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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Mochamad Rafila Putra Firmansyah - 5024231066

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, kebutuhan akan akses jaringan yang aman dan andal menjadi sangat penting, terutama bagi organisasi yang mengandalkan internet untuk operasional sehari-hari. Dalam lingkungan yang terkoneksi secara global, pertukaran data sering kali melibatkan jaringan publik yang rentan terhadap penyadapan, manipulasi, dan akses tidak sah. Oleh karena itu, teknologi Virtual Private Network (VPN) muncul sebagai solusi untuk membangun jalur komunikasi yang aman melalui jaringan publik. Dengan VPN, data dikirim dalam bentuk terenkripsi dan melewati terowongan virtual yang menjamin kerahasiaan dan integritas informasi. Hal ini memungkinkan perusahaan menghubungkan kantor pusat dengan cabang atau karyawan remote dengan tingkat keamanan yang setara dengan jaringan lokal privat.

Di sisi lain, semakin beragamnya jenis layanan jaringan yang digunakan—seperti video streaming, panggilan suara melalui internet (VoIP), hingga layanan cloud—menyebabkan lalu lintas jaringan menjadi semakin padat dan kompleks. Dalam kondisi seperti ini, tidak semua data dapat diperlakukan secara sama. Beberapa jenis data, terutama yang bersifat real-time, memerlukan penanganan khusus agar tidak mengalami gangguan seperti delay atau jitter. Untuk itu, konsep Quality of Service (QoS) diperkenalkan sebagai mekanisme pengelolaan lalu lintas jaringan yang memungkinkan penentuan prioritas dan alokasi sumber daya secara efisien. Dengan adanya QoS, layanan-layanan penting dapat tetap berjalan dengan lancar meskipun jaringan mengalami kepadatan, sehingga kualitas pengalaman pengguna tetap terjaga.

1.2 Dasar Teori

Virtual Private Network (VPN) adalah teknologi jaringan yang memungkinkan pengguna untuk membuat koneksi aman dan terenkripsi melalui jaringan publik seperti internet. Tujuan utama dari VPN adalah untuk menjaga kerahasiaan data, integritas, serta autentikasi selama proses komunikasi. VPN bekerja dengan cara membuat “terowongan” antara dua titik dalam jaringan melalui protokol tunneling seperti IPSec, PPTP, L2TP, atau OpenVPN. Data yang dikirim melalui tunneling ini dienkripsi sehingga tidak bisa dengan mudah disadap atau dimodifikasi oleh pihak ketiga. VPN sering digunakan untuk menghubungkan kantor pusat dengan cabang, memberikan akses aman bagi pekerja jarak jauh, serta menghindari pembatasan geografis dalam mengakses internet.

Quality of Service (QoS) adalah mekanisme dalam jaringan komputer yang bertujuan untuk mengatur prioritas lalu lintas data agar performa jaringan tetap optimal, khususnya ketika terjadi kemacetan atau persaingan bandwidth. QoS memungkinkan administrator jaringan untuk mengklasifikasikan, menjadwalkan, dan mengontrol jenis layanan berdasarkan parameter tertentu seperti latency, jitter, packet loss, dan throughput. Penerapan QoS sangat penting dalam layanan real-time seperti video conferencing, VoIP, atau streaming, yang sensitif terhadap keterlambatan. Beberapa metode umum dalam QoS adalah queueing (antrian paket berdasarkan prioritas), traffic shaping, dan policing, serta pengaturan bandwidth minimum atau maksimum untuk kelas tertentu.

2 Tugas Pendahuluan

2.1 1. Konfigurasi VPN IPSec Site-to-Site

Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

- **Phase 1 (ISAKMP SA):** Fase ini membangun *Security Association* antara dua perangkat VPN. Parameter yang disepakati antara lain algoritma enkripsi (contoh: AES-256), metode autentikasi (pre-shared key atau sertifikat digital), dan metode pertukaran kunci (seperti Diffie-Hellman). Mode yang digunakan dapat berupa *Main Mode* atau *Aggressive Mode*.
- **Phase 2 (IPSec SA):** Menetapkan SA untuk lalu lintas data sesungguhnya dengan menentukan protokol (*ESP* atau *AH*), algoritma integritas (contoh: SHA-256), serta periode lifetime kunci.

Parameter Keamanan yang Disepakati

- **Algoritma Enkripsi:** `AES-256`, `3DES`
- **Autentikasi:** `Pre-shared key`, `RSA Signature`
- **Lifetime Key:** 3600 detik (atau sesuai kebijakan)
- **Integrity Algorithm:** `SHA-256`
- **Diffie-Hellman Group:** Group 14 (2048-bit)

Contoh Konfigurasi VPN Site-to-Site pada MikroTik

```
/ip ipsec proposal
add name="vpn-proposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc

/ip ipsec peer
add address=192.168.100.1/32 exchange-mode=main secret="vpnpass123" dh-group=modp2048

/ip ipsec policy
add dst-address=192.168.2.0/24 sa-dst-address=192.168.100.1 sa-src-address=192.168.1.1 tunnel=ye
```

2.2 2. Skema Queue Tree

Pembagian Bandwidth Sekolah

Sebuah sekolah memiliki bandwidth sebesar 100 Mbps yang dibagi sebagai berikut:

- 40 Mbps untuk e-learning
- 30 Mbps untuk guru dan staf (akses email, cloud)
- 20 Mbps untuk siswa (browsing umum)
- 10 Mbps untuk CCTV dan update sistem

Konfigurasi Parent dan Child Queue

```
/queue tree
add name="total-bandwidth" parent=global max-limit=100M

add name="e-learning" parent="total-bandwidth" max-limit=40M priority=1
add name="guru-staf" parent="total-bandwidth" max-limit=30M priority=3
add name="siswa" parent="total-bandwidth" max-limit=20M priority=5
add name="cctv-update" parent="total-bandwidth" max-limit=10M priority=8
```

Penandaan Paket (Marking)

Untuk mengarahkan lalu lintas ke antrian yang tepat:

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet new-packet-mark=e-learning-pkt
add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru-staf-pkt p
add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-mark=siswa-pkt passt
add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv-pkt passth
```

Penerapan Marking ke Queue

```
/queue tree
set e-learning packet-mark=e-learning-pkt
set guru-staf packet-mark=guru-staf-pkt
set siswa packet-mark=siswa-pkt
set cctv-update packet-mark=cctv-pkt
```

Referensi

- Odom, W. (2020). *CCNA 200-301 Official Cert Guide*. Cisco Press.
- MikroTik Documentation. (n.d.). *IPSec Configuration Examples*. `https://wiki.mikrotik.com`
- Tanenbaum, A.S. & Wetherall, D.J. (2011). *Computer Networks* (5th ed.). Pearson Education.
- Cisco Systems. (2021). *VPN Configuration Guide*. `https://www.cisco.com`