

# Network Security

---

## Making it Safe

Presented

by

---

**Rashid Hussein**

© Copyright

**Somalitech.com**

# Table of contents

---

<b>1. Overview.....</b>	<b>3</b>
<b>2. Network security methods.....</b>	<b>4</b>
2.1.1 Introduction.....	4
2.1.2 A Network Security Policy.....	5
2.1.3 IP Security Arithmetic.....	6
2.1.4 Vertual Private Networks.....	6
2.1.5 Spyware Detection.....	6
2.2 Firewalls.....	7
2.2.1 Static.....	7
2.2.2 Dynamic.....	8
2.2.3 Proxies.....	10
2.2.4 Firewall & Antivirus Softwares on the Internet.....	12
<b>3. Secure Network Designs.....</b>	<b>13</b>
3.1.1 Example1 of a Secure Network, Intranet and Servers.....	13
3.1.2 Example2 of a Secure Network.....	14
3.1.3 Types of Server.....	15
3.1.4 Internet Connections (Broadband).....	16
<b>4. Recommendations.....</b>	<b>17</b>
<b>5. Bibliography.....</b>	<b>18</b>

# 1. Overview

---

The aim of this documentation is to investigate the currently preferred methods for building a secure corporate network that includes local servers, an intranet, and a broadband Internet connection.

This report will contain recommended methods and a sample of a network security designs with a clearly labelled diagrams. Also, the source of the information in this report will be acknowledged and can be found at the end of this documentation.

If you find errors or omissions throughout the documentation, or perhaps have a better solution to possible problems, or have any other relevant ideas of improving the documentation, please email me so these changes may be incorporated into the document.

## 2. Network Security Methods

---

### 2.1.1 Introduction

The risks and threats to organizations with networked computer environments are on the increase. According to Matta Security limited, companies are being forced to embrace the Internet and the electronic channels that are built between un-trusted Internet-based hosts, and publicly accessible corporate servers.

Many organizations have been using the Internet to increase their productivity and also to attract more business via e-commerce online ordering of products. On the other hand, hackers, viruses and intruders have been using the Internet as a tool of damaging and stealing, which costs organizations a million of pounds every year.

Because of the sophisticated programs and untraceable viruses, which have been used by the hackers, there is no a single way or "silver bullet" of preventing hackers. As a result many organizations have been failing to keep intruders away from their systems.

However, there are ways of reducing these attacks by implementing a prevention approach.

The full spectrum of security embraces several phases <sup>1</sup>:

- Prevention
- Detection
- Recovery

Without a good planning or designing a secure network before anything else, it will be almost impossible to prevent attackers.

“Many people try to secure their network by installing a single tool, a "silver bullet" or "universal cure" to all their problems. They often install such a tool without much planning. It doesn't matter if the tools are a firewall, PKI system, smart cards, or other such tools. Without proper planning, testing, and maintenance, no such tool can present a true defense, or provide true security”<sup>2</sup>.

So before begin anything else is a good idea to:

- Develop a list of points of entry into your network
- Create a corporate security policy from which your network security policy will follow. Include policies on access to confidential and sensitive information, what actions are taken in the event of a breach, and by whom.

### **2.1.2 develop a network security policy:**

Starting with your corporate security policy, develop a network security policy. The following elements are recommended <sup>3</sup>:

- Create a firewall
- Isolate confidential information
- Create a demilitarized zone
- Develop an authentication scheme
- Develop an encryption system
- Develop a social engineering block system

### **2.1.3 Plan for IP security arithmetic**

IP security architecture (IPSec) is an open, standards-based security architecture that provides the following features:

- Data integrity (prevents attacks based on ill-formed data)
- Replay protection (prevents attacks based on replaying messages)
- Secure creation and automatic refresh of encryption keys
- Strong cryptographic algorithms
- Certificate-based authentication

### **2.1.4 Plan for virtual private networks**

Virtual private networks (VPNs) use IPSec to create a secure, private connection, or tunnel, through a public network such as the Internet. Several tools are available for each platform to turn ordinary Internet connections into VPNs. Considering the need for communication between remote users, branch offices, and corporate partners, VPNs are an important way to encrypt and authenticate information between remote nodes of the corporate network

### **2.1.5 Plan for virus and Spyware protection**

Viruses and other harmful software, called malware, disguises itself as legitimate business content, only to run malicious activity after it is inside the company network. Malware is the most pervasive form of network security breach. Each host on your network should be equipped with antivirus and antispymware applications that are updated weekly and run at least weekly. These programs are designed to block malware before it can replicate themselves over your network 4.

## 2.2 Firewalls

Simply put, a firewall is a system or group of systems that enforces an access control policy. Once you have determined that levels of connectivity you wish to provide, it is the firewall's job to insure that no additional access beyond this scope is allowed.

### Firewall types

According to Chris Brenton <sup>5</sup> (Author of Mastering Network Security) there are three types of Firewalls:

- Static packet filtering
- Dynamic packet filtering
- Proxy

#### 2.2.1 Static Packet Filtering

Static packet filtering controls traffic by using information stored within the packet headers. It can use the following information when regulating traffic flow:

- Destination IP address or subnet
- Source IP address or subnet
- Destination service port
- Source service port
- Flag (TCP only)

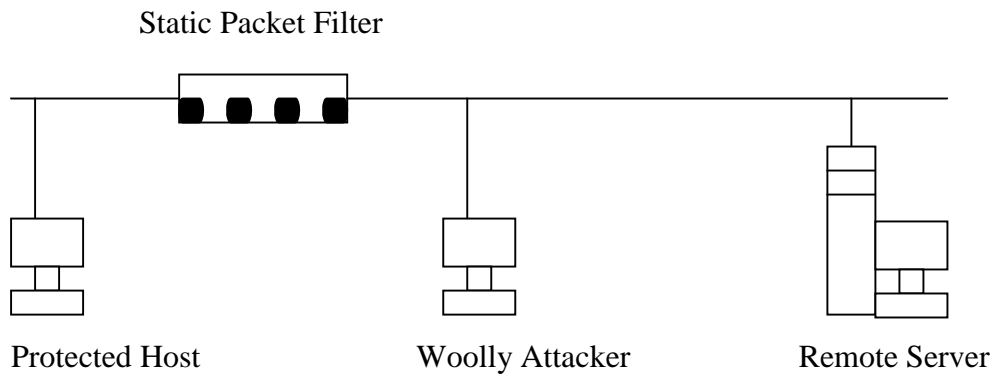
However, static packet filtering are non-intelligent filtering devices. They offer little protection against advanced types of attack. They look at a minimal amount of information in order to determine which traffic should be allowed to pass and which traffic should be blocked. Many routers have the ability to perform static packet filtering.

### 2.2.2 Dynamic Packet Filtering

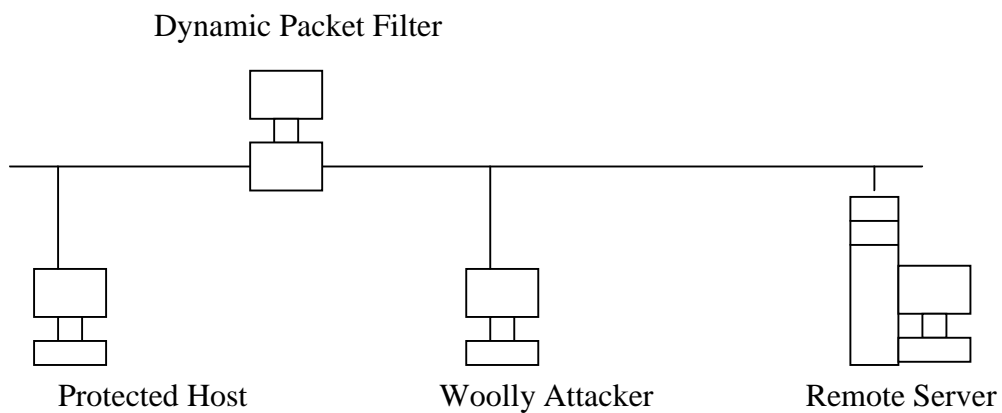
Dynamic filtering takes static packet filtering one step further by maintaining a connection table in order to monitor the state of a communication session. It does not simply rely on the flag settings. This is a powerful feature, which can be used to better control traffic flow.

*The differences between static and dynamic packet filtering*

*Example of A Static Packet Filter*



*Example of A Dynamic Packet Filter*



The figures above illustrate two separate network configuration. The first one its internal host is protected by static packet filter where the other is dynamic packets filter. The ACL on both firewalls may look something like this:

- Allow the protected host to establish any service sessions with the remote control.
- Allow any session that has already been established to pass.
- Drop all other traffic.

The first rule allows the protected host to establish connections to the remote server. This means that the only time a packet with the SYN bit set is allow to pass is if the source address is from the protected host and the destination is the remote server. When this is true, any service on the remote server many be accessed.

The second rule is a catchall. Basically it says, “If the traffic appears to be part of a previously established connection, let it pass.” In other words, all traffic is OK provided that the SYN bit is not set and all other bits are off.

Both Firewalling devices use the same ACL. The difference is in the amount of information each has available in order to control traffic.

Dynamic packet filters are intelligent devices that make traffic-control decisions based on packet attributes and state tables. State tables enable the Firewalling device to “remember” previous communication packet exchanges and make judgments based on this additional information.

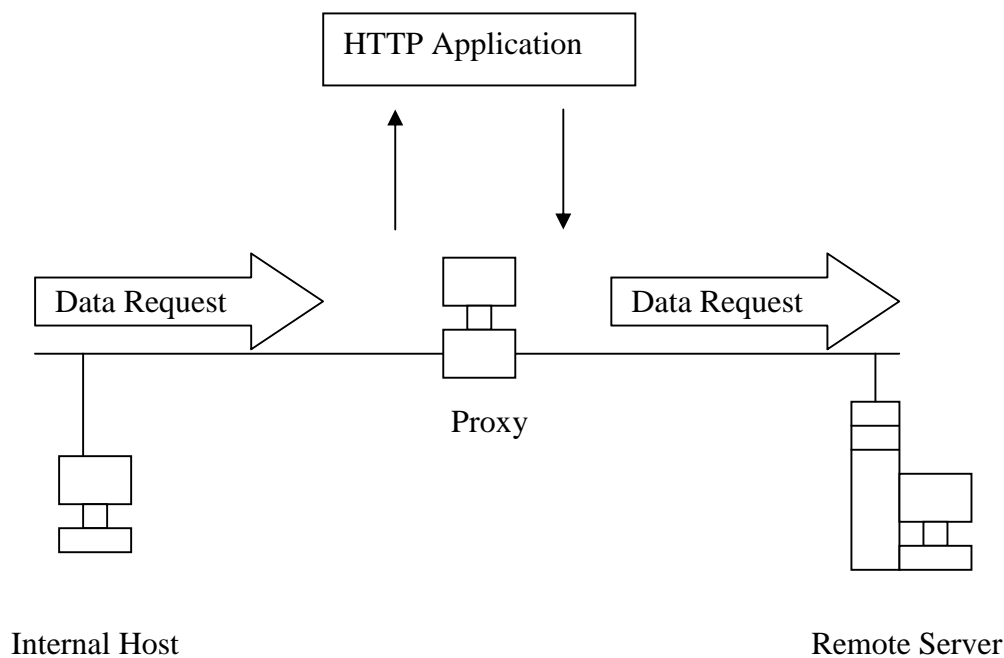
The biggest limitation of a dynamic packet filter is that it cannot make filtering decisions based upon payload, which is the actual data contained within the packet. In order to filter on payload, you must use a proxy-based firewall.

### 2.2.3 Proxies

A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between two network segments. Proxies are often used instead of filtering to prevent traffic from passing directly between networks. With the proxy acting as mediator, the source and destination systems never actually “connect” with each other. The proxy plays middleman in all connection attempts.

Unlike its packet-filtering counterparts, a proxy does not route any traffic. In fact, a properly configured proxy will have all routing functionality disabled. As its name implies, the proxy stands in or speaks for each system on each side of the firewall.

*A proxy mediating a communication session*



When internal host wishes to request a web page from the remote server, it formulates the request and transmits the information to the gateway leading to the remote network, which in this case is the proxy server.

Once the proxy receives the request, it identifies what type of service the internal host is trying to access. Since in this case the host has requested a Web page, the proxy passes the request to a special application used only for processing HTTP sessions. This application is simply a program running in memory that has the sole function of dealing with HTTP communications.

When the HTTP application receives the request, it verifies that the ACL allows this type of traffic. If the traffic is acceptable, the proxy formulates a new request to the remote server – only it uses itself as the source system. In the other hand, the proxy does not simply pass the request along; it generates a new request for the remote information.

This new request is then sent to the remote server. If the request were checked with a network analyzer, it would look like the proxy had made the HTTP request, not the internal host. For this reason, when the remote server responds, it responds to the proxy server.

Once the proxy server receives reply, it again passes the response up to the HTTP application. The HTTP application then scrutinizes the actual data sent by the remote server for abnormalities. If the data is acceptable, the HTTP application creates a news packet and forwards the information to the internal host.

As we can see, the two end systems never actually exchange information directly. The proxy constantly butts into the conversation to make sure that all goes securely.

#### 2.2.4 Firewall & Antivirus Softwares

There are also different types of Firewall and Antivirus softwares that widely available on the Internet. Some of these softwares are free and can be downloaded from the vendors' websites but others are shareware and need to be purchased before you can download.

The Most popular Firewall and Antivirus Softwares are:

- Norton Antivirus
- McAfee Firewall
- Zone Alarm
- Spayware Doctor
- Panda Antivirus
- The Shield Pro
- Ad-aware
- F-secure

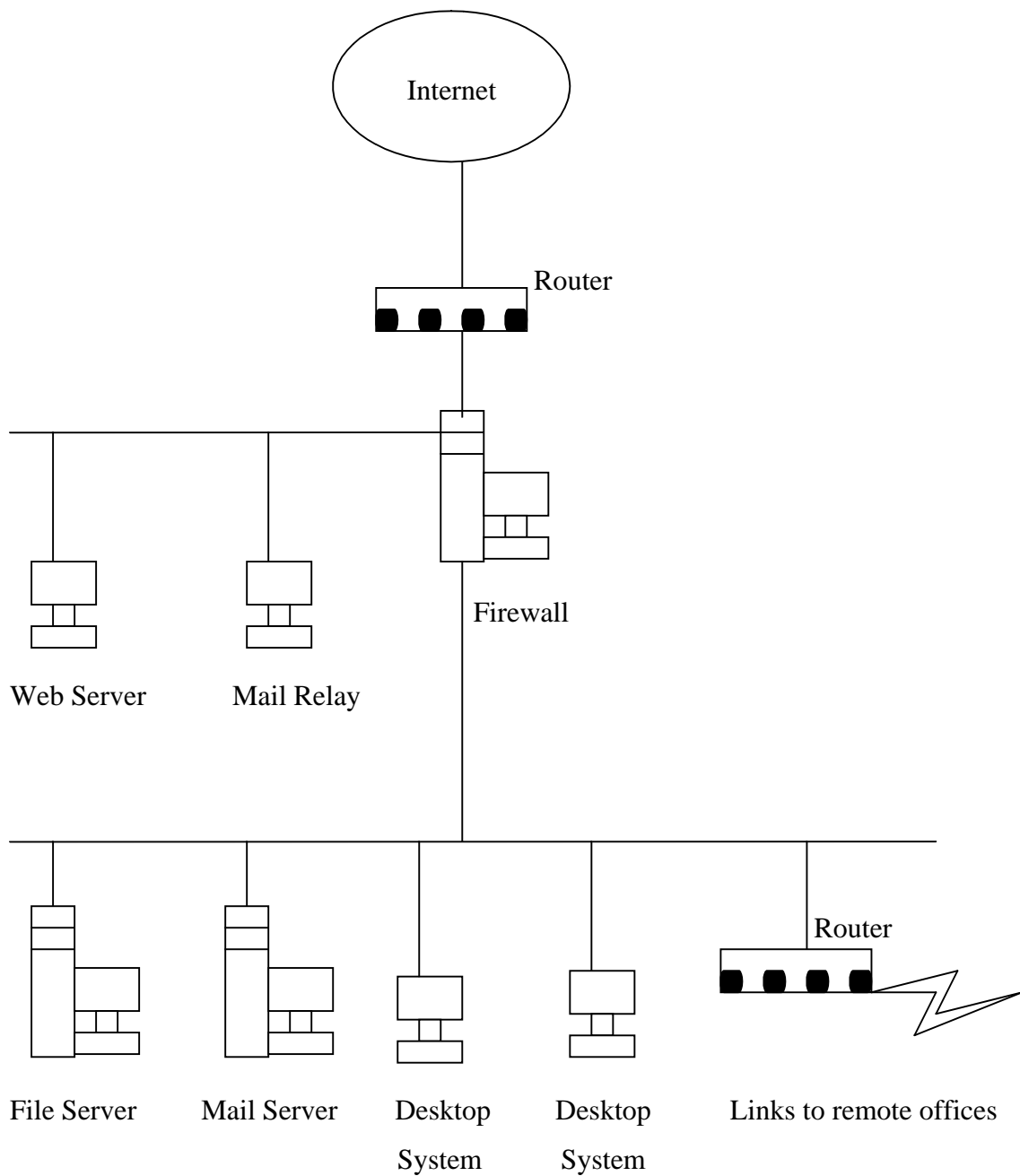
These softwares can be installed on any computer in the Network in order for protection and scanning viruses. Antivirus softwares' real benefit is to remove viruses, which might come from the internal users of the Network such as students and staff at the organization. Some antivirus softwares have both internal and external protection facilities using Firewalls.

# 3. Secure Network Designs

## 3.1.1 Example 1

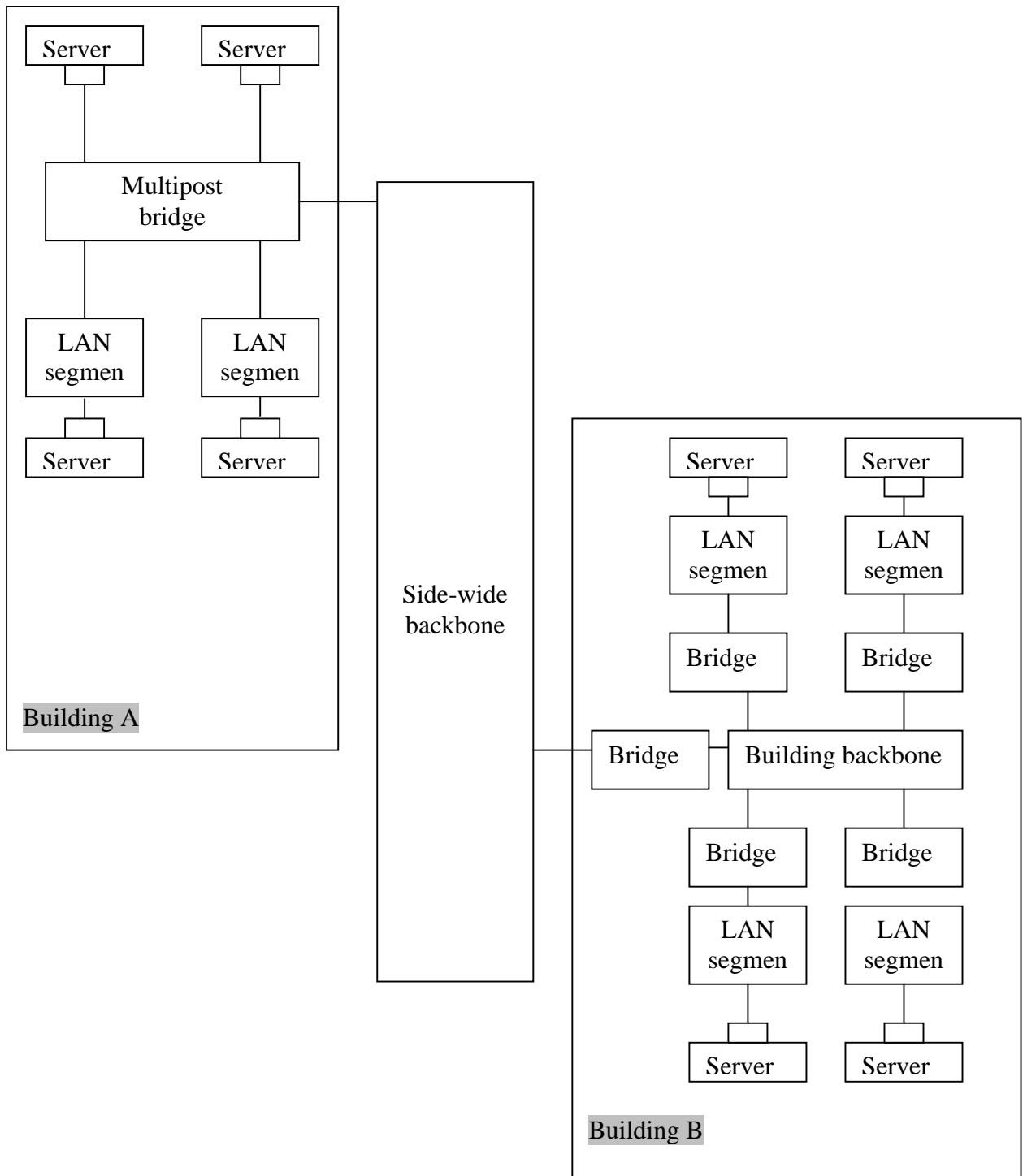
Figure 1[5]

While there are many different opinions on this topic according to Chris Brenton and Willian Stallings, the most common deployment is shown below.



### 3.1.2 Example 2

Figure 2 [7]



### 3.1.3 Types of Server

There are broadly three classes of server [8]:

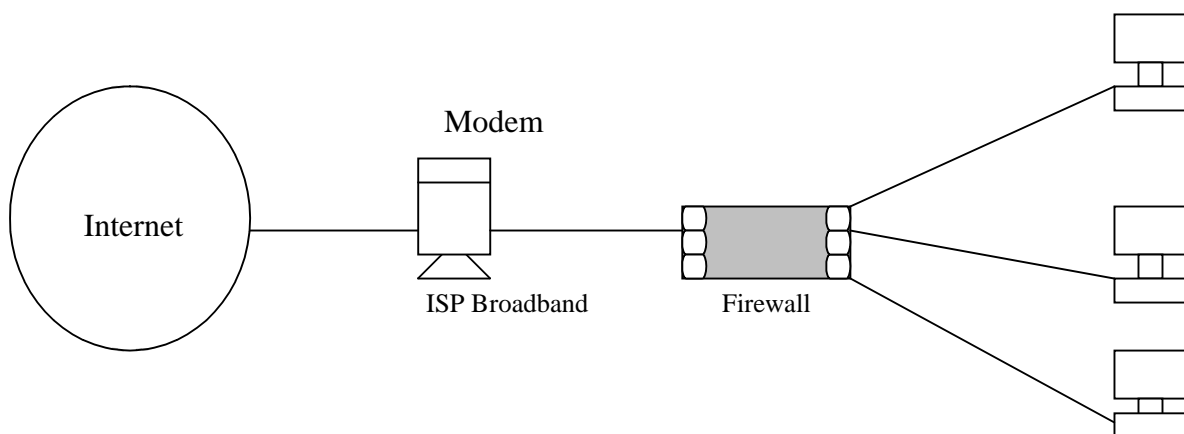
- **Device servers** – these share devices such as disk drives and printers to requesters
  - **Disk servers**
  - **File servers / Application servers**
  - **Printer servers**
  - **Modem servers**
- **Communications servers** – these provide message sending and receiving facilities on the network
  - **Email servers**
- **Management servers** – these provide organizational services such as password management and names for the network stations.
  - **Network synchronizers**
  - **Name servers**
  - **Permissions servers**

### 3.1.4 Broadband Internet Connection

Broadband in *general* refers to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission. In network engineering this term is used for methods where two or more signals share a medium [A5].

Nowaday, broadband is widely used and more computers being connected to the Internet via broadband. However, broadband users are more vulnerable to attacks compared with “dial-up users”. The reason is that Broadband connection is always “ON” and it can be easily attacked by viruses, intruders and Hackers unless protected properly.

#### Where to place broadband modem on the network?



For security reason it is essential to place a firewall, such as proxies between the systems and ISP modem. In this way we can eliminate any attacks using filtering routers and firewalls.

# 4. Recommendation

---

Without security measures and controls in place, data might be subject to an attack. These attacks can be passive, active, network based or Non-Network based attacks.

Using the following measures can help to prevent all these attacks:

- Consult with network experts before actually buying any network devices. This not only can help the organization to choose the right network devices but also to save them a lot of money.
- Use the latest virus protection software on each computer in the network. Also Anti-virus software should be frequently updated.
- User a Firewall such as a network appliance or a personal firewall package. Firewall softwares should be updated regularly. Also hardware Firewalls should be configured properly.
- Use the Internet only through Rooter firewalls and Proxies and don't connect the computers directly to broadband.
- It is also recommended the users such students and staff to be trained and well informed about virus and how to use the system safely.
- Disable java, JavaScript and ActiveX
- For web sites, use SSL.
- Always backup the necessary files, system files and configurations on the network.

These measures are the most recommended methods for network security. Using these methods will definitely help to reduce any potential attacks from the Internet.

# Bibliography

---

## *Web sites:*

- 1) <http://staff.washington.edu/gray/papers/credo.html>
- 2) <http://www.ph.utexas.edu/security/network-security.html>
- 3) 3...[http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/ip\\_hae\\_web/networksecurity.htm](http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/ip_hae_web/networksecurity.htm)
- 4) [http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphae\\_web/networksecurity.htm](http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphae_web/networksecurity.htm)
  
- A5) <http://en.wikipedia.org/wiki/Broadband>

## *Books*

- 5) Chris Brenton, 1999 "*Mastering Network Security*", US, Sybex inc.
- 6) William Stallings, 2000, "Network Security Essentials", US, Prentice-Hall, inc.
- 7) Fred Halshal, 1992, "Data Communication and Computer Network", US, Addison-wesley.
- 8) Mike James, 1989, "Low Cost PC Network", UK, Anchor Press ltd.

## References

[http://elias.decus.ch/presentations/ge\\_19970415\\_av/TSLD011.HTM](http://elias.decus.ch/presentations/ge_19970415_av/TSLD011.HTM) *Generic*

### *Firewall Functions*

A straightforward, simple outline of firewall functions, part of a sales presentation for the Alta Vista Firewall.

<http://www.ukiahsoft.com/securitywp.html> *NetRoad FireWALL White Paper*

A sales piece for the NetRoad FireWALL from Ukiah Software, Inc., containing a Firewall Primer with excellent descriptions of firewall types. More technical but it defines terms and is well written.

<http://www.infosecuritymag.com/fire.htm> *Fire in the Hole*

An August 1998 article by Edward Skoudis. Written for savvy readers but with lots of good basic information about firewalls and the then-current state of the firewall art.

[http://mmm.wiwi.hu-berlin.de/IMI/s\\_firewalls.html](http://mmm.wiwi.hu-berlin.de/IMI/s_firewalls.html) *Network Security and Firewalls*

Another good reference, which though highly technical explains more about what those "layers" are and how security works in each layer.

<http://www.examcram2.com/articles/article.asp?p=101741&seqNum=3&rl=1>