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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Theo Kawalisa Pinem - 5024231008

2025

multirow

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi jaringan komputer saat ini, kebutuhan untuk menghubungkan berbagai jaringan yang berbeda jenis semakin meningkat. Salah satu solusi yang banyak digunakan adalah dengan menggunakan teknik tunneling. Tunneling memungkinkan data dari satu perangkat melewati jaringan yang tidak sejenis, seperti dari jaringan lokal (LAN) ke jaringan luas (WAN), dengan cara membungkus data agar bisa dikenali dan diteruskan oleh jaringan perantara. Proses ini penting karena tidak semua jaringan bisa langsung saling terhubung tanpa bantuan teknologi semacam ini. Selain itu, tunneling juga sering digunakan dalam pengamanan jaringan seperti VPN (Virtual Private Network), di mana data yang dikirimkan perlu dienkripsi agar aman dari gangguan pihak ketiga. Melalui praktikum ini, praktikan diharapkan bisa memahami bagaimana cara kerja tunneling serta mengenal jenis-jenis protokol yang digunakan, seperti GRE, IPSec, hingga SSH dan L2TP, sehingga nantinya bisa diterapkan dalam konfigurasi jaringan nyata.

1.2 Dasar Teori

Tunneling adalah teknik dalam jaringan komputer yang digunakan untuk mengirim data dari satu jaringan ke jaringan lain dengan membungkus (encapsulation) data asli ke dalam format yang sesuai dengan jaringan perantara. Proses ini bisa diibaratkan seperti memasukkan satu paket ke dalam paket lainnya, agar bisa dikirim melalui jalur yang tidak langsung kompatibel dengan paket aslinya. Setelah data sampai di tujuan, paket pembungkus akan dibuka (decapsulation) sehingga data kembali ke bentuk semula. Beberapa protokol tunneling yang umum digunakan antara lain GRE (Generic Routing Encapsulation), IP-in-IP, dan protokol yang lebih aman seperti IPSec dan SSH.

Salah satu protokol tunneling yang cukup populer adalah IPSec. IPSec merupakan protokol yang memberikan perlindungan terhadap data melalui proses enkripsi dan autentikasi. Cara kerjanya dimulai dari pertukaran kunci antara dua perangkat melalui proses yang disebut IKE (Internet Key Exchange), lalu dilanjutkan dengan pengiriman data melalui terowongan aman. IPSec mendukung dua mode operasi, yaitu Tunnel Mode yang mengenkripsi seluruh paket data termasuk alamat IP, dan Transport Mode yang hanya mengenkripsi bagian isi dari data. Selain itu, protokol ini juga dilengkapi dengan fitur seperti ESP (Encapsulation Security Payload) dan AH (Authentication Header) yang bertugas untuk memastikan integritas dan keamanan data.

Dengan mempelajari dasar teori tunneling dan praktik langsung melalui simulasi, mahasiswa diharapkan dapat memahami konsep dan implementasi tunneling dalam jaringan komputer, serta dapat membedakan dan memilih jenis protokol yang sesuai dengan kebutuhan jaringan tertentu.

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:

(a) Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)

Jawaban :

IKE Phase 1

Tujuan utama dari fase ini adalah membangun ISAKMP Security Association (SA) antara dua router yang berperan sebagai endpoint VPN. Di fase ini, dilakukan pertukaran informasi untuk membangun jalur komunikasi yang aman dan terenkripsi.

Langkah - langkah :

i. Autentikasi dilakukan menggunakan pre-shared key, digital certificate, atau metode lain.
ii. Negosiasi parameter keamanan seperti algoritma enkripsi dan hash.
iii. Proses Diffie-Hellman key exchange untuk menghasilkan shared secret (kunci bersama).
iv. Terbentuknya Secure Tunnel (ISAKMP SA) yang digunakan untuk mengamankan fase berikutnya.

IKE Phase 2

Setelah fase 1 berhasil, dilanjutkan ke fase 2 untuk membuat IPSec SA, yaitu jalur aman tempat lalu lintas data akan dikirim.

Langkah - langkah :

i. Negosiasi parameter enkripsi dan autentikasi untuk trafik data.
ii. Menentukan protokol IPSec yang akan digunakan: ESP (Encapsulation Security Payload) atau AH (Authentication Header).
iii. Penentuan lifetime key (masa berlaku sesi).
iv. Setelah selesai, koneksi aman siap digunakan untuk komunikasi data.

(b) Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

Jawaban :

Agar koneksi VPN berhasil dan aman, kedua pihak (kantor pusat dan cabang) harus menyepakati parameter beserta keterangannya seperti berikut:

i. Algoritma Enkripsi : Digunakan untuk menyamarkan isi data. Contoh: AES-256, 3DES
ii. Algoritma Hashing : Menjamin integritas data. Contoh: SHA-256, SHA-1
iii. Metode Autentikasi : Biasanya menggunakan Pre-Shared Key (PSK) atau Digital Certificate
iv. Diffie-Hellman Group : Menentukan kekuatan kunci. Contoh: Group 14 (2048-bit), Group 5 (1536-bit)
v. Lifetime Key : Masa berlaku koneksi sebelum renegosiasi. Biasanya: 3600 detik
vi. Mode : Tunnel Mode (untuk site-to-site)

(c) Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Jawaban :

Asumsi IP Addteess :

i. Kantor Pusat: 192.168.1.0/24, IP Router: 10.0.0.1
ii. Kantor Cabang: 192.168.2.0/24, IP Router: 10.0.0.2

Konfigurasi di MikroTik :

```
/ip ipsec peer add address=10.0.0.2 exchange-mode=main secret="vpnkey" /ip ipsec
proposal add name="vpn-proposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc
pfs-group=modp2048 /ip ipsec identity add peer=10.0.0.2 secret="vpnkey" /ip ipsec
policy add src-address=192.168.1.0/24 dst-address=192.168.2.0/24  sa-dst-address=10.0.0
sa-src-address=10.0.0.1 tunnel=yes proposal=vpn-proposal
```

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

   (a) 40 Mbps untuk e-learning

   (b) 30 Mbps untuk guru & staf (akses email, cloud storage)

   (c) 20 Mbps untuk siswa (browsing umum)

   (d) 10 Mbps untuk CCTV & update sistem

   Buatlah skema Queue Tree yang lengkap:

   (a) Parent dan child queue

   (b) Penjelasan marking

   (c) Prioritas dan limit rate pada masing-masing queue

   (a) Parent dan Child Queue
   Jawaban :
   Parent Queue : Interface ether1, Max Limit: 100 Mbps
   Child Queue :

      i. e-learning: 40 Mbps (Prioritas 1)
      ii. guru-staf: 30 Mbps (Prioritas 2)
      iii. siswa: 20 Mbps (Prioritas 3)
      iv. cctv-sistem: 10 Mbps (Prioritas 4)

   (b) Penjelasan Marking
   Jawaban :
   Trafik ditandai menggunakan IP > Firewall > Mangle berdasarkan IP atau layanan masing-masing.
   Mark digunakan untuk menghubungkan trafik dengan child queue yang sesuai.
   Contoh :

      i. IP server e-learning → mark packet → e-learning
      ii. IP guru/staf → mark packet → guru-staf

   (c) Prioritas dan Limit Rate
   Jawaban :

Tabel 1: Prioritas dan Limit Bandwidth

Kategori	Limit Bandwidth	Prioritas
E-learning	40 Mbps	1 (Tertinggi)
Guru & Staf	30 Mbps	2
Siswa	20 Mbps	3
CCTV & Sistem	10 Mbps	4

Referensi :

1. MikroTik Wiki: https://wiki.mikrotik.com/wiki/Manual:Queue
2. MikroTik Mangle and Queue Tree Configuration Guides