ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

A Pragmatic Analysis on Software Firewalls

Kirti Walia
Research Scholar
Punjab Technical University
Jalandhar Kapurthala Road
Punjab

Dr. S.N.Panda
Professor and Principal
Regional Institute of Management & Technology
Mandi Gobindgarh
Punjab

Dr. H.C. Agrawal
Professor
Regional Institute of Management & Technology
Mandi Gobindgarh
Punjab

Abstract: ***Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but it could not recognize all instances and forms of attack, and attacks sent from one internal host to another often do not pass through network firewalls. Because of these and other factors, network designers now often include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect mobile devices that are placed directly onto external networks. Threats have gradually moved from being most prevalent in lower layers of network traffic to the application layer, which has reduced the general effectiveness of firewalls in stopping threats carried through network communications. However, firewalls are still needed to stop the significant threats that continue to work at lower layers of network traffic. Firewalls can also provide some protection at the application layer, supplementing the capabilities of other network security technologies. There are several types of firewalls, each with varying capabilities to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies. Understanding the capabilities of each type of firewall, and designing firewall policies and acquiring firewall technologies that effectively address an organization's needs, are critical to achieving protection for network traffic flows. This research paper provides an overview of firewall technologies, types and discusses their security capabilities and relative advantages and disadvantages. It also provides examples of where firewalls can be placed within networks and the implications of deploying firewalls in particular locations. The paper also provides comparison between different software firewall types.***

I. INTRODUCTION

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential. Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems [1]. Firewalls can protect both individual computers and corporate networks from hostile intrusion from the Internet, but must be understood to be used correctly. Software firewalls are program based applications that run on a computer.

They work by monitoring all open ports on a computer and checking all the information that is received on them. Each monitored port is specifically dedication to each program that has access to the internet, so the software firewall, is configured to contain a list of applications available to access the internet on certain ports. Therefore, if the allowed application is using a specified port, the software firewall will check the contents coming in on that port and pass it though to the computer if acceptable [2]. If an application attempting to access information that is not allowed/configured to from the internet, the firewall will block all incoming/outgoing information and notify the user that that program is trying to access the internet, thus allowing the user to determine if the application is safe to have access to the internet.

A software firewall can protect a computer and notify the user of any activities trying to access the personal computer from anywhere outside the computer. The software firewall gives a lot of control over the information passing through the computer and can be a very effective way for an advanced user to protect its computer from the outside. If the software firewall is configured properly it can be very effective, but it can also be difficult to configure. For local area networks, software firewalls must be installed on each machine on the network and configured separately. Depending on the size of the network and the amount of configuration needed, it can be very cumbersome and difficult to maintain a software firewall on a network.

II. SPECIFICS OF APPLICATION SOFTWARE FIREWALLS

Application firewalls (AFs) operate at the application layer of the network stack. They are proxy-based (forward and/or reverse proxy) firewalls that "run interference" between a "trusted" (internal) application and an "untrusted" (external) application. AFs operate by presenting each application with a set of proxies for all

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

available application-level services [3]. Like lower-layer proxy servers, application-level proxy servers give the connected applications the impression that they are communicating directly with one another when, in fact, all traffic from each application is intercepted and inspected by the AF, which either rejects that traffic (if it violates a filtering rule) or passes it to the counterpart proxy facing the other application, which then routes it to that application.

An AF's filtering and policy rule set can be quite sophisticated. It can implement fine-grained blacklisting and white listing of application-level objects (e.g., URLs/URIs [Uniform Resource Identifiers], email [electronic mail] addresses) and/or content conveyed via various application layer protocols (Hyper Text Transfer Protocol [HTTP], File Transfer Protocol [FTP], Post Office Protocol 3 [POP3], Simple Mail Transfer Protocol [SMTP], etc.), and can block packets received from any Web site, sender, database, etc. that are either on a blacklist or not on a white list. They can also implement more granular policies to block only certain types of content from a specific source, or from a specific type of source. For example, they may block Internet Messaging (IM) traffic but not HTTP traffic originating from any Web site, but may block all FTP traffic originating from only certain Web sites. Some AFs can also detect anomalous content—e.g., content that is incorrectly formatted, or contains patterns that are indicative of malware/viruses, or URLs or content containing patterns indicative of known exploits of server or client software vulnerabilities.

AFs are either network- or host-based. A network-based AF is interposed not just between two applications, but between two networks, enabling it to filter application layer traffic originating from either network, and preventing undesirable application traffic from an application on the external network from reaching clients or servers on the internal protected network [4]. Host-based AFs is co-located on the same host as the application it protects, where it monitors all application layer input data, output data, and/or system service calls made from, to, or by the protected application. Modern personal firewalls are virtually always hybrids of host-based network and application firewalls. AFs tend to be dedicated to certain types of applications.

Currently, the most prevalent AFs are Web AFs (WAFs), [2] but there are also numerous email firewalls, as well as a growing number of XML (Web service) and database firewalls. The last of these is typically deployed to protect databases from Web-originated application attacks such as SQL injections, database root kits, and data loss. Some database firewalls include automated Standard Query Language (SQL) learning capabilities to assist in policy configuration based on their analysis of trends found through the aggregated queries directed to a specific database. A newer trend in stateful inspection is the addition of a stateful protocol analysis capability, referred to by some vendors as deep packet inspection [5]. Stateful protocol analysis improves upon standard stateful inspection by adding basic intrusion detection technology—an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations.

This allows a firewall to allow or deny access based on how an application is running over the network. For instance, an application firewall can determine if an email message contains a type of attachment that the organization does not permit (such as an executable file), or if instant messaging (IM) is being used over port 80 (typically used for HTTP). Another feature is that it can block connections over which specific actions are being performed (e.g., users could be prevented from using the FTP "put" command, which allows users to write files to the FTP server). This feature can also be used to allow or deny web pages that contain particular types of active content, such as Java or ActiveX, or that have SSL certificates signed by a particular certificate authority (CA), such as a compromised or revoked CA [6]. Application firewalls can enable the identification of unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent.

These suspicious commands often originate from buffer overflow attacks, DoS attacks, malware, and other forms of attack carried out within application protocols such as HTTP. Another common feature is input validation for individual commands, such as minimum and maximum lengths for arguments. For example, a username argument with a length of 1000 characters is suspicious—even more so if it contains binary data. Application firewalls are available for many common protocols including HTTP, database (such as SQL), email (SMTP, Post Office Protocol [POP], and Internet Message Access Protocol [IMAP]), voice over IP (VoIP), and Extensible Markup Language (XML) [7]. Another feature found in some application firewalls involves enforcing application state machines, which are essentially checks on the traffic's compliance to the standard for

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

the protocol in question.

This compliance checking, sometimes call "RFC compliance" because most protocols are defined in RFCs issued by the Internet Engineering Task Force (IETF), can be a mixed blessing. Many products implement protocols in ways that almost, but not completely, match the specification, so it is usually necessary to let such implementations communicate across the firewall. Compliance checking is only useful when it detects and blocks communication that can be harmful to protected systems. Firewalls with both stateful inspection and stateful protocol analysis capabilities are not full-fledged intrusion detection and prevention systems (IDPS), which usually offer much more extensive attack detection and prevention capabilities [8]. For example, IDPSs also use signature-based and/or anomaly-based analysis to detect additional problems within network traffic.

III. COMPARISON OF APPLICATION SOFTWARE FIREWALLS

Name	Type of Firewall	OS	Format	License	Developer
Art of defence hyperguard	WAF	Runson Solaris, Linux, BSD Unix, and Windows	Software	Commercial	art of defence (United Kingdom [UK])
BalaBit IT Security Zorp	WAF	Included (ZorpOS—customized version of Ubuntu Linux 6.06)	Software	Commercial	BalaBit IT Security (Hungary)
Barracuda Web Application Firewalls	WAF	Included	Appliance	Commercial	Barracuda Networks AG (Sweden)
BugSec WebSniper	WAF	Included	Appliance	Commercial	BugSec (Israel)
CloudShield DNS Defender	WAF (with SIF)	Runs on CloudShield Packet Operating System (CPOS™)	Software	Commercial	CloudShield/SAIC
Deny All rFTP	AF (File Transfer)	Included (hardened HP-UX Server)	Appliance or Software	Commercial	Deny All Security Solutions (FR)
DigiPortal ChoiceMail Enterprise and ChoiceMail Small Business	AF (Email)	Runs on Windows NT, 2000, XP, Vista, SBS, Server 2000/2003/2008	Software	Commercial	DigiPortal Software
Excelerate SpamGate	AF (Email)	Included; Virtual Server: requires VMware	Appliance or Software	Commercial	Excelerate Software, Inc.
Forum Sentry XML Gateway	AF (XML)	Appliance: Included; Software version runs on Windows, Linux, Solaris, in a VM (VMware), or in an Amazon Elastic	Appliance or Software	Commercial	Forum Systems

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

		Compute Cloud (EC2) Amazon Machine Image (AMI)			
Horizon Network Security SPAM Cracker	AF (Email)	Runs on Linux (Included when firewall is purchased with hardware platform)	Software	Commercial	Horizon Network Security
IMGate Mail Firewall	AF (Email)	Runs on FreeBSD 7	Software	Open source	IMGate Project
Imperva SecureSphere File Firewall	AF (FTP)	Included (virtual appliances also require VMware ESX/ESXi 3.5/4.0)	Appliance or Software	Commercial	Imperva

IV. ISSUES WITH SOFTWARE FIREWALLS

Software based solutions are usually less expensive to acquire, and there are actually a number of free firewall applications available to download. However, the principle of you get what you pay for certainly applies here. Free solutions do not offer the comprehensive features of more expensive applications [9]. Additionally, technical support is not readily available, and the overall effectiveness of free firewalls is suspect enough to where they should not even be considered except for personal use or protecting marginally important resources.

One major problem with software based firewalls is that, since they are installed on an existing operating system, they are susceptible to the same viruses and malicious attacks as their host machine, thereby increasing the likelihood that the firewall can be disabled or otherwise rendered useless in the event of an attack. Also, one must ensure that the host system has enough hardware resources (CPU and memory) available for the firewall to operate effectively. If those resources are insufficient, the firewall will perform poorly, and network throughput will suffer. Another disadvantage of software firewalls is that not only do the network administrators have to worry about keeping the firewall software updated and properly patched, but the operating system the solution is installed on must be diligently 'hardened' and patched as well. To improve the effectiveness and security of their firewalls, organizations should implement the following recommendations:

Firewall policy that specifies how firewalls should handle inbound and outbound network traffic. A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. Organizations should conduct risk analysis to develop a list of the types of traffic needed by the organization and how they must be secured—including which types of traffic can traverse a firewall under what circumstances. Examples of policy requirements include permitting only necessary Internet Protocol (IP) protocols to pass, appropriate source and destination IP addresses to be used, particular Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to be accessed, and certain Internet Control Message Protocol (ICMP) types and codes to be used [10]. Generally, all inbound and outbound traffic not expressly permitted by the firewall policy should be blocked because such traffic is not needed by the organization. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the organization's networks.

***Identify all requirements that should be considered when determining which firewall to imple*ment.** There are many considerations that organizations should include in their firewall selection and planning processes. Organizations need to determine which network areas need to be protected, and which types of firewall technologies will be most effective for the types of traffic that require protection [11]. Several important

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

performance considerations also exist, as well as concerns regarding the integration of the firewall into existing network and security infrastructures. Additionally, firewall solution design involves requirements relating to physical environment and personnel as well as consideration of possible future needs, such as plans to adopt new IPv6 technologies or virtual private networks (VPN).

V. CONCLUSION

The choice between choosing the firewall is purely preference, but there should be some thought when choosing. The best and most minimum that one should do to protect a computer is to have a hardware firewall in place. The ease of setting up and the range of protection for various numbers of computers is an obvious choice. To improve the protection, adding a software firewall can pretty much eliminate most if not all incoming or outgoing harmful materials from the internet. Although more configurations are required with a software firewall, there is more flexibility and control for the user. In the ideal situation the best would be to have both hardware and software firewalls they both will give the good protection from the internet.

REFERENCES

[1] Blekinge Institute of Technology, Sweden, Firewalls http://www.its.bth.se/staff/hjo/.

[2] Ronald Pacchiano, Firewall Debate: Hardware vs. Software, http://www.smallbusinesscomputing.com/webmaster/article.php/3103431.

[3] Design the Firewall System, http://www.cert.org/security-improvement/practices/p053.html.

[4] D.E. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architectures, 4th edition, Prentice Hall, NJ, 2000.

[5] Tomas Olovsson, A Secure Network Architecture, http://www.appgate.com/knowledge_center/tomas.pdf

[6] E.D. Zwicky, S. Cooper, and D.B. Chapman, Building Internet Firewalls.

[7] Amon, Cherie and Thomas W. Shinder, and Anne Carasik-Henmi. The Best Damn Firewall Book Period, Second Edition (2007, Syngress Publishing).

[8] Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition (2003, Addison Wesley Professional).

[9] Komar, Brian, Ronald Beekelaar, and Joern Wettern. Firewalls for Dummies, Second Edition (2003, For Dummies).

[10] Liu, Alex X. Firewall Design and Analysis, First Edition (2010, World Scientific Publishing Company).

[11] Noonan, Wes and Ido Dubrawsky. Firewall Fundamentals, First Edition (2006, Cisco Press).

[12] Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41 Revision 1, Sept 2009