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

Laporan Sementara
Praktikum Jaringan Komputer

VPN QoS

Ahmad Dafa Salam - 5024231024

4 Juni 2025

1 Pendahuluan

1.1 Latar Belakang

Praktikum ini bertujuan untuk memahami bagaimana membangun koneksi aman menggunakan VPN (Virtual Private Network) dan mengelola trafik jaringan menggunakan teknik pembagian bandwidth. Dalam dunia jaringan komputer, keamanan data dan efisiensi lalu lintas menjadi dua aspek penting yang harus diperhatikan. VPN berfungsi melindungi komunikasi data agar tidak mudah disadap oleh pihak ketiga, sedangkan manajemen bandwidth memastikan setiap layanan mendapat alokasi kecepatan internet sesuai kebutuhannya. Praktikum ini mengombinasikan konsep tunneling, IPSec, dan Queue Tree agar peserta mampu mengamankan sekaligus mengatur jaringan secara efektif.

1.2 Dasar Teori

Virtual Private Network (VPN) adalah teknologi yang memungkinkan koneksi pribadi yang aman melalui jaringan publik seperti internet. Salah satu cara kerja VPN adalah dengan melakukan tunneling, yaitu membungkus paket data dalam protokol baru agar bisa melewati jaringan yang tidak aman tanpa mengubah isi data. Tunneling ini didukung oleh berbagai protokol, seperti GRE, PPTP, dan IPSec. Dari ketiganya, IPSec merupakan salah satu yang paling aman karena menyediakan autentikasi, enkripsi, serta integritas data. IPSec bekerja dalam dua fase negosiasi, yakni IKE Phase 1 untuk pertukaran kunci dan IKE Phase 2 untuk membentuk kanal komunikasi yang aman, dengan parameter seperti algoritma enkripsi, metode autentikasi, dan masa berlaku kunci yang harus disepakati bersama.

Manajemen bandwidth dalam jaringan bertujuan mengatur distribusi kecepatan internet kepada berbagai jenis trafik atau pengguna agar layanan penting tetap berjalan optimal. Mikrotik menyediakan fitur Queue Tree yang memungkinkan pembagian bandwidth dengan struktur hierarkis (parent dan child queue). Trafik jaringan ditandai (marking) berdasarkan IP, port, atau protokol, lalu dialokasikan ke antrian tertentu dengan limit kecepatan dan prioritas berbeda. Contohnya, dalam jaringan sekolah, bandwidth dapat dibagi untuk e-learning, akses guru, siswa, serta sistem keamanan seperti CCTV, agar semua berjalan efisien dan adil.

Penggabungan antara VPN dan manajemen bandwidth memberikan manfaat ganda: keamanan dan kontrol lalu lintas. Dalam praktikum ini, peserta tidak hanya mengonfigurasi koneksi VPN menggunakan protokol PPTP dan IPSec, tetapi juga mengimplementasikan teknik pengaturan bandwidth dengan Queue Tree. Dengan begitu, peserta memperoleh pemahaman menyeluruh tentang bagaimana menjaga data tetap aman sekaligus menjamin kestabilan performa jaringan untuk berbagai kebutuhan pengguna.

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

Untuk membangun jaringan privat yang aman antara dua lokasi geografis seperti kantor pusat dan cabang, protokol IPSec dapat dimanfaatkan dalam skema VPN site-to-site. IPSec bekerja dalam dua fase yang dikenal sebagai IKE (Internet Key Exchange).

Pada tahap pertama (IKE Phase 1), kedua perangkat jaringan—umumnya berupa router—akan bernegosiasi untuk membentuk jalur komunikasi awal yang aman. Di fase ini, proses autentikasi identitas dilakukan dan parameter kriptografi disepakati bersama. Parameter yang umum digunakan mencakup algoritma enkripsi seperti `AES-256`, metode autentikasi berbasis `pre-shared key (PSK)`, serta waktu hidup kunci (lifetime), misalnya 86400 detik (1 hari). Hasil dari fase ini adalah terbentuknya *ISAKMP SA*, yaitu kanal aman yang memungkinkan pertukaran kunci enkripsi secara terenkripsi.

Tahap selanjutnya, IKE Phase 2, digunakan untuk membuat kesepakatan lebih lanjut mengenai bagaimana data aktual akan dienkripsi dan dikirim. Protokol seperti `ESP (Encapsulation Security Payload)` biasanya dipakai di fase ini karena mendukung baik enkripsi maupun autentikasi. Tujuan dari fase ini adalah membentuk *IPSec SA*, yakni kesepakatan pengamanan untuk sesi data utama.

Untuk implementasi sederhana pada MikroTik, berikut contoh konfigurasi umum:

```
/ip ipsec proposal
add name=secure-proposal auth-algorithms=sha256 \
enc-algorithms=aes-256-cbc lifetime=1d

/ip ipsec peer
add address=203.0.113.1 exchange-mode=main \
secret=MySecretKey name=peer-branch

/ip ipsec policy
add src-address=192.168.100.0/24 dst-address=192.168.200.0/24 \
sa-src-address=198.51.100.2 sa-dst-address=203.0.113.1 tunnel=yes \
proposal=secure-proposal
```

Konfigurasi tersebut mencerminkan pengamanan jalur antar dua jaringan privat melalui IPSec VPN.

Referensi: MikroTik Documentation, “IPsec Configuration Guide”, `https://help.mikrotik.com/docs/display/ROS/IPsec`

2. **Skema Queue Tree untuk Pembagian Bandwidth Sekolah:**

   Dalam sebuah lingkungan sekolah dengan total bandwidth sebesar 100 Mbps, pengelolaan alokasi internet berdasarkan fungsi pengguna sangat penting untuk efisiensi jaringan. Pembagian bandwidth bisa dilakukan dengan memanfaatkan `Queue Tree`, salah satu fitur pada MikroTik yang mendukung manajemen antrian secara hierarkis.

Proses pertama yang dilakukan adalah menetapkan **parent queue** dengan batas maksimal 100 Mbps. Lalu dibuat **child queue** untuk masing-masing kategori pengguna, yaitu e-learning, guru dan staf, siswa, serta sistem CCTV dan update otomatis.

Contoh struktur Queue Tree:

- `Parent Queue: queue-total`, max-limit = 100M
- `Child Queues:`
  - `e-learning`, max-limit = 40M, priority = 1
  - `guru-staf`, max-limit = 30M, priority = 2
  - `siswa`, max-limit = 20M, priority = 3
  - `cctv-update`, max-limit = 10M, priority = 4

Untuk mengarahkan trafik ke masing-masing antrian, perlu dilakukan penandaan paket dengan fitur `mangle`. Teknik ini memungkinkan identifikasi berdasarkan alamat IP tujuan, port layanan, atau subnet tertentu. Contohnya, trafik dari LMS untuk e-learning ditandai dengan packet-mark "e-learning", lalu diarahkan ke queue yang sesuai.

Contoh mangle rule sederhana:

```
/ip firewall mangle
add chain=forward dst-address=192.168.10.0/24 \
action=mark-packet new-packet-mark=e-learning passthrough=yes
add chain=forward dst-address=192.168.20.0/24 \
action=mark-packet new-packet-mark=guru-staf passthrough=yes
add chain=forward dst-address=192.168.30.0/24 \
action=mark-packet new-packet-mark=siswa passthrough=yes
add chain=forward dst-address=192.168.40.0/24 \
action=mark-packet new-packet-mark=cctv-update passthrough=yes
```

Dengan pendekatan ini, administrator dapat memprioritaskan trafik penting (seperti e-learning) di atas trafik sekunder (misalnya update sistem), sekaligus menjamin penggunaan bandwidth yang adil dan stabil di seluruh jaringan.

Referensi: MikroTik Wiki – Queue Tree and Bandwidth Management,
`https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues`