The current firewall technology computer science essay

Technology, Computer

Currently firewall technology as a specialized engineering solution rather than a scientifically based solution. Currently firewall is classified in to three category packet filtering, proxy server, and stateful firewall. This paper is main focus on the various type of firewall available and their pros and cons.

Originally computer network was design for data communication to share the resources. The sharing of resources was bounded between universities. Eventually businesses, corporations, government agencies were begun to use internet. So network become vital part of their institution. Computer networking, however, is not without risks as Howard illustrates in his analysis of over 4000 security incidents on the Internet between 1989 and 1995 [1]. A neutral approach to network protection draws from several other fields, such as physical security, personnel security, operations security, communication security, and social mechanisms. [2] According to definition firewall is " a set of mechanisms that can enforce a network domain security policy on communication traffic entering or leaving a network policy domain" [3]. In simple word firewall is guard point which gives control point of entry or exit from computer or network. It is a first line of defence and it is also a contact point of the network. It is very important to choose and design firewall to guard inside network from outside attack.

Case Study

Figure 1: ABC. Ltd network [6]

Above figure shows our case study network . Consider a case where company ABC. Ltd want to implement a firewall for their campus design.

Company whole network is divided in to three parts, inside network, Demilitarized Zone (DMZ) and outside network. Inside network has ip address 10. 1. 1. 0/24. DMZ is further divided in to two sub section; one is protected DMZ which has ip address 192. 168. 11. 0/24 and dirty DMZ which is dump host whose ip address is 192. 168. 1. 0/24. Dump host is a computer which got nothing important in it. These dump hosts are act as a honey pot which is use to lure attacker so that network security designer know different type of attack and help them to design security policy. DMZ is a zone where company put their services like web services, FTP services etc. Company has remote office which uses secure VPN to connect to the main campus network.

There are different type of firewall technology which are packet filtering, proxy server and stateful firewall, Network Address Translation (NAT), Software firewall. Each firewall has their advantages and disadvantages. Rest portion of this paper is describe pro and cons of different firewall.

Packet Filtering

This is one of the simple types of firewall. This firewall is work on OSI layer 3 and 4. It filter packet by looking at IP address, TCP/UDP port number. It compare the incoming packet against pre define rule configure in to the router. After comparing router make decision to allow or deny the packet [4]. An access list is used to create rule to make decision. Figure shows the working of the packet filtering firewall.

Figure 2: Packet Filtering in Router [4]

Pros

The simplest of the firewall technologies to configure. Only required access list to configure the firewall.

Packet filtering capabilities are easily available in many hardware and software routing products, both commercially and they are freely available over the Internet.

It is less processor intensive. Adding a filtering rule to a router produces little or no additional performance overhead.

It is use for all type of application because it operates at the OSI layer 3 (Network) and layer 4 (Transport) layer.

Only one router is required to protect entire network.

Cons

The packet filter has no intelligent to identify the authenticity of source. A well trained intruder can spoof inside IP address and can fool the firewall as the packet is from inside network.

Since filtering rule is configuring manually it add administrative workload. Adding complex rule to the firewall decrease the router performance.

In some cases, the filtering is incompatible with certain caching

Strategies commonly used for performance enhancement.

Some policies cannot readily be enforced by normal packet filtering routers.

Example

The following example shows how to build basic packet filtering firewall

Consider a scenario of company whose inside network is lying in IP address range 10. 1. 1. 0/24. Ethernet 0/1 is inside interface and Ethernet 0/0 is outside interface. To protect against IP spoofing attack following access list policy is configure

```
Access list 100 deny ip 10. 1. 1. 0 0. 0. 0. 255 any log

Access list 100 deny ip 127. 0. 0. 0 0. 255. 255. 255 any log

Access list 100 deny ip 172. 16. 0. 0 0. 15. 255. 255 any log

Access list 100 deny ip 192. 168. 0. 0 0. 0. 255. 255 any log

Access list 100 deny ip 224. 0. 0. 0 15. 255. 255. 255 any log

Access list 100 deny ip host 255. 255. 255. 255 any log

Access list 100 permit ip any 10. 1. 1. 0 0. 0. 0. 255

Interface Ethernet 0/0

Ip access-group 100 in
```

An access list is basic tool to configure for packet filtering. Generally all routers support this tool. Above example is configured and tested on Cisco router. There are free download is available on internet few examples are Tuneup 1. 0, Truxtis, Visnetic. Packet filtering firewall is simple in configuring and freely available on internet it is good solution for small business where not much complex firewall implementation is required.

In our case study implementation of packet filtering is not a wise solution. A simple reason is it is very cumbersome. Example shows that just to stop ip spoofing we need to configure eight commands. Sometime it is difficult to troubleshoot and

manage for network administrator.

Application Layer Firewall

Application Layer Firewall is also known as a proxy server. According to dictionary meaning of proxy is “ A person authorized to act for another; an agent or substitute”. Same definition is valid for proxy server in network security. Proxy server is a software package install on device and act behalf of protected network which allows or denies access across network [5, 7].

Figure 3: Proxy Server [4]

Above figure shows the working of proxy server. Proxy server works at layer 7 of Open System Interconnection (OSI) system model [4]. It intercepts and established the connection behalf of internal host to the outside network. As shown in figure when inside network is trying to connect outside network, application layer firewall which is install on router is intercept the secession and check the request is valid or not. If it is not valid request it discard the packet and if it is a valid request it repackage the request and send it to outside network as the packet is send by itself. When outside network response the request proxy server repackaged the response and sends it back to the original inside network. In some case proxy server block all connection from outside network and allowed only inside network to go outside. The only traffic is allowed from outside is the response from outside network to inside network. In some case both inbound and outbound traffic is allowed but under strict observation [4, 5, 7].

Example

A good example, and the one we probably see the most, is a web proxy. When configured to use a proxy, your web browser contacts the proxy server for each web access instead of going directly to the target server on the internet. The proxy server then turns around and makes the " real" request of the web server. The proxy server gets the response, and then passes it back to you.

Another example is proxy server is Tibia proxy which is game proxy server. Tibia is a popular multiplayer online computer game hosted on Internet servers. To play Tibia requires establishing a network connection to TCP port 7171 on the server. Depending on your network setup and your Internet Service Provider (ISP), your direct connection to the Tibia server and ability to play the game may be blocked by a network firewall or proxy server. Setting up a Tibia proxy avoids this common connection problem. A Tibia proxy is a special Internet server (separate from the game server) that does not require a port 7171 connection. Instead, the Tibia proxy server will accept requests on alternative network ports (such as port 80) that will typically not be restricted by firewalls / proxies. The Tibia proxy, in turn, makes its own direct connection to the game server (on port 7171) and translates messages between the Tibia server and your client in real time to allow game play [8].

Pros

Act as an intermediary between outside network and protected network. It prevent direction connection between source and destination

It is application aware firewall so that it can analyzes application inside the payload

Support user level authentication

It able to log the traffic and can do user level authentication

Cons

It is processor intensive so it is slower than packet filtering

Need to configure internal client about proxy server

Sometime it does not support all type of application. For example Sling Player 2. 0 does not supported by proxy server.

It is single point failure. Proxy server is install on device so if that device gets compromised then whole security compromised.

Stateful Packet Filtering

Figure 4: Stateful Firewall [4]

In the mid-1990s, packet filters and proxy servers were the two technologies used to build firewall systems. As the number of applications that needed to pass through firewalls increased, proxy server vendors could not keep up with the development of new proxy servers. On the other hand, packet filtering also could not support the dynamic nature of the many modern applications. Thus, a new technology was born [4, 11].

Stateful packet filtering is a combination of packet filtering and application level gateway firewall [11]. It contains advantages of both. It is also refer as a application aware firewall. Stateful firewall not only examines IP header information but also up to application layer information for better inspection. The working of stateful firewall is as follow. When host from inside network send a packet to outside network it check authorization of the network and if it is authorized then it allow the packet outside the network and maintain state table. State table is a table which keep track of the active network connection which is TCP secession or UDP communication passing across it. This is also called as saving of state. When destination network respond to the initial request it compare the response with the information saved in state table to allow or denied the packet [11].

Example

Cisco Adaptive Security Appliances in short Cisco ASA [9], Cisco PIX firewall, Check Point [10] are example of stateful firewall.

Pros

It work at network level and transport level but also at application layer

It is not a processor intensive as proxy server

Temporarily open the outside port so it reduces the possibility of attack that work against static packet filtering.

Because of the state table it is faster than application layer gateway

Support almost all the services.

Cons

It allows direct connection to inside host once the request to enter the network is granted. An attacker may exploit the vulnerability of that host and poison the network.

It required skill knowledge of different type of traffic and attacks

Network Address Translation

This is one of the simplest methods to protect inside network. Network Address Translation (NAT) is quite similar to the packet filtering. When it configure on router it translate internal private network to outside public network. It maintain translation table so when reply come from outside to inside it send back to correct host. There are three type of NAT static NAT, dynamic NAT, port address translation (PAT) [12].

Pros

It is very simple to configure

It hide private network behind one public IP address

Unlikely proxy server it does not requires any configuration on inside host.

Cons

It is difficult to troubleshoot end-to-end

NAT cause problem when Virtual Private Network (VPN) is configured

Like packet filter firewall it work at network and transport level of OSI model so it translate packet based on ip address

Personal Firewall

The personal firewall is an application which is install on computer to protect personal computer from different virus and different kind of attack [13]. It allow or deny request from computer based on configure policies. Many personal firewall like does intrusion detection. An example of this type firewall is Host Base Intrusion Prevention (HIPS) which block the communication if it finds any suspicious activity [14].

Pros

Prompt user for outgoing connection

Allow user to control which application is permitted to connect interne od LAN

Dose auditing for all user of the computer

Tell user that application is attempting to connect internet and gives information about destination server with which application want to connect

It dose virus scanning automatically every day and remove them

Cons

It is an application running on host so it gives some load on CPU

If system get affected by malware or spyware, it can modify the firewall cause security issue

Recommendation

By looking at different type of firewall and comparing their advantages and drawback we can conclude that stateful firewall is good solution for our scenario. The product like Cisco ASA or Check Point is ideal to guard against different type of attack. They also does intrusion detection and prevention and can virtualized these firewall which save cost of buying extra firewall.