Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dengan IPSEC

Yudhi Nendra Kurniawan - 5024231012

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital saat ini, kebutuhan akan komunikasi data yang aman dan efisien antar jaringan semakin penting, terutama bagi institusi seperti perusahaan, sekolah, dan organisasi yang memiliki banyak cabang atau pengguna. Salah satu teknologi yang digunakan untuk menjembatani komunikasi aman antar lokasi adalah Virtual Private Network (VPN), di mana protokol seperti IPSec dan PPTP berperan dalam menciptakan "terowongan" virtual untuk melindungi pertukaran data dari akses tidak sah. IPSec, dengan fitur enkripsi dan autentikasinya, sangat cocok untuk koneksi site-to-site yang membutuhkan jaminan kerahasiaan dan integritas data. Sementara itu, PPTP memberikan solusi VPN yang lebih sederhana namun masih relevan untuk kebutuhan remote access dalam skala kecil hingga menengah. Di sisi lain, pengelolaan bandwidth juga menjadi tantangan tersendiri, terutama di lingkungan dengan banyak pengguna dan jenis trafik yang beragam. Dalam hal ini, penerapan teknik seperti Queue Tree pada router MikroTik memungkinkan administrator untuk mengalokasikan bandwidth secara terstruktur dan memprioritaskan trafik penting seperti e-learning, akses guru, atau sistem keamanan jaringan. Praktikum ini dirancang agar peserta dapat memahami implementasi langsung dari teknologi VPN dan manajemen bandwidth tersebut, serta menguasai konfigurasi teknis yang sesuai dengan kebutuhan nyata di dunia kerja dan pendidikan.

1.2 Dasar Teori

Dalam pengelolaan jaringan modern, keamanan dan efisiensi penggunaan bandwidth menjadi dua aspek utama yang harus diperhatikan. Untuk menjamin keamanan komunikasi data antar jaringan yang terhubung melalui internet, digunakan teknologi Virtual Private Network (VPN). VPN menciptakan “terowongan” virtual antara dua titik komunikasi sehingga data dapat dikirimkan secara aman dan terlindung dari pihak ketiga. Salah satu protokol VPN yang paling umum digunakan untuk komunikasi antar situs atau cabang adalah IPSec (Internet Protocol Security). IPSec bekerja pada lapisan jaringan (Layer 3 OSI) dan menyediakan tiga fitur utama, yaitu enkripsi untuk menjaga kerahasiaan data, autentikasi untuk memastikan identitas pihak yang terlibat, dan integritas untuk mencegah perubahan data selama transmisi. Dalam implementasinya, IPSec memiliki dua fase negosiasi: IKE (Internet Key Exchange) Phase 1, yang bertugas membentuk Security Association (SA) antara dua peer dan melakukan pertukaran kunci secara aman; serta IKE Phase 2, yang digunakan untuk menyepakati parameter keamanan lanjutan seperti algoritma enkripsi (misalnya AES, 3DES), metode autentikasi (pre-shared key, digital signature), dan masa aktif kunci (lifetime key). IPSec mendukung dua mode kerja, yakni Tunnel Mode yang mengenkripsi keseluruhan paket IP dan cocok untuk site-to-site VPN, serta Transport Mode yang hanya mengenkripsi payload data, cocok untuk host-to-host VPN. Selain IPSec, protokol PPTP (Point-to-Point Tunneling Protocol) juga sering digunakan karena konfigurasi yang sederhana dan kompatibel di banyak sistem operasi, meskipun dari sisi keamanan tidak sekuat IPSec. PPTP bekerja pada lapisan data-link dan menggunakan protokol GRE (Generic Routing Encapsulation) untuk mengenkapsulasi data. Protokol ini banyak digunakan untuk kebutuhan remote access oleh pengguna individu atau organisasi kecil karena kemudahan dalam setup dan dukungan built-in pada sistem operasi seperti Windows. Di samping aspek keamanan, jaringan juga perlu dikelola secara efisien agar trafik penting mendapatkan prioritas, terutama dalam kondisi bandwidth terbatas. Untuk itu, digunakan metode pengaturan bandwidth melalui Queue Tree pada router Mik-

roTik. Queue Tree merupakan fitur manajemen trafik berbasis antrean (queue) yang memungkinkan pembagian bandwidth secara hierarkis, di mana satu antrean induk (parent queue) dapat memiliki beberapa antrean anak (child queue) berdasarkan kategori trafik, IP address, port, atau jenis layanan. Queue Tree memerlukan konfigurasi tambahan berupa mangle rules, yaitu proses menandai koneksi atau paket (packet marking) untuk mengidentifikasi lalu lintas mana yang akan dikenakan aturan bandwidth tertentu. Keunggulan Queue Tree dibandingkan Simple Queue adalah fleksibilitasnya dalam mengelompokkan trafik, menetapkan prioritas (priority), serta mengatur kecepatan maksimum (max-limit) dan jatah minimum (limit-at) untuk setiap antrean. Kombinasi antara VPN sebagai solusi keamanan dan Queue Tree sebagai alat pengendali lalu lintas membuat administrator jaringan mampu membangun sistem yang tidak hanya aman, tetapi juga optimal dari sisi kinerja. Hal ini sangat penting, khususnya di lingkungan pendidikan dan korporasi yang memiliki berbagai jenis trafik seperti e-learning, layanan cloud, CCTV, serta kebutuhan akses guru dan siswa yang berbeda tingkat prioritasnya.

2 Tugas Pendahuluan

1. IPSec adalah protokol keamanan jaringan yang umum digunakan untuk membangun koneksi VPN site-to-site antara dua jaringan berbeda, misalnya antara kantor pusat dan cabang. Proses koneksi ini terbagi dalam dua fase penting: IKE (Internet Key Exchange) Phase 1 dan Phase 2. Fase pertama bertujuan membentuk jalur komunikasi aman dan melakukan pertukaran parameter keamanan seperti algoritma enkripsi (contoh: AES-256), metode autentikasi (pre-shared key), dan parameter kunci Diffie-Hellman serta masa berlaku kunci (lifetime). Setelah fase ini berhasil, maka Phase 2 digunakan untuk menyepakati bagaimana data aktual akan dienkripsi dan ditransmisikan menggunakan protokol seperti ESP (Encapsulation Security Payload). Dalam implementasi MikroTik RouterOS, konfigurasi meliputi penambahan peer, proposal, dan policy IPSec, serta NAT bypass untuk memastikan trafik IPSec tidak terganggu. .

2. Pengaturan bandwidth dengan metode Queue Tree sangat efektif untuk mengelola trafik jaringan secara adil dan terprioritaskan. Dalam studi kasus ini, bandwidth sebesar 100 Mbps dibagi menjadi empat kategori layanan: e-learning (40 Mbps), guru staf (30 Mbps), siswa (20 Mbps), dan CCTV serta update sistem (10 Mbps). Untuk merealisasikan pembagian ini, dibuat satu parent queue dengan bandwidth total, kemudian beberapa child queues yang masing-masing diberi priority berbeda. Sebelum mengatur antrean, dilakukan proses packet marking menggunakan fitur mangle pada MikroTik untuk mengidentifikasi trafik berdasarkan IP, port, atau protokol tertentu. Queue Tree lebih unggul dari Simple Queue dalam hal fleksibilitas dan kemampuan mengelola trafik kompleks

3. Router tanpa firewall berarti tidak ada screening atas lalu lintas yang masuk dan keluar, sehingga jaringan menjadi sangat rentan. Hal ini dapat menyebabkan berbagai risiko seperti downtime jaringan lengkap karena serangan DDoS, infeksi malware, eksploitasi port terbuka, serta pencurian atau kerusakan data bisnis . Sumber dari ITS ASAP dan Minerva bahkan menyebut tanpa firewall, "network downtime" bisa terjadi dan kerugian bisa membahayakan eksistensi bisnis . Diskusi di forum F5 dan DevCentral menambahkan bahwa membuka semua port sama artinya seperti mengundang kerusakan dan ekspos risiko serangan secara langsung

- https://cloudzy.com/knowledge-base/ipsec-site-to-site-vpn-mikrotik/
- https://getlabsdone.com/how-to-configure-ipsec-vpn-site-to-site-on-mikrotik/
- https://help.mikrotik.com/docs/display/ROS/IPsec
- https://wiki.mikrotik.com/wiki/Manual:Queue_Tree_with_Mangle