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

# Laporan Sementara
# Praktikum Jaringan Komputer

## Firewall & NAT

Edward Natasaputra - 5024231023

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Perkembangan teknologi jaringan dan kebutuhan akan koneksi yang aman antar kantor atau cabang perusahaan semakin meningkat seiring bertambahnya ancaman keamanan di dunia maya. Virtual Private Network (VPN) merupakan solusi efektif untuk menjamin keamanan komunikasi data melalui jaringan publik seperti internet. Salah satu protokol keamanan yang banyak digunakan adalah IPSec (Internet Protocol Security), yang menyediakan enkripsi dan autentikasi data secara end-to-end.

Selain keamanan, manajemen bandwidth juga menjadi perhatian penting, terutama untuk mengatur prioritas dan alokasi kapasitas jaringan yang terbatas agar aplikasi kritikal tetap berjalan lancar tanpa terganggu trafik lain yang kurang prioritas. Oleh karena itu, pengaturan antrian dan prioritas trafik menggunakan mekanisme seperti Queue Tree sangat dibutuhkan untuk memaksimalkan performa jaringan.

## 1.2 Dasar Teori

### 1.2.1 Tunneling dan VPN

Tunneling adalah teknik mengirimkan paket data melalui jaringan dengan membungkus paket asli ke dalam paket lain agar bisa melewati jaringan dengan protokol berbeda. VPN memanfaatkan tunneling untuk membuat "terowongan digital" yang aman, memungkinkan jaringan privat tersembunyi berjalan di atas jaringan publik.

Beberapa protokol tunneling yang umum digunakan antara lain:

- **GRE (Generic Routing Encapsulation)**: Membungkus paket IP dengan header tambahan.
- **IPSec**: Menyediakan enkripsi dan autentikasi data, ideal untuk koneksi VPN.
- **L2TP (Layer 2 Tunneling Protocol)** dan **PPTP**: Protokol VPN yang sering dipakai pada berbagai sistem operasi.
- **SSL Tunneling**: Menggunakan SSL untuk enkripsi komunikasi aman.

### 1.2.2 IPSec

IPSec adalah protokol keamanan yang berfungsi untuk mengenkripsi dan mengautentikasi paket data IP. Fungsi utamanya adalah menjaga kerahasiaan, integritas, dan keaslian data yang dikirimkan antar perangkat.

**Fitur Utama IPSec:**

- Autentikasi pengirim data.

- Enkripsi isi data agar tidak dapat dibaca oleh pihak tidak berwenang.
- Integritas data untuk memastikan data tidak diubah selama transmisi.
- Manajemen kunci secara otomatis menggunakan IKE (Internet Key Exchange).

**Mode IPSec:**

- **Tunnel Mode**: Mengamankan seluruh paket IP, digunakan untuk koneksi antar jaringan (site-to-site).
- **Transport Mode**: Mengamankan payload paket IP, umumnya untuk komunikasi end-to-end antar host.

### 1.2.3 Manajemen Bandwidth dengan Queue

Manajemen bandwidth penting untuk mengatur trafik agar aplikasi kritikal mendapatkan prioritas lebih tinggi. MikroTik menyediakan dua fitur utama:

**Simple Queue:** Mudah diatur, cocok untuk manajemen bandwidth sederhana per IP atau interface.

**Queue Tree:** Lebih kompleks dan fleksibel, memungkinkan pembuatan struktur parent-child dan pengaturan prioritas trafik secara rinci.

Tabel berikut menunjukkan perbandingan kedua metode:

**Tabel 1:** Perbandingan Simple Queue dan Queue Tree

| Fitur | Simple Queue | Queue Tree |
|---|---|---|
| Tingkat Kesulitan | Mudah | Menengah - Sulit |
| Struktur | Satu tingkat (sederhana) | Bertingkat (parent-child) |
| Membutuhkan Marking | Tidak | Ya |
| Fleksibilitas | Terbatas | Tinggi |
| Cocok untuk | User/IP spesifik | Pengaturan trafik kompleks |
| Keuntungan | Cepat diatur, langsung jalan | Kustomisasi dan kontrol mendalam |
| Kekurangan | Terbatas untuk trafik kompleks | Setup lebih rumit |

# 2 Tugas Pendahuluan

## 2.1 Studi Kasus Konfigurasi VPN IPSec

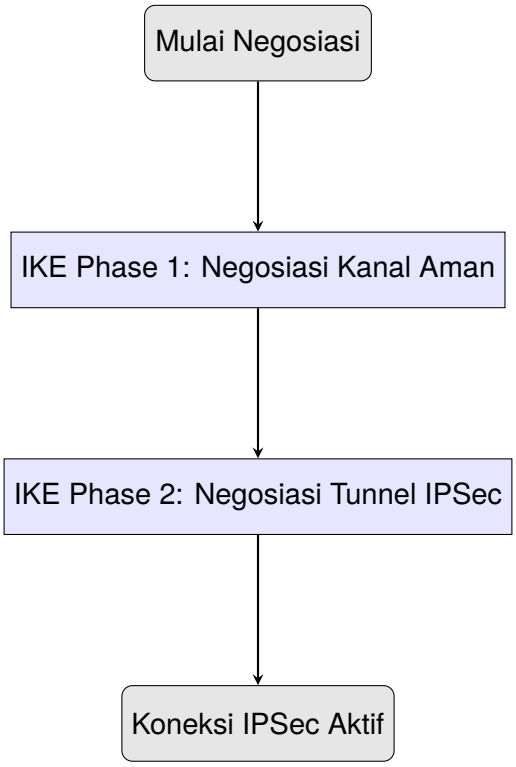
Sebuah perusahaan ingin membuat koneksi VPN IPSec yang aman antara kantor pusat dan cabang. Berikut adalah uraian lengkapnya.

## 2.2 Fase Negosiasi IPSec

Negosiasi IPSec terbagi menjadi dua fase utama:

- **IKE Phase 1:** Membentuk kanal aman dan saling otentikasi antar perangkat. Di fase ini, algoritma enkripsi dan metode autentikasi disepakati, serta kunci sesi (security association) dibuat.
- **IKE Phase 2:** Negosiasi untuk pembuatan tunnel IPSec yang digunakan untuk meng-enkripsi data, termasuk menentukan parameter enkripsi, autentikasi, dan lifetime key.

Diagram sederhana fase IKE:




**Gambar 1:** Tahapan Negosiasi VPN IPSec

## 2.3 Parameter Keamanan yang Disepakati

Parameter utama yang harus disetujui kedua perangkat adalah:

- **Algoritma Enkripsi:** Contohnya AES-256, DES, 3DES.
- **Metode Autentikasi:** Pre-shared key (PSK) atau sertifikat digital.
- **Lifetime Key:** Durasi kunci sesi sebelum diganti, misal 8 jam atau 3600 detik.

### 2.3.1 Contoh Konfigurasi Sederhana Router (Site-to-Site)

Berikut adalah contoh konfigurasi IPSec site-to-site pada router (MikroTik):

```
/ip ipsec peer
add address=IP_REMOTE exchange-mode=main secret="pre_shared_key"
/ip ipsec proposal
add name="default" auth-algorithms=sha1 enc-algorithms=aes-256-cbc
/ip ipsec policy
add src-address=10.0.0.0/24 dst-address=10.1.0.0/24 protocol=all action=encrypt \
proposal=default peer=peer1
```

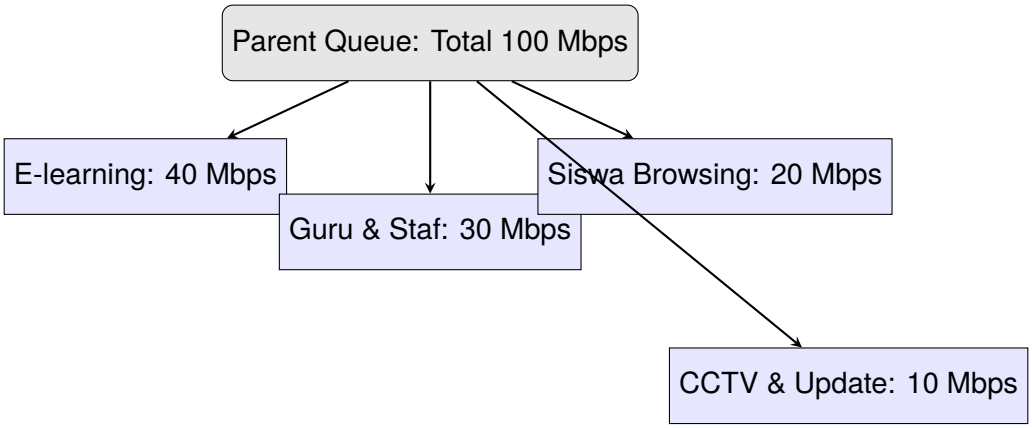
# 3 Skema Queue Tree untuk Manajemen Bandwidth Sekolah

Sebuah sekolah memiliki bandwidth 100 Mbps yang dialokasikan sebagai berikut:

**Tabel 2:** Alokasi Bandwidth Sekolah

| Penggunaan | Bandwidth | Keterangan |
|---|---|---|
| E-learning | 40 Mbps | Prioritas tinggi, aplikasi pembelajaran |
| Guru & Staf | 30 Mbps | Akses email, cloud storage |
| Siswa (Browsing umum) | 20 Mbps | Prioritas sedang |
| CCTV & Update Sistem | 10 Mbps | Prioritas rendah |

### 3.0.1 Skema Queue Tree




**Gambar 2:** Skema Queue Tree untuk Alokasi Bandwidth Sekolah

### 3.0.2 Penjelasan Marking dan Prioritas

Untuk mengelola trafik, tiap jenis trafik diberi marking menggunakan fitur mangle agar dapat dikenali dan dialokasikan bandwidth sesuai prioritas.

- **Marking Paket:** Paket data dari aplikasi e-learning ditandai sebagai prioritas tertinggi agar tidak terhambat.
- **Prioritas dan Limit Rate:** Masing-masing child queue diberikan limit rate sesuai alokasi bandwidth, dengan prioritas E-learning dan Guru lebih tinggi daripada browsing siswa dan CCTV.

### 3.0.3 Contoh Konfigurasi Queue Tree MikroTik (Sederhana)

```
/queue tree
add name="parent" max-limit=100M parent=global
add name="elearning" parent=parent packet-mark=elearning-mark max-limit=40M priority=1
add name="guru-staf" parent=parent packet-mark=guru-staf-mark max-limit=30M priority=2
add name="siswa" parent=parent packet-mark=siswa-mark max-limit=20M priority=3
add name="cctv-update" parent=parent packet-mark=cctv-mark max-limit=10M priority=4
```

## Referensi


- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
- Durojaiye, B. (2020). *MikroTik RouterOS by Example*. CreateSpace Independent Publishing Platform.
- RFC 4301 - Security Architecture for the Internet Protocol (IPSec), IETF.
- MikroTik Documentation, https://wiki.mikrotik.com