BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi yang cukup pesat dari waktu ke waktu membuat pekerjaan yang dilakukan manusia pada umumnya dapat diselesaikan dengan cepat. Dan untuk lebih memudahkan di perlukan juga jaringan dan jaringan komputer. Jaringan komputer sudah menjadi kebutuhan sangat penting bagi institusi yang menerapkan pengolahan data berbasis komputer. Semua data yang berkaitandengan institusi tersebut disimpan dalam komputer. Semua kegiatan yangberkaitan dengan transaksi harian institusi didasarkan pada data tersebut. Kebutuhan jaringan komputer semakin terasa apabila data diletakkan pada komputer-komputer yang berbeda.

Keberadaan jaringan komputer sangat membantu dalam proses penyampaian data dari suatu komputer ke komputer lain. Dalam jaringan juga perlu keamanan sistem keamanan jaringan komputer adalah suatu sistem untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. disini penulis mengimplementasikan DNS Over Https sebagai keamanan jaringan, DNS Over Https adalah DNS melalui HTTPS (DoH) menggunakan HTTPS protokol untuk mengirim dan mengambil kueri dan respons DNS terenkripsi. Protokol DoH telah diterbitkan sebagai standar yang diusulkan oleh *IETF as RFC 8484*. Permintaan dan tanggapan DNS secara historis telah dikirim sebagai teks biasa, berpotensi membahayakan privasi pengguna internet termasuk pengunjung situs web HTTPS

terenkripsi. DoH mencegah calon penyerang dan atau otoritas pemerintah membaca kueri DNS pengguna, dan juga mengubur lalu lintas DNS di *port 443* (port HTTPS standar), di mana sulit untuk membedakan dari lalu lintas terenkripsi lainnya.

Mikrotik adalah sistem operasi Linux base yang diperuntukkan sebagai network router. Mikrotik juga menggunakan sistem operasi berbasis Linux dan menjadi dasar network router. Sistem operasi (OS) ini sangat cocok untuk membangun administrasi jaringan komputer yang berskala kecil hingga besar dan bisa digunakan untuk membuat keamanan jaringan.[1]

Berdasarkan hasil penelitian dalam mengakses internet memang menjadi sebuah masalah bagi mereka yang sering bekerja di luar kantor. Masalahnya dengan mengakses WiFi gratis pada kafe atau mall, justru akan mudah dihack oleh para hacker. Para tangan jahil tersebut bisa mengetahui situs apa yang sedang kita kunjungi dan bahkan tidak jarang mengambil nama pengguna dan sandi milik orang lain. Dalam jaringan diperluakan juga keamanan dan privasi pengguna juga ancaman dari Man in the middle (MITM) dan untuk melindungi pengguna dari itu penulis mengemplemtasikan router mikrotik agar menutup celah dan mengamankan sebuah web.

Adapun dalam pembuatan laporan ini penulis mengambil beberapa dari penelitian antara lain.penelitian Dedy Hariyadi, M. Roykhul Jinan, Nur Seto Bayuaji, Anas Sufi Hasan tahun 2019 dengan judul"Analisis Jaringan Pada Aplikasi Pengamanan Akses Internet."[2], penelitian Taufik Hidayat,Catur Iswahyudi,Suraya tahun 2018 dengan berjudul "Optimalisasi Kinerja Server Menggunakan Manajemen DNS Optimizing Server Performance Using DNS Management"[3], penelitian Yaser M. Banadaki tahun 2020 dengan judul "Detecting Malicious DNS over HTTPS Traffic in Domain Name System using Machine Learning Classifiers"[4] penelitian Sani Muhlison, Kusnawi tahun 2019 dengan judul "Analisa Dan Implementasi DNS SERVER Sebagai FIltering Konten Negatif Menggunakan Metode RPZ (RESPONSE POLICY ZONE)"[5] penelitian Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar,Jordan Holland, Austin Hounsel, Paul Schmit tahun 2019 dengan judul

“How DNS over HTTPS is Reshaping Privacy,Performance, and Policy in the Internet Ecosystem”[6]

Berdasarkan latar belakang di atas penulis merancang manajemen dan keamanan jaringan yang berjudul “**IMPLEMENTASI DOMAIN NAME SERVER OVER PROTOKOL HYPERTEXT TRANSFER PROTOKOL SECURE BERBASIS ROUTER MIKROTIK**”

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, penulis merumuskan masalah sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan DNS over https pada jaringan berbasis router mikrotik?
2. Bagaimana agar terhindar dari situs atau web yang berbahya?
3. Bagaimana menjaga keamanan privasi pengguna di jaringan agar terhindar dari tindakan pencurian data?
4. Bagaimana agar terhidar dari serangan Man-in-the-middle(MITM)?

1.3. Batasan Masalah

Berdasarkan latar belakang diatas, penulis memutuskan masalah sebagai berikut:

1. Implementasi ini di bangun untuk mempermudah pengguna dalam mengakses jaringan dan juga terhindar dari serangan MITM
2. Implementasi ini menggunkan routeros versi 6.47
3. Implementasi ini menggunakan router board mikrotik versi *Mikrotik* Router Indoor RB750r2
4. Implementasi ini menggunakan winbox versi 3.14

1.4. Tujuan dan Manfaat Penelitian

Dari latar belakang dan rumusan masalah penulis mengambil tujuan dan manfaat dari laporan ini adalah sebagai berikut:

1.4.1. Tujuan

Adapun tujuan yang akan di capai dalam penelitian ini antara lain:

1. Untuk melindungi privasi dan keamanan pengguna dengan mencegah serangan Man-in-the-middle(MITM).
2. Untuk membuat jaringan lebih aman dari ancaman kejahatan.
3. Untuk mempermudah pengguna jaringan internet agar tidak terjadi kendala apapun.

1.4.2. Manfaat

Adapun manfaat yang akan di capai dari penelitian ini antara lain:

1. Agar dapat mengimplementasikan DNS Over Https dengan mengguanakan rourteros mikrotik versi.
2. Agar mengakses internet lebih cepat dan privasi *client* lebih aman.
3. Agar trafik pengguna jaringan jadi tidak bisa dipantau atau dialihkan ke situs lain yang berbahaya.

1.5. Sistematika Penulisan

Agar laporan penelitian ini dapat tersusun dengan rapi dan terarah, maka penulisa menyusun secara sistematis sehingga diharapkan tahap-tahap pembahasan pada laporan ini akan jelasa kaitannya antara satu bab dengan bab yang lainnya. Adapun isi dari masing-masing bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, perumusan masalah, manfaat dan tujuan penelitian, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang tinjauan pustaka, menguraikan teori-teori yang mendukung judul, dan mendasari pembahasan secara detail.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang pengertian dari alat bantu yang digunakan untuk mengembangkan suatu jaringan.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang cara-cara pengembangan suatu sistem dengan metode dengan metode penelitian yang digunakan.

BAB V PENUTUP

Dalam bab ini menguraikan tentang kesimpulan dari pembahasan pada bab-bab sebelumnya dan saran dari penulis yang kiranya bermanfaat. Kesimpulan adalah mengemukakan kembali masalah penelitian kemudian menyimpulkan bukti-bukti yang diperoleh dan akhirnya menarik kesimpulan apakah hasil yang didapat (dikerjakan) layak untuk digunakan (diimplementasikan). Saran merupakan manifestasi dari penulis untuk dilaksanakan.