ABSTRACT

The increasing need for fast and secure internet access has become crucial for every company, especially those related to financing and investment. Like FIF, branch offices and the head office communicate through an MPLS connection. Many applications and websites are disrupted, causing data traffic links to focus on a single connection. Therefore, this research aims to improve network service performance, data traffic management, and enhance network security in companies.

This research employs two methodologies: active/passive methodology and firewall filtering methodology. The active/passive methodology aims to test the Fortigate device with a failover configuration that ensures the availability and reliability of the Astinet network and IP VPN. The firewall filtering methodology is used to protect the security of the data network.

The implementation resulted in Auto Link Failover with an average packet loss percentage of 11% for VPN and 6% for Astinet. Then, a comparison of data transfer between the Astinet link and VPN under conditions with only one link was made. The data accessed by users was 36.41 bps, 24.79 bps, 7.95 bps, and 5.35 bps on the Astinet link, while the data accessed with the IPsec VPN link was 1860 bps, 9.28 bps, 31.63 bps, and 2.63 bps. Thus, the traffic steering obtained with an average bandwidth used by VPN is 1980 bps, while Astinet is 3180 bps, which is slightly larger and still able to perform load balancing. Then, the web filtering feature implemented on Fortigate can restrict access to certain sites or websites and block the download of protected files identified as data that is not allowed to be accessed on Fortigate SD WAN devices.

Keywords: *SD-WAN, Fortigate, Astinet, VPN, QOS.*