Paper on Types of Firewall and Design Principles

Vidthya Redya[1], Dr. K. Shahu Chatrapati[2], Dr. V. N. Kamalesh[3]

[1]Research Scholar, Computer Science and Engineering, JNTU Hyderabad, India

[2]Senior Asst. Professor, JNTU Hyderabad, AP, India

[3]Professor and Special Officer Regional Office, Mysore Regional centre, Visvesvaraya Technological University

Abstract: ***This paper deals with Firewall, its characteristics, its capabilities, its Limitations, Types of Firewalls, Firewall Design principles. What is demilitarized zone (DMZ) and an example of a Firewall with DMZ.***

Keywords: Firewall, Packet Filtering, Gate way, Proxies, Policy, Demilitarized Zone (DMZ)

1. Firewall

A firewall is a dedicated hardware, or software or a combination of both, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. A firewall is a device or devices that control traffic between different areas of The Systems network. In a more robust design The System typically see two or three firewall devices, as well as many other security components to protect company resources.

2. Firewall Characteristics

2.1. Firewall Capabilities

A firewall defines a single choke point that keeps unauthorized users out the protected network.

- A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several Internet functions that are not security related.
- A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private network.

2.2. Firewall Limitations

The firewall can not protect against attacks that bypass the firewall.

- The firewall does not protect against internal threats.
- The firewall can not protect against the transfer of virus-infected programs or files.

2.3 Design Goals

All traffic from inside to outside, and vice verse, must pass through the firewall.

- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration. This implies the use of a trusted system with a secure operating system

2.4 Methods of Control in Firewall

- User control:- Only authorized users are having access to the other side of the firewall
- Access control:-The access over the firewall is restricted to certain services. A service is characterized e.g. by IP address and port number.
- Behavior control:-For an application, the allowed usage scenarios are known. E.g. filters for e-mail attachments (virus removing)
- Direction control:-Different rules for traffic into the Intranet and outgoing traffic to the Internet can be defined

3. Types of Firewall

3.1 Packet Filtering

Packet filtering is the simplest packet screening method. A *packet filtering firewall* does exactly what its name implies -- it filters packets. The most common implementation is on a router or dual-homed gateway. The packet filtering process is accomplished in the following manner. As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters. An allow or deny decision is made based on the results of the comparison. Each packet is examined individually without regard to other packets that are part of the same connection.

3.2. Application Gateways / Proxies

An application gateway / proxy is considered by many to be the most complex packet screening method. This type of firewall is usually implemented on a secure host system configured with two network interfaces. The application gateway/proxy acts as an intermediary between the two endpoints. This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination. Each endpoint can only communicate with the other by going through the gateway/proxy.

3.3 Circuit-level Gateway

Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions. Once a session has been established, it leaves the port open to allow all other packets belonging to that session to pass. The port is closed when the session is terminated. In many respects this method of packet screening resembles application gateways/proxies and adaptive proxies, but circuit-level gateways operate at the transport layer (layer 4) of the OSI model.

3.4 Design Guidelines

The System should follow five basic guidelines when designing a firewall system:

- Develop a security policy.
- Create a simple design solution.
- Use devices as they were intended.
- Implement a layered defense to provide extra protection.
- Consider solutions to internal threats that should be included in The Systems design.

The following subsections cover these five key design points.

3.4.1 Developing a Security Policy

One of the first things The System do when designing a firewall system is to create a security policy. The policy should define acceptable and unacceptable behavior, should state restrictions to resources, and should adhere to the company's business plan and policies. Without a security policy, it is practically impossible to develop a security solution that will meet The Systems company's needs.

The key to a good design is basing it on a security policy. Basically, a policy defines who is allowed to access resources, what they are allowed to do with resources, how resources should be protected and what actions are taken when a security issue occurs. Without a security policy, it is impossible to design a firewall system that will protect The Systems assets. Designing a security policy is address the following items:

- The resources that require access from internal and external users
- The vulnerabilities associated with these resources
- The methods and solutions that can be used to protect these resources
- A cost-benefit analysis that compares the different methods and solutions

3.4.2 Designing Simple Solutions

A firewall system design should be kept simple and should follow The Systems security policy. The simpler the design is, the easier it will be to implement it, maintain it, test and troubleshoot it, and adapt it to new changes.

3.4.3 Using Devices Correctly

Network devices have functional purposes; they were built with a specific purpose in mind. For example, a Layer 2 switch is used to break up a collision or bandwidth domain, and it also uses VLANs to break up broadcast domains: It is typically not a good device to use to filter traffic because the filtering is done by creating filtering rules based on MAC addresses. The problem with this approach is that MAC addresses tend to change quite a bit: NICs fail, PCs and servers are upgraded, devices are moved to different locations in the network, and so on. Filtering is done best when logical addressing is deployed.

Using the wrong product to solve a security problem can open The System to all kinds of security threats.

3.4.4 Creating a Layered Defense

A security design typically uses a layered defense approach. In other words, The System usually do not want one layer of defense to protect network. If this one layer is compromised, The Systems entire network will be exposed.

Instead, The System should use a multilayer defense in The Systems firewall system design. With multiple layers, if one layer is compromised, The System still have other layers behind it protecting The System.

3.4.5 Dealing with Internal Threats

Too often, security personnel are concerned about protecting a company's resources and assets from outside threats. Remember that it is much easier to attack The Systems assets from within; plus, most threats and attacks (60 to 70 percent) are internal attacks. Therefore, a good firewall system not only protects The System from external threats, but also allows The System to minimize internal threats.

4. DMZ

Most firewall systems use a demilitarized zone (DMZ) to protect resources and assets. A DMZ is a segment or segments that have a higher security level than that of external segments, but a lower security level than that of internal segments. DMZs are used to grant external users access to public and e-commerce resources such as web, DNS, and e-mail servers without exposing The Systems internal network. A firewall is used to provide the security-level segmentation among the external, DMZ, and internal resources. Basically, the DMZ acts as a buffer between different areas in a network.

4.1 DMZ Rules and Traffic Flow

To help enforce security more easily, each area in the firewall system is assigned a security level. This could be something as simple as low, medium, and high, or something more sophisticated, such as a number between 1 and 100, where 1 is the lowest security level and 100 is the highest. Typically, traffic from a more secure (higher) layer is permitted to a lower layer, but not vice versa.For traffic to go from a lower layer to a higher layer, it must be permitted explicitly: In other words, The System must set up a filtering rule that allows this traffic to go from a lower level to a higher level. If two areas have the same security level, such as medium, the traffic between the two areas is either permitted or denied, based on the process that the product uses.

The network shown in Figure 2 illustrates how security levels work.

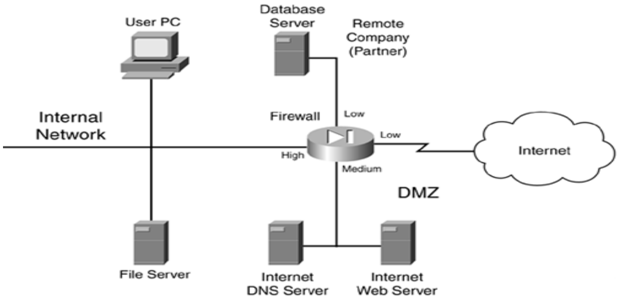

Figure 2: Security Level Example

In this example, a firewall is used to separate different areas of a network. The firewall has the following four interfaces:

- A connection to the Internet, assigned a low security level
- A connection to the DMZ, where public servers are located, assigned a medium security level
- A connection to a remote company that is working on a project for them, assigned a low security level
- A connection to the internal network, assigned a high security level

This company has assigned the following rules:

- High- to low-level access: permit
- Low- to high-level access: deny
- Same-level access: deny

Given these rules, the following traffic is allowed automatically to travel through the firewall:

- Internal devices to the DMZ, the remote company, and the Internet
- DMZ devices to the remote company and the Internet

Any other type of traffic flow is restricted. One advantage of this design is that, because the remote company and the Internet are assigned the same level, traffic from the Internet cannot reach the remote company and the remote company cannot use The Systems Internet access for free.Another advantage of security levels is that they create a layered approach to security. For example, for either hackers on the Internet or the remote company to access internal resources in Figure 2, they probably first must hack into The Systems DMZ and then use this as a stepping stone to hack into The Systems internal network. Using this layered approach, The System make the hacker's job much more difficult and The Systems network much more secure.

4.2. DMZ Types

DMZs come in many types of designs. The System can have a single DMZ, multiple DMZs, DMZs that separate the public network from The Systems internal network, and DMZs that separate traffic between internal networks. The following sections show some of these implementations.

4.3.1 Single DMZ:-Single DMZs come in two types:

- Single segment
- Service-leg segment

Figure 3 shows an example of a single DMZ with a single segment. In this example, there are two firewalls: a perimeter firewall and a main firewall, with the DMZ segment between the two. One disadvantage of this design is that two firewalls are needed: one to protect the DMZ from the Internet and one to protect the internal network from the DMZ and the Internet.

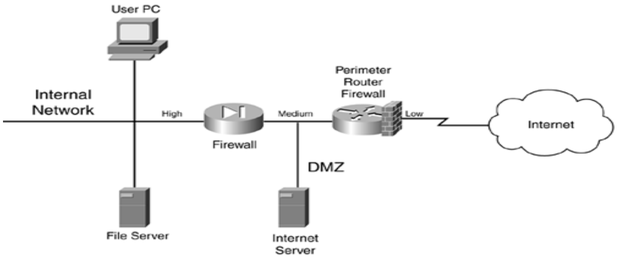

Figure 3: Single DMZ with a Single Segment

Most firewall designs use a service-leg DMZ, which is shown in Figure 4. In this example, a router is used to connect to the Internet. The design in Figure 4 has two advantages over the single-segment DMZ shown in Figure 3:

- The firewall sometimes can be connected directly to the Internet, removing the extra cost of the perimeter router.
- All security-level polices can be defined on one device.

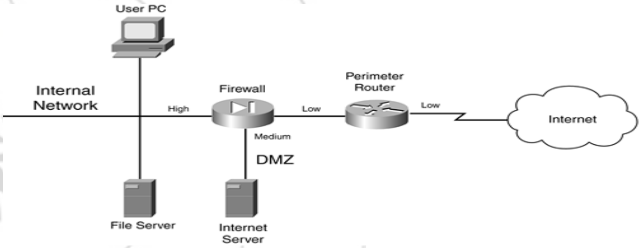

Figure 4: Single DMZ with a Service-Leg Segment

The main problem with this approach, however, is that, because a single firewall is handling all security policies, a successful DoS attack can degrade the firewall's performance. In the best case, only The Systems throughput is affected; in the worst case, the firewall might crash. With a single-segment DMZ, because the policies are spread between the two firewalls, there is less likelihood of an overload occurring. This is especially true for traffic between the DMZ and the internal network. If a hacker is attacking a web server on the DMZ, the perimeter firewall takes the brunt of this attack, which allows the internal firewall to handle DMZ/internal traffic without affect.

4.3.2 Multiple DMZs

A firewall system can be used to separate multiple areas of The Systems network, including multiple DMZs. Figure 5 shows an example of a network with multiple DMZs. In this example, a firewall is used to break up a network into four areas: the internal network, a DMZ for Company A's server, a DMZ for Company B's server, and the Internet. In this example, the internal network is assigned a high security level, both company servers are assigned a medium security level, and the Internet is assigned a low security level. Assume that high-to-low access is allowed by default but that same-to-same is denied. In this example, the internal network can access any resource, and each company server can access the Internet, but not the other company's server. The System would need to set up security rules to allow

Internet access into the two servers on the medium-security segments, as well as communication between the two servers, if this is desired.

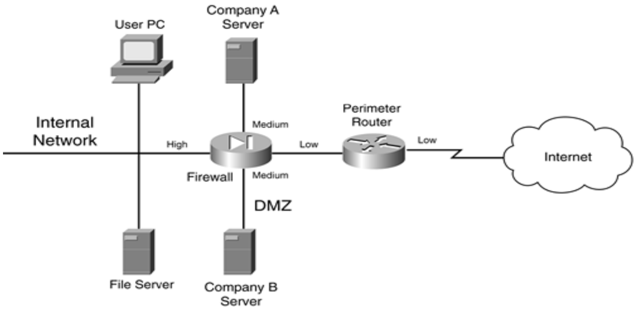

Figure 5: Multiple DMZ Example

Actually, this type of design is very common in ISPs. Most ISPs offer web-hosting services and use this type of design to separate each company's server(s) from the others.

4.4 Internal DMZ

Another type of DMZ is an internal one. An internal DMZ enables The System to provide separation between different parts of The Systems internal network. Most people assume that a DMZ is used to separate The Systems internal services from those that The System offer to the public, such as a web or e-commerce server; however, they can be used effectively to protect resources in one part of The Systems company from another.

Figure 6 illustrates the usefulness of an internal DMZ. In this example, a firewall is used to separate the internal network (in the right of the figure) from the engineering and accounting users. In this example, both engineering and accounting are assigned a medium level of security. Assume that same security level to the same security level is denied by default; in other words, if two interfaces have the same security level, they cannot, by default, communicate with each other. With this configuration, accounting and engineering are allowed to send traffic to the internal network but not themselves. Internal users cannot access either of these two groups because the internal users are on a lower security level interface. To allow these last types of access, The System would need to configure security rules on The Systems firewall to allow same-to-same or low-to-medium levels of access.

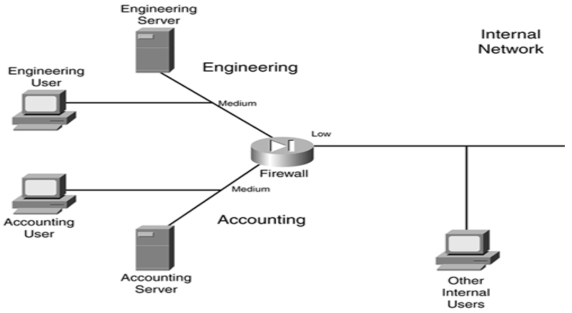

Figure 6: Internal DMZ Example

As The System can see in this example, The System easily can protect important resources in The Systems network from other internal users. Internal DMZs enable The System to accomplish the following:

- Control traffic between areas
- Localize security problems

5. Components

Now that The System have a basic understanding of firewall system design practices, this section takes a closer look at the components that make up a firewall system. A good firewall system typically contains the following components:

- Perimeter router
- Firewall
- VPN
- IDS

5.1 Perimeter Router Component

The main purpose of the perimeter router is to provide a connection to a public network, such as the Internet, or a different company. It is used to convert data-link layer media types from a LAN to either a WAN or MAN medium. The functions of the perimeter router can include the following:

- Routing through static routes or a dynamic routing protocol
- Filtering through either packet filtering or state full filtering
- Terminating VPN connections
- Providing address translation

5.2. Firewall Component

The main purpose of the firewall component is to separate The Systems network into different security levels and control traffic between these levels. Typically, The System find a firewall component near the perimeter of the network, protecting The System from external threats as well as providing controlled access to a public DMZ segment. However, The System also might find firewall components inside The Systems internal network, separating critical resources so that they are better protected.

The functions of the firewall can include the following:

- State full filtering
- User authentication of connection with CTPs
- Connection filtering with CGFs
- Address translation

5.2 VPN Component

The main purpose of the VPN component is to provide a protected connection between two devices, two networks, or a device and a network. This protection can include encryption, authentication, and packet-integrity checking, preventing eavesdrop attacks from prying eyes. VPNs are a cost-effective, remote-access solution because they enable The System to use a public network, in a secure manner, to connect two private networks. This is cheaper than purchasing private WAN links to provide connectivity.

The functions of the VPN component can include the following:

- Protecting (encrypting) traffic between LAN sites and remote access users

- Assigning addressing information to remote access clients
- Using simple packet filters to restrict traffic flow

5.3 IDS Component

The main purpose of the IDS component is to detect, and possibly prevent, reconnaissance, DoS, and unauthorized access attacks. To understand the different kinds of network attacks that The Systems company is facing, The System need an intimate understanding of the different kinds of traffic flowing through The Systems network, as well as the intentions of this traffic.

Most traffic entering or traversing The Systems network has a valid purpose: to access web pages with HTTP, resolve names to addresses with DNS, send e-mail with SMTP, and so on. However, a small percentage of traffic has malicious intentions. In these cases, a hacker might be executing a reconnaissance attack to determine what kinds of resources are available in The Systems network, and then might execute a DoS attack to affect their level of service or carry out an unauthorized attack to open a back door into The Systems network. An IDS solution should be capable of detecting these kinds of threats.
IDS components fall under one of three categories:

- Anomaly-based
- Signature-based
- Hybrid-based

5.3.1 Anomaly-based solutions

Anomaly-based solutions capture traffic over a period of time and use this as a reference for what is valid. These systems then compare new traffic to what is considered to be "normal" and look for anomalies. One disadvantage of anomaly-based solutions is that they tend to generate a lot of false positives. This is because traffic patterns change; if The System do not stay up-to-date on a database of normal traffic flows, false positives are bound to happen.

5.3.2 Signature-based solutions

Signature-based solutions compare traffic to signatures to look for attacks. A signature is a static definition of things to examine in packet or packets; these can include header information as well as data. Signature-based solutions have a lot less false positive alarms. However, their main disadvantage is that they cannot detect new kinds of attacks unless The System keep The Systems signature database updated. This is where an anomaly-based solution shines: It can detect new kinds of attacks without a software upgrade.

In many of today's IDS solutions, a hybrid approach is used, with both signatures and anomaly detection used in tandem to provide the best possible intrusion detection. IDS solutions come in two flavors:

- Network-based IDS
- Host-based IDS

A network-based IDS solution is a protocol analyzer on steroids: It plugs into The Systems network at key points and monitors traffic. Network-based systems can be used to detect attacks against many different devices. A good network-based IDS solution should have the capability, when an attack is detected, to access (log into) The Systems firewall component and configure a temporary filter to block the malicious traffic. This is an excellent tool for shutting down the hacker's access even into public areas of The Systems network.

A host-based IDS solution is IDS software running on a host, such as a PC or file server, that detects attacks only against that host. This can provide an additional measure of protection for critical servers that are not necessarily protected by a firewall or IDS component. One downside of host-based solutions is that they require extra processing power to examine packet information sent to the host.

The IDS component should play a key role in The Systems firewall system. The functions of the IDS component can include these:

- Monitoring traffic for statistical purposes
- Examining traffic for network threats
- Reporting network threats and possibly taking action to prevent the threats

6. Component Placement

This section talks about where these components are placed in a network design. As The System will see, The System can design a network in many different ways, each with advantages and disadvantages.

6.1 Simple Firewall System Design

To help understand where components are placed in a firewall system, I use two examples. The first example, shown in Figure 2-28, is the simpler of the two designs.

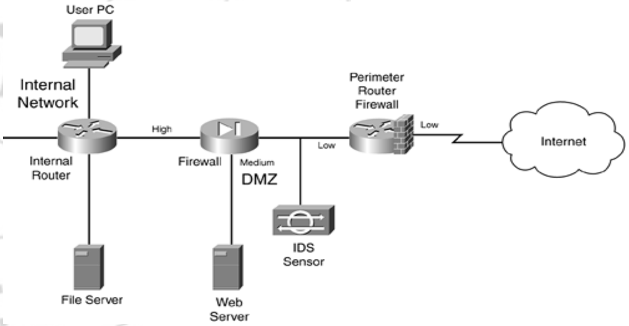

Figure 7: Simple Firewall System Design

In this example, a perimeter router with basic packet filtering screens traffic as it enters the network. A standalone IDS device is used to detect attacks that the perimeter packet-filtering firewall did not filter.

The traffic then is processed by a stateful firewall. The stateful firewall has set up three security levels: low for the Internet side, medium for the DMZ, and high for the internal network. A security rule was added on the stateful firewall to allow traffic from the Internet to only the web server. All other traffic from a lower security level to a higher one is prohibited; however, higher-to-lower movement is permitted, allowing the web server administrator located on the internal network to log into the DMZ web server to update web pages.

An internal router in this design provides routing to internal segments. If The System need to set up security levels and restrict access to areas of this network, The System can use basic packet-filtering services on the router.

One of the advantages of this design is its simplicity: It has a minimum of three layers of defense: the packet-filtering firewall at the perimeter, the IDS, and the stateful firewall. Optionally, The System can turn the internal router into a packet-filtering firewall.

This design has some disadvantages, however:

- Any attacks directed at the perimeter router/firewall are not seen by the IDS, which might be useful in determining who is trying to hack into the router and how they are trying to do it.
- No IDS exists on the inside the network, so The System cannot easily determine whether internal attacks are occurring.
- The internal router might provide only simple packet filtering, which makes it difficult to implement security levels for internal users. However, this can be remedied by using a different type of firewall, such as a stateful firewall or an AGF.

6.2 Enhanced Firewall System Design

The second firewall system design is shown in Figure 8. As The System can see, it has more components and rectifies some of the security deficiencies in the simple firewall system design. I examine the perimeter router component first. As in the last example, the perimeter router/packet-filtering firewall is performing basic filtering of traffic as it comes into the Internet. Nothing is different in this example except for what the bottom-right IDS device is doing: monitoring both the external Internet segment and the segment between the packet-filtering perimeter router and the stateful firewall. This allows the IDS to see what attacks are directed at the router, as well as what attacks are getting through the router.

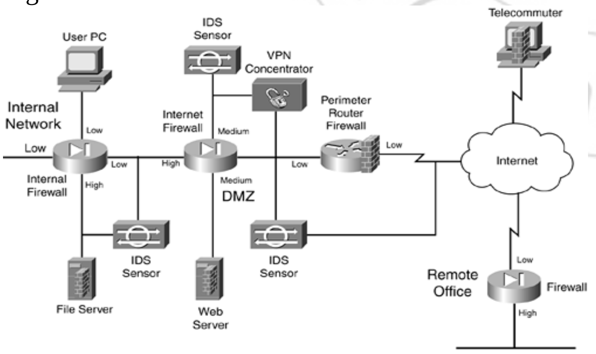

Figure 8: Enhanced Firewall System Design

Next is the VPN concentrator. It is used to provide encrypted connections for the remote office connection (from the remote office firewall to the concentrator), as well as to terminate remote-access user connections from telecommuters and SOHO users. Notice that an IDS sensor behind the VPN concentrator is examining the unencrypted traffic. This is placed here just in case one of the remote access users or the remote office becomes compromised: The IDS can view the unencrypted traffic to detect network threats, which the IDS device connected between the perimeter router and the Internet firewall cannot because the traffic is encrypted at this point.

In addition, when the unencrypted traffic is sent to the Internet firewall from the external users, it is assigned a medium level of security, which means that it can be routed back to the Internet without any filtering and to the DMZ (assuming that same-to-same level of access is allowed). To access an internal resource, the internal firewall needs a security rule configured.

The Internet firewall provides a second layer of filtering after it passes the perimeter router/firewall. It handles traffic from the VPN concentrator, the Internet, and the DMZ. Notice that the server in the DMZ has a host-based firewall installed, adding protection to it.

The bottom-left IDS is monitoring the Internet Firewall-to-Internal Firewall segment as well as the internal high-security segment, detecting attacks that get through the respective firewalls. Plus, the host-based firewall software is installed on the internal file server.

Inside the network, an internal stateful firewall is used to provide security levels. In this example, the file-server connection has a high security level, and all of the other connections are set to low. This means that rules must be configured on the internal firewall to allow any type of traffic to reach the internal file server.

In all, this is a good security design. It uses IDS components at key places to monitor critical traffic, and it has a layered defense approach, with a packet-filtering firewall and two stateful firewalls. Plus, host-based firewall software is used on critical servers. A VPN also is used to protect traffic across the Internet.

This design also has some disadvantages, however:

- It costs a lot more than the simple design.
- The IDS systems are monitoring a lot of traffic and are generating a lot of logging information. If someone does not take the time to examine the IDS logs carefully, attacks could slip through the cracks.
- Much more configuration and management need to be done, to ensure that the correct security policies are implemented on the firewalls: the perimeter packet-filtering firewall, the two stateful firewalls, and the two host-based software firewalls. In this scenario, The System definitely want to look at management software that enables The System to define all The Systems security policies from one desktop, and then have these polices converted into the configuration commands and downloaded and executed on The Systems firewall devices.

Design Considerations:-Here are some important points to remember when placing components in a firewall system:

- Use a packet-filtering firewall for the boundary router, to provide an extra level of protection. If The System are really concerned about security, use a stateful firewall for this component.
- All servers that have publicly available resources should be placed in a DMZ. Servers that handle critical

processes or financial transactions should have host-based firewall software installed on them. In addition, all unnecessary services on these servers should be disabled.

- For DMZ servers with sensitive information, consider using a multiple DMZ design. This is especially true if The System have a web server and a database server that it interfaces with. Put the web server on a lower security level than the database server.
- If external users or remote sites that traverse a public network want to access internal resources, require a VPN. This ensures that any sensitive data is protected.
- VPN connections, as well as remote-access connections through private networks, should be terminated on their own DMZ on the Internet firewall. An IDS system should be used to examine this traffic after it is decrypted. This also allows the traffic to go right back out to the Internet, but because it is going through the firewall, The System have more control over what is allowed.
- For critical internal resources, use an IDS component to monitor key segments to detect network threats. The System can add extra security by segmenting The Systems internal network into different security levels. This can compartmentalize The Systems network and restrict access from the general population of users to areas that they have no business being in, such as accounting and R&D.
- For e-mail, The System should have a public e-mail server in the DMZ that accepts all incoming and outgoing mail services. I highly recommend that The System have antivirus, spam, and host-based firewall software running on this server. I also recommend that The System use a limited form of a CGF that can examine mail content and make filtering decisions on it, to catch networking threats that the antivirus software cannot deal with. After e-mail is processed, it then can be forwarded to an internal server. I also recommend that all outgoing e-mail be forwarded through the DMZ e-mail server and have the same processes performed on it (remember that someone on the inside might try to use The Systems e-mail server for malicious purposes).

I could list probably a dozen or so more items, but these are the more important ones. As The System can see from this list, The System have The Systems work cut out for The System.

6.3 Firewall Implementation

Now that The System have chosen The Systems components for The Systems firewall system, The System need to set them up and configure The Systems security policies on them. Typically, The System use either a command-line interface (CLI) or a graphical user interface (GUI) to perform the configuration. Cisco products support both methods, but this book focuses on the CLI, which is the most common method used by Cisco administrators.

7. Conclusion

This paper deals with Firewall, its characteristics, its capabilities, its Limitations, Types of Firewalls, Firewall Design principles. What is demilitarized zone (DMZ) and an example of a Firewall with DMZ. The future of this paper is to develop the and implementation of different kinds of firewall and their usage and compare our firewall with available firewall in the market and prepare a comparative graph.

References

[1] Data Communications and Networking, Fourth Edition Titles By Behrouz A. Forouzan McGraw-Hill Forouzan Networking Series

[2] *Computer Networks*, co-authored with David J. Wetherall [14] (1st ed. 1981, 2nd ed. 1994, 3rd ed. 1996, 4th ed. 2002, 5th ed. 2010).

[3] *Bal, H. E.; Steiner, J. G.; Tanenbaum, A. S. (1989). "Programming languages for distributed computing systems". ACM Computing Surveys* ***21*** *(3): 261. doi:10.1145/72551.72552*

[4] Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences ISSN: 1936-2447 (Print) 1936-2455 (Online)

[5] Database System Concepts, Fourth Edition, Silberschatz−Korth−Sudarshan, McGraw−Hill Companies, 2001.

[6] Introduction to *Database. Systems. Database Systems,*8th edition, *c j date.*

[7] *Software Engineering: A practitioner's Approach, 8/e by Roger.S.Pressman* , McGraw-Hill Edition.

[8] *File Organizationfor Database Design by Gio Wiederhold*, McGraw-Hill Edition in 1987

[9] E.S. Al-Shaer and H.H. Hamed. Firewall policy advisor for anomaly discovery and rule editing. 8th International Symposium on Integrated Network Management , pages 17–30, 2003.

[10] Frederic Avolio. Firewalls and Internet security, the second hundred (Internet) years.The Internet Protocol Journal, 2(2):24–32, June 1999. http://www.cisco.com/warp/public /759/ipj_2-2/ ipj_2-2_fis1.html Accessed 2002 Feb 20.

[11] Frederick M. Avolio and Marcus J. Ranum. A network perimeter with secure external access. In Internet Society Symposium on Network and Distributed Systems Security, 3-4 Feb. 1994, San Diego, CA, USA , pages 109–119, Reston, VA, USA, February 1994. Internet Society.http://www.ja.net/CERT/Avolio_and_Ranum/isoc94.ps 2002.

[12] Mary L. Bailey, Burra Gopal, Michael A. Pagels, Larry L. Peterson, and Prasenjit Sarkar. PATHFINDER: A pattern-based packet classifier. In 1st Symposium on Operating Systems Design and Implementation, 14-17 November 1994, Monterey, CA, USA, pages 115–123, Berkeley, CA, November 1994. USENIX Association.

[13] Yair Bartal, Alain J. Mayer, Kobbi Nissim, and Avishai Wool. Firmato: A novel firewall management toolkit. In 1999 IEEE Symposium on Security and Privacy, 9-12 May 1999, Oakland, CA, USA , pages 17–31, Los Alamitos, CA, USA, 1999. IEEE. http://www.wisdom.weizmann.ac.il/˜kobbi/papers/firmato.ps Accessed 2002 Feb 20.

[14] S.M. Bellovin, C. Cohen, J. Havrilla, S. Herman, B. King, J. Lanza, L. Pesante, R. Pethia, S. McAllister, G. Henault, R.T. Goodden, A. P. Peterson, S. Finnegan,

K. Katano, R.M. Smith, and R.A. Lowenthal. Results of the security in ActiveX workshop Pittsburgh, Pennsylvania USA August 22-23, 2000. Technical report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburg, PA 15213, USA, December 2000. ttp://www.cert.org/reports/activeX_report.pdf

[15] Canghong Zhang, Based on nework security firewall technology, Information technology, Chinese new technology new product, 2009.

[16] Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000

[17] Kuang Chu, network security and firewall technology, Chongqing university publishing house,2005

[18] S. Smith, E. Palmer, and S. Weingart, "Using a high-performance, programmable secure coprocessor," in Proc. International Conference on Financial Cryptography, Anguilla, British West Indies, 1998.

[19] P. Liu and S. Jajodia ,"Multi-phase damage confinement in data base systems for intrusion tolerance," in Proc. 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, June 2001.

[20] S. W. Lodin and C. L.Schuba, "Firewalls fend off invasions from the net," IEEE Spectrum, vol. 35, no. 2, 1998.

[21] A. Wool, "A quantitative study of firewall configuration errors," Computer, vol.no. 6,2004.

[22] M. R. Lyu and L. K. Y. Lau, " Firewall security: policies, testing and performance evaluation," in Proc. 2000 International Conference on Computer Systems and Applications.

[23] J. J¨urjens and G . Wimmel, "Specification based testing of firewalls," in Proc. 200 International Andrei Ershov Memorial Conference on Perspectives of System Informatics.

[24] Check Point's Press Release "Check Point Introduces Revolutionary Internet Firewall Product Providing Full Internet Connectivity with Security; Wins 'BEST OF SHOW' Award at Net world Interpol „".