Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.359 – 367

RESEARCH ARTICLE

Firewall and Its Policies Management

Er. Smriti Salaria[1], Er. Nishi Madaan[2]

[1]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
[2]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
[1] Smritisalaria@yahoo.in; [2] nishi.02.bti@gmail.com

Abstract: Firewalls are core elements in network security. A firewall element determines whether to accept or discard a packet that passes through it based on its policy. Firewall allows separation between frontend and backend entity so as to ensure security. In this paper we have critically analyzed various firewall management policies and techniques and also have covered our views such that its major types, classification and applications.

Keywords: Firewall; Firewall types; proxy server; Firewall policies; Firewall Policies types

I. INTRODUCTION

A firewall is software or hardware based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Due to the increasing threat of network attacks, firewall has become more important elements to secure our data from the unauthorized attacks on the network. Its task is ideally to filter out unwanted network traffic coming from or going to the secured network. The filtering decision is based on the firewall policy which is set of ordered filtering rules defined according to predefined security policy requirements. The effectiveness of firewall security is dependent on providing policy management techniques/tools that enables network administrators to analyze, purifying and verify the correctness of written firewall legacy rules.

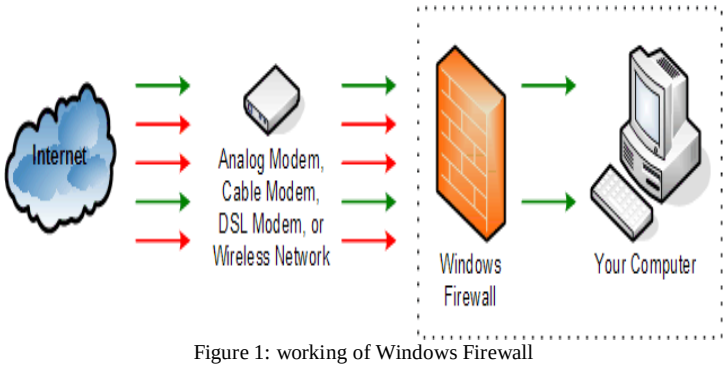

Figure 1: working of Windows Firewall

A. Need of firewall:

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals

- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization

B Types of firewall

Basically there are three types of firewall.
a). Network layer firewall.
b). Application layer firewall.
c).proxy firewall.

a). Network layer firewall:-

Network layer firewalls also called packet filters; operate relatively low level of TCP/IP protocol stack not allowing packets to pass through the firewall unless they match the established rule set. Network layer generally fall into two subcategories stateful and stateless. In stateful , firewall maintain context about active sessions and use that state information to speed packet processing and on the other hand stateless firewall require less memory and can be faster for simple filters that require less time to filter than to look up a session.

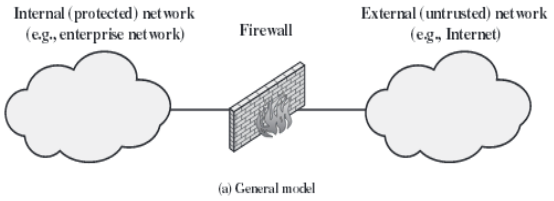

Figure 2: Network Layer Firewall.

b). Application layer firewall:-

Application layer firewall work on the application level of the TCP/IP stack (i.e. all browser traffic, all telnet or all FTP traffic) and may intercept all packets travelling to or from an application. It is used to block the other packets. Application layer filtering goes beyond packet filtering and allows you to be much more granular in your control of what enters or exits the network. While packet filtering can be used to completely disallow a particular type of traffic (for example, FTP), it cannot "pick and choose" between different FTP messages and determine the legitimacy of a particular FTP message.

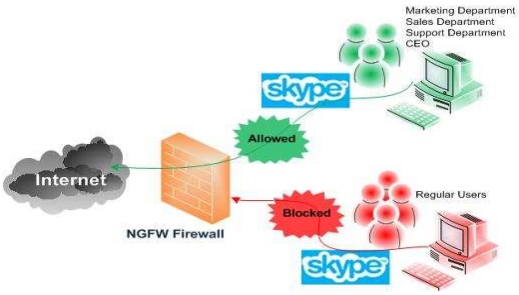

Figure 3: Application Layer Firewall.

c). Proxy firewall filters:-

Proxy firewalls are the most secure types of firewalls, but this comes at the expense of speed and functionality, as they can limit which applications your network can support. The enhanced security of a proxy firewall is because, unlike with other types of firewall, information packets don't pass through a proxy. Instead the proxy acts as an intermediary - computers make a connection to the proxy which then initiates a new network connection based on the request; effectively a mirror of the information transfer. This prevents direct connections and packet transfer between either sides of the firewall, which makes it harder for intruders to discover where the location of the network is from packet information. A firewall proxy provides internet access to computers on a network but is mostly deployed to provide safety or security by controlling the information going in and out of the network. Firewall proxy servers filter, cache, log, and control requests coming from a client to keep the network secure and free of intruders and viruses.

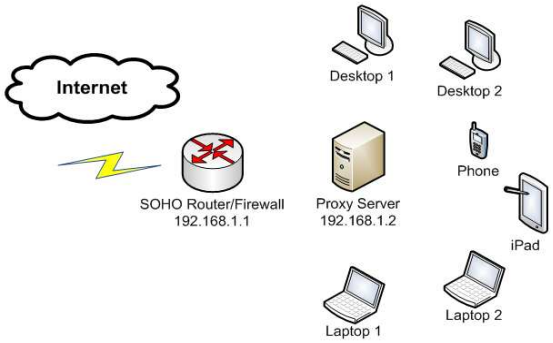

Figure 4: Proxy Server.

II. POLICIES OF FIREWALL MANAGEMENT

A. Firewall policy Modeling

As a basic requirement of any firewall policy management, we first modeled the relations of firewall rules in the policy. We describe formally our model of firewall rules relations and policies.

Formalization of Firewall Rule Relations

To be able to build a useful model for filtering rules, we need to determine all the relations that may relate two or more packet filters. In which we match two values, two values are equals if they matched, inclusive if one values is subset of another, distinct otherwise. Example

Definition 1: Rules Rx and Ry are exactly matched if every field in Rx is equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are exactly matched since all corresponding fields in both rules are equal.

1: tcp, 140.192.37.10, any, 163.122.51.∗, 21, accept
2: tcp, 140.192.37.10, any, 163.122.51.∗, 21, deny

Definition 2: Rules Rx and Ry are inclusively matched if they do not exactly match and if every field in Rx is a subset or equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are inclusively matched since they do not exactly match and every field in rule 1 is a subset or equal to the corresponding field in rule 2. Rule 1 is the subset match of the relation while rule 2 is the superset match.
1: tcp, 140.192.37.10, any, 163.122.51.∗, 80, accept
2: tcp, 140.192.37.∗, any, 163.122.51.∗, any, deny

Definition 3: Rules Rx and Ry are completely disjoint if every field in Rx is not a subset and not a superset and not equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are completely disjoint since all corresponding fields in both rules are distinct.
1: tcp, 140.192.37.10, 2000, 163.122.51.50, 80, accept
2: udp, 140.192.37.20, 3000, 163.122.51.60, 21, accept

Definition 4: Rules Rx and Ry are part subset or a superset or equal to the corresponding field in Ry, and there is at least one field in Rx that is not a subset and not a superset and not equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are partially disjoint (or partially matched) since all fields in rule 1 are related to the corresponding fields in rule 2 except the destination port field.
1: tcp, 140.192.37.10, any, ∗.∗.∗.∗, 80, accept
2: tcp, 140.192.37.∗, any, ∗.∗.∗.∗, 21, deny

Definition 5 Rules Rx and Ry are correlated if some fields in Rx are subsets or equal to the corresponding fields in Ry, and the rest the fields in Rx are supersets of the corresponding fields in Ry.

For example, Rule 1 and rule 2 below are correlated since they have the same protocol, source and destination ports, and the source address of rule 1 is a subset of the corresponding fields in rule 2 , and the destination address of rule 1 is a superset of that of rule 2.
1: tcp, 140.192.37.10, any, ∗.∗.∗.∗, 80, accept
2: tcp, ∗.∗.∗.∗, any, 140.192.37.∗, 80, deny

B. Firewall policy Anomaly detection

A firewall policy anomaly is defined as the existence if two or more different filtering rules that match the same packets. Here we define different types of anomalies that may exist among filtering rules in a firewall policy.

Firewall policy anomaly types:

1). Shadowing anomaly: A rule is shadowed when a previous rule matches all the packets that matches this rule, such that the rule of shadowed will never be evaluated. Shadowing is a critical error in the policy as the filtering rules never be effects.
2). Correlation anomaly: Two rules are correlated , if they have different filtering actions, if the first rule in order to matches some packets that matches the second rule and the second rule matches some packets that match the first rule.
3). Redundancy anomaly: A rule is redundant if there is another rule that produces the same matching and action such that if the redundant rule is removed, the security policy will not be affected.
4). Generalization anomaly: A rule is a generalization of another rule if the first rule matches all the packets that the second one could match but not the opposite.

C. Automated correction of policy fault

[5] Lupu and M. Sloman. "*Conflict Analysis for Management Policies."* In Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM'1997), May 1997.

[6] S. Cobb, *"ICSA Firewall Policy Guide v2.0,"* NCSA Security White Paper Series, 1997.

[7]J. Wack, K. Cutler, and J. Pole, *"Guidelines on Firewalls and Firewall* Policy," NIST Recommendations, SP 800-41, Jan. 2002.

[8]A. Wool, *"Architecting the Lumeta Firewall Analyzer,"* Proc. 10th USENIX Security Symp, Aug. 2001.

[9]W. Cheswick and S. Belovin, Firewalls and Internet Security, Addison-Wesley, 1995

[10]J.A. Jones and M. J. Harrold. Empirical evaluation of the tarantula automatic fault-. Localization technique. In proceedings of the 20th IEEE/ACM International Conference on Automated Software Engineering, Pages 273-282, 2005

[11]E. Al-Shaer and H. Hamed. Firewall Policy Advisor for anomaly discovery and rule editing. In Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on, pages 17–30, 2003.

[12]T. Tran, E.Al-Shaer, and R. Boutaba. PolicyVis: Firewall Security Policy Visualization and Inspection. In proceedings of 21st Large Installation System Administration Conference. Nov, 2007.

