

ABSTRACT

Redundant System Firewall, a *firewall* system consisting of two or more *firewalls* that work simultaneously to form a *firewall* that is *redundant*. Replace each other if one system can not provide services that should be executed. The use of a single *firewall* is vulnerable to a network has many weaknesses, among them are prone to *hackers* who could take advantage of the weaknesses of the hardware and *firewall* configuration that can cause the *firewall* does not function properly. *Redundant* systems *firewall* configuration contains two or more *firewalls* that work simultaneously, forming a transparent system of *firewalls*, if there is a *firewall* that does not work, then the other *firewall* to replace its function.

Redundant Firewall Implementation System will help the performance of the network system, strengthen the protection of internal networks to the global Internet network that is vulnerable to intruders. This system uses *Virtual IP* technology where one or more hosts in the configured *firewall* will be a working IP address to *Virtual* address.

In the implementation of *Redundant Firewall* systems, have been tested on types of attacks, types of DDoS attacks (Distributed Denial of Service) is one type of attacks that exploit the system where the system will be sent in the request very large number, the system can not handle the request will not be up system resources so that the whole system performance will be disrupted.

Implementation results show that the type of DDoS attacks (ICMP Flood, UDP Flood dan TCP/SYN Flood) can cause system *Redundant Firewall* having failover, *Firewall Master* can not handle all requests from users, *Firewall Slave* which will replace the work function of the firewall Master.

Keyword : *Firewall, Redundant, Virtual IP*