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

Laporan Sementara
Praktikum Jaringan Komputer

VPN QoS

Zaky Ahmad Septyan Pradana - 5024231051

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, kebutuhan akan jaringan yang aman, stabil, dan efisien menjadi sangat krusial, terutama untuk mendukung komunikasi dan pertukaran data antar lokasi yang berjauhan. Teknologi jaringan seperti tunneling, VPN (Virtual Private Network), serta manajemen bandwidth menjadi solusi utama dalam menjawab tantangan ini, baik untuk sektor bisnis, pendidikan, maupun pemerintahan.

Pelaksanaan praktikum ini bertujuan untuk memahami dan mengimplementasikan konfigurasi jaringan menggunakan perangkat Mikrotik, khususnya dalam hal pengelolaan bandwidth dengan Queue Tree serta pengamanan komunikasi data menggunakan protokol IPSec. Permasalahan umum yang sering terjadi dalam jaringan seperti akses internet yang tidak merata, rawannya penyadapan data, hingga inefisiensi alokasi bandwidth, menjadi latar penting perlunya pembelajaran topik ini.

Dengan mempelajari konfigurasi VPN IPSec, peserta praktikum dapat memahami bagaimana membangun koneksi terenkripsi antara dua lokasi jaringan (seperti kantor pusat dan cabang), yang sangat relevan dalam dunia kerja saat ini, di mana remote access dan keamanan data menjadi prioritas utama. Di sisi lain, melalui penerapan Queue Tree, peserta belajar mengatur prioritas trafik jaringan sesuai kebutuhan, misalnya memisahkan jalur akses untuk pembelajaran daring, pegawai, siswa, hingga perangkat CCTV.

Topik-topik ini tidak hanya penting dari sisi teknis, tetapi juga memiliki aplikasi nyata dalam mendesain dan mengelola jaringan modern yang aman, terstruktur, dan efisien. Oleh karena itu, praktikum ini memiliki urgensi tinggi dalam membekali mahasiswa dengan kompetensi praktis dan teoritis yang dapat diterapkan langsung dalam lingkungan kerja profesional.

1.2 Dasar Teori

Jaringan komputer merupakan sistem yang menghubungkan dua atau lebih perangkat komputer untuk saling bertukar data, aplikasi, dan sumber daya. Dalam penerapannya, khususnya pada jaringan luas (Wide Area Network/WAN), transmisi data sering kali harus melewati jaringan publik seperti internet. Hal ini menimbulkan kebutuhan akan mekanisme pengamanan dan pengelolaan lalu lintas data yang efisien. Salah satu teknologi yang dikembangkan untuk menjawab kebutuhan tersebut adalah Virtual Private Network (VPN), yaitu sebuah metode untuk membuat jalur komunikasi pribadi yang aman melalui jaringan publik. VPN memungkinkan dua lokasi jaringan yang berbeda secara geografis untuk terhubung seolah-olah berada dalam satu jaringan lokal.

Salah satu protokol VPN yang populer dan aman adalah Internet Protocol Security (IPSec). IPSec berfungsi sebagai sistem keamanan pada lapisan jaringan yang menyediakan layanan seperti enkripsi, autentikasi, dan integritas data. IPSec bekerja dengan dua protokol utama, yaitu Encapsulation Security Payload (ESP) yang mendukung enkripsi dan autentikasi, serta Authentication Header (AH) yang hanya menyediakan autentikasi dan integritas tanpa enkripsi. Selain itu, terdapat protokol Internet Key Exchange (IKE) yang digunakan untuk pertukaran kunci dan negosiasi parameter keamanan. Proses kerja IPSec terbagi dalam dua fase, yaitu Phase 1 yang membangun jalur aman awal untuk negosiasi kunci, dan Phase 2 yang membuat tunnel untuk pengiriman data. IPSec memiliki dua mode kerja, yaitu Tunnel Mode yang mengenkripsi keseluruhan paket IP dan cocok untuk koneksi antar jaringan (site-to-site), serta Transport Mode yang mengenkripsi hanya bagian payload data dan

digunakan untuk koneksi host-to-host.

Selain aspek keamanan, pengelolaan lalu lintas data atau bandwidth management juga menjadi bagian penting dalam perancangan jaringan. Manajemen bandwidth bertujuan untuk mengalokasikan kapasitas jaringan secara proporsional berdasarkan kebutuhan dan prioritas pengguna. Salah satu fitur unggulan pada perangkat Mikrotik dalam hal ini adalah Queue Tree. Queue Tree merupakan metode manajemen bandwidth yang bersifat hierarkis dengan menggunakan struktur parent dan child. Dalam penerapannya, Queue Tree memungkinkan pembagian bandwidth secara lebih fleksibel, misalnya berdasarkan jenis trafik, alamat IP, port, atau protokol tertentu. Untuk mendukung Queue Tree, diperlukan proses penandaan paket (marking) melalui fitur mangle pada Mikrotik, yang membantu mengidentifikasi dan memisahkan jenis trafik sebelum dialokasikan ke queue tertentu. Setiap queue dapat diatur dengan prioritas berbeda, sehingga layanan penting seperti video conference atau VPN mendapatkan jalur yang lebih cepat dibandingkan aktivitas lain seperti browsing atau streaming.

Penggunaan perangkat Mikrotik dalam praktikum ini sangat relevan karena sistem operasi RouterOS yang dimilikinya mendukung berbagai fitur jaringan modern, mulai dari routing, firewall, VPN, hingga bandwidth management. Oleh karena itu, pemahaman teori-teori dasar ini sangat penting agar peserta praktikum mampu mengimplementasikan konfigurasi jaringan yang aman dan efisien menggunakan VPN IPSec dan Queue Tree, yang keduanya sangat dibutuhkan dalam dunia industri dan lingkungan kerja saat ini.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1 Studi Kasus Konfigurasi VPN IPSec

1.1 Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

- **Phase 1:** Membentuk secure communication channel (ISAKMP SA) dengan autentikasi dan pertukaran kunci (Diffie-Hellman). Menggunakan Main Mode atau Aggressive Mode.
- **Phase 2:** Membentuk IPSec SA untuk transfer data, melalui negosiasi parameter enkripsi dan integritas (ESP/AH). Menggunakan Quick Mode.

1.2 Parameter Keamanan yang Harus Disepakati

- **Algoritma Enkripsi:** AES-256, 3DES
- **Metode Autentikasi:** Pre-shared key (PSK) atau sertifikat
- **Algoritma Hashing:** SHA-1, SHA-256
- **Lifetime Key:** Umumnya 3600 detik

1.3 Contoh Konfigurasi IPSec Router (MikroTik)

```
/ip ipsec peer
add address=192.168.1.2/32 auth-method=pre-shared-key secret="vpnkey" exchange-mode=
    main

/ip ipsec proposal
add name="default" auth-algorithms=sha256 enc-algorithms=aes-256-cbc pfs-group=none

/ip ipsec policy
add src-address=192.168.10.0/24 dst-address=192.168.20.0/24 sa-dst-address
    =192.168.1.2 sa-src-address=192.168.1.1 tunnel=yes proposal=default
```

Referensi:

- https://datatracker.ietf.org/doc/html/rfc4306
- https://help.mikrotik.com/docs/display/ROS/IPsec

2 Manajemen Bandwidth dengan Queue Tree

2.1 Alokasi Bandwidth 100 Mbps

- 40 Mbps untuk **E-learning**
- 30 Mbps untuk **Guru & Staf**
- 20 Mbps untuk **Siswa**
- 10 Mbps untuk **CCTV & Update Sistem**

2.2 Konfigurasi Parent Queue

```
/queue tree
add name="TOTAL-BW" parent=global queue=default max-limit=100M
```

2.3 Konfigurasi Child Queue

```
/queue tree
add name="E-learning" parent="TOTAL-BW" packet-mark=e-learning-mark limit-at=30M max-
    limit=40M priority=1

add name="Guru-Staf" parent="TOTAL-BW" packet-mark=guru-mark limit-at=20M max-limit
    =30M priority=2

add name="Siswa" parent="TOTAL-BW" packet-mark=siswa-mark limit-at=10M max-limit=20M
    priority=3

add name="CCTV-Update" parent="TOTAL-BW" packet-mark=cctv-mark limit-at=5M max-limit
    =10M priority=4
```

2.4 Penandaan Paket (Marking)

```
/ip firewall mangle
add chain=forward protocol=tcp dst-port=443,80 src-address=192.168.1.0/24 action=mark
    -packet new-packet-mark=e-learning-mark passthrough=yes

add chain=forward src-address=192.168.2.0/24 action=mark-packet new-packet-mark=guru-
    mark passthrough=yes

add chain=forward src-address=192.168.3.0/24 action=mark-packet new-packet-mark=siswa
    -mark passthrough=yes

add chain=forward src-address=192.168.4.0/24 action=mark-packet new-packet-mark=cctv-
    mark passthrough=yes
```

Referensi:

- https://help.mikrotik.com/docs/display/ROS/Queues
- https://help.mikrotik.com/docs/display/ROS/Firewall