# Firewall Scenario and Issues

Gursimrat Singh[#1], Amitoj kaur[#2], Amardeep Singh[*3]

[#]*Student, M.Tech, CE, Punjabi University*
*Patiala, India*
[1]gursimratsinghvirk@gmail.com
[3]amitoj.kaur09@gmail.com
[*]*Professor, Punjabi University*
*Patiala, India*

***Abstract*— Firewall is a bridge between a computer and the network. It objective is to monitor the network traffic by viewing each incoming and outgoing packet. Firewall checks whether the packet should be allowed or not. It protects the PC from the Trojan horse attacks and other viruses. There are various research going on the implementation of the firewalls and the various security issues concerned with it. Next Generation Firewall Deep Inspection Policy by integrating Intrusion Prevention System. Also Purdue University is developing a prototype firewall to prevent hacking of the medical devices.**

***Keywords*— Firewall, Cisco ISO, Cisco PIX, NGFW**

## I. INTRODUCTION

### *A. What is a Firewall?*

A **firewall** either software-based or hardware-based is used to help to keep a network secure. Firewall controls the incoming and outgoing of network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A bridge is built between an internal network that is assumed to be secured and trusted, and another network which is usually an external network, such as an Internet which is not assumed to be secure and trusted, by the network's firewall. Software- based firewalls is included in many personal computer operating systems to protect against threats from the public Internet. . Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions [3]. The computer is absolutely isolated from the internet by the firewall using a "wall of code" that inspect each individual "packet" of data as it arrives at either side of the firewall — inbound to or outbound from your computer — to determine whether it should be allowed to pass or be blocked [2].

**When a Firewall is needed?**

- When computer's files need to be accessed remotely across the Internet.
- While operating any sort of Internet server such as Personal Web Server.
- While using any sort of Internet-based remote control or remote access program such as PC Anywhere, Laplink, or Wingate.
- When a person wants to properly and safely monitor his/her Internet connection for intrusion attempts.
- If a person wants to preemptively protect himself from compromise by "inside the wall" Trojan horse programs like NetBus and Back Orifice.

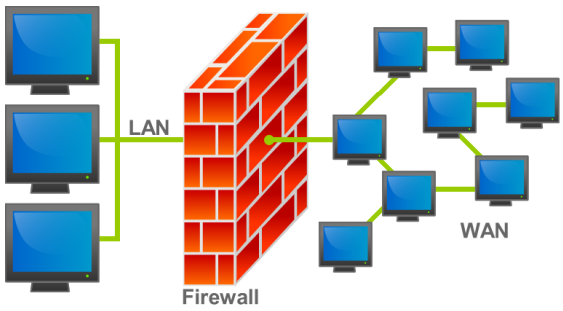


Fig. 1. Illustration of where a firewall could be located in the network

### *B. How a firewall works?*

All internet communication is accomplished by the exchange of individual "packets" of data. Each packet is transmitted by its source machine toward its destination machine. Packets are the fundamental unit of information flow across the Internet. Even though we refer to "connections" between computers, this "connection" is actually comprised of individual packets travelling between those two "connected" machines. Essentially, they "agree" that they're connected and each machine sends back "acknowledgement packets" to let the sending machine know that the data was received.
In order to reach its destination — whether it's another computer two feet away or two continents distant — every Internet packet must contain a destination address and port number. And, so that the receiving computer knows who sent the packet, every packet must also contain the IP address and a port number of the originating machine. In other words, any packet travelling the net contains — first and foremost — its complete source and destination addresses. As we've seen earlier on this site, an IP address always identifies a single

machine on the Internet and the port is associated with a particular service or conversation happening on the machine [2]

Since the firewall software inspects each and every packet of data as it arrives at your computer — **BEFORE it's seen by any other software running within your computer** — the firewall has total veto power over your computer's receipt of anything from the Internet.

A TCP/IP port is only "open" on your computer if the first arriving packet which requests the establishment of a connection is answered by your computer. If the arriving packet is simply ignored, that port of your computer will effectively disappear from the Internet. No one and nothing can connect to it. But the **real power** of a firewall is derived from its ability to be selective about what it lets through and what it blocks. Since every arriving packet must contain the correct IP address of the sender's machine, (in order for the receiver to send back a receipt acknowledgement) the firewall can be **selective** about which packets are admitted and which are dropped. It can "filter" the arriving packets based upon any combination of the originating machine's IP address and port and the destination machine's IP address and port.

So, for example, if you were running a web server and needed to allow remote machines to connect to your machine on port 80 (http), the firewall could inspect every arriving packet and **only** permit connection initiation on your port 80. New connections would be denied on **all** other ports. Even if your system were to inadvertently pick up a Trojan horse program which opened a Trojan listening port to the outside world, no passing Trojan scanner could detect or know of the Trojan's existence since all attempts to contact the Trojan inside your computer would be blocked by the firewall!But what about **you** originating your own connections to other machines on the Internet? For example, when you surf the web you need to connect to web servers that might have **any** IP address. You wouldn't want all those to be blocked just because you want to block everyone from getting into **your** machine. It turns out that this is easy for a firewall too. Since each end of an Internet connection is always acknowledging the other end's data, every packet that flows between the two machines has a bit set in it called the "ACK" bit. This bit says that the packet is **ack**nowledging the receipt of all previous data. But this means that only the very first packet which**initiates** a new connection would NOT be acknowledging any previous data from the other machine. In other words, a firewall can easily determine whether an arriving packet is **initiating** a new connection, or **continuing** an existing conversation. Packets arriving as part of an **established** connection would be allowed to pass through the firewall, but packets representing new connection attempts would be discarded. Thus, a firewall can permit the establishment of outbound connections while blocking any new connection attempts from the outside [2].

## II. Current Work going on Firewalls

### *A. New Firewall to Safeguard against Medical-Device Hacking*

Researchers at Purdue and Princeton universities have created a prototype firewall to block hackers from interfering with wireless medical devices such as pacemakers, insulin-delivery systems and brain implants. The team had previously demonstrated how medical devices could be hacked, potentially leading to catastrophic consequences [1].What motivated the professors to work on this problem was the ease with which the medical devices were hacked. the risk of devices being hacked is low but that security measures are merited before "attacks" in the lab are replicated on real systems. The team has created a prototype system called MedMon, for medical monitor, which acts as a firewall to prevent hackers from hijacking the devices. They demonstrated how MedMon could protect a diabetes system consisting of a glucose monitor and an insulin pump, which communicate with each other wirelessly[1]. It's an additional device that one could wear, so that one wouldn't need to change any of the existing implantable devices. This system could be worn as a necklace, or it could be integrated into one's cell phone, for example. Many implantable devices have wireless transmitters and receivers, which enable health-care providers to perform diagnostics and to download data. For example, a diagnostic test is performed periodically to make sure they are running properly. And during health emergencies, medical personnel must be able to access the systems. However, having wireless access also opens the door to potential hackers, who might alter the insulin dosage or direct pacemakers to malfunction, harming or killing a patient. There is very little work that exists on this important topic and the security vulnerabilities of such systems are not well understood. The MedMon prototype, which has been tested and shown to protect an insulin pump from hacking, monitors communications going into and coming out of any implantable or wearable medical device. It uses "multi-layered anomaly detection" to identify potentially malicious transactions. Upon detecting potentially malicious activity, the firewall can raise an alarm to the user or block "malicious packets" from reaching the medical device by using electronic jamming similar to technology used in military systems.The prototype is a proof of concept and would need to be miniaturized. A provisional patent application has been filed on the concept [1].

### *B. Cisco IOS Firewalls*

The Cisco IOS Firewall is a security-specific option for Cisco IOS Software. It integrates robust firewall functionality and intrusion detection for every network perimeter. It adds greater depth and flexibility to existing Cisco IOS security solutions (i.e., authentication, encryption, and failover), by delivering state-of-the-art security features: stateful, application-based filtering; dynamic per-user authentication

and authorization; URL Filtering and others. When combined with Cisco IOS IPSec and Cisco IOS Technologies such as L2TP tunnelling and Quality of Service (QoS), Cisco IOS Firewall provides a complete, integrated virtual private network (VPN) solution [4].

**Router-Based Firewall Functionality:**

Cisco IOS Firewall is available on a wide range of Cisco IOS Software releases. It offers sophisticated security and policy enforcement for connections within an organization (intranet) and between partner networks (extranets), as well as for securing Internet connectivity for remote and branch offices.

The Cisco IOS Firewall is the best choice for integrating multiprotocol routing with security policy enforcement and enabling managers to configure a Cisco router as a firewall. It scales to allow customers to choose a router platform based on bandwidth, LAN/WAN density, and multiservice requirements; simultaneously, it benefits from advanced security. These guidelines must be referred while choosing the right Cisco router for varied security environments:

• *Small/home offices:* Cisco 800, UBR900, and 1700 Series Routers

• *Branch and extranet environments:* Cisco 2600, 3600 and 3700 Series Routers

• *VPN and WAN aggregation points or other high-throughput environments:* Cisco 7100, 7200, 7400, 7500, RSM Series Routers; Cat 5k and Cat6k switches.

**Key Benifits:**

- Flexibility
- Investment protection
- VPN support
- Scalable deployment
- Easier Provising

*C. Cisco PIX Firewall*

The Cisco PIX Firewall is the world's leading dedicated firewall appliance. It has received the highest level of security certification granted to any firewall product. The Cisco PIX Firewall is a turnkey appliance with unmatched performance and unparalleled features. Integration of third-party content solutions, such as NetPartner's WebSENSE URL management software, further enhances the industry-leading capabilities of the Cisco PIX Firewall. For IP-based network security, the Cisco PIX Firewall is the clear choice for those requiring dedicated firewall appliances. When combined with IP Security (IPsec), Cisco PIX Firewall provides an integrated virtual private network (VPN) solution [4].Cisco Systems' PIX Firewall series addresses many of the security needs of companies—without the overhead and performance limitations of proxy servers. Its high performance and low cost of ownership make it a compelling solution for corporate network protection.

Cisco's PIX Firewall series ensures high security through its adaptive security algorithm (ASA) and the use of stateful information. Each time a TCP connection is established for inbound or outbound connections through the PIX Firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular connection. This information creates a connection object in the PIX Firewall series. Thereafter, inbound and outbound packets are compared against session flows in the connection table and are permitted through the Cisco PIX Firewall only if an appropriate connection exists to validate their passage. This connection object is temporarily set up until the connection is terminated.

*D. New Generation Firewalls(NGFW)*

IT managers in corporate and mid-size businesses have to balance both network performance and network security concerns. While security requirements are critical to the enterprise, organizations should not have to sacrifice throughput and productivity for security. Next-generation firewalls (NGFWs) have emerged as the solution to this thorny problem. Earlier-generation firewalls pose a serious security risk to organizations today. Their technology has effectively become obsolete as they fail to inspect the data payload of network packets circulated by today's Internet criminals. Many vendors tout Stateful Packet Inspection (SPI) speeds only, but the real measure of security and performance is deep packet inspection throughput and effectiveness. To address this deficiency, many firewall vendors adopted the malware inspection approach used by traditional desktop anti-virus solutions: buffer downloaded files, then inspect for malware. The downside to this method not only introduces significant latency, it also poses significant security risks, since temporary memory storage can limit the maximum file size [6].

A next-generation firewall applies deep packet inspection (DPI) firewall technology by integrating intrusion prevention systems (IPS), and application intelligence and control to visualize the content of the data being accessed and processed.

Gartner defines an NGFW as "a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks". At minimum, Gartner states an NGFW should provide:

- Non-disruptive in-line bump-in-the-wire configuration
- Standard first-generation firewall capabilities, e.g., network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc.
- Integrated signature based IPS engine
- Application awareness, full stack visibility and granular control

- Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc.
- Upgrade path to include future information feeds and security threats
- SSL decryption to enable identifying undesirable encrypted applications[6]

As NGFW products become more widely used, focus will shift toward manageability and scalability— until the next threat wave. 2012 will be the year most mainstream firewall vendors catch up to the smaller innovative vendors in feature count. The innovative vendors must show that they have the same management tools, as well as third-party ecosystem support and scale, as the larger vendors. Enterprises should continue to focus on threat-facing capabilities, throughput and manageability as key evaluation criteria for firewalls, with technical criteria typically weighted two times to three times cost criteria. Firewall policy management (FPM) products (see Note 1) are a distinct, adjacent market. Gartner recommends FPM tools be considered where the complexity of the environment exceeds the firewall console capability, where the firewall rule base is exceptionally large or dynamic, where there is more than one brand of firewall in use, if a complex transition to another brand of firewall is planned, or if workflow tools are required as part of firewall rule management [7].

The Strategic Planning Assumptions for the enterprise firewall market are:

- Virtualized versions of enterprise network safeguards will not exceed 2% of the market through 2012, or 20% through 2016.
- Through 2015, more than 75% of enterprises will continue to seek security from a vendor different from their infrastructure vendor.
- Less than 5% of Internet connections today are secured using NGFWs. By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs [7].

**The evolution of Next-Generation Firewalls**

The SPI generation of firewalls addressed security in a world where malware was not a major issue and web pages were just documents to be read. Ports, IP addresses, and protocols were the key factors to be managed. But as the Internet evolved, the ability to deliver dynamic content from the server and client browsers introduced a wealth of applications we now call Web 2.0.

Today, applications from Salesforce.com to SharePoint to Farmville all run over TCP port 80 as well as encrypted SSL (TCP port 443). A next-generation firewall inspects the payload of packets and matches signatures for nefarious activities such as known vulnerabilities, exploit attacks, viruses and malware all on the fly. DPI also means that administrators can create very granular permit and deny rules for controlling specific applications and web sites. Since the contents of packets are inspected, exporting all sorts of statistical information is also possible, meaning administrators can now easily mine the traffic analytics to perform capacity planning, troubleshoot problems or monitor what individual employees are doing throughout the day. Today's firewalls operate at layers, 2, 3, 4, 5, 6 and 7 of the OSI model.

**Vendors**

a) Barracuda Networks
b) Check Point Software Technologies
c) Cisco
d) Fortinet
e) HP
f) Juniper Networks
g) McAfee
h) (NETASQ
i) SonicWALL
j) Stonesoft
k) WatchGuard

## III. Issues in Firewalls

### *A. Issues caused by application having difficulties to be aware of network needs*

This is an issue were applications try to adapt towards the needs of the network.

- **Software and port numbers**

Port numbers and number of ports are unknown until the application starts. The consequence is that firewall administrators need to create big holes (up to 10.000 ports) if the application is not capable of determining the amount of ports to be used and/or the port numbers are unknown. Trying to push all traffic though a single hole (e.g. HTTP port 80) causes referral problems. In general, only specific, predetermined applications that use a low number of very well-defined ports (or "well-known ports") can be supported adequately.

- **Hardware**

Applications that want to be aware of the underlying network have difficulties with:

a) Understanding the number and kind of firewalls located within the routing path.
b) Pushing high performance data streams across long connections that need enough buffer space and switching capacity. If applications were aware of buffer sizes and delays, they could adjust their transmission rates more effectively to avoid packet drops in any kind of forwarding device, including firewalls.
c) Opening multiple high performance channels (wavelengths) over a single fiber. There are no firewalls that are able to deal with multiple wavelengths on a single fiber. If these wavelengths have been divided into individual fibers by DWDM equipment, firewalls are not able to deal with 16, 32 or 64 links of 10 Gb/s each currently. Current

firewalls can deal with up to 5 Gb/s links, and, if they act as packet filters only, may handle multiple 10 Gb/s links, but they are not able to deal with several hundred Gb/s coming in through multiple 10 Gb/s interfaces. Though load balancing firewalls are available since some time, these cannot handle such high communication streams [9].

*B. Some other Issues include:*

- **Speed Issues**

Firewalls are set to operate at a certain speed, appropriate to the network connection. Firewalls that operate at a faster speed than the network connection will not function. Therefore, the firewall always has to match the speed of the network. If the firewall does not match the speed of the connection, it will let data pass through unmonitored; a great security risk. To avoid experiencing a problem like this, it is essential to update the firewall regularly.

- **Conflicts with FTP Programs**

Firewalls can't keep up with all the data being transmitted by FTP programs when there is a large influx of data. Also, due to the dual-socket data transfer in FTP programs, a firewall may not recognize some of the data properly, meaning it might recognize data that is coming in as going out. Due to the inability of some firewall programs to accurately recognize data in FTP programs, they pose a security risk to the server that uploads data with the FTP program. However, these problems are uncommon when using a trusted, stable firewall.

- **Disabling Security Policies**

There are fake (malware) firewalls that disable or modify the security policies of your computer's network connection, which then opens the network ports, allowing any kind of data to pass through. Always be sure that the firewall you are using is from a brand-name company with a reputable track record, and a reputation for producing quality firewalls.

- **Blue Screen of Death**

The BSOD, which is a message to the user that his computer has malfunctioned, unnecessarily appears due to problems with firewalls in Windows computers. This issue can be fixed by updating your firewall to the latest version [8].

## IV. CONCLUSIONS

Firewall can be hardware based or software based. It keeps control over the incoming and the outgoing traffic. Now a day's New Generation Firewall is in the market. There are various vendors like McAfee, Cisco etc that are having these firewalls and provide the enterprises with the firewalls. Each vendor has its own strengths and weakness. There are many issues to be resolved. Firewalls are not much in trend now a days but it is assumed that by next 2 or 3 years many of the people and enterprises will be using firewalls due to increase in the use of network and social sites. The problem of speed and BSOD must be resolved and work must be done on it in order to make firewalls better for future use.

## ACKNOWLEDGMENT

I would like to thanks my GUIDE Dr. Amardeep Singh for his thorough guidance in my work. I would also like to thanks my parents, friends to help me to get through the work.

## REFERENCES

[1]http://www.purdue.edu/newsroom/research/2012/story-print-deploy-layout_1_19214_19214.html

[2] http://www.grc.com/su-firewalls.htm

[3] http://en.wikipedia.org/wiki/Firewall_(computing)

[4] Cisco IOS firewall, Cisco Systems, Inc

[5] Cisco's PIX Firewall Series and Stateful Firewall Security, Cisco Systems, Inc

[6]http://www.techrepublic.com/blog/security/next-generation-firewalls-security-without-compromising-performance/8545

[7]Greg Young, John Pescatore, "Magic Quadrant for Enterprise Network Firewalls", Gartner, December-2011

[8]http://www.ehow.com/list_7164443_firewall-security-issues.html

[9] Ralph Niederberger**,** William Allcock**,** Leon Gommans, Egon Grünter, Thijs Metsch, Inder Monga, Gian Luca Volpato, Christian Grimm, "Firewall Issues FI – RG", August 16, 2006