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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Hilmy Abid Syafi Abiyyu - 5024231029

2025

1 Pendahuluan

1.1 Latar Belakang

Penggunaan Virtual Private Network (VPN) seperti PPTP, L2TP, dan EOIP menjadi solusi yang banyak digunakan untuk menjamin keamanan komunikasi data antar jaringan yang terpisah secara geografis. VPN memungkinkan terbentuknya tunnel atau terowongan virtual di atas jaringan publik seperti internet, sehingga data dapat dikirimkan secara terenkripsi dan aman. Selain itu, dengan meningkatnya kebutuhan akses data antar kantor atau perangkat secara jarak jauh, pemahaman dan penerapan protokol-protokol tunneling menjadi esensial dalam dunia jaringan.

Quality of Service (QoS) berkaitan dengan bagaimana bandwidth dibagi dan diprioritaskan untuk jenis trafik tertentu agar performa jaringan tetap optimal, terutama ketika bandwidth terbatas. Fitur seperti Simple Queue, Queue Tree, serta pengaturan Bandwidth Limiting dan Prioritas Traffic memungkinkan administrator jaringan untuk mengendalikan dan mengoptimalkan distribusi data dalam jaringan.

1.2 Dasar Teori

Tunnel adalah teknik untuk mengenkapsulasi paket data agar dapat dikirim melalui jaringan publik dengan cara yang aman. Point-to-Point Tunneling Protocol (PPTP) merupakan protokol VPN yang sederhana dan banyak digunakan karena konfigurasinya mudah, meskipun memiliki kelemahan dari sisi keamanan. Layer 2 Tunneling Protocol (L2TP) adalah pengembangan dari PPTP yang memberikan keamanan lebih baik, terutama jika dikombinasikan dengan IPsec. Sementara itu, Ethernet Over IP (EOIP) adalah protokol tunneling proprietary dari MikroTik yang memungkinkan pengiriman frame Ethernet melalui IP dan sangat berguna untuk menghubungkan dua jaringan lokal seolah-olah berada dalam satu segmen.

Quality of Service (QoS) adalah mekanisme untuk mengatur trafik jaringan agar penggunaan bandwidth dapat disesuaikan dengan kebutuhan. Simple Queue digunakan untuk membatasi bandwidth per IP atau perangkat dengan konfigurasi yang mudah. Queue Tree adalah versi lanjutan yang memungkinkan pengaturan trafik berdasarkan jenis layanan seperti HTTP, VoIP, dan lain-lain serta memberikan prioritas berdasarkan klasifikasi. Dengan Bandwidth Limiting, administrator bisa menetapkan batas kecepatan unggah dan unduh, mencegah pengguna tertentu menghabiskan bandwidth. Prioritas Traffic memungkinkan trafik penting seperti suara atau video untuk mendapatkan jalur lebih cepat daripada trafik lain yang kurang prioritas.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:
   - Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)
   - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
   - Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Pada IKE Phase 1, kedua perangkat biasanya router atau firewall melakukan pertukaran informasi untuk membentuk jalur komunikasi yang aman disebut sebagai ISAKMP Security Association (SA). Di fase ini, dilakukan autentikasi identitas kedua perangkat, pertukaran kunci Diffie-Hellman, serta negosiasi algoritma enkripsi dan metode autentikasi. Fase ini dapat dijalankan dalam dua mode, yaitu Main Mode (lebih aman karena identitas terenkripsi) dan Aggressive Mode (lebih cepat tapi kurang aman). IKE Phase 2, di mana kedua perangkat menyepakati parameter untuk mengamankan lalu lintas data, seperti penggunaan protokol Encapsulating Security Payload (ESP), algoritma enkripsi data, dan masa berlaku kunci. Tunnel IPSec yang terbentuk di fase ini akan digunakan untuk mengirimkan data antar jaringan secara terenkripsi.

Parameter keamanan penting harus disepakati oleh kedua pihak. Algoritma enkripsi seperti AES-256 atau 3DES digunakan untuk menyandikan data agar tidak bisa dibaca oleh pihak yang tidak berwenang. Autentikasi data dilakukan dengan algoritma seperti HMAC-SHA256 untuk memastikan integritas dan keaslian data. Metode autentikasi antar perangkat bisa berupa pre-shared key (PSK), yang umum digunakan karena sederhana, atau sertifikat digital untuk keamanan lebih tinggi. Selain itu, lifetime key juga perlu ditentukan, yaitu durasi berlakunya Security Association sebelum diperbarui misalnya 3600 detik (1 jam) untuk fase 2 dan 86400 detik (1 hari) untuk fase 1.

Memulai koneksi IPSec pada router MikroTik dilakukan dengan mengatur IPsec Proposal yang mencakup algoritma keamanan, membuat IPsec Peer dengan IP tujuan dan shared key, mendefinisikan IPsec Policy untuk menentukan lalu lintas yang dienkripsi, serta memastikan port UDP 500 dan 4500 terbuka di firewall.

2. Koneksi IPSec pada router MikroTik, dimulai dengan - 40 Mbps untuk e-learning
   - 30 Mbps untuk guru $\&$ staf (akses email, cloud storage)
   - 20 Mbps untuk siswa (browsing umum)
   - 10 Mbps untuk CCTV $\&$ update sistem
   Buatlah skema Queue Tree yang lengkap:
   - Parent dan child queue
   - Penjelasan marking
   - Prioritas dan limit rate pada masing-masing queue

Menandai lalu lintas menggunakan fitur Mangle yang kemudian dengan tujuan router bisa mengenali jenis data berdasarkan IP address, protokol, atau port tertentu. Misalnya, lalu lintas dari dan ke platform e-learning ditandai sebagai “e-learning-mark”, IP khusus guru dan staf ditandai sebagai “guru-staf-mark”, subnet siswa ditandai “siswa-mark”, dan IP perangkat CCTV atau server update ditandai “cctv-update-mark”. Penandaan ini dilakukan di menu /ip firewall mangle dengan chain forward dan action mark-packet.

Setelah proses penandaan selesai, Queue Tree dikonfigurasi dengan membuat sebuah parent queue bernama “Total-Bandwidth” dengan parent global dan max-limit=100M. Lalu dibuat child queue untuk masing-masing kategori. Queue untuk e-learning diberi limit-at dan max-limit

40 Mbps dengan prioritas tertinggi (priority=1) karena kebutuhan akses stabil. Untuk guru dan staf, alokasikan 30 Mbps dengan priority=2. Siswa diberi 20 Mbps dengan priority=3, sementara CCTV dan update sistem diberi alokasi 10 Mbps dengan priority=4, karena tidak membutuhkan bandwidth besar secara real-time. Fitur monitoring di MikroTik digunakan untuk memantau penggunaan bandwidth dan memastikan bahwa alokasi berjalan sesuai dengan yang diinginkan sehingga dapat dilakukan monitoring yaitu bandwidth dibagi sesuai kebutuhan dan prioritas masing-masing jenis layanan, sehingga koneksi internet lebih stabil dan efisien.

Link Referensi Tugas Pendahuluan 1
Link Referensi Tugas Pendahuluan 2
Link Referensi Tugas Pendahuluan 3
Link Referensi Tugas Pendahuluan 4
Link Referensi Tugas Pendahuluan 5