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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan Qos

Andriy Shevtiyan - 5024231080

2025

1 Pendahuluan

1.1 Latar Belakang

Kemajuan teknologi informasi yang sangat pesat menuntut sistem jaringan komputer untuk memiliki tingkat keamanan dan kinerja yang optimal. Di era globalisasi saat ini, kebutuhan untuk mengakses jaringan secara aman dari berbagai lokasi serta memastikan kualitas transmisi data menjadi semakin krusial. Oleh karena itu, penguasaan terhadap aspek keamanan dan efisiensi jaringan sangat diperlukan.

Praktikum ini bertujuan untuk memberikan pengalaman langsung dalam penerapan dua elemen penting dalam pengelolaan jaringan, yaitu Virtual Private Network (VPN) dan Quality of Service (QoS). Kedua aspek ini memiliki peran penting dalam membangun jaringan yang handal, baik dari sisi perlindungan data maupun pengelolaan lalu lintas data.

Melalui praktikum ini, mahasiswa diharapkan mampu memahami permasalahan nyata yang sering ditemui dalam pengelolaan jaringan, serta dapat mengaplikasikan solusi teknis guna meningkatkan keamanan dan mutu layanan jaringan. Kompetensi ini penting sebagai bekal dalam menghadapi kebutuhan industri yang mengutamakan efisiensi dan keamanan dalam infrastruktur jaringan modern.

1.2 Dasar Teori

1.2.1 Virtual Private Network (VPN)

VPN merupakan teknologi jaringan yang memungkinkan terjadinya koneksi yang aman melalui jaringan publik seperti internet. VPN menciptakan jalur terenkripsi atau *tunnel* antara dua titik, sehingga data yang dikirimkan tidak dapat diakses oleh pihak yang tidak berwenang. VPN banyak digunakan untuk menghubungkan jaringan antar lokasi atau mengakses jaringan internal dari luar kantor dengan aman.

Beberapa protokol VPN yang umum digunakan antara lain:

- **PPTP (Point-to-Point Tunneling Protocol)**: Protokol VPN lama yang mudah digunakan, namun kurang dari segi keamanan.
- **L2TP/IPSec (Layer 2 Tunneling Protocol)**: Kombinasi L2TP dengan IPSec untuk memberikan koneksi yang lebih aman.
- **OpenVPN**: Protokol open-source yang fleksibel dan mendukung enkripsi kuat serta berbagai platform.
- **IPSec**: Protokol tingkat jaringan yang mengamankan lalu lintas IP menggunakan enkripsi dan otentikasi.

1.2.2 Quality of Service (QoS)

QoS adalah metode dan mekanisme dalam jaringan yang digunakan untuk mengatur dan mengelola lalu lintas data guna menjamin kualitas layanan. QoS bertujuan memastikan

aplikasi penting seperti *VoIP*, video streaming, atau layanan real-time lainnya mendapatkan prioritas yang layak.

Parameter utama dalam QoS mencakup:

- **Bandwidth**: Kapasitas maksimal jalur komunikasi dalam mentransmisikan data.
- **Latency (Delay)**: Waktu yang dibutuhkan sebuah paket data untuk sampai ke tujuan.
- **Jitter**: Fluktuasi waktu kedatangan antar paket yang dapat mengganggu aplikasi real-time.
- **Packet Loss**: Jumlah atau persentase paket data yang hilang selama pengiriman.

Beberapa teknik implementasi QoS meliputi:

- **Traffic Shaping**: Mengatur arus lalu lintas agar sesuai dengan kapasitas jaringan.
- **Priority Queuing**: Memberikan prioritas lebih tinggi pada jenis lalu lintas tertentu.
- **Bandwidth Allocation**: Pembagian bandwidth untuk memastikan layanan penting tetap berjalan lancar.

2 Tugas Pendahuluan

1. Studi kasus konfigurasi VPN IPSec: Sebuah perusahaan ingin menghubungkan kantor pusat dengan cabang secara aman. Jelaskan prosesnya secara rinci:

   Negosiasi dalam IPSec dilakukan dalam dua fase utama:

   - **Fase IKE 1:** Merupakan tahap awal untuk membentuk koneksi aman antara dua perangkat melalui autentikasi dan pembuatan saluran terenkripsi, dikenal sebagai ISAKMP SA. Dalam tahap ini, dilakukan kesepakatan parameter keamanan seperti algoritma enkripsi (contohnya AES), autentikasi (misalnya SHA-256), serta metode pertukaran kunci (Diffie-Hellman).
   - **Fase IKE 2 (Quick Mode):** Tahapan ini menghasilkan IPSec SA yang digunakan untuk mengenkripsi data yang ditransmisikan. Parameter yang disepakati meliputi protokol keamanan (ESP atau AH), algoritma enkripsi dan autentikasi, serta masa aktif kunci (key lifetime).

Parameter Keamanan yang Digunakan

Beberapa parameter keamanan umum yang diterapkan antara lain:

- **Algoritma Enkripsi:** AES-256 untuk tingkat keamanan tinggi

- **Algoritma Autentikasi:** HMAC-SHA256 untuk menjaga integritas dan keaslian data
- **Key Lifetime:** 86400 detik (24 jam)
- **Diffie-Hellman Group:** Group 14 (2048-bit)
- **Mode Operasi:** Tunnel Mode untuk komunikasi antar jaringan berbeda

Contoh Konfigurasi Router (IPSec Site-to-Site)

```
/ip ipsec peer
add address=203.0.113.2 exchange-mode=main secret="vpnkey123" \
enc-algorithm=aes-256 hash-algorithm=sha256 dh-group=modp2048

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

/ip ipsec policy
add dst-address=192.168.2.0/24 sa-dst-address=203.0.113.2 \
sa-src-address=203.0.113.1 src-address=192.168.1.0/24 \
tunnel=yes proposal=vpn-proposal
```

Konfigurasi di atas menggambarkan penerapan koneksi IPSec secara sederhana pada router dengan parameter keamanan sesuai standar untuk membentuk VPN antar kantor.

2. Sebuah sekolah memiliki akses internet:

   Tujuan Pengaturan Bandwidth

   Pengelolaan bandwidth bertujuan untuk mendistribusikan kapasitas jaringan sesuai prioritas dan kebutuhan pengguna. Dengan total bandwidth 100 Mbps, dibagi ke dalam empat layanan utama:

   - **40 Mbps** untuk e-learning (prioritas tertinggi)
   - **30 Mbps** untuk guru dan staf (akses email dan penyimpanan cloud)
   - **20 Mbps** untuk siswa (akses internet umum)
   - **10 Mbps** untuk CCTV dan pembaruan sistem

   Penandaan Lalu Lintas (Mangle Rule)

   Digunakan untuk mengelompokkan lalu lintas berdasarkan subnet IP sumber.

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet \
new-packet-mark=elearning passthrough=yes

```

```
add chain=forward src-address=192.168.20.0/24 action=mark-packet \
new-packet-mark=guru_staf passthrough=yes

add chain=forward src-address=192.168.30.0/24 action=mark-packet \
new-packet-mark=siswa passthrough=yes

add chain=forward src-address=192.168.40.0/24 action=mark-packet \
new-packet-mark=cctv_update passthrough=yes
```

Penjelasan: Aturan ini berfungsi untuk menandai paket berdasarkan alamat IP sehingga lalu lintas dapat diarahkan ke antrian (queue) yang sesuai.

Konfigurasi Queue Tree

Queue Tree digunakan untuk mengatur alokasi bandwidth secara terstruktur.

```
/queue tree
add name="queue_parent" parent=ether1 max-limit=100M

add name="queue_elearning" parent=queue_parent packet-mark=elearning \
limit-at=40M max-limit=40M priority=1

add name="queue_guru_staf" parent=queue_parent packet-mark=guru_staf \
limit-at=30M max-limit=30M priority=2

add name="queue_siswa" parent=queue_parent packet-mark=siswa \
limit-at=20M max-limit=20M priority=3

add name="queue_cctv_update" parent=queue_parent packet-mark=
    cctv_update \
limit-at=10M max-limit=10M priority=4
```

Keterangan:

- `queue_parent` merupakan induk antrian dengan total bandwidth 100 Mbps.
- Setiap anak antrian memiliki `limit-at` sebagai jaminan bandwidth minimum dan `max-limit` sebagai batas maksimum.
- `priority` menentukan prioritas penanganan trafik, di mana nilai lebih rendah berarti prioritas lebih tinggi.

Ringkasan Alokasi Bandwidth dan Prioritas

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

Kesimpulan: Penerapan teknik Queue Tree dan Mangle memungkinkan pengaturan bandwidth yang efektif, memastikan setiap layanan mendapatkan alokasi sesuai kebutuhannya, dan memprioritaskan trafik penting secara adil.