Abstract

As the communication via internet is growing very fast, network security becoming the essential need of an organization or user. It include protecting data from unauthorized access, protecting data from damage and implementing policies and procedures for network security breaches and data losses. Due to exhaustion problem of IPv4 addresses we will soon switch over IPv6. To solve this problem we are presenting a Framework of a firewall for IPv6 and IPv4 networks using a field-programmable gate array (FPGA). The FPGA implements, the accept or deny rules of the firewall in Hardware using Verilog Hardware Description Language. A hardware based firewall offers the advantages of speed over a software firewall, in addition to direct interfacing with network devices, such as an Ethernet. This firewall would have the ability to process the data packets based on source and destination TCP/UDP port number, source and destination IPv4 and IPv6 address, and combination of source IP address, and destination port number. Incoming and outgoing IPv6 packets addresses first converted into IPv4 addresses for filtering decisions.
A Framework of an Internet Firewall for IPv6 using FPGA

- Ayman Kayssi, Louis Harik, Rony Ferzli, Mohammad Fawaz, "FPGA-BASED INTERNET PROTOCOL FIREWALL CHIP"; 0-7803-6542-9/00 IEEE 2000
- Darrell Latunas, Ron Bolton, "Dynamic Silicon Firewall"; CCECE/CCGEI, IEEE 2005
- Arief Wicaksana, Arif Sasongko, "Fast and Reconfigurable Packet Classification Engine in FPGA-Based Firewall"; International Conference on Electrical Engineering and Informatics, 978-1-4577-0752-0/11 IEEE 2011

Index Terms

Computer Science  Network Security

Keywords

Firewall  IP  FPGA  Protocol  ROM  Packet