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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling

Ernita Kartika Weni - 5024231013

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan meningkatnya kebutuhan akan konektivitas antar jaringan yang semakin kompleks, kemampuan untuk menghubungkan dua sistem yang berada pada infrastruktur berbeda menjadi semakin krusial. Salah satu pendekatan yang umum digunakan untuk menjawab tantangan ini adalah teknik tunneling. Metode ini memungkinkan data dikirimkan melalui sebuah "terowongan" virtual di dalam jaringan yang pada dasarnya tidak secara langsung mendukung jenis data tersebut. Dengan tunneling, komunikasi antar perangkat tetap dapat dilakukan secara lancar meskipun berada di jaringan yang berbeda jenis, misalnya antara LAN dan WAN, atau antar lokasi yang terpisah secara geografis. Lebih dari itu, tunneling juga menjadi fondasi penting dalam menciptakan koneksi yang aman melalui jaringan publik seperti internet. Salah satu penerapan nyatanya adalah melalui Virtual Private Network (VPN), yang memanfaatkan protokol-protokol tertentu untuk menjaga kerahasiaan dan integritas data selama proses transmisi. Modul ini disusun untuk memperkenalkan konsep dasar dari tunneling, prinsip kerja encapsulation, serta berbagai protokol pendukung seperti GRE, IPSec, dan L2TP. Selain aspek keamanan, modul ini juga akan membahas pentingnya pengelolaan bandwidth dalam jaringan. Akan dikupas perbandingan antara metode Simple Queue dan Queue Tree pada perangkat MikroTik, serta bagaimana pengaturan prioritas trafik dapat memastikan layanan-layanan penting tetap berjalan optimal, terutama saat jaringan berada dalam kondisi padat.

1.2 Dasar Teori

1. **Virtual Private Network (VPN)**
   Virtual Private Network (VPN) merupakan teknologi yang memungkinkan pengguna untuk membentuk koneksi jaringan privat secara aman melalui infrastruktur jaringan publik seperti internet. VPN bekerja dengan cara mengenkripsi lalu lintas data dan membuat *terowongan virtual* (*tunnel*) yang melindungi informasi dari potensi intersepsi oleh pihak yang tidak berwenang. Salah satu implementasi VPN yang banyak digunakan pada tingkat organisasi adalah *site-to-site VPN*, yang memungkinkan dua jaringan lokal (LAN) di lokasi berbeda terhubung seolah-olah berada dalam satu jaringan yang sama. Teknologi ini mempermudah komunikasi antar cabang perusahaan atau antar instansi tanpa harus bergantung pada koneksi fisik langsung.

2. **IPSec (Internet Protocol Security)**
   IPSec adalah seperangkat protokol yang digunakan untuk mengamankan komunikasi data pada lapisan jaringan (*network layer*) dari model OSI. IPSec menyediakan layanan keamanan seperti otentikasi, integritas, dan enkripsi data. Terdapat dua mode utama dalam IPSec, yaitu:

   - **Transport Mode**: hanya mengenkripsi *payload* dari paket IP, sedangkan *header* IP tetap terbuka.
   - **Tunnel Mode**: mengenkripsi seluruh paket IP dan membungkusnya dalam paket IP baru, cocok untuk VPN antar situs.

   IPSec terdiri dari dua protokol utama:

   - **Authentication Header (AH)**: menyediakan integritas dan otentikasi data, tetapi tidak mengenkripsi isi pesan.

- **Encapsulating Security Payload (ESP)**: menyediakan enkripsi, integritas, dan otentikasi.

3. **Tunneling dan Encapsulation**
   Tunneling merupakan proses mengenkapsulasi paket data dalam protokol lain untuk dikirimkan melalui jaringan yang berbeda. Proses ini memungkinkan protokol yang tidak secara *native* didukung oleh jaringan untuk dikirimkan melaluinya. *Encapsulation* sendiri mengacu pada pelapisan data asli dengan *header* tambahan dari protokol tunneling. Beberapa protokol tunneling umum di antaranya:

   - **GRE (Generic Routing Encapsulation)**: protokol tunneling sederhana yang mendukung berbagai protokol layer 3.
   - **L2TP (Layer 2 Tunneling Protocol)**: digunakan untuk tunneling di layer 2, sering dikombinasikan dengan IPSec untuk keamanan.
   - **IPSec**: berfungsi sebagai protokol keamanan sekaligus mekanisme tunneling pada layer 3.

4. **Manajemen Bandwidth** Manajemen bandwidth adalah proses pengaturan alokasi kapasitas jaringan agar penggunaan sumber daya jaringan tetap efisien dan optimal. Tujuannya adalah untuk menjamin kualitas layanan (*Quality of Service* / QoS) terutama bagi aplikasi-aplikasi yang sensitif terhadap keterlambatan (*delay*), *jitter*, atau kehilangan paket. Dalam lingkungan jaringan yang terbatas sumber dayanya, pengelolaan bandwidth menjadi penting agar trafik prioritas seperti video konferensi, layanan daring, atau sistem administrasi tidak terganggu oleh trafik lain yang bersifat sekunder.

5. **Simple Queue dan Queue Tree pada MikroTik**
   MikroTik RouterOS menyediakan fitur pengaturan antrean (*queue*) yang dapat digunakan untuk membatasi dan mengatur bandwidth. Dua metode utama yang disediakan adalah:

   - **Simple Queue**: metode pengaturan bandwidth yang mudah dikonfigurasi dan cocok untuk kebutuhan dasar. Setiap antrean berdiri sendiri dan tidak memiliki struktur hierarki.
   - **Queue Tree**: metode antrean berbasis pohon (*hierarchical queuing*), memungkinkan pembagian bandwidth secara lebih fleksibel dan terstruktur. Queue Tree cocok untuk skenario di mana terdapat beberapa jenis layanan yang membutuhkan prioritas berbeda, karena mendukung konsep *parent-child queue* dan *priority class*.

   Queue Tree menggunakan fitur *HTB (Hierarchical Token Bucket)* yang memungkinkan bandwidth dibagi ke dalam kelas-kelas tertentu. Jika suatu kelas tidak menggunakan seluruh alokasinya, kelas lain dapat meminjam kapasitas tersebut, membuat pemanfaatan bandwidth menjadi lebih efisien.

2 Tugas Pendahuluan

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

   - Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)

- Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
- Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Jawab :

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

- IKE Phase 1 (Internet Key Exchange Phase 1) bertugas membuat channel aman (secure channel) antara dua endpoint IPSec, yaitu kantor pusat dan cabang. Proses ini dilakukan dengan negosiasi parameter keamanan dan otentikasi. Fase ini menghasilkan ISAKMP Security Association (SA) yang digunakan untuk melindungi fase kedua.
- IKE Phase 2 bertujuan untuk negosiasi parameter enkripsi dan integritas data yang akan digunakan dalam proses pertukaran data VPN. Fase ini membangun IPSec Security Association yang mengatur bagaimana data dienkripsi dan dikirimkan secara aman melalui tunnel.

(b) Parameter Keamanan yang Harus Disepakati

- Algoritma Enkripsi
  Contoh algoritma yang sering digunakan adalah AES (Advanced Encryption Standard) dengan ukuran kunci 128-bit atau 256-bit. Alternatif lain adalah 3DES, meskipun sudah mulai jarang dipakai karena kurang efisien.
- Metode Autentikasi
  Menggunakan Pre-shared Key (PSK) atau sertifikat digital (digital certificates) untuk memastikan identitas kedua endpoint.
- Lifetime Key
  Parameter yang menentukan masa aktif kunci enkripsi sebelum diganti. Contoh: Phase 1 lifetime 24 jam, Phase 2 lifetime 1 jam.

(c) Konfigurasi Sederhana Pada Sisi Router untuk IPSec Site-to-Site
Contoh konfigurasi dasar (pseudo-config) untuk router Mikrotik:

```
1 /ip ipsec peer add address=<IP_KANTOR_CABANG> auth-method=pre-
    shared-key secret=<PSK> exchange-mode=ike2
2 /ip ipsec proposal add name=proposal-aes auth-algorithms=sha256
     enc-algorithms=aes-128-cbc
3 /ip ipsec policy add src-address=<IP_KANTOR_PUSAT>/24 dst-
    address=<IP_KANTOR_CABANG>/24 \
4     protocol=all action=encrypt level=require ipsec-protocols=
    esp proposal=proposal-aes
```

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
- Penjelasan marking
- Prioritas dan limit rate pada masing-masing queue

Jawab :

(a) Struktur Parent dan Child Queue

i. Parent Queue: Total bandwidth 100 Mbps
   - Child Queue 1: E-learning (40 Mbps)
   - Child Queue 2: Guru & Staf (30 Mbps)
   - Child Queue 3: Siswa (20 Mbps)
   - Child Queue 4: CCTV & Update Sistem (10 Mbps)

ii. Penjelasan Marking
   Marking adalah proses mengidentifikasi dan menandai paket data berdasarkan jenis layanan atau prioritas agar bisa dikelola oleh Queue Tree. Contohnya:
   - Pakai mangle rules untuk menandai paket HTTP/HTTPS yang berasal dari server e-learning dengan label e-learning
   - Paket email dan cloud storage ditandai sebagai guru-staf
   - Paket browsing umum ditandai siswa
   - Paket CCTV dan update sistem diberi tanda cctv-update

iii. Prioritas dan Limit Rate pada Masing-Masing Queue
   - E-learning: Prioritas tertinggi dengan limit 40 Mbps agar kelas daring berjalan lancar
   - Guru & Staf: Prioritas tinggi, limit 30 Mbps untuk kebutuhan kerja penting
   - Siswa: Prioritas sedang, limit 20 Mbps untuk browsing dan aktivitas ringan
   - CCTV & Update Sistem: Prioritas paling rendah, limit 10 Mbps agar tidak menggganggu aktivitas utama

   Konfigurasi Queue Tree (MikroTik):

```
/queue tree
add name=total-bandwidth parent=ether1 max-limit=100M

add name=queue-elearning parent=total-bandwidth packet-mark=
   elearning \
    limit-at=40M max-limit=40M priority=1

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

add name=queue-siswa parent=total-bandwidth packet-mark=
   siswa \
```

```
11      limit-at=20M max-limit=20M priority=3
12
13  add name=queue-cctv parent=total-bandwidth packet-mark=cctv
        \
14      limit-at=10M max-limit=10M priority=4
```

Referensi:

- Mikrotik Indonesia. (2023). *Konfigurasi Queue Tree di Mikrotik untuk Manajemen Bandwidth*. Diakses dari: https://mikrotik.co.id
- Kominfo. (2022). *Manajemen Jaringan dan Bandwidth Sekolah*. Jakarta: Direktorat Jenderal Aplikasi Informatika.