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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Susilo Hendri Yudhoyono - 5024231016

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi informasi yang pesat, keamanan komunikasi data antar dua titik atau lebih menjadi kebutuhan yang sangat penting. Di tengah tingginya aktivitas pertukaran data melalui jaringan lokal maupun internet, risiko seperti penyadapan, manipulasi, dan pencurian informasi semakin meningkat. Untuk mengatasi hal ini, digunakanlah teknologi tunneling, yaitu proses membungkus (encapsulation) paket data ke dalam format tertentu agar dapat dikirim secara aman melalui jaringan publik. Tunneling menjadi fondasi utama dalam implementasi Virtual Private Network (VPN), yang memungkinkan dua lokasi berjauhan terhubung secara aman seolah-olah berada dalam satu jaringan lokal. Dengan teknologi ini, komunikasi antar titik tidak hanya menjadi lebih efisien, tetapi juga terlindungi dari berbagai ancaman keamanan siber.

Di tengah meningkatnya penggunaan internet dan jumlah perangkat yang terhubung ke jaringan, efisiensi penggunaan bandwidth menjadi sangat penting agar kinerja jaringan tetap optimal. Tanpa pengelolaan yang tepat, bandwidth dapat terbuang sia-sia dan menyebabkan layanan penting terganggu akibat penggunaan yang tidak seimbang. Oleh karena itu, diperlukan manajemen bandwidth yang mampu mengatur alokasi dan prioritas lalu lintas data secara efisien, agar setiap pengguna dan aplikasi mendapatkan akses sesuai kebutuhannya. Dengan manajemen yang baik, jaringan dapat berfungsi lebih stabil, responsif, dan adil, terutama dalam lingkungan dengan trafik data yang tinggi dan beragam.

1.2 Dasar Teori

Tunneling adalah metode penting dalam jaringan komputer modern yang digunakan untuk mengamankan komunikasi data antara dua titik atau lebih. Dalam praktiknya, tunneling membungkus (encapsulate) paket data asli ke dalam format baru agar dapat dikirim melalui jalur yang terenkripsi dan tidak mudah diakses oleh pihak yang tidak berwenang. Beberapa jenis protokol tunneling yang umum digunakan antara lain GRE (Generic Routing Encapsulation) yang membungkus paket IP dengan header tambahan agar bisa melewati jaringan yang berbeda, serta IP-in-IP yang secara sederhana memasukkan satu paket IP ke dalam paket IP lain. Untuk keamanan tinggi, protokol seperti IPSec (Internet Protocol Security) dan SSH (Secure Shell) digunakan untuk mengenkripsi data sehingga tidak bisa dibaca oleh pihak ketiga. IPSec sendiri bekerja dengan mengenkripsi data, memverifikasi keasliannya, dan membuat jalur aman melalui pertukaran kunci rahasia menggunakan IKE (Internet Key Exchange). IPSec mendukung dua mode yaitu Tunnel Mode yang membungkus seluruh paket IP, dan Transport Mode yang melindungi data tanpa mengganti header aslinya. Protokol dalam IPSec mencakup ESP (Encapsulation Security Payload) untuk enkripsi dan autentikasi, serta AH (Authentication Header) yang hanya menjamin integritas data.

Manajemen bandwidth diperlukan agar penggunaan jaringan tetap efisien dan tidak terjadi pemborosan sumber daya. Di MikroTik, terdapat dua metode utama: Simple Queue, yang mudah digunakan untuk membatasi kecepatan per pengguna atau IP, cocok untuk jaringan kecil; dan Queue Tree, yang lebih kompleks dan fleksibel karena dapat mengelompokkan dan mengatur bandwidth berdasarkan jenis trafik (seperti streaming, gaming, atau download) menggunakan aturan mangle dan struktur antrian bertingkat. Queue Tree lebih cocok untuk jaringan besar yang membutuhkan pembagian bandwidth yang lebih terkontrol dan adil.

2 Tugas Pendahuluan

1. **Konfigurasi VPN IPSec Site-to-Site**

   VPN IPSec terdiri dari dua fase utama:

   - Pada IKE Phase 1, kedua perangkat akan menyepakati beberapa parameter penting untuk membentuk kanal aman (ISAKMP SA), yaitu algoritma enkripsi seperti AES-256 atau 3DES, metode autentikasi seperti Pre-Shared Key (PSK) atau sertifikat digital (RSA), algoritma integritas seperti SHA-256 atau MD5, grup Diffie-Hellman untuk pertukaran kunci (misalnya Group 14), serta masa aktif kunci atau lifetime, biasanya selama 86400 detik (1 hari).
   - IKE Phase 2 akan dilakukan untuk menyepakati parameter IPSec Security Association (IPSec SA), yaitu protokol IPSec yang digunakan (biasanya ESP), algoritma enkripsi (misalnya AES), algoritma integritas (misalnya SHA-256), penggunaan Perfect Forward Secrecy (PFS) yang dapat diaktifkan dengan grup Diffie-Hellman tambahan, masa aktif IPSec SA (biasanya 3600 detik atau 1 jam), dan seleksi lalu lintas (traffic selector) yang menentukan subnet mana saja yang akan diizinkan untuk saling berkomunikasi melalui tunnel.

2. **Manajemen Bandwidth dengan Queue Tree (100 Mbps)**

   Pembagian bandwidth:

   - 40 Mbps untuk e-learning (prioritas 1)
   - 30 Mbps untuk guru dan staf (prioritas 2)
   - 20 Mbps untuk siswa (prioritas 3)
   - 10 Mbps untuk CCTV dan update sistem (prioritas 4)

   Teknis Implementasi:

   - Menggunakan **Queue Tree** dengan satu parent queue (100 Mbps) dan empat child queue sesuai alokasi masing-masing.
   - Trafik ditandai menggunakan marking dengan firewall mangle berdasarkan IP atau jenis pengguna.
   - Setiap queue diberi limit-at, max-limit, dan priority agar layanan penting seperti e-learning tetap lancar meski jaringan sibuk.

Referensi

- https://youtu.be/JYLbNWOCc2c?si=o7Bae548-ZQQ79ca
- https://youtu.be/L_LWTQWOBa8?si=MgpMaRKw7iQLHQ-T
- https://citraweb.com/artikel/372/