VIRTUAL PRIVATE NETWORK DENGAN ALGORITMA RABBIT SEBAGAI PENGAMANAN TRANSMISI DATA

ABSTRAK

Virtual Private Network (VPN) merupakan metode untuk membangun jaringan privat dengan memanfaatkan infrastruktur jaringan publik seperti internet. Penelitian ini dilakukan dengan tujuan untuk membuat prototipe perangkat personal VPN *gateway* yang dapat digunakan untuk mengamankan *remote access* seorang *traveler user* ke dalam internal *resources*-nya. Prototipe perangkat personal VPN gateway ini dibuat dengan menggunakan aplikasi inti OpenVPN-R yang merupakan hasil modifikasi dari OpenVPN versi 2.3.10 dengan OpenSSL versi 1.0.2h dan diimplementasikan ke dalam sebuah *Single Board Computer* (SBC) Raspberry Pi 3 Model B+. Modifikasi yang dilakukan adalah dengan menambahkan algoritma *stream cipher* Rabbit pada OpenSSL sebagai salah satu alternatif pilihan TLS *ciphersuites* pada OpenVPN. Prototipe perangkat personal VPN *gateway* yang dihasilkan dari penelitian ini memiliki *ciphersuites* Rabbit, dapat bekerja secara *platform independent*, dan memiliki fitur tambahan *inbuilt firewall*. Dari hasil pengujian performa diperoleh hasil bahwa *ciphersuites* 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 dibandingkan dengan *ciphersuites* algoritma standar lainnya seperti AES-256, Camellia-256, Triple-DES (3DES), dan Seed.(R)

Kata kunci *:* Algoritma *Stream Cipher* Rabbit, OpenVPN-R, SBC Raspberry Pi 3 Model B+, VPN-SSL

VIRTUAL PRIVATE NETWORK DENGAN ALGORITMA RABBIT SEBAGAI PENGAMANAN TRANSMISI DATA

ABSTRACT

Virtual Private Network (VPN) is a method to build private network by utilizing public network infrastructure such as internet. This research was conducted with the aim to create prototype personal device VPN gateway that can be used to secure the remote access of a traveler user into its internal resources. The prototype of the VPN personal gateway device is built using OpenVPN-R core applications that are modified from OpenVPN version 2.3.10 with OpenSSL version 1.0.2h and implemented into a single Board Computer SBp Raspberry Pi 3 Model B +. The modification is to add Rabbit stream cipher algorithm to OpenSSL as one of the alternative options of TLS ciphersuites on OpenVPN. The prototype personal VPN gateway device generated from this research has Rabbit ciphersuites, can work platform independent, and has additional features inbuilt firewall. From the results of performance testing results show that ciphersuites have relatively better performance to transfer data from small size (1 MB) to large size (5 MB, 10 MB, 50 MB, 100 MB), in addition to memory usage and CPU Utilization was relatively better compared to other standard algorithm ciphersuites such as AES-256, Camellia-256, Triple-DES (3DES), and Seed. (R)

Keywords: Stream Cipher Rabbit Algorithm, OpenVPN-R, SBC Raspberry Pi 3 Model B+, VPN-SSL