International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.3, pp : 306-309 1 March 2014

Network Security Using Linux/Unix Firewall

Archit Uprit
Scientist 'B',Central Pollution Control Board, Parivesh Bhavan, CBD Cum Office Complex, East Arjun Nagar, Delhi - 110032, archit.uprit@gmail.com

ABSTRACT *-> **Network Security concerns with concept of designing a secured network is the most important task in any enterprise or organization development. Securing a network mainly involves web filtering, application control, applying policies and rules in your network to protect from unauthorized access. Servers such as application server, web server, Database server are critical devices in your network which require complete Network security for proper working in any organization. This paper demonstrates how you can secure your Network components and critical servers using Untangle Firewall and how you can manage Network Bandwidth by protecting your network from gateway level viruses and block unwanted traffic from untangle firewall.***

KEYWORDS-untangle firewall, IDS (Intrusion detection system),WIPS (Wireless intrusion protection system),RDP(Remote desktop protocol),DDOS(Distributed denial of service attack).

INTRODUCTION

Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor organization network. Drawing the line that separates internal and external networks is known as firewall. Firewall filters the traffic based on ipaddress, protocol and port which enable the Network Administrator which systems and services (HTTP, FTP, SMTP, etc) are publicly accessible. Linux Firewall delivers an integrated family of applications that simplify and consolidate the network and security products that Organization need at the Network Gateway Level. Linux Firewall also controls the flow of traffic between external and private network. Filtering Decision is based on Firewall policy implemented and configured by Network Administrator. For each type of network size and Bandwidth different policies configured and implemented in network. Every internal and external packet arrives at firewall, must be checked the policies configured by Network Administrator based on the configured policies the firewall decides the packets to allow or deny.

1. Intrusion Detection System(IDS) =-An Intrusion Detection System goes beyond and below firewall filtering by looking at the pattern of network connections recognizing port scans, specific signatures of threats and denial of service attacks. IDS uses a packet inspection engine in conjunction with a standard NAT firewall to recognize the pattern in network traffic.

2. Intrusion Prevention System(IPS) - Intrusion Prevention System is also known as Intrusion Detection system. The main function of Intrusion prevention system is to identify malicious activity, log information about this activity, attempt to block/stop it and report it. Intrusion prevention systems are considered the extension of intrusion detection systems because they both monitor traffic and network activities for malicious activities. The main Difference between IPS and IDS unlike intrusion detection systems, intrusion prevention system are placed at Network gateway level to prevent/block intrusions that are detected.

Classified of intrusion detection system .

It is classified into four basic type:-

a. Network Based intrusion prevention system (NIPS): Monitors the entire network for suspicious activity by analyzing protocol traffic like HTTP, TCP, RDP etc.

b. Wireless intrusion prevention system (WIPS): Monitors the wireless network for suspicious traffic by analyzing wireless networking protocols like DHCP (Dynamic Host Configuration Protocol).

c. Network Behavior Analysis (NBA): examines the network traffic to identify the threats that generate unusual traffic flows such as DDOS (distributed denial of service attacks), certain form a malware and policy violations.

d. Host Based Intrusion Prevention System: an installed software package which monitors a single host in network for suspicious activity by analyzing events occurring in that host.

INTRODUCTION OF LINUX/UNIX

a. Linux/Unix is an open source operating system like Debian and Free BSD(Berkley Software Distribution) both are Unix like Operating system it has main beneficial features where user can modify and customize the code according to Organization Requirement.

b. Linux/Unix is an Operating System was born in the late 1960s. it originally began as a one man project led by Ken Thompson of Bell Labs, and has since grown to become the most widely used operating system.

Advantages of Linux/Unix system as firewall

a. Linux/Unix supports servers like Apache/ SSH servers to run on it and it also use a program called pf (packet filter) with iptables.

b. With Linux/Unix Firewall you do more like traffic analysis/shaping and CPU load intrusion detection etc.

c. Upgradability: Every time a new kernel or version of userland apps come out you can get bug fixes and new features.

d. Security: In Linux you have the source code with you can modify and verify it correctness. In Case of Proprietary Software if License expires your services like Web Filtering / Packet Filtering/ Spam Filtering Stops getting signatures.

Firewall Rules and Policies to Secure Network

a. Different Firewall usually provides different rule logic with different parameters. But some basic rules are common to all. They all allow action to be defined allowing or denying network traffic. Many applications using rules like firewall, Captive Portal, Application Control, Bandwidth Control, etc. All of these rules essentially share the same logic.

b. Rules and policies are configured by the Network Administrator to Manage Network Traffic for example firewall uses the rule to block or deny traffic. Whereas Bandwidth Controller uses rule to determine how to prioritize a session.

c. Each Rule has several properties mentioned below:

1. An enable checkbox.
2. A name/description
3. A set of Conditions
4. An Action or Set of Action

d. Let's take a simple example: We want to block TCP traffic to port 80 on server. There is a web service running on the server that you don't want to allow access to.

1. First create a rule and enable it.
2. Give Descriptive name to that Rule like Blocking TCP port 80 to serverX.
3. Now you will need to add some conditions that match only the traffic you want to block.
4. So in this example we will add TCP protocol which uses Port No 80.
5. Destination Address is 1.2.3.4(IP Address of the Server).
6. Destination Port is Port 80.
7. Finally set the action to Block or Deny and save it.

NAT Translation supporting security

a. NAT(Network Address Translation) is a mode of NAT that maps one internal address to one external address for example if a network has an internal servers at 192.168.1.10,1:1 NAT can map 192.168.1.10 to 1.2.3.4 where 1.2.3.4 is an external ip address provided by your ISP.

b. The NAT translation represents a level of indirection. Thus it dynamically creates a type of Firewall between the organizations network and the public internet. It is more difficult for any internal devices to access directly by someone malicious because the internal user don't have publically known IP addresses.

c. A large number of internal users can share single Public IP address this saves money and also conserves Ip address space. In addition to that an increased number of systems are possible because of the IP Address Space.

Literarture review- In[1] researchers have proposed the untangle firewall and its advantages over the network where client server load . This paperwork demonstrates the tasks needed to enhance the network security in Linux environment. The various security modules existing in Linux makes it different from other operating systems. we analyzing network packets using the most popular open source network protocol analyzer wire shark and on the basis of analyzing the packet work has been done on writing the script to block/allow the network traffic using ip firewall and after blocking traffic further capturing and analyzing of packets using wire shark.

Network firewalls are devices or systems that control the flow of traffic between networks employing different security postures. The network traffic flow is controlled according to a firewall policy. The filtering decision is based on a firewall policy defined by network administrator. For each type of network traffic, there are one or more different rules. Every network packet, which arrives at firewall, must be checked against defined rules until first matching rule is found.

The packet will be then allowed or banned access to the network, depending on the action specified in the matching rule[3].

Packet filtering allows you to explicitly restrict or allow packets by machine, port, or machine and port. For instance, you can restrict all packets destined for port 80 (WWW) on all machines on your LAN except machine X and Y. Ip firewalls are used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user- defined chains[4].

Firewall rules

Different firewalls usually provide different rule logic with different parameters. But some basic elements are common to all. They all allow an action to be defined allowing or banning specific network traffic. Also, all of them allow checking for most important elements in packets like IP addresses, ports and protocol. Software for firewall rule optimization (FIRO) was originally developed for ip firewalls firewall command tool. One of the most important functionalities of ip firewalls

firewall is stateful inspection. Stateful inspection automatically opens only the ports necessary for internal packets to access the Internet. It only allows transfer of packets which are defined in firewall rules and which are part of established connections.

Consideration of network administrator .

As a Network Administrator, the tasks generally fall into the following areas:

1. Designing and planning the network.
2. Setting up the network.
3. Maintaining the network.
4. Expanding the network with Security Measures
5. Network monitoring.

About 70 percent of new attacks target Web enabled and their number is growing. Network Administrator should implement Web security solutions that provide secure Web access as well as protect Web servers and application servers. The security solutions must be easy to deploy and should also provide integrated access control.

FUTURE WORK – The security can be enhanced by the implementation of security policies at different tiers of internal and external work .These policies shall be updated by using the advantages of file security given by LINUX/UNIX .The implicit security can be concrete by applying parallel filtering of web and network based packets on the basis of policies defined by the firewall administrator .In future multiple firewalls with untangled policy shall be applied and the intrinsic security shall be provided by the mature linux/unix file level security .

1. **Res**earchers can work on the the various compatibility modes of linux/unix running devices providing unilateral security from external attack .
2. The operating system security can be expanded to the gateway level by making the files unix based .
3. A Distributed firewall protection mechanism can be developed on linux platform using advance policies at the packet level
4. A system can be developed ranging between wired and wireless medium applying the proposed method .
5. Port filtering and scanning mechanism can be developed to secure the system .
6. Application level session monitoring and control system can be developed at internal and external network .
7. Network load on servers can be worked upon by security policies and load sharing techniques to migrate processes creating vulnerable files and actions .

CONCLUSION-

The suggestion and proposed method can lead to secure network and servers bearing high load and deadlock states .

Te default security provided by LINUX/UNIX adds on to the Untangle firewall security . Whereas linux unix acts as secure platform for implementing security policies defined by the network administrators. The session termination of unwanted and delayed sessions of applications leads to load balancing which leads to a high performance and secured client server setup .

References-

i. *Sachin Taluja,Pradeep verma, Rajeshwar Dua , "Network security using IP firewall" ,International journa; of advance research in computer science and softeare engineering .Volume 2,august 2012.*

ii. *Enhancing Network Security in Linux Environment, Technical Report, IDE1202,February 2012*

iii. *Michael R. Lyu and Lorrien K. Y. Lau,"Firewall Security: Policies, Testing and Performance Evaluation",M. Goncalves, "Firewalls", McGraw-Hill, 1998 & Internet Firewalls and Securitywww.linuxsecurity.com/resource_files/firewalls/nsc/500619.html & Designing Scalable and Effective Decision Support for Mitigating ...web.eecs.umich.edu/.../securecomm11_vulnerability_m United States*

iv. *Packet Filtering using IP Tables in Linux,"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011"ISSN (Online): 1694-0814 [4]Linux - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Linux & Security Issues – Linux.orgwww.linux.org/article/view/security-issues & Quick HOWTO:Ch14 : Linux Firewalls Using iptables - Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_: United States. &Packet filtering using iptables, http://netfilter.org/documentation/HOWTO/packet-filtering- OWTO-7.html*

v. *Guidelines on Firewalls and Firewall Policy, Computer Security Division, National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009) Gaithersburg, MD 20899-8930, September 2009*

vi. *Packet Filtering using IP Tables in Linux,"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011"ISSN (Online): 1694-0814 [4]Linux - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Linux & Security Issues – Linux.orgwww.linux.org/article/view/security-issues & Quick HOWTO:Ch14 : Linux Firewalls Using iptables - Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_:_... - United States. &Packet filtering using iptables, http://netfilter.org/documentation/HOWTO/packet-filtering- OWTO-7.html*

vii. *Michael R. Lyu and Lorrien K. Y. Lau,"Firewall Security: Policies, Testing and Performance Evaluation",& M. Goncalves, "Firewalls", McGraw-Hill, 1998 & Internet Firewalls and Securitywww.linuxsecurity.com/resource_files/firewalls/nsc/500619.html & Designing Scalable and Effective Decision Support for*

Mitigating ...web.eecs.umich.edu/.../securecomm11_vulnerability_m... - United States

viii. Tihomir Katić Predrag Pale,"Optimization of Firewall Rules "Proceedings of the ITI 2007 29 Int. Conf. onInformation Technology Interfaces, June 25-28, 2007, Cavtat, Croatia &Manual: IP/Firewall/Filter - MikroTikWikiwiki.mikrotik.com/wiki/Manual: IP/Firewall/Filter & iptables - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Iptables &Net filter - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Net filter.& Firewall Policy Change-Impact Analysis ALEX X. LIU, Michigan State University & Guidelines on Firewalls and Firewall Policy, Computer Security Division, National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009) Gaithersburg, MD 20899-8930, September 2009

ix. Daniel Bilar,"PacketProcessingInIptables"Computer science at UNO Spring 2011" & Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_:_... - United States. &Packet filtering using iptables

x. ipfirewallsHome,http://www.netfilter.org/& iptables Scripting, http://www.linuxdoc.org/ [14]iptables command,http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-iptables-options.html