian dapat digunakan pada beragam perangkat keras, mulai dari komputer jinjing dan *desktop* hingga telepon dan server. Debian fokus pada kestabilan dan keamanan. Debian banyak digunakan sebagai basis dari banyak distribusi GNU/Linux lainnya. Sistem operasi Debian merupakan gabungan dari perangkat lunak yang dikembangkan dengan lisensi GNU, dan utamanya menggunakan kernel Linux, sehingga populer dengan nama Debian GNU/Linux. Sistem operasi Debian yang menggunakan kernel Linux merupakan salah satu distro Linux yang populer dengan kestabilannya. Dengan memperhitungkan distro berbasis Debian, seperti Ubuntu, Xubuntu, Knoppix, Mint, dan sebagainya, maka Debian merupakan distro Linux yang paling banyak digunakan di dunia.[4]

Proyek Debian ditata kelola oleh *the Debian Constitution* dan *the Social Contract* yang menetapkan struktur tata kelola dari proyek secara eksplisit berikut menyatakan tujuan dari proyek yaitu pengembangan sebuah sistem operasi Fitur yang menonjol dari Debian adalah sistem manajemen APT, repositori dengan jumlah paket yang banyak, kebijakan paket yang ketat, dan kualitas rilis yang terjaga. Praktik ini memungkinkan pemutakhiran yang sederhana antar rilis, begitupun untuk penghapusan paket. Standar instalasi Debian menggunakan lingkungan dekstop GNOME.

CD sisanya, yang terbagi dalam 5 DVD atau 30 CD, memuat paket yang tersedia dan tidak dibutuhkan untuk instalasi standar. Metode instalasi lainnya adalah menggunakan CD net install yang ukurannya lebih kecil daripada CD/DVD instalasi normal. Di dalamnya memuat paket minimum untuk memulai instalasi dan mengunduh paket yang dipilih saat instalasi menggunakan APT (memerlukan koneksi internet).[11] CD/DVD tersebut dapat dengan bebas diunduh melalui web, BitTorrent, jigdo, atau membelinya dari penjual.[12]

## 2.7 Pengertian VirtualBox

Virtualbox adalah software virtualisasi untuk menginstall sebuah OS “Operating System”, kita tahu bahwa arti dari kata virtuallilsasi merujuk pada kamus Oxford adalah “Convert (something) to a computer-generated simulation of reality” yang artinya Mengubah/mengkonversi (sesuatu) ke bentuk simulasi dari bentuk yang nyata atau real. Nah jadi buat para agan agan yang mau coba-coba buat latihan mengingstall OS, tidak usah repot-repot harus menginstall ulang PC/Laptop agan (ribetlah) hehe, kita cuma perlu software Virtualbox ini untuk coba-coba atau belajar menginstall sebuah Operating System.

### 2.7.1 Fungsi dari Virtualbox :

1. Mencoba operating system yang berbeda dengan operating system utama
2. Mencoba operating system yang baru rilis atau masih dalam tahap uji
3. Mencoba untuk membuat sebuah simulasi jaringan dan
4. Mungkin juga untuk mencoba simulasi menguji sebuah security, entah itu OS ataupun website

### 2.7.2 Manfaat Menggunakan Virtualbox :

1. Dapat bermanfaat bagi kaum awam untuk belajar menginstall operating system, tanpa perlu mengubah atau mengcopykan data data yang ada di hardisk
2. Dapat menginstall beberapa operating system secara Cuma-Cuma tanpa harus mempermanent-kannya ke dalam hardisk
3. Hemat uang, dalam arti tidak perlu membeli hardware-hardware atau computer baru untuk memakai banyak operating system

## 2.8 Pengertian Filezilla

FileZilla atau juga dikenal dengan sebutan FileZilla Client, adalah salah satu software FTP gratis, open source, cross-platform. Binari tersedia untuk Windows, Linux, dan Mac OS X. Software ini mendukung FTP, SFTP, dan FTPS (FTP di SSL/TLS). Sejak 5 Maret 2009, software ini adalah software kelima yang paling banyak diunduh sepanjang masa dari SourceForge.net.

FileZilla Server adalah produk lain dari FileZilla Client. Ini adalah server FTP yang didukung oleh proyek yang sama dan fitur-fitur dukungan untuk FTP melalui SSL atau TLS. Kode sumber FileZilla ditaruh pada SourceForge.net. Proyek ini tampil sebagai "Proyek Bulan Ini" pada bulan November 2003. Pada bulan Desember 2017, pengguna FileZilla mengkritik bahwa SourceForge dan pengembang FileZilla membundel pemasang aplikasi dengan perangkat lunak berbahaya di aplikasi tersebut.

Perangkat lunak komputer ini memiliki kelebihan pada kecepatan dan kemudahannya dalam melakukan transfer file. Jendela aplikasi terbagi menjadi dua, satu untuk menampilkan file dan folder di komputer lokal, dan satu lagi untuk menampilkan file dan folder di komputer server. Anda cukup melakukan drag dan drop untuk mentransfer file dari komputer ke server jaringan/internet, atau sebaliknya. FileZilla juga memungkinkan Anda melakukan koneksi ulang ke server yang terakhir Anda akses sebelumnya, cukup dengan menekan satu tombol. Program FileZilla banyak diaplikasikan dan digunakan oleh kalangan pengguna jaringan komputer dan internet.

FileZilla merupakan software gratis. FileZilla dapat dijalankan di sistem operasi Windows XP, Windows Vista, Windows 7, juga tersedia untuk Linux dsn Mac OS. Untuk menginstall versi terbaru program ini, komputer Windows Anda cukup memiliki harddisk dengan kapasitas kosong minimal 10 MB.

- Site manager (Manajer situs) ini memperbolehkan pengguna untuk mengatur daftar situs FTP beserta data koneksinya, seperti nomor port, protokol, dan apakah akan memakai log anonim atau normal. Untuk log normal, nama pengguna dan kata sandinya akan disimpan. Penyimpanan kata sandi adalah opsional.

- Message log (Log pesan) di bagian atas jendela. Fitur ini memperlihatkan output berjenis konsol (console-type) yang memperlihatkan intruksi yang dikirim oleh FileZilla dan respon yang diterima dari server.
- File and folder view di bawah pesan log (Message log), menyajikan sebuah bentuk grafis antarmuka untuk FTP. Pengguna dapat menavigasi folder serta melihat dan mengubah isinya pada komputer lokal dan server dengan menggunakan tampilan antarmuka gaya Explorer. Pengguna dapat men-drag dan drop file antara komputer lokal dan server.
- Transfer queue (Transfer antrian) Ditampilkan di sepanjang bagian bawah jendela, menunjukkan status real-time setiap antrian atau transfer file yang aktif.

## 2.9 Router

Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch Switchmerupakan penghubung beberapa alat untuk membentuk suatu Local Area Network (LAN). Sebagai ilustrasi perbedaan fungsi dari router dan switch merupakan suatu jalanan, dan router merupakan penghubung antar jalan. Masing-masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu. Dengan cara yang sama, switch menghubungkan berbagai macam alat, dimana masing-masing alat memiliki alamat IP sendiri pada sebuah LAN. Komunitas eLearning IlmuKomputer.Com Copyright © 2003-2007 IlmuKomputer.Com Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan IP Router. Selain IP Router, ada lagiAppleTalk Router, dan masih ada beberapa jenis router lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP.

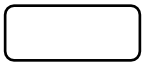
Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut denganinternetwork atau untuk membagi sebuah jaringan besar ke dalam beberapa ubnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan

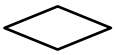
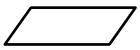
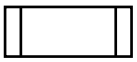
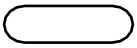
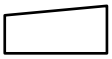
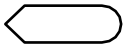
media yang berbeda (seperti halnya router wireless yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel UTP), atau berbeda arsistektur jaringan, seperti halnya dari Ethernet ke token ring. Router juga dapat digunakan untuk menghubungkan LAN ke sebuah layanan telekomunikasi seperti halnya telekomunikasi leased line atau Digital Subsciber Line (DSL). Router yang digunakan untuk menghubungkan LAN ke sebuah koneksi leased line seperti T1, atau T3, sering disebut sebagai access server. Sementara itu, router yang digunakan untuk menghubungkan jaringan lokal ke sebuah koneksi DSL disebut juga dengan DSL router. Router-routerjenis tersebut umumnya memiliki fungsi firewall untuk melakukan penapisan paket berdasarkan alamat sumber dan alamat tujuan paket tersebut, meski beberapa router tidak memilikinya. Router yang memiliki fitur penapisan paket disebut juga dengan packet-filtering raouter. Router umumnya memblokir lalu lintas data yang dipancarkan secara broadcast sehingga dapat mencegah adanya broadcast storm yang mampu memperlambat kinerja jaringan.

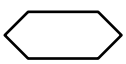
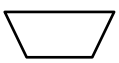
## 2.10 *Flowchart*

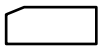
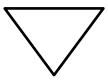
*Flowchart* merupakan sebuah diagram dengan simbol-simbol grafis yang menyatakan tipe operasi program yang berbeda. Sebagai *representasi* dari sebuah program, *flowchart* maupun algoritma dapat menjadi alat bantu untuk memudahkan perancangan alur urutan logika suatu program, memudahkan pelacakkan sumber kesalahan program, dan alat bantu untuk menerangkan logika program (Budiutomo, 2017). Simbol *Flowchart* dapat dilihat pada tabel 2.10.

**Tabel 2.10 Simbol *Flowchart***

| No. | Simbol | Nama Simbol | Keterangan |
|---|---|---|---|
| 1. |  | *Alternate Process* | Menyatakan segala jenis operasi yang diproses dengan menggunakan mesin yang memiliki *keyboard.* |

| | | | |
|---|---|---|---|
| 2. |  | *Decision* | suatu penyelesaian kondisi dalam program. |
| 3. |  | *Data* | Mewakili data *input* atau *output.* |
| 4. |  | *Predefined Process* | Suatu operasi yang rinciannya di tunjukkan di tempat lain. |
| 5. |  | *Document* | *Document input* dan *output* baik untuk proses manual, mekanik atau komputer. |
| 6. |  | *Terminator* | Untuk menunjukkan awal dan akhir dari suatu proses. |
| 7. |  | *Process* | proses dari operasi program komputer. |
| 8. |  | *Manual Input* | *Input* yang menggunakan *online* keyboard. |
| 9. |  | *Conector* | Penghubung ke halaman yang masih sama . |
| 10. |  | *Off-Page Connector* | Penghubung ke halaman lain. |
| 11. |  | *Display* | *Output* yang ditampilkan di monitor. |
| 12. |  | *Delay* | Menunjukkan penundaan. |

| | | | |
|---|---|---|---|
| 13. |  | *Preparation* | Memberi nilai awal suatu besaran. |
| 14. |  | *Manual Operation* | Pekerjaan manual. |

| | | | |
|---|---|---|---|
| 15. |  | *Card* | *Input* atau *output* yang menggunakan kartu. |
| 16. |  | *Punch Tape* | *Input* atau *output* menggunakan pita kertas berlubang. |
| 17. |  | *Merge* | Penggabungan atau penyimpanan beberapa proses atau informasi sebagai salah satu. |
| 18. |  | *Dirrect Access Storage* | *Input* atau *output* menggunakan drum magnetik. |
| 19. |  | *Magnetic Disk* | *Input* atau *output* menggunakan *hard disk.* |
| 20. |  | *Sequential Access Storage* | *Input* atau *output* menggunakan pita magnetik. |
| 21. |  | *Sort* | Proses pengurutan data di luar komputer. |
| 22. |  | *Stored Data* | *Input* atau *output* menggunakan *diskette.* |
| 23. |  | *Extract* | Proses dalam jalur paralel. |
| 24. |  | *Arrow* | Menyatakan jalan atau arus suatu proses. |
| 25. |  | *Summing Junction* | Untuk berkumpul beberapa cabang sebagai proses tunggal. |
| 26. |  | *Or* | Proses menyimpang dalam dua proses. |