Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Simple Taxonomy Survey of Firewall Policies

C.Poovinayaga Sastha, Dr.V.Palanisamy
[1,2] *Department of Computer Science and Engineering*
Alagappa University,
Karaikudi, India

Abstract—Any data passes through a internal network to an external network there are lot of vulnerable attacks are possible to hack or damage the data. One type of network attack is unauthorised penetration in to network due to openness of networks. It is possible to hack the data and resources of networks. Firewall is the suitable mechanism to protecting the website from attackers. It acts as a security guard between a private network and the outside Internet such that all incoming and outgoing packets have pass through it. Working of a firewall is to examine every incoming or outgoing packet and to decide whether to accept or discard it. This function is conventionally specified by a sequence of rules. Most of the threat attacks are attained only by a misconfiguration of firewall rules. A misconfigured firewall will, almost certainly only provide the illusion of network security and it will give adverse effect of legitimate traffic. So we can focus the firewall policy it is a basement for firewall rule generation. The firewall policy orders how the firewall should handle network traffic for specific IP addresses and address ranges, protocols, applications and content types based on the organisation's information security policies.

Keywords— Internet Security; Software Firewall; Computer Network Security; Hardware and Software Security.

I. INTRODUCTION

With the global Internet connection, network security has gained significant attention in research and industrial communities. Due to the increasing threat of network attacks. Firewalls have become important elements not only in enterprise networks but also in small size and home networks. Basically a firewall is a device or software that can inspect traffic at a deeper level than most network elements. It can be software that resides on a host and inspects traffic before it is allowed to interact with any other applications on that host. This type of firewall is known as a host-based firewall or personal firewall. A second type of firewall is a network firewall that does not reside on the computer system that it's protecting. It is a standalone device that must be inserted into the network so that it can inspect traffic that flows through it and make decisions on whether it will allow or deny a particular packet or flow of packets. Firewall consists of sequentially ordered set of rules. The basic requirement for rule generation in firewall is source address, destination address, source port, destination port, and protocol. Without these fields we can not generate even a single firewall rule. The rules can be developed either by manually and automatically. An error may be occurred in case of manually configured firewall it will give adverse effect of rules.

Based on the rules we can filter unwanted packets. The action field of firewall can be either ACCEPT or DENY. If a packet can match at least any one of the rule, it can compare the firewall's state table and it will be allowed to pass without further processing. If doesn't match any one of the rule it can be evaluated according to the rule set for new connections.

Simply we could describe the firewall policy design that helps to protect the computers in particular organization from unwanted network traffic that gets through the perimeter defences, or that originates from inside your network.

II. POLICY TYPES

Generally, firewalls should block all inbound and outbound traffic by the firewall policy that is not handled by the organisation. These practices, known as deny by default, decrease the risk of attack and can also reduce the volume of traffic carried on the organization's networks. Because of the dynamic nature of hosts, networks, protocols, and applications, deny by default is a more secure approach than permitting all traffic that is not explicitly forbidden. The firewall policies can be majorly divided into following four ways:

- ❖IP Address Protocols Based Traffic
- ❖Application Specific based Traffic
- ❖Based on the Network Activity
- ❖Based on the User's Identity.

A firewall policy shows how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed and categorize how they must be secured; including which types of traffic can traverse a firewall under what circumstances. This risk analysis should be based on an evaluation of threats; vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if systems or data are compromised.

A. Firewall policy based on the IP Address and its Characteristics

Firewalls allow only specified protocols to pass through. These protocols are such as the Internet Protocol, Transmission control Protocol, User Datagram Protocol, ICMP etc., some of the message Authentication codes, Authentication Header and their IP Security components such as the Encapsulating Security Payload can also be used. Sometimes they also can be blocked on both the sides of the firewalls also.

Address and their Characteristics: Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include the following necessities:

- ❖ Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location.
- ❖ Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment.
- ❖ The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, Address Allocation for Private Internets, which are reserved for private networks.
- ❖ Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter.
- ❖ Outbound traffic with invalid source addresses should be blocked (this is often called egress filtering). Systems that have been compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes these kinds of attacks more difficult to stop. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks.
- ❖ Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

IPV6 Protocol Characteristics: IPv6 is a new version of IP that is increasingly being deployed. For the features that are the same between IPv4 and IPv6, firewalls should work the same as that for the IPV4 Protocol. For example, blocking all inbound and outbound traffic that has not been expressly permitted by the firewall policy should be done regardless of whether or not the traffic has an IPv4 or IPv6 address.

In order to allow IPV6 to deploy, it's also posses the characteristics of IPV4. It should capable of using the protocols on both the Inbound and the outbound traffic. It also allows all the filtering rules that are capable of the IPv4 also. It should be capable of blocking the tunnelling, flooding when more number of packets being transmitted.

Many sites tunnel IPv6 packets in IPv4 packets. This is particularly common for sites experimenting with IPv6, because it is currently easier to obtain IPv6 transit from a tunnel broker through a v6-to-v4 tunnel than to get native IPv6 transit from an Internet service provider (ISP). A number of ways exist to do this, and standards for tunnelling are still evolving. If the firewall is able to inspect the contents of IPv4 packets, it needs to know how to inspect traffic for any tunnelling method.

TCP and UDP: Application protocols can use TCP, UDP, or both, depending on the design of the protocol. An application server typically listens on one or more fixed TCP or UDP ports. Some applications use a single port, but many applications use multiple ports. FTP uses at least two ports, one of which can be unpredictable, and while most web servers use only TCP port. Some applications use both TCP and UDP. Application clients typically use any of a wide range of ports.

As with other aspects of firewall rule sets, deny by default policies should be used for incoming TCP and UDP traffic. In addition to allowing and blocking UDP and TCP traffic, many firewalls are also able to report or block malformed UDP and TCP traffic directed towards the firewall or to hosts protected by the firewall. This traffic is frequently used to scan for hosts, and may also be used in certain types of attacks.

IPSec Protocols: An organization needs to have a policy whether or not to allow IPSec, Virtual Private Networks that start or end inside its network perimeter. The Encapsulating Security Protocols and Authentication Header protocols are used for IPSec VPNs, and a firewall that blocks these protocols will not allow IPSec VPNs to pass. Enforcing this policy will require people inside the organization to obtain the appropriate policy approval to open ESP and/or AH access to their IPSec routers. This will also reduce the amount of encrypted traffic coming from inside the network that cannot be examined by network security controls.

b. Firewall Policy based on the Applications

Most early firewall work involved simply blocking unwanted or suspicious traffic at the network boundary. Inbound application firewalls or application proxies take a different approach—they let traffic destined for a particular server into the network, but capture that traffic in a server that processes it like a port-based firewall. The application-based approach provides an additional layer of security for incoming
traffic by validating some of the traffic before it reaches the desired server.

An application firewall or proxy also prevents the server from having direct access to the outside network. If possible, inbound application firewalls and proxies should be used in front of any server that does not have sufficient security features to protect it from application-specific attacks. The main considerations when deciding whether or not to use an inbound application firewall or proxy are:

- ❖ Is a suitable application firewall available? Or, if appropriate, is a suitable application proxy available?
- ❖ Is the server already sufficiently protected by existing firewalls?
- ❖ Can the main server remove malicious content as effectively as the application firewall or proxy?

- Is the latency caused by an application proxy acceptable for the application?
- How easy it is to update the filtering rules on the main server and the application firewall or proxy to handle newly developed threats.

c. Firewall Policies Based on User Identity

Traditional packet filtering does not see the identities of the users who are communicating in the traffic traversing the firewall, so firewall technologies without more advanced capabilities cannot have policies that allow or deny access based on those identities. One of the most common ways to enforce user identity policy at a firewall is by using a VPN. Both IPSec VPNs and SSL VPNs have many ways to authenticate users, such as with secrets that are provisioned on a user-by-user basis, with multi-factor authentication.

NAC has also become a popular method for firewalls to allow or deny users access to particular network resources. In addition, application firewalls and proxies can allow or deny access to users based on the user authentication within the applications themselves. Firewalls that enforce policies based on user identity should be able to reflect these policies in their logs. That is, it is probably not useful to only log the IP address from which a particular user connected if the user was allowed in by a user-specific policy; it is also important to log the user's identity as well.

d. Firewall Policies Based on Network activity

Firewalls allow the networks to work on the time basis through which all the systems on the networks can gain the benefit. Time-based policies are useful in thwarting attacks caused by a logged-in user walking away from a computer and someone else sitting down and using the established connections. However, these policies can also be bothersome for users who make connections but do not use them frequently. If the user does not save the file back to the file server before the firewall-mandated timeout, the timeout could cause the changes to the file to be lost.

A different type of firewall policy based on network activity is one that throttles or redirects traffic if the rate of traffic matching the policy rule is too high. Another policy might be to drop incoming ICMP packets if the rate is too high. Crafting such policies is quite difficult because throttling and redirecting can cause desired traffic to be lost or have difficult-to diagnose transient failures.

III. CONCLUSION

A firewall is a combination of hardware and software or application software designed to control the flow of Internet Protocol traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset. Hence, in this survey paper employs a few different firewall policies and its characteristics.

REFERENCES

[1] Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. RFC 2401, November 1998.(Status: PROPOSED STANDARD)

[2] http://www.icsalabs.com/html/communities/firewalls/buyers_guide/index.shtml

[3] http://www.isc.org/services/public/lists/firewalls.html

[4] Building Internet Firewalls, 2nd Edition, Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, O'Reilly & Associates, Inc.June 2000

[5] Internet Firewalls: Frequently Asked Questions, Matt Curtin and Marcus J. Ranum, December 2000.

[6] E. Al-Shaer and H. Hamed. "*Firewall Policy Advisor for Anomaly Detection and Rule Editing."* IEEE/IFIP Integrated Management

[7] E. Al-Shaer and H. Hamed. *"Design and Implementation of Firewall Policy Advisor Tools."* Technical Report CTI- techrep0801, School of Computer Science Telecommunications and Information Systems, DePaul University, August 2002.

[8] NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800- 18-Rev1-final.pdf

[9] http://www.ranum.com/pubs/fwfaq

