DESIGN and IMPLEMENTATION OF SELF-SUFFICIENT FIREWALL GATEWAY SYSTEM

Roopa K.
Dept of CS and Engg.,
J.N.N College of Engineering,
Shimoga, Karnataka, INDIA -577204
email: roopasindhe@lycos.com
Ph No: 080-3391260 ®

Panduranga Rao MV
Dept of IS and Engg.,
J.N.N College of Engineering,
Shimoga, Karnataka, INDIA -577204
email: raomvp@yahoo.com
URL: http://www.raomvp.bravepages.com/

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop intruders from accessing any part of your computer system.

1. Abstract:

This article describes a full-featured Network security in the form of completely self-sufficient firewall gateway system. Service based personal firewall has been developed and integrated with the component based firewalling architecture. This application infers the unauthorized Network service requests. It thus provides the network administrator with an advanced functionality for monitoring and tracking the networks.

It employees the Linux operating system. Physical security of the firewall gateway system is provided by Administrator. It provides complete security to our Network services. The service based firewall simulated in a floppy drive, bundled with the following software components, Network interface card configuration tools, Network monitoring and reporting tools, A text based command line user interface, TCP dump 3.5.x software.

The firewall's purpose is to enforce the security policies we define. These policies reflect the decisions we've made about which internet services has to be accessible to our computers, which services we want to offer the world from our computers, which services we want to offer to specific remote users , and which services and programs we want to run locally for our own private use. Security policies are all about access control and authenticated use of private or protected services, programs, and files on our computers.

- **Key terms:** Simplicity, cost-effectiveness, availability, confidentiality, services, modification, fabrication.

2. Introduction

Firewall:

A component or set of components that restricts access between a protected network and the Internet, or between other sets of networks and possess the following properties;

- All traffic from inside to outside, and vice-versa, must pass through it.
- Only authorized traffic, as defined by the security policy, is allowed to pass through it.
- The system itself is immune to penetration.

Packet filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network, and vice versa). To accomplish packet filtering, we set up a set of rules that specify what types of packets (e.g., those to or from a particular IP address or port) are to be allowed and what types are to be blocked. Packet filtering may occur in a router, in a bridge, or on an individual host.

Packet filtering lets the network administrator control data transfer based on

- The address the data is coming from
- The address the data is going to
- The session and application protocols being used to transfer the data.
- Information regarding various transfer stored parameters in the packet.

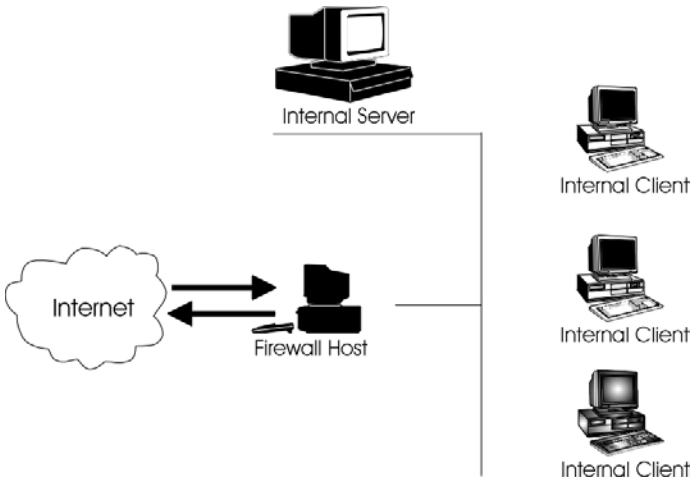

Figure 1.1: The network layout for the packet-filtering firewall host and the local network.

Service based personal firewall system will watch the all in-coming and out-going data packets based upon service. The system will starts-up when operating systems starts and it runs as daemon for monitoring the data packets. The network administrator will also be provided a GUI configuration and monitoring tool wherein he will be able to configure the firewall components and specify the firewall rules that will determine the access control policy of the network and organization.

Once the system is up and functioning as an operational firewall, the system administrator will be provided with options for loading additional modules

and advanced network tools and utilities which enhance the capabilities of the system, and provide the administrator with increased functionality.

2.1 Basic guidelines

The summary idea, is that the application layer represents communication between two programs. The transport layer represents how this communication is delivered between the two programs. Programs are identified by numbers called services ports. The network layer represents the communication using network interface cards, which are identified by numbers called IP addresses. The subnet layer represents how this communication is carried between each individual computer along the way. On an Ethernet network, these computer network interfaces are identified by numbers called Ethernet addresses, which you are probably familiar with as your network card's burned – in hardware MAC address.

3.1 Analysis:

Regardless of the size of the network to be protected, we have to identify the resources we have to protect the size of the network, the Internet services to be accepted and rejected, the network topology and the post-attack policy. A network security policy is designed for a particular computer network. Although there are generic network security policies available to help the security policy designer, the appropriateness of these policies for a particular network needs to be evaluated.

3.1.1 Packet Filtering

Packet filtering systems route packets between internal and external hosts, but they do it selectively. They allow or block certain types of packets in a way that reflects a site's own security policy as shown in Figure 3.1. The type of router used in a packet filtering firewall is known as a *screening router*.

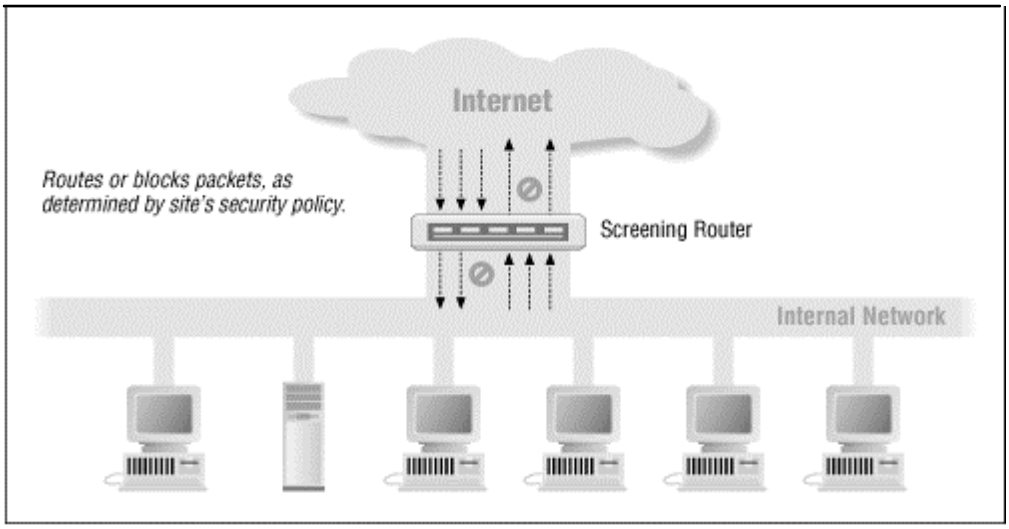

Figure 3.1: Using a screening router to do packet filtering

Every packet has a set of headers containing certain information. The main information is:

- IP source address

- IP destination address
- Protocol (whether the packet is a TCP, UDP, or ICMP packet)
- TCP or UDP source port
- TCP or UDP destination port
- ICMP message type

In addition, the router knows things about the packet that aren't reflected in the packet headers, such as:

- The interface the packet arrives on
- The interface the packet will go out on

The fact that servers for particular Internet services reside at certain port numbers lets the router block or allow certain types of connections simply by specifying the appropriate port number (e.g., TCP port 23 for Telnet connections) in the set of rules specified for packet filtering.

Here are some examples of ways in which we might program a screening router to selectively route packets to or from our site:

- Block all incoming connections from systems outside the internal network, except for incoming SMTP connections (so that you can receive email).
- Block all connections to or from certain systems you distrust.
- Allow email and FTP services, but block dangerous services like TFTP, the X Window System, RPC, and the "r" services (*rlogin*, *rsh*, *rcp*, etc.).

To understand how packet filtering works, let's look at the difference between an ordinary router and a screening router.

An ordinary router simply looks at the destination address of each packet and picks the best way it knows to send that packet towards that destination. The decision about how to handle the packet is based solely on its destination. There are two possibilities: the router knows how to send the packet towards its destination, and it does so; or the router does not know how to send the packet towards its destination, and it returns the packet, via an ICMP "destination unreachable" message, to its source.

A screening router, on the other hand, looks at packets more closely. In addition to determining whether or not it *can* route a packet towards its destination, a screening router also determines whether or not it *should*. "Should" or "should not" are determined by the site's security policy, which the screening router has been configured to enforce.

4.1 Design phase for setting up the firewall

Before setting up the firewall, analysis and design factors are to be focussed. The firewall is designed based on a site security policy.

Issues to be addressed by security policy:

- Selecting the Internet services and resources to be made accessible externally
- Determining the authorized and unauthorized accesses
- Determining Access location restrictions

- Reconstruction of the network topology
- Managing the user accounts
- Controlling the remote sites
- Setting the default rules
- Simplifying the policy
- Responding to policy violation

The other important aspects of design are

1. *Where would be the best location for the packet-filtering firewall?*
2. *What services should be monitored?*
3. *In what order are the rules to be evaluated?*
4. *What actions should the firewall host perform?*

4.1.1 Best location to place the packet-filtering firewall

Packet-filtering firewall is best installed at a choke point between the intranet and the Internet. Usually the gateway to the Internet is selected.

If the Internet router cannot handle the packet-filtering rules, a computer with two network interface cards should be installed between the intranet and the Internet router as shown in Figure 2.1. Both incoming and outgoing connections should be configured to transmit through the packet-filtering host.

4.1.2 What services should be monitored

After deciding on the location for installing the firewall software, we (network administrators) have to identify which connection holes should be opened for external connections, and which ones should be shut on the firewall host.

Most TCP/IP services could be supported by the packet-filtering firewall. However, not all Internet services could be monitored. For instance, most UDP/IP services could not be managed by packet-filtering firewall. Luckily, most UDP/IP network services could be omitted and many new services which use UDP/IP protocols can be configured to use TCP/IP protocol for packet transmission.

In configuring a packet-filtering firewall system, administrators must be aware that protocols are usually bi-directional. Therefore, if specific TCP/IP service has to be denied, both incoming and outgoing packets should be blocked.

The ACK bit field in the TCP/IP packet header can be used for identifying the "start-of-connection" packet. In an outgoing service connection, the ACK bit field is marked "on" in the first incoming response packet but not in the first incoming service request packet. With this piece of information, the direction of the communication requests can be determined and restricted.

However, not all the protocols have this field (examples include UDP/IP packets). Therefore, many packet-filtering firewalls cannot guard against these packets. Only products with dynamic packet-filtering (stateful inspection method), such as Checkpoint's Firewall-1, Morning Star's SecureConnect Router and KarlBridge, can handle these packets by "remembering" the state of the outgoing UDP/IP packets.

4.1.3 The order for evaluating the rules

The order for evaluating the permission and denial rules governs the characteristics of the packet-filtering firewall. In most firewalls, packet-filtering rules are determined on a first matched basis. Whenever a rule is matched, actions will be taken and the remaining rules are ignored. Therefore, if permission rules are analyzed before denial rules, even if a connection were explicitly defined in the denial rules, connection could still be established. Hence, firewall policies could be reversed depending on the order of rule evaluation.

Although there are different orders for analyzing filtering rules, the most important rules should always be defined in the earlier section of the rule table.

4.1.4 The actions should be performed by the firewall host

When defining the actions on the firewall host for handling the incoming and outgoing services, actions for permitted and rejected connections have to be specified. For instance, network administrators have to decide whether telnet service from the external sites is permitted, that the source addresses are within the trusted hosts list, and that the destination site is allowed.

Filtering rules for handling incoming and outgoing services should be defined separately. In rejection rules, deny action should be used instead of dropping the connections because whenever an external connection is dropped, incoming requests will not be cut immediately. So external users could not reconnect until the time out duration is exceeded. If rejected service is denied, users will not have to wait and network bandwidth will not be wasted.

If ICMP service is permitted on the firewall host, ICMP error codes should not be returned to the sender, because these error codes provide useful information about the local network. In addition, all actions should be logged for review.

In general, all rules should be kept as simple as possible. Communication speed will be slowed down by the number of rules defined.

5.1 Implementation of firewall

The illustration below on firewall configuration is based on the network topology. Default-Deny Rule is selected as the default-filtering rule. If the default rule is not clearly declared or if Default-Deny Rule is not used, explicit Default-Deny Rule can be defined as the last rule for rejecting connections from any location to any location using any protocol.

In Linux operating system, we implement packet filtering firewall using etherfind or tcpdump programs. These programs selects packets of the network for analysis. TCP dump 3.5.x is a tool for network monitoring and one of the most well-known sniffers. Built with the libpcap (packet capture library) interface, tcpdump collects information from packets on the network including those intended for other host, tcpdump does this through a network interface card's ability to enter into promiscuos mode where the tool then dumps packet header information depending on the Boolean expression being applied.

Network Layout:

The packet-filtering firewall consists of two network interface cards, different sub-networks are combined into one network range (from 201.123.50.0 -

201.123.50.255). Packet-filtering firewall is installed on the gateway between the local network and internet. The modified network structure is given as,

Local network:

- Class C network
- domain name: rao.net
- Full IP address range: 201.123.50.0 - 201.123.50.255
- Internet Servers used
  - Web Server: 201.123.50.80
  - FTP Proxy Server: 201.123.50.81
  - Mail Server: 201.123.50.82
  - Gopher Server: 201.123.50.83
  - DNS server: 201.123.50.84
  - NNTP Server: 201.123.50.86
  - FTP Server: 201.123.50.89
- Network address: 201.123.50.0
- Broadcast address: 201.123.50.255
- Netmasks: 255.255.255.0
- Gateway to the Internet router address: 201.123.50.1
- Firewall host:
  - host name: firewall.rao.net
  - IP address: 201.123.50.1

5.1.1 Basic Policy

Before specifically defining the characteristics and policies for individual services, some general policies which should be used for both packet-filtering and application-gateway firewall architecture are given:

- *source routing packets and routing table modification protocols must be denied*. If hackers can alter the route they travel into the network, they could bypass the firewall host as well as the bastion host. Therefore, all *incoming network management protocols* including *Simple Network Management Protocol* (*SNMP*) and *Routing Information Protocol* (*RIP*) should be denied. Furthermore, all packets with source routing should be rejected.

The firewall host holds:

- TCP/IP ports above *1023* should *not* be opened for incoming packets without the ACK bit.
- TCP/IP ports below *1023* should *only be opened* for incoming packets to the Internet servers.

Other TCP/IP, UDP and IP port connections *should be denied*.

5.1.2 Services and protection policies

- Spoofing rule ➔ This rule is added to the packet-filtering firewall for preventing hackers from using the internal addresses as their addresses. External sites are prevented from accessing internal services with source addresses as internal addresses.

- Telnet ➔ Telnet from internal clients to external clients are permitted, but only trusted external clients are permitted to access the internal network
- FTP ➔ FTP service for outgoing connections are permitted, and incoming FTP connections are also permitted but on the anonymous FTP server (201.123.50.89) using PASV mode FTP connections. For outgoing normal mode FTP services, a special denial rule is added for preventing external clients to connect through the FTP holes. In this example, only X11 service connections (TCP/IP 6000 - 6003) are blocked.
- SMTP and POP ➔ Mail services are permitted as usual.
- HTTP ➔ HTTP services are provided for both internal and external users.
- NNTP➔ Internal users could access any news server.
- Finger ➔ Finger services are permitted for internal users only.
- Archie ➔ Archie services are permitted for internal users to one Archie site only (e.g. archie.mcgill.ca).
- RealAudio and RealVideo ➔ Only outgoing RealAudio and RealVideo services are permitted. The data channel used for transmission is UDP/IP 7070.
- DNS ➔ One internal DNS server is setup to handle all DNS requests.
- Ping ➔ Ping service is allowed for internal users only.

5.1.3 Cost of setting up the firewall

Cost of the firewall is not solely represented by the price of the firewall product. The time used in installation and configuration of the firewall, the cost of network administrators for handling firewall administration and management work, and the cost of extra components required for setting up a firewall should also be included. In most cases, a personal computer or workstation would be required for firewall installation. Usually at least two network cards are needed on these firewall hosts. Furthermore, some firewall architectures may require extra screening routers for network security enhancement.

All these costs should be taken into consideration in setting up a firewall.

6.1 Disadvantages and future scope of study

The major disadvantages of the our packet filtering firewall is explained below, which inturn circumspect the future scope of study for further improvements.

1. IP spoofing may easily occur. Because the packet-filtering router permits or denies a network connection based on the source and destination addresses of the packet, any attack that uses valid IP address may not be detected. In order to handle this problem, the routing table has to be examined.
2. Logged information is not descriptive enough. If the packet filtering system is setup at the router, logging may not be available.
3. Partial access control cannot be used. In most of the packet-filtering firewalls, only the IP packets would be inspected, that is, examination of the network connections will be performed on the network layer only, not on the operations requested. For example, SMTP services can either be accepted or rejected, but not accepted based on user identity.

4. May not be able to guard against source routing attacks. In source routing attack, the route a packet used for traveling across the Internet was specified by the source station and this route is not the expected path to the destination and bypasses the firewall host.
5. Packet-filtering rules are comparatively harder to be designed and configured.
6. Not all protocols could be filtered by the packet filtering firewall. For instance, RPC-based protocols and any protocol which uses a composite form of TCP/IP and UDP/IP protocols may not be filtered by packet filtering firewalls.
7. Tiny fragment attacks may beat the packet-filter firewall. In this scheme an intruder uses the IP fragmentation feature to create extremely small fragments which contain separate TCP header information. Since user-defined filtering rules may only examine the first fragment and allow the other fragment to enter.
8. Data-driven attack cannot be prevented using packet-filter firewall.

7.1 Advantages of firewall

The major advantages of the our packet filtering firewall is explained as follows.

1. Transparent firewall system➔ As packet contents (what it does) is not intercepted by the packet-filtering firewall, from the network users point of view, packet-filtering firewall is almost transparent .
2. Fast network performance.
3. Simpler to configure than the other types of firewall .
4. Only one machine is required for protecting the entire network.
5. Packet filtering capability is available in many hardware and software routing products.
6. Network hiding is supported. Some packet-filtering firewalls such as the Cisco PIX router support the Network Address Translation services.

9. Conclusions:

In general, the suitability of a firewall architecture is determined by:

- Complexity on configuring the firewall
- Amount of activities controlled by the firewall
- Description stored in the log
- Scalablility of the firewall
- Administration of the firewall
- Price of the firewall

Normally, configuration of the firewall architecture is still required for enhancing the architecture from its assigned security level. However, This firewall architecture can be expanded by providing a "floppy solution". With this method, security policies could be configured on a management machine and transferred to the firewall machine using floppy diskettes. This allows network administrators to produce a set of security policy solutions on several floppy diskettes and distribute them to the appropriate departments. With the configuration diskettes, the whole firewall structure could be considered as a "blackbox". Companies

without any network and firewall administrators could use this firewall mechanism based on the security solution provided in the same.

If the firewall is not properly configured and thoroughly tested, the holes created in the firewall to the services supported may become the channels for external hackers to peek into and attack the internal network.

10. References and Acknowledgements:

The following references are useful to learn and implement the firewall mechanisms and to step towords cryptography.

- Building Internet Firewalls By D. Brent Chapman, Elizabeth D. Zwicky

1st Edition September 1995.

- The CERT Guide to system and Network Security Practices (addison - Wesley, 2001), by CERT author Julia Allen.
- Building Internet Firewalls, 2nd Edition

By Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman

- *Silicon Toad's Hacking Resources www.hackers.com*
- *Internet Security System www.iss.net*
- *Watchguard Firewall System www.watchguard.com*