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

# Laporan Sementara
# Praktikum Jaringan Komputer

## VPN & Queue

I Gusti Ngurah Eka Febrian Suantara Putra - 5024231078

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Sekarang ini, lalu lintas data terus meningkat dan pola kerja makin fleksibel, banyak orang bisa bekerja dari berbagai lokasi. Karena itu, organisasi butuh sistem yang bisa memastikan koneksi antar lokasi tetap aman dan lancar. Salah satu solusi yang banyak dipakai adalah Virtual Private Network (VPN), khususnya jenis yang menggunakan protokol IPSec di level jaringan. VPN ini bekerja seperti membuat jalur khusus yang dienkripsi, jadi meskipun datanya lewat internet umum, isi pesannya tetap terlindungi dari penyusup atau pihak tak diinginkan. Teknologi ini cocok digunakan oleh berbagai jenis organisasi, mulai dari perusahaan besar sampai institusi pendidikan, karena bisa menjaga komunikasi internal tetap aman.

Tapi keamanan saja belum cukup. Ada juga kebutuhan untuk memastikan layanan digital seperti kelas online, CCTV, sistem administrasi, atau update software bisa berjalan mulus tanpa berebut jaringan. Di sinilah MikroTik Queue Tree berperan. Fitur ini bisa mengatur pembagian bandwidth berdasarkan prioritas penggunaan. Jadi, aplikasi yang penting bisa tetap berjalan lancar walaupun jaringan sedang padat. Menariknya, sistem ini juga fleksibel—kalau ada bandwidth yang nganggur, bisa langsung dipakai oleh layanan lain tanpa perlu penyesuaian manual.

Modul 5 ini akan membahas dua hal penting tadi secara praktis: pertama, bagaimana caranya membuat koneksi VPN IPSec antar site to site, lalu kedua, bagaimana mengatur pembagian bandwidth 100 Mbps menggunakan Queue Tree sesuai kebutuhan sekolah.

## 1.2 Dasar Teori

VPN bekerja dengan membungkus paket data asli ke dalam paket lain menggunakan protokol tunneling. Dengan cara ini, data antar lokasi terlihat seperti lewat jaringan pribadi padahal sebenarnya tetap lewat internet publik. IPSec adalah salah satu protokol yang umum dipakai dan bekerja di lapisan IP. Dalam prosesnya, IPSec memanfaatkan dua protokol utama: ESP (untuk enkripsi) dan AH (untuk otentikasi dan integritas). Proses komunikasi aman ini diatur lewat dua jenis koneksi: satu untuk kontrol (IKE SA) dan satu lagi untuk data (IPSec SA).

Pada tahap awal, perangkat saling bernegosiasi menentukan algoritma enkripsi dan metode otentikasi yang akan digunakan. Biasanya, algoritma seperti AES untuk enkripsi dan HMAC-SHA untuk integritas banyak dipilih. Pertukaran kunci dilakukan lewat metode Diffie–Hellman, dan seluruh komunikasi dikemas agar tetap aman sepanjang sesi. Kalau ingin keamanan ekstra, bisa diaktifkan fitur Perfect Forward Secrecy, yang membuat setiap sesi menggunakan kunci baru, jadi kalau satu sesi bocor, sesi lainnya tetap aman.

IPSec punya dua mode: tunnel dan transport. Mode tunnel melindungi keseluruhan paket termasuk headernya, cocok untuk koneksi antar jaringan. Sementara mode transport hanya melindungi isi data, lebih sering dipakai untuk koneksi langsung antar perangkat.

Di sisi lain, untuk mengatur kualitas layanan atau Quality of Service (QoS), MikroTik menyediakan dua jenis antrean: Simple Queue dan Queue Tree. Simple Queue cocok kalau cuma ingin membatasi kecepatan perangkat tertentu. Tapi kalau tujuannya membagi bandwidth secara adil berdasarkan jenis layanan, Queue Tree lebih tepat. Queue Tree memungkinkan kita membuat struktur hierarki, misalnya semua layanan pendidikan dikelompokkan dalam satu antrian utama, lalu dibagi lagi menjadi subantrian seperti kelas online, CCTV, dan sebagainya.

Untuk memulai pengaturan ini, biasanya paket data akan diberi tanda dulu (marking) berdasarkan kriteria tertentu, seperti alamat IP, port, atau tipe layanan. Tanda ini lalu digunakan untuk mengarahkan paket ke antrean yang sesuai. Masing-masing antrean bisa diatur jatahnya, batas maksimalnya, dan prioritasnya. Sistem ini menggunakan metode pembagian yang fleksibel, jadi kalau ada antrean yang tidak memakai jatahnya, antrean lain bisa menggunakan sisa bandwidth tersebut.

Queue Tree ini bekerja setelah proses NAT (network address translation), jadi bisa diterapkan pada data asli maupun data yang sudah diubah. Karena sifatnya global, cukup satu konfigurasi saja di gateway router meskipun punya banyak port—ini jelas memudahkan manajemen jaringan secara keseluruhan. Dengan pengaturan yang tepat, layanan penting bisa tetap lancar tanpa harus mengorbankan pengguna lain.

## 2 Tugas Pendahuluan

1. **Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:**

   (a) **Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)**

   **Phase 1 – Pembentukan IKE SA** Langkah pertama dalam komunikasi IPSec adalah membentuk Security Association (IKE SA) antara dua peer. Kanal ini bersifat terenkripsi dan digunakan untuk negosiasi selanjutnya.

   1. **Exchange Proposal:** Kedua pihak bertukar parameter enkripsi seperti algoritma (contoh: AES-256, SHA-256), grup Diffie–Hellman, dan waktu hidup kunci.
   2. **Diffie–Hellman Key Exchange:** Kunci bersama dihitung berdasarkan pertukaran nilai publik untuk menciptakan key session.
   3. **Peer Authentication:** Identitas diverifikasi menggunakan Pre-Shared Key (PSK) atau sertifikat digital.
   4. **Pembentukan IKE SA:** Setelah validasi selesai, terbentuk kanal manajemen yang aman.

   **Phase 2 – Pembentukan IPSec SA (Quick Mode)** Fase kedua membentuk tunnel data aktual, yang akan mengenkripsi lalu lintas jaringan antar-subnet.

   1. **Selector:** Menentukan jaringan sumber dan tujuan yang akan dilindungi (misal: 10.10.10.0/24 ke 10.20.20.0/24).
   2. **Parameter Proteksi:** Negosiasi mengenai algoritma enkripsi (contoh AES-GCM), integritas (HMAC), dan Perfect Forward Secrecy (PFS).
   3. **Pembuatan IPSec SA:** Terbentuk dua SA — satu untuk keluar dan satu untuk masuk — lengkap dengan kunci dan masa aktif.
   4. **Transmisi Data:** Paket yang sesuai selector akan dienkapsulasi dan dikirim secara terenkripsi.

   **Kesimpulan:**
   Fase pertama membuat kanal aman untuk manajemen, sedangkan fase kedua digunakan un-

tuk komunikasi data terenkripsi. Selama IKE SA valid, tunnel dapat diperpanjang tanpa perlu autentikasi ulang.

2. **Parameter keamanan yang harus disepakati**

   Agar tunnel IPSec berhasil terbentuk, kedua endpoint harus menyetujui konfigurasi berikut:

   1. **Algoritma Enkripsi:** Contohnya AES-128 atau AES-256 untuk menyandikan data.
   2. **Algoritma Integritas:** Misalnya HMAC-SHA-256 untuk menjamin bahwa data tidak diubah saat transmisi.
   3. **Grup Diffie-Hellman:** Seperti grup 14 (2048 bit) atau grup 16 (4096 bit), digunakan untuk pertukaran kunci secara aman.
   4. **Waktu Hidup SA (Lifetime):** Contohnya 28.800 detik untuk IKE SA dan 3.600 detik untuk IPSec SA.
   5. **Metode Autentikasi Peer:** Dapat berupa Pre-Shared Key atau sertifikat digital (X.509).

**Catatan:** Ketidaksesuaian satu parameter saja dapat menyebabkan kegagalan pembentukan tunnel.

**Sebuah sekolah memiliki bandwidth internet sebesar 100 Mbps yang dialokasikan ke beberapa layanan. Buatlah skema Queue Tree yang lengkap berdasarkan pembagian berikut:**

- **40 Mbps** dialokasikan untuk **e-learning**.
- **30 Mbps** dialokasikan untuk **guru dan staf** (akses email, cloud storage).
- **20 Mbps** dialokasikan untuk **siswa** (browsing umum).
- **10 Mbps** dialokasikan untuk **CCTV dan update sistem**.

**Skema Queue Tree yang harus dibuat meliputi:**

a) Struktur **Parent dan Child Queue**.

b) Penjelasan mengenai **packet marking**.

c) Penetapan **prioritas** dan **limit rate** untuk masing-masing layanan.

1. **Parent dan Child Queue**

   Queue Tree di MikroTik bersifat hierarkis. Satu queue induk (parent) mewakili total bandwidth sekolah, sementara empat queue anak (child) mengatur pembagian berdasarkan jenis layanan.

```
# Parent queue 100 Mbps
/queue tree add name=total parent=global max-limit=100M

# Child queue untuk masing-masing layanan
/queue tree add name=elearning parent=total \
    limit-at=40M max-limit=40M priority=1 packet-mark=elearn_pkt

/queue tree add name=guru parent=total \
    limit-at=30M max-limit=30M priority=2 packet-mark=guru_pkt

/queue tree add name=siswa parent=total \
    limit-at=20M max-limit=20M priority=3 packet-mark=siswa_pkt

/queue tree add name=cctv parent=total \
    limit-at=10M max-limit=10M priority=4 packet-mark=cctv_pkt
```

**Penjelasan Marking**

Setiap paket diberi label (packet-mark) berdasarkan alamat tujuan subnet. Label ini digunakan untuk mengarahkan paket ke queue yang sesuai.

```
/ip firewall mangle
  add chain=prerouting dst-address=192.168.10.0/24 \
      action=mark-packet new-packet-mark=elearn_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.20.0/24 \
      action=mark-packet new-packet-mark=guru_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.30.0/24 \
      action=mark-packet new-packet-mark=siswa_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.40.0/24 \
      action=mark-packet new-packet-mark=cctv_pkt passthrough=yes
```

**Prioritas dan Limit Rate**

- **limit-at:** Menjamin bandwidth minimum tetap tersedia.
- **max-limit:** Batas maksimum yang bisa digunakan masing-masing queue.
- **priority:** Queue dengan angka lebih kecil memiliki prioritas lebih tinggi dalam kondisi bandwidth penuh.

  **Distribusi:**

  - E-learning: 40 Mbps (prioritas 1)
  - Guru & Staf: 30 Mbps (prioritas 2)
  - Siswa: 20 Mbps (prioritas 3)
  - CCTV & Update: 10 Mbps (prioritas 4)

# 3 Referensi


a) RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2), IETF, 2016.

b) William Stallings. (2022). *Network Security Essentials: Applications and Standards*, 7th Edition. Pearson.

c) Chandra, R. & Shenoy, P. (2020). “Performance analysis of QoS queue scheduling on MikroTik RouterOS”, *IJACSA*, 11(7), pp. 120–127.