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. 6, June 2014, pg.279 – 285

RESEARCH ARTICLE

FIRE-ROUTER: A NEW SECURE INTER-NETWORKING DEVICE

Er. Shikha Pandit[1], Er. Pritam Kumar[2], Er. Deepak Malik[3]

[1]Assistant Professor, Department of Computer Science Engineering, AITM, PALWAL, INDIA
[2]M.Tech Scholar, Department of Computer Science Engineering, AITM, PALWAL, INDIA
[3]M.Tech Scholar, Department of Computer Science Engineering, AITM, PALWAL, INDIA

[1] shikhapandit3@gmail.com; [2] parashar.pritam@gmail.com; [3] engr.deepakmalik@gmail.com

Abstract: As networking is the backbone of computer industry. With the growing need of development and expansion, every industry nowadays depends on networking. Networking includes special devices for specific task like router for path selection, switches for better connectivity, and firewalls for better security. With the increasing spoofing and snooping threats the need of security is increasing day by day. Thus, better security implementation with minimum cost has become the bottle neck for engineers to deal with. In this paper we discuss working of some important networking devices and propose a new device to deal with the above problem discussed.

Keywords: Router; Firewall; Security; Routing Protocols; Access Control List (ACL)

1. INTRODUCTION

1.1 **Router:** It is a inter network connecting device with basic task is to forward packet through the network with minimum cost. The minimum cost path used by router to forward packet is termed as the Optimal Path. There are multiple types of packets size used within a router like IPv4, IPv6, etc. These are termed as Routed Protocol with the primary aim is to find minimum cost path within network. Routing Protocols like RIP, OSPF, BGP, etc. follow this Optimal Path calculated by Routed Protocol. Router only forwards that packet(s) through that Optimal Path.

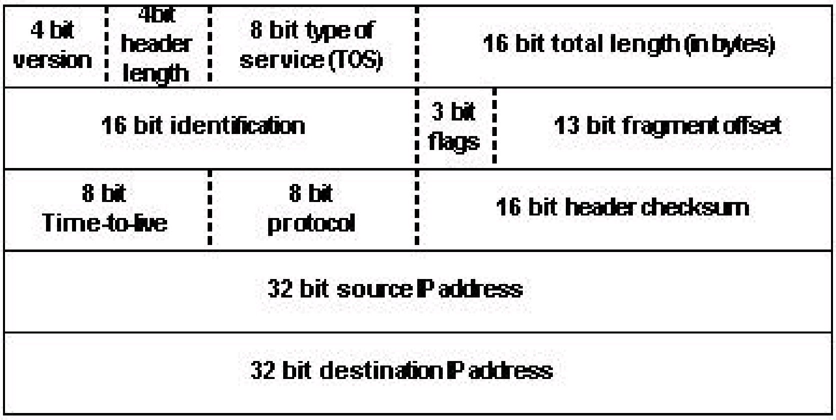
1.2 **Firewall:** It is security device used to provide secure environment over a network. It basic task is to provide safe and secure environment for working. If any unauthorized person or packet comes with a request to access the network, then it simply discards that request. There are policies configured on it based on which the firewall works and checks which are valid request and which should be block.

2. ROUTER

A router's primary task is simple: to route packets from one network to another network based on a set of rules which it is assigned. However this task gets a lot more complicated when the router is asked to route Internet traffic because of the massive number of networks on the Internet. It is also more complicated because of the increasing speed at which these networks are working at. And more recently routers are being asked to do an increasingly large number of additional tasks including resource reservation and multimedia Trans coding.

As stated, a routers task is to route packets from one network to another, however if the focus is IP routing then it is clear 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 contains a number of fields to aid routing, including a source address and a destination address, as well as other fields to aid Quality of Service (TOS field) and error correction (checksum).



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

Figure 1: An IP Version 4 packet.

A router performs the action of routing by utilising a routing table, which specifies where IP packets should be sent based on by looking at the destination address in the IP packet header. A routing table will indicate which network adapter would be used to forward the packet and hence which network the packet should be sent to. IP routers can also be more specific when routing traffic, for example it could route traffic from one source through a faster connection than traffic from another source because of a service-level-agreement.

There are different types of routers ranging from a router which attaches a single network to the Internet (figure 2), a router which connects two sections of the Internet (figure 3) and a router which routes traffic in the core of the Internet. Thus different requirements are placed on a router depending on its location on the global network.

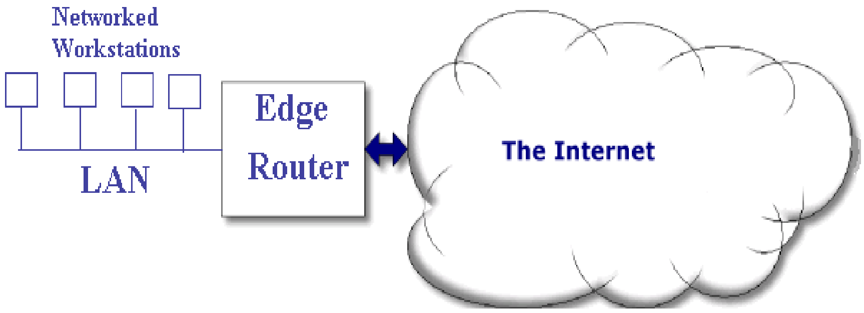


Figure 2: A router connecting a LAN to the Internet

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

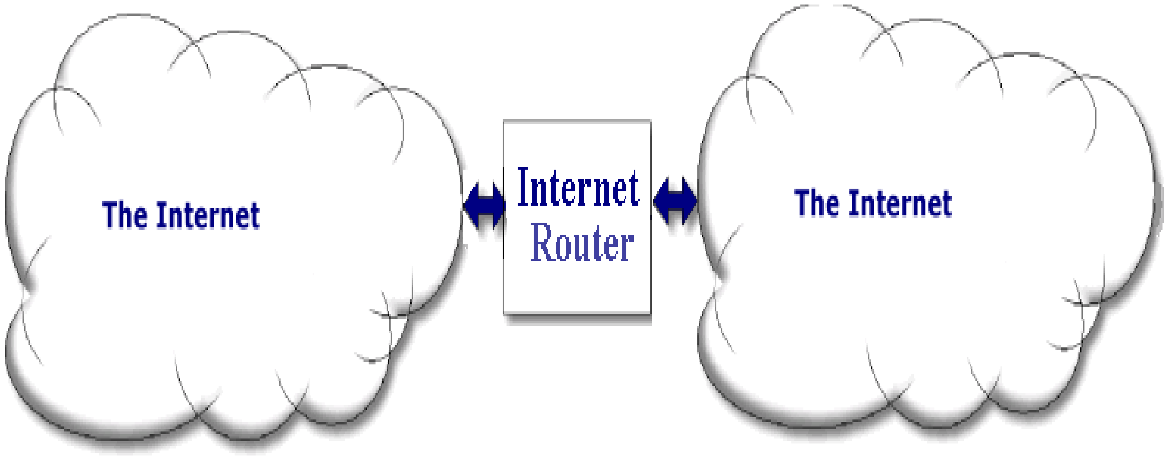


Figure 3: Router connecting two sections of the Internet

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.

3. FIREWALL

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but it could not recognize 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 often include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect mobile devices that are placed directly onto external networks.

Threats have gradually 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. While extremely powerful and versatile, ASA is less complex and more robust than packet filtering implementations. ASA provides performance and scalability advantages over application-level proxy firewalls [2].

PIX/ASA Security-Levels

Cisco security appliances protect **trusted** zones from **untrusted** zones.

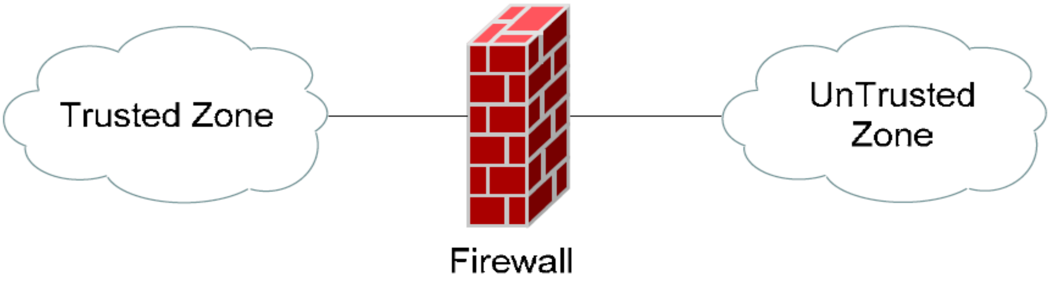


Figure 4: Basic Working of Firewall

Like most firewalls, a Cisco PIX/ASA will **permit** 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 permitted** [3].

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

A firewall is not limited 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.

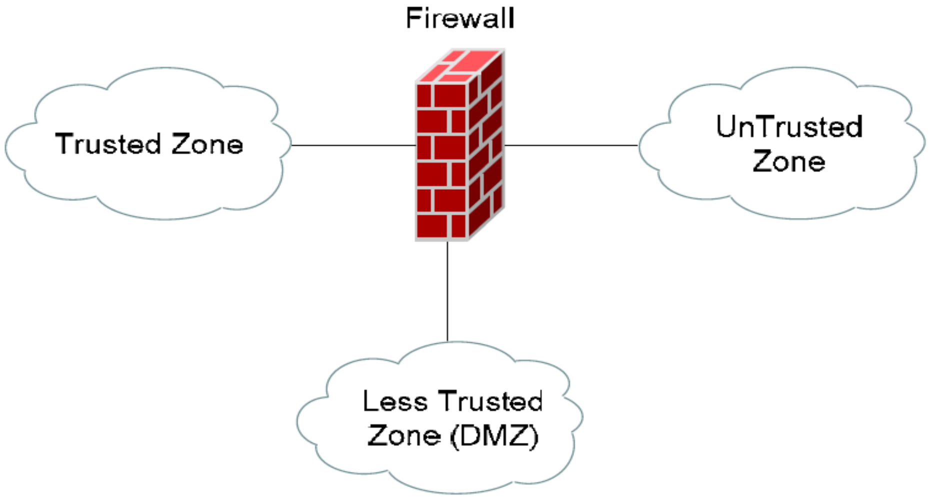


Figure 5: Different Zones in Firewall implementation

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

PIX/ASA Failover

Both PIX and ASA firewalls also support **failover**, providing a redundant environment for high-availability. This failover feature is similar to **HSRP (**Hot Standby Routing Protocol**).** One firewall remains in an **"active"** state, performing all normal firewall functions. Another firewall remains in a **"standby"** state, ready to take over if the primary firewall fails. Only specific PIX/ASA models support failover.

4. OUR PROPOSAL : FIRE-ROUTER

As router basic feature is to provide best path only, it also has some security features inside it. The security level present inside router doesn't provide much security as like firewall. The security algorithm and technique used inside router are not much helpful and can be easily breach. Whereas the security inside firewall is quite high as it uses dedicated security algorithms, one of which is Adaptive Security Algorithm (ASA) which is CISCO propriety. This ASA algorithm is not a single algorithm but a collection of many algorithms, each algorithm dedicated for a particular task. Even if a small portion of these algorithms is combined with router's security algorithm, the router security level is increased by significant value. As ASA firewall does Stateful inspection for filtering traffic using its security algorithms (one or many), the resulting router formed thus have a better security feature.

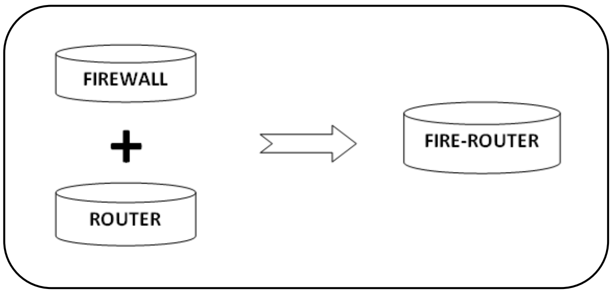


Figure 6: Diagram of combination Fire-Router

Although combining the security feature of firewall over router and forming a single device may result into a slightly lower performance device; as the computing overhead of the device is increased. But the performance can be increased by taking a higher configuration router. Taking a higher configuration router results in slightly more cost but the overall cost is decreased. Thus, doing this it helps in saving a cost of hardware device and a single device instead of two i.e. new router obtained has better security features as like firewall.

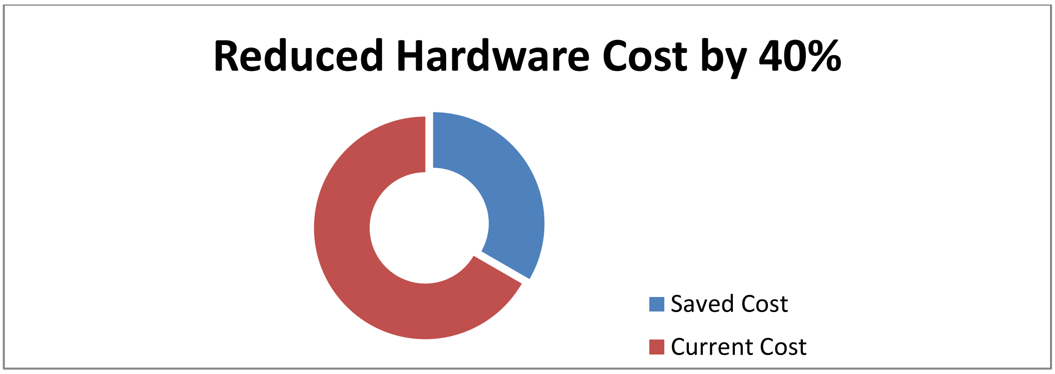


Figure 7: Effective Cost Diagram

Now the device first checks whether the packet is valid i.e. genuine or not. If the packet is genuine (valid) by checking in its firewall phase, then decide where to forward this packet via best path in router phase. Checking and calculating best path on the same device not only helps in saving the hardware cost but also in better filtering. Security is enhanced as whether the packet filtered and allowed to pass does really exist inside the network or not.

This can be represented as a flowchart shown in figure 8.

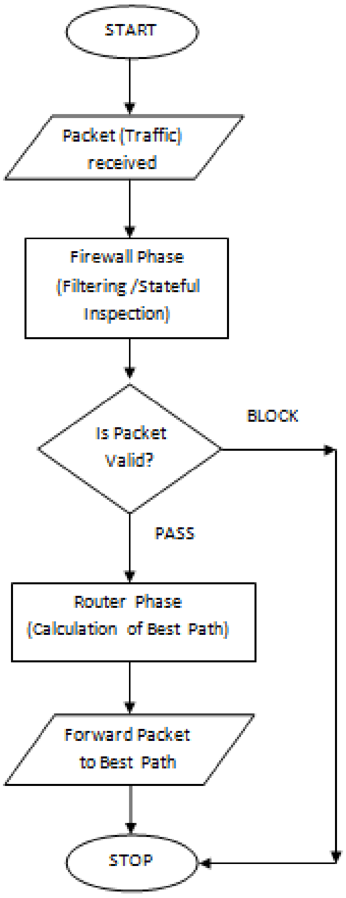

START
Packet (Traffic) received
Firewall Phase (Filtering /Stateful Inspection)
Is Packet Valid?
BLOCK
PASS
Router Phase (Calculation of Best Path)
Forward Packet to Best Path
STOP

Figure 8: Flow chart of working Algorithm of Fire-Router

Thus, a single device works like firewall for checking and finding best path to forward that packet like router.

Advantages:

1. Better Security inside router, best for small organizations which only uses router for security and not uses Firewall due to cost constraint.
2. Hardware cost is saved i.e. single hardware device instead of two different devices.
3. Single device, thus easy to manage instead of managing two different devices.
4. Easy implementation and installation as router security feature is only enhanced not change completely.
5. For big organisations, where security is a great concern, providing almost double security checking if combined with currently used scenario i.e. first by dedicated firewall and then again by router itself.

5. CONCLUSION AND FUTURE WORK

Thus the device formed by combining the features of firewall and router not only provide better security but also results in lower hardware cost. As security and cost are two major challenges to deal with, continuous work is to be done for maximising the security level with minimum cost. Due to overhead of computing the firewall as well as router working itself, it may possible that router doesn't generate log file sometimes. Work can also be done regarding for generating log files also.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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