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

Laporan Sementara
Praktikum Jaringan Komputer

Tunelling & IP Security

Ferdie Ewaldo Djohan - 5024231017

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, kebutuhan akan konektivitas jaringan yang aman dan efisien menjadi hal yang sangat penting bagi organisasi, perusahaan, dan institusi pendidikan. Tantangan utama yang dihadapi adalah bagaimana menciptakan komunikasi data yang aman antara lokasi yang berbeda, sambil memastikan penggunaan bandwidth yang optimal dan terdistribusi secara adil. Teknologi Virtual Private Network (VPN) dengan protokol IPSec telah menjadi solusi standar industri untuk mengatasi masalah keamanan komunikasi data melalui jaringan publik seperti internet. IPSec menyediakan layanan autentikasi, enkripsi, dan integritas data yang memungkinkan organisasi untuk menghubungkan kantor pusat dengan cabang-cabang secara aman tanpa harus mengeluarkan biaya besar untuk infrastruktur jaringan pribadi. Selain aspek keamanan, manajemen bandwidth juga menjadi perhatian utama dalam administrasi jaringan. Dengan terbatasnya bandwidth yang tersedia dan beragamnya kebutuhan aplikasi, diperlukan sistem Quality of Service (QoS) yang dapat mengatur prioritas dan alokasi bandwidth secara efektif. Implementasi Queue Management memungkinkan administrator jaringan untuk memastikan bahwa aplikasi kritis mendapat prioritas yang tepat, sementara aplikasi yang kurang penting dapat dibatasi penggunaan bandwidth-nya.

1.2 Dasar Teori

VPN adalah teknologi yang memungkinkan pembuatan koneksi jaringan privat melalui jaringan publik seperti internet menggunakan konsep tunneling, yaitu proses encapsulation data dari satu jaringan ke dalam format yang dapat diteruskan melalui jaringan lain yang berbeda. Proses ini melibatkan pembungkusan data asli dengan header tambahan untuk dapat melewati infrastruktur jaringan yang berbeda, kemudian dibuka kembali di sisi penerima. IPSec merupakan suite protokol keamanan yang menyediakan layanan autentikasi, enkripsi, dan integritas data pada layer network. IPSec bekerja dengan mengenkripsi dan mengautentikasi setiap paket IP yang dikirimkan melalui jaringan. Fitur utama IPSec mencakup autentikasi untuk memastikan data berasal dari sumber yang legitimate, enkripsi untuk mengacak isi data, integritas data untuk mencegah perubahan selama transmisi, dan manajemen kunci untuk distribusi kunci enkripsi yang aman. IPSec dapat beroperasi dalam Transport Mode (enkripsi payload saja) atau Tunnel Mode (enkripsi seluruh paket IP dengan header baru). IKE adalah protokol yang bertanggung jawab untuk negosiasi parameter keamanan dan pertukaran kunci dalam implementasi IPSec. Proses IKE terdiri dari dua fase utama. IKE Phase 1 membentuk secure channel antara dua peer IPSec dengan melakukan autentikasi identitas dan negosiasi parameter keamanan seperti algoritma enkripsi, algoritma hash, metode autentikasi, dan Diffie-Hellman group. IKE Phase 2 menggunakan secure channel dari Phase 1 untuk menegosiasikan IPSec Security Association yang melindungi data traffic aktual, termasuk protokol IPSec (ESP atau AH), algoritma enkripsi dan autentikasi untuk data traffic, serta lifetime Security Association. Quality of Service (QoS) adalah mekanisme untuk mengontrol dan mengoptimalkan penggunaan bandwidth jaringan. Dalam router MikroTik, terdapat dua pendekatan utama yaitu Simple Queue dan Queue Tree. Simple Queue merupakan metode sederhana untuk mengatur bandwidth per pengguna atau IP tanpa konfigurasi marking yang kompleks, cocok untuk jaringan kecil hingga menengah. Queue Tree menawarkan fleksibilitas tinggi dengan struktur hierarkis parent-child queue yang memungkinkan pembagian bandwidth granular berdasarkan jenis aplikasi, protokol, atau kategori pengguna, namun memerlukan mangle rules

untuk marking packet atau connection.

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)
   - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
   - Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site
   = IKE Phase 1 (Main Mode atau Aggressive Mode) dimulai dengan inisiasi koneksi dari salah satu peer IPSec. Kedua router bertukar proposal algoritma keamanan yang didukung, termasuk algoritma enkripsi (seperti AES-256, 3DES), algoritma hash (SHA-1, SHA-256), metode autentikasi (pre-shared key, certificate), dan Diffie-Hellman group untuk key exchange. Setelah parameter disepakati, kedua router melakukan autentikasi mutual dan menghasilkan shared secret yang akan digunakan untuk mengenkripsi komunikasi Phase 2. IKE Phase 2 (Quick Mode) menggunakan secure tunnel yang telah dibentuk pada Phase 1 untuk menegosiasikan IPSec Security Association. Dalam fase ini, parameter yang dinegosiasikan meliputi protokol IPSec (ESP untuk enkripsi dan autentikasi, atau AH untuk autentikasi saja), algoritma enkripsi untuk data traffic (AES, 3DES), algoritma autentikasi (HMAC-SHA1, HMAC-MD5), dan Perfect Forward Secrecy (PFS) group jika diperlukan. Algoritma enkripsi menentukan metode pengacakan data. AES-256 direkomendasikan untuk keamanan tinggi, sementara AES-128 memberikan keseimbangan antara keamanan dan performa. Metode autentikasi dapat menggunakan pre-shared key untuk implementasi sederhana atau digital certificate untuk skala enterprise. Lifetime key menentukan durasi validitas kunci enkripsi, dengan rekomendasi 8 jam untuk Phase 1 dan 1 jam untuk Phase 2 untuk menjaga keamanan optimal. Pada router kantor pusat, konfigurasi dimulai dengan pembuatan IPSec proposal yang mendefinisikan algoritma enkripsi dan autentikasi. Selanjutnya, dibuat IPSec peer yang menentukan alamat IP remote peer dan metode autentikasi. IPSec policy menghubungkan proposal dengan peer dan menentukan traffic yang akan dienkripsi berdasarkan source dan destination network. Terakhir, diperlukan konfigurasi routing untuk mengarahkan traffic antar-site melalui tunnel IPSec. Router cabang dikonfigurasi dengan parameter yang mirror dengan kantor pusat, dengan penyesuaian pada alamat IP peer dan network yang akan di-tunnel. Penting untuk memastikan bahwa kedua router memiliki konfigurasi yang sinkron untuk memungkinkan negosiasi IPSec yang sukses.

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

= Parent Queue utama dibuat dengan nama "Total-Bandwidth" dengan limit 100 Mbps yang akan menjadi root dari semua child queue. Di bawahnya, dibuat empat child queue utama: "E-Learning" (40 Mbps), "Staff-Network" (30 Mbps), "Student-Network" (20 Mbps), dan "Infrastructure" (10 Mbps). Child queue "E-Learning" dapat dipecah lebih lanjut menjadi sub-kategori seperti "Video-Streaming" (25 Mbps untuk platform pembelajaran video), "Interactive-Content" (10 Mbps untuk quiz dan simulasi), dan "File-Upload" (5 Mbps untuk pengumpulan tugas). Child queue "Staff-Network" dibagi menjadi "Email-Services" (10 Mbps), "Cloud-Storage" (15 Mbps), dan "Administrative-System" (5 Mbps). Implementasi Queue Tree memerlukan mangle rules untuk mengidentifikasi dan marking traffic berdasarkan kriteria tertentu. Untuk traffic e-learning, marking dilakukan berdasarkan destination port HTTP/HTTPS dan domain name dari platform pembelajaran. Traffic staff diidentifikasi berdasarkan source IP address dari subnet khusus staff atau berdasarkan protokol seperti IMAP/POP3 untuk email dan WebDAV untuk cloud storage. Marking traffic siswa dapat dilakukan berdasarkan source IP subnet siswa dengan exception untuk akses ke platform pembelajaran yang akan di-route ke queue e-learning. Traffic infrastructure diidentifikasi berdasarkan destination port RTSP untuk CCTV dan protokol update system yang spesifik. Priority queue diberikan nilai 1-8, dengan nilai 1 sebagai prioritas tertinggi. E-Learning mendapat prioritas 1 untuk memastikan kelancaran proses pembelajaran. Staff-Network mendapat prioritas 2 untuk mendukung operasional administrasi. Student-Network mendapat prioritas 3 untuk browsing umum. Infrastructure mendapat prioritas 4 sebagai background service. Limit-at untuk setiap queue ditetapkan sebagai guaranteed bandwidth minimum, sementara max-limit ditetapkan sebagai batas maksimum. Burst threshold dan burst time dikonfigurasi untuk memberikan fleksibilitas penggunaan bandwidth sesaat ketika ada spare capacity dari queue lain.