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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Gilang Gallan Indrana - 5024231030

5 Juni 2025

1 Pendahuluan

1.1 Latar Belakang

Dalam jaringan modern, keamanan dan efisiensi koneksi menjadi kebutuhan utama, terutama bagi organisasi yang memiliki kantor di lokasi berbeda. VPN berbasis IPSec digunakan untuk menjamin keamanan komunikasi antar jaringan dengan cara mengenkripsi dan mengautentikasi data melalui internet. Tanpa VPN, pertukaran data sensitif berisiko disadap atau dimodifikasi pihak tidak berwenang. Selain keamanan, manajemen lalu lintas jaringan juga penting. Layanan seperti e-learning, cloud storage, atau CCTV membutuhkan bandwidth yang stabil. Tanpa pengaturan yang baik, layanan penting bisa terganggu. Oleh karena itu, digunakan QoS (Quality of Service) dengan metode Queue Tree untuk membagi dan memprioritaskan bandwidth sesuai kebutuhan. Kombinasi VPN dan QoS memungkinkan jaringan yang aman dan efisien, menjamin komunikasi terenkripsi sekaligus menjaga kualitas layanan digital yang berjalan di dalamnya.

1.2 Dasar Teori

Virtual Private Network (VPN) dan Quality of Service (QoS) merupakan dua komponen penting dalam manajemen jaringan modern yang berfokus pada aspek keamanan dan efisiensi alokasi bandwidth. VPN, khususnya yang berbasis protokol IPSec (Internet Protocol Security), digunakan untuk membentuk koneksi aman antara dua titik jaringan yang berbeda lokasi, seperti antara kantor pusat dan kantor cabang. IPSec bekerja dengan membentuk “terowongan” aman melalui jaringan publik dengan cara mengenkripsi data yang dikirim dan menjamin bahwa data tersebut tidak dimodifikasi atau disadap oleh pihak ketiga. Proses pengamanan ini dilakukan melalui dua fase negosiasi utama yang dikenal sebagai IKE Phase 1 dan Phase 2. Pada Phase 1, kedua perangkat akan saling bernegosiasi untuk membentuk kanal aman dengan menyepakati parameter keamanan seperti algoritma enkripsi, autentikasi, grup Diffie-Hellman, serta masa berlaku kunci enkripsi. Setelah jalur aman terbentuk, Phase 2 dilanjutkan untuk menyepakati jenis lalu lintas data yang akan dilindungi serta bagaimana perlindungan itu diterapkan, baik menggunakan mode tunnel yang membungkus keseluruhan paket IP maupun mode transport yang hanya mengenkripsi bagian payload-nya. Sementara itu, dalam jaringan yang kompleks dan padat trafik, diperlukan pengaturan lalu lintas data yang efisien agar semua layanan dapat berjalan optimal. Inilah peran penting dari QoS. Salah satu metode implementasi QoS yang umum digunakan adalah Queue Tree. Queue Tree memungkinkan administrator jaringan mengelompokkan dan mengatur bandwidth berdasarkan jenis layanan, protokol, IP address, atau interface tertentu. Melalui mekanisme ini, dibuat struktur antrean bertingkat (parent-child), di mana bandwidth total yang tersedia dibagi ke dalam beberapa kategori lalu lintas data. Untuk mengimplementasikan Queue Tree secara efektif, terlebih dahulu dilakukan proses mangle atau penandaan paket (packet marking), yang memungkinkan router mengenali jenis trafik tertentu seperti e-learning, streaming, atau akses sistem staf. Setiap child queue kemudian dapat dikonfigurasi dengan batas kecepatan minimum, maksimum, serta tingkat prioritas yang berbeda, sehingga layanan penting akan mendapatkan akses bandwidth yang lebih cepat dan stabil. Integrasi antara VPN dan QoS menjadi strategi vital dalam pengelolaan jaringan profesional. VPN menjamin keamanan komunikasi data antar lokasi jaringan, sedangkan QoS menjamin bahwa tiap jenis layanan yang berjalan di jaringan tersebut mendapatkan alokasi bandwidth yang sesuai dengan tingkat kepentingannya. Dalam konteks organisasi seperti perusahaan atau institusi pendidikan, penerapan kedua teknologi ini secara bersamaan ti-

dak hanya meningkatkan keamanan komunikasi data, tetapi juga meningkatkan efisiensi operasional jaringan secara menyeluruh.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:

    - Fase negosiasi IPSec (IKE Phase 1 dan Phase 2) Negosiasi IPSec dibagi menjadi dua fase:
        - IKE Phase 1 bertugas membuat jalur komunikasi aman antara dua perangkat dengan autentikasi dan pembentukan kanal terenkripsi (ISAKMP SA). Parameter keamanan seperti algoritma enkripsi (AES), autentikasi (SHA-256), dan metode pertukaran kunci (Diffie-Hellman) disepakati di tahap ini.
        - IKE Phase 2 (Quick Mode) menghasilkan Security Association (IPSec SA) yang akan digunakan untuk mengamankan data sebenarnya. Pada fase ini, hanya parameter IPSec seperti protokol ESP/AH, jenis enkripsi dan autentikasi, serta lifetime key yang dinegosiasikan.
    - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
        - Enkripsi: AES-256 (standar keamanan tinggi)
        - Autentikasi: HMAC-SHA256 (menjamin integritas dan autentikasi)
        - Lifetime Key: Umumnya 86400 detik (24 jam)
        - Grup DH: Group 14 (2048-bit) untuk keamanan pertukaran kunci
        - Mode: Tunnel Mode untuk komunikasi antar jaringan berbeda (site-to-site)
    - Konfigurasi sederhana pada sisi router untuk memulai koneksi 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
```

2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

    - 40 Mbps untuk e-learning
    - 30 Mbps untuk guru dan staf (akses email, cloud storage)

- 20 Mbps untuk siswa (browsing umum)
- 10 Mbps untuk CCTV dan update sistem

Buatlah skema Queue Tree yang lengkap:

- Parent dan child queue
- Penjelasan marking
- Prioritas dan limit rate pada masing-masing queue

Penandaan (Mangle Rule untuk Mark Packet)

```
/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
```

Queue Tree Configuration

```
/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
```

Referensi

- MikroTik Documentation - IPSec Configuration
  https://help.mikrotik.com/docs/display/ROS/IPsec
- Cisco - IPSec VPN Configuration Guide
  https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-IKE-protocol
  14110-ike-debug.html
- MikroTik Wiki - Queue Tree
  https://wiki.mikrotik.com/wiki/Manual:Queue_Tree
- NetworkLessons - IPSec and Queue Tutorial
  https://networklessons.com/mikrotik/mikrotik-ipsec-site-to-site-vpn
  https://networklessons.com/mikrotik/mikrotik-queue-tree-example