ABSTRACT

Firewalls are no longer just perimeter devices for the data centers. Today, increasing attention is being paid to firewall performance, dynamic policy-based security, rapid scaling, high availability and application intelligence. Although the subject is highly discussed during recent times, not much practical research has been done on this topic. This research work attempts to focus on the same and try to evaluate performance of firewall technologies. Approach is suggested to improve performance of distributed firewall design. Initially, a structured method for testing firewall performance is proposed by evaluating and comparing performance of major firewalls in operation today. Detailed analysis and comparison is done in terms of cost, security, operational ease and implementation of Open source packet filter (PF) firewall, Checkpoint SPLAT and Cisco ASA in a testing environment with laboratory generated traffic in closed environment. Since, firewall needs to show robust performance along with application intelligence in order to withstand against Distributed Denial of Service (DDoS) attack, firewall performance during DDoS attack is studied and methods to improve performance is proposed.

With the growth of network complexity, it is very common to find firewall policies with thousands of rules. Modern firewall rulebase are growing in size and complexity at an exponential rate. As changes add up, the firewall rule base gets more complex. Firewall rulebase works on first-match principle. As a result, there exists scope of improvement in firewall performance, if highest utilized rule is brought ahead in rulebase. This will facilitate earlier matching and hence, less firewall resource utilization. This is carried out carefully without compromising overall firewall security or without loss of semantic integrity through a framework for rulebase reordering based on traffic conditions. To evaluate the performance of approach, performance testing on OpenBSD PF firewall is carried out by re-ordering rulebase under closed...
environment. After rulebase re-ordering, there is performance improvement in firewall throughput by 9.57% and improvement in concurrent sessions by 11.9%.

Further, system and method comprising standalone network design for interconnection of firewalls at multiple geographical locations connected through wide area Open Source network is proposed in order to improve scalability and security. This will overcome limitation and traditional bottleneck of static site to site Virtual Private Network (VPN). To evaluate the performance of the approach and proposed design, OpenBSD PF firewall performance testing is carried out under laboratory setup. OpenBSD PF firewalls are found running stable for a long time and capable of processing 360 kpps of traffic with 80% CPU load. Further, design for site requiring higher capacity is proposed by use of dedicated device for routing traffic inside a site. Under this high capacity site design, forwarding performance of firewalls is tested with different packet sizes under laboratory traffic by changing maximum transmission unit (MTU). It is also inferred that proposed setup under closed conditions is able to support up to 700 Mbps of traffic with standard size maximum transmission unit (MTU) of 256 bytes.