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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Alvito Aryo Putra - 5024231077

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital saat ini, keamanan dan efisiensi dalam pengelolaan jaringan menjadi aspek penting dalam mendukung operasional perusahaan atau lembaga pendidikan. VPN (Virtual Private Network) dengan protokol IPSec memberikan solusi koneksi aman antara dua lokasi berbeda melalui jaringan publik. Di sisi lain, manajemen bandwidth melalui sistem seperti Queue Tree memastikan distribusi lalu lintas data yang adil dan sesuai prioritas, terutama ketika sumber daya jaringan terbatas.

Selain keamanan, tantangan lain dalam komunikasi data lintas jaringan adalah perbedaan jenis protokol atau media transmisi. Di sinilah konsep **tunneling** berperan penting. Tunneling memungkinkan paket data melewati "terowongan virtual" melalui jaringan yang tidak sejenis, dengan proses encapsulation yang memastikan data tetap utuh sampai tujuan. Tunneling menjadi pondasi bagi implementasi VPN, khususnya saat membangun koneksi antar cabang atau akses remote yang aman.

1.2 Dasar Teori

Dalam jaringan komputer modern, terdapat berbagai teknologi yang dirancang untuk menjawab tantangan keamanan, interoperabilitas, dan efisiensi manajemen lalu lintas data. Salah satu konsep fundamental yang sering digunakan adalah **tunneling**, yaitu proses mengenkapsulasi paket data ke dalam format protokol lain agar dapat dikirim melalui jaringan yang berbeda jenis atau melalui media publik seperti internet. Dalam proses ini, data yang dikirim dibungkus terlebih dahulu dalam suatu protokol pengangkut, kemudian dibuka kembali saat mencapai tujuan. Mekanisme ini memungkinkan komunikasi antar dua titik di jaringan yang berbeda seolah-olah berada dalam satu jaringan lokal. Beberapa protokol tunneling yang umum digunakan antara lain GRE (Generic Routing Encapsulation), IPSec (Internet Protocol Security), SSH tunneling, serta PPTP dan L2TP. Tunneling merupakan dasar dari implementasi VPN (Virtual Private Network) yang memungkinkan koneksi jarak jauh yang aman.

Salah satu protokol tunneling yang paling aman dan banyak digunakan dalam implementasi VPN adalah **IPSec**. IPSec bekerja pada layer jaringan (Network Layer) dari model OSI dan menyediakan tiga fungsi utama yaitu enkripsi, autentikasi, dan integritas data. Dengan fitur enkripsi, data yang dikirim diacak sehingga tidak dapat dibaca oleh pihak yang tidak berwenang. Autentikasi memastikan bahwa data benar-benar berasal dari sumber yang sah, sementara integritas menjaga agar data tidak dimodifikasi selama transmisi. IPSec menggunakan dua mode operasi, yaitu tunnel mode dan transport mode. Pada tunnel mode, seluruh paket IP dibungkus dan dienkripsi, sehingga cocok untuk koneksi antar jaringan atau antar cabang perusahaan. Sementara itu, transport mode hanya mengenkripsi bagian payload dari paket IP, dan lebih cocok untuk komunikasi antar host. IPSec juga menggunakan protokol pendukung seperti ESP (Encapsulation Security Payload) dan AH (Authentication Header), serta proses pertukaran kunci melalui IKE (Internet Key Exchange) yang terdiri dari dua fase negosiasi keamanan.

Selain keamanan, efisiensi dalam pengelolaan bandwidth menjadi aspek penting dalam jaringan modern. Untuk mengatasi kebutuhan ini, perangkat seperti MikroTik menyediakan fitur **Queue Tree**, yaitu metode manajemen bandwidth yang bersifat hierarkis. Queue Tree memungkinkan pengelompokan dan pengaturan lalu lintas data berdasarkan jenis layanan, IP address, atau port tertentu dengan struktur bertingkat (parent-child). Dalam penggunaannya, Queue Tree memerlukan proses

marking atau penandaan paket melalui *mangle rule*, yang kemudian digunakan untuk memisahkan trafik sesuai kategori tertentu. Dengan struktur ini, administrator jaringan dapat menentukan limitasi kecepatan dan prioritas untuk masing-masing jenis trafik, misalnya mendahulukan lalu lintas video conference dibandingkan streaming atau download file. Hal ini sangat berguna dalam kondisi di mana bandwidth terbatas dan perlu dialokasikan secara bijak untuk menjamin kelancaran layanan utama.

Dengan mengintegrasikan teknologi tunneling seperti IPSec dan pengelolaan bandwidth melalui Queue Tree, sistem jaringan dapat menjamin konektivitas yang aman, stabil, dan efisien, terutama dalam skenario komunikasi antar cabang perusahaan atau institusi pendidikan yang mengandalkan akses internet secara intensif.

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:**

   Untuk membangun koneksi aman antar kantor menggunakan VPN IPSec, terdapat dua tahapan utama dalam proses negosiasi yang disebut IKE (Internet Key Exchange). Pada **Phase 1**, kedua router akan membuat tunnel awal (ISAKMP SA) yang bertujuan untuk mengautentikasi identitas dan menyepakati parameter enkripsi seperti algoritma (contoh: AES-256), metode autentikasi (misalnya pre-shared key), dan lifetime (contoh: 3600 detik). Proses ini menghasilkan kanal aman untuk melanjutkan ke Phase 2.

   Pada **Phase 2**, perangkat akan merundingkan Security Association (IPSec SA) untuk membentuk tunnel data yang aman menggunakan protokol seperti ESP (Encapsulation Security Payload). Tunnel ini akan digunakan untuk mentransmisikan data terenkripsi antar site.

   Contoh konfigurasi IPSec site-to-site pada MikroTik:

   ```
   /ip ipsec peer
   add address=203.0.113.1 exchange-mode=main secret=sharedsecret

   /ip ipsec policy
   add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 \
       sa-dst-address=203.0.113.1 sa-src-address=198.51.100.1 \
       tunnel=yes action=encrypt proposal=default
   ```

   Referensi: MikroTik Wiki, "IPSec Site-to-Site Configuration", 2023. https://wiki.mikrotik.com/wiki/Manual:IP/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 beserta penjelasan.

Untuk membagi bandwidth sesuai kebutuhan tersebut, dapat digunakan **Queue Tree** dengan pembagian struktur parent dan child queue. Parent queue akan menampung total bandwidth, sedangkan masing-masing child queue akan dialokasikan untuk kategori trafik tertentu berdasarkan marking yang dilakukan di mangle rules.

Struktur Queue Tree:

```
Parent Queue: total-bandwidth (100 Mbps)
 e-learning        : 40 Mbps (priority 1)
 guru-staf         : 30 Mbps (priority 2)
 siswa             : 20 Mbps (priority 3)
 CCTV & update     : 10 Mbps (priority 4)
```

Penandaan paket dilakukan berdasarkan IP sumber atau port layanan tertentu, misalnya IP LMS untuk e-learning atau port RTSP untuk CCTV. Setelah diberi marking, masing-masing queue diberi limit rate dan prioritas. Prioritas 1 berarti queue tersebut paling diutamakan jika bandwidth terbatas.

Referensi: MikroTik Documentation, "Queue Tree & Bandwidth Management", 2023. *https://wiki.mikrotik.com/wiki/Manual:Queue_Tree*