BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil pengujian implementasi *Virtual Private Network (VPN)* dengan protokol *L2TP/IPSec* pada *router* MikroTik RB951Ui-2HnD, maka didapatkan kesimpulan untuk menjawab rumusan masalah penelitian sebagai berikut:

1. Implementasi *VPN L2TP/IPSec* pada *router* MikroTik RB951Ui-2HnD dapat dilakukan tanpa memerlukan perangkat lunak dan lisensi tambahan karena sudah memiliki fitur tersebut didalamnya. Konfigurasi dapat dilakukan secara mudah menggunakan aplikasi Winbox dengan pembuatan *IP Pool*, *PPP profile*, menambahkan *user secret*, serta pengaturan *IPSec* untuk keamanan lalu lintas data. Klien Windows akan terhubung ke *VPN* menggunakan metode autentikasi *username* dan *password* serta *pre-shared key*.
2. Simulasi pengujian yang dilakukan menunjukkan bahwa protokol *VPN L2TP/IPSec* efektif melindungi data dalam lalu lintas jaringan lokal dari upaya serangan *Sniffing* dan *Man-in-the-Middle (MITM)*. Pada saat pengujian sniffing dalam kondisi *VPN* nonaktif, data seperti *IP Address*, paket *ICMP (ping)*, serta data lainnya dapat terbaca jelas oleh Wireshark di Kali Linux. Namun, setelah *VPN* diaktifkan, lalu lintas jaringan terenkripsi menggunakan protokol *ESP (Encapsulating Security Payload)*, sehingga data tidak dapat dibaca. Sedangkan dalam pengujian *Man-in-the-Middle (MITM)* menggunakan Ettercap, ketika kondisi *VPN* nonaktif informasi *login HTTP* yang dilakukan oleh klien Windows berhasil disadap. Namun setelah *VPN* diaktifkan, meskipun *ARP spoofing* berhasil dilakukan, Ettercap tidak dapat menampilkan isi data karena komunikasi telah terenkripsi oleh protokol *IPSec*.
3. Pengujian *Quality of Service (QoS)* menggunakan iperf3 menunjukkan bahwa implementasi VPN L2TP/IPSec berdampak pada penurunan performa jaringan. Rata-rata *throughput* turun dari 380 Mbps menjadi 10 Mbps saat VPN aktif, *latency* meningkat dari 0,93 ms menjadi 4,4 ms, dan *jitter* naik dari 2,55 ms menjadi 7,34 ms, sementara *packet loss* tetap 0% pada kedua

kondisi. Penurunan performa ini disebabkan beban kerja enkripsi-dekripsi protokol *IPSec* dan keterbatasan performa *router* MikroTik RB951Ui-2HnD ditunjukan dari *load CPU* yang mencapai 100% saat skenario berlangsung. Namun, jaringan masih stabil dan aspek keamanan jaringan meningkat.

5.2 Saran

Berdasarkan hasil penelitian ini, maka disampaikan beberapa saran sebagai berikut:

1. Penelitian lanjutan menggunakan topologi lebih kompleks seperti *site-to-site VPN* untuk mensimulasikan skenario dunia nyata,
2. Gunakan *router* dengan spesifikasi yang lebih tinggi agar proses enkripsi tidak terlalu membebani *CPU* dan meningkatkan performa jaringan.
3. Menambahkan kofigurasi *firewall* dan *filter rules* unutk memperkuat keamanan jaringan.
4. Kembangkan skenario keamanan *Virtual Private Network (VPN)* bukan hanya serangan *Sniffing* dan *Man-in-the-Middle (MITM)*.