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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Muhammad Fahri Fadillah - 5024231063

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, kebutuhan akan koneksi jaringan yang aman dan efisien menjadi sangat penting, terutama bagi organisasi yang memiliki kantor pusat dan cabang di lokasi berbeda. Salah satu teknologi yang dapat digunakan untuk menjembatani koneksi antar lokasi secara aman adalah VPN (Virtual Private Network) dengan protokol IPSec. IPSec memungkinkan komunikasi antar jaringan dilakukan melalui "terowongan" terenkripsi, sehingga data yang ditransmisikan tetap aman dari gangguan pihak ketiga.

Di sisi lain, manajemen bandwidth juga menjadi faktor krusial dalam menjaga performa jaringan, khususnya pada institusi seperti sekolah yang harus membagi bandwidth terbatas untuk berbagai kebutuhan seperti e-learning, akses staf, siswa, dan sistem keamanan. Penggunaan metode seperti Queue Tree pada perangkat jaringan MikroTik memungkinkan pengelolaan lalu lintas data secara lebih fleksibel dan presisi, termasuk penentuan prioritas dan pembatasan kecepatan.

1.2 Dasar Teori

Tunneling merupakan teknik yang digunakan untuk mengirimkan data antar jaringan yang berbeda jenis melalui media perantara, dengan cara membungkus (encapsulation) paket data asli ke dalam format baru agar bisa melewati jaringan yang tidak kompatibel secara langsung. Teknik ini memungkinkan komunikasi antar dua titik jaringan yang terpisah tetap berlangsung meskipun melalui jalur berbeda. Salah satu bentuk tunneling yang aman dan sering digunakan adalah melalui protokol IPSec (Internet Protocol Security). IPSec menyediakan mekanisme keamanan pada lapisan jaringan dengan fitur seperti enkripsi, autentikasi, dan integritas data. Fungsinya adalah untuk menjaga kerahasiaan dan keaslian data yang ditransmisikan, serta memastikan data tidak mengalami manipulasi di tengah jalan.

Dalam proses pembentukan koneksi VPN menggunakan IPSec, terdapat dua fase utama dalam proses negosiasi yang dikenal dengan IKE (Internet Key Exchange). Fase pertama (IKE Phase 1) bertujuan untuk membentuk saluran komunikasi yang aman antara dua perangkat, di mana keduanya akan bertukar kunci rahasia dan saling mengenali identitas. Setelah itu, fase kedua (IKE Phase 2) dilakukan untuk menyepakati parameter keamanan yang akan digunakan dalam komunikasi data, seperti algoritma enkripsi (misalnya AES atau 3DES), metode autentikasi (seperti SHA-1 atau SHA-256), serta masa berlaku kunci enkripsi (lifetime key). Mode komunikasi dalam IPSec juga dibedakan menjadi dua, yaitu Tunnel Mode untuk komunikasi antar jaringan dan Transport Mode untuk komunikasi antar host.

Sementara itu, dalam pengelolaan bandwidth jaringan, khususnya pada perangkat MikroTik, dikenal fitur Queue Tree yang memungkinkan pengaturan lalu lintas data secara hierarkis. Queue Tree menggunakan pendekatan parent-child queue, di mana total bandwidth dialokasikan ke parent queue dan dibagi lagi ke child queue berdasarkan kategori lalu lintas, seperti e-learning, akses staf, siswa, dan CCTV. Untuk bisa bekerja secara efektif, Queue Tree membutuhkan proses marking menggunakan fitur mangle, yaitu menandai paket data berdasarkan parameter tertentu seperti alamat IP, port, atau protokol. Setiap antrian (queue) juga bisa diatur dengan nilai prioritas (semakin kecil angkanya, semakin tinggi prioritasnya) serta limitasi bandwidth minimum dan maksimum (limit-at dan max-limit). Dengan manajemen ini, layanan penting seperti VPN dan video conference dapat diutamakan diband-

ingkan layanan yang bersifat sekunder seperti browsing atau streaming. Penggunaan Queue Tree sangat bermanfaat dalam kondisi jaringan yang padat atau ketika bandwidth terbatas dan harus dibagi secara adil dan efisien.

Tugas Pendahuluan

1. **Internet Key Exchange (IKE)** adalah protokol yang digunakan untuk menyusun mekanisme keamanan dalam membangun koneksi IPsec antara dua titik. Protokol ini bertugas menangani negosiasi parameter kriptografi serta autentikasi antar pihak yang terlibat.

    - **Fase IKE Tahap 1:** Pada tahap ini, kedua perangkat akan membentuk kanal komunikasi yang aman untuk menyepakati metode pertukaran kunci dan autentikasi.
    - **Fase IKE Tahap 2:** Setelah fase 1 berhasil, fase ini akan mengatur parameter untuk membentuk tunnel data menggunakan protokol ESP (Encapsulating Security Payload) atau AH (Authentication Header).

    Beberapa parameter penting dalam konfigurasi IKE/IPsec:

    - **Enkripsi:** Metode pengacakan data seperti AES-256 dan Triple DES digunakan untuk menjamin kerahasiaan isi data.
    - **Autentikasi:** Fungsi hash seperti HMAC-SHA256 atau SHA-1 digunakan untuk memastikan keaslian data.
    - **Grup Diffie-Hellman:** Menentukan kekuatan pertukaran kunci, seperti grup 14 (2048-bit).
    - **Waktu Aktif (Lifetime):** Menentukan berapa lama sebuah asosiasi keamanan berlaku, contohnya 1 jam (3600 detik) untuk fase 1.
    - **Mode Tunnel:** Digunakan untuk mengenkapsulasi paket IP asli dalam koneksi antar jaringan.
    - **Pre-Shared Key (PSK):** Kunci rahasia yang telah disepakati dan dimiliki oleh kedua endpoint sebagai bagian dari autentikasi.

    Langkah konfigurasi IPsec site-to-site:

    - Menyusun kebijakan IKE versi 1 (IKEv1 Policy).
    - Menentukan grup tunnel dan parameter autentikasi.
    - Mendefinisikan transform set untuk algoritma keamanan.
    - Membuat daftar akses (access list) untuk mengatur lalu lintas.
    - Membentuk crypto map yang akan digunakan untuk tunnel.
    - Menerapkan crypto map pada interface jaringan yang relevan.

2. **Manajemen Bandwidth dan Prioritas pada Router**

    - **Pengaturan Antrian (Queue):** Konfigurasi bandwidth dibagi menjadi antrian utama (parent) dan beberapa antrian turunan (child). Misalnya, bandwidth total 100 Mbps dapat dialokasikan ke:
        - Layanan e-learning: 40 Mbps

  - Akses guru dan staf: 30 Mbps
  - Pengguna siswa: 20 Mbps
  - Kebutuhan CCTV dan pembaruan sistem: 10 Mbps
- **Marking Paket:** Proses penandaan paket untuk mengelompokkan lalu lintas agar dapat diprioritaskan dan diarahkan sesuai rute yang ditentukan di tabel routing.
- **Prioritas dan Batasan Bandwidth:**
  - E-learning: Prioritas tertinggi (1), dibatasi maksimal 20 Mbps
  - Guru dan staf: Prioritas menengah (2), dibatasi 15 Mbps
  - Siswa: Prioritas rendah (3), dibatasi 10 Mbps
  - CCTV dan update sistem: Prioritas paling rendah (4), dibatasi 5 Mbps