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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan Qos

Davi Ariq Nugroho - 5024231075

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi yang begitu cepat menuntut sistem jaringan komputer untuk terus meningkatkan aspek keamanan serta performanya. Di tengah era globalisasi seperti saat ini, kemampuan untuk mengakses jaringan dengan aman dari berbagai lokasi serta menjaga kualitas transmisi data menjadi hal yang semakin vital. Oleh sebab itu, pemahaman mendalam mengenai keamanan dan efisiensi jaringan menjadi sangat penting.

Praktikum ini dirancang untuk memberikan pengalaman praktis dalam menerapkan dua komponen utama dalam manajemen jaringan, yaitu Virtual Private Network (VPN) dan Quality of Service (QoS). Kedua komponen ini memiliki peran sentral dalam menciptakan jaringan yang tangguh, baik dalam hal pengamanan data maupun pengaturan lalu lintas data.

Melalui kegiatan praktikum ini, mahasiswa diharapkan dapat memahami tantangan-tantangan nyata yang sering muncul dalam pengelolaan jaringan, serta mampu menerapkan solusi teknis guna meningkatkan aspek keamanan dan kualitas layanan jaringan. Kemampuan ini menjadi bekal penting dalam menjawab kebutuhan industri yang semakin menekankan efisiensi dan keamanan pada infrastruktur jaringannya.

1.2 Dasar Teori

1.2.1 Virtual Private Network (VPN)

VPN atau *Virtual Private Network* merupakan teknologi yang memungkinkan terbentuknya koneksi aman melalui jaringan publik seperti internet. Dengan menggunakan VPN, sebuah *tunnel* terenkripsi diciptakan antara dua titik, sehingga informasi yang dikirimkan tidak dapat diakses atau disadap oleh pihak yang tidak berwenang. Teknologi ini umumnya dimanfaatkan untuk menghubungkan jaringan dari lokasi yang berbeda atau mengakses jaringan internal organisasi secara aman dari luar lokasi.

Beberapa jenis protokol VPN yang sering digunakan antara lain:

- **PPTP (Point-to-Point Tunneling Protocol)**: Protokol yang mudah dikonfigurasi namun memiliki tingkat keamanan yang rendah.
- **L2TP/IPSec (Layer 2 Tunneling Protocol dengan IPSec)**: Kombinasi protokol tunneling dengan fitur enkripsi dan otentikasi untuk keamanan yang lebih baik.
- **OpenVPN**: Protokol sumber terbuka yang mendukung tingkat enkripsi tinggi dan kompatibel dengan berbagai sistem operasi.
- **IPSec**: Protokol yang bekerja pada lapisan jaringan dan menyediakan fitur enkripsi serta autentikasi untuk lalu lintas IP.

1.2.2 Quality of Service (QoS)

QoS atau *Quality of Service* adalah seperangkat teknik dalam pengelolaan jaringan yang bertujuan untuk menjamin kualitas transmisi data, khususnya untuk aplikasi yang sensitif terhadap waktu seperti *VoIP*, konferensi video, dan layanan real-time lainnya. QoS memastikan bahwa jenis data tertentu mendapat prioritas penanganan yang lebih tinggi di dalam jaringan.

Parameter-parameter penting dalam QoS meliputi:

- **Bandwidth**: Kapasitas maksimum kanal komunikasi dalam mentransmisikan data.
- **Latency (Delay)**: Waktu tempuh paket data dari sumber ke tujuan.
- **Jitter**: Variasi waktu antar kedatangan paket yang dapat menyebabkan gangguan pada aplikasi real-time.
- **Packet Loss**: Persentase paket data yang hilang selama proses transmisi.

Teknik-teknik yang digunakan dalam implementasi QoS antara lain:

- **Traffic Shaping**: Mengendalikan laju pengiriman data agar sesuai dengan kapasitas jaringan yang tersedia.
- **Priority Queuing**: Memberikan tingkat prioritas lebih tinggi pada jenis lalu lintas tertentu dibanding yang lain.
- **Bandwidth Allocation**: Menetapkan porsi bandwidth tertentu untuk aplikasi atau layanan yang dianggap penting.

2 Tugas Pendahuluan

1. **Studi Kasus Konfigurasi VPN IPSec**
   Sebuah perusahaan berniat menghubungkan kantor pusat dengan kantor cabang melalui jaringan yang aman. Solusi yang dipilih adalah membangun koneksi VPN dengan protokol IPSec. Proses pembentukan koneksi ini terdiri dari dua tahapan utama dalam protokol IKE (Internet Key Exchange), yaitu:

   - **IKE Phase 1:** Tahap inisialisasi koneksi, di mana dua perangkat saling melakukan autentikasi dan menyepakati parameter keamanan. Proses ini menghasilkan *ISAKMP Security Association* (SA) sebagai dasar saluran komunikasi yang aman. Parameter yang disepakati mencakup algoritma enkripsi (seperti AES), metode autentikasi (misalnya HMAC-SHA256), dan pertukaran kunci menggunakan algoritma Diffie-Hellman.
   - **IKE Phase 2 (Quick Mode):** Setelah kanal aman terbentuk, tahap ini bertugas membuat IPSec SA untuk mengenkripsi lalu lintas data aktual. Pada fase ini, ditentukan protokol (ESP atau AH), metode enkripsi dan autentikasi, serta durasi aktif kunci (key lifetime).

Parameter Keamanan IPSec

Konfigurasi standar yang digunakan meliputi:

- **Algoritma Enkripsi:** AES-256, memberikan tingkat keamanan tinggi
- **Autentikasi:** HMAC-SHA256, menjaga keaslian dan integritas data
- **Key Lifetime:** 86400 detik (setara 24 jam)
- **Diffie-Hellman Group:** Group 14 (2048-bit)
- **Mode:** Tunnel Mode, digunakan untuk menghubungkan dua jaringan berbeda

Contoh Konfigurasi Router untuk 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 ini menunjukkan implementasi VPN antar jaringan menggunakan IPSec, dengan pengaturan keamanan standar yang umum digunakan dalam lingkungan perusahaan.

2. **Manajemen Bandwidth di Lingkungan Sekolah**
   Sebuah sekolah yang memiliki akses internet ingin memastikan bahwa kapasitas jaringan 100 Mbps dapat didistribusikan secara optimal sesuai dengan kebutuhan berbagai pengguna.

   Tujuan Pengelolaan Bandwidth

   Distribusi bandwidth dilakukan untuk mengatur prioritas penggunaan berdasarkan fungsi dan kepentingan layanan, dengan rincian sebagai berikut:

   - **40 Mbps** untuk layanan e-learning (prioritas tertinggi)
   - **30 Mbps** untuk keperluan guru dan staf
   - **20 Mbps** untuk akses umum siswa
   - **10 Mbps** untuk sistem keamanan (CCTV) dan pembaruan perangkat

Penandaan Lalu Lintas dengan Mangle

Mangle digunakan untuk memberi tanda pada paket 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
```

Konfigurasi Queue Tree

Queue Tree digunakan untuk membagi bandwidth sesuai dengan tanda paket yang telah dibuat sebelumnya:

```
/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
```

Penjelasan:

- `queue_parent` berfungsi sebagai antrian utama dengan total bandwidth 100 Mbps.
- Setiap *child queue* dijatah bandwidth minimum (`limit-at`) dan batas maksimum (`max-limit`) sesuai kebutuhannya.
- Nilai `priority` menunjukkan tingkat prioritas—angka lebih kecil berarti prioritas lebih tinggi.

Tabel Alokasi Bandwidth dan Prioritas

Layanan	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:

Dengan penerapan sistem `Queue Tree` dan penandaan paket menggunakan `Mangle`, sekolah dapat menerapkan manajemen bandwidth yang efisien, adil, dan sesuai prioritas. Hal ini membantu menjaga performa layanan penting sekaligus menghindari kemacetan lalu lintas jaringan.