© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

A Review: Enhancing Security Of Network System Using Ip Filter And Cryptography

[1]Sheenu Sachdeva ,Research Scholar, Department of CSA, CDLU Sirsa, ssheenu75@gmail.com
[2]Er. Shilpa Jain, Asstt. Prof. Department of CSA, CDLU Sirsa, engishilpa19@gmail.com

Abstract- In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules [1]. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Routers that pass data between networks contain firewall components and can often perform basic routing functions as well. Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network [2]. In this research we have enhanced security of network at host-based firewall using One time password generation, We use the concept of socket programming (ip address+ port no.) with client server model. Also we enhance the cryptographic mechanism using the RSA algorithm. so here is three layer security we provide to our network during message transmission. This work done at host-based firewall.

Keyword: DHCP, VPN, RSA, OTP, IP, SOCKET PROGRAMMING.

1. Introduction

The term firewall originally referred to a wall intended to confine a fire or potential fire within a building. The predecessors to firewalls for Packet filters [5] act by inspecting the "packets" which are transferred between computers on the Internet. If a packet does not match the packet filter's set of filtering [11] rules, the packet filter will drop (silently discard) the packet or reject it (discard it, and send "error responses" to the source). Conversely, if the packet matches one or more of the programmed filters, the packet is allowed to pass. This type of packet filtering is done by socket programming (ip address+ port no.). The endpoint in an inter process communication is called a socket. Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. That is why when a socket is first created it is vital to match it with a valid IP address and a port number. The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers Packet filtering firewalls[7] work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly.