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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling and QoS

Bernanddus Nathaniel Arthur - 5024231041

2025

1 Pendahuluan

1.1 Latar Belakang

Materi yang dibahas dalam dokumen ini, meliputi Tunneling, IPSec (IP Security), dan Manajemen Bandwidth (Simple Queue vs. Queue Tree, dan Prioritas Trafik), muncul sebagai respons fundamental terhadap dua kebutuhan utama dalam dunia jaringan komputer modern: konektivitas yang mulus dan keamanan serta efisiensi transmisi data.Di satu sisi, kebutuhan akan konektivitas yang mulus menuntut kemampuan untuk menghubungkan berbagai jenis jaringan yang berbeda, seringkali tersebar secara geografis. Teknologi Tunneling hadir sebagai solusi inovatif untuk tantangan ini, memungkinkan data melintasi "terowongan digital" dari satu jaringan ke jaringan lain yang secara fisik atau logis berbeda, seolah-olah mereka berada dalam satu segmen. Ini sangat relevan dalam skenario di mana perangkat harus berkomunikasi melalui infrastruktur jaringan yang beragam, seperti dari jaringan lokal ke WAN (Wide Area Network) atau bahkan antar pusat data. Tanpa tunneling, interoperabilitas dan jangkauan komunikasi akan sangat terbatas.

Di sisi lain, seiring dengan peningkatan ketergantungan pada jaringan, muncul pula ancaman keamanan siber yang semakin kompleks dan kebutuhan efisiensi dalam pengelolaan trafik. Setiap data yang ditransmisikan, baik itu informasi pribadi, transaksi keuangan, atau data bisnis krusial, berpotensi menjadi target serangan. Di sinilah IPSec memainkan peran vital. Sebagai "bodyguard digital", IPSec menyediakan kerangka kerja keamanan yang komprehensif untuk melindungi komunikasi IP dengan fitur autentikasi, enkripsi, dan integritas data. Kemampuannya untuk membangun "terowongan aman" (seperti dalam VPN) menjadikan IPSec solusi pilihan untuk melindungi lalu lintas data sensitif, memastikan bahwa informasi tidak dapat diakses, diubah, atau dipalsukan oleh pihak yang tidak berwenang.Selanjutnya, dengan semakin padatnya lalu lintas data, manajemen bandwidth yang efektif menjadi krusial untuk memastikan kualitas layanan (QoS). Tanpa pengaturan yang tepat, jaringan dapat mengalami kemacetan, menyebabkan latensi tinggi, putusnya koneksi, dan pengalaman pengguna yang buruk untuk aplikasi-aplikasi penting. Konsep Simple Queue dan Queue Tree dalam manajemen bandwidth, bersama dengan Prioritas Trafik, mengatasi masalah ini. Kedua fitur ini memungkinkan administrator jaringan untuk mengatur alokasi kecepatan, membatasi penggunaan bandwidth, dan yang terpenting, memberi prioritas pada lalu lintas data yang lebih penting (seperti video conference atau akses ke sistem kritis perusahaan) dibandingkan dengan lalu lintas yang kurang mendesak (seperti streaming hiburan atau unduhan besar). Ini memastikan bahwa sumber daya jaringan yang terbatas dapat dimanfaatkan secara optimal, menjaga kelancaran operasi dan komunikasi vital.Secara keseluruhan, materi ini tidak hanya menjelaskan bagaimana jaringan dapat dihubungkan melintasi batas-batas teknis, tetapi juga bagaimana koneksi tersebut dapat diamankan dan dioptimalkan. Pemahaman mendalam tentang Tunneling, IPSec, dan Manajemen Bandwidth sangat penting bagi siapa pun yang terlibat dalam perancangan, implementasi, dan pemeliharaan infrastruktur jaringan yang tangguh, aman, dan efisien di era digital yang dinamis ini.

1.2 Dasar Teori

Tunneling adalah teknik jaringan yang memungkinkan paket data melintasi jaringan yang berbeda protokol atau topologi dengan cara membungkus satu paket di dalam paket lain, sebuah proses yang disebut enkapsulasi. Ini sangat berguna untuk menghubungkan jaringan yang tidak kompatibel, menciptakan koneksi aman seperti Virtual Private Network (VPN), atau melewati firewall . Beberapa protokol tunneling umum termasuk Generic Routing Encapsulation (GRE) untuk koneksi point-to-point, Layer 2 Tunneling Protocol (L2TP) yang sering dipasangkan dengan IPSec untuk keamanan, dan Virtual eXtensible Local Area Network (VXLAN) yang digunakan dalam virtualisasi pusat data . Untuk mengamankan komunikasi IP, IP Security (IPSec) adalah kumpulan protokol yang menyediakan autentikasi, kerahasiaan (enkripsi), integritas data, dan manajemen kunci. IPSec beroperasi dalam dua mode utama: Tunnel Mode, yang mengenkripsi seluruh paket IP asli dan ideal untuk VPN site-to-site, serta Transport Mode, yang hanya mengenkripsi payload dan cocok untuk komunikasi host-to-host .

Dalam manajemen bandwidth, MikroTik RouterOS menawarkan Simple Queue dan Queue Tree, keduanya berbasis Hierarchical Token Bucket (HTB). Simple Queue lebih mudah dikonfigurasi untuk pembatasan bandwidth per pengguna atau per IP, dengan pemrosesan berurutan yang bisa memengaruhi kinerja pada skala besar. Sebaliknya, Queue Tree dirancang untuk tugas antrian yang lebih kompleks dan fleksibel, seperti kebijakan prioritas global, dan sangat bergantung pada penandaan paket dari fasilitas Mangle untuk mengklasifikasikan trafik. Konsep ini mengarah pada prioritas trafik bandwidth, sebuah praktik penting dalam Quality of Service (QoS) yang memastikan data penting mendapatkan perlakuan istimewa . QoS bekerja dengan mengklasifikasikan trafik, menandai paket (misalnya dengan DSCP), menggunakan antrian prioritas, membentuk trafik, dan mengalokasikan bandwidth secara dinamis. Ini secara langsung mengurangi latensi (penundaan), jitter (variasi penundaan), dan meningkatkan throughput (kecepatan transfer data), yang krusial untuk pengalaman pengguna yang optimal dan operasi bisnis yang lancar

2 Tugas Pendahuluan

1. **Pengaturan VPN IPSec**

   - **Tahapan Negosiasi IPSec:**
     - **Phase 1:** Membangun ISAKMP SA (Security Association) antara dua perangkat VPN. Pada tahap ini, perangkat menyepakati parameter keamanan seperti algoritma enkripsi, metode autentikasi, dan cara tukar kunci. Mode yang dipakai bisa Main Mode (lebih aman) atau Aggressive Mode (lebih cepat).
     - **Phase 2:** Menetapkan IPSec SA untuk data sebenarnya. Protokol seperti

ESP (Encapsulating Security Payload) digunakan untuk mengenkripsi payload data.

- **Parameter Keamanan yang Disepakati:**
  - Algoritma enkripsi: `AES-256`, `3DES`
  - Metode autentikasi: `SHA-256`, `MD5`
  - Diffie-Hellman Group: `Group 2`, `Group 5`, `Group 14`
  - Durasi kunci: Phase 1 (`86400 detik`), Phase 2 (`3600 detik`)
- **Contoh Konfigurasi Dasar (Router Mikrotik):**

```
/ip ipsec proposal
add name="ipsec-proposal" auth-algorithms=sha256 enc-algorithms=
    aes-256-cbc pfs-group=none

/ip ipsec peer
add address=192.168.1.2/32 exchange-mode=main secret="vpnsharedkey
    " profile=default

/ip ipsec policy
add dst-address=192.168.2.0/24 src-address=192.168.1.0/24 sa-dst-
    address=192.168.1.2 \
    sa-src-address=192.168.1.1 tunnel=yes proposal=ipsec-proposal

```

2. **Distribusi Bandwidth di Lingkungan Sekolah**

- Total kapasitas bandwidth: **100 Mbps**
- Alokasi:
  - 40 Mbps untuk platform e-learning
  - 30 Mbps untuk penggunaan guru dan staf (akses email, penyimpanan awan)
  - 20 Mbps untuk akses umum siswa (browsing dan riset)
  - 10 Mbps untuk sistem CCTV dan update perangkat

3. **Rancangan Queue Tree Lengkap (Mikrotik)**

- **Antrian Induk:**

```
/queue tree
add name="Total-Bandwidth" parent=global limit-at=100M max-limit
    =100M

```

- **Antrian Turunan:**

```
/queue tree
add name="eLearning"   parent="Total-Bandwidth" packet-mark=
    elearning-mark  limit-at=40M max-limit=40M priority=1
add name="GuruStaf"    parent="Total-Bandwidth" packet-mark=guru-
    mark       limit-at=30M max-limit=30M priority=2
add name="Siswa"       parent="Total-Bandwidth" packet-mark=siswa-
    mark      limit-at=20M max-limit=20M priority=3
add name="CCTVUpdate"  parent="Total-Bandwidth" packet-mark=cctv-
    mark       limit-at=10M max-limit=10M priority=4

```

- **Pemberian Tanda Paket (Packet Marking):**

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet
    new-packet-mark=elearning-mark passthrough=yes
add chain=forward src-address=192.168.20.0/24 action=mark-packet
    new-packet-mark=guru-mark      passthrough=yes
add chain=forward src-address=192.168.30.0/24 action=mark-packet
    new-packet-mark=siswa-mark     passthrough=yes
add chain=forward src-address=192.168.40.0/24 action=mark-packet
    new-packet-mark=cctv-mark      passthrough=yes

```

- **Prioritas dan Batas Kecepatan:**
  - **Priority:** Menentukan urutan penanganan saat antrian penuh (semakin kecil angka, semakin tinggi prioritas).
  - **Limit-at:** Minimal bandwidth yang dijamin tersedia.
  - **Max-limit:** Maksimal bandwidth yang boleh dipakai.
- **Tabel Alokasi Antrian:**

Antrian	Prioritas	Limit-at	Max-limit
eLearning	1	40 Mbps	40 Mbps
Guru & Staf	2	30 Mbps	30 Mbps
Siswa	3	20 Mbps	20 Mbps
CCTV & Update	4	10 Mbps	10 Mbps