Analysis of ACL in ASA and Enhancing ASA in Firewall

Kumar Shiv, Bhardwaj Ekta, Poonam

[1]M.Tech scholar, Department of computer science & Engineering, NGFCET
[2]M.Tech scholar, Department of computer science & Engineering, NGFCET
[3]M.Tech scholar, Department of computer science & Engineering, NGFCET
Email: [1]skrawat88@gmail.com , [2]ektabhardwaj88@gmail.com, [3]er.poonam.it@gmail.com

Abstract:- Network security is the major issue in the present-day scenario, where every person, association depends on connected networks. Securing a network depends upon numbers of policy and rule that are implemented in a device (Firewall). Firewall is the most important network device that imposes association safekeeping. In this paper we travel the Firewall security and enhance its performance with existing rule, and make it more secure. We firewall methodology that helps in decision making and analyze is it fully capable to handle any unauthorized access? We analysis here the following things: clustering, load management, packet loss for this we have communicate router with routing table information with the firewall and monitor the packet. As well as implemented the policy and checked weather it passes or get deny by firewall.

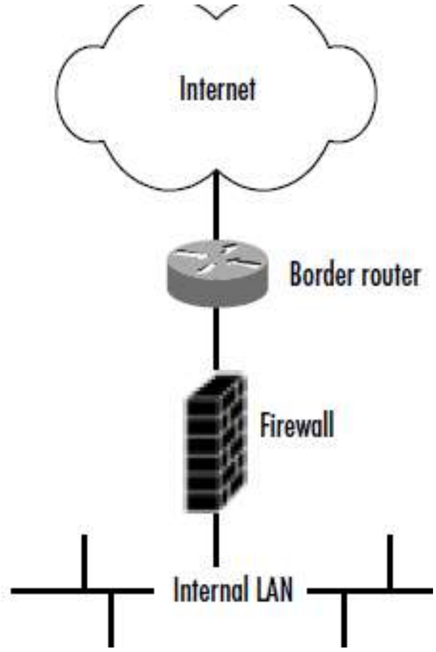
Keyword: *ACL, ASA Firewall, Network security, Validation error*

*****

Introduction

FIREWALLS have become central fixtures in secure network infrastructures. Firewalls are software and hardware systems that protect intra-networks from attacks originating in the outside Internet, by filtering and managing Internet traffic. Despite their critical role, firewalls have traditionally been tested without well-defined and effective methodologies. Currently, a diverse set of firewalls is being used. Because it is infeasible to examine each firewall separately for all potential problems, a general mechanism is required to understand firewall vulnerabilities in the context of firewall operations [1]

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 [2].



Firewall Policies

As part of your security assessment process, you should have a clear idea of the various business reasons for the different communications allowed through yourChanges to the firewall policy should be made sparingly and cautiously, only with management approval, and through standard system maintenance and change control processes.firewall.

Each protocol carries with it certain risks, some far more than others [3]

Address Translation

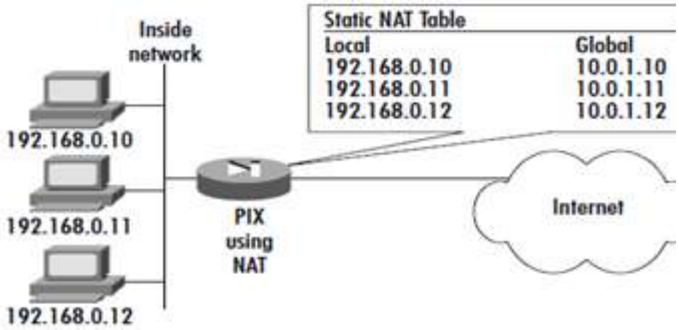
RFC 1918,“Address Allocation for Private Internets,” specifies certain nonregistered IP address ranges that are to be used only on private networks and are not to be routed across the Internet.[3]The RFC uses the term *ambiguous* to refer to these private addresses, meaning that they are not globally unique.The reserved ranges are:
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Network Address Translation (NAT), defined in RFC 1631, comes into play. Most organizations connected to the Internet use NAT to hide their internal addresses from the global Internet.This serves as a basic security measure that can make it a bit more difficult for an external attacker to map out the internal network. NAT is typically performed on the Internet firewall and takes two forms,
static or dynamic.When NAT is performed, the firewall rewrites the source and/or the destination addresses in the IP header, replacing them with translated addresses[4]

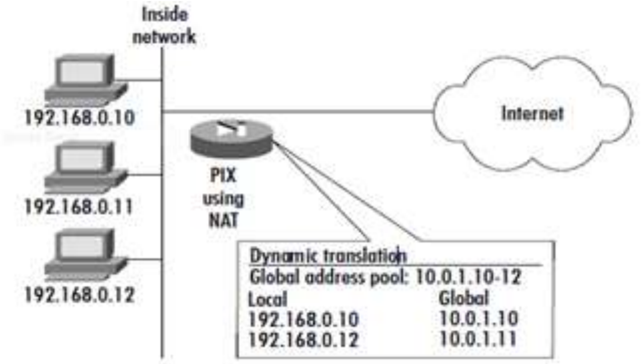
Address Translation

- **I. Static Translation**
- **II. Dynamic Translation**
- **III. Port Address Translation**
- **IV. Virtual Private Networking**

In static NAT, a permanent one-to-one mapping is established between inside local and inside global addresses. This method is useful when you have a small number of inside hosts that need access to the Internet and have adequate globally unique addresses to translate to.



In dynamic NAT is set up, a pool of inside global addresses is defined for use n outbound translation. When the NAT router or firewall receives a packet from an inside host and dynamic NAT is configured, it selects the next available address from the global address pool that was set up and replaces the source address in the IP header



Port Address happens when there are more internal hosts initiating sessions than there are global addresses in the pool? This is called overloading, a configurable parameter in NAT, also referred to as Port Address Translation, or PAT. In this situation, you have the possibility of multiple inside hosts being assigned to the same global source address.The NAT/PAT box needs a way to keep track of which local address to send replies back to.[3]

Configuring Dynamic Address Translation
Address translation is necessary to pass outbound traffic. Address translation (through NAT and/or PAT) maps local IP addresses to global IP addresses. Configuration of NAT/PAT is a two-step process:
□□□Identify the local addresses that will be translated (NAT command). Define the global addresses to translate to (*global* command).
The syntax of the *nat* command is as follows:

```
nat [(<if_name>)] <id> <local_address> [<netmask>
[outside] [dns] [norandomseq] [timeout <hh:mm:ss>]
[<connection_limit> [<embryonic_limit>]]
```

PROPOSED ARCHITECTURE

As security in an endless process, there is always scope for improvement. The security algorithm used in various firewall devices whether Cisco, Juniper, D-link, etc. are somehow based on ASA i.e. Adaptive Security Algorithm. Although ASA is widely used in CISCO networking devices mostly, there is threat of vulnerability. Various techniques are present in market to breach the security. Nowadays various soft-wares are available to crack the network free of cost over the internet. Thus, security of network is a major problem. To overcome this problem organization has to spend huge cost on networking devices such as firewall whether hardware or software. Good secure devices are not only costly during installation but needs a good maintenance cost too.[4]

Our research work consists of providing a solution for vulnerability problem with limited cost too. The work provide with a better algorithm design or some better technique of implementation of Security Algorithm so that these threats can be mitigated. The cost of device and its implementation is also a major challenge to deal with. Any enhancement in current technique or modification should be compatible with the existing networking device as well as in future.

As router provide us the best path only with security feature . As compare to firewall it provide us less security. The security algorithm and technique in router are not much secure. Whereas firewall is more secure with dedicated algorithm, Following are Adaptive Security Algorithm (ASA). This ASA algorithm is not a single algorithm but a collection of many algorithms, each algorithm dedicated for a particular task. This algorithm has significant role in firewall technology, their work is dedicated. If we see the actual flow of my purposed algorithm then it looks like this The device enter in routing phase where routing algorithm is work, which give us the best path for our packet, router nothing do more than it gives us the best path for our packet , then the next phase is firewall phase or we can say the second phase , at this phase ASA algorithm is working , we enhance the existing ASA ,with extra knowledge of routing table , which gives ASA extra feature to verify the packet validation , on behalf of source and destination address ,if packet is authenticate then forward to next phase , Router phase ,where router have already best path knowledge then router send , the packet to best path route ,

Due to this we enhancing our existing ASA and also its cost effective, as per aspect of organization or a developer

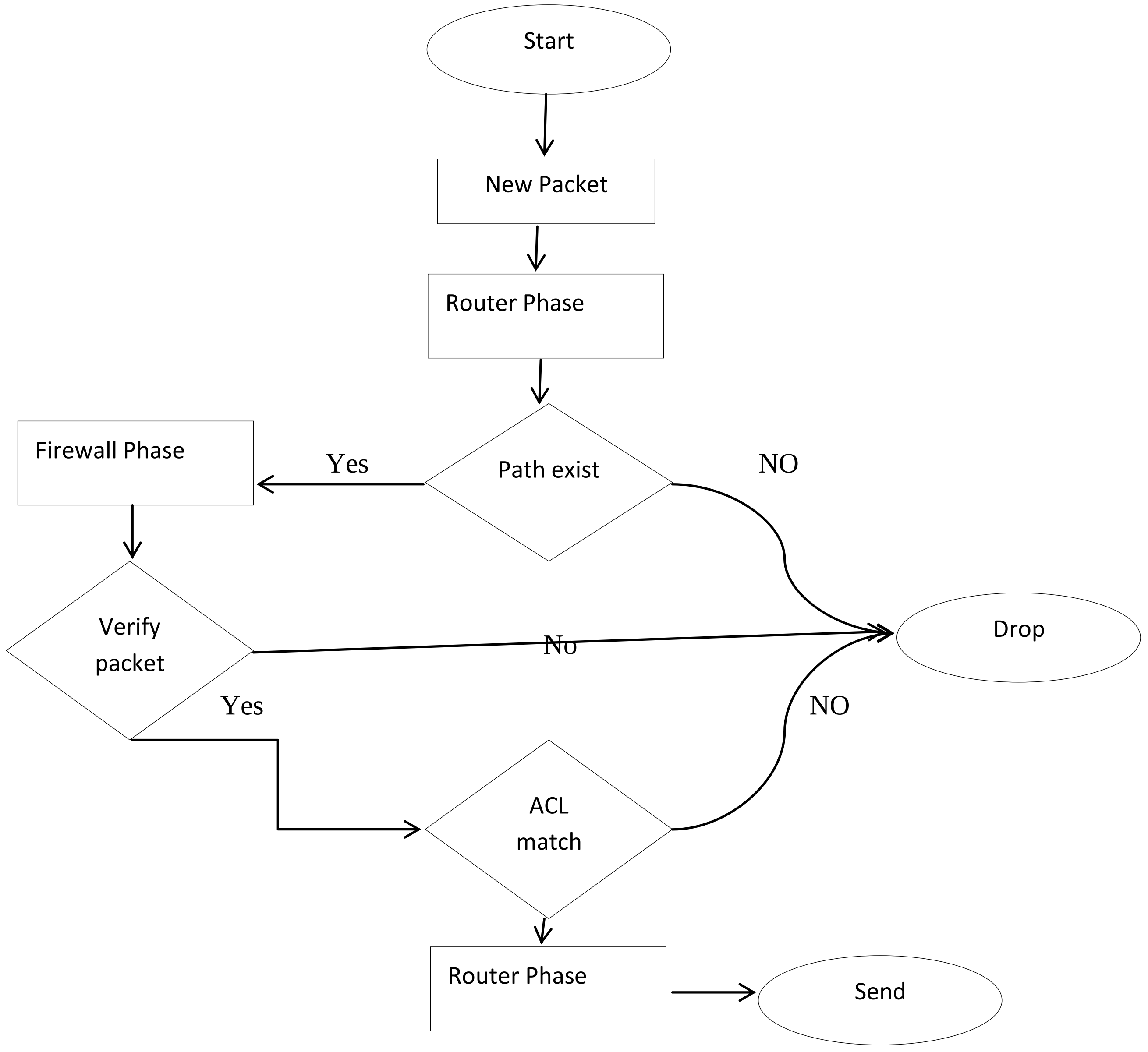


Fig. Flow of Routing Firewall Model

Combining the both device (Router + firewall) on a single platform my effect my thing like if the device configuration not increased then its performance may degraded, so that time performance is the big issue, so we must always remember this thing for the processing this device, configuration is high, doing this we are saving overall cost of a device, and enhancing the performance/ security for the device.

Due to this methodology firewall work separately of filtering the packet on the bases of IP Address and destination mac address, and newly added feature routing table source and destination address. In Existing firewall workings based on TCP/UDP port /IP Address, but this device work on several thing TCP/UDP port / MAC address of sender / IP Address of receiver, Destination port number , destination MAC address(future work), which obviously helps us to send the packet in a secure mode. Thus due to this approach a single device act like a firewall and router, which have cost/time/performance/security effective as compare to existing one router.

REFERENCES

[1] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen Center for Education and Research in Information Assurance and Security (CERIAS)

[2] [2] 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

[3] Export Compliance Guide: 2007 for Cisco ASA 5500 Series Adaptive Security Appliances.

[4] Shikha Pandit et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June-2014, pg. 279-285

[5] Understanding the Basic Configuration of the Adaptive Security Appliance (ASA): Andy Fox, Global Knowledge Instructor, 2009.

[6] Packet Flow through Cisco ASA Firewall: Cisco Systems, Inc. Updated: Jan 19, 2012 (ISBN 1-57870-046-9) Document ID: 113396

[7] Basic concepts of firewall: CISCO information at www.firewall.cx

[8] Cisco ASA Series Firewall CLI Configuration Guide: Software Version 9.1 Cisco Systems, Inc September 18, 2013.

[9] Off-Path TCP Sequence Number Inference Attack Reduce Security: by Zhiyun Qian, Z. Morley Mao 2012 IEEE Symposium on Security and Privacy.

[10] Cisco’s PIX Firewall Series and Stateful Firewall Security: White paper-2009.

[11] Cisco ASA 5510 Firewall Edition Bundle (ASA5510-K8): LASYSTEMS - Brusselsesteenweg 208 - 1730–Belgium 2013

[12] Network Security and Information Assurance : by R.N.Smith, IEEE Phoenix Section Computer Society Chapter Feb 27, 2010