IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A FIREWALL-A SECURE GATEWAY OF THE NETWORK

Ms. Renu*, Dr. Tapas Kumar

ABSTRACT

Computer security is a tough problem. Security on networked computers is much harder. If the machine is connected to a network, the situation is much complex. Firstly, many more entry points to the host than a simple login prompt must be protected. The mailer, the networked file system, and the database servers are all likely sources of danger. Furthermore, the authentication used by some protocols may be inadequate. Nevertheless, they must be run, to provide adequate service to local users. Second, there are now many more points from which an attack can be launched.

Your computers may be safe, but you may have users who connect from other machines that are less secure. This connection-even if duly authorized and immune to direct attack-may nevertheless be the vehicle for a successful penetration of your machines, if the source of the connection has been compromised. The usual solution to all of these problems is a firewall: a barrier that restricts the free flow of data between the inside and the outside. Used properly, a firewall can provide a significant increase in computer security.

KEYWORDS: Firewall, Router, ASA, Packet, ACL,TCP/IP Layers.

INTRODUCTION

Computer security is a difficult problem. Security on networked computers is much harder. The administrator of a single Host can-with a great deal of concern and consideration to details, and a careful and skilled user community-perhaps do an adequate job of keeping the machine secure. But if the machine is linked to a network, the situation is much tricky. Firstly, many more entry points to the host than a simple login prompt must be secured. The mailer, the networked file system, and the database servers are all potential sources of danger. Furthermore, the authentication used by some protocols may be inadequate. Nevertheless, they must be run, to provide sufficient service to local users. Second, there are now many more points from which an attack can be launched. If a computer's users are restricted to a single building, it is difficult for an outsider to try to penetrate system security [1].

Therefore there is a need to secure the entry–exit point of a network. One solution to this problem is firewall. Firewalls block or permit selected traffic based on various parameters (typically IP address, TCP or UDP port number) Another solution is via ACL feature of router with definite limitations.

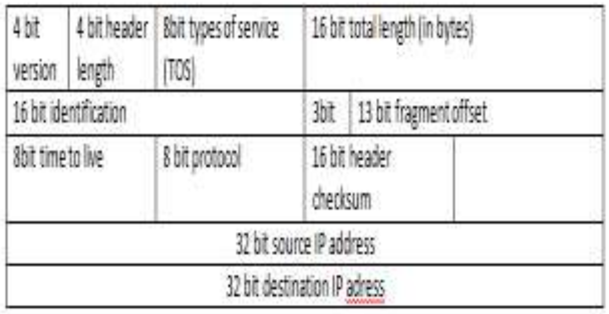
Routing

A routers most important task is simple: to route packets from one network to another network based on a set of rules which it is assigned. However this job gets a lot more complicated when the router is asked to route Internet traffic because of the huge number of networks on the Internet.As stated, a routers task is to route packets from one network to another, however if the focus is IP routing then it is obvious that a router does more than simply route packets from one network to another network, it must actually calculate the fastest route to a packets destination based on the information it has.

An IP packet as seen in figure 1.1 contains a number of fields to aid routing, together with a source address and a destination address, as well as other fields to aid Quality of Service (TOS field) and error correction (checksum).

A router performs the act of routing by utilizing a routing table, which specifies where IP packets should be sent based on by looking at the destination address in the IP packet header.

Figure 1.1:

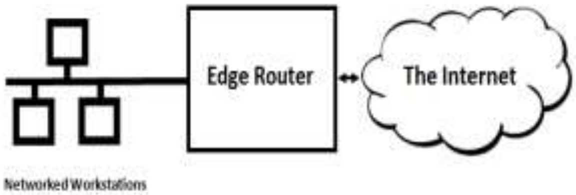


<table>
<tr><td>4 bit version</td><td>4 bit header length</td><td>8bit types of service (TOS)</td><td colspan="2">16 bit total length (in bytes)</td></tr>
<tr><td colspan="3">16 bit identification</td><td>3bit</td><td>13 bit fragment offset</td></tr>
<tr><td colspan="2">8bit time to live</td><td>8 bit protocol</td><td>16 bit header checksum</td><td></td></tr>
<tr><td colspan="5">32 bit source IP address</td></tr>
<tr><td colspan="5">32 bit destination IP adress</td></tr>
</table>

An IP Version 4 packet

There are different types of routers ranging from a router which attaches a single network to the Internet (figure 1.2), a router which connects two sections of the Internet (figure 1.3) and a router which routes traffic in the core of the Internet. Thus different requirements are to be found on a router depending on its location on the global network.

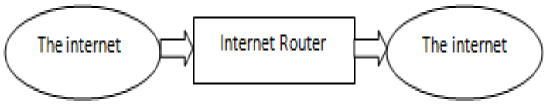
Figure 1.2:



A router connecting a LAN to the Internet

So, a router is a physical device that joins networks together and routes packet between these networks. This work can be done by several of different types of computer.

Fig.1.3:



Router connecting two sections of the Internet

The most common type of routing equipment for entirely hardware based routers specifically programmed to do a single task at deployment time. For example a router may be programmed to forward traffic from network A onto the Internet based upon a dynamically generated routing table created by a routing algorithm. This type of router is extremely efficient, reliable and proven technology usually based on propriety hardware and is such can be very expensive.

FIREWALL

Firewalls are devices or programs that manage the flow of network traffic between networks or hosts that use differing security postures. At one time, most firewalls were deployed at network perimeters. This provided some measure of security for internal hosts, but it could not make out all instances and forms of attack, and attacks sent from one internal host to another often do not pass through network firewalls. Because of these and other factors, network designers now frequently include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to care about mobile devices that are placed directly onto external networks.

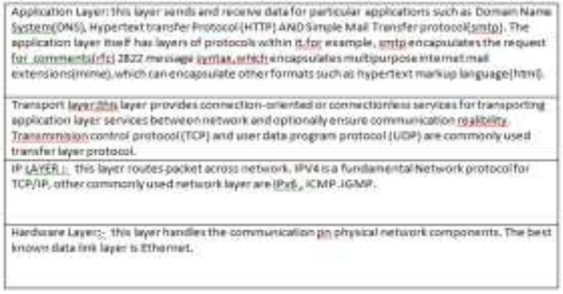
Threats have slowly moved from being most prevalent in lower layers of network traffic to the application layer, which has reduced the general effectiveness of firewalls in stopping threats carried through network communications. However, firewalls are still needed to stop the significant threats that continue to work at lower layers of network traffic. Firewalls can also provide some protection at the application layer, supplementing the capabilities of other network security technologies.

ASA: ADAPTIVE SECURITY ALGORITHM

Adaptive Security Algorithm (ASA) was introduced as being the heart of the PIX Firewall system. Recognizing that ASA is more than just an algorithm for controlling the direction of traffic flows. ASA defines and controls all aspects and features of the PIX devices. ASA provides performance and scalability advantages over application-level proxy firewalls [2].

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that make use of differing security postures. While firewalls are often discussed in the context of Internet connectivity, they may also have applicability in other network environments. For example, many enterprise networks use firewalls to limit connectivity to and from the internal networks used to service more responsive functions, such as accounting or personnel. By employing firewalls to manage connectivity to these areas, an organization can keep away from unauthorized access to its systems and resources. Inclusion of a proper firewall provides an additional layer of security. One way of comparing their capabilities is to look at the Transmission Control Protocol/Internet Protocol (TCP/IP) layers that each is capable to examine. TCP/IP communications are composed of four layers that work together to move data between hosts. When a user wants to move data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding more information. The lowest layer sends the accumulated data through the physical network, with the data then passed upwards through the layers to its destination. Simply put, the data produced by a layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are shown in table 1.1

Table 1.1: TCP/ IP Layers

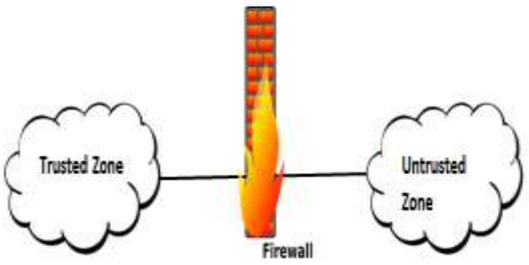


Application Layer: this layer sends and receive data for particular applications such as Domain Name System(DNS), Hypertext transfer Protocol (HTTP) AND Simple Mail Transfer protocol(smtp). The application layer itself has layers of protocols within it.for example, smtp encapsulates the request for comments(rfc) 2822 message syntax,which encapsulates multipurpose internet mail extensions(mime),which can encapsulate other formats such as hypertext markup language(html).
Transport layer:this layer provides connection-oriented or connectionless services for transporting application layer services between network and optionally ensure communication realibility. Transmission control protocol (TCP) and user data program protocol (UDP) are commonly used transfer layer protocol.
IP LAYER :- this layer routes packet across network. IPV4 is a fundamental Network protocol for TCP/IP, other commonly used network layer are IPv6 , ICMP ,IGMP.
Hardware Layer:- this layer handles the communication pn physical network components. The best known data link layer is Ethernet.

1.4 PIX/ASA SECURITY-LEVELS

Cisco security appliances protect trusted zones from untrusted zones.

Fig.1.4:



Basic Working of Firewall

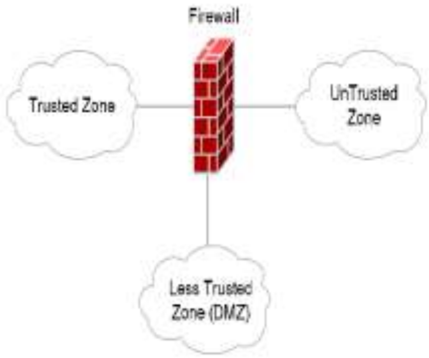
Like most firewalls, a Cisco PIX/ASA will allow traffic from the trusted interface to the untrusted interface, without any explicit configuration. However, traffic from the untrusted interface to the trusted interface must be explicitly acceptable [3].

Thus, any traffic that is not explicitly permitted from the untrusted to trusted interface will be implicitly denied.

A firewall is not restricted to only two interfaces, but can contain multiple 'less trusted' interfaces, often referred to as Demilitarized Zones (DMZ's).

To control the trust value of each interface, each firewall interface is assigned a security level, which is represented as a numerical value between 0 – 100 on the Cisco PIX/ASA. For example, in the above diagram, the Trusted Zone could be assigned a security value of 100, the Less Trusted Zone a value of 75, and the Untrusted Zone a value of 0.

Fig.1.5:



Different Zones in Firewall implementation

As stated previously, traffic from a higher security to lower security interface is (generally) permitted by default, while traffic from a lower security to higher security interface requires explicit permission [4].

ACCESS CONTROL LISTS

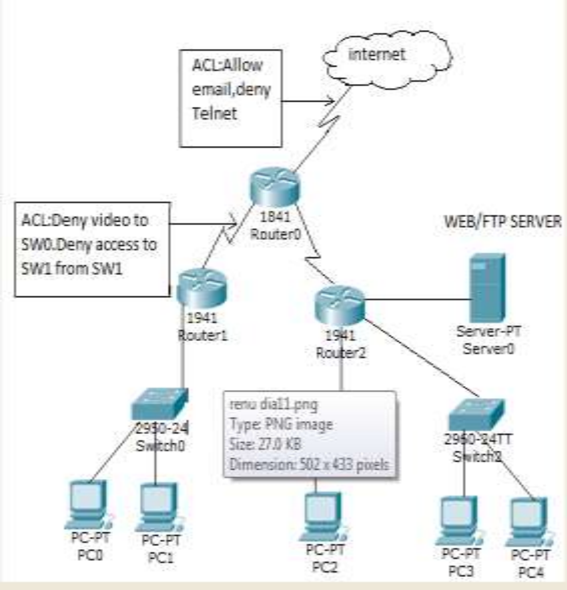
Access Control List (ACL) are filters that facilitate you to control which routing updates or packets are allowable or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks. This can be applied on routers (Cisco).The most significant reason to configure ACLs is to provide security for your network. However, ACLs can also be configured to control network traffic based on the TCP port being used.

HOW ACLS WORKS

A router acts as a packet filter when it forwards or denies packets according to filtering rules. As a Layer 3 device, a packet-filtering router uses rules to verify whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet. These rules are defined using access control lists or ACLs.

When a packet arrives at the router, the router extracts certain information from the packet header and makes decisions according to the filter rules as to whether the packet can pass through or be dropped. Packet filtering procedure works at the Network layer of the Open Systems Interconnection (OSI) model, or the Internet layer of TCP/IP.

Fig.2.1:



Simple Access List Configuration in Router

WHY USE ACLS

- confines network traffic to increase network performance.
- ACLs provide traffic flow control by restricting the delivery of routing updates.
- It can be used as additional security.
- Controls which type of traffic are forwarded or blocked by the router.
- Ability to control which areas a client access.

TYPES OF ACCESS CONTROL LISTS

Standard access-list

Standard access lists create filters based on source addresses and are used for server based filtering. Address based access lists differentiate routes on a network you want to control by using network address number (IP). Address-based access lists consist of a list of addresses or address ranges and a statement as to whether access to or from that address is permitted or denied.

Example of the command syntax for configuring a standard numbered IP ACL:
R1(config)# access-list {1-99} {permit | deny} source-addr [source-wildcard]

i. The first value {1-99} specifies the standard ACL number range.
ii. The second value specifies whether to permit or deny the configured source IP address traffic.
iii. The third value is the source IP address that must be matched.
iv. The fourth value is the wildcard mask to be applied to the previously configured IP address to indicate the range.

Extended access lists

Extended access lists create filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet based filtering for packets that traverse the network.
Example of the command syntax for configuring an extended numbered IP ACL:
Router(config)# access-list {100-199} {permit | deny} protocol source-addr [source-wildcard] [operator operand] destination-addr [destination-wildcard] [operator operand] [established]

i. Like the standard ACLs, the first value {100-199 or 2000 - 2699} specifies the ACL number range.
ii. The next value specifies whether to permit or deny according to the criteria that follows.
iii. The third value specifies protocol type (IP, TCP, UDP, or other specific IP sub-protocols).

Managing Firewall Access Rules
Access rules define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied (with the exception of less common AAA rules). In that sense, they are your first line of defense.

Understanding Access Rules
Access rules policies describe the rules that permit or deny traffic to travel an interface. Typically, you create access rules for traffic entering an interface, because if you are going to deny specific types of packets, it is better to do it before the device spends a lot of time processing them.

There are two separate access rules policies based on the IP addressing scheme. The Firewall > Access Rules policy is for IPv4 addresses, and the Firewall > IPv6 Access Rules policy is for IPv6 addresses. Other than the addressing scheme, and the tools available for use with the policies, configuring IPv4 and IPv6 access rules is the same.

When you set up access rules to devices, they become one or more entries (ACEs) to access control lists (ACLs) that are attached to interfaces. Typically, these rules are the first security policy applied to packets; they are your first line of defense. You apply access rules to filter out undesired traffic based on service (protocol and port numbers) and source and destination addresses, either permitting the traffic or denying (dropping) it. Each packet that arrives at an interface is examined to decide whether to forward or drop the packet based on criteria you specify. If you define access rules in the out direction, packets are also analyzed before they are allowed to leave an interface.

Thus, you should carefully consider the other types of firewall rules you intend to create when you define access rules. Do not create a blanket denial in an access rule for traffic that you actually want to inspect. On the other hand, if you know that you will never let a service from or to a specific host or network, use an access rule to reject the traffic.

Keep in mind that access rules are ordered. That is, when the device compares a packet against the rules, it searches from top to bottom and applies the policy for the first rule that matches it, and ignores all subsequent rules (even if a later rule is a better match). Thus, you should place precise rules above more general rules to ensure those rules are not ignored. To help you identify cases where IPv4 rules will never be matched, and to identify redundant rules, you can use the analysis and policy query tools.

ASA (ADAPTIVE SECURITY ALGORITHM)

There are several types of firewalls, each with varying capabilities to examine network traffic and permit or block specific instances by comparing traffic characteristics to existing policies. Understanding the capabilities of each type of firewall, and designing firewall policies and acquiring firewall technologies that effectively address an organization's needs, are critical to achieving protection for network traffic flows. This document provides an summary of firewall technologies and discusses their security capabilities and relative advantages and disadvantages in detail. It also provides examples of where firewalls can be placed within networks, and the implications of deploying firewalls in particular locations. To improve the effectiveness and security of their firewalls, organizations should put into practice the following recommendations:

Create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic.
A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. Organizations should perform risk analysis to develop a list of the types of traffic needed by the organization and how they have to be secured—including which types of traffic can cross a firewall under what circumstances. Examples of policy requirements contain permitting only necessary Internet Protocol (IP) protocols to pass, appropriate source and destination IP addresses to be used, particular Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to be accessed, and certain Internet Control Message Protocol (ICMP) types and codes to be used. Generally, all inbound and outbound traffic not expressly permitted by the firewall policy should be blocked because such traffic is not needed by the organization. This practice reduces the risk of attack and can also lessen the volume of traffic carried on the organization's networks.

GUIDELINES ON FIREWALLS AND FIREWALL POLICY
Identify all requirements that should be considered when determining which firewall to implement.

There are many considerations that organizations should include in their firewall selection and planning processes. Organizations need to find out which network areas need to be protected, and which types of firewall technologies will be most efficient for the types of traffic that require protection. Several important performance considerations also exist, as well as concerns regarding the integration of the firewall into existing network and security infrastructures.

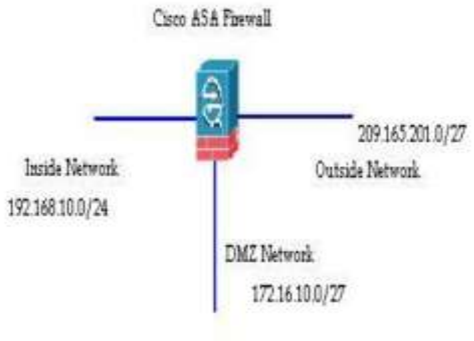
Firewall rule sets should be as exact as possible with regards to the network traffic they control. To create a ruleset involves determining what types of traffic are necessary, including protocols the firewall may need to use for management purposes. The details of creating rulesets vary widely by type of firewall and detailed products, but many firewalls can have their performance improved by optimizing firewall rulesets. For example, some firewalls confirm traffic against rules in a sequential manner until a match is found; for these firewalls, rules that have the highest chance of matching traffic patterns should be placed at the top of the list wherever possible.

Manage firewall architectures, policies, software, and other components throughout the life of the firewall solutions. There are many aspects to firewall management. For example, choosing the type or types of firewalls to install and their positions within the network can considerably affect the security policies that the firewalls can enforce. Policy rules may need to be updated as the organization's requirements change, such as when new applications or hosts are implemented within the network. Firewall component performance also needs to be monitored to make possible potential resource issues to be identified and addressed before components become overwhelmed. Logs and alerts should also be continuously monitored to identify threats—both successful and unsuccessful

BACKGROUND INFORMATION

The interface that receives the packet is called the ingress interface and the interface through which the packet exits is called the egress interface. When referring to the packet flow through any device, it can be easily simplified by looking at the task in terms of these two interfaces [5].
Here is a sample scenario:

Fig.2.3:



Implementation of Firewall

When an inside user (192.168.10.5) attempts to access a web server in the DMZ network (172.16.10.5), the packet flow looks like this:

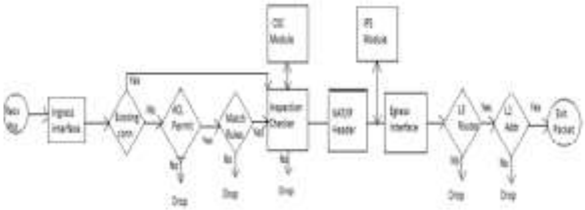
- Source address – 192.168.10.5
- Source port – 22966
- Destination address – 172.16.10.5
- Destination port – 8080
- Ingress interface – Inside
- Egress interface – DMZ
- Protocol used – TCP

By determining the details of the packet flow as described here, it is easy to isolate the issue to this specific connection entry.

CISCO ASA PACKET PROCESS ALGORITHM

Here is a diagram of how the Cisco ASA processes the packet that it receives:

Fig.2.4:



Flow Diagram of ASA

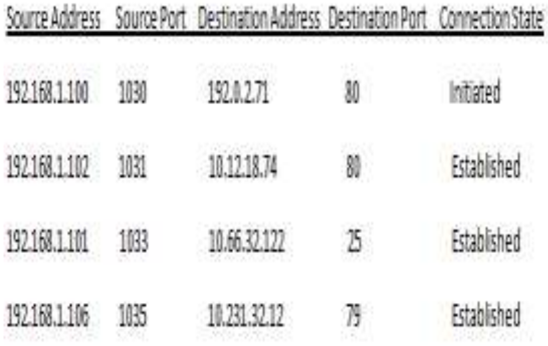
Here are the individual steps in detail [6]:

1. Packet is reached at the ingress interface.
2. Once the packet reaches the internal buffer of the interface, the input counter of the interface is incremented by one.
3. Cisco ASA will first confirm if this is an existing connection by looking at its internal connection table details. If the packet flow matches an existing connection, then the access−control list (ACL) check is bypassed, and the packet is moved forward.
   If packet flow does not match an existing connection, then TCP state is verified. If it is a SYN packet or UDP packet, then the connection counter is incremented by one and the packet is sent for an ACL check. If it is not a SYN packet, the packet is dropped and the event is logged.
4. The packet is processed as per the interface ACLs. It is verified in sequential order of the ACL entries and if it matches any of the ACL entries, it moves forward. Otherwise, the packet is dropped and the information is logged. The ACL hit count will be incremented by one when the packet matches the ACL entry.
5. The packet is verified for the translation rules. If a packet passes through this check, then a connection entry is created for this flow, and the packet moves forward. Otherwise, the packet is dropped and the information is logged.
6. The packet is subjected to an Inspection Check. This inspection verifies whether or not this specific packet flow is in compliance with the protocol. Cisco ASA has a built−in inspection engine that inspects each connection as per its pre−defined set of application−level functionalities. If it passed the inspection, it is moved forward. Otherwise, the packet is dropped and the information is logged.
   Additional Security−Checks will be implemented if a CSC module is involved.
7. The IP header information is translated as per the NAT/PAT rule and checksums are updated accordingly. The packet is forwarded to AIP−SSM for IPS related security checks, when the AIP module is involved.
8. The packet is forwarded to the egress interface based on the translation rules. If no egress interface is specified in the translation rule, then the destination interface is decided based on global route lookup.
9. On the egress interface, the interface route lookup is performed. Remember, the egress interface is determined by the translation rule that will take the priority.
10. Once a Layer 3 route has been found and the next hop identified, Layer 2 resolution is performed. Layer 2 rewrite of MAC header happens at this stage.
11. The packet is transmitted on wire, and Interface counters increment on the egress interface [8].
    The above steps are basic steps used in ASA whenever used. Proper functioning of these steps should be done for better quality of firewall working.

PACKET FILTERING

The most essential feature of a firewall is the packet filter. Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.

Table 2.1: State Table Example



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

CONCLUSION

Firewalls are one key factor in network performance. It is a critical component in the defense mechanism of every network connected to the internet.Access Control List(ACL) are filters that allow you to control which routing updates or packets are permitted or denied in or out of a network.Adaptive Security Algorithm(ASA) is heart of Cisco Firewall series.It is more sclable than application level proxy firewall.

REFERENCES

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

[2] Basic concepts of firewall: [2] CISCO information at www.firewall.cx

[3] Cisco ASA Series Firewall CLI Configuration Guide: [3] Software Version 9.1 Cisco Systems, Inc September 18, 2013.

[4] Introduction to PIX/ASA Firewalls v1.10: [4] by Aaron Balchunas, 2007.

[5] Export Compliance Guide: [5] 2007 for Cisco ASA 5500 Series Adaptive Security Appliances.

[6] IPSEC Site-to-Site VPNs on a PIX/ASA v1.21: [7] – Aaron Balchunas, at http://www.routeralley.com.

[7] Understanding the Basic Configuration of the Adaptive Security Appliance (ASA): [7] Andy Fox, Global Knowledge Instructor, 2009

[8] Off-Path TCP Sequence Number Inference Attack Reduce Security: [8] by Zhiyun Qian, Z. Morley Mao 2012 IEEE Symposium on Security and Privacy.

[9] Cisco's PIX Firewall Series and Stateful Firewall Security: [9] White paper-2009.

[10] Renu"ASA FIREWALL DEVICE" in National Conference on Interdisciplinary Research in Science & Technology (NCIRST-2015) at Lingaya's GVKS Inst. Faridabad

[11] Cisco ASA 5510 Firewall Edition Bundle (ASA5510-K8): [10] LASYSTEMS - Brusselsesteenweg 208 - 1730– Belgium 2013

[12] Network Security and Information Assurance : [11] by R.N.Smith, IEEE Phoenix Section Computer Society Chapter Feb 27, 2010

[13] Network Firewalls: [12] Steven M. Bellovin and William R. Cheswick April 30, 2009 IEEE Xplore.