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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dengan IPsec

Arhya Hafidz Hafidin - 5024231042

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital saat ini, kebutuhan akan komunikasi data yang aman dan efisien menjadi semakin krusial, terutama bagi organisasi atau institusi yang memiliki banyak cabang atau unit yang tersebar. Salah satu cara untuk menjaga keamanan dan integritas data saat melintasi jaringan publik adalah melalui penggunaan teknologi Virtual Private Network (VPN), khususnya dengan protokol IPSec. Dengan menggunakan IPSec tunneling, dua lokasi yang terpisah dapat terhubung secara aman melalui internet, seakan-akan berada dalam satu jaringan lokal. Praktikum ini memberikan pengalaman langsung mengenai proses konfigurasi dan negosiasi IPSec, serta bagaimana teknologi tersebut dapat diterapkan untuk mengamankan jaringan dalam situasi nyata.

Selain fokus pada aspek keamanan, pengelolaan lalu lintas jaringan juga menjadi elemen penting dalam menjaga kualitas layanan (Quality of Service). Dalam lingkungan jaringan yang memuat berbagai jenis trafik—seperti e-learning, streaming video, penelusuran internet, hingga sistem pengawasan CCTV dibutuhkan strategi untuk membagi dan memprioritaskan bandwidth sesuai kebutuhan masing-masing. Praktikum ini juga mencakup pembelajaran tentang perbedaan antara Simple Queue dan Queue Tree, serta cara melakukan konfigurasi dan penandaan trafik (packet marking) untuk mengelola sumber daya jaringan secara lebih efektif dan efisien.

1.2 Dasar Teori

IPSec (Internet Protocol Security) merupakan kumpulan protokol yang dirancang untuk melindungi komunikasi berbasis IP melalui proses otentikasi dan enkripsi. Proses kerja IPSec terbagi dalam dua tahap negosiasi, yaitu IKE Phase 1 dan IKE Phase 2. Pada tahap pertama, dibentuk jalur komunikasi yang aman antara dua perangkat dengan cara melakukan pertukaran kunci dan autentikasi. Selanjutnya, pada tahap kedua, dibentuk Security Association (SA) yang digunakan untuk mengenkripsi lalu lintas data yang dikirimkan. IPSec menyediakan dua mode utama, yakni transport mode dan tunnel mode, di mana tunnel mode sering digunakan untuk menghubungkan dua jaringan yang berbeda secara aman melalui internet.

Dalam hal pengelolaan bandwidth, terdapat dua metode yang umum digunakan pada perangkat MikroTik, yaitu Simple Queue dan Queue Tree. Simple Queue memiliki konfigurasi yang lebih sederhana dan cocok untuk membatasi bandwidth per perangkat, namun kurang efektif jika digunakan dalam pengaturan prioritas trafik yang lebih kompleks. Sebaliknya, Queue Tree memungkinkan pembagian dan pengelompokan bandwidth berdasarkan jenis trafik dengan prioritas yang berbeda. Metode ini memerlukan penandaan paket (packet marking) menggunakan fitur Mangle. Melalui pendekatan ini, administrator jaringan dapat menjamin alokasi bandwidth minimum bagi layanan penting dan menurunkan prioritas untuk trafik yang kurang penting, sehingga kualitas layanan jaringan tetap optimal.

2 Tugas Pendahuluan

1. Studi kasus konfigurasi VPN IPSec: Sebuah perusahaan ingin menghubungkan kantor pusat dengan cabang secara aman. Jelaskan prosesnya secara rinci:
   Negosiasi dalam IPSec dilakukan dalam dua fase utama:

- **Fase IKE 1**: Merupakan tahap awal untuk membentuk koneksi aman antara dua perangkat melalui autentikasi dan pembuatan saluran terenkripsi, dikenal sebagai ISAKMP SA. Dalam tahap ini, dilakukan kesepakatan parameter keamanan seperti algoritma enkripsi (contohnya AES), autentikasi (misalnya SHA- 256), serta metode pertukaran kunci (Diffie-Hellman).
- **Fase IKE 2 (Quick Mode**): Tahapan ini menghasilkan IPSec SA yang digunakan untuk mengenkripsi data yang ditransmisikan. Parameter yang disepakati meliputi protokol keamanan (ESP atau AH), algoritma enkripsi dan autentikasi, serta masa aktif kunci (key lifetime).

Parameter Keamanan yang Digunakan
Beberapa parameter keamanan umum yang diterapkan antara lain:

- Algoritma Enkripsi: AES-256 untuk tingkat keamanan tinggi
- Algoritma Autentikasi: HMAC-SHA256 untuk menjaga integritas dan keaslian data
- Key Lifetime: 86400 detik (24 jam)
- Diffie-Hellman Group: Group 14 (2048-bit)
- Mode Operasi: Tunnel Mode untuk komunikasi antar jaringan berbeda

Contoh Konfigurasi Router (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

Konfigurasi di atas menggambarkan penerapan koneksi IPSec secara sederhana pada router dengan parameter keamanan sesuai standar untuk membentuk VPN antar kantor.

2. Manajemen Bandwidth dan Prioritas pada Router

- **Pengelolaan Antrian (Queue Management)**: Pembagian bandwidth dilakukan dengan membuat antrian utama (parent) dan beberapa antrian turunan (child) untuk tiap jenis layanan. Sebagai contoh, total bandwidth sebesar 100 Mbps dapat dialokasikan menjadi: 40 Mbps untuk layanan e-learning, 30 Mbps untuk akses guru dan staf, 20 Mbps untuk pengguna siswa, dan 10 Mbps untuk kebutuhan CCTV serta pembaruan sistem.

- **Penandaan Paket (Packet Marking)**: Paket data yang melewati jaringan diberi tanda untuk mengelompokkan jenis lalu lintas. Penandaan ini digunakan agar trafik dapat dikenali, diprioritaskan, dan diarahkan sesuai jalur yang ditentukan dalam tabel routing.
- **Prioritas dan Batasan Bandwidth**:
  – Layanan e-learning diberikan prioritas tertinggi (1), dengan batas maksimal penggunaan 20 Mbps.
  – Akses guru dan staf memiliki prioritas menengah (2), dengan batas maksimum 15 Mbps.
  – Pengguna siswa mendapatkan prioritas rendah (3), dibatasi hingga 10 Mbps.
  – Lalu lintas untuk CCTV dan pembaruan sistem berada pada prioritas terendah (4), dengan batasan maksimal 5 Mbps.