



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

Laporan Sementara Praktikum Jaringan Komputer

Modul 5

Fioreno Malvin T - 5024231004

2025

1 Pendahuluan

1.1 Latar Belakang

IPSec dibuat untuk kebutuhan melindungi data sensitif yang dikirim melalui jaringan-jaringan publik seperti internet. Teknologi seperti VPN menggunakan IPSec pada dasarnya, dan memungkinkan pengiriman data antar lokasi, misalnya kantor pusat ke cabang secara aman dan efisien.

1.2 Dasar Teori

IPSec atau Internet Protocol Security adalah protokol keamanan yang digunakan untuk mengamankan komunikasi data melalui jaringan IP dengan mengenkripsi dan mengotentikasi paket-paket data, layaknya sebuah VPN. IPSec terdiri dari dua fase, yaitu IKE Phase 1 dan Phase 2. IKE Phase 1 membentuk saluran terenkripsi kedua end point, dan IKE Phase 2 handle parameter untuk mengamankan data, seperti algoritma enkripsi dan/atau metode autentikasi.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. Pada IKE Phase 1, fase ini mempersiapkan saluran yang aman dan mengautentikasi kedua endpoint. Sedangkan IKE Phase 2 membentuk tunnel IPSec agar transfer data menjadi aman. Parameter keamanan yang harus disepakati meliputi algoritma enkripsi (contohnya AES128), algoritma autentikasi (contohnya HMAC-SHA1), metode autentikasi (contohnya PSK/pre shared keys), diffie-hellman group, lifetime (84600 detik untuk phase 1 dan 3600 detik untuk phase 2)
2. Parent 100Mbps (GLOBAL), child Elearning 40Mbps prioritas 1,, Child guru dan staf 30Mbps prioritas 2, Siswa 20Mbps prioritas 3, CCTV dan update sistem 10Mbps prioritas 4
3. Referensi: Cisco Community – IPsec Tunnel: Understanding Phase 1 and 2; NetworkLessons – IPsec (Internet Protocol Security); Mikrotik Docs – IPsec and Site-to-Site Example; Mikrotik Docs – Queues and PCQ Example .