ABSTRAK

Meningkatnya kebutuhan akses internet yang cepat dan aman menjadi hal penting bagi setiap perusahaan terutama yang berkaitan dengan pembiayaan dan investasi. Seperti FIF kantor cabang dan kantor pusat berkomunikasi melalui koneksi MPLS. Banyak aplikasi dan website yang digunakan terganggu sehingga membuat link lalu lintas data berfokus pada satu koneksi saja. Oleh karena itu Penelitian ini bertujuan untuk meningkatkan kinerja layanan jaringan, pengelolaan lalu lintas data, dan peningkatan keamanan jaringan pada perususahaan.

Penelitian ini menggunakan dua metodelogi: metodelogi *active/passive* dan metodelogi *firewall filtering*. Metodelogi *active/passive* bertujuan untuk menguji perangkat fortigate dengan konfigurasi *failover* yang memastikan ketersediaan dan keandalan jaringan Astinet dan VPN IPsec. Metodelogi *firewall filtering* digunakan untuk melindungi keamanan jaringan data.

Hasil pengujian menunjukkan bahwa *Auto Link Failover* memiliki persentase paket loss VPN IPsec 11% dan astinet 6%. Kemudian perbandingan hasil kecepatan transfer data antara link Astinet dan VPN IPsec dalam kondisi dengan satu link saja, adalah 36,41 bps, 24,79 bps, 7,95 bps, dan 5,35 bps pada link Astinet, sedangkan pada link VPN IPsec adalah 1860 bps, 9,28 bps, 31,63 bps, dan 2,63 bps. *Traffic streering* yang didapatkan dengan rata-rata *bandwidth* yang digunakan VPN IPsec 1980 bps sedangkan Astinet 3180 bps sedikit lebih besar dan tetap dapat *load balancing*. Kemudian Fitur web filtering yang diimplementasikan pada fortigate dapat membatasi akses ke situs – situs atau web dan memblokir download file yang terproteksi sebagai data yang teridentifikasi tidak diperbolehkan diakses pada perangkat fortigate SD-WAN.

Kata Kunci: SD-WAN, Fortigate, Astinet, VPN, QOS.