BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat diperoleh simpulan sebagai berikut:

1. Algoritma stream cipher Rabbit berhasil diimplementasikan pada OpenVPN dalam bentuk *ciphersuites* Rabbit. OpenVPN membutuhkan *library* atau aplikasi lain untuk mensuplai algoritma kriptografi, salah satunya yaitu OpenSSL. Proses kompilasi antara *source code* OpenSSL dan *source code* OpenVPN dilakukan dengan skrip atau perintah khusus agar OpenVPN dapat mengenali algoritma baru yang diimplementasikan pada OpenSSL. Hasil modifikasi OpenVPN dari penelitian ini disebut dengan OpenVPN-R.
2. Tahap pembuatan perangkat AR-6000 pada penelitian ini meliputi:
    a. Kompilasi dan instalasi OpenVPN-R sebagai aplikasi inti pada SBC Raspberry Pi 3 Model B+
    b. Konfigurasi kartu jaringan (*networking*), *Secured Shell* (SSH) *server*
    c. Instalasi *Shoreline Firewall* (*Shorewall*) untuk membantu proses *routing*, IP *masquerading*, dan IP *forwarding*.
3. *Ciphersuites* Rabbit yang telah diimplementasikan pada OpenVPN-R memiliki performa yang relatif lebih baik untuk

mentransfer data dengan ukuran mulai dari yang kecil (1 MB) hingga ukuran yang besar (5 MB, 10 MB, 50 MB, 100 MB), selain itu pada penggunaan memori dan CPU Utilization pun relatif lebih baik.

4. Perangkat AR-6000 dari hasil penelitian ini dapat digunakan untuk melakukan *remote access* melalui jaringan lokal atau jaringan publik (internet). Perangkat ini memiliki kemampuan untuk melakukan mutual *authentication* dengan VPN *relay server* yang dituju dan melindungi transaksi data *traveler user* yang sedang mengakses internal *resources*-nya. Selain itu, perangkat ini juga dapat digunakan secara *platform independent*, relatif efisien dalam instalasi VPN pada PC, dan memiliki fitur tambahan *inbuilt firewall* dengan memanfaatkan *Shorewall* yang telah dinstall pada SBC Raspberry Pi 3 Model B+.

5.2 Saran

Perangkat AR-6000 pada penelitian ini masih dapat dikembangkan pada penelitian selanjutnya, antara lain:

1. Perlu dilakukan penelitian lebih lanjut untuk membuat *Graphical User Interface* (GUI) yang lebih baik, sehingga dapat memudahkan user untuk mengoperasikan perangkat AR-6000. Pembuatan UI tersebut dapat dilakukan dengan berbasis web. Salah satu contoh UI yang dibutuhkan adalah untuk konfigurasi koneksi perangkat AR-6000 ke WLAN *access point*.

2. Perlu dilakukan penelitian lebih lanjut untuk menambah fitur pada perangkat AR-6000. Contohnya adalah fitur personal *secure data storage* dan personal *message*/*file encryption*.
3. Perlu dilakukan penelitian lebih lanjut untuk menerapkan sistem proteksi pada perangkat AR-6000, diantaranya adalah *tamperproof* dan *zeroize* ketika microSD card pada perangkat dicabut. Sehingga dapat menutup kemungkinan adanya *cloning* microSD card oleh pihak yang tidak memiliki otoritas.