American Journal of Computer Science and Engineering
2017; 4(2): 8-22
http://www.openscienceonline.com/journal/ajcse

Open Science

Local Network Security Using Distributed Firewall

Umar Danjuma Maiwada

Faculty of Natural and Applied Science, Mathematics & Computer-Science Department, Ummar Musa Yar’adua University, Katsina, Nigeria

Email address

umar4pilot@gmail.com, umardanjumamaiwada@yahoo.com

To cite this article

Umar Danjuma Maiwada. Local Network Security Using Distributed Firewall. *American Journal of Computer Science and Engineering*. Vol. 4, No. 2, 2017, pp. 8-22.

Received: April 6, 2017; **Accepted**: June 5, 2017; **Published**: July 11, 2017

Abstract

Our Networks and computers at home, schools, offices, companies and other places are not secured because a number of confidential transaction occur every second and today computers are used mostly for transaction rather than processing of data, so Data security is needed to prevent hacking of data and to provide authenticated data transfer. Data security can be achieved by Firewall; a firewall is typically placed at the edge of a system and acts as a filter for unauthorized traffic. But conventional firewalls rely on the notions of restricted topology and controlled entry points to function. In most systems today, the firewall is the machine that implements the “security policy” for a system. Firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Distributed firewall is a mechanism to enforce a network domain security policy through the use of policy language Security policy is defined centrally. Distributed firewalls secure the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the Internet and the internal network because the most destructive and costly hacking attacks still originate from within the organization. This paper will introduce the concept of distributed firewall as a security policy of local networks. I will study Distributed firewall because it gives total security to a network.

Keywords

Local Networks, Security Policy, Firewall, Distributed Firewall

1. Introduction

Firewalls Interconnects networks with differing trust Imposes restrictions on network services, only authorized traffic is allowed. Auditing and controlling access can implement alarms for abnormal behavior. A firewall is typically placed at the edge of a system and acts as a filter for unauthorized traffic filters tend to be simple: source and destination addresses, source and destination ports. A firewall is a collection of components, interposed between two networks, which filter traffic between them according to some security policy. Conventional firewalls depend on the topology restriction of the networks. The controlled entry point - the firewall – divides the networks into two parts, internal and external networks. Since the firewall cannot filter the traffic it does not see, it assumes that all the hosts on the internal networks are trusted and all the hosts on the other side (external) are untrusted. Firewalls do not protect networks from internal attacks. Since everyone on the internal networks is trusted and the traffic within these trusted networks is not seen by the firewall, a conventional firewall cannot filter internal traffics, hence it cannot protect systems from internal threats.

For traditional firewalls, the only way to work around this is to deploy multiple firewalls within the internal networks, i.e. divide the network into many smaller networks, and protect them from each other. A firewall is the single entry point. This is the place traditional firewalls enforce their policy and filter the traffic. It is also a single point of failure. If the firewall goes down for any reason, the entire internal networks are isolated from outside world. Although high availability options, such as hot standby firewall configurations exist, they are usually cost prohibitive.

In Distributed Firewalls, Security policy is defined centrally and Enforcement of policy is done by network endpoint(s). Policy is one of the most often used terms in case of network security and in particular distributed firewall. A “security policy” defines the security criteria of a system. The security policy is defined for whom transmission is allowed or denies. The Distributed firewall is centrally managed and distributed over the network with the connected systems i.e. with end points. In the distributed firewall the security policy is centrally defined and implemented at the end host. The Distributed firewall filters the data traffic from internet as well as internal network. Because of the distributed nature the data on the protected side is not taken as trusted and hence the attacks which happens mostly from inside are detected and prevented.

2. Firewalls

A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.

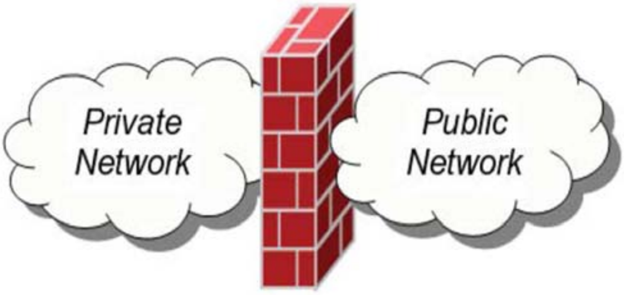


Figure 1. Firewall.

2.1. Firewall Policies

To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called firewall policies.

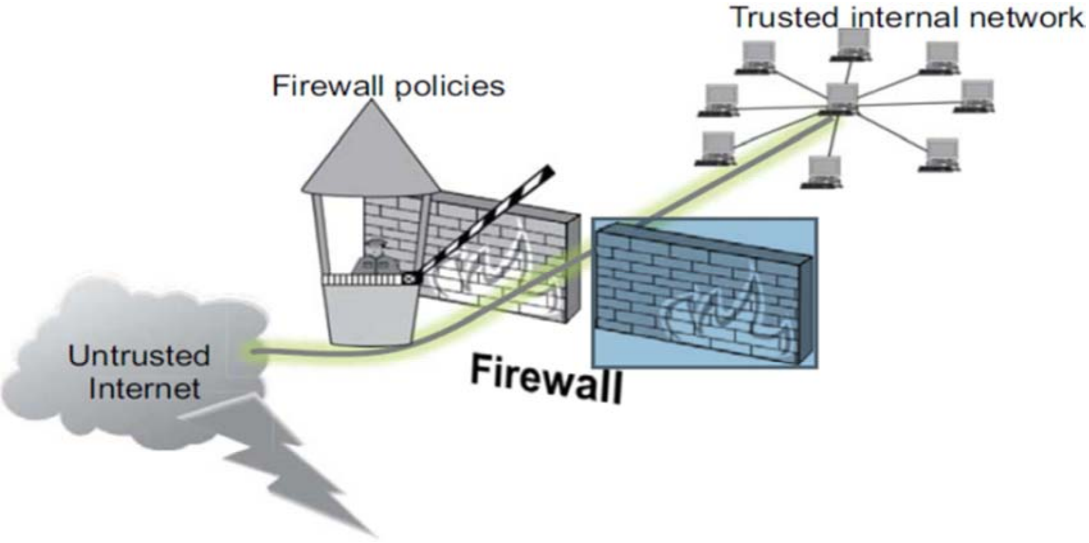


Figure 2. Firewall policies.

2.2. Policy Actions

a) Packets flowing through a firewall can have one of three outcomes:

– Accepted: permitted through the firewall

– Dropped: not allowed through with no indication of failure

– Rejected: not allowed through, accompanied by an attempt to inform the source that the packet was rejected

b) Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:

– TCP or UDP

– The source and destination IP addresses

– The source and destination ports

– The application-level payload of the packet (e.g., whether it contains a virus).

2.3. Blacklist and White List

a) There are two fundamental approaches to creating firewall policies (or rule sets) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network (or individual computer).

b) Blacklist approach

– All packets are allowed through except those that fit the rules defined specifically in a blacklist.

– This type of configuration is more flexible in ensuring that service to the internal network is not disrupted by the firewall, but is naïve from a security perspective in that it assumes the network administrator can enumerate all of the properties of malicious traffic.

c) Whitelist approach

– A safer approach to defining a firewall rule set is the default-deny policy, in which packets are dropped or rejected unless they are specifically allowed by the firewall.

2.4. Firewall Types

a) Packet filters (stateless)

– If a packet matches the packet filter's set of rules, the packet filter will drop or accept it

b) "Stateful" filters

– It maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.

c) Application layer

– It works like a proxy it can “understand” certain applications and protocols.

– It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities).

2.4.1. Stateless Firewall

A stateless firewall doesn’t maintain any remembered context (or “state”) with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously. Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.

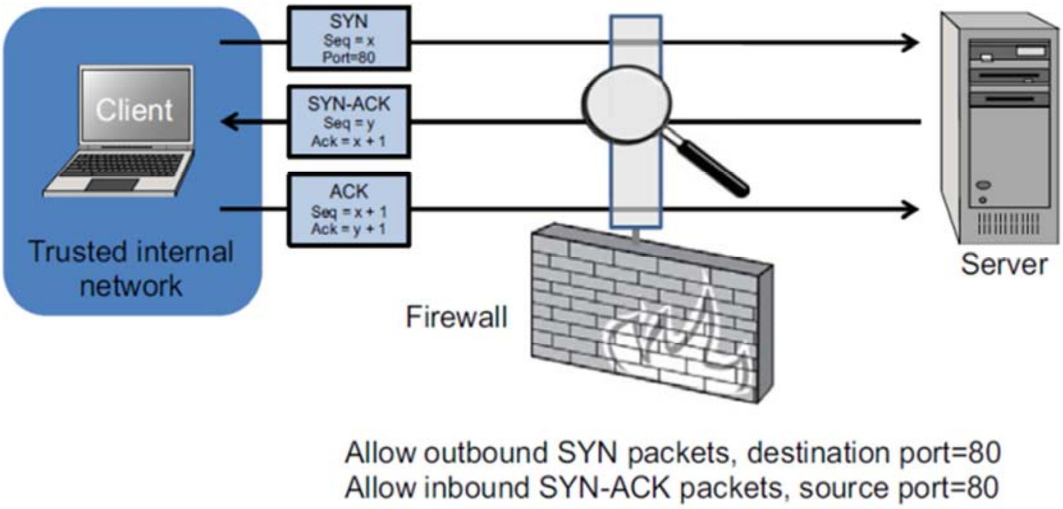


Figure 3. *Stateless firewalls.*

2.4.2. Statefull Firewalls

a) Stateful firewalls can tell when packets are part of legitimate sessions originating within a trusted network.
b) Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
c) Using these tables, Stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network. Allow only requested TCP connections.

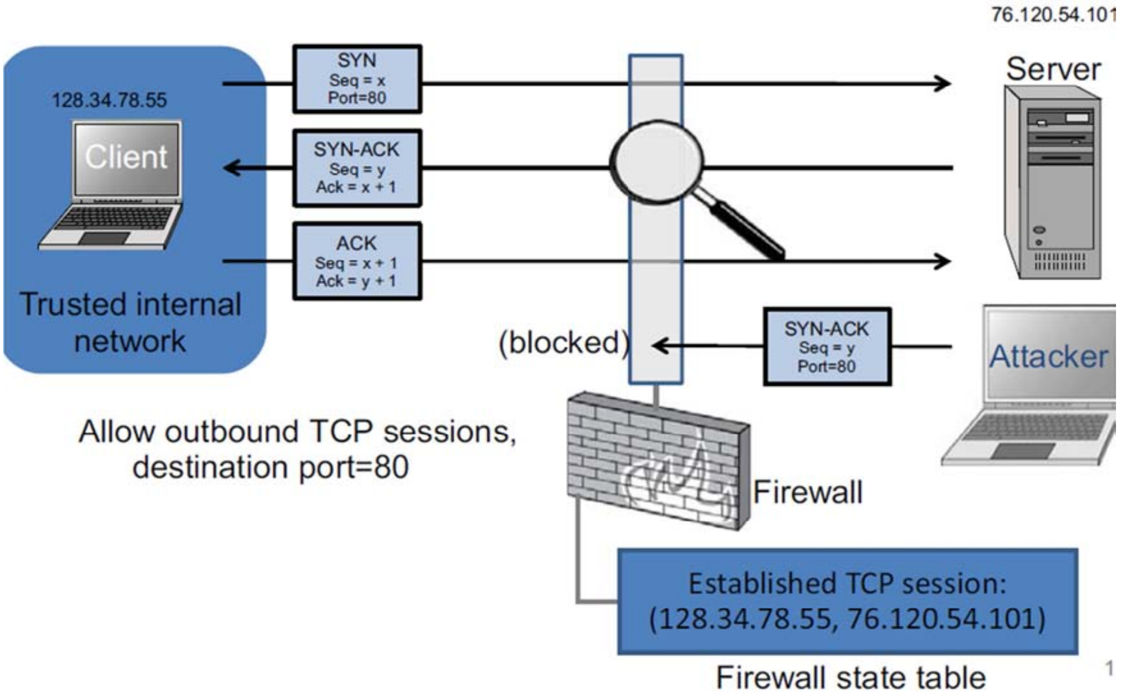


Figure 4. *Stateful firewall.*

3. Distributed Firewall

A distributed firewall is a mechanism to enforce a network domain security policy through the use of a policy language, a policy distribution scheme enabling policy control from a central point and certificates, enabling the identification of any member of the network policy domain.

Distributed firewalls secure the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the Internet and the internal network because the most destructive and costly hacking attacks still originate from within the organization. They provide virtually unlimited scalability. Distributed firewalls are host-resident security software applications that protect the enterprise network's servers and end-user machines against unwanted intrusion. They offer the advantage of filtering traffic from both the Internet and the internal network. This enables them to prevent hacking attacks that originate from both the Internet and the internal network. This is important because the most costly and destructive attacks still originate from within the organization.

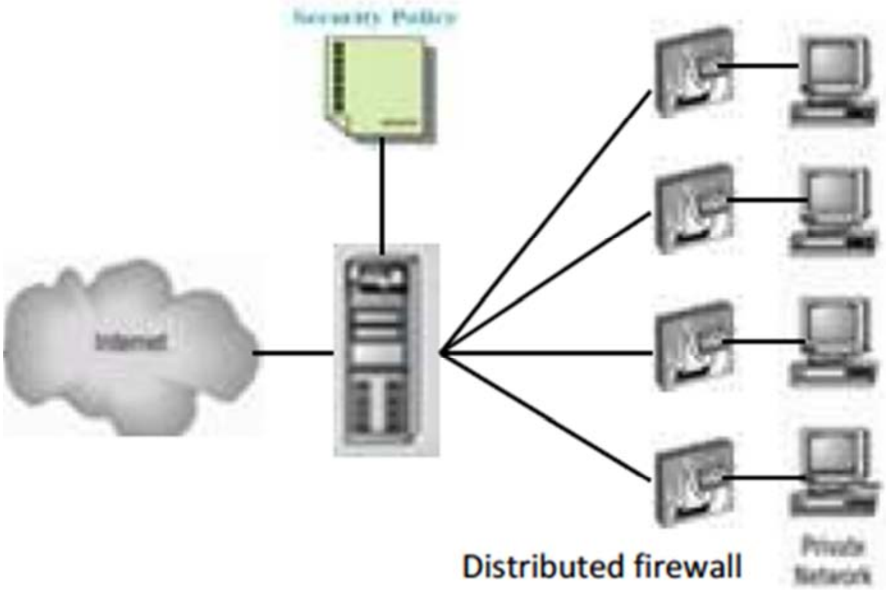


Figure 5. *Distributed Firewall.*

3.1. A Distributed Firewall Design

Distributed firewalls are host-resident security software applications that secure the enterprise network's servers and end-user machines against unwanted invasion. This endow them to prevent hacking attacks that originate from both the Internet and the internal network as given in the figure-6. They offer the feature of filtering traffic from both the Internet and the internal network. Usually deployed behind the traditional firewall, they give a second layer of security. Distributed firewalls secure the network by defending important network end-users, exactly where hackers want to invade.

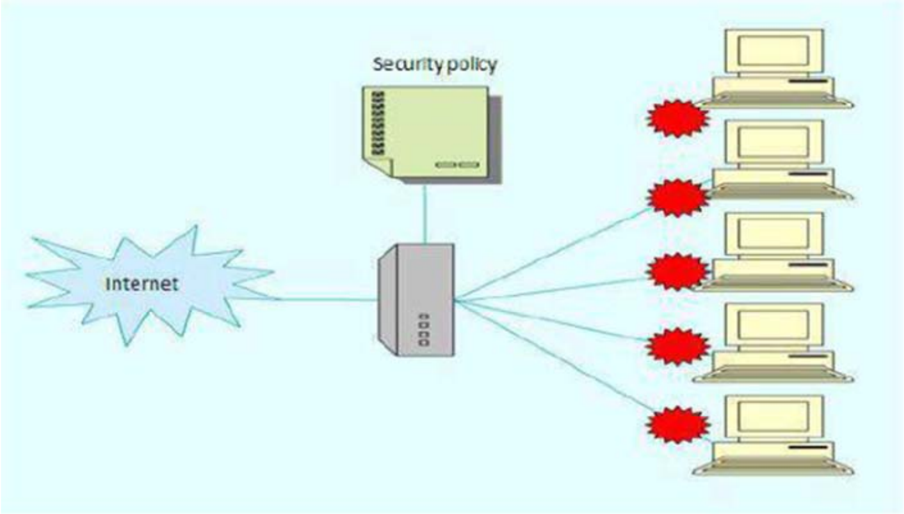


Figure 6. *Distributed Firewall Design.*

3.2. Architecture of Distributed Firewalls

The network security policies are deployed in a decentralized way. The management is not allowed the system administrators to set security policies from a server to host and fulfill the basic requirements of secure system and network administration. The concepts of distributed firewalls, the network topological constraints are weakened and a decentralized use of traffic filters all over network. Distributed firewall system consists of four elemental parts:

3.2.1. The Management Center

This is responsible for the management of all end-users in the network, data security policy ordinance and distribution, log file receiving from the host network and analysis, invasion detection and so on.

3.2.2. Policy Actuator

Policy actuator is installed in each host network or every gateway to receive the data security policy provided by the management center, and implements the policy. It elucidates and runs the data security policy program. It is the program to defend the endpoint host networks, and it is mainly to recognize the function of the conventional firewall. Additionally, it is also to attain the functions of communicating with the management control center and implementing communication link request for the remote user-end.

3.2.3. Remote Endpoint Connectors

The remote endpoint connectors are the programs especially designed for the remote endpoint host networking, to prove their existence to Maintaining the Integrity of the Specifications. The template is used to modify your paper and text style. All paper margins, columns width, text fonts and line spaces are prescribed; please do not alter them. For example, the main margin in this template measures proportionately more than is conventional. These dimensions and others are intended, using specifications that expect your paper as one part of the entire process, and not as an individual document. Please do not revise any of the current designations. Other hosts users on a simple network, specially the internal host-point, request to establish communication with the internal endpoint. The network users use certificates to prove there authorized identity of the remote network server, while the certificate is sent to the endpoint by the management center through a security policy document mode, which can merge the remote endpoint connectors and the policy actuators. Thus, in one side the communication between the remote endpoint and the local endpoint is convenient, in the other side the remote endpoint can be provided security protects [11].

3.2.4. Log Server

The log server is important for the collection of the distinct events done in the whole network, such as basic networks protocol rule, log files, user login event logs, user Internet access logs, for audit analysis.

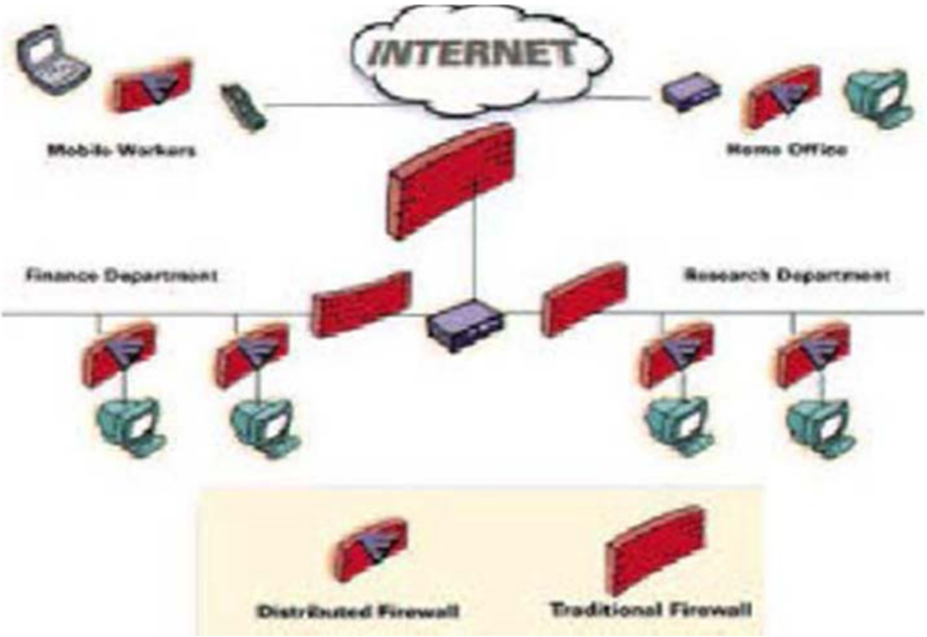


Figure 7. *Distributed firewall Architecture.*

3.3. Components of Distributed Firewall

a) A central management system used for implementing the data security policies.
b) A communication system to transmit these data security policies.
c) Implementation of the security policies in the user end.

3.3.1. Central Management System

Central Management system, a component of distributed firewalls, makes it practical to protect desktops, enterprise-wide servers, Tablets, laptops, and workstations. It gives greater control and efficiency and it reduce the maintenance costs of managing global security installations [12]. This feature addresses the need to maximize network security resources by enabling policies to be centrally configured, deployed, monitored, and updated. From a single workstation, distributed firewalls can be scanned to understand the current operating policy and to determine if updating is required.

3.3.2. Policy Distribution

The distributed firewall policy distribution scheme should guarantee the integrity of the policy during transfer. This policy can be dissimilar and differ with the implementation [12]. The distribution of policy can be either straight pushed to end systems, or pulled when needed.

3.3.3. User-End Implementation

The security policies transmitted from the central management server have to be implemented by the user-end. The end-user part of the Distributed Firewall does give any administrative control for the network administrator to control the implementation of security policies. The end-user allows traffic based on the security rules it has implemented [12].

3.4. Policies

One of the most often used term in case of network security and in particular distributed firewall is policy. It is essential to know about policies. A “security policy” defines the security rules of a system. Without a defined security policy, there is no way to know what access is allowed or disallowed. A simple example for a firewall is:

a) Allow all connections to the web server. Deny all other access.
b) The distribution of the policy can be different and varies with the implementation. It can be either directly pushed to end systems, or pulled when necessary.

3.4.1. Pull Technique

While booting up host pings to the central management server to check whether the central management server is up and active. It registers with the central management server and requests for its policies which it should implement. The central management server provides the host with its security policies. For example, a license server or a security clearance server can be asked if a certain communication should be permitted. A conventional firewall could do the same, but it lacks important knowledge about the context of the request. End systems may know things like which files are involved, and what their security levels might be. Such information could be carried over a network protocol, but only by adding complexity

3.4.2. Push Technique

The push technique is employed when the policies are updated at the central management side by the network administrator and the hosts have to be updated immediately. This push technology ensures that the hosts always have the updated policies at any time. The policy language defines which inbound and outbound connections on any component of the network policy domain are allowed, and can affect policy decisions on any layer of the network, being it at rejecting or passing certain packets or enforcing policies at the Application Layer.

3.5. Advantages of Distributed Firewalls

I. Topological independence is one of the main advantages of distributed firewalls. Since network security no longer depends on network topology, it provides more flexibility in defining the security perimeter [11].

II Network security is no more dependent on the single firewall so that problems like performance bottleneck and traffic congestion are resolved. [13], [24]

III Opposing to conventional firewalls, network security is no more dependent on the single firewall so that problems like performance bottleneck and traffic congestion are resolved. Besides, the load on the traditional firewall is reduced since a large amount of filtering is performed at the end hosts.

IV As mentioned earlier, filtering of certain protocols such as FTP is not so easy on a conventional firewall. Such kind of a process is much easier on distributed firewalls since all of the required information is available at the decision point, which is the end host in general.

V Security policy rules are distributed and established on an as-needed basis. Only the host that needs to communicate with the external network should determine the relevant policy. This approach dramatically eases the policy updating process and does not require each firewall to maintain the complete policy set.

VI The distributed firewalls network protect from hackers attacks that originate from both the Internet and the internal network Filtering of some protocols like File Transfer Protocol are not easy for traditional firewall, on the other hand it is easy for distributed firewalls since all of the necessary information is available at the decision point, which is the end-user host in general [8].

3.6. Disadvantages of Distributed Firewall

I If firewall command center is compromised, due to attack or mistake by the administrator, this situation is high risky for security of the entire network.

II Intrusion detection systems are less effective with distributed firewalls because complete network traffic is not on the single point.

III It is not so easy to implement an intrusion detection system in a distributed firewall environment. It is possible to log suspicious connections on local server but these logs need to be collected and analyzed by security experts in central services. [18]

IV Compliance of security policy for insiders is one of the major issues of distributed firewalls. This problem especially occurs when each ending host have the right of changing security policy. There can be some techniques to make modifying policies harder but it is not totally impossible to prevent it.

V Acceptance of the network security policy for internal users is one of the major problems of the distributed firewalls. This issue specially done when each ending user host has the right of changing security policy.

4. Local Network

A LAN is a network of computers and other components located relatively close together in a limited area. LANs operate at layer-2 of the Open Systems Interconnect (OSI) model, and can vary widely in size. They can consist of only two computers in a home office or small business, or include hundreds of computers in a large corporate or healthcare environment. Various LAN types are available, such as Ethernet, Token Ring, ARC Net and FDDI. The Ethernet-based technologies are by far the most prevalent within the modern network. This is partly due to the low cost of the technology, coupled with the performance it offers, and the general ease of deployment and maintenance in comparison to some of the legacy technologies. The guidance within this document covers good practice for implementing LANs comprising multiple layers and components. Smaller organizations, such as GP Surgeries and Clinics, may find that only the guidance within the 'Access Layer' and 'Server Layer' sections apply to their network infrastructure. A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, or office building [6]. A local area network is contrasted in principle to a wide area network (WAN), which covers a larger geographic distance and may involve leased telecommunication circuits, while the media for LANs are locally managed.

4.1. Network Security

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

4.2. Common Security Attacks and Their Counter Measures

a) Finding a way into the network
   i) Firewalls
b) Exploiting software bugs, buffer overflows
   ii) Intrusion Detection Systems
c) Denial of Service
   iii) Ingress filtering, IDS
d) TCP hijacking
   iv) IPSec
e) Packet sniffing
   v) Encryption (SSH, SSL, HTTPS)
f) Social problems
   vi) Education

4.3. Security in Local Network

The Assumptions and Challenges is to examine some of the security issues commonly found in the small to medium sized LAN set up for a business or other institution, and to identify some of the best practices from the perspective of the network designer. While no two networks are exactly alike, some of the typical challenges faced by the network designer include the following:

a) Securing the network from Internet launched attacks
b) Securing Internet facing web, DNS and mail servers
c) Containing damage from compromised systems, and preventing internally launched attacks
d) Securing sensitive and mission critical internal resources such financial records, customer databases, trade secrets, etc.
e) Building a framework for administrators to securely manage the network
f) Providing systems for logging and intrusion detection

Before beginning the design process, a security policy should be put in place, or updated to accurately reflect the goals of the company. Additionally, a realistic assessment of the risks faced, and identification of the resources (manpower, hardware, and budget) that are available should be made. Once the organization's security policy and the available resources have been identified the design process can begin. We will assume that we have adequate human resources and budget dollars to acquire and configure an optimum set of network technology. I will attempt to identify practices and technologies which can be tailored and applied appropriately to the individual site's needs.

4.4. Topology and Architecture

A critical step in designing our network is defining the network topology. The topology is the physical and logical layout of the network. On the physical side, we will need to provide distribution to the offices or buildings where the users are located. We will need to provide connectivity to the servers which comprise our intranet, to the Internet, and possibly to other company locations or business partners, remote users connecting via telephone lines, etc. The logical topology must be considered as well. It is bound to some degree by the physical topology, but with technologies such as Virtual LANs (VLANs) and Virtual Private Networks (VPNs) there is considerable flexibility in designing the logical topology. In laying out the logical topology we will need to consider our security policy, and decide what our trust model is. Which parts of the network are less trusted, and which are more? Which groups of devices and users should be logically grouped together, and which should be separated?

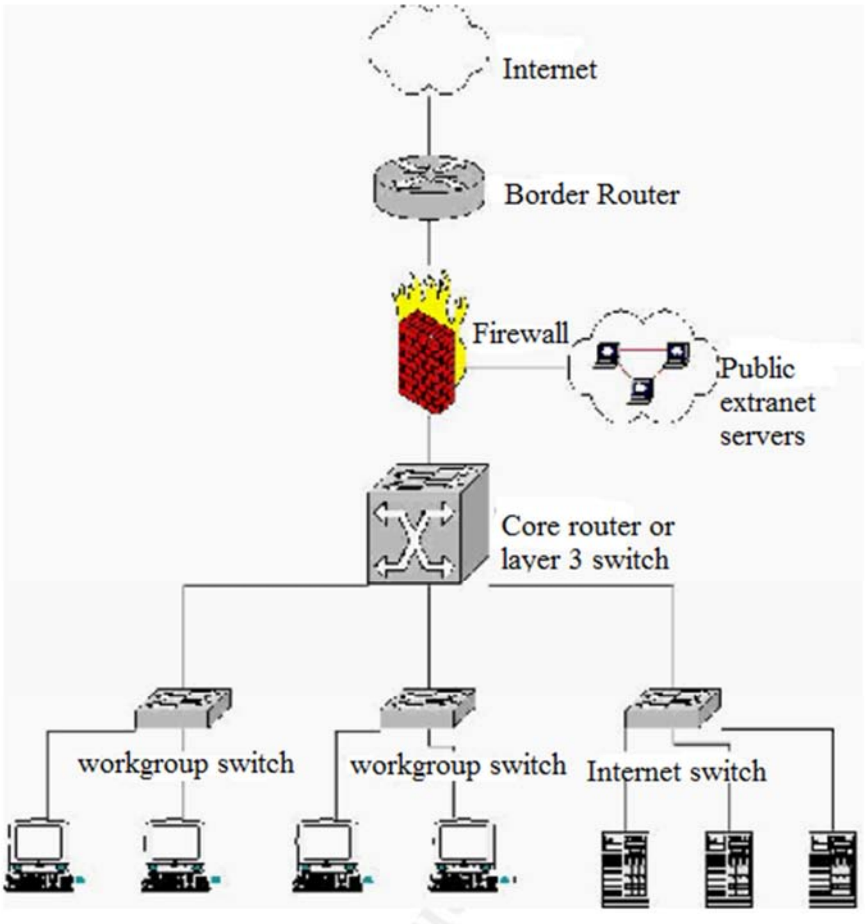


Figure 8. *Network Design.*

The basic design illustrates our connection to the Internet with a border router and firewall, and our public extranet servers which are connected to a third interface on the firewall. The firewall is one of four connections to a core router or, if higher performance is required, a layer 3 switch. The remaining connections to our core router are the floor or building switches which provide connectivity to the different departments and our intranet servers. This topology demonstrates how devices with similar functions and security profiles are grouped together -- the public extranet servers, user workstations, and the intranet servers. By creating separate security zones, we will be able to enforce our security policy with the appropriate firewall rules and layer 3 access lists [28]. One element our basic design lacks is the infrastructure for managing our network. We will need one or more management workstations, tftp servers, and one or more syslog servers at a minimum. Other typical servers for the management network are a one-time password (e.g. RSA SecurID or Axent Defender) server, RADIUS server, etc. Because these servers will form the foundation of our network management and security, we will want to create a separate management VLAN which is isolated from the rest of the network by access lists. The only traffic that we will allow in to the management network is either from the managed devices or protected by encryption.

4.5. Securing Routers and Switches

After the topology has been defined, let's take a look at building security into our network elements and configurations. Our design calls for segmenting the network into subnets based on function and, possibly, location. By implementing routing at the network core, our segments are isolated into individual broadcast domains. This improves performance and also improves security by preventing sniffing or arp based attacks between segments. Within each subnet the hosts are connected to an Ethernet switch. A switch provides high performance by putting each host in its own collision domain, and enhances security by making sniffing and arp based attacks difficult. A hub is a less expensive alternative to a switch for layer 2 connectivity, though it is less desirable both from a performance and a security standpoint.

4.6. Security in Local Network Using Firewall

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

a) Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
b) Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
c) Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
d) Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)

Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this may not be sufficient and in some cases is not cost-effective. Consider a network with hundreds or even thousands of systems, running various operating systems, such as different versions of UNIX and Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. This requires scalable configuration management and aggressive patching to function effectively. While difficult, this is possible and is necessary if only host-based security is used. A widely accepted alternative or at least complement to host-based security services is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function. The firewall, then, provides an additional layer of defense, insulating the internal systems from external networks. This follows the classic military doctrine of "defense in depth," which is just as applicable to IT security.

4.7. Firewall Basing

It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux. Firewall functionality can also be implemented as a software module in a router or LAN switch.

4.7.1. Bastion Host

A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway. Common characteristics of a bastion host are as follows:

a) The bastion host hardware platform executes a secure version of its operating system, making it a hardened system.
b) Only the services that the network administrator considers essential are installed on the bastion host. These could include proxy applications for DNS, FTP, HTTP, and SMTP.
c) The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.
d) Each proxy is configured to support only a subset of the standard application's command set.
e) Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.
f) Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks.
g) Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws. For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.
h) Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications. Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host.
i) A proxy generally performs no disk access other than to read its initial configuration file. Hence, the portions of the file system containing executable code can be made read only. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.
j) Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.

4.7.2. Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package. Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common location for such firewalls is a server. There are several advantages to the use of a server-based or work station based firewall:

a) Filtering rules can be tailored to the host environment. Specific corporate security policies for servers can be implemented, with different filters for servers used for different application.

b) Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall.

c) Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

4.7.3. Personal Firewall

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal computer. In a home environment with multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface. Personal firewalls are typically much less complex than either server-based firewalls or stand-alone firewalls. The primary role of the personal firewall is to deny unauthorized remote access to the computer. The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware. An example of a personal firewall is the capability built in to the Mac OS X operating system. When the user enables the personal firewall in Mac OS X, all inbound connections are denied except for those the user explicitly permits. The list of inbound services that can be selectively enabled, with their port numbers, includes the following:

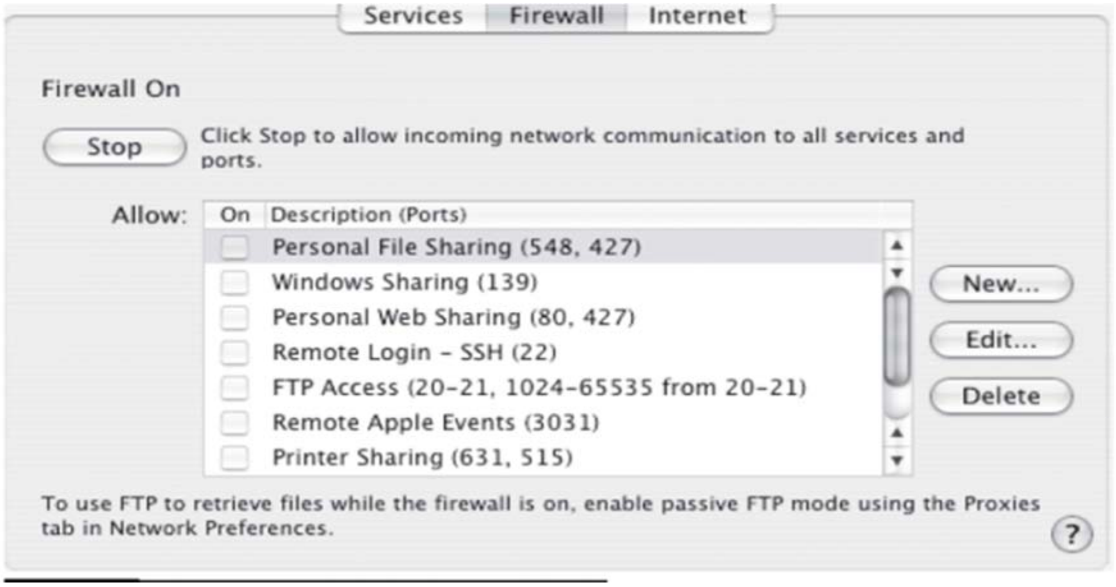
a) Personal file sharing (548, 427)

b) Windows sharing (139), • Personal Web sharing (80, 427), • Remote login - SSH (22)

c) FTP access (20-21, 1024-64535 from 20-21), • Remote Apple events (3031)

d) Printer sharing (631, 515), • IChat Rendezvous (5297, 5298), • ITunes Music Sharing (3869)

e) CVS (2401)



Firewall On

Click Stop to allow incoming network communication to all services and ports.

Allow:

On	Description (Ports)
□	Personal File Sharing (548, 427)
□	Windows Sharing (139)
□	Personal Web Sharing (80, 427)
□	Remote Login - SSH (22)
□	FTP Access (20-21, 1024-65535 from 20-21)
□	Remote Apple Events (3031)
□	Printer Sharing (631, 515)

To use FTP to retrieve files while the firewall is on, enable passive FTP mode using the Proxies tab in Network Preferences.

Figure 9. *Personal Firewall Interface.*

a) Gnutella/Lime wire (6346), • ICQ (4000), • IRC (194), • MSN Messenger (6891-6900)

b) Network Time (123), • Retrospect (497), • SMB (without netbios-445), • Timbuktu (407)

c) VNC (5900-5902), • WebSTAR Admin (1080, 1443)

When FTP access is enabled, ports 20 and 21 on the local machine are opened for FTP; if others connect to this computer from ports 20 or 21, the ports 1024 through 64535 are open.

For increased protection, advanced firewall features are available through easy-to-configure checkboxes. Stealth mode hides the Mac on the Internet by dropping unsolicited communication packets, making it appear as though no Mac is present. UDP packets can be blocked, restricting network traffic to TCP packets only for open ports. The firewall also supports logging, an important tool for checking on unwanted activity.

4.8. Firewall Location and Configuration

A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network. With that general principle in mind, a security administrator must decide on the location and on the number of firewalls needed. In this section, we look at some common options.

4.8.1. DMZ Networks

The distinction between an internal and an external firewall is that: An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.

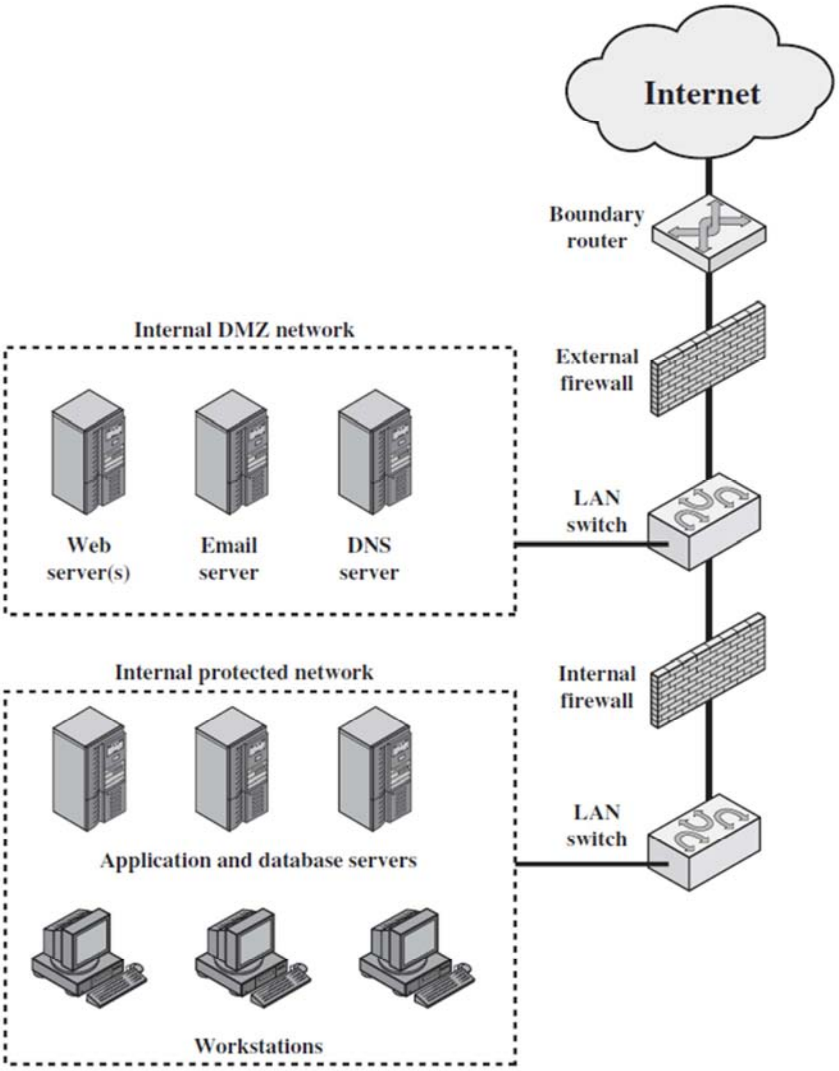


Figure 10. *Firewall Configuration.*

The external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

I The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

II The internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Internal firewall can protect the DMZ systems from attack from the internal protected network.

III Multiple internal firewalls can be used to protect portions of the internal network from each other. For example, firewalls can be configured so that internal servers are protected from internal workstations and vice versa.

A common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks.

4.8.2. Virtual Private Networks

Look at today's distributed computing environment, the virtual private network (VPN) offers an attractive solution to network managers. In essence, a VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security. At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs). The Internet or some other public network can be used to interconnect sites, providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider. That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites. But the manager faces a fundamental requirement security. Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed. In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec. An organization maintains LANs at dispersed locations. A logical means of implementing an IPsec is in a firewall, which essentially repeats. If IPsec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPsec could be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall and thus less desirable as an IPsec platform.

5. Security in Local Network Using Distributed Firewall

Restricting the network topology difficult in filtering certain protocols, expanding network and few more problems leads to the evolution of DISTRIBUTED FIREWALL.

Distributed firewalls are host-resident security software applications that protect the enterprise network's servers and end-user machines against unwanted intrusion. They offer the advantage of filtering traffic from both the Internet and the internal network. This enables them to prevent hacking attacks that originate from both the Internet and the internal network. This is important because the most costly and destructive attacks still originate from within the organization. A feature of distributed firewalls is centralized management. The ability to populate servers and end-users machines to configure and push out consistent security policies helps to maximize limited resources. The ability to gather reports and maintain updates centrally makes distributed security practical. Distributed firewalls help in two ways. Remote end-user machines can be secured. Secondly, they secure critical servers on the network preventing intrusion by malicious code and jailing other such code by not letting the protected server be used as a launch pad for expanded attacks.

5.1. Components to Implement a Distributed Firewall

In their simplest form, policies in a distributed firewall are functionally equivalent to packet filtering rules. However, it is desirable to use an extensible system (so that other types of applications and security checks can be specified and enforced in the future). The language and resolution mechanism should also support credentials for delegation of rights and authentication purposes. A mechanism for safely distributing security policies may be the IPsec key management protocol when possible, or some other protocol. The integrity of the policies transferred must be guaranteed, either through the communication protocol or as part of the policy object description (*e.g.* they may be digitally signed). A mechanism that applies the security policy to incoming packets or connections providing the enforcement part.

5.1.1. Central Management System

Central Management, a component of distributed firewalls, makes it practical to secure enterprise wide servers, desktops, laptops, and workstations. Central management provides greater control and efficiency and it decreases the maintenance costs of managing global security installations.

This feature addresses the need to maximize network security resources by enabling policies to be centrally configured, deployed, monitored, and updated. From a single workstation, distributed firewalls can be scanned to understand the current operating policy and to determine if updating is required.

5.1.2. Policy Distribution

The policy distribution scheme should guarantee the integrity of the policy during transfer. The distribution of the policy can be different and varies with the implementation. It can be either directly pushed to end systems, or pulled when necessary.

5.1.3. Host-End Implementation

The security policies transmitted from the central management server have to be implemented by the host. The host end part of the Distributed Firewall does provide any administrative control for the network administrator to control the implementation of policies. The host allows traffic based on the security rules it has implemented.

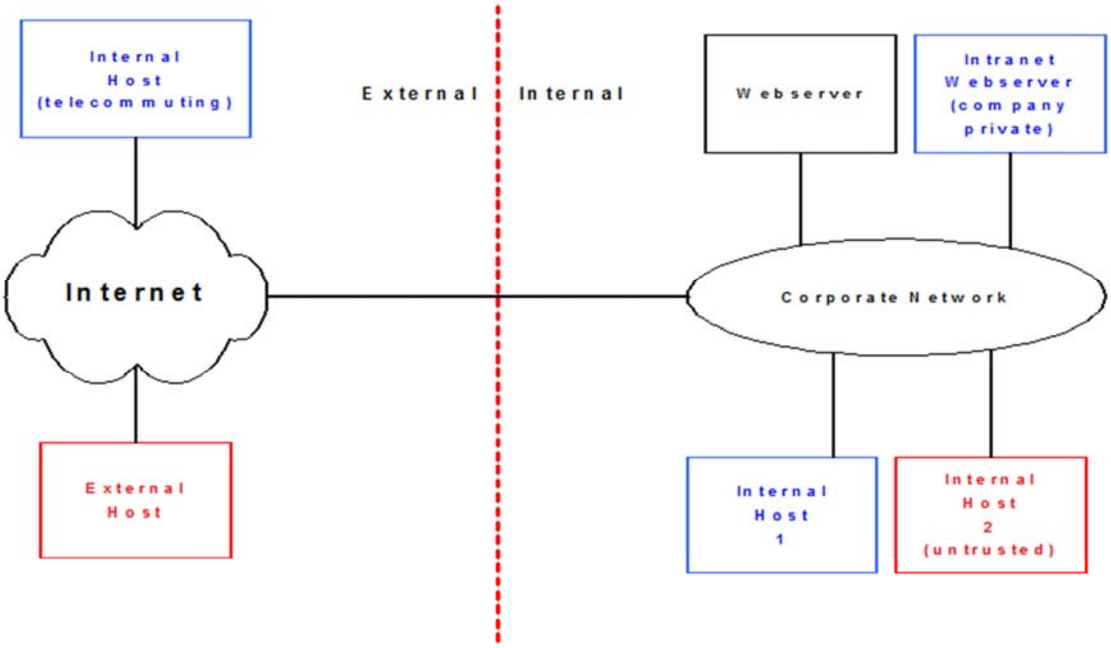

Internal Host (telecommuting)
External
Internal
Webserver
Intranet Webserver (company private)
Internet
Corporate Network
External Host
Internal Host 1
Internal Host 2 (untrusted)

Figure 11. *Distributed Firewall Example.*

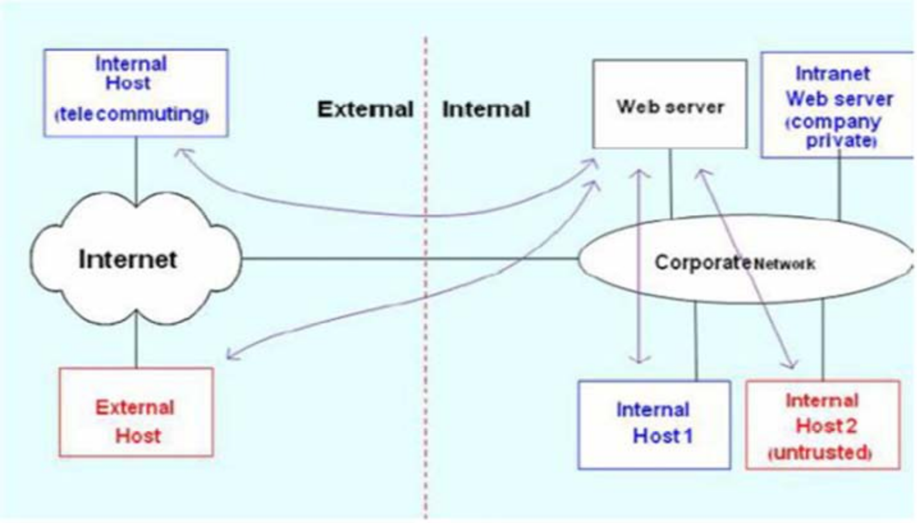

Internal Host (telecommuting)
External
Internal
Web server
Intranet Web server (company private)
Internet
Corporate Network
External Host
Internal Host 1
Internal Host 2 (untrusted)

Figure 12. *Connection to web Server.*

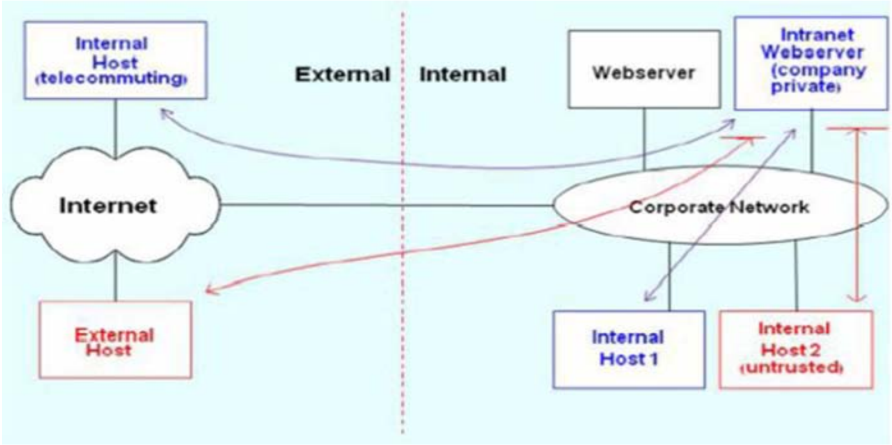

Internal Host (telecommuting)
External
Internal
Webserver
Intranet Webserver (company private)
Internet
Corporate Network
External Host
Internal Host 1
Internal Host 2 (untrusted)

Figure 13. *Connection to Internet.*

6. Implementation

Steven M. Bellovin in November 1999 proposed that, distributed firewalls are still in their infancy. But we see that several institutes and software/hardware manufacturers are working towards to making distributed firewalls a reality. A project supported by DARPA was fulfilled at the University of Pennsylvania in 2000 [21]. In this project, a prototype of distributed firewall was constructed. OpenBSD was chosen as the operating system, because it was an attractive platform for developing security applications with well-integrated security features and libraries. Keynote was chosen as the security policy language. It was also used to send credentials over an untrusted network. IPSec was used for traffic protection and user/host authentication. This was a concept-prove implementation. Other improvements, such as moving the policy daemon to the kernel and adding IP filters, etc., needed to be done on this prototype firewall. Currently, Network-1 Security Solutions Inc. is offering a commercial host-resident firewall, Cyber wall PLUS, on the windows platform. This host-resident firewall includes personal firewalls for remote users, firewall agents for workstations, and application server resident firewalls. It's very similar to distributed firewall. Actually, when multiple host-resident firewalls are centrally configured and managed, it indeed is a distributed firewall [3]. But Cyber wall PLUS still has its challenges currently. It cannot collect reports centrally **[3]**. We note that the necessary filtering is prescribed by the IPSEC architecture [KA98].

Specifically, the inbound Security Policy Database (SPD) is used to reject illegal input packets, while the outbound SPD can be used to control outgoing connections. An informal survey showed that most commercial IPSEC implementations either support port number-granularity security associations or will in the near future.

Application-level protection can be achieved by distributing application-specific policy files. Thus, web browsers can be told, by the central site, to reject, for example, all ActiveX controls or Java applets. Note that this is a hard problem for conventional firewalls [MRR97]; doing it on the end hosts is more securing, if the policy distribution problem can be solved.

The hardest problem is handling protocols such as FTP without touching the application. That is done most easily with per-process keying for IPSEC. For example, a policy rule for FTP would indicate that outbound connections to port 21 must be protected with IPSEC, and that all other TCP connections protected by that security association are legal. Since only that process can use that SA, and it would only have the FTP data channel open, an adequate level of protection can be achieved. Key Note is an especially attractive choice for a policy language. Indeed, Blaze, Ioannidis, and Keromytis [BFK99, BFIK99] explicitly note its suitability for configuring packet filters. Its advantages include the integration of credentials with policy specification, and an ability to use a single mechanism to specify policy at different levels.

7. Keynote

Trust Management is a relatively new approach to solving the authorization and security policy problem, and was introduced in [17]. Making use of public key cryptography for authentication, trust management dispenses with unique names as an indirect means for performing access control. Instead, it uses a direct binding between a public key and a set of authorizations, as represented by a safe programming language. This results in an inherently decentralized authorization system with sufficient expressibility to guarantee flexibility in the face of novel authorization scenarios.

Give response, Verifier Requester, Request, Key, Sig, KeyNote, Gather information local policy

Pass (remote credentials) information, Evaluate

Application Interactions with KeyNote. The Requester is typically a user that authenticates through some application-dependent protocol, and optionally provides credentials.

The Verifier needs to determine whether the Requester is allowed to perform the requested action. It is responsible for providing to KeyNote all the necessary information, the local policy, and any credentials. It is also responsible for acting upon KeyNote's response.

One instance of a trust-management system is KeyNote. KeyNote provides a simple notation for specifying both local security policies and credentials that can be sent over an untrusted network.

Policies and credentials contain predicates that describe the trusted actions permitted by the holders of specific public keys (otherwise known as principals). Signed credentials, which serve the role of "certificates," have the same syntax as policy assertions, but are also signed by the entity delegating the trust. For more details on the KeyNote language you can refer to [16].

Applications communicate with a "KeyNote evaluator" that interprets KeyNote assertions and returns results to applications. However, different hosts and environments may provide a variety of interfaces to the KeyNote evaluator (library, UNIX daemon, kernel service, etc.). A KeyNote evaluator accepts as input a set of local policy and credential assertions, and a set of attributes, called an "action environment," that describes a proposed trusted action associated with a set of public keys (the requesting principals). The KeyNote evaluator determines whether proposed actions are consistent with local policy by applying the assertion predicates to the action environment. The KeyNote evaluator can return values other than simply true and false, depending on the application and the action environment definition. An important concept in KeyNote (and, more generally, in trust management) is "monotonicity". This simply means that given a set of credentials associated with a request, if there is any subset that would cause the request to be approved then the complete set will also cause the request to be approved. This greatly simplifies both request resolution (even in the presence of conflicts) and credential management. Monotonicity is enforced by the KeyNote language (it is not possible to write non-monotonic policies).

8. Conclusion

Due to increase in line speed, connectivity, and complexity of protocols, conventional firewalls can no longer handle their purpose adequately. A new concept of firewall, distributed firewall was introduced. Distributed firewall can solve some known and thoroughly discussed problems which arise with the use of conventional firewalls residing at the networks perimeter. Distributed firewall retains the advantages of conventional firewalls, while solving many of their problems. A distributed firewall preserves central control of access policy, while reducing or eliminating any dependency on topology. Distributed firewall architecture requires high quality administration tools, and de facto places high confidence in them. We believe that this is an inevitable trend however, even if traditional firewalls are utilized; already, large networks with a modest number of perimeter firewalls are becoming difficult to manage manually. Distributed Firewalls provide the secure environment for internet access. In this security policy is specified using KeyNotes policies and distributed to the users and hosts in the networks. Applications communicate with a “keynote evaluator”. Monotonicity, means that gives a set of credentials associated with request, if there is any subset that would cause the request to be approved then the complete set will also cause the request to be approved. So, with the help of distributed firewall concept we can achieve the followings goals,

a) This Provide Complete data protection to the network.
b) Distributed firewall allows or denies the network traffic meant for a particular system based on the policy it has to follow.
c) Give Protection to the end-user of the networks from the inside and outside attacks.

Remote end-user machines can be secured so they can't be used as entry points into the enterprise network. They secure critical servers on the network preventing intrusion by malicious code and "jailing" other such code by not letting the protected server be used as a launch pad for expanded attacks. Since the firewall is distributed across an entire network, the load of processing is further distributed as the network grows, so performance remains high.

References

[1] A Thesis Proposal Presented to The Academic Faculty by Lane Thames Georgia Institute of Technology April 2008.

[2] AtulKahate, “Cryptography and Network Security”, ISBN-13: 978-0-07-064823-4, ISBN-10:0- 07-064823-9, McGraw Hill Higher Education.

[3] Avi Fogel, Pushing Security to Network Endpoints, http://www.nwfusion.com/archive/2000/99612_06-26-2000.html,

[4] Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security McGraw Hill Higher Education.

[5] Dr. Mostafa Hassan Dahshan “Security and Internet Protocol”, Computer Engineering 44

[6] Gary A. Donahue (June 2007) network warrior O’Reilly p5

[7] Gatus, G. E. P., Safavi-Naini, R. and Willy Susilo. 2004. Policy Distribution Using COPSPR in a Distributed Firewall. In Australian Telecommunication Networks and Applications Conference.

[8] HiralB. Patel, Ravi S. Patel, JayeshA. Patel, “*Approach of Data Security in Local Network using Distributed Firewalls*”, International Journal of P2P Network Trends and Technology-Volume1Issue3-2011.

[9] Robert Graham, Network Intrusion Detection, http://www.robertgraham.com/pubs/network-intrusion-detection.html

[10] Scott Granneman (2002), Security focus, http://online.securityfocus.com/infocus/1527

[11] Patel, Ravi S. Patel, Jayesh A. Patel; Thread, data, security in Local Network using distributed firewall, http://www.seminarprojects.com/Thread-data-security-in-localnetwork-using-distributed-firewalls.

[12] http://en.wikipedia.org

[13] Ioannidis, S. and Keromytis, A. D., and Bellovin, S. M. and J. M. Smith, "*Implementing a Distributed Firewall*", Proceedings of Computer and Communications Security (CCS), pp. 190-199, November 2000, Athens, Greece.

[14] Justin Weisz jweisz@andrew.cmu.edu Network Security 15-441 Networks Fall 2002.

[15] Kyle Wheeler, “Distributed Firewall Policy Validation”, December 7, 2004.

[16] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. The keynote trust management system version 2. Internet RFC 2704, September 1999.

[17] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *Proc. of the 17th Symposium on Security and Privacy*, pages 164–173. IEEE Computer Society Press, Los Alamitos, 1996.

[18] Oguzhan ÇAKI, March 2008, Thesis on “Access monitoring system for distributed firewall policies”

[19] Robert Stepanek, “Distributed Firewalls”, rost@cc.hut.fi, T-110.501 Seminar on Network Security, HUT TML 2001.

[20] Smith, R., Chen, Y., and Bhattacharya, S., \Cascade of distributed and cooperating firewalls in a secure data network," in IEEE Transactions on Knowledge and Data Engineering, vol. 15, pp. 1307{1315, 2003.

[21] Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, and Jonathan M. Smith, *Implementing a Distributed Firewall* http://www.cis.upenn.edu/~angelos/Papers/df.pdf

[22] Taylor, David. "Are there Vulnerabilities in VLAN Implementations?" Intrusion Detection FAQ. 12 Jul 2000. URL: http://www.sans.org/newlook/resources/IDFAQ/vlan.htm (15 Dec. 2002).

[23] Thames, L., Abler, R., and Saad, A., \Hybrid intelligent systems for network security," in Proceedings of the 2006 ACM Southeast Conference (ACMSE06), (Melbourne, Florida), 2006.

[24] William Stalling, "*Cryptography and Network Security Principles and Practices*", ISBN-978-81- 775-8774-6, PEARSON.

[25] W. R. Cheswick and S. M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 1994.

[26] Yunus ERDOĞAN,November 2008,Thesis on "DEVELOPMENT OF A DISTRIBUTED FIREWALL ADMINISTRATION TOOL".

[27] Zou, C., Towsley, D., and Weibo, G., \A firrewall network system for worm defense in enterprise networks," in Technical Report: TR-04-CSE-01, University of Massachusetts, (Amherst, Massachusetts), 2004.

[28] (Trudel, B., Convery, S. "SAFE: A Security Blueprint for Enterprise Networks."2000.)