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

# Laporan Sementara
# Praktikum Jaringan Komputer

## Tunneling

Ria Angela Tanujaya - 5024231074

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Di era sekarang, proses pertukaran data memerlukan metode yang aman agar data dapat terkirim tanpa gangguan serta terlindungi dari ancaman siber. Salah satu teknologi yang berperan penting dalam hal ini adalah tunneling, yang memungkinkan pengiriman data melalui "terowongan" virtual di antara jaringan berbeda. Terkait dengan itu, protokol seperti IPSec menawarkan keamanan tambahan dengan menyediakan fitur enkripsi dan autentikasi, menjadikannya fondasi utama dalam implementasi Virtual Private Network (VPN). Dengan banyaknya kebutuhan akses jarak jauh yang aman, pemahaman terhadap mekanisme kerja IPSec menjadi sangat penting. Selain keamanan, pengelolaan lalu lintas data juga merupakan aspek vital dalam jaringan. Ketika bandwidth terbatas, sistem jaringan perlu mampu memberikan prioritas kepada trafik penting agar performa layanan tetap optimal. Simple Queue dan Queue Tree pada perangkat seperti MikroTik menjadi solusi untuk pengaturan bandwidth secara efektif, baik dalam skala kecil maupun besar. Melalui praktikum ini, praktikan diharapkan mampu memahami dan menerapkan konsep tunneling, keamanan data dengan IPSec, serta manajemen bandwidth menggunakan Simple Queue dan Queue Tree.

## 1.2 Dasar Teori

Praktikum ini dilandasi oleh sejumlah konsep penting dalam jaringan komputer yang berkaitan erat dengan keamanan data, efisiensi komunikasi, dan manajemen lalu lintas jaringan. Tunneling merupakan metode untuk menghubungkan dua jaringan berbeda melalui jalur virtual yang disebut "terowongan". Proses ini dilakukan dengan cara encapsulation, yaitu membungkus paket data asli ke dalam format paket lain agar dapat dikirim melewati jaringan perantara. Tunneling memungkinkan data dari satu sistem dikirim ke sistem lain meskipun melewati infrastruktur jaringan yang berbeda, seperti dari jaringan lokal (LAN) ke jaringan luas (WAN). Salah satu protokol penting yang digunakan dalam tunneling adalah IPSec (Internet Protocol Security). IPSec berfungsi untuk melindungi data selama proses pengiriman melalui internet dengan cara mengenkripsi isi data, memastikan data berasal dari sumber yang sah, serta menjaga integritasnya agar tidak diubah di tengah jalan. IPSec banyak digunakan dalam VPN (Virtual Private Network) untuk menciptakan jalur komunikasi yang aman antara dua titik. Dalam pelaksanaannya, IPSec terdiri dari beberapa elemen utama seperti ESP (Encapsulation Security Payload), AH (Authentication Header), dan IKE (Internet Key Exchange). IPSec dapat berjalan dalam dua mode, yaitu transport mode dan tunnel mode, yang masing-masing digunakan sesuai dengan kebutuhan komunikasi antar perangkat atau antar jaringan. Selain aspek keamanan, jaringan juga perlu diatur agar penggunaan bandwidth tidak menyebabkan kemacetan atau gangguan pada layanan penting. Untuk itu, pengelolaan bandwidth menjadi bagian penting dalam pengaturan lalu lintas data. Di perangkat MikroTik, tersedia dua metode utama untuk mengelola bandwidth, yaitu Simple Queue dan Queue Tree. Simple Queue adalah metode sederhana yang cocok digunakan untuk mengatur bandwidth per pengguna atau per alamat IP secara langsung. Sementara itu, Queue Tree memberikan fleksibilitas lebih tinggi, memungkinkan pengaturan berdasarkan jenis trafik dan menggunakan struktur bertingkat, sehingga cocok untuk jaringan besar dengan kebutuhan pengaturan kompleks. Manajemen bandwidth juga erat kaitannya dengan prioritas trafik. Dalam kondisi jaringan padat, tidak semua jenis trafik memiliki tingkat kepentingan yang sama. Trafik penting seperti VPN, video conference, atau akses ke sistem kerja harus diprioritaskan agar tidak terganggu.

Oleh karena itu, sistem jaringan perlu memiliki mekanisme untuk mengatur prioritas ini, baik secara manual melalui pengaturan queue maupun otomatis melalui fitur Quality of Service (QoS).

## 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:

   - **Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)**
     Dalam implementasi VPN IPSec site-to-site, negosiasi awal dilakukan dalam dua fase: IKE Phase 1 dan IKE Phase 2, yang dijalankan oleh protokol IKE (Internet Key Exchange). Pada IKE Phase 1, tujuan utamanya adalah membentuk jalur komunikasi yang aman antara dua perangkat jaringan (biasanya router atau firewall). Proses ini disebut juga sebagai pembentukan IKE Security Association (IKE SA). Dalam fase ini, kedua pihak akan menyepakati beberapa parameter keamanan, seperti jenis algoritma enkripsi dan hashing yang akan digunakan, metode autentikasi (misalnya pre-shared key), serta grup Diffie-Hellman yang digunakan untuk melakukan pertukaran kunci secara aman. Jalur ini disebut "secure channel" dan digunakan untuk melindungi negosiasi selanjutnya. Biasanya IKE Phase 1 berjalan dalam mode Main Mode untuk keamanan maksimum atau Aggressive Mode jika kecepatan lebih diprioritaskan. Setelah IKE Phase 1 berhasil, maka dilanjutkan dengan IKE Phase 2, yang bertujuan membentuk IPSec Security Association (IPSec SA). Di fase ini, perangkat akan menegosiasikan bagaimana data aktual akan dienkripsi dan ditransmisikan. IKE Phase 2 dikenal sebagai Quick Mode, dan pada tahap ini, kedua belah pihak menyepakati parameter seperti jenis protokol keamanan (ESP atau AH), transform-set (kombinasi algoritma enkripsi dan hashing), serta lifetime dari IPSec SA. Setelah ini, tunnel VPN akan aktif, dan lalu lintas data antar kantor pusat dan cabang dapat berjalan dengan aman.
   - **Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)**
     Agar negosiasi antara kedua perangkat berjalan sukses dan koneksi aman bisa terbentuk, ada beberapa parameter penting yang harus disepakati oleh kedua pihak:
     - Algoritma Enkripsi: Ini adalah algoritma yang akan digunakan untuk menyandikan data agar tidak bisa dibaca oleh pihak yang tidak berwenang.
     - Algoritma Hashing (Integritas): Ini memastikan bahwa data tidak diubah selama transmisi.
     - Metode Autentikasi: Perangkat jaringan perlu memastikan bahwa mereka terhubung dengan mitra yang sah.
     - Diffie-Hellman Group: Ini adalah grup matematika yang digunakan untuk membentuk shared key secara aman di jaringan yang tidak aman.
     - Lifetime Key (Durasi SA): Ini adalah waktu berlaku untuk tunnel yang dibentuk. Contoh yang umum adalah 3600 detik (1 jam) untuk ISAKMP SA, dan 28800 detik (8 jam) untuk IPSec SA. Setelah waktu ini habis, tunnel perlu dinegosiasi ulang.
   - **Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site**
     Untuk membuat koneksi site-to-site VPN IPSec, administrator perlu mengkonfigurasi ro-

uter pada kedua sisi (kantor pusat dan cabang). Misalkan kantor pusat memiliki jaringan 192.168.1.0/24 dengan IP publik 1.1.1.1, dan kantor cabang memiliki jaringan 192.168.2.0/24 dengan IP publik 2.2.2.2.

```
! Tahap 1: Konfigurasi ISAKMP Policy (IKE Phase 1)
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400

crypto isakmp key mySharedKey address 2.2.2.2

! Tahap 2: Konfigurasi IPSec Transform Set (IKE Phase 2)
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac

! Buat ACL untuk menentukan trafik yang akan dienkripsi
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

! Tahap 3: Konfigurasi Crypto Map
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set MYSET
 match address VPN-TRAFFIC

! Tahap 4: Pasang crypto map ke interface publik
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 crypto map VPN-MAP
```

referensi: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

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

   Buatlah skema Queue Tree yang lengkap:
   - **Parent dan child queue**
   Queue Tree menggunakan struktur parent-child, dengan `ether1` sebagai parent (interface yang mengarah ke internet):

```
ether1 (100 Mbps)
 e-learning      → max-limit 40 Mbps, priority 1
 guru-staf       → max-limit 30 Mbps, priority 2
 siswa           → max-limit 20 Mbps, priority 3
 cctv-update     → max-limit 10 Mbps, priority 4
```

- **Penjelasan marking**

Untuk membagi bandwidth secara efisien dan sesuai prioritas, digunakan fitur **Queue Tree** pada MikroTik RouterOS. Untuk di mikrotiknya sebagai berikut:

**Listing 1:** Firewall Mangle Rules for Packet Marking

```
1
2   /ip firewall mangle
    add chain=forward src-address=192.168.10.0/24 action=mark-packet new-
    packet-mark=e-learning passthrough=yes
3   add chain=forward src-address=192.168.20.0/24 action=mark-packet new-
    packet-mark=guru-staf passthrough=yes
4   add chain=forward src-address=192.168.30.0/24 action=mark-packet new-
    packet-mark=siswa passthrough=yes
5   add chain=forward src-address=192.168.40.0/24 action=mark-packet new-
    packet-mark=cctv-update passthrough=yes
6
```

**Penjelasan:**

- `chain=forward` digunakan untuk menandai paket yang melewati router.
- `src-address` disesuaikan dengan IP masing-masing jaringan.
- `new-packet-mark` adalah label yang akan digunakan di Queue Tree.
- `passthrough=yes` artinya proses firewall akan tetap dilanjutkan.

- **Prioritas dan limit rate pada masing-masing queue**

| Kategori Layanan | Limit-at | Max-limit | Prioritas |
|---|---|---|---|
| E-learning | 30 Mbps | 40 Mbps | 1 (tertinggi) |
| Guru dan Staf | 20 Mbps | 30 Mbps | 2 |
| Siswa | 10 Mbps | 20 Mbps | 3 |
| CCTV dan Update | 5 Mbps | 10 Mbps | 4 (terendah) |

Referensi: https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues