iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Analysis of Security Features Offered by Firewall

Okoronkwo, Madubuezi C. M.Sc.
Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria

Abstract-In this period where most Internet users have dissimilar intent and with the unfasten, threatening scenery of the Internet world, the security of information consequently, becomes a top concern to all. Internet security is a major problem faced in fashionable growth. Firewalls are configured to guard against unauthorized interactive logins from the outside world. This helps prevent hackers from logging into machines on your network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside. This paper examines internet security with emphases on Firewall and how it can help secure the internet.

Keywords: Security; Internet; Firewall; Information.

I. INTRODUCTION

A firewall is software that screens incoming traffic to prevent hackers' access to its files. It is often installed on routers (devices that moves information or data across an internetwork from source to destination), servers, or some other device. It is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications [1]. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. The device physically and/ or logically is a first point of access into a networked system. They let only designated users have access to the networks. They can block access to unauthorized entries, effectively acting as security firewalls. Firewalls provide logging, auditing, and sucker traps to identify access attempts and to separate legitimate users from intrudes. Some firewalls offers comprehensive Security Suite that delivers an enterprise-wide security solution that goes far beyond the capabilities of previous Firewall solutions [2]. Figure 1 shows the basic configuration of a firewall.

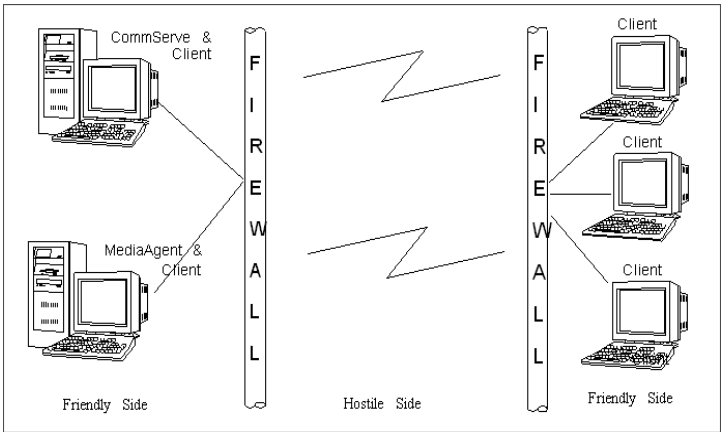


Figure1: Basic configuration of a firewall system.

II. TYPES OF FIREWALL TECHNIQUES

Firewalls are configured to guard against unauthenticated interactive logins from the external environment. This helps stop hackers from logging into the network. The different types of firewall techniques include:

A. Proxy server:

Proxy server intercepts all messages inflowing and parting the network. The proxy server efficiently hides the true network addresses.

B.Packet filters:

ISSN: 2321-9653

Packet filters looks at each packet inflowing or parting the network and accepts or rejects it based on user-defined rules

C.Application gateways:
Application gateways applies security mechanisms to specific applications, such as FTP and Telnet servers.

D.Circuit-level gateway:
Circuit-level gateway applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

III. FIREWALLS SECURITY SUITES

This unique and innovative Security Suite includes:

A. *Open Platform for Secure enterprise Connectivity (OPSEC)*

OPSEC integrates all aspects of network security through a single, extensible management framework. OPEC allows enterprises to take full advantage of the firewall security Suite and other security applications. The OPSEC framework provides central configuration and management for Firewall, while integrating third party security applications. OPSEC is both open and extensible, incorporating a variety of security applications in a single, centrally managed security system [3]. Enterprises can take full advantage of the latest security technologies and can upgrade individual components without having to reconfigure an entire security system.

B. Stateful Inspection Technology
Stateful Inspection Technology delivers full Firewall wall capabilities, assuring the highest level of network security. Firewall's powerful Inspection Module analyzes all packet communication layers and extracts the relevant communication and application state information. The Inspection Module understands and can learn any protocol and application. By employing this flexible, extensible technology, Firewall meets the dynamic security requirements of today's enterprise. The Firewall Inspection Module resides in the operating system kernel, below the Network layer, at the lowest software level. By inspecting communications at this level, Firewall can intercept and analyze all packets before they reach the operating systems. No packet is processed by any of the higher protocol layers unless Firewall verifies that it complies with the enterprise security policy. The Inspection Modules has access to the "raw message," and can examine data from all packet layers. In addition, Firewall analyzes state information from previous communications and other application. The Inspection Module examines IP addresses, port numbers, and any other information required in order to determine whether packet comply with the enterprise security policy [4]. The Inspection Modules stores, and update state and context information in dynamic connections tables. These tables are continually updated, providing cumulative data against which Firewall checks subsequent communications. Firewall follows the security principal of "All communications are denied unless expressly permitted". By default, Firewall drops traffic that is not explicitly allowed by the security policy and generates real-time security alerts, providing the system manager with complete network status. This inspection Module also understands the internal structures of the IP protocol family and applications built on top of them. For stateless protocols such UDP and RPC, the Inspection Module extracts data from a packet's application content and stores it in the state connections tables, providing context in cases where the application does not provide it. In addition, the Inspection Module can dynamically allow or disallow connections as necessary [5]. These capabilities provide the highest level of security for complex protocol.

C. Enterprise-wide security management
Firewall allows an enterprise to define and implement a single, centrally managed security policy. A firewall security policy is expressed in terms of a rule base and properties. The rule base is an ordered set of rules against which each communication is tested, while properties define over all standards of communication inspection. Firewall rules specify the source, destination, service and action taking for each communication. The security rules also specify which events are logged and the information included in each log entry. The security policy is managed and updated from a single, centralized work station. All communications between this work station and Firewalled enforcement points are authenticated and transmitted on secure channels [6]. A Firewall rule base specifies the actions taking on communication attempts-whether they are allowed, disallowed, logged, etc. A security policy is defined not only by the rule base, but also by the parameters in the properties set up window. Properties define the overall aspects of communication inspection without the need specify repetitive details in the rule

base. Firewall detects spoofed packets by checking that the source IP of a packet entering a Firewalled gateway corresponds to the appropriate gateway interface. Firewall's object-oriented interface allows security administrators to define anti-spoofing for all gateway interfaces and generate alerts. The Firewall Module includes the inspection module and security servers. The Firewall Module implements the security policy, logs events, and communicates with the management module using the Firewall daemons. A machine on which the Firewall Inspection Module is installed is known as a "Firewalled system". The Firewall Module can be installed on a broad range of platforms. It usually resides on the dual-homed host (a gateway) but can also be installed on a server. Inspection code is then generated and installed on the Firewall modules that will enforce the security policy.

D. Distributed client/Server Architecture

Although Firewall is deployed in a distributed configuration, security policy enforcement is completely integrated. Any number of Firewall modules can be set-up, monitored and controlled from a single workstation, but there still only one enterprise-wide security maintained by a single rule base and log file. Authorized management clients can access security control information from anywhere on the network.

E. Authentication

Firewall provides remote users and telecommuters secure, authenticated access to enterprise resources using multiple authentication schemes. Firewall authentication services securely validate users or clients that try to access the internal network. Modifications to local servers or client applications are not required. All authentication sessions can be monitored and tracked through the Authentication methods. Firewall provides three authentication methods:

1. User Authentication
2. Client Authentications
3. Session Authentication

User authentication provides accesses privileges on a per user basis for FTP, TELNET, HTTP, and RLOGIN, regardless of the user's IP address. If a local user is temporally away from the office and logging in on a different host, the security administrator may define rule that allows that user to work on the local network without extending access to all users on the same host. The firewall security servers implement user authentication on the gateway. Firewall intercepts a user's attempt to start an authenticated session on the requested server and directs the connection to the appropriate security server. After the user is authenticated, the firewall security server opens a second connection to the host. All subsequent packets of the session are intercepted and inspected by firewall on the gateway. Client Authentication enables an administrator to grant access privileges to a specific user at a specific IP address. In contrast to user Authentication, Client Authentication is not restricted to specific services, but provides a mechanism for authenticating any application, standard or custom. Firewall client Authentication is not transparent but it does not require any additional software or modifications on either the client or server. The administrator can determine how each individual is authenticated, which servers and applications are accessible, at what times and days, and how many sessions are permitted. Session Authentication can be used to authenticate any service on a per session basis. After the user initiates a connection to the server, firewall opens a connection with a session Authentication Agent. The Agent performs the required authentication, after which firewall allows the connection to continue to the requested server.

Some of the authentication schemes are:

S/key – The user is challenged to enter value of requested S/key iteration.

Secure ID-The user is challenged to enter the number displayed on Security Dynamics Secure ID card.

OS Password- The user is challenged to enter his or her OS password.

Internal-The user is challenged to enter his or her Internal Firewall-1 password on the gateway.

RADIUS-The user is challenged for a response, as defined by the RADIUS server.

F. Network Address translation

Firewall's Network Address Translation features provide complete Internet access for internal hosts with invalid or secret IP address. Internal host can be accessible from the internet, even though their internal IP addresses are invalid internet addresses. Firewall supports both IP address hiding and Static Address Translation, providing full internet connectivity for internal clients. At the same time, Firewall completely integrates Address Translation rules in the security policy, maintaining full network security. Firewall address rule can be simply generated and integrated into the enterprise security policy. Firewall provides three methods for configuring Address Translations:

i. Automatic Configuration

ISSN: 2321-9653

Address Translation properties can be defined for particular objects, such as workstations or networks. Address Translation rules are then automatically generated, and the object's properties are applied whenever it it used in the security policy.

ii. Address Translation Rule Base

Address Translation Rule base allows administrators to specify objects by names rather than by IP address, restrict rules to specified destination IP addresses, as well as to the specified source IP Addresses. It translates both source and destination IP addresses in the same packet, restricts rules to specified services (ports), and translates ports.

iii. Command Line Interface

Address Translation rule can be defined using a command line interface application. It is also possible to directly edit the text file SFWDIR/conf/xlate.conf.

Firewall supports two types of Address Translation modes to protect internal addressing scheme while providing full internal access:

a. Dynamic: Firewall translates many invalid addresses to a single valid address and dynamically assigns port numbers to distinguish between the invalid address. Dynamic address translation is called "Hide Mode," because the invalid addresses are hidden behind the valid address.

b. Static: Firewall translates each invalid address to a corresponding valid address.

G. Encryption

Firewall provides transparent, selective encryption for a wide range of services, allowing organizations to make full use of the internet for all business and connectivity needs. Multiple encryption schemes, key management and an internal Certificate Authority are fully integrated with other Firewall features. Firewalled gateways encrypt data communications traveling over the internet between private networks, creating secure, virtual private networks. Firewall implements encryption for corporate internetworks without the need to install and configure encryption software on every host in the network involved [7]. A Firewalled gateway performs encryption on behalf of its encryption domain-the local area network (LAN) or group of networks that it protects. Behind the gateway, in the internal networks, packets are not encrypted. Only packets traveling over public segment of the connection are encrypted.

Selective encryption features allows the transmission of both clear and encrypted data between the same workstations and networks. Instead of encrypting all communications between corporate networks, Firewall allows administrators to define the specific services that require encryption.

H. Content security

Firewall's extensive content security capabilities protect networks from various threats, including viruses and suspicious Java and Active code, while providing fine-tuned access control to the internet. Firewall content security is defined through resources objects, and implemented by a suite of security Servers at the application level. Content Security is fully integrated with other Firewall features, and is centrally managed through the intuitive graphical interface (as Check Point Firewall-1 Security Suite). In addition, OPSEC framework provides open APIs for integrating third-party content screening applications.

Anti-virus inspection is vital to enterprise security. Firewall integrates third-party anti-virus applications through the Content Vectoring Protocol (CVP). For example, if an FTP resources definition specifies anti-virus checking, Firewall intercept FTP attempts and sends the transferred files to a CVP server. The CVP server examines the transferred files and replies with inspection results to the Firewall module. Firewall processes the original connection depending on the reply. OPSEC management provides an open API for defining transactions between Firewall and third-party CVP servers. URL screening provides precise control over web access, allowing administrators to define undesirable or inappropriate web pages. Firewall checks web connection attempts using third-party URLs and their appropriate categories (i.e. permitted or denied). URL databases can be updated to provide a current list of blocked sites. OPSEC includes an API for integrating third-party URL screen applications.

Firewall's Java and ActiveX screening includes following capabilities: Stripping Java applet tags from HTML pages, stripping Java applets from all server-to-client replies, even if the reply is a compressed or achieved file, blocking Java attacks by blocking suspicious back connections, and stripping ActiveX tags from HTML pages.

I. Connection control

Firewall extends network connectivity by distributing a processing load among several servers. Firewall implements

load balancing using a network object known as a Logical Server, a group of servers providing the same service [8]. In the Rule Base, Administrators can define a rule directing connections of a particular service to the appropriate Logical Server. The Logical Server handles the connection attempt using one of five pre-defined load-balancing algorithms:

a. Server load: Firewall queries the server to determine which is best able to handle the new connection. There must be a load-measuring agent on the server.

b. Round Trip: Firewall uses PING to determine the round-trip times between the Firewall and each of the servers and chooses the server with the shortest round trip time.

c. Round Robin: Firewall imply assigns the next server in the list.

d. Random: Firewall assigns a server at random.

e. Domain: Firewall assigns the "closest" server, based on domain name.

Although a Logical Server may consist of several servers, the client is aware of only one server. When the service request reaches the Firewall, Firewall determines which of the servers in the group will fulfill the request, based on the load-balancing algorithm assigned to the logical server.

J. Router Management

Firewall provides centralized network and security management for routers throughout the enterprise. The enterprise security policy is defined and maintained from a single management station, while routers operate as security enforcement points.

Firewall manages routers in two ways:

a. Access Lists: Firewall downloads access Lists derived from the security policy to selected routers.

b. Stateful Inspection: The Firewall Inspection Module runs directly on specific routers and network devices. The standard Firewall features, with the exception of encryption, address translation, and client and session authentication are supported.

IV. CONCLUSION

This research has analyzed the capability of Firewalls technology as one of the most important security tool. They are configured to guard against unauthorized interactive logins from the outside world. This helps prevent hackers from logging into machines on the network. Firewalls Security Suites include: Open Platform for Secure enterprise Connectivity, Encryption, Connection control, Router Management, Stateful Inspection Technology, Content security, Network Address translation, Enterprise-wide security management, Distributed client/Server Architecture etc.

REFERENCES

[1] Check point Software Technologies, Inc. "Everything you need to know about network Security,"1998.

[2] Carnegie Mellon University, "Computer Security,"2001.

[3] Dave Lowe, "Getting to know Internet Security," Internet Industry Analyst NTCA epapers, Volume 1 Number 2B, 2001

[4] Richard Power, "2002 CSI/FBI computer crime and security," Computer Security Issues and Trends, Vol. VIII, No.1, Spring 2002

[5] Radia Perman, "Interconnections: Bridges and Routers," MA:Addison,1992.

[6] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly & Associates, Sebastopol, C.A, 199 5

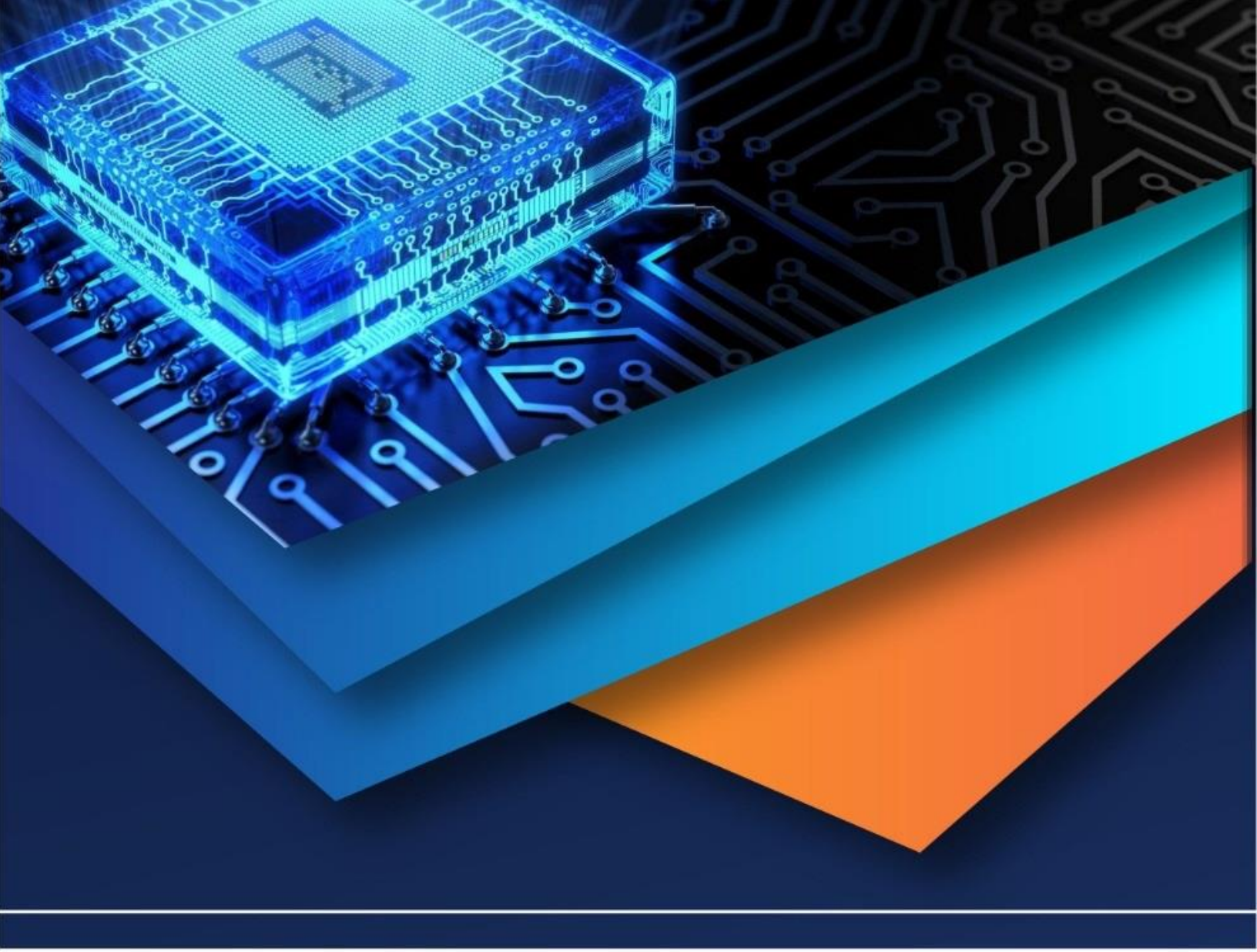
[7]http://www.vicomsoft.com/knowledge/reference/firewalls1.html

[8]http://www.freebsd.org/doc/en_US.ISO8859 1/books/handbook/firewalls.html

AUTHOR



Okoronkwo Madubuezi C. is currently a lecturer in Computer Science Department of Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. He has a Bachelor Degree in Computer Science from Michael Okpara University of Agriculture, Umudike, and a Master's Degree in Computer Science from Ebonyi State University, Abakaliki. He is presently pursuing a PhD programme in Computer Science from Nnamdi Azikiwe University, Awka, Anambra State of Nigeria with interest in System analysis, Design and Development. He is a member Computer Professionals of Nigeria.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)